universität wien

DISSERTATION / DOCTORAL THESIS

Titel der Dissertation /Title of the Doctoral Thesis

„Rechtliche Fragestellungen in der nationalen Umsetzung der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-RL)“

verfasst von / submitted by

Ing.in Mag.a Sylvia Mayer, MA

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Doktorin der Rechtswissenschaften (Dr. iur.)

Wien, 2020 / Vienna 2020

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 783 101
Dissertationsgebiet lt. Studienblatt / field of study as it appears on the student record sheet:	Rechtswissenschaften
Betreut von / Supervisor:	Priv.-Doz. Dr. Bernhard Müller

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs	Absatz
ABL	Amtsblatt
AEC	Austrian Energy CERT
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AkkG	Akkreditierungsgesetz
AMG	Arzneimittelgesetz
APCIP	Austrian Programme for Critical Infrastructure Protection
Art	Artikel
BGBl	Bundesgesetzblatt
BKA	Bundeskanzler(amt)
BMG	Bundesministeriengesetz
BMI	Bundesminister(ium) für Inneres
BMLV	Bundesminister(ium) für Landesverteidigung
BMEIA	Bundesminister(ium) für Europa, Internationales und Äußeres
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
bspw	beispielsweise
BT-Drs.	Bundestagsdrucksache
BVerfGE	Entscheidung des Bundesverfassungsgerichts
B-VG	Bundes-Verfassungsgesetz
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
BWG	Bankwesengesetz
bzw	beziehungsweise
C4	Cyber Crime Competence Center

CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
COM	Commission
CSC	Cyber Security Center
CSIRT	Computer Security Incident Response Team
CSIS	Center for Strategic and International Studies
DDoS	Distributed Denial of Service
dh	das heißt
DIN	Deutschen Institut für Normung e.V.
DNS	Domain-Namen-Systeme
DuD	Datenschutz und Datensicherheit
DSB	Datenschutzbehörde
DSG	Datenschutzgesetz
DSGVO	Datenschutzgrundverordnung
DSP	Digital Service Provider
DSRL	Datenschutz-Richtlinie für die Strafverfolgung und Justiz
EB	Erläuternde Bemerkungen
EBA	European Banking Authority
EBG	Erdölbevorratungsgesetz
E-ControlG	Energie-Control-Gesetz
eIDAS-VO	Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
EisbG	Eisenbahngesetz
ElWOG	Elektrizitätswirtschafts- und –organisationsgesetz
EMRK	Europäische Menschenrechtskonvention

ENISA	Europäischen Agentur für Netz- und Informationssystemsicherheit
EPCIP	European Programme for Critical Infrastructure Protection
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUV	EU-Vertrag
evtl	eventuell
FIRST	Forum of Incident Response and Security Teams
FMA	Finanzmarktaufsicht
GehSO	Geheimschutzordnung des Bundes
gem	gemäß
GovCERT	Government Computer Emergency Response Team
GP	Gesetzgebungsperiode
GRC	Europäische Grundrechtecharta
Hrsg	Herausgeber
idF	in der Fassung
IEC	International Electrotechnical Commission
IKDOK	Innerer Kreis der Operativen Koordinierungsstrukturen
IKT	Informations- und Kommunikationstechnologien
IOC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protokoll
iSd	im Sinne des
ISO	International Organization for Standardization
IT	Informationstechnologie

ITSiG	IT-Sicherheitsgesetz
iVm	in Verbindung mit
iZm	in Zusammenhang mit
lit	litera
KWK	Kraft-Wärme-Kopplung
LNG	Liquefied Natural Gas
mE	meines Erachtens
MilCERT	Military Cyber Emergency Response Team
MS	Mitgliedstaaten
NIS	Netz- und Informationssystemsicherheit
NISG	Netz- und Informationssystemsicherheitsgesetz
NIS-RL	Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen
NISV	Netz- und Informationssystemsicherheitsverordnung
NV	Nutzungsverordnung
ÖBH	Österreichisches Bundesheer
OES	Operators of Essential Services
OGH	Oberster Gerichtshof
OpKoord	Operative Koordinierungsstruktur
ÖSCS	Österreichische Strategie für Cybersicherheit
ÖSS	Österreichische Sicherheitsstrategie
OTC	over the counter (im Sinne von OTC-Derivaten)
PolKG	Polizeikooperationsgesetz
PPP	Public Private Partnership
PSD	Payment Service Directive

PSG	Produktsicherheitsgesetz
PStSG	Polizeiliches Staatsschutzgesetz
RL	Richtlinie
RTR	Rundfunk und Telekom Regulierung
RV	Regierungsvorlage
Rz	Randziffer
SKI	Schutz kritischer Infrastruktur
SKKM	Staatliches Krisen- und Katastrophenmanagement
Slg	Sammlung
SPG	Sicherheitspolizeigesetz
SPoC	Single Point of Contact
StGG	Staatsgrundgesetz
StPO	Strafprozeßordnung
stRsp	ständige Rechtsprechung
SWP	Stiftung Wissenschaft und Politik
TKG	Telekommunikationsgesetz
TLD	Top-Level-Domain
ua	unter anderem
VfGH	Verfassungsgerichtshof
VfSlg	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des Verfassungsgerichtshofes
Vgl	vergleiche
VO	Verordnung
VStG	Verwaltungsstrafgesetz
VwGH	Verwaltungsgerichtshof

Z	Ziffer
ZaDiG	Zahlungsdienstegesetz
zT	zum Teil

1. Einleitung

Unsere Gesellschaft ist in zunehmendem Maße von bestimmten Diensten und Technologien abhängig.[1] Strom, Wasser, Bargeld oder Gesundheitsleistungen als so genannte kritische Infrastrukturen sorgen für die Daseinsvorsorge[2] und das Funktionieren unserer Gesellschaft. Sie haben im Konzept der zivilen Sicherheit ihren festen Platz[3] und Ausfälle bzw. Störungen dieser Unternehmen können sich unmittelbar auf viele Menschen und auf schwerwiegende Art und Weise auswirken. Ebendiese Dienste sind jedoch mittlerweile in hohem Maße abhängig von der Informations- und Kommunikationstechnologie (IKT).[4] Energienetze und Wasserpumpen werden über zentrale Server gesteuert, Patientendaten in Krankenhäusern ausschließlich über digitale Systeme verwaltet und Transaktionen mehrheitlich über bargeldlosen Zahlungsverkehr abgewickelt. Darüber hinaus zählt das Internet zur Grundlage unserer zivilen und wirtschaftlichen Gesellschaft. Es gibt nur mehr einen sehr geringen Anteil von Menschen, der nicht täglich im Internet arbeitet, seine Mails abruft oder über soziale Netzwerke kommuniziert. Experten gehen davon aus, dass bis zum Jahr 2020 mehr als 50 Milliarden Geräte miteinander vernetzt sein werden: von Smartphones über Autos bis hin zu Industriemaschinen.[5] Dieses so genannte Internet of Things (IoT)[6] birgt ebenso viele Gefahren, wie beispielsweise 2017 das Mirai-Botnetz gezeigt hat. Dabei wurden IoT-Geräte wie Netzwerkkameras und Heimrouter (120.000 Systeme in den ersten 24 Stunden) gehackt und für Distributed Denial-of-Service Attacken genutzt, um Websites und Webdienste durch eine große Anzahl gleichzeitiger Abfragen zu überlasten.[7] In dem Maß, in dem die Bevölkerung sehr hohe Sicherheitsstandards und eine hohe Versorgungssicherheit gewohnt ist, sind die Auswirkungen eines „Dennoch-Störfalls“ überproportional hoch.[8]

Aus all diesen Gründen ist die Informations- und Kommunikationstechnologie eine der wichtigsten Grundpfeiler unserer Gesellschaft – und muss entsprechend vor Ausfällen und Angriffen geschützt werden.

---

[1] Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 final.

[2] *Wolff*, Zivile Sicherheit als Infrastrukturgewährleistung und Daseinsvorsorge, in Gusy/Kugelmann et al. (Hrsg), Rechtshandbuch Zivile Sicherheit (2017), Rz 6..

[3] *Engels*, Zivile Sicherheit in Kritischen Infrastrukturen - Öffentliche Netze, in Gusy/Kugelmann et al. (Hrsg), Rechtshandbuch Zivile Sicherheit (2017), Rz 1.

[4] *Grudzien*, IT-Sicherheitsgesetz - Gedanken zur Implementierung, Datenschutz und Datensicherheit - DuD, 1/2016, S. 29.

[5] *Abolhassan*, Security Einfach Machen, IT-Sicherheit als Sprungbrett für die Digitalisierung (2017), S. V.

[6] *Pohlmann*, Zur Entwicklung einer IT-Sicherheitskultur, Datenschutz und Datensicherheit - DuD, 1/2016, S. 38.

[7] *Klein-Hennig/Schmidt*, Zurück auf Los - Die IT-Sicherheit zurück in der Steinzeit, Datenschutz und Datensicherheit - DuD, 2017, S. 605.

[8] *Wiater*, Bürger und Unternehmen als Akteure der Zivilen Sicherheit, in Gusy/Kugelmann et al. (Hrsg), Rechtshandbuch Zivile Sicherheit (2017), Rz 5.

Grundsätzlich muss zwischen Cyberkriminalität im eigentlichen Sinn und Cyberkriminalität im erweiterten Sinn unterschieden werden[9], wobei sich die gegenständlich dargestellten und in der Arbeit umfassten Risiken auf die erste Kategorie beschränken und dabei beispielsweise Hacking, Cyber-Vandalismus und die Verbreitung von Viren inkludiert.

Die Bedrohung von Cyber-Angriffen ist in den letzten Jahren stark gestiegen und wird auch in den kommenden Jahren das größte Risiko[10] für Wirtschaft und Bevölkerung darstellen.[11] Die wirtschaftlichen Schäden durch Cyberangriffe schätzt das Center for Strategic and International Studies (CSIS) weltweit auf mehr als 400 Milliarden Euro pro Jahr[12]; in Österreich haben 72 % der Unternehmen in einer im Jahr 2017 durchgeführten Umfrage angegeben, in den letzten 12 Monaten Versuche von Cyberangriffen festgestellt zu haben.[13] 69 % der Unternehmen in Europa haben kein oder nur grundlegendes Verständnis ihrer Verletzlichkeit durch Cyber-Risiken.[14] Darüber hinaus haben auch die Möglichkeiten der Kriegsführung im Cyberraum den Charakter des modernen Konflikts grundlegend verändert.[15]

Aufgrund der steigenden Zahl von Geräten mit Verbindung zum Internet steigt auch deren Verwundbarkeit. Durch spezialisierte Suchmaschinen im Internet, wie beispielsweise Shodan[16], können Industrie-Steuerungsanlagen gefunden und mit entsprechenden Mitteln angegriffen oder deaktiviert werden. Beispielsweise wurde das industrielle Steuerungssystem einer Urananreichungsanlage im Iran 2010 durch eine komplexe Malware (Stuxnet) angegriffen und signifikant beschädigt.[17] Im Dezember 2015 waren im Zuge einer Attacke auf das ukrainische Stromnetz mehr als 700.000 Haushalte zeitweise ohne Strom.[18] Eine Studie über die Gefahr eines großräumigen und lang andauernden Ausfalls der Stromversorgung kommt zum Ergebnis, dass bereits bei einem Stromausfall von nur wenigen Tagen die flächendeckende und bedarfsgerechte

[9] McGuire/Downling, "Cyber Crime: a review of the evidence," (2013), S. 4.
[10] Zur besonderen Gefahr durch gezielte Angriffe, insbesondere solche mit nachrichtendienstlichem, politischem oder ethischem Hintergrund, siehe *Könen*, IT-sicherheit gesetzlich geregelt, Datenschutz und Datensicherheit - DuD, 1/2016, S. 12.
[11] Mehr zur Situation in Deutschland in *Bundesamt für Sicherheit in der Informationstechnik*, „Die Lage der IT-Sicherheit in Deutschland“, 2018.
[12] *Abolhassan*, Security Einfach Machen, IT-Sicherheit als Sprungbrett für die Digitalisierung, S. VI.
[13] Statista 2018, Hat Ihr Unternehmen in den letzten 12 Monaten Versuche von Cyberangriffen festgestellt?, https://de.statista.com/statistik/daten/studie/552445/umfrage/erfahrungen-von-oesterreichischen-unternehmen-mit-cyber-angriffen/, abgerufen am 05.05.2019.
[14] *European Commission*, State of the Union 2017 - Factsheet Cybersecurity.
[15] *Ischinger*, Sicherheitspolitik: Regeln für den Cyberraum, in Abolhassan (Hrsg), Security Einfach Machen (2017), S. 14.
[16] *Simon/Moucha*, Verwundbarkeitsprüfungen mit Shodan, Datenschutz und Datensicherheit - DuD, 2016, S. 723.
[17] *Klimburg/Tirmaa-Klaar*, Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for action within the EU, 2011, S. 54.
[18] *Ischinger* in Abolhassan, Security Einfach Machen, S. 15.

Versorgung der Bevölkerung mit lebensnotwendigen Gütern und Dienstleistungen nicht mehr gewährleistet werden kann.[19] Europäische Telekommunikationsbetreiber konnten im Jahr 2017 169 Vorfälle mit beträchtlichen Auswirkungen verzeichnen, wobei Systemfehler für 62 % der Vorfälle verantwortlich waren.[20]

Der Staat ist in diesem Umfeld ein Akteur von vielen (neben bspw. Innovatoren, Betreibern und Dienstleistern, Wirtschaft und Privaten als Nutzern). Ebenso müssen daher auch alle anderen Akteure ihre Verantwortung jeweilig wahrnehmen. Dennoch kommt dem Staat auch weiterhin eine besondere Rolle bei der Absicherung grundrechtlicher und wirtschaftlicher Freiheiten zu.

Die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (kurz NIS-RL)[21], gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union (AEUV), insbesondere auf Art. 114[22], wurde auf Vorschlag der Europäischen Kommission aus Februar 2013, nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente, nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses, gemäß dem ordentlichen Gesetzgebungsverfahren am 6. Juli 2016 beschlossen und im August 2016 im Amtsblatt der Europäischen Union kundgemacht bzw. veröffentlicht.[23]

Ziel der Richtlinie ist vor allem, das allgemeine Niveau der Netz- und Informationssicherheit zu erhöhen und so zum Funktionieren des Binnenmarktes beizutragen.
Dazu soll jeder Mitgliedsstaat eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festlegen und nationale Behörden einrichten, die für die Umsetzung der festgelegten Maßnahmen verantwortlich sind. Darunter fallen unter anderem die Koordination der österreichischen Strategie, die Wahrnehmung der grenzüberschreitenden Zusammenarbeit als Single Point of Contact (SPoC), die Entgegennahme und Analyse von Meldungen über signifikante Sicherheitsvorfälle, die Erstellung von Lagebildern über diese Vorfälle sowie die Überprüfung der Sicherheitsmaßnahmen in Unternehmen.

Der Anwendungsbereich der Richtlinie gliedert sich in Betreiber wesentlicher Dienste und Anbieter digitaler Dienste. Unter den Betreibern wesentlicher Dienste werden so genannte kritische Infrastrukturen aus den Bereichen Energie, Transport, Wasser, Gesundheit, Digitales, Bankwesen

[19] *Klett/Ammann*, Gesetzliche Initiativen zur Cybersicherheit, Computer und Recht, 2/2014.
[20] Annual Incident Reports 2017, https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017, abgerufen am 06.09.2018.
[21] Richtlinie (EU) 2016/1145 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl 2016 L 194/1.
[22] Mehr zum rechtlichen Hintergrund im Primärrecht siehe Kapitel 6.2.
[23] *Anderl/Heußler/Mayer et al.*, NISG::Kommentar (2019), Einleitung, Rz 1.

und Finanzmarktinfrastrukturen verstanden, die eine wesentliche Bedeutung für die Aufrechterhaltung gesellschaftlicher Funktionen haben und deren Ausfall oder Störung schwerwiegende Auswirkungen auf die Bevölkerung haben könnte. Anbieter digitaler Dienste sind in der Richtlinie als Online-Marktplätze, Online-Suchmaschinen und Cloud Service Provider geregelt.

Diese Betreiber und Anbieter werden konkreten Verpflichtungen unterworfen, nämlich der Meldung schwerwiegender Störfälle in ihren IKT-Systemen[24] sowie das Treffen geeigneter technischer und organisatorischer Sicherheitsmaßnahmen[25], um Ausfälle zu verhindern.

2. Grundlagen der Untersuchung

2.1. Untersuchungsbedingungen

Die NIS-RL musste von den Mitgliedsstaaten bis spätestens Mai 2018 in nationales Recht umgesetzt werden. Dementsprechend wurde bereits im Februar 2016 unter der Federführung des Bundeskanzleramtes eine interministerielle Arbeitsgruppe eingesetzt, die an einem Entwurf für das sogenannte Bundesgesetz zur Gewährleistung der Sicherheit von Netz- und Informationssystemen arbeitete.[26] Parallel dazu entwickelte auf europäischer Ebene die EU-Kooperationsgruppe (Vertreter aller Mitgliedsstaaten sowie der Europäischen Kommission) Dokumente zur Unterstützung der Mitgliedsstaaten, vor allem in Bezug auf die Identifizierung der Betreiber wesentlicher Dienste.[27]

Ursprüngliches Ziel dieser Arbeit war die Untersuchung der NIS-RL, die Untersuchung verfassungsrechtlicher und einfachgesetzlicher Rahmenbedingungen im nationalen Recht und die Erarbeitung rechtlicher Umsetzungsoptionen.

Aufgrund des Umstandes, dass das Bundesgesetz zur Umsetzung der Richtlinie mit 28. Dezember 2018 im BGBl. I Nr. 111/2018 vor Finalisierung gegenständlicher Dissertation kundgemacht wurde, wird das Gesetz sodann in die Betrachtungen der Dissertation mit aufgenommen. Nichtsdestotrotz werden alle Umsetzungsoptionen der NIS-RL sowie rechtliche Fragestellungen im Rahmen der Umsetzung diskutiert.

[24] Siehe dazu Kapitel 7.5.6.
[25] Siehe dazu Kapitel 7.5.4.
[26] Verfasserin dieser Arbeit (Mitarbeiterin im Bundesministerium für Inneres) weist dieses Wissen aufgrund der Mitarbeit in dieser Arbeitsgruppe auf.
[27] Siehe dazu bspw. Reference document on Incident Notification for Operators of Essential Services, 2018.

Anzumerken ist außerdem, dass die Verfasserin dieser Arbeit als eine von vier AutorInnen (Axel *Anderl, Vinzenz Heußler, Sylvia Mayer, Bernhard Müller)* am ersten Gesetzeskommentar zum NIS-Gesetz[28] mitwirkte und dieser im November 2019 veröffentlicht wurde.[29] Da in diesen Kurzkommentar einige Ideen der gegenständlichen wissenschaftlichen Arbeit eingeflossen sind, wird teilweise darauf verwiesen und die dort vertretenden Meinungen näher ausgeführt bzw. rechtlich begründet.

2.2. Forschungsinteresse und Forschungsfragen

Die Umsetzung der Richtlinie in nationales Recht muss mit der bereits bestehenden nationalen Rechtslage im Einklang stehen. Einerseits sind bestehende verfassungsrechtliche und einfachgesetzliche Normen, die den Schutz kritischer Infrastruktur und Cybersicherheit oder sonstige Rahmenbedingungen regeln, zu berücksichtigen. Ebenso sollte bei Vorliegen mehrerer Optionen zur Umsetzung jene gewählt werden, die aufgrund existierender Strukturen und Organisationen am besten geeignet erscheint, wobei dies in der Arbeit zu beleuchten und diskutieren sein wird. Dabei wird auch ein Blick auf die (verfassungs-)rechtlichen Zuständigkeiten sowohl der Sicherheitsbehörden als auch des Österreichischen Bundesheeres sowie deren Abgrenzung voneinander geworfen.

In gegenständlicher Arbeit zu untersuchen sind auch kompetenzrechtliche Zuständigkeiten der Europäischen Union, des Bundes und der Länder. Die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit – als möglicherweise primärer Kompetenztatbestand der Cybersicherheit – ist gemäß Art. 10 Abs. 1 Z 7 B-VG sowohl in Gesetzgebung als auch Vollziehung Zuständigkeit des Bundes, wodurch die Umsetzung der Richtlinie in Form eines Bundesgesetzes unproblematisch sein könnte. Daneben bestehen jedoch auch kompetenzrechtliche Zuständigkeiten der Länder in verschiedenen Materien, wie beispielsweise dem Sektor Gesundheit sowie dem Elektrizitätswesen. Dabei wird zu untersuchen sein, ob eigene landesgesetzliche Regelungen notwendig sein werden.

Die verfassungsrechtliche Auseinandersetzung wird sich außerdem auf die Frage des Eingriffs in Grundrechte durch weitgehende Verpflichtungen für Unternehmen beziehen und insbesondere deren Verhältnismäßigkeit untersuchen.

Ein zentraler Punkt der Richtlinienumsetzung ist deren Anwendungsbereich. Dazu müssen die Mitgliedsstaaten entsprechend den Vorgaben der NIS-RL ihre nationalen Betreiber identifizieren,

[28] Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), StF BGBl. I Nr. 111/2018.
[29] *Anderl et al.*, NISG::Kommentar.

die einen wesentlichen Dienst erbringen. Dazu bestehen innerstaatlich theoretisch mehrere Möglichkeiten. Dies könnte durch Veröffentlichung einer Liste als Verordnung[30], als „Selbst-Identifizierung“ [31] der Betreiber oder durch Kundmachung von Kriterien und Identifizierung der Behörden durch Bescheid[32] umgesetzt werden.

Weitere rechtliche Fragen im Zuge der Umsetzung könnten sich in Bezug auf bereits bestehende Verpflichtungen zur Meldung von sicherheitsrelevanten Vorfällen sowie bestehende verpflichtende Sicherheitsstandards für Unternehmen in der österreichischen Rechtsordnung stellen, wobei zu untersuchen sein wird, ob sich diese Verpflichtungen widersprechen oder Möglichkeiten bestehen, diese im Rahmen einer Verwaltungsvereinfachung zusammenzuführen.

Darüber hinaus ist den Mitgliedsstaaten die Höhe der Sanktionierung der Verwaltungsübertretungen offengehalten. Orientiert man sich hierbei an der Datenschutzgrundverordnung (DSGVO)[33] und deren Strafhöhen, kommt es zu unverhältnismäßigen Differenzen zu den Geldstrafen im nationalen gerichtlichen Strafrecht. Andererseits erscheint ein zu großer Unterschied zu den Strafen der DSGVO wenig zielführend, da dort ebenso Meldepflichten und Sicherheitsvorkehrungen hinsichtlich Daten und Systemen[34] geregelt werden. Ebenso wird der für Meldeprozesse erforderliche Austausch von personenbezogenen Daten (IP-Adressen) zwischen privaten Unternehmen und das dabei bestehende Verhältnis zur Datenschutzgrundverordnung anzusprechen sein.

Eine für die Unternehmen wichtige Frage stellt die Geltung des Prinzips der Amtswegigkeit nach den Bestimmungen der Strafprozessordnung (StPO)[35] im Rahmen der Meldepflicht dar, demnach die Kriminalpolizei bei jedem Verdacht einer Straftat Ermittlungen einzuleiten hat. Da dies nicht immer im Interesse der Betreiber liegt, wird im Rahmen der Arbeit nach rechtlichen Möglichkeiten gesucht, diese Ermittlungspflicht – insbesondere bei freiwilligen Meldungen – hintanzuhalten.

[30] Dies würde wohl dem Schutz der Betreiber zuwiderlaufen, da die Veröffentlichung einer Liste erst recht potenzielle Angriffsziele für Angreifer darstellen könnte.
[31] Wurde in dieser Form in Deutschland im IT-Sicherheitsgesetzt umgesetzt; siehe Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), BGBl. I 31/2018 (Deutschland).
[32] Aufwändiges behördliches Verfahren mit der Herausforderung der jährlichen Evaluierung.
[33] Mehr zur DSGVO siehe Kapitel 7.5.2.7.
[34] Die DSGVO regelt Meldepflichten für Vorfälle, bei denen personenbezogene Daten betroffen sind sowie Sicherheitsvorkehrungen für Systeme, in denen personenbezogene Daten verarbeitet werden; mehr zur Abgrenzung in Kapitel 7.5.6.9.
[35] Strafprozessordnung 1975 (StPO), BGBl. Nr. 631/1975 idF BGBl. I Nr. 70/2018.

Nicht Bestandteil des Gegenstandes dieser Untersuchung sollen aufgrund deren Umfanges die datenschutzrechtlichen Bestimmungen des NIS-Gesetzes sein, da es sich dabei um einen separaten Untersuchungsgegenstand handelt.

Darüber hinaus wird die Umsetzung zu den Anbietern digitaler Dienste nicht näher beleuchtet, da dem nationalen Gesetzgeber in diesem Bereich kaum Umsetzungsmöglichkeiten gegeben werden (Vollharmonisierung).[36]

Im Rahmen der gegenständlichen wissenschaftlichen Arbeit sollen somit folgende Forschungsfragen untersucht werden:

- Welche nationalen Regelungen bestehen bereits hinsichtlich des Schutzes kritischer Infrastruktur und der Cybersicherheit und auf welche verfassungsrechtlichen Kompetenzen stütze sich diese Regelungen?
- Auf welche Kompetenz stützen sich die Regelungen der NIS-RL im Primärrecht der EU bzw. kommt es dadurch möglicherweise zu einem Ausweiten an Kompetenzen im Bereich der Sicherheit?
- Welche nationalen Umsetzungsoptionen ermöglicht die NIS-RL bzw. in welcher Form kann die Umsetzung in nationales Recht erfolgen?
- Welche rechtlichen (insb. auch verfassungsrechtlichen) Schwierigkeiten und Fragestellungen ergeben sich aufgrund der bestehenden österreichischen Rechtslage im Zuge der Umsetzung im NIS-Gesetz?

2.3. Methodische Vorgangsweise

Die gegenständliche Arbeit wurde grundsätzlich in drei größere Bereiche gegliedert. Dem Leser soll dabei durch einen Einblick in die aktuelle Gesetzeslage und die nationalen Strukturen am Beginn der Einstieg in die rechtliche Diskussion erleichtert werden.

Die rechtliche Untersuchung wird sich auf kompetenzrechtliche Tatbestände sowohl auf EU- als auch nationaler Ebene als auch verfassungsrechtliche Fragen der Umsetzung stützen und in weiterer Folge die einzelnen Tatbestände des NIS-Gesetzes in Gegenüberstellung mit den Regelungen der NIS-RL näher beleuchten.

[36] Siehe insb. ErwGr 48, 49, 53, 54 NIS-RL.

Im ersten Teil erfolgte eine Untersuchung der nationalen Rechtslage nach bereits bestehenden Regelungen, die im Zuge der Umsetzung berücksichtigt werden müssen, sowie der Schnittstellen zu sonstigen zu beachtenden EU-Rechtsakten.[37]

Im zweiten Teil werden die Regelungen zu Cybersicherheit auf EU-Ebene untersucht, wobei insbesondere ein Fokus auf die Kompetenzregelung im Primärrecht gelegt werden soll.[38]

Im dritten Teil der Arbeit werden die Regelungen des NIS-Gesetzes sowie deren Erläuternde Bemerkungen vollständig durch eine systematische Inhaltsanalyse (qualitativ, deduktiv) erfasst, diskutiert sowie den Vorgaben der NIS-RL und deren Erwägungsgründen gegenübergestellt. Kernbereich dieser Diskussion sind die verschiedenen Optionen der Umsetzung in nationales Recht sowie rechtliche Fragestellungen und Schwierigkeiten, die sich durch in Kraft befindliche nationale Normen ergeben, und die rechtsdogmatisch analysiert und beantwortet werden.[39]

3. Schutz kritischer Infrastruktur und Cybersicherheit in Österreich

3.1. Schutz kritischer Infrastruktur in Österreich

Der Schutz kritischer Infrastruktur und die Cybersicherheit sind in der aktuellen Österreichischen Sicherheitsstrategie an mehreren Stellen erwähnt. Angriffe auf die Sicherheit der IT-Systeme und die Bedrohung strategischer Infrastruktur stellen Herausforderungen, Risiken und Bedrohungen für Österreich dar. Im Rahmen der festgelegten sicherheitspolitischen Werte ist die Sicherstellung der Versorgung der Bevölkerung mit lebensnotwendigen Gütern sowie der Schutz kritischer Infrastrukturen ein zentrales Interesse und politisch-strategisches Ziel Österreichs.[40]

Der Schutz kritischer Infrastruktur ist in Österreich grundsätzlich im Österreichischen Programm zum Schutz kritischer Infrastruktur (APCIP)[41] aus 2014 festgelegt. Die erste diesbezügliche Strategie entstand am 2. April 2008 (Masterplan APCIP 2008)[42] in Anlehnung an das Europäische Programm zum Schutz kritischer Infrastruktur (EPCIP)[43], welches im Jahr 2006 durch die Europäische Kommission entwickelt wurde.

[37] Kapitel 3 und 4.2.4.
[38] Kapitel 6.2.
[39] Kapitel 7.
[40] *Bundeskanzleramt*, Österreichische Sicherheitsstrategie, 2013, S. 7, 9.
[41] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014.
[42] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2008.
[43] Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen, COM(2006) 786 final. Zur Europäischen Richtlinie zum Schutz kritischer Infrastruktur RL 114/2008 siehe Kapitel 5.1.

Im Programm (APCIP) werden kritische Infrastrukturen als jene Infrastrukturen (Systeme, Anlagen, Prozesse, Netzwerke oder Teile davon) definiert, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde.[44]

Im neuen Masterplan aus 2014 werden - im Gegensatz zum Programm aus 2008 - keine Sektoren aufgelistet, denen die Betreiber kritischer Infrastruktur zugeordnet werden könnten. Der Masterplan aus 2008 definierte – auch aus dem Europäischen Programm abgeleitet – noch die zwölf Teilbereiche Energie, Informations- und Kommunikationstechnologien, Wasser, Lebensmittel, Gesundheit, Finanzen, Transport, Chemische Industrie, Forschungseinrichtungen, Verfassungsmäßige Einrichtungen, Sozial- und Verteilsysteme und Hilfs- und Einsatzkräfte.

Als Kriterien für die Einstufung kritischer Infrastrukturen wurden unter anderem die Anzahl der betroffenen Bürger, wirtschaftliche Auswirkungen, die zeitliche Dauer, mangelnde Substitutionsmöglichkeiten sowie bestehende Interdependenzen angeführt.[45]

In Bezug auf gegenständliches Programm zum Schutz kritischer Infrastrukturen stellt sich die Frage nach dessen rechtlicher Natur. Das Programm wurde erstmals am 2. April 2008[46] und in aktualisierter Form am 4. November 2014[47] von der Bundesregierung aufgrund eines Ministerratsvortrags beschlossen. Der Ministerrat ist die Tagung der Bundesregierung als kollegiales Verwaltungsorgan des Bundes unter Vorsitz des Bundeskanzlers.[48] *Raschauer* führt dazu an, dass der für den jeweiligen Fachbereich zuständige Bundesminister für die Durchführung der Beschlüsse der Bundesregierung im Ministerrat verantwortlich ist.[49] Bei diesen Beschlüssen kann meines Erachtens somit von Weisungen des jeweils zuständigen Bundesministers an seine nachgeordneten Organe ausgegangen werden. Aufgrund des Charakters einer Weisung liegt keine Außenwirkung, beispielweise für Unternehmen der kritischen Infrastruktur, vor.[50]

Das Programm zum Schutz kritischer Infrastruktur in der Form eines Ministerratsvortrages ist damit mE eine (interne) Weisung an die nachgeordneten Organe des für den jeweiligen Fachbereich zuständigen Bundesministers.

---

[44] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, 6.
[45] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2008, S. 6.
[46] Ministerratsvortrag 48/17 vom 27. März 2008.
[47] Ministerratsvortrag 38/5 vom 30. Oktober 2014.
[48] *Raschauer*, Allgemeines Verwaltungsrecht[3] (2009), Rz 249.
[49] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 250.
[50] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 947.

3.1.1. Prinzipien

Der Schutz kritischer Infrastruktur erfolgt in Österreich anhand der im Programm festgelegten Prinzipien, von denen aufgrund deren rechtlicher Bedeutsamkeit einige zu nennen sein werden. Das Prinzip der Subsidiarität und Selbstverpflichtung der Unternehmen legt fest, dass Eigentümer und Betreiber kritischer Infrastruktur in erster Linie selbst für die Aufrechterhaltung ihrer Leistungen und den Schutz ihrer Einrichtungen/Anlagen verantwortlich sind. Aufgrund des nationalen Interesses an der Versorgungsfunktion dieser Betreiber[51] sollen sich diese in einer (freiwilligen) Selbstverpflichtung zu einer erhöhten Resilienz und damit zu Schutzstandards bekennen, die für ihre Branche gemeinsam definiert wurden. Aufgrund dessen sind Politik und Verwaltung für die Gestaltung der Rahmenbedingungen verantwortlich, um dadurch ein klar definiertes Schutzziel zu erreichen. [52]

Das Prinzip der Vertraulichkeit regelt, dass Informationen nur auf Basis von Vertraulichkeit ausgetauscht werden[53] und nur in jener Informationstiefe vorliegen, die die jeweilige Aufgabenstellung erfordert und das Prinzip der Verhältnismäßigkeit legt fest, dass Kosten und Maßnahmen zur Erhöhung des Schutzniveaus in einem ausgeglichenen Verhältnis[54] zum jeweiligen Risiko und zu den Möglichkeiten zur Gefahrenminderung stehen sollen.[55]

Der Schutz kritischer Infrastruktur in Österreich unterliegt darüber hinaus dem all-hazards-approach. Demnach sollen kritische Infrastruktur vor einem breiten Spektrum möglicher Gefahren geschützt werden, von intentionalen Angriffen über Störungen und Naturkatastrophen.[56]

Als strategisches Ziel werden im Österreichischen Programm zum Schutz kritischer Infrastruktur resiliente Unternehmen[57] definiert, wodurch ein Beitrag zur gesamtstaatlichen Resilienz Österreichs geleistet werden soll.[58] Diese Resilienz soll grundsätzlich durch eine „Public Private

[51] Mehr zum rechtlichen Hintergrund der staatlichen Aufgabe zur Daseinsvorsorge siehe Kapitel 7.5.1.1 und 7.5.1.2.
[52] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, S. 8.
[53] Zur Bedeutung des Prinzips der Vertraulichkeit im Informationsaustausch im NISG siehe Kapitel 7.5.9.
[54] Zum Verhältnis hinsichtlich des Auferlegens von Verpflichtungen bzw. Eingriff in verfassungsrechtlich gewährleistete Rechte durch den Staat siehe Kapitel 7.5.1.
[55] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, S. 8.
[56] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, S. 8. Dieser Grundsatz liegt auch dem NIS-Gesetz zugrunde, das sowohl Angriffe als auch sonstige Störungen in den sachlichen Anwendungsbereich aufgenommen hat – siehe dazu Kapitel 7.5.6.
[57] In einer durch hohe Ausgangssicherheit dem stetig anwachsenden Risiko – auch als Chance zu begreifend – zugewandten Gesellschaft, welche weiterhin liberal strukturiert sein will, muss dann andererseits auch die Eigenverantwortlichkeit von Strukturen wie Unternehmen, Vereinen oder Verbänden bis hin zum Einzelnen gestärkt werden – ganz im Sinne einer „resilient society“ – siehe *Weyand*, Demokratie und Sicherheit: Zum Kommunikationsprozess Staat - Gesellschaft im Kontext der Zivilen Sicherheit, in Gusy/Kugelmann et al. (Hrsg), Rechtshandbuch Zivile Sicherheit (2017), Rz 4.
[58] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, S. 8.

Partnership“ (PPP) – im Gegensatz zur verpflichtenden Umsetzung von Maßnahmen – erzielt werden.[59]

Eine der im Programm aufgelisteten, wesentlichen Maßnahmen der staatlichen Stellen ist die Ausweisung der strategischen Unternehmen, die kritische Infrastruktur betreiben.[60]

3.1.2. Bestehende Strukturen und Organisationen

Für die Koordination des Schutzes kritischer Infrastruktur sind in Österreich das Bundeskanzleramt gemeinsam mit dem Bundesministerium für Inneres unter Einbindung der betroffenen Bundesministerien, der Länder sowie sonstiger Stakeholder zuständig. [61] Im Bundesministerium für Inneres erfolgt die Umsetzung des APCIP durch das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT).[62]

Die Zuständigkeit des Bundesministeriums für Landesverteidigung wird differenziert gesehen. Im Österreichischen Programm zum Schutz kritischer Infrastruktur ist das Österreichische Bundesheer lediglich als Akteur im Rahmen von Assistenzeinsätzen (Art. 79 Abs. 2 B-VG) angeführt.[63] *Müller* sieht die Zuständigkeit darüber hinaus in bestimmten Fällen auch in der militärischen Landesverteidigung selbst (Art. 79 Abs. 1 B-VG) als Aufgabe des Bundesheeres.[64] Auf diese rechtliche Frage soll in Kapitel 4.1 (Verfassungsrechtliche Bestimmungen) näher eingegangen werden.

3.2. Cybersicherheit in Österreich

Die Digitalisierung verschiedenster gesellschaftlicher Bereiche bringt auch die Notwendigkeit einer gesamtgesellschaftlich neuen Ausrichtung mit sich. Die Gewährleistung von Cybersicherheit ist eine zentrale gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft im nationalen und internationalen Kontext, wofür die im Jahr 2013 veröffentlichte Österreichische Strategie für Cybersicherheit (ÖSCS)[65] ein umfassendes Konzept bietet und im Jahr 2019 in einer ÖSCS 2.0[66] erneuert werden soll.

---

[59] Zum rechtlichen Hintergrund der Public Private Partnership siehe Kapitel 7.5.1.2.
[60] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, S. 12.
[61] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, S. 10.
[62] Zuständigkeiten zu finden unter http://www.bvt.gv.at/; abgerufen am 17.03.2018.
[63] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, S. 11.
[64] *Müller*, Landesverteidigung auch im Inland möglich, publiziert in Die Presse – Rechtspanorama, 22.08.2016.
[65] *Bundeskanzleramt*, Österreichische Strategie für Cybersicherheit, 2013.
[66] Hinweis auf die Arbeiten an einer neuen Strategie zu finden unter https://www.digitales.oesterreich.gv.at/cyber-sicherheit-plattform, abgerufen am 05.05.2019.

Wenn von Cybersicherheit gesprochen wird, kann damit die Sicherheit des Internets (Internet als Schutzobjekt), die Sicherheit im Internet (Internet als Medium zur Übertragung rechtswidriger Inhalte) oder die Sicherheit vor dem Internet (Internet als Angriffsmittel) gemeint sein.[67] Die österreichische Strategie definiert den Begriff als Sicherheit der Infrastruktur des Cyberraumes, der im Cyberraum ausgetauschten Daten und vor allem der Menschen, die den Cyberraum nutzen.[68] Der Cyberraum ist nach der österreichischen Strategie sowie der Cyber-Sicherheitsstrategie für Deutschland[69] der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Diesem liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.

Die Zusammenarbeit zwischen Staat und Privaten ist insbesondere im Rahmen der Cybersicherheit so wesentlich und unübersehbar. Einerseits fungieren Private als Hersteller jener Soft- und Hardwareelemente, die für Cyberangriffe zweckentfremdet werden. Darüber hinaus werden nahezu alle Infrastrukturen der kritischen Infrastrukturen von privatwirtschaftlichen Akteuren gewartet und sind auch Ziele von Cyberangriffen.[70] Betrachtet man die Cybersicherheits-Landschaft, kann von sechs unterschiedlichen Gruppen von Stakeholdern gesprochen werden: Governance, Betreibern, Herstellern und Dienstleistern, Strafverfolgung, Computer Emergency Response Teams (CERTs) und Usern.[71] Die Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor ist daher umso wichtiger und wird nur anhand festgelegter Rahmen und Regularien funktionieren. Hier vor allem bedeutsam ist der Informationsaustausch hinsichtlich aktueller Risiken und Gefahren, der wohl nur auf freiwilliger Basis umfassend funktionieren kann. In den meisten Teilen Europas sowie in den USA (durch sogenannte Information Sharing and Analysis Center) sind diese Plattformen anhand Public Private Partnerships organisiert.[72]

Wesentliche Prinzipien der Strategie sind wiederum Rechtsstaatlichkeit, Subsidiarität, Selbstregulierung und Verhältnismäßigkeit.[73] Eine in der Strategie festgelegte Maßnahme im Rahmen der Governance ist die Schaffung eines zeitgemäßen ordnungspolitischen Rahmens, wobei

[67] *Leisterer*, Zivile Cybersicherheit in Europa: Entwicklung des Bereichs der Netz- und Informationssicherheit im Unionsrecht, in Gusy/Kugelmann et al. (Hrsg), Rechtshandbuch Zivile Sicherheit (2017), S. 102.
[68] *Bundeskanzleramt*, Österreichische Strategie für Cybersicherheit, 2013, S. 4.
[69] Cyber-Sicherheitsstrategie für Deutschland, 2016, S. 46.
[70] *Klimburg*, Gesamtstaatliche Ansätze zur Cybersicherheit, Strategie und Sicherheit, 1/2012, S. 463.
[71] *Pospisil/Gusenbauer/Huber et al.*, Cyber-Sicherheitsstrategien - Umsetzung von Zielen durch Kooperation, Datenschutz und Datensicherheit - DuD, 2017, S. 629.
[72] *Klimburg*, Strategie und Sicherheit, 2012, S. 466.
[73] *Bundeskanzleramt*, Österreichische Strategie für Cybersicherheit, 2013, S. 8.

bei der Festlegung von Verpflichtungen für nicht-staatliche Akteure der ausgewogene Einsatz von Anreizen und Sanktionen zu erwägen ist.[74]

Die IKT-Sicherheitsziele unterscheiden sich in ihrer Ausrichtung anhand des jeweiligen Stakeholders, der diese verfolgt, und können in politisch-rechtliche, ökonomische, technische, gesellschaftliche und organisatorische Ziele unterteilt werden.[75] Einer der wesentlichsten Parameter ist die Notwendigkeit von mehr Expertise, Fähigkeiten, Ressourcen und Strukturen in Bezug auf Cybersicherheit.[76]

Der „Cyberwar" wird grundsätzlich terminologisch von der „Cybersicherheit" getrennt und versteht sich als kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln vorwiegend aus dem Bereich der Informationstechnik.[77] Da die wichtigste Infrastruktur des Staates, wie die Versorgung mit Energie, Gesundheitsdienstleistungen und dem öffentlichen Verkehr, mittlerweile umfassend von Netz- und Informationssystemen abhängig ist, ist schon heute der virtuelle Raum des Cyberwar der entscheidende Ort für Kampfhandlungen.[78] In der Österreichischen Cybersicherheitsstrategie findet die Cyberverteidigung jedoch nur am Rande und begleitend zu Cybersicherheitsmaßnahmen Erwähnung, prominenter als wesentliche Aufgabe des österreichischen Bundesheeres wird diese in der Teilstrategie Verteidigungspolitik 2014 formuliert.[79]

3.2.1. Bestehende Strukturen und Organisationen

Computer Emergency Response Teams (CERTs) bzw. Computer Security Incident Response Teams (CSIRTs)[80] entstanden als private Einrichtungen der Praxis zu Unterstützung bei IT-Sicherheitsvorfällen und ohne konkreten rechtlichen Rahmen.[81] Neben CERT.at als österreichisches nationales CERT und als solches bisheriger Ansprechpartner für IT-Sicherheit im nationalen Umfeld existieren auch das (staatliche) Government Computer Emergency Response Team (GovCERT) als

[74] *Bundeskanzleramt*, Österreichische Strategie für Cybersicherheit, 2013, S. 12.
[75] *Pospisil et al.*, Datenschutz und Datensicherheit - DuD, 2017, S. 630.
[76] *Ischinger* in Abolhassan, Security Einfach Machen, S. 16.
[77] *Bundeskanzleramt*, Österreichische Strategie für Cybersicherheit, 2013, S. 22.
[78] *Kriesel/Kriesel*, Cyberwar - relevant für Sicherheit und Gesellschaft? Eine Problemanalyse, Zeitschrift für Außen- und Sicherheitspolitik (ZFA), 4/2011, S. 208. So auch *BMLVS*, Teilstrategie Verteidigungspolitik 2014, 2014, S. 11; *BMLVS*, Teilstrategie Verteidigungspolitik 2014, 2014.
[79] *BMLVS*, Teilstrategie Verteidigungspolitik 2014, 2014.
[80] Begriffe werden synonym verwendet, siehe dazu Tschohl/Hötzendorfer/Quirchmayr et al., "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs," in *ResearchGate*, ed. Institute (2017), S. 1.
[81] Tschohl/Hötzendorfer/Quirchmayr et al., "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs," in *ResearchGate* (2017), S. 1.

CERT für die öffentliche Verwaltung[82], das Military Cyber Emergency Response Team (MilCERT) für die militärischen Einrichtungen sowie im erweiterten Kreis CERTs privater Unternehmen (bspw. das CERT des Bundesrechenzentrums, das CERT der Raiffeisen Informatik oder das CERT der A1 Telekom Austria AG).[83] Zur Förderung der Zusammenarbeit der CERTs in Österreich wurde im Bundeskanzleramt ein CERT-Verbund geschaffen, der eine Kommunikationsplattform für die österreichischen CERTs bietet.[84]

Bereits vor Inkrafttreten der NIS-RL bzw. des nationalen NIS-Gesetzes erfüllten verschiedene staatliche Einrichtungen im Rahmen bereits bestehender Regelungen Aufgaben der Cybersicherheit. Dazu gehören das zur Vorbeugung und Prävention von Cyberkriminalität sowie zur operativen internationalen Kooperation in diesem Bereich eingerichtete Cyber Crime Competence Center (C4)[85] und das für den vorbeugenden Schutz von kritischen Infrastrukturen installierte Cyber Security Center (CSC)[86] innerhalb des Bundesministeriums für Inneres, deren Aufgabenerfüllung von den allgemeinen Bestimmungen des Sicherheitspolizeigesetzes (SPG)[87] gedeckt ist.

Darüber hinaus wurde für den Fall der Cyberverteidigung innerhalb des Bundesministeriums für Landesverteidigung das Kommando Führungsunterstützung Cyber Defence eingerichtet, welches neben den Land- und Luftstreitkräften nunmehr als drittes Kommando in Bezug auf die neue Dimension „Cyber“ fungierte. Dieses Kommando wurde jedoch im Jahr 2018 im Zuge einer Reform wieder aufgelöst.[88]

[82] Mehr zum GovCERT sowie den CERT-Strukturen in Österreich siehe *Huber*, Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation (2015), S. 12.
[83] *Bundeskanzleramt*, Österreichische Strategie für Cybersicherheit, 2013, S. 11.
[84] *Huber/Helllwig/Quirchmayr*, Wissensaustausch und Vertrauen unter Computer Emergency Response Teams - eine europäische Herausforderung, Datenschutz und Datensicherheit - DuD, 3/2016, S. 163.
[85] *Bundeskanzleramt*, Österreichische Strategie für Cybersicherheit, 2013, S. 11. Zum C4 als nationale Koordinierungs- und Meldestelle zur Bekämpfung der Cyberkriminalität siehe *Einzinger/Skopik/Fiedler*, Keine Cyber-Sicherheit ohne Datenschutz, Datenschutzrechtliche Herausforderungen bei der Etablierung von nationalen CERTs, Datenschutz und Datensicherheit - DuD, 11/2015, S. 725.
[86] Zu finden unter www.bvt.gv.at; abgerufen am 24.03.2018.
[87] Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG), BGBl. Nr. 566/1991 idF BGBl. Nr. 56/2018.
[88] Zu finden unter www.bundesheer.at; abgerufen am 24.03.2018. Aktuell (Stand 05.05.2019) erfolgt innerhalb des Bundesministeriums für Landesverteidigung eine Organisationsreform, wobei eine neue Struktur für die Aufgaben der Cyberverteidigung abzusehen ist.

4. Bestehende nationale Regelungen zum Schutz kritischer Infrastruktur und zur Cybersicherheit in Österreich

Bereits vor Inkrafttreten der NIS-RL und des NIS-Gesetzes waren in Österreich zahlreiche Bestimmungen zur Regelung des Schutzes kritischer Infrastruktur generell als auch zu Sicherheitsvorkehrungen und Meldepflichten für diese Betreiber in Geltung. Diese sind bei Umsetzung der NIS-RL in jenen Bereichen zu berücksichtigen, in denen es für die Mitgliedstaaten noch Spielraum in der Umsetzung der NIS-RL gibt. Im Rahmen der Stärkung des Wirtschaftsstandortes und auch der Deregulierung ist darauf zu achten, bestehende Verpflichtungen für Betreiber zu nutzen, gegebenenfalls darauf aufzubauen und diesen möglichst nicht zu widersprechen, um insbesondere „Doppelgleisigkeiten" und Informationsverluste zu vermeiden.

4.1. Verfassungsrechtliche Bestimmungen

4.1.1. Kompetenzrechtliche Einordnung des Schutzes kritischer Infrastruktur und der Cybersicherheit im österreichischen Verfassungsrecht

Das B-VG regelt eine Reihe von Kompetenztatbeständen in seinen Artikeln 10 – 15, wobei untersucht werden soll, ob ein eigenständiger Tatbestand des Schutzes kritischer Infrastruktur, der Cybersicherheit oder der Daseinsvorsorge generell gegeben ist. In den Kompetenztatbeständen findet sich kein Hinweis auf einen dieser Bereiche. Da die Cybersicherheit – insbesondere auch schon aus begrifflichen Gründen - auch in den generellen Bereich der Sicherheit fallen könnte, ist zu untersuchen, ob die Materie der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit gem. Art. 10 Abs. 1 B-VG betroffen sein bzw. ob es sich bei der Sicherheit von Netz- und Informationssystemen um die Abwehr von allgemeinen Gefahren handeln könnte. Ein Argument dafür könnte sein, dass großflächige und längerfristige Ausfälle von Systemen der Elektrizitätsversorgung, von Krankenhäusern, Banken oder öffentlichen Verkehrsmitteln oftmals auch mit Auswirkungen auf die öffentliche Ruhe, Ordnung und Sicherheit verbunden sein können, sodass deren Abwehr (im Rahmen der Vorbeugung gerichtlich strafbarer Handlungen[89]) von der Materie des Art. 10 Abs. 1 Z 7 erfasst sein könnte. Der Regelungsbereich der NIS-RL geht jedoch weiter. Einerseits sind auch Anbieter digitaler Dienste, beispielsweise Online-Marktplätze oder Online-Suchmaschinen, betroffen, deren Ausfall die öffentliche Ruhe, Ordnung und Sicherheit wohl

[89] *Davy/Davy*, Gezähmte Polizeigewalt? Aufgaben und Neuordnung der Sicherheitspolizei in Österreich (1991), S. 41.

in keiner Weise beeinträchtigt. Außerdem werden von der NIS-RL nicht nur Angriffe auf Netz- und Informationssysteme, sondern darüber hinaus auch sonstige Störungen – auch nur technischer Natur – geregelt, die zu Ausfällen oder Beeinträchtigungen der Systeme führen[90]. Materien wie beispielsweise das Gewerbe (Art. 10 B-VG) sind daher ebenso betroffen wie das Elektrizitätswesen oder Heil- und Pflegeanstalten (Art. 12 B-VG) sowie das allgemeine Krisen- und Katastrophenwesen[91] (Art. 15 B-VG) (Generalklausel zugunsten der Länder[92]). Darüber hinaus ist in den Erwägungsgründen der NIS-RL das intendierte Ziel des Funktionierens des Binnenmarktes angeführt[93], das weit über die Kompetenz der öffentlichen Ruhe, Ordnung und Sicherheit (Art. 10 Abs. 1 Z 7 B-VG) hinausgeht. Daran anknüpfend ist somit von einer so genannten „Querschnittsmaterie“[94] auszugehen. Eine solche liegt vor, wenn eine Sachmaterie keinem einzelnen Kompetenztatbestand zugeordnet werden kann, sondern in verschiedenen Kompetenztatbeständen Deckung findet.[95]

Anzudenken wäre theoretisch auch das Vorliegen einer Annexmaterie, wonach eine Sachmaterie gewisse ergänzende Zuständigkeiten nach sich zieht und der zuständige Gesetzgeber auch diese Themen regeln kann.[96] Dabei handelt es sich vor allem um das Verwaltungsverfahrensrecht, die Festlegung von Verwaltungsstraftatbeständen und Strafsanktionen der Verwaltung, Enteigungsmaßnahmen und Eigentumsbeschränkungen im Interesse der Sachmaterie und verwaltungspolizeiliche Maßnahmen.[97] Im Hinblick auf den oben dargestellten Umfang des Begriffes der Cybersicherheit muss das Vorliegen einer Annexmaterie verneint werden, da es sich neben der Gewährleistung des Funktionierens wesentlicher Dienste, die noch zur jeweiligen Sachmaterie argumentiert werden könnten, um (auch EU-weit) koordinierte Meldepflichten, koordinierte Überprüfungsmechanismen sowie die Einrichtung von Strukturen wie den Computer-Notfallteams handelt.

Nähere Ausführungen zur kompetenzrechtlichen Zuordnung sind in Kapitel 7.1.1. (Kompetenzdeckungsklausel im NISG) zu finden.

[90] ErwGr 2, 3 RL 2016/1148.
[91] Der längerfristige Ausfall von Elektrizität und anderen wesentlichen Diensten kann selbstverständlich auch zu Krisen führen.
[92] *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11] (2015), Rz 269.
[93] ErwGr 1 RL 2016/1148.
[94] *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11], Rz 1090.
[95] *Biner/Trauner*, Lehrbuch öffentliches Recht - Grundlagen[4] (2016), S. 52.
[96] *Berka*, Verfassungsrecht (2012), Rz 422.
[97] *Biner/Trauner*, Lehrbuch öffentliches Recht - Grundlagen[4], S. 260.

4.1.2. Schutz kritischer Infrastruktur als Aufgabe des Österreichischen Bundesheeres

Eingegangen werden soll auch auf die verfassungsrechtliche Zuständigkeit des Österreichischen Bundesheeres in Angelegenheiten des Schutzes kritischer Infrastruktur.

Das Bundesheer ist originär für die militärische Landesverteidigung zuständig (Art. 79 Abs. 1 B-VG). Als Teil der militärischen Landesverteidigung gilt neben der allgemeinen Einsatzvorbereitung[98] zur militärischen Landesverteidigung auch der Schutz militärischer Rechtsgüter vor gefährlichen Angriffen, wofür den Streitkräften ähnliche operative Befugnisse[99] wie den Sicherheitsbehörden zukommen.[100] Darüber hinaus kann das Bundesheer in so genannten „Assistenzeinsätzen" tätig werden, soweit die gesetzmäßige zivile Gewalt seine Mitwirkung in Anspruch nimmt (Art. 79 Abs. 2 B-VG). Dies gilt beispielsweise zur Aufrechterhaltung der Ordnung und Sicherheit im Inneren (Art. 79 Abs. 2 Z 2) zur Unterstützung der Sicherheitsbehörden.

Bezugnehmend auf die Materien des Schutzes kritischer Infrastrukturen besteht eine eindeutige Zuständigkeit des Bundesheeres im Assistenzeinsatz zur Unterstützung der Sicherheitsbehörden[101], sofern es sich um einen notwendigen Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (Art. 79 Abs. 2 Z 1 lit. a B-VG) oder zur Aufrechterhaltung der Ordnung und Sicherheit im Inneren (Art. 79 Abs. 2 Z 2 B-VG) handelt und die zivilen Behörden das Bundesheer dafür in Anspruch nehmen. Bei Angriffen auf Einrichtungen der kritischen Infrastruktur ist wohl in den meisten Fällen von einer Betroffenheit der Sicherheit im Inneren auszugehen. Darüber hinaus fällt der Schutz kritischer Infrastruktur dann eindeutig in die Zuständigkeit des Bundesheeres, sofern es sich bei diesen Infrastrukturen auch um militärische Rechtsgüter handelt.

Fraglich ist hingegen in diesen Angelegenheiten das Vorliegen der originären Zuständigkeit des Bundesheeres, nämlich der militärischen Landesverteidigung. Diese Zuständigkeit ist zweifelsfrei immer dann gegeben, wenn Angriffe von außen durch andere Völkerrechtssubjekte ausgehen und auf die Souveränität der Republik Österreich abzielen, dh eine Gefahr für die Existenz, Unabhängigkeit oder immerwährende Neutralität Österreichs ist.[102] Von anderen Staaten ausgehende militärische Angriffe, die wesentliche Infrastrukturen Österreichs, beispielsweise verfassungsmäßige Einrichtungen oder die Stromversorgung, betreffen und dadurch die

[98] Allgemeine Einsatzvorbereitung gem. § 2 Abs. 3 Wehrgesetz (WG) 2001, StF BGBl. I Nr. 146/2001 idF BGBl. I Nr. 100/2018.
[99] Diese Befugnisse sind im Militärbefugnisgesetz (MBG) geregelt.
[100] *Adamovich/Funk/Holzinger et al.*, Österreichisches Staatsrecht (2009), Rz 53.025.
[101] So auch das Österreichische Programm zum Schutz kritischer Infrastruktur, siehe Kapitel 3.1.
[102] EB RV 1461 BlgNr 13. GP, 5 mit Hinweis auf *Pernthaler*, Umfassende Landesverteidigung (1970), S. 1-4, 6, 7 u. 37.

Souveränität der Republik Österreich gefährden, werden als Fall der militärischen Landesverteidigung zu qualifizieren sein.

Vorgänge im Staatsinnern werden nur insofern in Betracht gezogen, als sie im Zusammenhang mit von außen drohenden Gefahren stehen.[103] Insbesondere im Hinblick auf terroristische Anschläge im Inland, beispielsweise auch gegen kritische Infrastrukturen wie Verkehrseinrichtungen, bestehen in diesem Zusammenhang unterschiedliche Auffassungen. *Müller* argumentiert beispielsweise, dass auch bei Terroranschlägen im Inland dann die Zuständigkeit des Bundesheeres zur militärischen Landesverteidigung gegeben sein kann, wenn terroristische Akte so massiv gesetzt werden, dass sie mit einem militärischen Angriff gleichgehalten werden können. Dies hänge von verschiedenen Kriterien wie beispielsweise davon ab, ob die Terroristen militärisch organisiert und ausgebildet sind, ob durch die Terrororganisation ein Außenbezug vorhanden ist und ob derartige Aktionen gleichzeitig oder in einem engen zeitlichen Zusammenhang gesetzt werden, sodass man von flächigen Angriffen auf den Staat ausgehen könnte.[104] *Pernthaler* argumentierte schon 1970, dass der klassische Kriegsbegriff nicht mehr zeitgemäß sei.[105]

Dazu ist aus meiner Sicht anzumerken, dass sich der Terrorismus, für den es keine generelle Definition gibt,[106] grundsätzlich primär nicht gegen die Existenz bzw. Souveränität eines Staates richtet, sondern vielmehr ideologische und psychologische Ziele verfolgt.[107] Auch wenn Terroristen militärisch organisiert und ausgebildet sein sollten, handelt es sich mE um keinen militärischen Angriff iSd Art. 79 Abs. 1 B-VG, sofern die Terroristen (als nicht-staatliche Akteure)[108] nicht durch andere Völkerrechtssubjekte beauftragt bzw. gesteuert werden, sondern für sich und ihre eigenen Interessen agieren.[109] Davon ist auch bei großflächigen und gleichzeitigen Angriffen im Staatsgebiet nicht abzurücken, welche zweifelsohne die innere Ordnung der Republik – nicht jedoch die Existenz oder Souveränität - aufs Höchste gefährden würden.

---

[103] EB RV 1461 BlgNr 13. GP, 5.

[104] *Müller*, Landesverteidigung auch im Inland möglich, publiziert in Die Presse – Rechtspanorama, 22.08.2016.

[105] *Pernthaler*, Umfassende Landesverteidigung.

[106] Ein Versuch einer Definition findet sich im Lexikon der Politik: „Terrorismus ist […] als Gewaltstrategie zu definieren, die primär durch die Verbreitung von Furcht und Schrecken […] das bestehende Herrschaftssystem auszuhöhlen und eine mehr oder weniger grundlegende politisch-gesellschaftliche Umwälzung herbeizuführen sucht, siehe Kleines Lexikon der Politik, Band 1145 (2011), S. 623f.

[107] *Fichtenbauer*, Freiheitliche Vorstellungen zur Landesverteidigung, Strategie und Sicherheit, 1/2013, S. 515.

[108] *Bock*, Terrorismus (2009), S. 16.

[109] Klar vom Terrorismus zu unterscheiden sind die so genannten Guerilla, die im Gegensatz zum Terrorismus mit militärischer Strategie unterlegt sind, siehe *Mitterer*, Terrorismus - Der Krieg des 21. Jahrhunderts (2014), S. 8.

Die Abwehr klassischer, ideologisch motivierter Terroranschläge ist daher immer eine Aufgabe der Sicherheitsbehörden im Rahmen der Aufgaben und Befugnisse nach dem Sicherheitspolizeigesetz (SPG)[110], wenngleich bei derartigen Angriffen wahrscheinlich das Bundesheer im Rahmen der Assistenzleistung zur Unterstützung herangezogen werden würde, beispielsweise wenn seitens der Terroristen militärische Waffen verwendet werden.

Müller ist gleichzeitig insofern zuzustimmen, dass die militärische Landesverteidigung nicht mehr nur auf die klassischen kriegerischen Auseinandersetzungen begrenzt ist sondern sich auch in anderen Formen ergeben kann. Terroristische Anschläge, die mit militärischen Mitteln und vom Ausland gesteuert mit dem Ziel erfolgen, die Souveränität Österreichs zu gefährden, beispielsweise durch Destabilisierung der verfassungsmäßigen Einrichtungen, wären als Fall der militärischen Landesverteidigung durchaus denkbar.

4.1.3. Cybersicherheit bzw. Cyberverteidigung als Aufgabe des österreichischen Bundesheeres

Die militärische Literatur sprach nach dem Zweiten Weltkrieg zunehmend von der „Leere des Gefechtsfeldes“,[111] da auf einem modernen Schlachtfeld „nicht mehr viel zu sehen sei“. Dies gilt insbesondere für den Krieg der Zukunft, der im virtuellen Raum stattfinden wird. Ein Beispiel dafür war der Konflikt zwischen Estland und Russland im Jahr 2007, der in der baltischen Republik zu einem digitalen Kollaps führte bzw. den Staat komplett lahmlegte.[112]

Verfassungsrechtlich bedeutend ist die Abgrenzung zwischen der Cybersicherheit als Aufgabe der Sicherheitsbehörden und der Cyberverteidigung im Rahmen der militärischen Landesverteidigung. Letztere ist nach *Anderl/Heußler/Mayer/Müller* immer dann gegeben, sofern sich Angriffe gegen militärische IKT-Systeme richten (militärischer Eigenschutz), der Angriff begleitend zu einem „konventionellen“ Angriff erfolgt, der Angriff von einem anderen Staat ausgeht oder derart massiv ist, dass er als souveränitätsgefährdend[113] einzustufen ist.[114] Dieser Ansicht ist zuzustimmen, wenngleich in diesem Zusammenhang darauf hinzuweisen ist, dass die Adressierung eines Cyberangriffes (bspw. Zuordnung zu einem anderen Völkerrechtssubjekt) meist sehr lange Zeit in Anspruch nimmt und oft schwer nachweisbar ist.[115] Bis zu einer eindeutigen Zuordnung zu einem

[110] Siehe die Bestimmungen zur Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit gem. § 3ff SPG.
[111] *Kriesel/Kriesel*, Zeitschrift für Außen- und Sicherheitspolitik (ZFA), 2011, S. 207
[112] Berichterstattung dazu siehe beispielsweise http://www.welt.de/webwelt/article3198864/Wie-die-Bundeswehr-den-Cyberwar-gewinnen-will.html (abgerufen am 27.10.2019).
[113] Zur Definition der Gefahr für die Souveränität Österreich siehe weiter oben.
[114] *Anderl et al.*, NISG::Kommentar, § 24, Rz 19.
[115] Die Entscheidungen zu Abwehr von Cyberangriffen sind jedoch gegebenenfalls in Minuten zu treffen, siehe *Kriesel/Kriesel*, Zeitschrift für Außen- und Sicherheitspolitik (ZFA), 2011, S. 214.

anderen Völkerrechtssubjekt ist mE immer von einer Zuständigkeit der Sicherheitsbehörden auszugehen. Über das Vorliegen eines Falles der Cyberverteidigung entscheidet der Bundesminister für Landesverteidigung im Rahmen der ihm von der Bundesregierung erteilten Ermächtigung (Art. 80 Abs. 2 B-VG).[116]

Als Teil der militärischen Landesverteidigung sind auch Maßnahmen der allgemeinen Einsatzvorbereitung des Bundesheeres (§ 2 Abs. 3 WG 2001) zu verstehen. Aus diesem Grund ist es bereits ohne das Vorliegen eines Verteidigungsfalles zulässig, sich mit aktuellen Angriffsmustern und möglichen Verteidigungsszenarien zu beschäftigen.

Neben der militärischen Landesverteidigung kann die Zuständigkeit – wie auch schon bei der Aufgabe des Schutzes kritischer Infrastruktur – auch zum Schutz militärischer Rechtsgüter sowie im Fall von Assistenzeinsätzen für die zivile Gewalt vorliegen.

Näheres zu rechtlichen Möglichkeiten des Österreichischen Bundesheeres im Falle der Cyberverteidigung ist in Kapitel 4.2.4 (Militärbefugnisgesetz) zu finden.

4.2. Einfachgesetzliche Regelungen in Bezug auf den Schutz kritischer Infrastruktur und Cybersicherheit

4.2.1. Bundesministeriengesetz

Im Bundesministeriengesetz (BMG)[117] sind unter anderem die Aufgabenbereiche der einzelnen Ministerien geregelt, unter deren Zuhilfenahme mögliche Zuständigkeiten der Fachministerien für Bereiche des NIS-Gesetzes bewertet werden könnten.

Gemäß der Anlage zu § 2 BMG, Teil 2, A, Ziffer 1 umfasst der Aufgabenbereich des Bundeskanzleramtes unter anderem die Angelegenheiten der allgemeinen Regierungspolitik einschließlich der Koordination der gesamten Verwaltung des Bundes, soweit sie nicht in den Wirkungsbereich eines anderen Bundesministeriums fallen. Dazu gehören insbesondere auch Angelegenheiten der strategischen Netz- und Informationssicherheit.

Gem. Anlage zu § 2, Teil 2, H Ziffer 1 BMG ist das Bundesministerium für Inneres für die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit sowie für die Koordination in Angelegenheiten des staatlichen Krisenmanagements und des staatlichen Katastrophenschutzmanagements zuständig.

[116] Siehe auch *Anderl et al.*, NISG::Kommentar, § 24, Rz 18.
[117] Bundesgesetz über die Zahl, den Wirkungsbereich und die Einrichtung der Bundesministerien (Bundesministeriengesetz 1986 – BMG), BGBl. Nr. 76/1986 idF BGBl. I Nr. 61/2018.

Die Aufgabenverteilung lässt darauf schließen, dass sowohl dem Bundeskanzleramt als auch dem Bundesministerium für Inneres Zuständigkeiten in Bezug auf die Sicherheit von Netz- und Informationssystemen zukommen, wobei die Abgrenzung in Kapitel 7.2.1 (Möglichkeiten der Einrichtung zuständiger Behörden in Österreich) noch zu untersuchen sein wird.[118]

4.2.2. Sicherheitspolizeigesetz

Die Sicherheit von Netz- und Informationssystemen von Betreibern wesentlicher Dienste war bisher in der nationalen Rechtsordnung zwar nicht direkt, indirekt jedoch im Rahmen des vorbeugenden[119] Schutzes kritischer Infrastrukturen im Sicherheitspolizeigesetz (SPG) geregelt.

Demnach obliegt den Sicherheitsbehörden seit einer Novelle 2014[120] der besondere Schutz von Einrichtungen, Anlagen, Systemen oder Teilen davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern oder den öffentlichen Verkehr haben (§ 22 Abs. 1 Z 6 SPG).[121] In Rahmen dieser Aufgabe stellt sich die Frage, ob der Gesetzgeber hier lediglich von der physischen Sicherheit, oder auch von dem Schutz von Netz- und Informationssystemen ausgeht. Richtet man sich nach den Erläuternden Bemerkungen[122], soll den Sicherheitsbehörden aufgrund einer immer größer werdenden Abhängigkeit der Bevölkerung von funktionierenden Infrastrukturleistungen auch und vor allem im Bereich der Computerkriminalität die entsprechende Aufgabenerfüllung übertragen werden. Wie dieser vorbeugende Schutz konkret aussieht, regelt das SPG nicht. *Hauer/Keplinger* definieren dies im Gegensatz zum allgemeinen Schutz, der allen Personen, Einrichtungen und Sachen bereits durch die Existenz der Sicherheitsexekutive, die insbesondere im Streifendienst

[118] Zur möglichen Abgrenzungen und näheren Ausführungen im Zusammenhang mit den im NISG regelten Aufgaben des Bundeskanzlers und Bundesministers für Inneres siehe Kapitel 7.2.1.

[119] Das Recht der zivilen Sicherheit, das über den eingriffslegitimierenden Akt der Gefahrenabwehr hinaus vorausschauende Vermeidung, Vorsorge und nachsorgende Bewältigung in einen integrierten Ansatz umfassender Sicherheitsgewährleistung einbezieht, ist Ausdruck eines Trends der Versicherheitlichung auch und gerade in Zeiten intensiver, etwa terroristischer Bedrohungen, siehe *Schöndorf-Haubold*, Das Recht der Zivilen Sicherheit an der Schnittstelle von nationaler, europäischer und internationaler Zuständigkeit, in Gusy/Kugelmann et al. (Hrsg), Rechtshandbuch Zivile Sicherheit (2017), Rz 2..

[120] BGBl. Nr. 43/2014.

[121] Zur Unterscheidung der Definition kritischer Infrastrukturen in § 22 SPG zur Definition von Betreibern wesentlicher Dienste im NISG siehe Kapitel 7.1.2.

[122] „Vor dem Hintergrund, dass der Schutz kritischer Infrastrukturen und die Gewährleistung von Cyber-Sicherheit in diesem Bereich von besonderer Bedeutung für die Gesundheit, Sicherheit, das wirtschaftliche und soziale Wohl der Bevölkerung und das Funktionieren staatlicher Einrichtungen ist, erscheint es notwendig, bestimmte Einrichtungen und Systeme als sensibel zu erkennen und besonders zu schützen, weshalb eine eigenständige sicherheitspolizeiliche Aufgabe geschaffen werden soll, siehe EB RV der Novelle des Sicherheitspolizeigesetzes, BGBl. Nr. BGBl. Nr. 43/2014.

ihren Ausdruck findet, zuteil wird. Der besondere Schutz sei demnach eine erhöhte Aufmerksamkeit auf die besonders zu schützenden Interessen, wobei es das Gesetz der fachkompetenten Einschätzung der Sicherheitsbehörde anheimgestellt lasse, welche Maßnahmen sie im Interesse des besonderen Schutzes zu ergreifen für zweckdienlich hält.[123] Nach *Wimmer* sollen die Sicherheitsbehörden im Rahmen des vorbeugenden Schutzes Einrichtungen schützen, die erfahrungsgemäß besonders geneigt sind, Opfer bzw. Objekte gefährlicher Angriffe zu werden, wovon der Gesetzgeber im Fall von kritischen Infrastrukturen offenbar ausgeht.[124]

In Gegenüberstellung dieser Bestimmung mit dem Regelungskontext des NISG ist jedoch festzustellen, dass es sich bei § 22 SPG um eine Aufgabe der Sicherheitsbehörden handelt, an die kaum konkrete Befugnisse bzw. weitere Maßnahmen – die mit Cybersicherheit in Zusammenhang stehen – geknüpft sind. Insbesondere begründet § 22 keine subjektiven Rechtsansprüche der Unternehmen.[125] Die Sicherheitsbehörden waren bisher beispielsweise ermächtigt, die Unternehmen hinsichtlich möglicher Gefahren zu beraten oder Handlungsempfehlungen weiterzugeben. Eine Verpflichtung für die Behörden zum Tätigwerden bestand insofern, Betreiber über einen bevorstehenden (konkreten) gefährlichen Angriff in Kenntnis zu setzen (§ 22 Abs. 4 SPG), wobei zu diesem Zweck auch personenbezogene Daten übermittelt werden durften, damit sich die Betreiber entsprechend schützen können (bspw. um entsprechende Vorkehrungen im IT-System zu veranlassen) (§§ 53 Abs. 1 Z 3 iVm 56 Abs. 1 Z 4).[126]

4.2.3. Polizeiliches Staatsschutzgesetz

Auch im Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (Polizeiliches Staatsschutzgesetz – PStSG)[127] ist der Schutz kritischer Infrastruktur und die Cybersicherheit explizit geregelt.

Der polizeiliche Staatsschutz dient neben dem Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit sowie von Vertretern ausländischer Staaten, internationaler Organisationen und anderer Völkerrechtssubjekte nach Maßgabe völkerrechtlicher Verpflichtungen auch dem Schutz kritischer Infrastruktur (§ 1 Abs. 2 PStSG). Noch deutlicher – in Bezug auf das NIS-Gesetz – fällt die Beschreibung des Bundesamtes für

[123] *Hauer/Keplinger*, Sicherheitspolizeigesetz (2005), S. 250.
[124] *Wimmer*, § 22 SPG, in Thanner /Vogl (Hrsg), Sicherheitspolizeigesetz, Kommentar (2013), S. 210.
[125] *Hauer/Keplinger*, Sicherheitspolizeigesetz[4] (2011), Anm. 1.
[126] Zur Abgrenzung von der Übermittlung von Handlungsempfehlungen durch den BMI und Computer-Notfallteams in Vollziehung des NISG siehe Kapitel 7.5.6.
[127] Polizeiliches Staatsschutzgesetz (PStSG), BGBl. Nr. 2016/5.

Verfassungsschutz und Terrorismusbekämpfung (BVT) als Zentralstelle[128] aus. Demnach erfüllt das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung für den Bundesminister für Inneres die zentrale Funktion der operativen Koordinierungsstelle für Meldungen über jede Form von Angriffen auf Computersysteme von verfassungsmäßigen Einrichtungen sowie kritischen Infrastrukturen (§ 4 PStSG).

Bei den in § 4 angeführten Aufgaben handelt es sich um jene Funktionen, deren österreichweite Zentralisierung am Gebiet des polizeilichen Staatsschutzes angezeigt erscheint.[129] Dies macht insofern Sinn, als die operative Koordinierungsstelle für Meldungen lediglich innerhalb einer Organisationseinheit eingerichtet sein sollte und eine ebensolche Struktur in den Landesämtern für Verfassungsschutz und Terrorismusbekämpfung einerseits aufgrund der unwesentlichen Bedeutung der Regionalität des Vorfalles (Angriffe auf Systeme können ortsunabhängig erfolgen) und andererseits aufgrund der beschränkten Ressourcen von IT-Fachpersonal im öffentlichen Dienst nicht erforderlich erscheint. Bei genannter Koordinierungsstelle handelt es sich um das „Cyber Security Center (CSC)", welches über Angriffe gegen verfassungsmäßige Einrichtungen und kritische Infrastrukturen informiert werden soll, um dadurch großflächige Angriffe und Angriffsmuster erkennen zu können und Handlungsempfehlungen an (potenziell) Betroffene weitergeben zu können.[130]

Darüber hinaus obliegt dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung gemäß § 7 PStSG auch die „polizeilich staatsschutzrelevante Beratung"[131] von potentiell betroffenen natürlichen und juristischen Personen zur Vorbeugung verfassungsgefährdender Angriffe, insbesondere auf dem Gebiet der Cybersicherheit.

Mit den Bestimmungen der §§ 4 und 7 PStSG wurden somit schon im Jahr 2016 die später im NIS-Gesetz geregelte Aufgabe des Bundesministers für Inneres (BMI) zur operativen Koordinierung und Unterstützung dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung zugewiesen.

Untersucht werden soll nachfolgend der grundsätzliche Unterschied in den Aufgaben nach dem PStSG und dem NIS-Gesetz. Zwar kommt dem Bundesminister für Inneres auch nach den Regelungen des PStSG die Aufgabe der operativen Koordinierungsstelle zu. Dies ist in ähnlicher Form in § 5 Abs. 1 Z 3 NISG[132] geregelt, wonach der Bundesminister für Inneres Meldungen über

[128] Die Aufgaben in § 4 sind deshalb als solche der „Zentralstelle" definiert, da diese nur dem Bundesamt und nicht den bei den Landespolizeidirektionen eingerichteten für Verfassungsschutz zuständigen Organisationseinheiten zukommen sollen.
[129] *Reindl-Krauskopf*, PStSG Polizeiliches Staatsschutzgesetz (2016), S. 33.
[130] *Keplinger/Kutschera/Pühringer*, Polizeiliches Staatsschutzgesetz (2016), S. 28.
[131] *Reindl-Krauskopf*, PStSG Polizeiliches Staatsschutzgesetz, S. 12.
[132] Zu den Aufgaben des Bundesministers für Inneres siehe Kapitel 7.2.3.

Risiken, Vorfälle oder Sicherheitsvorfälle entgegennehmen und analysieren, regelmäßig ein diesbezügliches Lagebild erstellen und die Meldungen sowie das Lagebild und zusätzliche relevante Informationen an inländische Behörden oder Stellen weiterleiten soll. Jedoch schränkt das PStSG diese Aufgabe auf Angriffe auf Computersysteme nach den Bestimmungen des Strafgesetzbuches ein, wohingegen das NIS-Gesetz durch die Koordinierungen von Risiken und nicht zwangsweise strafrechtsakzessorischen Vorfällen sehr viel weiter reicht.[133]

Darüber hinaus knüpfen sich an die Aufgaben des Bundesministers für Inneres im Rahmen des NIS-Gesetzes zahlreiche Befugnisse zur Datenverarbeitung (§ 9), Datenübermittlung (§ 10) sowie zum Betrieb von IKT-Lösung zur Vorbeugung von Sicherheitsvorfällen (§ 13), die in dieser Bandbreite im PStSG nicht zu finden sind. Wo im PStSG lediglich eine sehr wenig konkret formulierte Aufgabe zur operativen Koordinierung festgelegt ist, weitet das NIS-Gesetz die Möglichkeiten des Bundesministers darüber hinaus auf die Befugnis zur Einschau in Netz- und Informationssysteme (§ 17 NISG) aus.

Zusammengefasst lässt sich damit feststellen, dass dem Bundesminister für Inneres im Rahmen des PStSG lediglich eine offene Aufgabe (ohne daran anknüpfende Befugnisse) zur operativen Koordinierung von Angriffen zugewiesen wurde, das NIS-Gesetz diese Aufgabe jedoch einerseits auch um die Koordinierung von Meldungen über Risiken oder sonstiger technischer Störungen ausweitet sowie weitreichende Befugnisse zur Gewährleistung einer funktionierenden Netz- und Informationssystemsicherheit regelt.

4.2.4. Militärbefugnisgesetz (MBG)

Das Militärbefugnisgesetz[134] regelt die Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung. Unter anderem die Aufgabenerfüllung der Cyberverteidigung betreffend erging am 27.02.2019 eine Regierungsvorlage zum Wehrrechtsänderungsgesetz 2019 (WRÄG 2019)[135], die das Thema Cybersicherheit und den möglichen Beitrag des Bundesheeres dazu im Rahmen eines Einsatzes zur militärischen Landesverteidigung näher definieren sollte.

Einerseits sollte die Zulässigkeit der Erfüllung von Aufgaben der militärischen Landesverteidigung (auch) im Ausland durch eine Ergänzung in § 3 Abs. 3 MGB im Interesse der Rechtssicherheit ausdrücklich geregelt werden. Unstrittig war bereits bisher, dass im Rahmen eines so genannten

[133] Zur (sehr weiten) Definition des Sicherheitsvorfalles iZm dem NISG siehe Kapitel 7.5.6.
[134] Bundesgesetz über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz – MBG), StF BGBl. I Nr. 86/2000 idF BGBl. I Nr. 32/2018.
[135] EB RV 509 BlgNr XXVI. GP, S. 8f.

Verteidigungsfalles[136] einsatzbezogenes militärisches Handeln durch Organe des Bundesheeres auch auf fremdem Staatsgebiet erfolgen darf. [137] Durch diese Regelung soll die Abwehr von Cyberangriffen aus dem Ausland, beispielsweise durch auf fremdem Staatsgebiet betriebene Server, ermöglicht werden. Auf dieses Szenario bezieht sich konkret Satz 2 in § 3 Abs. 3, da dies auch für Maßnahmen gelten soll, die in Österreich gesetzt werden und Auswirkungen auf fremdem Staatsgebiet haben. Dabei ist an den Zugriff auf Server im Ausland und deren Neutralisierung zu denken.[138]

Außerdem sollten durch das Wehrrechtsänderungsgesetz 2019 die Mittel zur Ausübung unmittelbarer Zwangsgewalt im Wachdienst (neben technischer Sperren und Diensthunde) auf Computersysteme ausgeweitet werden (§ 17 MBG). Dadurch sollte ausdrücklich klargestellt werden, dass bei Cyberangriffen auch (offensive und defensive) technische Mittel zur Abwehr derartiger Angriffe rechtlich zulässig seien. Als Beispiele führen die Erläuternden Bemerkungen[139] technische Einrichtungen zur Erkennung von Angriffen auf Netz- und Informationssysteme[140] oder zur Neutralisierung von Computersystemen, die für Cyberangriffe verwendet werden, an. Laut *Müller* wird damit der Computer zum Einsatzmittel im Cyberkrieg.[141]

Das Wehrrechtsänderungsgesetz 2019 würde meines Erachtens einen großen Fortschritt zur Rechtssicherheit hinsichtlich der Maßnahmen zur Cyberverteidigung in Österreich bringen. Auf sonstige (insb. sicherheitsbehördliche) Möglichkeiten zur Abwehr von Cyberangriffen wird in Kapitel 7.6.2 (Mögliche Reaktion auf eine Cyberkrise) näher eingegangen.

[136] Verteidigungsfall im Sinne der Entschließung des Nationalrates 1643 BlgNr, XIII. GP („Verteidigungsdoktrin“).
[137] Vgl. Art. 52 der Satzung der Vereinten Nationen, BGBl. Nr. 120/1956.- so darf etwa ein Staat, der angegriffen wird, in Ausübung des Selbstverteidigungsrechtes alle notwendigen und verhältnismäßigen Maßnahmen ergreifen, um diesen Angriff abzuwehren.
[138] Siehe dazu EB RV 509 BlgNr XXVI. GP, S. 13.
[139] EB RV 509 BlgNr XXVI. GP, S. 15.
[140] Diese Befugnis kommt den Sicherheitsbehörden gem. § 13 NISG zu, siehe dazu Kapitel 7.3.1.
[141] *Anderl et al.*, NISG::Kommentar, § 24, Rz 21.

5. Schnittstellen zu anderen relevanten Unionsrechtsakten

5.1. Richtlinie 114/2008 zum Schutz kritischer Infrastruktur

Gemäß Art. 1 Abs. 4 NIS-RL gilt die NIS-RL unbeschadet der Richtlinie 2008/114/EG[142] des Rates über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, die im Dezember 2008 veröffentlicht wurde.

Vorausgegangen war dieser Richtlinie ein Ersuchen des Rates „Justiz und Inneres" an die Kommission im Dezember 2005, einen Vorschlag für ein Europäisches Programm für den Schutz kritischer Infrastrukturen vorzulegen[143], wobei der dort zu berücksichtigende Ansatz sowohl von Menschen ausgehende technologische Bedrohungen als auch Naturkatastrophen berücksichtigt, vor allem jedoch die Gefahr möglicher Terroranschläge im Fokus haben sollte.[144]

Inhalt der Richtlinie war die Ermittlung und Ausweisung so genannter europäischer kritischer Infrastrukturen, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen hätte. Als kritische Infrastruktur werden gemäß Art. 2 der Richtlinie die in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon bezeichnet, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten. Für jede europäische kritische Infrastruktur sollen Sicherheitspläne oder gleichwertige Maßnahmen vorliegen sowie Sicherheitsbeauftragte zur Gewährleistung einer funktionierenden Kommunikation eingerichtet werden.

Gemäß Anhang II der Richtlinie haben die Sicherheitspläne bestimmte Mindestangaben zu enthalten, unter anderem Verfahren zur Sicherung von Informationssystemen, wobei hier keine konkreten Maßnahmen vorgeschrieben werden. Daraus lässt sich schließen, dass die Sicherheitspläne die Sicherung von Informationssystemen berücksichtigen sollen, darüber hinaus jedoch keine speziellen Standards vorgeschrieben sind, so wie dies in der NIS-RL geregelt wird. In einem ersten Schritt wurden europäische kritische Infrastrukturen bzw. Schwellwerte für deren Ermittlung nur für die Sektoren Energie (Strom, Öl und Gas) sowie Verkehr (Straßenverkehr, Schienenverkehr, Luftverkehr, Binnenschifffahrt, Hochsee- und Küstenschifffahrt und Häfen)

[142] RL 2008/114/EG des Rates v. 8.12.2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl. EU 2008 Nr. L 345/75 (Risikoanalyse, Ermittlung und Ausweisung, Sicherheitspläne, Sicherheitsbeauftragte);
[143] Zum Europäischen Programm für den Schutz kritischer Infrastruktur (EPCIP) siehe auch Kapitel 3.1.
[144] ErwGr 3 RL 114/2008.

geregelt. Eine darüberhinausgehende Einbeziehung weiterer Sektoren, wie beispielsweise dem Sektor der Informations- und Kommunikationstechnologien, erfolgte bis jetzt noch nicht.

Wenngleich die RL 114/2008 zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die NIS-RL auf den ersten Blick eine ähnliche Zielsetzung aufweisen, bestehen doch grundlegende Unterschiede. Dies soll einerseits durch die unterschiedlichen Begrifflichkeiten unterstrichen werden. Wo die RL 114/2008 von kritischen Infrastrukturen spricht, verweist die NIS-RL auf Betreiber wesentlicher Dienste, wenngleich in beiden Fällen grundsätzlich dieselbe Art von Unternehmen gemeint zu sein scheint. Die RL 114/2008 definiert kritische Infrastrukturen als Anlagen, Systeme oder Teile davon mit wesentlicher Bedeutung, wobei hier aus teleologischen Gesichtspunkten (insb. die Mindestanforderungen in den Sicherheitsplänen in Anhang II) primär auf physische Anlagen abzustellen sein wird.

Die NIS-RL definiert Betreiber wesentlicher Dienste als öffentliche oder private Einrichtung, welche bestimmte Kriterien, insbesondere die Abhängigkeit von IT-Systemen, erfüllt (Art. 4 Z 4 NIS-RL). Auch anhand der in den Anhängen der beiden Richtlinien angeführten (Teil-)Sektorenlisten (wenngleich die RL 114/2008 im ersten Schritt nur die Sektoren Energie und Verkehr anführte, eine Ausdehnung selbiger jedoch ankündigte) lässt sich im Grunde erkennen, dass ein sehr ähnlicher Adressatenkreis angesprochen wird.

Maßgeblicher Unterschied ist, dass es sich bei der RL 114/2008 um die Ermittlung europäischer kritischer Infrastrukturen – also jener Infrastrukturen, deren Ausfall grenzüberschreitende Auswirkungen hätte – handelt, wohingegen die NIS-RL die nationalen Betreiber wesentlicher Dienste identifizieren und deren Sicherheitsniveau anheben möchte. Warum nicht dennoch auch in der NIS-RL der Begriff „Betreiber kritischer Infrastruktur“ gewählt wurde, lässt sich wohl nur dadurch erklären, dass es sich bei den Betreibern wesentlicher Dienste um stark von IT-Systemen abhängigen Dienste handelt und durch verschiedene Begriffe die Unterscheidung im Verständnis zum Ausdruck gebracht werden sollte. Möglicherweise sollte auch in Anlehnung auf die Einbeziehung von Anbietern digitaler Dienste in den Richtlinientext eine einheitliche Begrifflichkeit[145] verwendet werden.

Im Zusammenhang mit genannter Richtlinie 114/2008 stellt sich die Frage nach deren Umsetzung in der nationalen Rechtsordnung, insbesondere zur vorgesehenen Erstellung von Sicherheitsplänen und Nennung von Sicherheitsbeauftragten durch europäische Betreiber kritischer Infrastruktur. Wie in Kapitel 3.1 (Schutz kritischer Infrastruktur in Österreich) angeführt, wurden die nationalen Maßnahmen per Ministerratsvortrag (MRV) im Österreichischen Programm zum Schutz kritischer

[145] Betreiber *wesentlicher* Dienste, Anbieter *digitaler* Dienste.

Infrastrukturgeregelt. Andere Rechtsgrundlagen zur Umsetzung finden sich in der nationalen Rechtsordnung nicht, von der grundsätzlichen Aufgabe der Sicherheitsbehörden zum vorbeugenden Schutz kritischer Infrastruktur (die aber nicht weiter auf die Richtlinienbestimmungen eingeht, siehe Kapitel 4.2.2 [Sicherheitspolizeigesetz]) abgesehen.

Ein Blick in das Programm zum Schutz kritischer Infrastruktur zeigt im Zusammenhang mit genannter Richtlinie lediglich einen Verweis auf bilaterale Vereinbarungen mit Deutschland, der tschechischen und der slowakischen Republik, die den Schutz europäischer kritischer Infrastrukturen in den jeweiligen Ländern verbessern soll.[146] Gemeint sind damit wohl Vereinbarungen zur Identifizierung europäischer kritischer Infrastrukturen, die eben genannte Länder betreffen.

Darüber hinaus sieht das Österreichische Programm im Kapitel der staatlichen Maßnahmen die Ausweisung strategischer Unternehmen vor (Maßnahme 6), wobei nicht von europäischen kritischen Infrastrukturen die Rede ist, sondern wohl nur die nationalen gemeint sind. Im Kapitel betreffend die Verpflichtungen der Betreiber wird die Einrichtung einer umfassenden Sicherheitsarchitektur durch die Unternehmen geregelt (Maßnahme 14). Die Erstellung von Sicherheitsplänen findet sich im gesamten Programm nicht. Erfasst ist – entsprechend der Vorgabe der Richtlinie – die vorgesehene Nominierung von Points of Contact für die staatlichen Stellen durch die Unternehmen (Maßnahme 17).

Fest steht somit, dass nicht alle in der Richtlinie genannten Maßnahmen innerstaatlich durch das Programm zum Schutz kritischer Infrastruktur geregelt wurden. Darüber hinaus ist jedoch auch zu hinterfragen, ob das Programm selbst zur Richtlinienumsetzung ausreicht, oder nicht vielmehr gesetzliche Maßnahmen beschlossen hätten werden müssen. Art. 288 Abs. 3 AEUV sieht für Richtlinien grundsätzlich vor, dass diese für jeden Mitgliedstaat hinsichtlich des zu erreichenden Ziels verbindlich seien, den innerstaatlichen Stellen jedoch die Wahl der Form und Mittel überlasse.[147] Somit verlangt Art. 288 AEUV nicht, dass die Bestimmungen einer Richtlinie förmlich und wörtlich in einer ausdrücklichen besonderen Gesetzesvorschrift wiedergegeben werden.[148] Generell muss die Umsetzung schon auf der Basis von Art. 288 Abs. 3 AEUV die praktische Wirksamkeit (effet utile) der Richtlinie unter Berücksichtigung des mit ihnen verfolgten Zwecks am besten gewährleisten.[149] Richtlinienumsetzungen haben nach der Rechtsprechung des EuGH

[146] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, S. 5.
[147] Dazu auch *Frenz*, Handbuch Europarecht, Band 5, Wirkungen und Rechtsschutz (2010), Rz 899.
[148] Siehe dazu bspw EuGH, Rs 231/87 u. 129/88, Slg. 1989, 3233 (3277, Rz 23) – Ufficio distrettuale ua; Rs C-446/98, Slg. 2000, I-11435 (11473, Rz 31) – Fazenda Publica.
[149] Siehe dazu EuGH, Rs 48/75, Slg. 1976, 497 (517, Rz 69/73) – Royer.

jedenfalls dann per Gesetz oder Verordnung zu ergehen, sofern durch die Richtlinie den Bürgern subjektive Rechte zukommen und diese mithin hinreichend transparent sein müssen.[150] Eine Regelung durch (interne) Verwaltungsvorschriften – wie bspw. der nationale MRV qualifiziert werden kann – kann jedoch ausnahmsweise erfolgen, soweit Richtlinien nicht die Rechtsposition von Dritten beeinflussen, sondern lediglich auf die nationale Verwaltungspraxis oder –organisation abzielen.[151]

Da die Richtlinie 114/2008 keine subjektiven Rechte Dritter regelt, kann somit zusammenfassend festgestellt werden, dass ein Beschluss des Ministerrats als interne Weisung an die nachgeordneten Organe (siehe dazu näher Kapitel 3.1 [Schutz kritischer Infrastruktur in Österreich]) ausreichend zur Umsetzung der Richtlinie geeignet erscheint. Nichtsdestotrotz wurde die Richtlinie wie weiter oben erörtert nicht vollständig umgesetzt, da wesentliche Bestandteile, wie die Identifizierung europäischer kritischer Infrastrukturen oder die Erstellung von Sicherheitsplänen durch die Betreiber, nicht geregelt sind.

5.2. Datenschutzgrundverordnung

Am 25. Mai 2018 trat die Datenschutz-Grundverordnung (DSGVO) in Kraft, die im Jahr 2016 vom europäischen Gesetzgeber verabschiedet wurde.[152] Damit soll eine Förderung der digitalen Wirtschaft im europäischen Binnenmarkt erreicht werden.[153]

Schon die DSGVO regelte bereits Pflichten für Unternehmen, die jenen der NIS-RL auf den ersten Blick ähnlich sind, jedoch einen anderen Zweck verfolgen. Wo die DSGVO bei ihren Vorgaben auf den Schutz personenbezogener Daten abzielt, bezwecken die Pflichten der NIS-RL die Sicherheit von Netz- und Informationssystemen. Gleichzeitig ist jedoch festzustellen, dass oftmals durch einen Vorfall beide Schutzziele betroffen sein können.[154] Aus diesem Grund sieht auch die NIS-RL eine enge Zusammenarbeit der zuständigen Behörden mit den Datenschutzbehörden vor.[155]

Eine dieser sich überschneidenden Bestimmungen ist das Treffen technischer und organisatorischer Sicherheitsmaßnahmen.[156] Zum Zwecke des Datenschutzes sind unter Berücksichtigung des

[150] Siehe dazu EuGH, Rs C-59/89, Slg. 1991, I2607 (2632, Rz 23) – Kommission/Deutschland; ebenso Rs. C-131/88, Slg. 1991, I-825 (867 f. Rz 6ff) – Grundwasserschutzrichtlinie; ua.
[151] *Frenz*, Handbuch Europarecht, Band 5, Wirkungen und Rechtsschutz, Rz 930.
[152] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl 2016, L 119/1.
[153] Siehe ErwGr 7, 9 DSGVO.
[154] Häufig können bei Sicherheitsvorfällen iSd NISG auch personenbezogene Daten iSd DSGVO betroffen sein.
[155] Siehe ErwGr 63 NIS-RL.
[156] Zur ähnlich lautenden Bestimmung der NIS-RL bzw. des NIS-Gesetzes siehe Kapitel 7.5.4.

Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DSGVO). Dabei beschränkt Art. 32 DSGVO die Bandbreite möglicher Maßnahmen nicht, Beispiele sind bauliche Maßnahmen zur Verhinderung eines unbefugten physischen Zugriffs, regelmäßige Schulungen von Angestellten und regelmäßige Überprüfungen des Datenschutzniveaus.[157]

Eine zweite Bestimmung, die sowohl im Datenschutzregime als auch zur Sicherheit von Netz- und Informationssystemen[158] vorgesehen ist, ist jene der Meldepflicht für Vorfälle. Zum Zwecke des Datenschutzes ist im Falle einer Verletzung des Schutzes personenbezogener Daten eine unverzügliche[159] Meldung vorgesehen (Art. 33 Abs. 1 DSGVO). Eine wesentliche Unterscheidung zur Meldepflicht nach dem NIS-Gesetz besteht im Umfang derselben, da bei der Meldung an die Datenschutzbehörde die Folgen der Verletzung des Schutzes personenbezogener Daten und die Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung im Vordergrund stehen.[160]

Ergänzend anzumerken ist, dass auch das NIS-Gesetz Datenschutzbestimmungen (§§ 9 ff NISG) vorsieht, um die Verarbeitung personenbezogener Daten zur Gewährleistung der Sicherheit von Netz- und Informationssystemen zu gewährleisten. Eine der Herausforderung bisher war auch, dass Unternehmen ungern Informationen über Cybervorfälle weitergaben, da sie befürchteten, dass sie dadurch Datenschutzbestimmungen verletzen könnten.[161] Dies wurde einerseits durch die DSGVO[162], als auch durch Übermittlungsbefugnisse im NISG (§ 10) gelöst.

[157] *Voigt/Von dem Bussche*, EU-Datenschutz-Grundverordnung (DSVO) : Praktikerhandbuch (2018), S. 48.
[158] Zur Bestimmung der Meldepflicht der NIS-RL bzw. des NISG siehe Kapitel 7.5.6.
[159] Möglichst binnen 72 Stunden.
[160] Zum Unterschied zwischen DSGVO und NIS-Gesetz siehe auch *Anderl et al.*, NISG::Kommentar, § 19, Rz 28.
[161] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit"), COM(2017) 477 final/3, 2.3.
[162] Siehe dazu ErwGr 49 DSGVO.

5.3. Richtlinie 2015/2366 für Zahlungsdienste im Binnenmarkt (PSD 2)

Für die Unterstützung des Wirtschaftswachstums der Union ist eine kontinuierliche Weiterentwicklung eines integrierten Binnenmarktes für sichere elektronische Zahlungen entscheidend.[163] Darüber hinaus haben sich die Sicherheitsrisiken für elektronische Zahlungen erhöht, was der größeren technischen Komplexität dieser Zahlungen und den neuen Arten von Zahlungsdiensten geschuldet ist und wovor Nutzer von Zahlungsdiensten angemessen geschützt werden sollten.[164]

Dementsprechend regelt die Richtlinie 2015/2366[165], dass Zahlungsdienstleister angemessene Risikominderungsmaßnahmen und Kontrollmechanismen zur Beherrschung der operationellen und der sicherheitsrelevanten Risiken im Zusammenhang mit den von ihnen erbrachten Zahlungsdienste schaffen.[166] Dazu wurden von der European Banking Authority (EBA) Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten herausgegeben.[167] Anhand dieser Leitlinie sollen unter anderem eine Risikobewertung, Schutzmaßnahmen wie die Integrität und Vertraulichkeit der Daten und Systeme, die physische Sicherheit, eine Zugriffskontrolle sowie die kontinuierliche Überwachung und Erkennung eingeführt werden.[168]

Neben der verpflichtenden Umsetzung dieser Sicherheitsvorkehrungen sind im Falle schwerwiegender Betriebs- oder Sicherheitsvorfälle unverzüglich die zuständigen Behörden zu unterrichten.[169] Die im Rahmen dieser Bestimmung veröffentlichten Leitlinien geben als Kriterien für die Klassifizierung schwerwiegender Vorfälle unter anderem die Zahl betroffener Zahlungsvorgänge, betroffene Zahlungsdienstnutzer, die Dienstausfallzeit sowie wirtschaftliche Auswirkungen vor. [170]

[163] ErwGr 5 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, ABl 2015 L 337/35.
[164] ErwGr 7 der RL (EU) 2015/2366; PSD 2.
[165] RL (EU) 2015/2366; PSD 2.
[166] Art. 95 Abs. 1 RL (EU) 2015/2366; PSD 2.
[167] Art. 95 Abs. 2 RL (EU) 2015/2366; PSD 2.
[168] EBA, "Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationallen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 (PSD2)," (2018).
[169] Art. 96 RL (EU) 2015/2366; PSD 2
[170] EBA, "Leitlinien für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie (EU) 2015/2366 (PSD2)," (2017).

Die Richtlinie wurde in Österreich mit dem Bundesgesetz über die Erbringung von Zahlungsdiensten (ZaDiG 2018) [171] umgesetzt, wobei der Umgang mit operationellen und sicherheitsrelevanten Risiken sowie die Meldung von Vorfällen in den §§ 85, 86 ZaDiG geregelt wurde.

Zur Abgrenzung zu den demselben Schutzzweck dienenden Bestimmungen des NIS-Gesetzes siehe Kapitel 7.5.7.

5.4. Richtlinie 2013/40 über Angriffe auf Informationssysteme

Die NIS-RL weist in ihrer Bestimmung zur Abgrenzung des Gegenstandes und Anwendungsbereiches (Art. 1 Abs. 4 NIS-RL) ausdrücklich darauf hin, dass sie unbeschadet der Richtlinie 2013/40/EU[172] gilt. Das Ziel dieser Richtlinie sind die Angleichung des Strafrechts der Mitgliedstaaten im Bereich von Angriffen auf Informationssysteme sowie die Verbesserung der Zusammenarbeit zwischen den zuständigen Behörden, Agenturen und Einrichtungen.[173]

Auch die Notwendigkeit der Verbesserung der Fähigkeit zum Schutz kritischer Infrastrukturen wird erwähnt, wobei die gegenständliche Richtlinie ihren Beitrag durch strengere Strafen bei Cyberangriffen leisten soll.[174] Dabei handelt es sich auch um das zentrale Abgrenzungselement zur NIS-RL , die ihren Beitrag zum Schutz kritischer Infrastruktur durch die Verpflichtung zu Sicherheitsvorkehrungen und Meldepflichten bei Vorfällen im Bereich der Prävention regelt, wohingegen die Richtlinie 2013/40/EU Maßnahmen als Reaktion auf Angriffe darstellt. [175]

5.5. Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie)

Die NIS-RL führt in ihren Erwägungsgründen[176] aus, dass die den Betreibern wesentlicher Dienste und Anbietern digitaler Dienste auferlegten Verpflichtungen nicht für Unternehmen gelten sollen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/EG[177] bereitstellen und die den besonderen Sicherheits- und Integritätsanforderungen jener Richtlinie unterliegen. Insbesondere

[171] Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018), BGBl. I Nr. 17/2018 idF BGBl. I Nr. 37/2018.
[172] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl 2013 L 218/8.
[173] ErwGr 1 RL 2013/40/EU.
[174] ErwGr 4 RL 2013/40/EU.
[175] Vgl. *Leisterer* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, S. 108.
[176] ErwGr 7 NIS-RL.
[177] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl 2002 L 108/33.

sind die öffentlichen Kommunikationsnetze oder -dienste aus eben diesem Grund nicht von den in Anhang II der NIS-RL gelisteten Sektoren bzw. Teilsektoren wesentlicher Dienste umfasst.

Die Rahmen-Richtlinie wurde mit der RL 2009/140/EG[178] unter anderem um jene zwei Artikel ergänzt, die nunmehr die unionsrechtliche Vorgabe für Maßnahmen zur Sicherheit und Integrität von Netzen und Diensten von Telekommunikationsbetreibern bilden (Art. 13a und 13b Rahmen-Richtlinie).

Art 13a Rahmen-Richtlinie regelt die Ergreifung angemessener technischer und organisatorischer Maßnahmen zur angemessenen Beherrschung der Risiken für die Sicherheit von Netzen und Diensten (Abs. 1), die Ergreifung geeigneter Maßnahmen, um die Integrität der Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen (Abs. 2) sowie die Mitteilung einer Verletzung der Sicherheit oder einen Verlust der Integrität an die zuständige nationale Regulierungsbehörde, die bzw. der beträchtliche Auswirkungen auf den Betrieb der Netze oder die Bereitstellung der Dienste hatte (Abs. 3).

Gegebenenfalls hat die nationale Regulierungsbehörde dabei die Regulierungsbehörden anderer Mitgliedsstaaten, die ENISA[179] oder auch die Öffentlichkeit zu unterrichten, wenn die Bekanntgabe im öffentlichen Interesse liegt (Abs. 3). Zur einfacheren Auslegung wurden von der ENISA Leitlinien[180] für die Umsetzung der Vorgaben des Art. 13a Abs. 1 und 2 sowie Leitlinien[181] für die Umsetzung der Vorgaben des Art 13a Abs. 3 erlassen.

Diese Verpflichtungen wurden in Österreich mit der 7. TKG-Novelle in § 16a Telekommunikationsgesetz (TKG)[182] umgesetzt. Zur Abgrenzung zu Sicherheitsvorkehrungen und Meldepflichten nach dem NIS-Gesetz siehe Kapitel 7.5.4 sowie 7.5.5.

[178] Richtlinie 2009/140/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste, ABl 2009 L 337/37.

[179] Europäische Agentur zur Sicherheit von Netz- und Informationssystemen.

[180] ENISA, „Technical Guideline on Security Measures“, siehe https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures, abgerufen am 27.10.2018.

[181] ENISA, „Technical Guideline on Incident Reporting“, siehe https://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting, abgerufen am 27.10.2018.

[182] Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I Nr. 70/2003 idF BGBl. I Nr. 111/2018.

5.6. Verordnung 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO)

Die eIDAS-VO[183] soll das Vertrauen in das Online-Umfeld von Verbrauchern, Unternehmen und öffentlicher Verwaltung zur Verwendung elektronischer Transaktionen oder digitaler Dienste stärken, wodurch die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der Union erhöht werden soll.[184] Die eIDAS-VO sieht vor, dass qualifizierte und nichtqualifizierte Vertrauensanbieter[185] geeignete technische und organisatorische Maßnahmen zur Beherrschung der Sicherheitsrisiken im Zusammenhang mit den von ihnen erbrachten Vertrauensdiensten ergreifen (Art. 19 Abs. 1 eIDAS-VO). Darüber hinaus haben diese Anbieter unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme von dem betreffenden Vorfall, jede Sicherheitsverletzung oder jeden Integritätsverlust, die bzw. der sich erheblich auf den erbrachten Vertrauensdienst oder die darin vorhandenen personenbezogenen Daten auswirkt, zu melden (Art. 19 Abs. 2 eIDAS-VO).

Auch wenn ein direkter Zusammenhang zwischen dieser Verordnung und der NIS-RL nicht auf den ersten Blick ersichtlich ist, gibt es insofern eine Überschneidung, als digitale Zertifikate üblicherweise als Authentifikationsmechanismus im Bankwesen, bei Cloud Services oder anderen wesentlichen Diensten verwendet werden, die im Anwendungsbereich des NIS-Regimes liegen. Ein Sicherheitsvorfall, der diese Zertifizierungen beeinträchtigt, kann sich somit auch zu einem Sicherheitsvorfall für Netz- und Informationssysteme von wesentlichen Diensten entwickeln. [186]

[183] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl 2014, L 257/73.
[184] ErwGr 1, 2 eIDAS-VO.
[185] Ein Vertrauensdiensteanbieter ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt (Art. 3 Z 19 eIDAS-VO);
[186] Reference document on Incident Notification for Operators of Essential Services, 2018, S. 13.

6. Cybersicherheit auf EU-Ebene

6.1. Die grenzüberschreitende Bedeutung von Cybersicherheit

Neben den enormen Vorteilen der Digitalisierung entstehen durch die Vernetzung von Systemen auch zahlreiche Risiken, die von Beginn an mitgedacht werden müssen. Diese Schwachstellen lassen sich durch die prinzipiell globale Verfügbarkeit des so genannten Netzes weltweit ausnutzen, weshalb Cybersicherheit eine globale Herausforderung darstellt.[187] Die Vernetzung erfolgt oft grenzüberschreitend, sodass Cybersicherheit nicht mehr nur in einem Staat alleine bewältigt werden kann. Beim Cyberspace wird immer schon von einem territorial entgrenzten Raum[188] gesprochen.

Das grenzübergreifende und vielschichtige Internet wurde zu einer der wirkungsvollsten Triebkräfte für den globalen Fortschritt, die ohne staatliche Aufsicht oder Regulierungen auskommen, wobei jedoch immer deutlicher wird, dass Vorgaben in Bezug auf Transparenz, Verantwortlichkeiten und Sicherheit notwendig sind.[189]

Das Internet spielt insbesondere bei der Erleichterung des grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehrs eine tragende Rolle. Daher sind sichere Netz- und Informationssysteme unerlässlich für das reibungslose Funktionieren des Binnenmarktes.[190] Aus diesem Grund bedarf es auch einer engeren internationalen Zusammenarbeit, damit die Sicherheitsstandards und der Informationsaustausch verbessert werden können. [191]

In den Erwägungsgründen der NIS-RL ist die Feststellung zu finden, dass bestehende Fähigkeiten nicht ausreichen, um ein hohes Sicherheitsniveau von Netz- und Informationssystemen in der Union zu gewährleisten. Dies führe dazu, dass Verbraucher und Unternehmen ein unterschiedliches Schutzniveau genießen und die Sicherheit von Netz- und Informationssystemen in der Union generell untergraben wird. [192] Um wirksam auf diese Herausforderungen reagieren zu können, ist deshalb ein umfassender Ansatz auf Unionsebene erforderlich, der gemeinsame

[187] *Leisterer* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, S. 102.
[188] *Leuschner*, Sicherheit als chartarechtliches Gewährleistungsziel in der EU, in Gusy/Kugelmann et al. (Hrsg), Rechtshandbuch Zivile Sicherheit (2017), Rz 1f.
[189] Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Cybersicherheitsstrategie der Europäischen Union - ein offener, sicherer und geschützter Cyberraum, Join(2013) 1 final.
[190] ErwGr 3 NIS-RL.
[191] ErwGr 43 NIS-RL.
[192] ErwGr 5 der NIS-RL.

Mindestanforderungen für Kapazitätsaufbau und -planung, Informationsaustausch, Zusammenarbeit sowie gemeinsame Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beinhaltet.[193]

6.2. Kompetenzgrundlage der Europäischen Union

Die NIS-RL spricht in ihren Erwägungsgründen von der Notwendigkeit einer Regulierung der Cybersicherheit, die für das reibungslose Funktionieren des Binnenmarktes (Art. 114 AEUV) erforderlich ist (siehe vorheriges Kapitel). In diesem Kapitel soll untersucht werden, ob diese Kompetenzgrundlage korrekt angewandt wurde oder die EU nicht vielmehr durch die Regelungen der NIS-RL ihre Kompetenz überschritten hat.

6.2.1. Kompetenz zum reibungslosen Funktionieren des Binnenmarktes

Die Art. 2 bis 6 AEUV regeln formal einen Kompetenzkatalog, wobei verschiedene Bereiche der Union entweder ausschließlich (Art. 3) oder in geteilter Zuständigkeit mit den Mitgliedstaaten (Art. 4-6) zugewiesen werden. Der Hauptbereich des Binnenmarktes befindet sich in geteilter Zuständigkeit der Union mit den Mitgliedstaaten (Art. 4 Abs. 2 lit. a AEUV). Das Ziel der Verwirklichung des Funktionierens des Binnenmarkts – ein Raum, in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleistet ist – findet sich in Art. 26 AEUV. [194]

Art. 114 AEUV dient der funktionalen Rechtsangleichung[195] und enthält eine an nur wenige, noch dazu final ausgerichtete Tatbestandsvoraussetzungen geknüpfte Ermächtigung der EU, die mitgliedstaatlichen Rechts- und Verwaltungsvorschriften[196] durch „Maßnahmen“, also durch alle möglichen verschiedenen Handlungsformen, anzugleichen[197], welche die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben (Art. 114 Abs. 1 AEUV). Der EuGH sieht in

[193] ErwGr 6 der NIS-RL.

[194] Den EU-Binnenmarkt zu vollenden, heißt die Voraussetzungen für einen europaweiten gemeinsamen Markt zu schaffen. Siehe *Müller*, Daseinsvorsorge und die EU: Anmerkungen zu einem alten Streit und jüngeren Entwicklungen, in Bos /Dieringer (Hrsg), Die Genese einer Union der 27, Die Europäische Union nach der Osterweiterung (2008), S. 206.

[195] *Kahl*, AEUV Art. 114, in Calliess /Ruffert (Hrsg), EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar (2011), Rz 8.

[196] Erfasst werden von Art. 114 (Rechts- und Verwaltungsvorschriften) jedenfalls alle Vorschriften mit abstrakt-generellem Charakter, die von einer staatlichen oder sonstigen, mit hoheitlichen Befugnissen ausgestatteten Stelle erlassen werden. Regelungen Privater unterfallen dem Art. 114 jedenfalls dann, wenn der Staat sich diese zu Eigen gemacht hat, etwa durch einen Verweis auf die „anerkannten Regeln der Technik“. Siehe *Rossi*, Artikel 114 AEUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (2012), Rz 5.

[197] *Rossi* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 2.

dieser Rechtsangleichungsbestimmung „die Milderung“ der sich aus der Unterschiedlichkeit nationaler Vorschriften ergebenden Hindernisse aller Art.[198] Solche Hindernisse sind jene, die geeignet sind, den innerunionalen Handel unmittelbar oder mittelbar, tatsächlich oder potentiell zu behindern.[199]

Die NIS-RL argumentiert diesbezüglich in ihren Erwägungsgründen, dass Netz- und Informationssysteme mit den zugehörigen Diensten eine zentrale Rolle in der Gesellschaft spielen. Für wirtschaftliche und gesellschaftliche Tätigkeiten und insbesondere für das Funktionieren des Binnenmarkts sei es demnach von entscheidender Bedeutung, dass sie verlässlich und sicher sind.[200] Mit der NIS-RL solle durch den Aufbau von Vertrauen ein besseres Funktionieren des Binnenmarktes bezweckt werden.[201]

In diesem Zusammenhang ist auch die EU-Strategie für einen digitalen Binnenmarkt[202] zu nennen, die auf drei Pfeilern, unter anderem Schaffung der richtigen Bedingungen für florierende digitale Netze und Dienstleistungen, beruht. Zu solchen Bedingungen zählt neben Regelungen zum Datenschutz[203] wohl auch die Sicherheit der Netz- und Informationssysteme dieser Dienstleistungen. Eine schwere Störung dieser Systeme in einem MS kann auch andere MS und die EU insgesamt in Mitleidenschaft ziehen.[204]

Die Europäische Kommission schätzt, dass Europa sein BIP um fast 500 Mrd. Euro jährlich[205] steigern kann, sobald der digitale Binnenmarkt vollendet ist. Durch die genannte Initiativen zu Cybersicherheit und Datenschutz setzt die EU wichtige Eckpfeiler für eine digitale Standortpolitik Europas.[206]

Auf die NIS-RL und ihre Kompetenz zurückkommend könnte sich die EU grundsätzlich auf die Rechtsangleichung des Art. 114 AEUV beziehen, da Dienstleistungen, die den freien Binnenmarkt gewährleisten, ohne funktionierende Netz- und Informationssysteme nicht mehr denkbar sind. Der EuGH sieht den Ermessensspielraum des Art. 114 AEUV insbesondere in jenen Bereichen gegeben, die durch komplexe technische Eigenheiten gekennzeichnet sind.[207]

---

[198] EuGH, Rs. 193/80, Slg. 1981, 3019, Rz. 17.
[199] EuGH, Rs 8/74, Slg. 1974, 837, Rz 2/4 – Dassonville.
[200] ErwGr 1 der NIS-RL.
[201] ErwGr 31.
[202] COM(2015) 192 final .
[203] *Sparenberg/Pohlmann*, Cybersecurity made in EU, Datenschutz und Datensicherheit - DuD, 4/2018, S. 220.
[204] *Bendiek*, Kritische Infrastruturen, Cybersicherheit und Datenschutz: die EU schlägt Pföcke für digitale Standortpolitik ein, SWP-Aktuell, 35/2013, S. 2
[205] durchschnittlich 1000 Euro pro Kopf.
[206] *Bendiek*, SWP-Aktuell, 2013, S. 1
[207] EuGH, Rs C-66/04, Slg. 2005, I-10553, Rn 45.

Dabei stellte sich in der Vergangenheit bereits öfter die Frage, ob im Sinne des Art. 114 AEUV bereits potenzielle Handelshemmnisse, dh Handelshemmnisse, die noch nicht bestehen, jedoch möglicherweise entstehen können, durch präventive Rechtsangleichung des Gesetzgebers der Europäischen Union abgewendet werden können.[208] Lehre[209] und Rechtsprechung[210] gehen von dieser Möglichkeit aus, wobei Art. 114 AEUV nur dann als Rechtsgrundlage herangezogen werden dürfe, wenn aus dem Rechtsakt objektiv und tatsächlich hervorgehe, dass er den Zweck hat, die Voraussetzungen für die Errichtung und das Funktionieren des Binnenmarktes zu verbessern.[211]

Da hier im Fall des Art. 114 AEUV durch Rechtsangleichung Kompetenzen zu Lasten der Mitgliedstaaten auf die Europäische Union verlagert werden, reicht es nicht aus, diesen Nachweis nur in Form abstrakter Auffassungen und durch nicht belegbare Behauptungen zu führen.[212] Vielmehr müsse das Entstehen solcher Hindernisse wahrscheinlich sein und die fraglichen Maßnahmen ihre Vermeidung bezwecken.[213]

Das Vereinigte Königreich Großbritannien argumentierte (schlussendlich erfolglos) in einer Klage gegen die Rechtsgrundlage zur Einrichtung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA)[214], dass die Begründung der Verordnung in Bezug auf die Wahrscheinlichkeit, dass unterschiedliche nationale Anforderungen an die Informationssicherheit zu Handelshemmnissen führten, unzureichend wäre. Die bloße Möglichkeit einer heterogenen Umsetzung der Anforderungen an die Netzsicherheit und der Umstand, dass diese Anforderungen zu ineffizienten Lösungen und Hindernissen für den Binnenmarkt führen könnten, wären keine ausreichende Begründung. [215] Das Parlament entgegnete dem, der Unionsgesetzgeber habe angesichts der technischen Komplexität und der schnellen Entwicklung des in Rede stehenden Bereiches die Verordnung erlassen, um Handelshemmnisse und den Effizienzverlust zu verhindern, zu denen es bei einer nicht koordinierten Regelung der technischen und organisatorischen Durchführung durch die Mitgliedstaaten kommen könne. [216]

---

[208] *Seidel*, Präventive Rechtsangleichung im Bereich des Gemeinsamen Marktes, Europarecht, 1/2006, S. 26.
[209] *Rossi* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar. Ebenso *Kahl* in Calliess /Ruffert, EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar, Rz 18.
[210] EuGH, Rs. C-376/98, Slg. 2000, I-8419, Rz 86 – Tabakwerbung zur TabakwerbeRL, 98/43/EG.
[211] EuGH, Rs C-66/04, Slg. 2005, I-10553.
[212] *Seidel*, Europarecht, 2006, S. 28.
[213] EuGH, Rs. C-350/92, Slg. 1995, I-1995, Rz 35 – Schutzzertifikat für Arzneimittel.
[214] Mehr zur ENISA, siehe Kapitel 6.3.
[215] EuGH, Rs C-217/04, Slg. 2006 I-3798, Verordnung (EG) Nr. 460/2004 - Europäische Agentur für Netz- und Informationssicherheit - Wahl der Rechtsgrundlage, Rz 20.
[216] EuGH, Rs C-217/04, Slg. 2006 I-3798, Verordnung (EG) Nr. 460/2004 - Europäische Agentur für Netz- und Informationssicherheit - Wahl der Rechtsgrundlage, Rz 25.

6.2.2. Prinzipien der begrenzten Einzelermächtigung und des „effet utile“

Hinsichtlich der grundsätzlichen Zuständigkeiten bzw. Kompetenzen der EU ist auf die begrenzte Einzelermächtigung, die Subsidiarität und die Verhältnismäßigkeit zu verweisen (Art. 5 Abs. 1 EUV). Nach dem Grundsatz der begrenzten Einzelermächtigung wird die EU nur innerhalb der Grenzen der Zuständigkeiten tätig, die die Mitgliedstaaten ihr übertragen haben. Alle der EU nicht in den Verträgen übertragenen Zuständigkeiten verbleiben demnach bei den Mitgliedstaaten (Art. 5 Abs. 2 EUV).

Da der EU die Kompetenz der Netz- und Informationssystemsicherheit nicht ausdrücklich zugewiesen wurde[217], könnte nun argumentiert werden, dass die Zuständigkeit dafür eigentlich in der Hand der Mitgliedstaaten verbleiben müsste.[218] Für jeden verbindlichen Rechtsakt der EU muss nicht nur eine ausdrückliche, sondern auch die richtige Kompetenzgrundlage gesucht werden, da dies für Organkompetenz, Handlungsformen und Verfahren entscheidend ist.[219]

In diesem Zusammenhang ist auf das Prinzip des „effet utile“ (Effizienz und Wirksamkeit) zu verweisen, welches sich auf das Verständnis einer Vorschrift bezieht, die nach ihrem Ziel und ihrer Zweckrichtung auszulegen ist.[220] Obwohl das Prinzip der begrenzten Einzelermächtigung dem scheinbar widerspricht, soll das Prinzip „effet utile“ trotzdem gelten – die begrenzte Einzelermächtigung enthält demnach kein grundsätzliches Gebot einer restriktiven Auslegung von Kompetenznormen.[221]

---

[217] In materiell-rechtlicher Hinsicht ist die Steuerungswirkung der Infrastrukturverantwortung primärrechtlich sonst nur schwach ausgeprägt. Im europäischen Katastrophenschutz spielen Cyberangriffe auf kritische Infrastrukturen für die Anwendung der Solidaritätsklausel des Art. 222 AEUV nur bei Terroranschlägen auf Infrastrukturen eine Rolle – vgl. Beschluss des Rates vom 24.06.2014 über die Vorkehrungen für die Anwendung der Solidaritätsklausel durch die Union (2014/415/EU9, ABl. Nr. L 192 S. 53, ber. ABl. Nr. L 221 S. 26 und ABl. Nr. L 275 S. 7. Art. 2 Abs. 1 b), siehe dazu *Leisterer* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, S. 105. Dazu auch *Vedder*, Artikel 222 AEUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (2012), Rz 1ff.

[218] Als selbstverständliche Konsequenz des Grundsatzes der Einzelermächtigung konstatiert Art. 4 Abs. 1 EUV deklaratorisch, dass alle nicht der Union übertragenen Zuständigkeiten bei den Mitgliedstaaten bleiben. Siehe *Vedder* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 5.

[219] *Calliess*, EUV Art. 5, in Calliess /Ruffert (Hrsg), EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar (2011), Rz 7.

[220] Der EuGH erkennt in ständiger Rechtsprechung an, dass auf Grundlage des effet utile dem Unionsrecht auch über den Wortlaut von Kompetenzzuweisungen hinaus eine umfassende Nutzwirkung zukommen muss. Dieser Rechtsprechung wurde vorgeworfen, dass sie den Effektivitätsgrundsatz als Grundlage für die Schaffung von Rechtsinstituten genutzt hat, für die es keinen konkreten vertraglichen Anknüpfungspunkt gibt. Soweit kein rechtlicher Anknüpfungspunkt vorhanden sei, könne auch der Effektivitätsgrundsatz keine Anwendung finden - *Frenz*, Handbuch Europarecht, Band 5, Wirkungen und Rechtsschutz, Rz 427-31.

[221] *Vedder* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 9.

Der Grundsatz der begrenzten Einzelermächtigung wirkt wiederum direkt beschränkend für eine Auslegung anhand des „effet utile“ und einen allzu weitreichenden Geltungsanspruch der Unionsziele gegenüber mitgliedstaatlicher Souveränität. Er schließt generalklauselartige Kompetenzzuweisungen wie Art. 114 AEUV jedoch nicht aus[222], wobei diese Bestimmung aber gleichzeitig keine allgemeine Kompetenz zur Regelung des Binnenmarkts[223] enthalten soll.[224]

Der EuGH betonte im Jahr 1998, dass die Vorgehensweise, den Art. 95 EGV (heute Art. 114 AEUV) dahin auszulegen, dass er dem Gemeinschaftsgesetzgeber eine allgemeine Kompetenz zur Regelung des Binnenmarktes gewährte, nicht nur dem Wortlaut der genannten Bestimmungen widerspräche, sondern auch mit dem niedergelegten Grundsatz, dass die Befugnisse der Gemeinschaft auf Einzelermächtigungen beruhen, unvereinbar wäre.[225] Der EuGH änderte seine diesbezügliche Linie[226] jedoch zunehmend.[227] Beispielsweise durfte die Richtlinie über die Vorratsdatenspeicherung (2006/24/EG) auf der Grundlage von Art. 95 EGV erlassen werden. Denn sie betreffe in überwiegendem Maß das Funktionieren des Binnenmarkts und nicht die Ermittlung, Feststellung und Verfolgung von Straftaten.[228]

Frenz versucht, die beiden Grundsätze folgendermaßen gegenüberzustellen: Der Grundsatz des „effekt utile“ ermögliche eine dynamische und anpassungsfähige Interpretation der auf Integration und Fortentwicklung ausgerichteten unionsrechtlichen Vorschriften. Dem Gerichtshof der EU werde damit die Möglichkeit eröffnet, auf neue Entwicklungen innerhalb der Unionsrechtsordnung geeignet zu reagieren.[229] Jedoch verlange das Prinzip der begrenzten Einzelermächtigung eine sachliche Begrenzung der von der nationalen auf die europäische Ebene übertragenen Hoheitsrechte, die es ausschließt, dass Zuständigkeiten „zur dynamischen Fortentwicklung übertragen“ oder erweiternd abgerundet oder sachlich ausgedehnt werden.[230]

---

[222] *Vedder* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 7.

[223] Die Entscheidung des EuGH zur Weitergabe von Fluggastdaten hat die Möglichkeiten der Inanspruchnahme der Generalklausel des Art. 95 EGV (nunmehr Art. 114 AEUV) ein wenig beschränkt und sie dadurch zugleich wieder mehr in das System der begrenzten Einzelermächtigung und des Subsidiaritätsprinzips zurückgeholt - EuGH, verb. Rs 317/04 u. 318/04, Parlament/Rat u. Kommission, Slg. I-2006, 4721, insb. Rn 67ff.

[224] *Frenz*, Handbuch Europearecht, Band 6, Institutionen und Politiken (2011), Rz 2189.

[225] EuGH, Rs. C-376/98, Slg. 2000, I-8419 – Tabakwerbung zur TabakwerbeRL, 98/43/EG.

[226] *Calliess* in Calliess /Ruffert, EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar, Rz 14.

[227] Zunächst bezieht sich diese Änderung auf das Urteil EuGH, Rs. C-380/03, Slg 2006, I-11573 – geänderte Tabakwerberichtlinie.

[228] EuGH, Rs. C-301/06 - Richtlinie zur Vorratsdatenspeicherung.

[229] *Frenz*, Handbuch Europarecht, Band 5, Wirkungen und Rechtsschutz, Rz 436.

[230] *Frenz*, Handbuch Europarecht, Band 5, Wirkungen und Rechtsschutz, Rz 427. *Calliess/Ruffert* sehen die effet utile-Auslegung mit dem Prinzip der begrenzten Einzelermächtigung vereinbar und argumentieren dies

Zusammenfassend lässt sich im Ergebnis mE feststellen, dass die Kompetenzgrundlage des Art. 114 AEUV dem Prinzip der begrenzten Einzelermächtigung des Art. 5 Abs. 2 AEUV nicht widerspricht. Eine Rechtsangleichung erscheint insbesondere deshalb erforderlich, da die technische Entwicklung der letzten Jahre eine immer stärkere Interdependenz zwischen den Mitgliedstaaten hervorruft. Der Ausfall von Netz- und Informationssystemen eines Energieversorgers eines Mitgliedstaates beispielsweise kann zu einem Kaskadeneffekt in der gesamten EU führen und das Funktionieren des Binnenmarktes massiv beeinträchtigen. Dies gilt gleichermaßen für Mitgliedstaaten-übergreifende Finanz- oder Transportsysteme, die alle vom Anwendungsbereich der NIS-RL betroffen sind. Somit kann es nur im Interesse aller Mitgliedstaaten sein, gewährleistet zu wissen, dass sich die Sicherheitsstandards dieser Systeme aller Mitgliedstaaten auf einem hohen Niveau befinden. Ob diese Hemmnisse bereits bestehen, dh ob in einigen Mitgliedstaaten sehr geringe Standards dieser Einrichtungen gegeben sind, kann nicht beurteilt werden – potenzielle Handelshemmnisse bestehen jedoch jedenfalls.

6.2.3. Subsidiarität und Verhältnismäßigkeit

Neben dem Prinzip der begrenzten Einzelermächtigung sieht Art. 5 AEUV Abs. 1 das Subsidiaritätsprinzip[231] und das Prinzip der Verhältnismäßigkeit[232] vor. [233]

Das Subsidiaritätsprinzip besagt, dass die Union in jenen Bereichen, die nicht in ihre ausschließliche Zuständigkeit fallen, nur tätig werden darf, sofern und soweit die Ziele der in Betracht gezogenen Maßnahmen von den Mitgliedstaaten weder auf zentraler noch auf regionaler oder lokaler Ebene ausreichend verwirklicht werden können[234], sondern vielmehr wegen ihres Umfangs oder ihrer

mit der weniger weitreichenden Auslegungsmethode als jener der anerkannten implied powers, siehe *Calliess* in Calliess /Ruffert, EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar, Rz 18.

[231] Nähere Regelungen zum Subsidiaritätsprinzip, insb. zur verfahrensmäßigen Sicherstellung der Einhaltung der Subsidiarität, zu finden im Protokoll (Nr. 2) über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit, ABl 2008 C 115/206.

[232] Das Verhältnismäßigkeitsprinzip besagt, dass die finanzielle Belastung und der Verwaltungsaufwand der Union, der nationalen Regierungen, der regionalen und lokalen Behörden, der Wirtschaftsteilnehmer und der Bürgerinnen und Bürger so gering wie möglich zu halten sind und in einem angemessenen Verhältnis zu dem angestrebten Ziel zu stehen haben, siehe RL (EU) 2008/Protokoll (Nr. 2) über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit, Art. 5 S. 5.

[233] Der Subsidiaritätsgrundsatz und der Verhältnismäßigkeitsgrundsatz wurden eingeführt, um einer zu unionsfreundlichen Auslegung zu begegnen, siehe *Vedder* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 9.

[234] Im Rahmen dieser als „Negativkriterium" bezeichneten Formulierung soll geprüft werden, ob die angestrebte Maßnahme transnationale Aspekte hat, die durch die Mitgliedstaaten nicht zufriedenstellend geregelt werden können, siehe *Calliess* in Calliess /Ruffert, EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar, Rz 34.

Wirkung auf Unionsebene besser[235] zu verwirklichen sind (Art. 5 Abs. 3 AEUV). Bei der Subsidiarität geht es somit um die Frage der Kompetenzausübung im Hinblick auf durch die Verträge bereits verteilten Kompetenzen, und nicht um eine eigenständige Kompetenzverteilung per se.[236]

Dabei ist jedenfalls die Verhältnismäßigkeit zu berücksichtigen, sodass die Maßnahmen der Union inhaltlich wie formal nicht über das für die Erreichung der Ziele der Verfassung erforderlich Maß hinausgehen (Art. 5 Abs. 4 AEUV). Ein Vergleich des geplanten Handelns auf Unionsebene mit den Folgen eines Verzichts auf Unionshandeln und den Möglichkeiten auf mitgliedstaatlicher Ebene muss für ersteres deutliche Vorteile ergeben.[237] Für die Sicherheitsgewährleistung soll unionsverfassungsrechtlich klargestellt sein, dass die überkommene staatliche Garantie nur insoweit gemeinschafts-/unionsrechtlich zu überlagern ist, als ihre Einlösung auf mitgliedstaatlicher Ebene entweder als solche (z. B. wegen transnationaler Bezüge) oder aber im Blick auf die Erreichung anderer Unionsziele (z. B. die Ausübung der Grundfreiheiten im Binnenmarkt) Defizite aufweist, und daher besser im Rahmen der Gemeinschaft/der Union zu erledigen ist.[238]

Die ErwGr der NIS-RL sprechen diesbezüglich davon, dass ein hohes gemeinsames Sicherheitsniveau in der EU von den Mitgliedstaaten selbst nicht ausreichend verwirklicht hätte werden können, sondern vielmehr wegen der Wirkung der Maßnahme auf Unionsebene besser zu verwirklichen war, und dadurch im Einklang mit dem Subsidiaritätsprinzip stehe. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.[239]

Dieser Begründung kann man sich nur anschließen und feststellen, dass die Regelung auf Unionsebene deutliche Vorteile gegenüber der mitgliedstaatlichen Ebene bringt. Diese führt einerseits zu einheitlich hohen Standards, die durch mitgliedstaatliche Regelungen wohl nicht zu erreichen gewesen wären. Darüber hinaus wird durch eine unionsweite Meldepflicht von Sicherheitsvorfällen das Ziel erreicht, alle Mitgliedstaaten über aktuelle, schwerwiegende Vorfälle zu informieren, von denen sie betroffen sein könnten und die eine Gefahr für die Sicherheit ihrer

[235] Die Bewertung im Rahmen dieses „Positivkriteriums“ muss ergeben, dass eine Maßnahme auf EU-Ebene wegen ihrer breiteren allgemeineren Wirkung dem angestrebten Ziel näher komme als ein individuelles Handeln der Mitgliedstaaten, siehe *Calliess* in Calliess /Ruffert, EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar, Rz 40.
[236] *Calliess* in Calliess /Ruffert, EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar, Rz 21.
[237] *Vedder* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 18.
[238] *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union (2002), S. 592.
[239] ErwGr 74 der RL.

Netz- und Informationssysteme betrifft. Die in Art. 5 Abs. 3 EUV geforderte Transnationalität kann im Rahmen der Cybersicherheit mE wohl kaum in Frage gestellt werden.

Da aus Sicht des EuGH ein europäischer Rechtsakt erst dann rechtswidrig ist, wenn er zur Erreichung der Ziele „offensichtlich ungeeignet" ist[240], und dafür keine Gründe vorliegen, erscheint mE auch die Verhältnismäßigkeit gegeben.

6.2.4. Vorbehalt der Aufrechterhaltung der öffentlichen Ordnung und der Schutz der inneren Sicherheit als mitgliedstaatliche Aufgabe

Der Vertrag über die Europäische Union (EUV) sieht vor, dass die Union die grundlegenden Funktionen des Staates, insbesondere die Wahrung der territorialen Unversehrtheit, die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der nationalen Sicherheit zu achten hat. Insbesondere die nationale Sicherheit fällt weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten (Art. 4 Abs. 2 EUV).[241]

Mit Art. 72 AEUV wird den Mitgliedstaaten zur Aufrechterhaltung der öffentlichen Ordnung und zum Schutz der inneren Sicherheit die finale Zuständigkeit zugewiesen. Der Begriff der öffentlichen Ordnung ist dabei eher eng auszulegen[242], der Begriff der inneren Sicherheit meint auch ordnungsrechtliche Maßnahmen, die den Raum der Freiheit und Sicherheit gewährleisten. [243]

Anzumerken ist in diesem Zusammenhang, dass Art. 72 AEUV keine Kompetenzschranke bzw. keine negative Kompetenzabgrenzungsregelung darstellt und die Union somit nicht von vornherein von jeglicher Regelungsmaßnahme[244] ausschließt.[245] [246]

---

[240] EuGH, Rs C-491/01, BAT, Slg. 2002, I-11453 Rn 123, auch *Vedder* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 1ff.

[241] Auch als ordre-public-Vorbehalt zugunsten der Mitgliedstaaten bezeichnet, siehe *Rossi*, AEUV Art. 72, in Calliess /Ruffert (Hrsg), EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar (2011), Rz 1.

[242] Die Vorbehaltsklausel ist mithin zwar unionsrechtlich auszulegen, den Mitgliedstaaten ist aber in der Anwendung ein weiter Beurteilungsspielraum zuzubillen, den der EuGH durch eine entsprechende Rücknahme seiner Kontrolldichte zu respektieren hat. Umgekehrt wird man von den Mitgliedstaaten eine substantiierte Begründung für die Inanspruchnahme des ordre-public-Vorbehalts fordern können, siehe *Rossi* in Calliess /Ruffert, EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar, Rz 7.

[243] *Rosenau/Petrus*, Artikel 72 AEUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (2012), Rz 2.

[244] Die Rolle der Union im Rahmen der Sicherheitsgewährleistung beschränkt sich bislang weitgehend auf die Unterstützung, Koordinierung und Finanzierung nationaler Maßnahmen, siehe *Schöndorf-Haubold* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rn. 3.

[245] *Rosenau/Petrus* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 5.

[246] Cybersicherheitspolitik als zwischen MS und EU-Ebene geteilter Kompetenzbereich, siehe Bendiek, "Gemeinsame Außen- und Sicherheitspolitik der EU: von der Transformation zur Resilienz," ed. (SWP) (Berlin2017), S. 21.

Möstl argumentiert hier, dass die Befugnisse zur Verwirklichung des Binnenmarktes in einem breiten Bereich des wirtschaftsbezogenen Ordnungsrechts die Grundlage für Maßnahmen darstellen, die früher Bestandteil der mitgliedstaatlichen Sicherheitsgewährleistung waren.[247]

Vedder meint dazu, dass Art. 72 AEUV natürlich Einschränkungen des Binnenmarktes rechtfertigen und die Unionskompetenzen – und dies gilt auch für jene zur Verwirklichung des Binnenmarktes - in diesem Bereich begrenzen kann. [248] Somit ist festzustellen, dass gegenständlicher EU-Rechtsakt zur Gewährleistung der Sicherheit von Netz- und Informationssystemen dann als rechtswidrig anzusehen wäre, sofern dies eindeutig in den Bereich der öffentlichen Ordnung und Schutz der inneren Sicherheit fallen würde.

Zu beobachten ist nach *Schöndorf-Haubold* eine stetig fortschreitende Zentralisierung und damit unionale Versicherheitlichung. Dabei kommt es zur Verrechtlichung von Pflichten zum Informationsaustausch und zur Kooperation sowie durch die allmähliche Ausbildung eines Einsatzrechts für die unterschiedlichen gemeinsamen operativen Teams, die bereits einen Baustein eines übergreifenden unionalen Sicherheitsrechts darstellen.[249]

Im Zusammenhang mit Art. 72 AEUV ist nun die Frage zu stellen, ob Regelungen zur Sicherheit von Netz- und Informationssystemen den Bereich der öffentlichen Ordnung oder den Schutz der inneren Sicherheit betreffen und aus diesem Grund in der alleinigen Zuständigkeit der Mitgliedstaaten liegen sollten. Die NIS-RL selbst sieht in ErwGr 8 vor, dass die Möglichkeit der Mitgliedstaaten, Maßnahmen zu ergreifen, die für die Wahrung der wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung erforderlich sind, von der Richtlinie unberührt bleiben sollen. [250]

Meines Erachtens regelt die NIS-RL nicht eindeutig Bereiche, die genannter Vorbehaltsklausel zu subsumieren sind. Möglicherweise könnte argumentiert werden, dass ordnungsrechtliche Maßnahmen vorgesehen werden, die den Raum der Sicherheit gewährleisten (Art. 72 AEUV). Hier verschwimmen jedoch die Grenzen zwischen Bedingungen zum Funktionieren des Binnenmarktes, ziviler Sicherheit[251] bzw. Daseinsvorsorge, polizeilichen[252] bzw. ordnungsrechtlichen Aufgaben

[247] *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, Rz 524.
[248] *Vedder* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 12.
[249] *Schöndorf-Haubold* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rn. 8.
[250] ErwGr 8 der NIS-RL.
[251] Zur zivilen Sicherheit als grenzüberschreitende Aufgabe siehe *Leuschner* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, S. 174.
[252] So ist etwa die RL 2013/40/EU über Angriffe auf Informationssysteme auf die Kompetenz zum Erlass von Strafrechtsnormen zur Bekämpfung von Computerkriminalität gemäß Art. 83 Abs. 1 AEUV gestützt.

sowie militärischer Verteidigung bzw. Cyberverteidigung.[253] In diesem Zusammenhang wird auch oftmals von Cybersicherheit als Querschnittsbereich[254] oder Mehrebenensystem[255] gesprochen. [256]

Der im Primärrecht genannte Raum der Freiheit, der Sicherheit und des Rechts (Art. 67 AEUV) der Europäischen Union bringt es meines Erachtens mit sich, dass die Union auch Regelungen trifft, die diesen Raum der Sicherheit gewährleisten, ohne explizit in den mitgliedstaatlichen Vorbehalt (Art. 72 AEUV) einzugreifen. [257] Der Spielraum der Union zur Gewährleistung eines Raums der Sicherheit vergrößert sich, je weiter die Maßnahmen von der eigentlichen inneren Sicherheit im engeren Sinne entfernt sind.[258]

6.2.5. Vorbehalt der Daseinsvorsorge als mitgliedstaatliche Aufgabe

Neben dem Prinzip der begrenzten Einzelermächtigung, der Subsidiarität, dem Verhältnismäßigkeitsgrundsatz und dem Vorbehalt der nationalen Sicherheit soll schlussendlich noch untersucht werden, ob Regelungen zur Daseinsvorsorge[259] in die Zuständigkeit der Mitgliedstaaten fallen. Dadurch könnte die NIS-RL, die wesentliche Bedingungen für Betreiber der nationalen Daseinsvorsorge festlegt, rechtswidrig sein.

Grundsätzlich haben die EU und die Mitgliedstaaten im Rahmen ihrer jeweiligen Befugnisse im Anwendungsbereich der Verträge dafür Sorge zu tragen, dass die Grundsätze und Bedingungen für das Funktionieren von Diensten von allgemeinem[260] wirtschaftlichem Interesse[261] so gestaltet sind,

---

[253] So auch *Leisterer* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, S. 104. Sowie *Bendiek*, Europäische Cybersicherheitspolitik, SWP, 2012, S. 20 ff.

[254] Zur Cybersicherheit auf Ratsarbeitsebene als Querschnittsaufgabe siehe Bendiek, "Gemeinsame Außen- und Sicherheitspolitik der EU: von der Transformation zur Resilienz," S. 21.

[255] Zum Begriff des Mehr-Ebenen-Systems der Europäischen Union siehe *Vedder* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 8.

[256] Die Regelung des Marktes setzt grundsätzlich auf verschiedenen Ebenen an. Die globale Standardsetzung sollte in internationalen Foren erfolgen, der Datenschutz sollte einheitlich auf der EU-Ebene geregelt sein, und die Verfolgung digitaler Straftaten gehört auch auf die nationale Ebene (gegebenenfalls EU-weite Koordinierung). Darauf ergibt sich, dass die digitale Regulierung als eine Mehrebenenstruktur zu verstehen ist, *Bendiek*, Digitale Agenda und Cybersicherheit, in Weidenfeld /Wessels (Hrsg), Jahrbuch der Europäischen Integration 2016 (2016), S. 229.

[257] Ähnlich dazu *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, S. 529.

[258] „Je ziviler die Sicherheit, desto europäischer kann sie potenziell werden“, siehe *Schöndorf-Haubold* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rn. 4.

[259] Mehr dazu siehe Kapitel 7.5.1.1.

[260] Material liegt der Unterschied eines privaten zu einem Dienst von allgemeinem wirtschaftlichen Interesse darin, dass die Allgemeinwohlorientierung bei dem einen das eigentliche Ziel der Tätigkeit ist, bei dem anderen nur Mittel zum Zweck der Gewinnerzielung, siehe Supiot C.J.E.G. 1994, 379, 383 in *Linder*, Daseinsvorsorge in der Verfassungsordnung der Europäischen Union (2004), S. 126.

[261] Allgemeines wirtschaftliches Interesse: im Interesse der Allgemeinheit erbracht und daher von den MS mit besonderen Gemeinwohlverpflichtungen verbunden; gemeint sind insbesondere Verkehrs-, Energieversorgungs- und Telekommunikationsdienste, siehe ABl. 1996 C 281/3, S. 3. Die Kommission spricht

dass diese ihren Aufgaben nachkommen können (Art. 14 AEUV).[262] Dabei wird der Union eine Verbandskompetenz zur gesetzlichen Festlegung der funktionsgerechten Gestaltung dieser Grundsätze und Bedingungen verliehen, begrenzt um die Zuständigkeit der Mitgliedstaaten.[263]

Nicht unerwähnt bleiben soll auch Art. 36 GRC, wonach die Union den Zugang zu Dienstleistungen von allgemeinem wirtschaftlichen Interesse, wie er durch die einzelstaatlichen Rechtsvorschriften und Gepflogenheiten geregelt ist, anzuerkennen und zu achten hat. Art. 36 GRC wendet sich somit explizit an die EU. Ob durch diese Bestimmung überhaupt ein Recht im eigentlichen Sinne vorliegt, ist umstritten.[264]

Für Unternehmen, die mit Dienstleistungen von allgemeinem wirtschaftlichem Interesse betraut sind, gelten die Vorschriften der Verträge, insbesondere die Wettbewerbsregeln, soweit die Anwendung dieser Vorschriften nicht der Erfüllung der ihnen übertragenen besonderen Aufgabe rechtlich oder tatsächlich verhindert (Art. 106 AEUV).

Hier ist insbesondere der Begriff der „Betrauung“ („mit Dienstleistungen von allgemeinem wirtschaftlichem Interesse „betraut“) wesentlich. Nach Ansicht des EuGH genügt hier nicht die bloße Erbringung derartiger Dienstleistungen. Vielmehr bedarf es zusätzlich der Betrauung mit ihnen. Sie kann durch Gesetz erfolgen, doch ist die Betrauung durch eine Rechtsvorschrift nach jüngerer Praxis nicht zwingend erforderlich.[265] Entscheidend ist somit, dass das Unternehmen nicht aus eigener Initiative und zur Gewinnerzielungsabsicht handelt, sondern zur Erbringung einer Leistung (zB staatlicher Versorgungsauftrag) herangezogen wird.[266]

Es kann daher mE davon ausgegangen werden, dass der Begriff der Unternehmen, die mit Dienstleistungen von allgemeinem wirtschaftlichem Interesse betraut sind, jedenfalls enger auszulegen sein wird als jener der Betreiber wesentlicher Dienste. Wo im Sektor der Energieversorgung von einer staatlichen Betrauung auszugehen sein wird[267], ist dies in den

---

von Diensten als wirtschaftliche bzw. marktbezogene Tätigkeiten von allgemeinem Interesse, siehe Mitteilung "Leistungen der Daseinsvorsorge" vom 20.09.2000, COM (2000) 580, ABl. EG C 17/4

[262] Art. 1 und 2 des „Protokolls (Nr. 26) über Dienste von allgemeinem Interesse“, ABl. EU 2012 C 326/308.

[263] *Müller-Graff*, Artikel 14 AEUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (2012), Rz 6.

[264] Siehe dazu *Linder*, Daseinsvorsorge in der Verfassungsordnung der Europäischen Union, S. 196.

[265] EuGH, Rs C-159/94, Kommission/Frankreich, Slg. 1997, I-5815.

[266] *Linder*, Daseinsvorsorge in der Verfassungsordnung der Europäischen Union, S. 94.

[267] Siehe dazu Kapitel 7.1.1.1, insbesondere bspw. die Regelungen des Elektrizitätswirtschafts- und –organisationsgesetzes 2010 – ElWOG 2010).

Bereichen des Bankwesens[268], der Finanzmarktinfrastrukturen[269] oder Digitalen Infrastrukturen[270] nicht der Fall.

Diese Regelung des Art. 106 AEUV bestätigt, dass auch Unternehmen der Daseinsvorsorge[271] an unionsrechtliche Bestimmungen gebunden sind[272], wobei sie mit entsprechender Begründung von einzelnen unionsrechtlichen Verpflichtungen entlastet werden können.[273] Beispiele für Regelungen in diesen Bereichen finden sich im Telekommunikationssektor und in der Stromversorgung.[274]

Im Hinblick auf die Zuständigkeit der Union zur Regelung der NIS-RL ergibt sich - unabhängig von der Frage der staatlichen Betrauung - aus Art. 106 AEUV kein Grund, der ein bestimmtes Unternehmen oder Unternehmen eines konkreten Sektors von diesen unionsrechtlichen Vorgaben ausnehmen sollte. Die Verpflichtung zur Umsetzung von Sicherheitsstandards verbessert vielmehr die Erfüllung dieser Aufgaben für die Allgemeinheit, als sie zu verhindern, wie in Art. 106 vorgesehen.

[268] Siehe dazu Kapitel 7.1.1.3, insbesondere die fehlende Betrauung zur Einrichtung privater Kreditinstitute (anders ist dies für die Oesterreichische Nationalbank zu sehen (siehe Nationalbankgesetz 1984 – NBG), die jedoch keinen Betreiber wesentlicher Dienste im Sinne des NISG darstellt.

[269] Siehe dazu Kapitel 7.1.1.4, worunter bspw. die Wiener Börse zu sehen sein wird.

[270] Siehe dazu Kapitel 7.1.1.7, worunter bspw. private Internetanbieter zu subsumieren sind.

[271] Zum Umstand, dass das Konzept der gemeinwohlorientierten Daseinsvorsorge nicht mehr allein als rechtfertigungsbedürftiger Ausnahmefall zu interpretieren sei, siehe *Schwarze*, Daseinsvorsorge im Lichte des europäischen Wettbewerbsrechts, Europäische Zeitschrift für Wirtschaftsrecht, 11/2001, S. 337.

[272] Die EU-Kommission betont die Geltung insbesondere der wettbewerbs- und binnenmarktrechtlichen Bestimmungen ungeachtet des öffentlich- oder privatrechtlichen Status eines Unternehmens, siehe Mitteilung vom 30. September 2000, Nr. 21.

[273] *Müller-Graff* in Vedder /Heintschel von Heinegg, Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar, Rz 13.

[274]Zu den unterschiedlichen Ausprägungen wettbewerblicher Elemente in den regulatorischen Regimen einzelner Bereiche der Daseinsvorsorge, wie beispielsweise dem Telekommunikationssektor und der Stromversorgung, siehe *Müller* in Bos /Dieringer, Die Genese einer Union der 27, Die Europäische Union nach der Osterweiterung. Mehr zu diesen Rechtsakten der Union siehe Kapitel 4.2.4.

6.3. Entwicklung

Grundsätzlich stehen hinter der Netz- und Informationssystemsicherheit auf Europäischer Ebene zwei Themen, die im vergangenen Jahrzehnt schrittweise vorangetrieben wurden. Dabei handelt es sich einerseits um einen wirtschaftlichen Ansatz zur Gewährleistung der Weiterentwicklung der IT-Industrie in Europa. Darüber hinaus sollte auch der Schutz kritischer Infrastruktur, eng verknüpft mit der Terrorismusbekämpfung, gestärkt werden.[275]

Im September 2017 aktualisierte die EU die ursprünglich aus dem Jahr 2013 stammende Cybersicherheitsstrategie[276] mit dem Ziel, die europäische kritische Infrastruktur besser zu schützen und digital selbstbestimmter gegenüber anderen Regionen der Welt zu werden. Die NIS-RL als erste horizontale Rechtsvorschrift zur Bewältigung der Herausforderungen der Cybersicherheit[277] ist ein wesentlicher Teil dieses neuen vorgelegten Sicherheitspakets.
Die Entwicklungen europäischer Maßnahmen in Bezug auf Digitalisierung und die diesbezügliche Sicherheit begannen jedoch schon sehr viel früher. 2001 verabschiedete die Kommission eine Mitteilung „Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz“[278], im Jahr 2005 wurde der Rahmenbeschluss des Rates über Angriffe auf Informationssysteme[279] veröffentlicht, der 2013 durch die Richtlinie über Angriffe auf Informationssysteme[280] ersetzt wurde, und 2006 wurde eine Strategie für eine sichere Informationsgesellschaft[281] veröffentlicht.

Im Jahr 2007 veröffentlichte die Europäische Kommission die Mitteilung „Eine allgemeine Politik zur Bekämpfung der Internetkriminalität“[282], deren Ziel eine bessere Koordinierung der

[275] Europäisches Parlament, Cybersecurity and Cyberpower: concepts, conditions and capabilities for cooperation for action within the EU, http://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf, S. 32.
[276] Join(2013) 1 final .
[277] Mitteilung der Kommission an das Europäische Parlament und den Rat - Bestmögliche Netz- und Informationssicherheit - hin zu einer wirksamen Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, COM(2017) 476 final, 2.
[278] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz, COM(2001)298 final.
[279] Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl 2005, L 69/67.
[280] RL (EU) 2013/40; Richtlinie über Angriffe auf Informationssysteme.
[281] Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine Strategie für eine sichere Informationsgesellschaft - "Dialog, Partnerschaft und Delegation der Verantwortung", COM(2006) 251 final.
[282] Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen, Eine allgemeine Politik zur Bekämpfung der Internetkriminalität, COM(2007) 267 final.

Bekämpfung der Internetkriminalität war und die beispielsweise einen verstärkten Dialog zwischen dem öffentlichen und dem privaten Sektor zur Schaffung gegenseitigen Vertrauens und Meldung sachdienlicher Informationen als eine von vielen Maßnahmen institutionalisieren wollte. Daneben entstand 2008 die EU-Richtlinie zum Schutz kritischer Infrastruktur[283] zur Identifizierung europäischer kritischer Infrastruktur und zur Implementierung eines gemeinsamen Ansatz um deren Schutz zu verbessern. Der Fokus der Richtlinie lag in einem ersten Schritt auf den Sektoren Energie und Transport und sollte später weitere Sektoren, wie die Informations- und Kommunikationstechnologien, miteinbinden, was jedoch bis zum heutigen Tag nicht geschehen ist.

Im Dezember 2009 wurde vom Rat der Europäischen Union „Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger“[284] angenommen, das einen signifikanten Schritt in der Agenda der Inneren Sicherheit der Europäischen Union darstellte. In diesem Programm wurden unter anderem EU-Regularien zur Gewährleistung eines hohen Levels der Netzwerksicherheit und zur Reaktion in Folge von Cyberangegriffen angekündigt.[285]

Die ebenso im Jahr 2009 veröffentlichte Mitteilung der Kommission über den Schutz kritischer Informationsinfrastrukturen[286] legte Maßnahmen zur Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität mit dem Ziel des Schutzes Europas vor Cyber-Angriffen und Störungen großen Ausmaßes vor. Zu diesen zählten Public-Private-Partnership-Plattformen, das Aufsetzen eines europäischen Systems für Warnungen und Informationsaustausch, länderübergreifende Cyber-Übungen sowie der Aufruf an alle Mitgliedstaaten, eigene Computer-Notfallteams einzurichten.

2010 wurde in der Mitteilung der EU-Kommission über die EU-Strategie der Inneren Sicherheit[287] die Cyberkriminalität als einer von fünf Schwerpunkten festgelegt und die Verbesserung des Reaktionsvermögens gegenüber Cyberangriffen durch den Aufbau von Computer-Notfallteams als eine der wesentlichen Eckpunkte der Strategie dargestellt. In diesem Jahr wurde auch Digitale

[283] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl 2008 L 345/75.
[284] Informationen der Organe, Einrichtungen und sonstigen Stellen der Europäischen Union, Europäischer Rat, Das Stockholmer Programm - Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl C 115/1.
[285] ABl C 115/1 S. 39.
[286] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen, "Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität", COM(2009) 149 final.
[287] Mitteilung der Kommission an das Europäische Parlament und den Rat, EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa, COM(2010) 673 final.

Agenda für Europa[288] als Teil der vom Europäischen Rat verabschiedeten Strategie Europa 2020 veröffentlicht, die als einen Schwerpunkt die Nutzung der Wirtschaftspotenziale der EU-Mitgliedstaaten für die Schaffung eines gemeinsamen digitalen Marktes und gemeinsamer Infrastruktur setzte.

In der ersten EU-Cybersicherheitsstrategie[289] vom 7. Februar 2013 wird als eine der Maßnahmen der Aufbau von Kapazitäten bei Behörden und im Privatsektor und die Zusammenarbeit dieser zur Stärkung der Widerstandsfähigkeit gegenüber Cyberangriffen festgelegt, um dadurch das reibungslose Funktionieren des Binnenmarktes zu stärken. In der Strategie ersucht die Kommission das Europäische Parlament und den Rat, den Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union zügig zu verabschieden.

Wesentlich war auch die Weiterentwicklung[290] der Rolle der Europäischen Agentur für Netz- und Informationssystemsicherheit (ENISA), die 2004 als beratendes Organ für Mitgliedstaaten und EU-Organisationen in Bezug auf die Netz- und Informationssystemsicherheit eingerichtet wurde.[291] Mit dem Vorschlag für eine Verordnung über die EU-Cybersicherheitsagentur (ENISA) über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik[292] aus Februar 2018 soll die Europäische Agentur ein ständiges Mandat und einen klaren Zuständigkeitsbereich bekommen, insbesondere in Bezug auf die NIS-RL. Künftig ist auch angedacht, einen EU-Rahmen für die Zertifizierung der Cybersicherheit mit dem Ziel zu schaffen, IKT-Produkte und -Dienstleistungen formell anhand festgelegter Cybersicherheitsstandards bewerten zu können.[293] Insbesondere bei kritischen und hochsensiblen Anwendungen, auf deren Funktionieren wir im

[288] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine Digitale Agenda für Europa, COM(2010) 245 final.
[289] Join(2013) 1 final .
[290] Die bisherigen Aufgaben der ENISA sind in der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Euopäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004, ABl L 165/41 festgelegt.
[291] Die ENISA sollte die Mitgliedstaaten und die Kommission mit Fachkompetenz, als Berater und als Mittler für den Austausch bewährter Verfahren unterstützen. Insbesondere sollte die Kommission die ENISA bei der Anwendung der NIS-RL zurate ziehen und die Mitgliedstaaten sollten berechtigt sein, die ENISA zurate zu ziehen – siehe ErwGr 36 NIS-RL.
[292] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit"), COM(2017) 477 final/3, S. 6.
[293] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit"), COM(2017) 477 final/3,

täglichen Leben angewiesen sind und die in zunehmendem Maße digital und miteinander verbunden sind, sollen die entscheidenden IKT-Komponenten in diesen Produkten und Systemen strengen Sicherheitsüberprüfungen unterzogen werden.[294]

7. Schwierigkeiten und rechtliche Fragestellungen in der nationalen Umsetzung

Das nun folgende Kapitel wird sich mit der Umsetzung der NIS-RL durch das nationale Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz), im Folgenden NIS-Gesetz, auseinandersetzen. Dabei sollen aufgrund des bestehenden nationalen verfassungsrechtlichen und einfachgesetzlichen Rahmens sowie aufgrund existierender Strategien und eingerichteter Strukturen die Herausforderungen und Möglichkeiten der Umsetzung der NIS-RL in Österreich beleuchtet und diskutiert werden. Die Frist zur Umsetzung der Richtlinie durch die Mitgliedstaaten mit 9. Mai 2018[295] wurde von Österreich überschritten; das nationale NIS-Gesetz trat mit 29. Dezember 2018 in Kraft.

Wird eine Richtlinie nicht fristgerecht oder falsch umgesetzt, kann dies nach der kasuistischen Judikatur des EuGH unter bestimmten Voraussetzungen zur unmittelbaren Anwendung der Richtlinie führen; dies grundsätzlich dann, wenn die Richtlinie inhaltlich unbedingt und hinreichend genau bestimmt ist und den Einzelnen begünstigt.[296] Dabei wird zwischen der vertikalen Drittwirkung (Richtlinien begründen subjektive Rechte der Bürger gegenüber den Mitgliedstaaten) und der horizontalen Drittwirkung (Rechte zwischen den Bürgern) unterschieden, wobei letztere grundsätzlich verneint wird.[297] [298] Die geforderte hinreichend genaue Bestimmtheit ist im gegenständlichen Fall zu verneinen, da aus dem Richtlinientext keine Begünstigungen Einzelner zu entnehmen ist.

---

[294] Siehe auch ErwGr 50 der RL.

[295] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl L 194/1.

[296] *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11], Rz 246/8. Siehe auch EuGH, Rs C-226/07 (Rz 23) – Flughafen Köln/Bonn; Rs C-397-403/01, Slg. 2004, I-8835 (8915, Rz 103) – DRK; Rs C-62/00, Slg. 2002, I-6325 (6358, Rz 25) – Marks & Spencer; ua.

[297] *Hummer*, Neueste Entwicklungen im Zusammenspiel von Europarecht und nationalem Recht der Mitgliedstaaten (2010), S. 163ff.

[298] Auch wenn die Richtlinie nur die Ziele klar und eindeutig definiert und den Mitgliedstaaten einen Ausgestaltungsspielraum überlässt (und somit nicht hinreichend bedingt zu sein scheint), hat der EuGH bereits eine unmittelbare Anwendbarkeit bejaht - betraf die unmittelbare Anwendbarkeit von Art. 2, 3 UVP-RL, die wegen der Umsetzungsoffenheit in vielen Details vielfach verneint wurde, siehe EuGH, Rs. C-431/92, Slg. 1995, I-2189 (2224, Rz 37ff) – Großkrotzenburg.

Das NIS-Gesetz selbst enthält neben einfachgesetzlichen Bestimmungen aufgrund der kompetenzrechtlichen Notwendigkeit auch eine Regelung in Verfassungsrang sowie eine Reihe von Verordnungsermächtigungen. Die Inhalte der Verordnungen selbst werden in dieser Arbeit nur allgemein und im Rahmen des Erfordernisses zum besseren Verständnis des Bundesgesetzes erläutert.

7.1. Abschnitt 1 - Allgemeine Bestimmungen

7.1.1. Kompetenzdeckungsklausel (Verfassungsbestimmung)

„Das Prinzip der doppelten Bindung besagt, dass der nationale Gesetzgeber im Rahmen der Umsetzung von Unionsrecht zugleich die Vorgaben des nationalen (Verfassungs-)Rechts beachten muss“.[299] Die Frage der nationalen Gesetzgebungs- und Vollziehungskompetenz in Umsetzung der Richtlinie richtet sich gemäß Art. 23d Abs. 5 B-VG nach der allgemeinen bundesstaatlichen Kompetenzverteilung (Art. 10-15 B-VG). Aus diesem Grund ist der Bund nur insoweit zur Gesetzgebung zuständig, als es sich dabei um eine ihm verfassungsrechtlich übertragene Kompetenz handelt.[300] Festzuhalten ist jedenfalls, dass die Zuständigkeit zur Erlassung einer Durchführungsregelung nicht automatisch deshalb auf den Bund übergeht, weil ein Land seiner sich aus der bundesstaatlichen Kompetenzverteilung ergebenden Verpflichtung nicht fristgerecht nachkommt (was in Bezug auf die NIS-RL der Fall war) – dies wäre gegebenenfalls erst nach Feststellung einer Vertragsverletzung durch ein Urteil des EuGH der Fall.[301]

§ 1 NIS-Gesetz als Verfassungsbestimmung sieht eine so genannte Kompetenzdeckungsklausel[302] vor. Demnach sind die Erlassung, Aufhebung sowie Vollziehung von Vorschriften, wie sie in diesem Bundesgesetz enthalten sind, auch in den Belangen Bundessache, hinsichtlich derer das Bundes-Verfassungsgesetz (B-VG), BGBl. Nr. 1/1930, etwas anderes bestimmt. Dies soll jedoch nicht im Bereich der Hoheitsverwaltung von Ländern und Gemeinden gelten, die auf freiwilliger Basis gemäß § 22 Abs. 5 die Verpflichtungen nach dem NIS-Gesetz auch in Hinblick auf ihre wichtigen Dienste für anwendbar erklären können. Die in diesen Vorschriften geregelten Angelegenheiten können in unmittelbarer Bundesverwaltung besorgt werden.

[299] *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11], Rz 246/8.
[300] Zur Feststellung, dass es sich bei klaren Zuständigkeiten letzten Endes um ein wichtiges Postulat des Rechtsstaats handelt siehe *Barfuß*, Ressortzuständigkeit und Vollzugsklausel, Eine verfassungs- und verwaltungsrechtliche Untersuchung zur Zuständigkeit der Bundesminister (1968), S. 3.
[301] *Öhlinger/Potacs*, EU-Recht und staatliches Recht[6] (2017), S. 119.
[302] *Perthold-Stoitzner*, Verfassungsrecht (2015), S. 6., *Berka*, Verfassungsrecht, Rz 400.

Im Folgenden soll näher untersucht werden, warum und insbesondere in welchen Bereichen eine verfassungsrechtliche Zuständigkeit der Länder in der Vollziehung vorhanden bzw. warum eine solche Kompetenzdeckungsklausel erforderlich ist.

Art. 10-15 B-VG regelt die Aufteilung der staatlichen Aufgaben – konkret der Gesetzgebung und der Vollziehung[303] – zwischen dem Bund und den Ländern. Zur Einordnung des Schutzes kritischer Infrastruktur bzw. der Netz- und Informationssystemsicherheit in die Kompetenztatbestände bzw. dem Vorliegen einer so genannten Querschnittsmaterie[304] siehe Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**. Zur genaueren Untersuchung des Vorliegens einer Bundes- und/oder Landeszuständigkeit in gegenständlicher Vollziehung sind im Folgenden die einzelnen, durch das NIS-Gesetz zu regelnden Sektoren sowie sonstige relevante Bestimmungen des Gesetzes zu untersuchen.

7.1.1.1. Sektor Energie

Da das B-VG keinen allgemeinen Kompetenztatbestand der Energieversorgung kennt, erfolgt die kompetenzrechtliche Analyse aufgrund der in der NIS-RL genannten Teilsektoren „Elektrizität", „Erdöl" und „Erdgas".

Insbesondere im Bereich der Energieversorgung existieren bereits zahlreiche Bestimmungen in Verfassungsrang bzw. zur geänderten Kompetenzregelung. In § 1 ElWOG 2010[305] findet sich gleichsam eine Kompetenzgrundlage in Verfassungsrang wie in § 1 E-ControlG[306], § 1 Ökostromgesetz 2012[307], § 1 Energielenkungsgesetz 2012[308], § 1 Bundes-Energieeffizienzgesetz 2014[309], § 1 Erdölbevorratungsgesetz 2012[310], und § 1 KWK-Gesetz[311]. Diese bestehenden

[303] Gegenstand der bundesstaatlichen Kompetenzverteilung sind in Wirklichkeit die Zuständigkeiten zur Gesetzgebung und Verwaltung (Begriff der Vollziehung in gewisser Weise irreführend), siehe dazu *Berka*, Verfassungsrecht, Rz 395.
[304] *Berka*, Verfassungsrecht, Rz 423.
[305] Bundesgesetz, mit dem die Organisation auf dem Gebiet der Elektrizitätswirtschaft neu geregelt wird (Elektrizitätswirtschafts- und –organisationsgesetz 2010 – ElWOG 2010), BGBl. I Nr. 110/2010 idF BGBl. I Nr. 108/2017.
[306] Bundesgesetz über die Regulierungsbehörde in der Elektrizitäts- und Erdgaswirtschaft (Energie-Control-Gesetz – E-ControlG), BGBl. I Nr. 110/2010 idF BGBl. I Nr. 108/2017.
[307] Bundesgesetz über die Förderung der Elektrizitätserzeugung aus erneuerbaren Energieträgern (Ökostromgesetz 2012 – ÖSG 2012), BGBl. I Nr. 75/2011 idF BGBl. I Nr. 108/2017.
[308] Bundesgesetz über Lenkungsmaßnahmen zur Sicherung der Energieversorgung (Energielenkungsgesetz 2012 – EnLG 2012), BGBl. I Nr. 41/2013.
[309] Bundesgesetz über die Steigerung der Energieeffizienz bei Unternehmen und dem Bund (Bundes-Energieeffizienzgesetz – EEffG) BGBl. I Nr. 72/2014.
[310] Bundesgesetz über die Haltung von Mindestvorräten an Erdöl und Erdölprodukten (Erdölbevorratungsgesetz 2012 – EBG 2012), BGBl. I Nr. 78/2012 idF BGBl. I Nr. 163/2015.
[311] Bundesgesetz, mit dem Bestimmungen auf dem Gebiet der Kraft-Wärme-Kopplung neu erlassen werden (KWK-Gesetz), BGBl. I Nr. 111/2008 idF BGBl. I Nr. 27/2015.

Kompetenzdeckungsklauseln können nicht zur Erlassung bundesgesetzlicher Regelungen im Anwendungsbereich der NIS-RL angewandt werden.

Elektrizität (Art. 12 Abs. 1 Z 5)

Das Elektrizitätsrecht und seine Struktur unterliegt im österreichischen Verfassungsrecht einer stark bundesstaatlichen Kompetenzverteilung.[312]

Die NIS-RL definiert in Anhang II Z. 1 lit. a Betreiber wesentlicher Dienste im Teilsektor Elektrizität als Elektrizitätsunternehmen mit Versorgungsfunktion[313], Verteilernetzbetreiber und Übertragungsnetzbetreiber. In den Kompetenztatbeständen des B-VG finden sich zum Elektrizitätswesen einerseits die „Normalisierung und Typisierung elektrischer Anlagen und Einrichtungen, Sicherheitsmaßnahmen auf diesem Gebiet“ (Art. 10 Abs. 1 Z 10 B-VG), das Starkstromwegerecht, soweit sich die Leitungsanlage auf zwei oder mehrere Länder erstreckt (Art. 10 Abs. 1 Z 10 B-VG) sowie das „Elektrizitätswesen, soweit es nicht unter Art. 10 fällt“ (Art. 12 Abs. 1 Z 5 B-VG).
„Unter Normalisierung und Typisierung wurde die technische Einheitlichkeit der elektrischen Einrichtungen innerhalb des Bundesgebietes, namentlich hinsichtlich Stromart, Periodenzahl (Frequenz) und Stromspannung verstanden, unter Sicherheit die Hintanhaltung von Gefahren für Menschen und von Beeinträchtigungen anderer Anlagen.“[314] Es ist daher davon auszugehen, dass damit die gegenseitige Beeinträchtigung bzw. das funktionierende Zusammenwirken verschiedener Stromanlagen geregelt werden soll und nicht die Sicherheit der Anlagen selbst. Auch die Auswirkungen hinsichtlich der Beeinträchtigung und des Ausfalls dieser Anlagen fällt nicht unter diese Bestimmung, sondern lediglich gesundheitliche Auswirkungen durch die Gefahr der Schädigung durch elektrischen Strom selbst („Insbesondere Maßnahmen zur Bekämpfung der Gefahr von Schädigungen der Gesundheit und des Lebens von Menschen durch elektrischen Strom sind für den Kompetenztatbestand Sicherheitsmaßnahmen auf dem Gebiet elektrischer Anlagen und Einrichtungen typisch.“[315]). Der gegenständliche Kompetenztatbestand gem. Art. 10 Abs. 1 Z 10 B-VG kommt somit nicht zur Anwendung.

---

[312] *Mayerhofer*, Artikel 12 Abs 1 Z 5 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (2015), Rz 1.zitiert nach Hauer, Energierecht (Elektrizitätsrecht) in Hauer (Hrsg), Wirtschaftsverwaltungsrecht (2013) 135 (139).
[313] Art. 2 Nummer 35 iVm Nummer 19 RL 2009/72/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG, ABl. 2009, L 211/55.
[314] *Raschauer*, Artikel 10 Abs 1 Z 10 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (2011), Rz 129.
[315] *Raschauer* in Kneihs /Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, Rz 134.

Anders verhält sich dies mit dem Starkstromwegerecht, soweit sich die Leitungsanlage auf zwei oder mehrere Länder erstreckt (Art. 10 Abs. 1 Z 10 B-VG). „Der Bund ist demnach zuständig, den Betreibern solcher Leitungen im öffentlichen Interesse besondere Pflichten aufzuerlegen. Er ist außerdem befugt, Starkstromleitungen einem verwaltungspolizeilichen Regime zu unterwerfen (Genehmigungspflicht, behördliche Aufsicht, Aufträge).[316] Da sich Übertragungsnetze typischerweise über mehrere Bundesländer erstrecken und Starkstrom übertragen, und mit dem NIS-Gesetz bestimmte Pflichten geregelt werden, kann in Bezug auf diese Anlagen von einer Anwendung des Art. 10 Abs. 1 Z 10 ausgegangen werden.

Die dritte in Frage kommende Kompetenz findet sich in Art. 12 Abs. 1 Z 5 B-VG (Elektrizitätswesen, soweit es nicht unter Art. 10 fällt), der im Vergleich zu den vorher genannten Tatbeständen die allgemeinere Regelung darstellt. „Im Lichte des Versteinerungsmaterials erscheint Art. 12 Abs. 1 Z 5 daher als spezifischer Gewerberechtstatbestand mit wirtschaftslenkenden Elementen.“[317] Wesentlich wird in diesem Zusammenhang wohl die Zuordnung des Elektrizitätsbetreibers im Rahmen der Daseinsvorsorge bzw. als Betreiber eines für die Bevölkerung wesentlichen Dienstes sein. Nach *Potacs/Rogatsch* fällt der Betrieb von Elektrizitätsunternehmen unter einem versorgungspolitischen Gesichtspunkt unter Art. 12 Abs. 1 Z 5 B-VG.[318]

Als Ergebnis darf daher festgestellt werden, dass die Regelungen zur Netz- und Informationssicherheit bei Übertragungsnetzbetreibern in die Kompetenz des Art. 10 Abs. 1 Z 10 B-VG (Zuständigkeit des Bundes in Gesetzgebung und Vollziehung) und aller sonstigen Verteilernetzbetreiber in die Auffangkompetenz des Art. 12 Abs. 1 Z 5 B-VG zu subsumieren sind. Demnach kommt dem Bund diesbezüglich die Grundsatzgesetzgebung, dem Land die Ausführungsgesetzgebung und Vollziehung zu.

Erdöl (Art. 10 Abs. 1 Z 8 B-VG)

Die NIS-RL definiert in ihrem Anhang II Z 1 lit. b Betreiber wesentlicher Dienste im Teilsektor Erdöl als Betreiber von Erdöl-Fernleitungen, Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern. Regelungen zu diesen Tatbeständen könnten sich in Art. 10 Abs. 1 Z 10 B-VG („Bergwesen“) sowie Art. 10 Abs. 1 Z 8 B-VG („Gewerberecht“) finden.

[316] *Raschauer* in Kneihs /Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, Rz 143, 45.
[317] *Mayerhofer* in Kneihs /Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, Rz 7. Zur Interpretation der Kompetenzbestimmungen siehe auch *Berka*, Verfassungsrecht, Rz 427.
[318] *Potacs/Rogatsch*, in Holoubek /Potacs (Hrsg), Öffentliches Wirtschaftsrecht I (2013), Rz 853.

„Unter den typisch gewerberechtlichen Zwecken sind unter anderem solche zu verstehen, die dem Schutz des Gewerbes dienen."[319] „Unter den Kompetenztatbestand „Bergwesen" fällt im Kern gekürzt formuliert die Regelung des Gewinnens von mineralischen Rohstoffen mit typisch bergbautechnischen Mitteln und Methoden."[320] Demnach können mE Regelungen zu Betreibern von Anlagen zur Produktion von Erdöl unter den Tatbestand des Bergwesens subsumiert werden, wohingegen die Raffination und Aufbereitung von Erdöl sowie der Transport[321] (sofern nicht in unmittelbarem Zusammenhang mit der Gewinnung) unter den Tatbestand der „Angelegenheiten des Gewerbes und der Industrie (Art. 10 Abs. 1 Z 8 B-VG) fallen. Nach höchstgerichtlicher Rechtsprechung[322] wurde in Bezug auf den Transport von Erdgas in Rohrleitungen außerhalb von Bergwerksanlagen festgehalten, dass die Stoffveredelung, dh die weitere Bearbeitung bzw. Umwandlung des bergmännisch gewonnen Rohstoffes, seit jeher eine gewerbliche Tätigkeit bildete.

Die Erdöllagerung fällt ebenso in die Kompetenz des Gewerberechtes (Art. 10 Abs. 1 Z 8 B-VG), sofern sie nicht in unmittelbarem Zusammenhang mit dem Bergbaubetrieb selbst erfolgt.[323]

Erdgas (Art. 10 Abs. 1 Z 8 B-VG)

Die NIS-RL definiert in Anhang II Z 1 lit c. Versorgungsunternehmen, Verteilernetzbetreiber, Fernleitungsnetzbetreiber, Betreiber einer Speicheranlage, Betreiber einer LNG-Anlage[324] sowie Erdgasunternehmen, die Funktionen der Gewinnung, Fernleitung, Verteilung, Lieferung, Kauf oder Speicherung von Erdgas wahrnehmen und die kommerzielle, technische und/oder wartungsbezogene Aufgaben im Zusammenhang mit diesen Funktionen erfüllen.

Dabei kann auf die Ausführungen im Teilsektor Erdöl verwiesen werden. [325]

[319] *Müller*, Artikel 10 Abs 1 Z 8 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (2015), Rz 16.
[320] VfSlg 13.299/1992.
[321] Siehe auch § 1 Rohrleitungsgesetz (Bundesgesetz über die gewerbsmäßige Beförderung von Gütern in Rohrleitungen, BGBl. Nr. 411/1975 idF BGBl. I Nr. 40/2017), wonach das Bundesgesetz für die gewerbsmäßige Beförderung von Gütern in Rohrleitungen gilt; nicht jedoch für Rohrleitungsanlagen, die bergrechtlichen Vorschriften unterliegen oder die sich innerhalb der gewerblichen Betriebsstätte von Unternehmen befinden, die der Gewerbeordnung unterliegen;
[322] VfSlg 14.972/1997. So auch *Raschauer* in Kneihs /Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, Rz 28.
[323] *Raschauer* in Kneihs /Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, Rz 26.
[324] Liquefied Natural Gas (LNG) steht für Flüßiggas.
[325] *Müller* in Kneihs /Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, Rz 44.

7.1.1.2. Sektor Verkehr

Die NIS-RL unterteilt den Sektor Verkehr in ihrem Anhang II Z 2 in den Luftverkehr, Schienenverkehr, die Schifffahrt und den Straßenverkehr, wobei das österreichische Verfassungsrecht in Bezug auf diese Teilsektoren unterschiedliche Zuständigkeiten vorsieht.

Teilsektor Luftverkehr (Art. 10 Abs. 1 Z 9 B-VG)

Gem. Anhang II Z 2 lit. a NIS-RL gelten Luftfahrtunternehmen, Flughafenleitungsorgane sowie Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste bereitstellen, als Betreiber wesentlicher Dienste im Luftverkehr.

Der Kompetenztatbestand des „Verkehrswesens bezüglich Luftfahrt" des Art. 10 Abs. 1 Z 9 B-VG wird umfassend verstanden und kann hier angewendet werden. „Diesem unterliegen bezüglich der Luftfahrt alle Regelungen betreffend die notwendigen bodengebundenen Anlagen, die Zulassung von Flugzeugen, Piloten und Luftfahrtunternehmen sowie die Regelungen des Luftverkehrs im engeren Sinne (insbesondere die Flugsicherung)."[326]

Teilsektor Schienenverkehr (Art. 10 Abs. 1 Z 9 B-VG)

Anhang II Z 2 lit. b des Anhanges II nennt Infrastrukturbetreiber als auch Eisenbahnunternehmen als Betreiber wesentlicher Dienste im Teilsektor Schienenverkehr.

Zum Kompetenztatbestand des „Verkehrswesens bezüglich der Eisenbahn" des Art. 10 Abs. 1 Z 9 B-VG hat der Verfassungsgerichtshof in seiner Rechtsprechung mehrfach ausgeführt, dass darunter das Eisenbahnwesen überhaupt zu verstehen sei (umfassendes Begriffsverständnis).[327] „Dies umfasst neben der Planung, Errichtung und Instandhaltung alle für den Betrieb der Eisenbahn wesentlichen Angelegenheiten."[328]

Schifffahrt (Art. 10 Abs. 1 Z 9 B-VG bzw. Art. 11 Abs. 1 Z 6)

Anhang II Z 2 lit. b NIS-RL nennt Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt sowie Leitungsorgane von Häfen als Betreiber wesentlicher Dienste im Teilsektor der Schifffahrt.

Die Kompetenztatbestände des „Verkehrswesens bezüglich Schifffahrt" sowie die „Strom- und Schifffahrtspolizei" gem. Art. 10 Abs. 1 Z 9 B-VG sind insoweit eingeschränkt, als diese Angelegenheiten nicht unter Art. 11 B-VG fallen. Art. 11 Abs. 1 Z 6 B-VG regelt demnach die

[326] *Wallnöfer*, Artikel 10 Abs 1 Z 9 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (2015), Rz 24.
[327] VfSlg 15.552/1999.
[328] VfSlg 17.424/2004.

Binnenschifffahrt hinsichtlich der Schifffahrtskonzessionen, Schifffahrtsanlagen und Zwangsrechten an solchen Anlagen, soweit sie sich nicht auf die Donau, den Bodensee, den Neusiedlersee und auf Grenzstrecken sonstiger Grenzgewässer bezieht; darüber hinaus Strom- und Schifffahrtspolizei auf Binnengewässern mit Ausnahme der Donau, des Bodensees, des Neusiedlersees und der Grenzstrecken sonstiger Grenzgewässer. Art. 11 Abs. 1 Z 6 B-VG differenziert hinsichtlich der Zuständigkeit somit nach Gewässern, wobei internationale Gewässer in den Anwendungsbereich des Art. 10 Abs. 1 Z 9 B-VG fallen. „Unter dem Begriff der Schifffahrtspolizei werden unter anderem Bestimmungen über Sicherheitsvorkehrungen zur Verhütung von Unfällen verstanden."[329] Da es sich auch bei Maßnahmen zur Sicherheit von Netz- und Informationssystemen um Sicherheitsvorkehrungen handelt, ist der Tatbestand der Schifffahrtspolizei betroffen. Demnach fällt die Kompetenz für Regelungen, soweit nicht Binnenschifffahrt auf den genannten internationalen Gewässern betroffen ist, in den Bereich des Art. 11 Abs. 1 Z 6 B-VG, in allen anderen Fällen unter Art. 10 Abs. 1 Z 9 B-VG. Selbiges gilt für den Betrieb von Häfen („Schifffahrtsanlagen").

Straßenverkehr (Art. 11 Abs. 1 Z 4 B-VG)

Im Teilsektor Straßenverkehrs werden gem. Anhang II Z 2 lit. d NIS-RL Straßenverkehrsbehörden sowie Betreiber intelligenter Verkehrssysteme als Betreiber wesentlicher Dienste definiert. In Betracht kommen die Kompetenztatbestände des Art. 10 Abs. 1 Z 9 B-VG („Kraftfahrwesen") sowie Art. 11 Abs. 1 Z 4 B-VG („Straßenpolizei").

Der Verfassungsgerichtshof stellte bereits mehrmals fest, dass der Kompetenztatbestand des Kraftfahrwesens „alle Angelegenheiten des Kraftfahrzeuges und seines Lenkers" umfasst und davon „nur die nach der Eigenart der Kraftfahrzeuge notwendigen verkehrspolizeilichen Bestimmungen, ferner die Bestimmungen über die Beschaffenheit der Fahrzeuge und ihren Betrieb betroffen sein" können.[330] Demnach fallen Regelungen der Netz- und Informationssicherheit für Straßenverkehrsbehörden sowie intelligente Verkehrswege nicht unter gegenständlichen Kompetenztatbestand.

In den Kompetenzbereich des Art. 11 Abs. 1 Z 4 B-VG („Straßenpolizei") fallen „Regelungen, die der Sicherheit, Leichtigkeit und Flüssigkeit des Verkehrs dienen."[331] Die Aufgabe sowohl von Straßenverkehrsbehörden als auch von Betreibern intelligenter Verkehrssysteme ist es ganz

[329] *Muzak*, Artikel 11 Abs 1 Z 6 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (2012), Rz 16.
[330] Ständige Judikatur seit VfSlg 2977/1956; vgl bspw. VfSlg 4180/1962, 4243/1962, 4381/1963, 6937/1972, 8035/1977, 11.493/1987, 15.885/2000.
[331] *Resch*, Artikel 11 Abs 1 Z 4 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (2012), Rz 7.

grundsätzlich, einerseits für die Sicherheit des Straßenverkehrs zu sorgen, als auch für die Leichtigkeit und Flüssigkeit des Verkehrs Maßnahmen zu treffen. Dies Gewährleistung der Flüssigkeit des Verkehrs gilt insbesondere für Betreiber intelligenter Verkehrssysteme, deren eigentliches Ziel dies darstellt.

Der Straßenverkehr fällt mE somit zur Gänze in den Kompetenztatbestand des Art. 11 Abs. 1 Z 4 B-VG.

7.1.1.3. Sektor Bankwesen

Unter dem Begriff des Bankwesens werden gemäß Anhang II Z 3 NIS-RL Kreditinstitute[332] verstanden. Diese Kompetenz fällt zur Gänze unter das Bankwesen gemäß Art. 10 Abs. 1 Z 5 1. Tb, welches als Gesamtheit aller der Versorgung mit Geld, der Vermittlung von Krediten und dem Zahlungsverkehr dienenden öffentlichen und privaten Kreditinstitute und Unternehmen verstanden werden kann.[333] Die Gesetzgebung und Vollziehung des Bankwesens fällt somit ausschließlich in die Kompetenz des Bundes.

7.1.1.4. Sektor Finanzmarktinfrastrukturen

Die Finanzmarktinfrastrukturen stellen gemäß Anhang II Z 4 NIS-RL die Betreiber von Handelsplätzen sowie zentrale Gegenparteien dar. In Art. 10 Abs. 1 Z 5 1. Tb B-VG findet sich der Begriff des Börsewesens. Darunter werden die regelmäßig an bestimmten Orten und zu bestimmten Zeiten stattfindenden Zusammenkünfte von Kaufleuten zum Zwecke des Abschlusses von Handelsgeschäften in Wertpapieren und vertretbaren Waren verstanden[334], unter denen die Betreiber von zentralen Handelsplätzen[335] zweifelsohne subsumiert werden können. Schwieriger erscheint hier die Einordnung des einigermaßen unbekannten Begriffes der zentralen Gegenpartei. Darunter wird eine juristische Person, die zwischen die Gegenparteien der auf einem oder mehreren Märkten gehandelten Kontrakte tritt und somit als Käufer für jeden Verkäufer bzw. als Verkäufer für jeden Käufer fungiert, verstanden.[336] Da es sich dabei um Modalitäten der Abwicklung

[332] Im Sinne des Artikels 4 Nummer 1 Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012., ABl. 2013, L 176/1.

[333] *Raschauer*, Artikel 10 Abs 1 Z 5 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (2011), Rz 23.

[334] VfSlg 17.160/2004.

[335] Im Sinne des Artikels 4 Nummer 24 Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU, ABl 2014 L 173/349.

[336] Im Sinne des Artikels 2 Nummer 1 Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister., ABl 2012, L 201/1.

von Handelsgeschäften[337] und somit ebenso um die Kompetenz des Börsewesens handelt, zählen Regelungen zu Finanzmarktinfrastrukturen zur Gänze zur Kompetenz des Art. 10 Abs. 1 Z 5 1. Tb B-VG.

7.1.1.5. Sektor Gesundheitswesen

Die NIS-RL beschreibt den Sektor des Gesundheitswesens in Anhang II Z 5 als Einrichtungen der medizinischen Versorgung (einschließlich Krankenhäuser und Privatkliniken) bzw. konkreter als jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt.[338] In den Erläuternden Bemerkungen zum NIS-Gesetz[339] wird das Gesundheitswesen in Krankenanstalten und das Rettungswesen unterteilt, Betreiber im Bereich des Arzneimittel-Handels im Sinne des Arzneimittelgesetzes[340] werden nicht unter diesen Begriff subsumiert.[341]

Dies ist mE insofern nicht nachvollziehbar, als die Gesundheitsversorgung in der Richtlinie 2011/24/EU Gesundheitsdienstleistungen darstellt, die von Angehörigen der Gesundheitsberufe gegenüber Patientinnen erbracht werden, um deren Gesundheitszustand zu beurteilen, zu erhalten oder wiederherzustellen, einschließlich der Verschreibung, Abgabe und Bereitstellung Arzneimitteln und Medizinprodukten. Die NIS-RL verweist eben auf den Begriff der Gesundheitsdienstleister im Sinne oben angeführter Richtlinie, weshalb Betreiber im Teilsektor der Arzneimittel-Versorgung jedenfalls auch vom Begriff des Gesundheitswesens erfasst gewesen wären. In diesem Zusammenhang erscheint die NIS-Richtlinie vom nationalen Gesetzgeber unzureichend umgesetzt.[342]

Art. 10 Abs. 1 Z 12 B-VG legt das Gesundheitswesen mit Ausnahme des Leichen- und Bestattungswesens sowie des Gemeindesanitätsdienstes und Rettungswesens, hinsichtlich der Heil- und Pflegeanstalten, des Kurortewesens und der natürlichen Heilvorkommen jedoch nur die sanitäre Aufsicht, als Bundeskompetenz fest. Sowohl der Bereich der Krankenanstalten als auch jener der Rettungsdienste fallen somit nicht in den Regelungsbereich dieser Kompetenz.

---

[337] *Raschauer* in Kneihs /Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, Rz 20.

[338] Art. 3 lit. g Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung, ABl. 2011, L 88/45.

[339] EB RV NISG.

[340] Bundesgesetz vom 2. März 1983 über die Herstellung und das Inverkehrbringen von Arzneimitteln (Arzneimittelgesetz – AMG), BGBl. Nr. 185/1983 idF BGBl. I Nr. 59/2018.

[341] Siehe auch NIS-Verordnung, wo Arzneimittel nicht von den wesentlichen Diensten umfasst sind.

[342] Darüber hinaus können auch Ärzte, Zahnärzte sowie sonstige in Österreich bestehende Gesundheitsberufe wie Hebammen und Krankenpfleger unter den Gesundheitsbegriff subsumiert werden.

Art. 12 Abs. 1 Z 1 regelt die Zuständigkeit für „Heil- und Pflegeanstalten“, wobei davon sowohl öffentliche als auch nicht-öffentliche Krankenanstalten, insbesondere in Form selbstständiger Ambulatorien, erfasst sind.[343] Dienste im Rettungswesen zählen mangels sonstiger Regelung unter die Landeszuständigkeit in Gesetzgebund und Vollziehung gemäß Art. 15 Abs. 1 B-VG.

Dementsprechend ist der Begriff des Gesundheitswesens im Sinne der NIS-RL im Bereich der Kompetenzen des Art. 12 und 15 B-VG unter der Voraussetzung zu subsumieren, dass der nationale Gesetzgeber lediglich Krankenanstalten und Rettungsdienste in den Anwendungsbereich aufgenommen hat.

7.1.1.6. Sektor Trinkwasserlieferung und -versorgung

Die Trinkwasserlieferung und –versorgung umfasst gemäß Anhang II Z 6 NIS-RL Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“[344], jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch nur ein Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist, die nicht als wesentliche Dienste eingestuft werden.

Unter den Begriff des Ernährungswesens einschließlich der Nahrungsmittelkontrolle gemäß Art. 10 Abs. 1 Z 12 B-VG fallen nicht nur Maßnahmen zur Überwachung der Nahrungsmittel vom sanitären Standpunkt, sondern auch Maßnahmen, die unmittelbar die Sicherstellung der Versorgung der Bevölkerung mit Nahrungsmitteln zum Inhalt haben.[345] Maßnahmen zur Sicherung der Netz- und Informationssysteme im Sektor Wasser stellen demgegenüber jedoch lediglich ein Unterstützung bzw. ein Mittel zur Versorgung dar und haben keine unmittelbare Wirkung.

Darüber hinaus kommt Art. 10 Abs. 1 Z 10 mit seinem Kompetenztatbestand des Wasserrechts in Betracht. Zu den vom Kompetenztatbestand erfassten öffentlichen Rücksichten zählen jedenfalls die Versorgung der Allgemeinheit mit Trink- und Nutzwasser[346], wobei Regelungen zur Aufrechterhaltung und zur Sicherstellung der Nutz- und Trinkwasserversorgung nach dem Versteinerungsmaterial[347] ebenso darunter zu subsumieren sind.

Dementsprechend sind Regelungen im Bereich der Trinkwasserlieferung und –versorgung gemäß Art. 10 Abs. 1 Z 10 B-VG als Bundeskompetenz zu bewerten.

---

[343] VfSlg. 13.023/1992.
[344] Im Sinne des Art 2 Nummer 1 lit a Richtlinie 98/83/EG des Rates vom 3. November 1998 über die Qualität von Wasser für den menschlichen Gebrauch, ABl. 1998, L 330/32.
[345] VfGH 5748/1968.
[346] *Raschauer* in Kneihs /Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, Rz 83.
[347] *Raschauer* in Kneihs /Lienbacher, Rill-Schäffer-Kommentar Bundesverfassungsrecht, Rz 78.

7.1.1.7. Sektor Digitale Infrastruktur und Anbieter digitaler Dienste

Digitale Infrastrukturen sind gemäß Anhang II Z 7 NIS-RL Internet-Exchange-Points (IXP)[348], Domain-Namen-Systeme (DNS)-Diensteanbieter[349] sowie TLS-Name-Registries[350]. Entsprechende Kommunikationsdienste werden im nationalen Recht grundsätzlich im Telekommunikationsrecht geregelt. § 3 Z 11 TKG definiert so genannte Kommunikationsnetze als Übertragungssysteme und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen, die die elektronische Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelte, einschließlich Internet) und mobile terrestrische Netze sowie andere Formen, unabhängig von der Art der übertragenen Informationen.

Auch Anbieter digitaler Dienste, die sich gemäß Anhang III der Richtlinie aus Online-Marktplätzen, Online-Suchmaschinen und Cloud-Computing-Diensten zusammensetzen, stellen einen Teilbereich oben genannter fester Netze (einschließlich Internet) dar.

Kommunikationsdienste werden unter den Kompetenztatbestand des Fernmeldewesens gemäß Art. 10 Abs. 1 Z 9 B-VG subsumiert, wodurch die Kompetenz zu Regelungen im Bereich der Digitalen Infrastruktur sowie Anbietern digitaler Dienste in Gesetzgebung und Vollziehung dem Bund obliegt.

7.1.1.8. Zusammenfassende Darstellung

Zusammenfassend kann nun festgestellt werden, dass Gesetzgebung und Vollziehung überwiegend gem. Art. 10 B-VG in die Zuständigkeit des Bundes fallen. Wie oben näher ausgeführt, sind Regelungen zu einigen Teilsektoren entweder in Ausführungsgesetzgebung und Vollziehung Landessache (Art. 12 B-VG), in Vollziehungszuständigkeit der Länder (Art. 11 B-VG) oder in Gesetzgebung und Vollziehung Landessache (Art. 15 B-VG).

Die Begründung von Vollziehungszuständigkeiten des Bundeskanzlers und des Bundesministers für Inneres sowie die Bundesgesetzgebung wäre nach geltender Verfassungsrechtslage in den entsprechend oben dargestellten Bereichen nicht zulässig, wodurch das Erfordernis einer Verfassungsänderung (wie in § 1 NISG realisiert) besteht.

---

[348] Gemäß Art. 4 Z 13 NIS-RL eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet- Datenverkehr; ein IXP dient nur der Zusammenschaltung autonomer Systeme; ein IXP setzt nicht voraus, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; auch wird der betreffende Datenverkehr weder verändert noch anderweitig beeinträchtigt.

[349] Gemäß Art. 4 Z 15 NIS-RL eine Einrichtung, die DNS-Dienste im Internet anbietet.

[350] Gemäß Art. 4 Z 16 NIS-RL eine Einrichtung, die die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top-Level-Domain (TLD) verwaltet und betreibt.

7.1.2. Gegenstand und Ziele des Gesetzes (Anwendungsbereich)

7.1.2.1. Schutzziel

In § 2 NIS-Gesetz sind Gegenstand und Ziele des Gesetzes geregelt. Demnach sollen Maßnahmen festgelegt werden, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste und Einrichtungen des Bundes erreicht werden soll.

Um das konkrete Schutzziel[351] des Gesetzes bewerten zu können, müssen die Legaldefinitionen des § 3 NISG herangezogen werden. Dort wird in § 3 Z 2 die Netz- und Informationssystemsicherheit als die Fähigkeit von Netz- und Informationssystemen definiert, Sicherheitsvorfällen (Z 6) vorzubeugen, diese abzuwehren und zu beseitigen. Als Sicherheitsvorfall gilt eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat, wobei angegebene Parameter zu berücksichtigen sind (§ 3 Z 6). Die NIS-RL selbst sieht in ihrer Begriffsbestimmung ebenso die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit als Bestandteil der Sicherheit von Netz- und Informationssystemen vor (Art. 4 Z 2).

Zumindest angesprochen werden soll, dass beim Schutzziel der Sicherheit von IT-Systemen meist von der so genannten „CIA-Triade“[352] ausgegangen wird, die im Hinblick auf die allgemeinen Schutzziele auf die Vertraulichkeit, die Integrität und die Verfügbarkeit von Systemen abzielt.[353]

---

[351] Schutzziele erlauben Organisationen, unterschiedliche Anforderungen und Logiken in ihren Verfahren und Datenverarbeitungen punktuell aufeinander zu beziehen, siehe *Rost*, Die Ordnung der Schutzziele, Datenschutz und Datensicherheit - DuD, 2018, S. 14.

[352] Die „Heilige Dreifaltigkeit der IT-Sicherheit“ wird durch das CIA-Prinzip ausgedrückt: Confidentiality, Integrity und Availability (Vertraulichkeit, Integrität, Verfügbarkeit), siehe dazu *Abolhassan*, Security Einfach Machen, IT-Sicherheit als Sprungbrett für die Digitalisierung, S. 54. Siehe auch *Rost*, Datenschutz und Datensicherheit - DuD, 2018, S. 14, der von den „konventionellen Schutzzielen“ spricht.

[353] *Gordon*, Official (ISC) Guide to the CISSP CBK[4] (2015). Informationen sollen nicht von Unbefugten mitgelesen werden können (Vertraulichkeit), sollen unverändert beim Empfänger ankommen (Integrität) und der Benutzer soll sich nicht als jemand anders ausgeben können (Authentizität) bzw. seine Urheberschaft auch nicht abstreiten können (Nichtabstreitbarkeit), siehe dazu Henninger/Scheuermann/Schneider et al., "Zurechenbarkeit von Aktionen in virtuellen Welten, Schlussbericht," ed. Gesellschaft (Bundesministerium für Bildung und Forschung (BMBF), 2004). *Toufar*, IT-Recht, in Hofmann /Schmidt (Hrsg), Masterkurs IT-Management, Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker (2010), S. 347. In der österreichischen Rechtsordnung ist bspw. in der Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bedienstete des Bundes (IKT-Nutzungsverordnung – IKT-NV), BGBl. II Nr. 281/2009 idF BGBl. II Nr. 107/2018 die korrekte Funktionsfähigkeit als Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der IKT-Infrastruktur (§ 1 Z 3 IKT-NV) definiert.

Neben diesen drei „elementaren Schutzzielen“[354] werden in der Fachliteratur teilweise ebenso weitere Schutzziele der IT-Sicherheit genannt, darunter die Authentizität, die Verbindlichkeit/Nichtabstreitbarkeit, die Zurechenbarkeit[355], die Verdecktheit, Nachweisbarkeit, Verlässlichkeit, Unverkettbarkeit, Unbeobachtbarkeit und Anonymität.[356]

Nun stellt sich mE die Frage, warum der Richtlinientext (und auch die nationale Umsetzung) das zusätzliche Ziel der Authentizität vorsehen, obwohl dieses möglicherweise von den drei grundsätzlichen Schutzzielen ohnedies abgedeckt gewesen wäre.[357] Ein Blick auf das deutsche BSI-Gesetz[358] zeigt, dass dort die Sicherheit in der Informationstechnik durch die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit[359] oder Vertraulichkeit von Informationen betreffen (§ 2 Abs. 2 BSIG), definiert wird und sich dieses somit nur auf die grundlegenden drei Schutzziele bezieht.

Bedner/Ackermann sehen die Authentizität gewährleistet, wenn durch geeignete Kontrollmaßnahmen sichergestellt wird, dass Daten und Informationen wirklich aus der angegebenen Quelle stammen und dass die Identität eines Benutzers oder eines angeschlossenen Systems korrekt ist. Die Authentizität sei demnach von den ursprünglichen drei Schutzzielen nicht umfasst, sondern die Notwendigkeit zweier weiterer übergeordneter Schutzziele, nämlich die Kontingenz[360] und die Transparenz, gegeben.[361] Im Datenschutz sehen *Rost/Pfitzmann* zusätzlich die Unverkettbarkeit als genuines Schutzziel[362], *Bock/Meissner* zusätzlich die Intervenierbarkeit[363].[364]

---

[354] Zur Verfügbarkeit, Integrität und Vertraulichkeit als elementare Schutzziele siehe *Rost/Pfitzmann*, Datenschutz-Schutzziele - revisited, Datenschutz und Datensicherheit - DuD, 6/2009, S. 353.
[355] *Gordon*, Official (ISC) Guide to the CISSP CBK[4].
[356] *Bedner/Ackermann*, Schutzziele der IT-Sicherheit, Datenschutz und Datensicherheit - DuD, 5/2010, S. 323.
[357] Zur früheren Ansicht, dass alle Schutzziele durch die drei übergeordneten Schutzziele abgedeckt seien, siehe *Bedner/Ackermann*, Datenschutz und Datensicherheit - DuD, 2010, S. 323.
[358] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Art. 1 G v. 23.6.2017 I 1885 (Deutschland).
[359] Unversehrtheit kann als Synonym für die Integrität von Informationen gesehen werden.
[360] Zur Notwendigkeit des Schutzziels der Kontingenz zusätzliches viertes elementares Schutzziel siehe *Rost/Pfitzmann*, Datenschutz und Datensicherheit - DuD, 2009.
[361] *Bedner/Ackermann*, Datenschutz und Datensicherheit - DuD, 2010, S. 323ff.
[362] *Rost/Pfitzmann*, Datenschutz und Datensicherheit - DuD, 2009, S. 357. Genauso (konkret wird von drei Schutzziel-Dualen gesprochen) *Jensen*, Zur Messbarkeit von Schutzzielen, Datenschutz und Datensicherheit - DuD, 1/2018, S. 23.
[363] *Bock/Meissner*, Datenschutz-Schutzziele im Recht, Datenschutz und Datensicherheit - DuD, 6/2012, S. 425.
[364] Die gesetzlichen Regelungen im Datenschutzrecht lassen sich ihrem normativen Zweck nach stets auf mindestens eines der sechs fundamentalen Schutzziele zurückführen, siehe *Robrahn/Bock*, Schutzziele als Optimierungsgebote, Datenschutz und Datensicherheit - DuD, 1/2018, S. 8.

Hinsichtlich der Schutzziele muss nach *Bock/Meissner* jedoch zwischen Datenschutz[365] und Datensicherheit – die der Sicherheit von Netz- und Informationssystemen entspricht – unterschieden werden, wobei im Bereich der IT-Sicherheit die drei Schutzziele der Verfügbarkeit, Integrität und Vertraulichkeit seit langem anerkannt sind.[366]

Es ist erkennbar, dass Schutzziele unterschiedlich definiert, geordnet und strukturiert werden und diesbezüglich offenbar kein einheitlicher Standard herrscht. [367] Nichtsdestotrotz kristallisieren sich die drei elementaren Schutzziele der Vertraulichkeit, Verfügbarkeit und Integrität im Bereich der IT-Sicherheit als zentrale Schutzziele heraus.

Trotzdem führt sowohl die NIS-Richtlinie als auch das NIS-Gesetz als zusätzliches Ziel jenes der Authentizität an. ME kann dieses Ziel als Teil der Vertraulichkeit, die voraussetzt, dass nur befugt – und somit nur von authentifizierten Benutzern - auf Verfahren und Daten zugegriffen werden kann[368], bewertet werden und wäre somit von den allgemeinen drei Schutzzielen umfasst. Für eine eigenständige Auflistung im Richtlinientext sowie im NIS-Gesetz bestand meines Erachtens keine Notwendigkeit.

7.1.2.2. Sachlicher Anwendungsbereich

Auch die Struktur des sachlichen Anwendungsbereiches muss aufgrund der Zahl an Verweisen und der inhaltlichen Streuung im Gesetz näher untersucht werden.
Sowohl die Betreiber wesentlicher Dienste (§ 3 Z 10 NISG), als auch die Anbieter digitaler Dienste (§ 3 Z 12) und Einrichtungen der öffentlichen Verwaltung (§ 3 Z 19) werden im Gesetz legal definiert.

§ 3 Z 10 spricht bei Betreibern wesentlicher Dienste von Einrichtungen mit Niederlassung in Österreich, die einen wesentlichen Dienst erbringen. Unter einem wesentlichen Dienst wird gemäß § 3 Z 9 ein Dienst verstanden, der in einem der in § 2 genannten Sektoren erbracht wird und der eine wesentliche Bedeutung insbesondere für die Aufrechterhaltung des öffentlichen Gesundheitsdienstes, der öffentlichen Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Verkehrs oder die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologien hat und dessen Verfügbarkeit abhängig von Netz- und Informationssystemen ist.

[365] Die DSGVO verweist in ihrem Art. 32 auf die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.
[366] *Bock/Meissner*, Datenschutz und Datensicherheit - DuD, 2012, S. 425f.
[367] Zur Kritik von Pfitzmann am Wildwuchs beim Ausrufen immer neuer Schutzziele durch immer neue Organisationen in einem internen Arbeitspapier siehe *Rost*, Datenschutz und Datensicherheit - DuD, 2018, S. 13.
[368] *Bock/Meissner*, Datenschutz und Datensicherheit - DuD, 2012, S. 427.

§ 16 Abs. 1 NISG regelt die Ermittlung der Betreiber wesentlicher Dienste und legt fest, dass für jeden in § 2 genannten Sektor jene Betreiber wesentlicher Dienste mit Niederlassung in Österreich ermittelt werden, die einen wesentlichen Dienst (§ 3 Z 9) erbringen.

Hier ist einerseits die neuerliche Voraussetzung der Niederlassung in Österreich unnötig, da diese bereits in der Legaldefinition des § 3 Z 10 bei Betreibern wesentlicher Dienste geregelt wird. Darüber hinaus ist die neuerliche Nennung der Erbringung eines wesentlichen Dienstes überflüssig, da dies ebenso eine Voraussetzung eines Betreibers wesentlicher Dienste in der Legaldefinition des § 3 Z 10 darstellt.

Des Weiteren bezieht sich § 16 Abs. 1 auf die in § 2 genannten Sektoren[369], obwohl in der Legaldefinition des § 3 Z 9 ein wesentlicher Dienst bereits dahingehend beschrieben wird, als dieser eine besondere Bedeutung für den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser und die weiteren Bereiche haben soll. Auffallend bei dieser Konstruktion ist, dass die betroffenen Sektoren scheinbar zweimalig aufgelistet sind. Einerseits werden die Sektoren in § 2 auf die sieben genannten Bereiche beschränkt, andererseits erfolgt eine Einschränkung der Wesentlichkeit ebenso in der Legaldefinition der wesentlichen Dienste gem. § 3 Z 9.

Für diese Doppelnennung spricht wohl nur, dass die bereits im österreichischen Recht existente Legaldefinition der kritischen Infrastruktur[370] – worum es sich bei Betreibern wesentlicher Dienste im Grunde handelt – mit dem Ziel einer Kontinuität und Komplementarität der Rechtsordnung Verwendung finden und andererseits in § 2 eine klare und eindeutige Nennung des Anwendungsbereiches (konsistent mit der Auflistung der NIS-RL) erfolgen sollte. Anders ist es nicht zu erklären, dass die Beschränkung auf die genannten Sektoren nicht klar und deutlich in der Legaldefinition der wesentlichen Dienste (§ 3 Z 9) erfolgen und die explizite Nennung der Sektoren in § 2 entfallen konnte. Als Beispiele dafür ist „der öffentliche Gesundheitsdienst“ [371] (§ 3 Z 9) und der Sektor „Gesundheit“ (§ 2 Z 5), „die öffentliche Versorgung mit Wasser“ (§ 3 Z 9) und der Sektor „Trinkwasserversorgung“ (§ 2 Z 6) oder „der öffentliche Verkehr“ (§ 3 Z 9) und der Sektor „Verkehr“ (§ 2 Z 2) zu erwähnen.

Des Weiteren auffällig im Vergleich dieser eng im Zusammenhang stehenden Definitionen ist, dass die Sektoren Bankwesen und Finanzmarktinfrastrukturen nicht von der Definition der

[369] Dabei handelt es sich gem. § 2 NISG um die Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur.
[370] § 22 Abs. 1 Z 6 SPG sowie § 74 Abs. 1 Z 11 StGB, mehr zur Legaldefinition im SPG in Kapitel 4.2.2.
[371] In den EB der Strafrechts-Novelle 2015 wird festgehalten, dass der Begriff des „öffentlichen Gesundheitsdienstes“ im Sinne dieser Bestimmung auch die Sozialversicherungsträger umfasst, siehe 98/ME XXV. GP RV EB Strafrechtsänderungsgesetz 2015.

Wesentlichkeit eines Dienstes in § 3 Z 9 umfasst zu sein scheinen. Diese auf den ersten Blick zu enge Legaldefinition des § 3 erweitert sich in Anbetracht der teleologischen Interpretation derselben aus dem Sicherheitspolizeigesetz (siehe auch Kapitel 4.2.2), die unter dem Begriff der „Informations- und Kommunikationstechnologien“ auch den elektronischen Zahlungsverkehr umfasst sieht. [372]

Im Rahmen der teleologischen Interpretation der Wesentlichkeit eines Dienstes im Sinne einer kritischen Infrastruktur bzw. der Daseinsvorsorge sind unter den lebenswichtigen Gütern (§ 3 Z 9) mE wohl auch Lebensmittel zu subsumieren[373], deren Produktion bzw. Verteilung jedoch nicht vom Anwendungsbereich des NISG umfasst sein sollen.[374] Aus diesem Grund erscheint bei Verwendung dieser Definition aus dem Sicherheitspolizeigesetz zur Definition der Wesentlichkeit eines Dienstes nichtsdestotrotz eine Einschränkung auf die tatsächlich relevanten Sektoren in § 2 erforderlich.

Zusammenfassend kann mE nunmehr festgestellt werden, dass trotz des Bestrebens, bereits in der österreichischen Rechtsordnung existente Begriffe mit ähnlicher Bedeutung zu verwenden, eine einfachere Struktur durch eine einmalige neue Definition im NIS-Gesetz zu erreichen gewesen wäre.

Über die NIS-RL hinausgehende Einbeziehung von Sektoren unter Betrachtung des Deregulierungsgrundsätzegesetzes

Die NIS-RL gibt in ihrem Anhang II taxativ aufgelistete Sektoren vor, die in dieser Form auch vom NIS-Gesetz in § 2 übernommen wurden. Auffallend ist, dass die in der Richtlinie vorgegebenen Sektoren nicht alle Bereiche der so genannten kritischen Infrastruktur, auf deren Schutz die Richtlinie grundsätzlich abzielt, auflistet. Dazu zählen beispielsweise die Lebensmittelversorgung, die Abwasserentsorgung sowie die öffentliche Verwaltung.

[372] Der Begriff der IKT umfasst jegliches Kommunikationsinstrument oder Kommunikationsanwendung, inklusive Radio, Fernsehen, Mobiltelefonie, Hardware und Software für Computer und Netzwerke, Satellitensysteme sowie die verschiedenen Dienstleistungen und Anwendungen, die damit verbunden sind. Darunter fallen beispielsweise die von staatlicher Seite geführten Rechenzentren oder der gesamte elektronische Zahlungsverkehr, siehe XXV. GP RV EB SPG-Novelle 2014.

[373] Diese Interpretation ergibt sich aus dem Sicherheitspolizeigesetz, welches in seiner Definition von kritischen Infrastrukturen von „lebenswichtigen Gütern“ spricht und in einem Ansatz der gesamtheitlichen Daseinsvorsorge damit die Lebensmittelversorgung wohl miteinschließt.

[374] Auch die NIS-RL schließt den Lebensmittelsektor nicht in den Anwendungsbereich mit ein, siehe Anhang II NIS-RL.

Begründet kann dies mit der (scheinbar) fehlenden, umfassenden Abhängigkeit der Unternehmen in diesen Bereichen von Informations- und Kommunikationssystemen werden[375], wenngleich dies wohl mE nicht der Realität und noch viel weniger der nahen Zukunft entsprechen wird.

Beispielsweise erfolgt die Logistik in großen Zentrallagern von Lebensmittelhändlern mittlerweile mit automatisiert gesteuerten Maschinen, bei deren Ausfall eine Belieferung der einzelnen Filialen kaum mehr vorstellbar wäre. Darüber hinaus erfolgt die Warenbestellung einzelner Filialen mittlerweile ebenso automatisiert und eine händische Bestellung ist heutzutage kaum mehr möglich.[376] Ähnliches gilt für die Abwasserentsorgung, deren Pump- und Leitsysteme automatisiert betrieben werden.[377]

Darüber hinaus sollte die Richtlinie nicht nur die Gegenwart, sondern viel mehr die Zukunft ins Auge fassen. Auch wenn offenbar der Eindruck bestand, die Abhängigkeit dieser beiden Bereiche sei nicht im großen Ausmaß gegeben, so lässt die fortschreitende Digitalisierung doch nur erahnen, dass sich die diesbezüglichen Interdependenzen in den nächsten Jahren kontinuierlich verstärken werden. Insbesondere aufgrund dieses Umstandes wäre es mE wünschenswert gewesen, auch die für die Bevölkerung wesentlichen Sektoren der Lebensmittelversorgung und der Abwasserentsorgung in den Richtlinientext mit aufzunehmen.

Im Zuge dieser Diskussion stellt sich natürlich die Frage, ob es nicht dem nationalen Gesetzgeber möglich gewesen wäre, über die Richtlinie hinaus weitere Sektoren aufzunehmen. In der NIS-RL wurde ausdrücklich der Grundsatz der Mindestharmonisierung festgelegt (Art. 3). Demnach kann der nationale Gesetzgeber Bestimmungen erlassen oder aufrechterhalten, mit denen ein höheres Sicherheitsniveau von Netz- und Informationssystemen erreicht werden soll – darunter ist auch die Einbeziehung zusätzlicher Sektoren zu verstehen.

Dies gilt insbesondere für öffentliche Verwaltungen, die für andere Sektoren und Dienste als die in den Anhängen II und III der Richtlinie aufgeführten zuständig sind.[378] Die EU-Kommission geht sogar so weit, die Einbeziehung der öffentlichen Verwaltung in den Anwendungsbereich der nationalen Rechtsvorschriften zu erwägen.[379] Erfolgt ist dies beispielsweise in Deutschland, wo im IT-

[375] Zur Kritik an der Einbeziehung zusätzlicher Sektoren im IT-Sicherheitsgesetz in Deutschland siehe *Heinickel/Feiler*, IT-SiG-E - europarechtlicher Kontext und die Bedürfnisse der Praxis, Computer und Recht, 11/2014, S. 711.

[376] Mehr dazu *Amann*, Bedeutung von Produktionskompetenz im Supply Chain Management : Entwicklung einer marktorientierten Steuerungskonzeption am Beispiel der Lebensmittelindustrie (2009). Ebenso *Hofer/Hofmann/Stölzle*, Management der Filiallogistik im stationären Einzelhandel: Eine ressourcenorientierte Betrachtung, Marketing: Zeitschrift für Forschung und Praxis, 2/2009.

[377] Mehr dazu *Hiessl*, Alternativen der kommunalen Wasserversorgung und Abwasserentsorgung (2003).

[378] COM(2017) 476 final , Annex 1, S. 6.

[379] COM(2017) 476 final , Annex 1, S. 25.

Sicherheitsgesetz die genannten Bereiche der Lebensmittelversorgung und Abwasserentsorgung ebenso in den Anwendungsbereich aufgenommen wurden.

Sieht man sich den Anwendungsbereich des NIS-Gesetzes genauer an, fällt auf, dass die Einrichtungen der öffentlichen Verwaltung hier neben den aus der Richtlinie bekannten Betreibern wesentlicher Dienste und Anbietern digitaler Dienste ebenso erfasst sind (§ 2 NISG). Zu diskutieren ist in Bezug darauf, ob diese „Übererfüllung der Richtlinie" dem Bundesgesetz über die Grundsätze der Deregulierung (Deregulierungsgrundsätzegesetz)[380] widersprechen könnte.

§ 1 Abs. 4 Deregulierungsgrundsätzegesetz regelt, dass bei der Vorbereitung der Umsetzung von Rechtsakten der Europäischen Union darauf zu achten ist, dass die vorgegebenen Standards nicht ohne Grund übererfüllt werden. Das Verbot dieser unbegründeten Übererfüllung - auch als „Gold Plating" bezeichnet - hat eine Verwaltungsreduktion für Bürgerinnen und Bürger sowie für Unternehmen zum Ziel.[381] Dieses Ziel ist auch im Regierungsprogramm 2017-2022 häufig erwähnt, insbesondere mit dem Hintergrund, die heimische Wirtschaft nicht mit erheblichen Kosten zu belasten und die österreichische Wettbewerbsfähigkeit nicht massiv zu gefährden.[382]

Ebenso gilt der Grundsatz, dass anlässlich der geplanten Erlassung von Bundesgesetzen zu prüfen ist, ob die zu erlassenden Bestimmungen notwendig und zeitgemäß sind und ob die angestrebten Wirkungen nicht auch auf andere Weise erreicht werden könnten (§ 1 Abs. 1 Deregulierungsgrundsätzegesetz). Gem. § 1 Abs. 2 ist sicherzustellen, dass der aus der Erlassung von Bundesgesetzen resultierende bürokratische Aufwand sowie die finanziellen Auswirkungen für Bürgerinnen und Bürger sowie für Unternehmen gerechtfertigt und adäquat sind. Zur Vermeidung weiterer Belastungen wird jede Neuregelung, aus der zusätzlicher bürokratischer Aufwand oder zusätzliche finanzielle Auswirkungen erwachsen, nach Tunlichkeit durch Außerkraftsetzung einer vergleichbar intensiven Regulierung kompensiert.

Anlässlich dieser Bestimmung ist einerseits zu prüfen, ob die Einbeziehung der Einrichtungen der öffentlichen Verwaltung gesetzwidrig ist bzw. ob die Einbeziehung weiterer Sektoren rechtswidrig gewesen wäre.[383]

[380] Bundesgesetz über die Grundsätze der Deregulierung (Deregulierungsgrundsätzegesetz), BGBl. I Nr. 45/2017.
[381] 1503 der Beilagen XXV. GP, RV Deregulierungsgrundsätzegesetz, Vorblatt und WFA.
[382] Arbeitsprogramm der österreichischen Bundesregierung 2013-2018, 2013, S. 132.
[383] 78/ME XXVI. GP, ME NIS-Gesetz, Vorblatt und WFA führen ausdrücklich an, dass eine Übererfüllung unionsrechtlicher Vorgaben, die zu einer Mehrbelastung der betroffenen Unternehmen führt, nicht vorliegt.

Eine SWP-Studie aus dem Jahr 2012 ergab, dass das deutsche Regierungsnetz pro Tag vier bis fünf Mal unter Beteiligung fremder Nachrichtendienste attackiert werde.[384] 2018 wurden großangelegte Hacker-Angriffe auf das deutsche Regierungsnetz bekannt[385]. 2017 fanden zahlreiche Angriffe auch auf österreichische Regierungsnetze statt, wie beispielsweise auf Server des Bundesministeriums für Europa, Internationales und Äußeres[386] sowie auf das Parlament[387].

Auch die EU-Kommission stellt in ihren Empfehlungen fest, dass die Gesellschaft und die Wirtschaft als Ganzes großes Interesse an einem hohen Sicherheitsniveau der Netz- und Informationssysteme der öffentlichen Verwaltung haben.[388] Auch wenn die Einbeziehung EU-Recht nicht widerspricht, stellt sich die Frage, ob die zusätzliche Einbeziehung mit der Vorgabe des Deregulierungsgrundsätzegesetzes, „Gold-Plating" zu vermeiden, vereinbar ist. Dieses Verbot gilt grundsätzlich nur für die Übererfüllung von EU-Recht „ohne Grund". Dieser Grund ist jedoch zweifelsfrei gegeben.

Einerseits stehen – wie bereits weiter oben dargestellt – insbesondere Regierungsnetze im Fokus von Angreifern, deren modi operandi wichtige Erkenntnisse für die gesamte Netz- und Informationssystemsicherheit bringen können. Andererseits ist das Funktionieren der staatlichen Systeme oftmals wichtige Voraussetzung für wirtschaftliche Prozesse. Ein Grund für die Übererfüllung kann somit jedenfalls argumentiert werden. Darüber hinaus ist zu diskutieren, ob mit dem Verbot des „Gold Plating" nicht viel mehr auf eine Deregulierung privater Unternehmen bzw. der Wirtschaft abgezielt wurde, und nicht so sehr darauf, ob der Staat sich selbst zu verstärkten Maßnahmen verpflichtet. Das Arbeitsprogramm der Regierung (2017-2022) als auch die Materialien zum Deregulierungsgrundsätzegesetz bestätigen diese Annahme. Auch der darauf resultierende bürokratische Aufwand (§ 1 Abs. 2) ist demnach wohl gerechtfertigt und adäquat, weshalb die Einbeziehung der Einrichtungen der öffentlichen Verwaltung mE nicht dem Deregulierungsgrundsätzegesetz widerspricht.

Legaldefinition zu Einrichtungen der öffentlichen Verwaltung

Neben der Einbeziehung der Einrichtungen der öffentlichen Verwaltung soll auch deren Legaldefinition in § 3 NISG näher untersucht werden. Einrichtungen der öffentlichen Verwaltung

[384] *Bendiek*, SWP, 2012, S. 10.
[385] https://derstandard.at/2000075216495/Hacker-drangen-in-deutsches-Regierungsnetz-ein, abgerufen am 24.06.2018.
[386] https://derstandard.at/2000053654097/Tuerkische-Hacker-Attacke-auf-Aussenministerium, abgerufen am 24.06.2018.
[387] http://wien.orf.at/news/stories/2824188/, abgerufen am 24.06.2018.
[388] COM(2017) 476 final , Annex 1, S. 25.

definiert das NIS-Gesetz mit den Einrichtungen des Bundes und jener Länder, die von der Möglichkeit gem. § 22 Abs. 5 NISG Gebrauch gemacht haben (§ 3 Z 19).

Als Einrichtungen des Bundes versteht das NIS-Gesetz das Bundeskanzleramt, die Bundesministerien, die Gerichtshöfe öffentlichen Rechts, den Rechnungshof, die Volksanwaltschaft, die Präsidentschaftskanzlei und die Parlamentsdirektion; weitere Dienststellen des Bundes können vom zuständigen Bundesminister durch Verordnung bestimmt werden (§ 3 Z 18).

Aus Sicht von *Anderl/Heußler/Mayer/Müller* erscheint die Auswahl der Einrichtungen willkürlich.[389] Nicht verständlich sei demnach, wieso der Rechnungshof und die Volksanwaltschaft für die Funktionsfähigkeit des (Rechts-)Staates essentiell sein sollen, nicht jedoch beispielsweise der Oberste Gerichtshof oder die Sicherheitsbehörden.

Meines Erachtens findet sich jedoch sehr wohl eine rechtliche Begründung für diese Auswahl. Nach *Adamovich/Funk* sind neben den in Art. 19 Abs. 1 B-VG genannten obersten Organen der Vollziehung (Bundespräsident, Bundesminister und Staatssekretäre sowie Mitglieder der Landesregierungen) auf Grund ausdrücklicher bundesverfassungsgesetzlicher Anordnung weiters oberste Organe der Verwaltung des Bundes der Präsident des Nationalrates, der Präsident des Rechnungshofes, der Vorsitzende der Volksanwaltschaft, der Präsident des Verwaltungsgerichthofes und der Präsident des Verfassungsgerichtshofes.[390] Ähnlich dazu *Wimmer* in *Thanner/Vogl*, der die Volksanwaltschaft jedoch nicht von diesem Begriff umfasst sieht.[391] Die in § 3 Z 18 genannten Organisationen sind die Geschäftsapparate der hier genannten Obersten Organe – die diesbezügliche Einbeziehung erscheint mE somit durchaus schlüssig.

Wo *Anderl/Heußler/Mayer/Müller* eine Erweiterung der Definition im NIS-Gesetz zumindest auf die Sicherheitsbehörden fordern, wäre meines Erachtens der bereits in der Rechtsordnung verwendete Begriff der verfassungsmäßigen Einrichtungen (§ 22 Abs. 1 Z 2 SPG)[392] zielführender gewesen, anstatt eine eigene (durch Legaldefinition eingeschränkte) Begrifflichkeit der Einrichtungen des Bundes zu schaffen. Dies kann damit begründet werden, dass eben bereits das Sicherheitspolizeigesetz in § 22 Abs. 1 den vorbeugenden Schutz bestimmter Rechtsgüter nennt, und damit neben den kritischen Infrastrukturen auch die verfassungsmäßigen Einrichtungen davon

[389] *Anderl et al.*, NISG::Kommentar, § 3, Rz 47.
[390] Siehe dazu *Adamovich et al.*, Österreichisches Staatsrecht, Rz 47.005.
[391] *Wimmer* in Thanner /Vogl, Sicherheitspolizeigesetz, Kommentar.
[392] *Wimmer* in *Thanner/Vogl* subsumiert darunter jene Einrichtungen des Bundes oder der Länder, die im Staatsgefüge eine wesentliche Rolle spielen und denen eine verfassungsgesetzliche Bestandsgarantie zukommt, siehe *Wimmer* in Thanner /Vogl, Sicherheitspolizeigesetz, Kommentar, S. 211.

umfasst.[393] Wenn diesen Einrichtungen bereits durch Bundesgesetz eine so wesentliche Bedeutung eingeräumt wird ist mE unverständlich, warum dieser Ansatz nicht durch das NISG vervollständigt wird.

Die gesetzliche Möglichkeit, weitere Dienststellen des Bundes durch Verordnung dem Anwendungsbereich unterliegend zu bestimmen, kann sich anhand einer systematischen Interpretation in Bezug auf die Regelung in § 22 Abs. 5 (wonach die Länder die Pflichten gem. NISG auch in Hinblick auf die von ihren Einrichtungen erbrachten wichtigen Dienste für anwendbar erklären können) wohl nur auf die unmittelbare Bundesverwaltung beziehen.[394]

Einbeziehung der Sektoren Lebensmittelversorgung und Abwasserentsorgung in den Anwendungsbereich

Zusätzlich soll untersucht werden, ob die Einbeziehung der Lebensmittelversorgung und der Abwasserentsorgung (denkbar wäre mE auch noch der Bereich der Chemischen Industrie und des Postwesens)[395] über den Richtlinientext hinaus in das NIS-Gesetz zulässig gewesen wäre.

Wenngleich bei den Einrichtungen der öffentlichen Verwaltung eine Begründung für die Übererfüllung argumentiert werden konnte, so fällt dies für die beiden angeführten Bereiche mE schwererer. Einerseits sind – zumindest medial – keine IT-Angriffe auf Lebensmittelhändler oder Abwasserversorger bekannt, die Ausfälle dieser Betreiber befürchten lassen würden. Auf der anderen Seite besteht keine so große Abhängigkeit der anderen im NIS-Gesetz genannten Sektoren (§ 2) von diesen beiden Bereichen, wie dies möglicherweise bei der öffentlichen Verwaltung der Fall ist.

Darauf lassen auch die Empfehlungen der EU-Kommission schließen, die zwar auf eine Einbeziehung der öffentlichen Verwaltung, nicht aber der anderen beiden Bereiche dezidiert hinweisen. Aus diesem Grund wäre die Einbeziehung von Unternehmen aus der Lebensmittelbranche bzw. der Abwasserversorgung ein ideales Beispiel für ein so genanntes „Gold Plating“ (im Sinne der Verschlechterung der Wettbewerbsfähigkeit nationaler Unternehmen) und würde aus diesem Grund mE dem Deregulierungsgrundsätzegesetz widersprechen.

Sieht man sich das die NIS-RL umsetzende IT-Sicherheitsgesetz in Deutschland an, fällt neben zahlreichen anderen Bereichen auch die Einbeziehung von Rechenzentren („Dienstleister für IT“) ins Auge, die ebenso wenig vom Richtlinientext umfasst sind und deren Einbeziehung auf den ersten

[393] Mehr zur Bestimmung im Sicherheitspolizeigesetz in Kapitel 4.2.2.
[394] *Anderl et al.*, NISG::Kommentar, § 3, Rz 49.
[395] Dabei handelt es sich mE ebenso um Bereiche, die eine wesentliche Bedeutung für das Funktionieren der Daseinsvorsorge haben.

Blick sinnvoll erscheint. Dem ist zu entgegnen, dass es sich bei den Rechenzentren (die aufgrund der betriebenen Services) um Dienstleister für Betreiber wesentlicher Dienste zum Betrieb derer IT-Systeme handelt und von den Rechenzentren damit die Sicherheitsvorkehrungen mittelbar ohnedies über die Verpflichtung der Betreiber wesentlicher Dienste selbst erfüllt werden müssen.[396]

Einbeziehung der Telekommunikationsdienste in den Anwendungsbereich

Auf den ersten Blick überraschend erscheint die Tatsache, dass Betreiber von Telekommunikationsdiensten (zum Beispiel Mobilfunkbetreiber) nicht von den in Annex II angeführten Sektoren und Teilsektoren umfasst sind. Die Mobilfunkversorgung stellt heutzutage neben der Energieversorgung wohl die wesentlichste Versorgungsader einer Gesellschaft dar und ist gerade auch deshalb einer Bedrohung durch Hacker-Angriffe ausgesetzt. Der Grund für die Nichteinbeziehung dieses Sektors liegt in bereits bestehenden besonderen Sicherheits- und Integritätsanforderungen, die für Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste im Sinne der Richtlinie 2002/21/E des Europäischen Parlaments und des Rates bereitstellen, gelten, wie auch Erwägungsgrund 7 NIS-RL klarstellt. Jene Richtlinie wurde in Österreich im Telekommunikationsgesetz 2003 (TKG 2003) umgesetzt.[397]

Mehr zu den Sicherheitsvorkehrungen und Meldepflichten im Rahmen des Telekommunikationsgesetzes sowie zur Überschneidung mit den Bestimmungen des NIS-Gesetzes sind in den Kapiteln 0 (Sicherheitsvorkehrungen) sowie 7.5.6 (Meldepflicht) zu finden.

[396] Mehr dazu siehe Kapitel 7.5.4.6.
[397] Mehr zum EU-rechtlichen Hintergrund siehe Kapitel 5.5.

7.2. Abschnitt 2 - Aufgaben und Strukturen

7.2.1. Möglichkeiten der Einrichtung zuständiger Behörden in Österreich

Die in der NIS-RL festgelegten behördlichen Aufgaben sollen in den EU-Mitgliedstaaten von den dort einzurichtenden, so genannten „zuständigen Behörden“[398] umgesetzt werden. Nach der Rechtsprechung des EuGH steht es jedem Mitgliedstaat frei, die Kompetenzen innerstaatlich zweckmäßig zu verteilen.[399] „Dies wird auch als Grundsatz der institutionellen Autonomie der Mitgliedstaaten bezeichnet.“[400] Angesichts unterschiedlicher nationaler Verwaltungsstrukturen und um bestehende Aufsichts- oder Regulierungsbehörden[401] beibehalten zu können, soll es möglich sein, mehr als nur eine nationale Behörde zu benennen und mit den Aufgaben zu betrauen[402] sowie bestehende Organisationsstrukturen zu nutzen.[403]

In Österreich obliegen dem Bundeskanzler sowie dem Bundesminister für Inneres verschiedene Aufgaben im Rahmen des NIS-Gesetzes, wobei diese nach strategischen und operativen Gesichtspunkten aufgeteilt wurden. Eine neue zuständige Behörde wurde nicht eingerichtet.

Diese Aufteilung sollte dem gem. Art. 77 Abs. 2 B-VG durch das Bundesministeriengesetz (BMG)[404] festgelegten Wirkungsbereich der Bundesministerien entsprechen. Ob dies der Fall ist, wird in den nächsten beiden Kapiteln zu den Aufgaben des Bundeskanzlers[405] und des Bundesministers für Inneres[406] genauer diskutiert. Diesbezüglich soll aber sogleich festgestellt werden, dass das BMG grundsätzlich nur den allgemeinen Wirkungsbereich regelt und sich der besondere Wirkungsbereich vielmehr in erster Linie aus den die einzelnen Gebiete der Verwaltung regelnden Bundesgesetzen ergibt. Demgegenüber haben die Regelungen des BMG somit nur subsidiären Charakter.[407]

Anzumerken ist, dass die Vollziehung des NIS-Gesetzes dem Bundeskanzler und dem Bundesminister für Inneres als monokratische Organe zugewiesen ist, das BMG dagegen den Wirkungsbereich des Bundeskanzleramtes und des Bundesministeriums für Inneres regelt. Der

---

[398] Siehe bspw. ErwGr 32 NIS-RL.
[399] EuGH Rs C-131/88 (Kommission/Deutschland), Slg 1991, I-825 Rz 71.
[400] *Öhlinger/Potacs*, EU-Recht und staatliches Recht[6], S. 149.
[401] Mehr zu den Aufgaben der Regulatoren in Österreich siehe *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.053.
[402] ErwGr 30 NIS-RL.
[403] ErwGr 37 NIS-RL.
[404] Mehr zum Bundesministeriengesetz siehe Kapitel 4.2.1.
[405] Kapitel 7.2.2.
[406] Kapitel 7.2.3.
[407] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 47.017.

Unterschied kann damit begründet werden, dass die Geschäfte der obersten Bundesverwaltung unter anderem von den Bundesministern als Einzelorganen besorgt werden und diese mit der Leitung eines Bundesministeriums und damit des diesem Bundesministeriums zugewiesenen sachlichen Aufgabenbereiches (Ressort im funktionellen Sinn im Sinne des BMG) betraut sind. [408] *Barfuß* spricht davon, dass „Ressort und Ressortminister erst und nur in ihrer Kombination Leben, politische Realität und spezifische juristische Bedeutung erhalten".[409]

In einer im Jänner 2016 veröffentlichten Studie[410] über die verschiedenen Ansätze der Mitgliedstaaten zum Schutz kritischer Informationsinfrastrukturen (Critical Information Infrastructure Protection - CIIP)[411] wurden zwei grundlegende Profile zu behördlichen Zuständigkeiten in diesem Bereich beschrieben, die in ähnlicher Form auch für die Zuständigkeiten im Rahmen der Sicherheit von Netz- und Informationssystemen Anwendung finden können.

Der dezentrale Ansatz beinhaltet ein Subsidiaritätsprinzip, eine enge Zusammenarbeit zwischen den öffentlichen Stellen und sektorspezifischen Rechtsvorschriften. Anstatt eine zentrale Stelle einzurichten, werden die NIS-Aufgaben bestehenden, sektorspezifischen Behörden zugeordnet, die eine hohe Expertise in den jeweiligen Sektoren und enge Verbindung zu den zugehörigen Betreibern auszeichnet. Nachteil dieses Ansatzes sind die möglicherweise unterschiedlichen Umsetzungsgrade und die uneinheitliche Anwendung der Sicherheit von Netz- und Informationssystemen in den jeweiligen Materiengesetzen der Sektoren. Jedenfalls muss aber eine zentrale Anlaufstelle als Schnittstelle für grenzüberschreitende Angelegenheiten eingerichtet werden, die auch die Zusammenarbeit zwischen den dezentralen Behörden koordinieren könnte.[412]

Der zentrale Ansatz zeichnet sich durch eine für alle Sektoren zuständige zentrale Behörde und umfassende Rechtsvorschriften aus, wodurch in dieser Behörde eine hohe Kompetenz zur Sicherheit von Netz- und Informationssystemen vorliegt. Darüber hinaus kann durch die zentrale Zuständigkeit eine einheitliche Anwendung der NIS-RL erleichtert werden.[413]

Die Verwaltungsstrukturen in Österreich hätten grundsätzlich beide Varianten ermöglicht. Ein dezentraler Ansatz durch Zuständigkeiten der Regulierungsbehörde Energie-Control Austria für die

---

[408] Zum Unterschied siehe auch *Adamovich et al.*, Österreichisches Staatsrecht, Rz 47.010, 47.11.

[409] *Barfuß*, Ressortzuständigkeit und Vollzugsklausel, Eine verfassungs- und verwaltungsrechtliche Untersuchung zur Zuständigkeit der Bundesminister, S. 7.

[410] ENISA, Stocktaking, Analysis and Recommendations on the protection of CIIs, https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis , abgerufen am 09.09.2018.

[411] Siehe auch COM(2009) 149, 30.3.2009, bestätigt durch die Entschließung des Rates 2009/C 321/01, sowie die Mitteilung COM(2011) 163, bestätigt durch die Schlussfolgerungen des Rates 10299/11.

[412] Dezentraler Ansatz wird beispielsweise in Schweden verfolgt.

[413] Zentraler Ansatz wird beispielsweise in Frankreich verfolgt.

Regulierung der Elektrizitäts- und Erdgaswirtschaft (E-Control)[414] im Sektor Energie, die Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)[415] für Digitale Infrastrukturen sowie der jeweiligen Fachministerien in den Sektoren Gesundheit, Verkehr, Wasser und Finanzen hätte Vorteile in Bezug auf bereits bestehende Regulierungsaufgaben in anderen Bereichen der jeweiligen Sektoren, andererseits jedoch den entscheidenden Nachteil mit sich gebracht, das Expertise zur Netz- und Informationssystemsicherheit in all diesen Organisationen aufgebaut hätte werden müssen und eine einheitliche Vorgehensweise nur sehr schwer umsetzbar gewesen wäre.

Die zentrale Variante war insofern naheliegend, als im Bundeskanzleramt und im Bundesministerium für Inneres bereits Organisationseinheiten zur Cybersicherheit eingerichtet waren[416] und deren Aufgaben lediglich um jene in Umsetzung des NIS-Gesetzes erweitert werden mussten.

7.2.2. Aufgaben des Bundeskanzlers

Dem Bundeskanzler kommen in Vollziehung des NIS-Gesetzes so genannte strategische Aufgaben zu (§ 4 Abs. 1 NISG). Darunter fallen unter anderem die Koordination der Erstellung einer Strategie (§ 4 Abs. 1 Z 1), die Vertretung von Österreich in EU-weiten und internationalen Gremien (Z 2), die generelle Koordination der öffentlich-privaten Zusammenarbeit im Bereich der Sicherheit von Netz- und Informationssystemen (Z 3) und weitere taxativ aufgezählte Aufgaben. Wesentlich erscheinen die Verordnungsermächtigungen in Abs. 2 zur Festlegung von Kriterien für die Parameter der Erheblichkeit einer Störung von Netz- und Informationssystemen (§ 4 Abs. 2 Z 1), zur näheren Regelungen zur Ermittlung von Betreibern wesentlicher Dienste (Z 2), von Sicherheitsvorkehrungen (Z 3) sowie von Ausnahmen von Verpflichtungen für Betreiber wesentlicher Dienste (Z 4).

Die in § 4 zugewiesenen Aufgaben scheinen mit dem generellen Wirkungsbereich des Bundeskanzleramts nach dem BMG, nämlich den Angelegenheiten der strategischen Netz- und Informationssicherheit[417] in Übereinstimmung.

Die Erstellung einer Strategie und eines jährlichen Berichtes zur Sicherheit von Netz- und Informationssystemen (§ 4 Abs. 1 Z 1) erfolgte bereits vor Umsetzung der NIS-RL in Form der

[414] Energie-Control-Gesetz – E-ControlG, siehe dazu auch Kapitel 7.1.1 zu nationalen Zuständigkeiten im Bereich der Energieversorgung.
[415] Bundesgesetz über die Einrichtung einer Kommunikationsbehörde Austria („KommAustria“) (KommAustria-Gesetz – KOG), BGBl. I Nr. 32/2001 idF BGBl. I Nr. 78/2018.
[416] Siehe dazu Kapitel 3.2.1.
[417] Anlage zu § 2 BMG, Teil 2, A, Ziffer 1.

Österreichischen Strategie für Cybersicherheit[418] und des darauf basierenden Berichtes. Diese Strategie soll anhand der Vorgaben der NIS-RL entsprechend weiterentwickelt werden.[419]

Die einzelnen Aufgaben des Bundeskanzlers werden nachfolgend in den Ausführungen zu den jeweiligen Bestimmungen näher beleuchtet (siehe ab Kapitel 7.3).

7.2.3. Aufgaben des Bundesministers für Inneres

Dem Bundesminister für Inneres kommen in der nationalen Rechtsordnung bereits zahlreiche Aufgaben zu, die einen sehr engen Bezug zu jenen des NIS-Gesetzes aufweisen. Dabei ist beispielsweise auf die Aufgabe des Schutzes kritischer Infrastruktur im Rahmen des Sicherheitspolizeigesetzes[420] sowie die Aufgabe der operativen Koordinierungsstelle für Meldungen über jede Form von Angriffen auf Computersysteme im Rahmen des Polizeilichen Staatsschutzgesetzes[421] zu verweisen.

Ihm kommen eine Vielzahl von koordinierenden, operativen und vorbeugenden Aufgaben zu, die von der organisatorischen Leitung der Koordinierungsstrukturen IKDOK (Innerer Kreis der operativen Koordinierungsstrukturen) und OpKoord (Operative Koordinierungsstrukturen), dem Betrieb einer Meldesammelstelle, der Weitergabe von relevanten Informationen sowie der Überprüfung der Sicherheitsvorkehrungen und der Einhaltung der Meldepflicht reichen.

Ebenso wie bei den Aufgaben des Bundeskanzlers ist zu untersuchen, ob sich dieses breite Aufgabenspektrum mit den zugewiesenen Zuständigkeiten im Rahmen des BMG deckt bzw. mit diesen vereinbar ist.[422] Dazu zählen beispielsweise Angelegenheiten des Sicherheitswesens, sofern sie keinem anderen Ministerium zugewiesen sind, sowie Angelegenheiten des staatlichen Krisenmanagements.[423] Wie bereits in Kapitel 7.1.1 (Kompetenzdeckungsklausel) näher ausgeführt, fällt die Vollziehung des NIS-Gesetzes nicht nur unter den Kompetenztatbestand des Art. 10 B-VG (Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit), sondern stellt eine sogenannte Querschnittsmaterie dar. Dementsprechend dürften dem Bundesministerium für Inneres im Rahmen seiner Zuständigkeiten nach dem BMG lediglich die Angelegenheiten der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit sowie des staatlichen Krisenmanagements im Zusammenhang mit der Netz- und Informationssystemsicherheit zukommen.

---

[418] Siehe Kapitel 3.2.
[419] EB RV NIS-Gesetz, S. 6.
[420] Siehe dazu Kapitel 4.2.2.
[421] Siehe dazu Kapitel 4.2.3.
[422] Siehe dazu Bundeskanzleramt-Verfassungsdienst, Bundesministeriengesetz 1973; Gestaltung von Vollzugsklauseln in Gesetzen, GZ 52.938-2c/74, 1974.
[423] Siehe dazu Kapitel 4.2.1.

Die im Rahmen des § 5 NISG dem Bundesminister für Inneres zugewiesenen Aufgaben gehen jedoch weit darüber hinaus. Sowohl der Betrieb der zentralen Anlaufstelle (Single Point of Contact - SPoC) für die Sicherheit von Netz- und Informationssystemen (§ 5 Abs. 1 Z 1 NISG) als auch die organisatorische Leitung der Koordinierungsstrukturen (§ 5 Abs. 1 Z 2) fällt wohl eher unter die dem Bundeskanzler nach dem BMG zugewiesenen Aufgabe der strategischen Netz- und Informationssicherheit bzw. unter Angelegenheiten der Koordination der gesamten Verwaltung des Bundes[424] als unter die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit. Dementsprechend hätten diese Aufgaben dem BMG entsprechend gesetzlich beim Bundeskanzler verankert werden sollen.

Bei den Aufgaben der Entgegennahme und Analyse von Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle und der Erstellung des Lagebildes (§ 5 Abs. 1 Z 3) als auch bei der Erstellung Weitergabe von relevanten Informationen zur Vorbeugung von Sicherheitsvorfällen (§ 5 Abs. 1 Z 4) und der Überprüfung der Sicherheitsvorkehrungen und der Einhaltung der Meldepflichten (§ 5 Abs. 1 Z 5) wird dagegen von einem engeren und begründbaren Zusammenhang mit dem Sicherheitswesen auszugehen sein. Die Aufgabenerfüllung durch den Bundesminister für Inneres entspricht damit der grundlegenden Aufgabenverteilung des BMG.

7.2.4. Zentrale Anlaufstelle

Die NIS-RL sieht die Einrichtung einer zentralen Anlaufstelle (SPoC) vor (Art. 8 Abs. 3), um dadurch die grenzüberschreitende Zusammenarbeit und Kommunikation zu erleichtern und die effektive Umsetzung der Richtlinie zu ermöglichen.[425] Diese zentrale Anlaufstelle wird in Österreich beim Bundesminister für Inneres eingerichtet und als operative Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit den zuständigen Stellen in anderen Mitgliedstaaten sowie der Kooperationsgruppe[426] und dem CSIRT-Netzwerk dienen (§ 6 Abs. 1).

Letztere Aufgabe, nämlich die Zusammenarbeit des Bundesministers für Inneres (als zentraler Anlaufstelle) mit der Kooperationsgruppe und dem CSIRTs-Netzwerk, erscheint hinsichtlich der sonstigen damit in Zusammenhang stehenden Aufgaben zumindest fragwürdig. Die Vertretung Österreichs in der Kooperationsgruppe (sowie in anderen EU-weiten und internationalen Gremien

[424] Anlage zu § 2 BMG, Teil 2, A, Ziffer 1.
[425] ErwGr 31 NIS-RL.
[426] Die Kooperationsgruppe aus Vertretern der Mitgliedstaaten, der Kommission und der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) soll auf der Grundlage der beträchtlichen Fortschritte, die im Rahmen des Europäischen Forums der Mitgliedstaaten zur Förderung von Gesprächen und des Austauschs bewährter Vorgehensweisen, unter anderem zur Entwicklung von Grundsätzen für die europäische Zusammenarbeit bei Cyberkrisen, erzielt worden sind, eingerichtet werden – siehe ErwGr 4 NIS-RL.

betreffend Netz- und Informationssystemsicherheit) ist (auch) eine Aufgabe des Bundeskanzlers (§ 4 Abs. 1 Z 2).

Eine eindeutige Trennung der Art bzw. Inhalte der Zusammenarbeit kann anhand der grundsätzlichen Aufgaben der betroffenen Stellen erfolgen, wenngleich dies in der praktischen Umsetzung schwierig zu gestalten sein wird. Die Zusammenarbeit des Bundeskanzlers mit der Kooperationsgruppe kann in Bezug auf die dem Bundeskanzler zugewiesenen Aufgaben erfolgen, wie beispielsweise zur österreichischen Strategie für Cybersicherheit (§ 4 Abs. 1 Z 1) bzw. der Cybersicherheitsstrategie der Europäischen Union, dem jährlichen Bericht zur Sicherheit von Netz- und Informationssystemen (§ 4 Abs. 1 Z 1), zur Festlegung von Kriterien zur Feststellung der Erheblichkeit eines Sicherheitsvorfalles (§ 4 Abs. 2 Z 1), zur Festlegung von Sicherheitsvorkehrungen (§ 4 Abs. 2 Z 3) sowie zur Ermittlung von Betreibern wesentlicher Dienste und der Erstellung/laufenden Aktualisierung einer Liste von wesentlichen Diensten (§ 4 Abs. 1 Z 6) und zur Konsultation mit den zuständigen Behörden anderer Mitgliedstaaten im Sinne des § 4 Abs. 1 Z 7.

Die Zusammenarbeit des Bundesministers für Inneres als zentrale Anlaufstelle mit der Kooperationsgruppe kann sich lediglich auf zusammenfassende Berichte (samt Informationen über die Anzahl der eingegangenen Meldungen, Angaben über die Art der gemeldeten Sicherheitsvorfälle, wie zum Beispiel die Arten der Sicherheitsverletzungen, deren Schwere und Dauer etc.) beziehen[427], die im Rahmen der grenzüberschreitenden Zusammenarbeit der Kooperationsgruppe – zum Zwecke der wirksamen Information der Mitgliedstaaten und der Europäischen Kommission – vorgelegt werden (Art. 10 NIS-RL).[428]

Für die Vorlage dieses Berichtes der zentralen Anlaufstelle an die Kooperationsgruppe findet sich im NIS-Gesetz jedoch keine passende Bestimmung. Was konkret nun die Aufgabe des Bundesministers für Inneres als zentraler Anlaufstelle in Zusammenarbeit mit der Kooperationsgruppe sein soll, bleibt unbeantwortet.[429]

Anderl/Heußler/Mayer/Müller sehen auch die Abgrenzung in der Zusammenarbeit der zentralen Anlaufstelle mit dem CSIRTs-Netzwerk schwierig, da diese eigentlich als Aufgaben den Computer-Notfallteams zukommt (§ 14 Abs. 2 Z 6).[430] Im Rahmen dessen sollen die Computer-Notfallteams den Bundeskanzler sowie den Bundesminister für Inneres über Aktivitäten des CSIRTs-Netzwerks informieren, womit im Grunde ihnen die Aufgabe der operativen Verbindungsstelle zukommt.

[427] *Anderl et al.*, NISG::Kommentar, § 6, Rz 3.
[428] ErwGr 33 NIS-RL.
[429] So auch *Anderl et al.*, NISG::Kommentar, § 6, Rz 3.
[430] *Anderl et al.*, NISG::Kommentar, § 6, Rz 4.

Wiederum sei nicht zu erkennen, welche Aufgabe hier für den Bundesminister für Inneres als zentraler Anlaufstelle verbleibt.

Die Wahrnehmung der zentralen Anlaufstelle durch den Bundeskanzler wäre mE die bessere Lösung gewesen, weil dieser die Aufgabe hat, Österreich in EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen zu vertreten (§ 4 Abs. 1 Z 2 NISG).

7.2.5. Koordinierungsstrukturen

Die Bedeutung der Kooperation, Koordination und Kommunikation hat insbesondere im Zeitalter der Cybersicherheit zugenommen.[431] In diesem Zusammenhang ist einerseits eine enge Kooperation zwischen den verschiedenen nationalen, für Cybersicherheit zuständigen öffentlich-rechtlichen Organisationen sowie mit privatwirtschaftlichen Akteuren relevant.[432] Zu diesem Zweck institutionalisiert das NIS-Gesetz zwei verschiedene Koordinierungsstrukturen, die oben genannten Zielen Rechnung tragen sollen und die beide vom Bundesminister für Inneres organisatorisch geleitet werden (§ 5 Abs. 1 Z 1).

Zum einen wird der Innere Kreis der Operativen Koordinierungsstrukturen (IKDOK) eingerichtet, der eine interministerielle Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen darstellt, bestehend aus Vertretern des Bundeskanzlers, des Bundesministers für Inneres, des Bundesministers für Landesverteidigung und des Bundesministers für Europa, Integration und Äußeres (§ 3 Z 4). Aufgaben dieses IKDOK sind die Erörterung und Aktualisierung des Lagebildes[433], die Erörterung der Erkenntnisse, die gemäß § 13 Abs. 1 und 2 (technische Einrichtungen) gewonnen wurden und die Unterstützung des Koordinationsausschusses im Cyberkrisenmanagement (§ 7 Abs. 1).

Eine Einbeziehung des Bundesministers für Landesverteidigung und des Bundesministers für Europa, Integration und Äußeres findet sich in der Vollziehung des NISG ansonsten lediglich im Koordinationsausschuss (§ 25), darüber hinaus sind keine weiteren Aufgaben dieser beiden Organe vorgesehen. Sinnvoll erscheint dies jedoch allemal, als Sicherheitsvorfälle im Rahmen des NIS-Gesetzes sich zu einem Fall der Cyberverteidigung entwickeln können und die Cyberdiplomatie[434] im Fall internationaler Sicherheitsvorfälle unverzichtbar sein kann.[435]

---

[431] *Klimburg*, Strategie und Sicherheit, 2012, S. 463 ff.
[432] Dieser Ansatz wird in Deutschland mit der so genannten Allianz für Cyber-Sicherheit verfolgt, siehe dazu *Klett/Ammann*, Computer und Recht, 2014, S. 94.
[433] Zur Bedeutung eines Lagebildes siehe auch *Skopik/Fiedler/Lendl*, Cyber Attack Information Sharing, Datenschutz und Datensicherheit - DuD, 4/2014, S. 252.
[434] EB RV NIS-Gesetz, S. 9.
[435] *Anderl et al.*, NISG::Kommentar, § 7, Rz 2.

Darüber hinaus wäre mE auch die Einbeziehung des Bundesministers für Digitalisierung und Wirtschaftsstandort anzudenken, da dieser für Angelegenheiten der Digitalisierung einschließlich der staatlichen Verwaltung für das Service und die Interaktion mit Bürgern und Unternehmen verantwortlich zeichnet.[436]

Der IKDOK soll auch dem Austausch klassifizierter Informationen zwischen den Teilnehmern dienen (§ 7 Abs. 1 letzter Satz). Der Zugang zu klassifizierten Informationen darf nach den Bestimmungen der dies regelnden Geheimschutzordnung des Bundes (GehSO)[437] Bediensteten des Bundes nur gewährt werden, wenn dies für die Erfüllung der dienstlichen Aufgaben erforderlich ist und (bei Vorliegen gewisser Klassifizierungsstufen) eine Sicherheitsüberprüfung gemäß Sicherheitspolizeigesetz oder eine Verlässlichkeitsprüfung gemäß Militärbefugnisgesetz durchgeführt wurde (§ 6 Abs. 1 GehSO). Diese Sicherheitsüberprüfung ist im NIS-Gesetz als Voraussetzung für die Teilnahme am IKDOK vorgesehen (§ 3 Z 4 NISG).

Zur Erleichterung der Organisation des IKDOK und zur Wahrnehmung der sonstigen Aufgaben kann der Bundesminister für Inneres eine IKT-Lösung betreiben, die den anderen IKDOK-Teilnehmern bereitzustellen ist (§ 12 Abs. 1 NISG), wobei unter anderem personenbezogene Daten von Teilnehmern, die zur Ermöglichung und im Zuge der Teilnahme an den Koordinierungsstrukturen zu organisatorischen Zwecken erforderlich sind, verarbeitet werden (§ 9 Abs. 2 Z 1).

Neben dem IKDOK als Plattform der behördlichen Zusammenarbeit wird die Operative Koordinierungsstruktur (OpKoord), eine Struktur zur Koordination auf der operativen Ebene im Bereich der Sicherheit von Netz- und Informationssystemen, eingerichtet (§ 7 Abs. 2 NISG). Die OpKoord besteht aus den oben dargestellten Teilnehmern des IKDOK und den Computer-Notfallteams (§ 3 Z. 5). Zweck der Einrichtung dieser etwas größeren Plattform ist die Erörterung eines gesamtheitlichen Lagebildes, welches auch die Meldungen über Risiken und Vorfälle enthält, die unmittelbar und vollständig nur in den Computer-Notfallteams eingehen (§ 14 Abs. 2 Z 1).[438] Die OpKoord kann auch um Vertreter von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste sowie Einrichtungen der öffentlichen Verwaltung erweitert werden, wenn diese von einem Risiko, Vorfall oder Sicherheitsvorfall betroffen sind (§ 7 Abs. 2).

[436] Anlage zu § 2 BMG, Teil 2, F, Ziffer 26.
[437] Geheimschutzordnung des Bundes – GehSO auf Grund des § 12 BMG 1986, BGBl. Nr. 76 idF BGBl. I Nr. 6/2007.
[438] Zur Notwendigkeit des regen Austauschs sicherheitsrelevanter Informationen zwischen Unternehmen und dem Staat zur Entstehung eines Cyber-Lagebildes siehe *Einzinger/Skopik*, Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken, Datenschutz und Datensicherheit - DuD, 09/2017, S. 573.

7.3. Abschnitt 3 – Befugnisse

7.3.1. Betrieb von IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen (§ 13)

Dem Bundesminister für Inneres obliegt die Aufgabe der Erstellung und Weitergabe von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Sicherheitsvorfällen (§ 5 Abs. 1 Z 4 NISG). Diese Informationen kommen einerseits aus Erkenntnissen von gemeldeten Risiken, Vorfällen oder Sicherheitsvorfällen, sowohl nationalen als auch über die zentrale Anlaufstelle eingehenden aus anderen Mitgliedstaaten (§ 6).

Darüber hinaus kann der Bundesminister für Inneres zu diesem Zweck IKT-Lösungen betreiben, um Risiken oder Vorfälle frühzeitig zu erkennen (§ 13 Abs. 1 erster Satz). Für die Erkennung von Sicherheitsvorfällen werden diese Lösungen nicht benötigt, da selbige alleine aufgrund deren Definition (§ 3 Z 6) und der damit einhergehenden Auswirkungen auf die Gesellschaft erkannt werden. Die Aufgabe der IKT-Lösungen geht über den Richtlinientext hinaus, die einen Betrieb solcher IKT-Lösungen nicht vorsieht. Aus diesem Grund soll diese Bestimmung nur oberflächlich beleuchtet werden.

Die frühzeitige Erkennung soll dem Zweck dienen, etwaige Störungen bzw. wichtige Informationen zu deren Vermeidung so früh wie möglich und proaktiv[439] anderen Betreibern, Anbietern oder Einrichtungen zur Verfügung zu stellen. Denn auch wenn eine Störung von Netz- und Informationssystemen oft nicht gänzlich verhindert werden kann, ist es wichtig, den Zeitraum zwischen der Durchführung und der Erkennung eines Angriffes möglichst gering zu halten.[440]

Sucht man in der österreichischen Rechtsordnung den Begriff der IKT-Lösung, findet man diesen im IKT-Konsolidierungsgesetz definiert.[441] Demnach wird hierbei die Gesamtheit aller informationstechnologischen Maßnahmen und technischen Mittel verstanden, die erforderlich sind, um Nutzern Funktionen und Informationen automationsunterstützt zur Verfügung zu stellen.[442]

§ 13 NISG unterscheidet beim Betrieb von IKT-Lösungen zwischen dem so genannten IOC-basierten Frühwarnsystem bzw. Sensornetzwerk[443] (Abs. 1), Honeypots (Abs. 2, 1. Halbsatz Teil 1) sowie Sinkholes (Abs. 2, 1. Halbsatz Teil 2).

---

[439] EB RV NISG, S. 14.
[440] *Einzinger/Skopik/Fiedler*, Datenschutz und Datensicherheit - DuD, 2015, S. 723.
[441] Bundesgesetz, mit dem IKT-Lösungen und IT-Verfahren bundesweit konsolidiert werden (IKT-Konsolidierungsgesetz – IKTKonG), BGBl. I Nr. 35/2012 idF BGBl. I Nr. 104/2018.
[442] EB RV NIS-Gesetz, S. 13.
[443] *Anderl et al.*, NISG::Kommentar, § 13, Rz 4.

IOC-basiertes Frühwarnsystem (Abs. 1)

Betreiber, Anbieter sowie Einrichtungen der öffentlichen Verwaltung können an diesen vom Bundesminister für Inneres betriebenen IKT-Lösungen teilnehmen und dabei festlegen, welche Daten dabei an den Bundesminister übermittelt werden (§ 13 Abs. 1 zweiter Satz).

Da im Gesetz nur sehr unzureichend definiert, muss zur genaueren Beschreibung dieser IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen ein Blick in die Erläuternden Bemerkungen geworfen werden. Dabei soll es sich um technische Einrichtungen[444] handeln, die konfiguriert und (physisch) vor den Netzwerken der Teilnehmer platziert werden und dadurch Angriffe, das Vorgehen des Angreifers im Netz des Teilnehmers und seine Kommunikation mit Schadsoftware erkennen können.[445]

Anderl/Heußler/Mayer/Müller verstehen darunter einzelne Sensoren, die bei Betreibern, Anbietern sowie Einrichtungen des Bundes auf freiwilliger Basis eingesetzt werden. Das Netzwerk dieser Sensoren („Sensornetzwerk") ermögliche es, aktuelle Bedrohungsmuster zu erkennen und jeweils allen Sensoren zur Verfügung zu stellen, sodass Angriffe frühestmöglich erkannt und dementsprechend verhindert werden.[446] Dieser Interpretation hinsichtlich des grundsätzlichen technischen Aufbaus und Zwecks kann trotz der unbestimmten Formulierung in § 13 Abs. 1 mE gefolgt werden, wenngleich inhaltliche Fragen – wie weiter unten angeführt – noch offen bleiben.

Die nähere Beschreibung in den Erläuternden Bemerkungen lässt erkennen, dass die einzelne IKT-Lösung zwar vom Bundesminister für Inneres konfiguriert und betrieben, durch (freiwillige)[447] Teilnahme eines Betreibers wesentlicher Dienste[448] jedoch vor dessen Netzwerk platziert wird. Dabei sollen mittels Vertrag zwischen dem Bundesminister und dem teilnehmenden Betreiber wesentlicher Dienste die Teilnahmemodalitäten, wie insbesondere die Örtlichkeit der Anbringung der technischen Einrichtung sowie die Bestimmung, welche Daten übermittelt werden, geregelt werden.[449]

---

[444] Die Wirkungsorientierte Folgenabschätzung (WFA) zum NIS-Gesetz geht vom Einsatz zweier technischer Einrichtungen (und somit teilnehmenden Betreibern) für 2019, fünf Einrichtungen 2020 und vier Einrichtungen 2021 aus, wobei die Kosten pro technischer Einrichtung mit EUR 40.000 veranschlagt werden.
[445] EB RV NIS-Gesetz, S. 14.
[446] *Anderl et al.*, NISG::Kommentar, § 13 Rz 2.
[447] EB RV NIS-Gesetz, S. 14.
[448] Es kann sich auch um einen Anbieter digitaler Dienste oder eine Einrichtung der öffentlichen Verwaltung handeln, wobei in weiterer Folge zur einfacheren Lesbarkeit immer vom Betreiber ausgegangen wird.
[449] EB RV NIS-Gesetz, S. 14.

Grundsätzlich ist der Bundesminister für Inneres berechtigt, technische Daten[450] von Personen, die im Rahmen des § 13 (Betrieb von IKT-Lösungen) ermittelt wurden, zu verarbeiten (§ 9 Abs. 5 Z 3). Dies geschieht nach den Erläuternden Bemerkungen in einem Dateisystem („Threat Intelligence"), in der Informationen zu aktuellen Bedrohungen aufbereitet werden. Erkennungsmuster dieser Bedrohungen („Indicator of Compromise - IOC")[451] werden darüber hinaus über technische Schnittstellen an die technischen Einrichtungen übermittelt werden. Diese gleichen die beim teilnehmenden Betreiber wesentlicher Dienste aus- und eingehenden Datenströme[452] mit diesen Erkennungsmustern ab und sollen somit automatisch Angriffe erkennen.[453] Eine Befugnis zur Datenübermittlung ist dafür mE nicht erforderlich, da die Übermittlung vom Bundesminister für Inneres eben nicht an den Betreiber wesentlicher Dienste, sondern an die (auch) vom Bundesminister betriebene technische Einrichtung erfolgt.

Fraglich ist in diesem Zusammenhang jedoch der Abgleich dieser in der vom Bundesminister für Inneres betriebenen technischen Einrichtung verarbeiteten Erkennungsmuster mit dem ein- und ausgehenden Datenverkehr des Teilnehmers. Zu untersuchen ist dabei, ob es im Rahmen des Abgleichs zu einer Übermittlung durch den Betreiber wesentlicher Dienste und (wenn auch nur sehr kurzfristigen) Verarbeitung (auch) personenbezogener Daten durch den Bundesminister für Inneres in dieser technischen Einrichtung kommt, um einen solchen Abgleich überhaupt erst durchführen zu können.

Das Verarbeiten personenbezogener Daten ist denkbar weit definiert und umfasst jegliche Handhabung personenbezogener Daten, beginnend mit ihrer Erhebung, über das Ordnen, Verändern, Auswerten, Abfragen, Verwenden, Übermitteln und Gespeichert-Halten bis hin zum Löschen oder Vernichten.[454] *Anderl/Heußler/Mayer/Müller* sehen im Abgleich einen Vergleich der Bedrohungsmuster (IOCs) mit den Meta-Daten des Ein- und ausgehenden Datenstroms (insb. IP-Adresse des Absenders und Empfängers)[455], womit es theoretisch durch die kurzfristige

[450] Um welche Daten es sich dabei handeln kann, wird in den Erläuternden Bemerkungen näher beschrieben. Je nach vertraglicher Vereinbarung zwischen dem Bundesminister für Inneres und der betroffenen Einrichtung zählen darunter insbesondere technische personenbezogene Daten wie IP-Adressen zugreifender Systeme oder Personen, Ports (Adresskomponenten für die Kommunikation, um Datenpakete einer Anwendung zuzuordnen) und Log-Files (Protokollierung von Programmabläufen oder Zugriffen auf eine bestimmte Ressource).

[451] Zur Notwendigkeit des Austausches von IOCs zur Erkennung von Angriffen siehe auch *Einzinger/Skopik/Fiedler*, Datenschutz und Datensicherheit - DuD, 2015, S. 723.

[452] Zum technischen Prozess einer Datenübertragung siehe *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet (2016), S. 16f.

[453] EB RV NIS-Gesetz, S. 14.

[454] Siehe auch *Feiler/Forgó*, EU-DSGVO (2017), S. 3.

[455] *Anderl et al.*, NISG::Kommentar, § 13, Rz 7.

Verarbeitung dieser Meta-Daten zu einer Verarbeitung personenbezogener Daten kommen könnte.[456]

Die Erläuternden Bemerkungen[457] nennen zu den Daten, die bei solchen IKT-Lösungen ermittelt werden, technische personenbezogene Daten wie beispielsweise Hashes[458] (Prüfziffern für die Erkennung von Schadsoftware), womit subsumiert werden könnte, dass es lediglich zum Vergleich von Hash-Werten (und nicht der unverschlüsselten Meta-Daten selbst) kommen könnte. Da jedoch sowohl das Gesetz als auch die Erläuternden Bemerkungen dazu nichts Näheres festlegen, werden diese Fragen meines Erachtens in den vertraglichen Vereinbarungen zwischen Bundesminister für Inneres und dem jeweiligen Teilnehmer zu regeln sein und hier nicht abschließend beantwortet werden können.

§ 13 sieht für die Teilnahme von Betreibern, Anbietern oder Einrichtungen an den IKT-Lösungen als Ersatz einen Pauschalbetrag vor, der mit Verordnung des Bundesministers für Inneres festgelegt werden soll (§ 13 Abs. 1 letzter Satz). *Ander/Heußler/Mayer/*Müller erkennen hier richtig, dass es sich aufgrund der Freiwilligkeit der Teilnahme bei diesem Frühwarnsystem um keine Inpflichtnahme privater Unternehmen wie bei der Einrichtung zur Überwachung des Fernmeldeverkehrs handelt.[459]

Im Falle einer Alarmierung aufgrund der Übereinstimmung eines in der IKT-Lösung verarbeiteten IOCs mit einem Teil des ein- oder ausgehenden Datenstroms ist eine Weiterleitung an den Bundesminister für Inneres zur Analyse und Bewertung sowie Aufnahme in die Threat Intelligence und Verarbeitung im Lagebildprozess des IKDOK vorgesehen.[460] Bei einer solchen Weiterleitung kann es durchaus zum Entstehen eines Anfangsverdachtes (§ 1 Abs. 3 StPO) und somit zum Entstehen einer Ermittlungsverpflichtung im Rahmen der Amtswegigkeit (§ 2 Abs. 1) kommen.[461]

Dies kann meines Erachtens dazu führen, dass Unternehmen davor zurückschrecken könnten, an den IKT-Lösungen teilzunehmen, da sie befürchten müssen, ohne eigenen Einfluss einer Vielzahl von Ermittlungsverfahren (und möglicherweise einem damit einhergehenden Reputationsverlust bei Bekanntwerden) ausgesetzt zu sein.

---

[456] § 9 Abs. 5 Z 3 ermächtigt den Bundesminister für Inneres zur Verarbeitung technischer Daten von Personen, die im Rahmen des § 13 ermittelt wurden.
[457] EB RV NIS-Gesetz, S. 11.
[458] Zu Hash-Werten von Rufnummern als personenbezogene Daten im Sinne der DSGVO siehe *Voitel*, Sind Hash-Werte personenbezogene Daten?, Datenschutz und Datensicherheit - DuD, 11/2017.
[459] *Anderl et al.*, NISG::Kommentar, § 13, Rz 5.
[460] *Anderl et al.*, NISG::Kommentar, Rz 9.
[461] Mehr zum Entstehen eines Anfangsverdachtes und zur Ermittlungspflicht siehe Kapitel 7.5.9.

Honeypots und Sinkholes

Der Bundesminister für Inneres ist neben dem Betrieb des IOC-basierten Frühwarnsystems (§ 13 Abs. 1) zudem berechtigt, IKT-Lösungen zu betreiben und zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen.

Unter „Honeypots" werden nach den Erläuternden Bemerkungen vermeintlich verwundbare Systeme bzw. Systemteile verstanden, die in ihrer primären Anwendungsform im Internet verfügbar sind. Sie sind dabei nicht real verwundbar, sondern zeichnen Angriffsversuche lediglich auf und geben dem Angreifer dadurch das Gefühl, einen erfolgreichen Angriff durchgeführt zu haben. Ihre primäre Aufgabe liegt darin, die Vorgehensweise von Angreifern zu analysieren sowie die angewandten Angriffsmethoden zu erkennen.[462]

Bei solchen Angriffsversuchen muss es sich nicht immer um gezielte Angriffe auf das jeweilige System, sondern kann es sich häufig auch um so genannte Portscans handeln. Diese dienen dem Aufspüren von Sicherheitslücken und es soll dabei in Erfahrung gebracht werden, welche Dienste auf einem Rechnersystem aktiv und erreichbar sind. [463]

Zu diskutieren ist in diesem Zusammenhang die mögliche Einstufung von Honeypots als Verleitung zur Begehung von strafbaren Handlungen. Personen dürfen nach den Bestimmungen der Strafprozessordnung[464] nicht zur Unternehmung, Fortsetzung oder Vollendung einer Straftat verleitet werden (§ 5 Abs. 3 StPO). Das so genannte Lockspitzelverbot verbietet jede Verleitung zu Straftaten, umgekehrt ist es im Strafverfahren der öffentlichen Hand nicht schlechthin verboten, dem Beschuldigten eine Falle zu stellen.[465]

Nach *Wiederin* ist Verleiten mehr, als eine Gelegenheit zu schaffen. „Für eine Tatprovokation reicht es nicht hin, eine Leiter bereitzustellen, um einem Dieb sein Geschäft zu erleichtern. Ebenso wenig genügt es, ein Auto mit eingelegtem Zündschlüssel vor ihm abzustellen oder ihn durch eine halboffene Tasche zu reizen."[466] Auch der OGH sieht eine rechtswidrige Einflussnahme nur, „wenn eine über eine bloß passive Ermittlungstätigkeit hinausgehende Einflussnahme auf das kriminelle

[462] EB RV NIS-Gesetz, S. 15. Zur näheren Definition und Beschreibung siehe auch *Chovancová/Ádám/Baláz et al.*, Securing Distributed Computer Systems Using An Advanced Sophisticated Hybrid Honeypot Technology, Computing and Informatics, 1/2017, S. 114, *Guizani/Rayes/Khan et al.*, Network Modeling and Simulation, A Practical Perspective (2010), S. 45 ff.
[463] Zur Beschreibung von Portscans siehe *Vogelgesang/Möllers/Potel*, Auf der Jagd nach Schwachstellen - Eine strafrechtliche Bewertung von Portscans, Datenschutz und Datensicherheit - DuD, 8/2017.
[464] Strafprozeßordnung 1975 (StPO), BGBl. Nr. 631/1975 idF BGBl. I Nr. 70/2018.
[465] *Wiederin*, § 5, in Fuchs /Ratz (Hrsg), Wiener Kommentar zur Strafprozessordnung (2013), Rz 110.
[466] *Wiederin* in Fuchs /Ratz, Wiener Kommentar zur Strafprozessordnung, Rz 116.

Verhalten im Sinne einer Anstiftung erfolgt."[467] Diesen Ausführungen folgend ist mE auch das Bereitstellen von verwundbaren Systemen im Netz alleine nicht ausreichend, um eine Verleitung zu einer Straftat gem. § 5 Abs. 3 StPO zu begründen.

§ 13 Abs. 2 spricht neben dem Betrieb von IKT-Lösungen (in Form von Honeypots, wie oben dargestellt) auch von der Nutzung dieser Lösungen nach Einwilligung der betroffenen Einrichtung. Die Erläuternden Bemerkungen definieren diese Einrichtungen als so genannte „Sinkholes". Dies sind Maßnahmen, die dahingehend Abhilfe schaffen, dass sie den Datenverkehr zwischen infizierten netzwerkfähigen Geräten und so genannten Command and Control Servern[468] analysieren. Sie haben somit die Möglichkeit, Botnetze entsprechend zu untersuchen und die Kommunikation zwischen infizierten Geräten und Command and Control Servern so einzuschränken, dass kein Schaden verursacht werden kann.[469]

Anderl/Heußler/Mayer/Müller sehen die Umsetzung in der Umleitung von Zugriffen infizierter Rechner auf schädliche Command and Control Server auf ein Sinkhole, welches entweder vom Bundesminister für Inneres selbst betrieben oder bei einer Domain-Registrierungsstelle genutzt werden kann.[470] Auch hier ist – wie im Fall der Honeypots weiter oben – der Gesetzestext so offen formuliert, sodass daraus keine weiteren (rechtlichen) Erkenntnisse ableitbar sind. Darüber hinaus wird es mE auch hier vertraglicher Vereinbarungen zwischen dem Bundesminister für Inneres und jenen Betreibern bedürfen, deren IKT-Lösungen genutzt werden.

7.3.2. Das Determinierungsgebot (Art. 18 B-VG) im Zusammenhang mit dem Betrieb von IKT-Lösungen

Da die Formulierung des „Betriebs von IKT-Lösungen" gem. § 13 Abs. 1 und 2 NISG m Gesetzestext sehr unbestimmt erscheint, soll in diesem Zusammenhang die ausreichend konkrete Determinierung dieser Regelung im Sinne des Art. 18 B-VG untersucht werden.[471] Der Grundgedanke des Legalitätsprinzips im Zusammenwirken mit dem Gedanken der Gewaltenteilung ist die Zuordnung von Gesetzgebungs- und Vollziehungsfunktionen an unterschiedliche (und damit getrennte) Organe.[472] Der Gesetzgeber muss das Verwaltungshandeln in einem solchen Maß

[467] OGH 14.12.1999, 11 OS 86/99.
[468] Zur Rolle von Command-Control-Servern und ihrer zentralen Rolle bei der Bekämpfung von Botnetzen siehe *Einzinger/Skopik/Fiedler*, Datenschutz und Datensicherheit - DuD, 2015, S. 723f.
[469] EB RV NISG, S. 15.
[470] Zur Beschreibung von Sinkholes siehe *Anderl et al.*, NISG::Kommentar, § 13, Rz 15.
[471] Gesetze, die das Handeln der Vollziehung nur ungenügend determinieren, sind gem. Art 18 B-VG verfassungswidrig. Man spricht in diesem Zusammenhang von einer „formalgesetzlichen Delegation", weil unbestimmte Gesetze die Vollziehung nur scheinbar binden, siehe *Berka*, Verfassungsrecht, Rz 495.
[472] *Eberhard*, Das Legalitätsprinzip im Spannungsfeld von Gemeinschaftsrecht und nationalem Recht, Zeitschrift für öffentliches Recht (ZÖR), 1/2008, S. 83.

determinieren, dass die wesentlichen Voraussetzungen und Inhalte des behördlichen Handelns aus dem Gesetz ersichtlich sind.[473]

Die in der Literatur vorbereitete und vom VfGH ab den 1950'er Jahren entwickelte Judikatur[474] zum „differenzierten Legalitätsprinzip"[475] besagt, dass die Intensität der gebotenen Determinierung nicht immer dieselbe ist.[476] Danach bestimmt der Regelungsgegenstand die verfassungsrechtlich gebotene Regelungsdichte auf einfachgesetzlicher Ebene.[477] Angesichts der unterschiedlichen Lebensgebiete, Sachverhalte und Rechtsfolgen, die Gegenstand und Inhalt gesetzlicher Regelung sein können, ist ganz allgemein davon auszugehen, dass Art. 18 B-VG einen dem jeweiligen Regelungsgegenstand adäquaten Determinierungsgrad verlangt.[478] Aus der Konzeption des B-VG ergibt sich nach der Judikatur des VfGH[479] und der Lehre[480], dass sich der Bestimmtheitsmaßstab des Gesetzes anhand verschiedener Faktoren nach den einzelnen Sachgebieten und der Eingriffsnähe der Regelung, dem Rechtsschutzbedürfnis oder den eingesetzten Handlungsformen der Verwaltung abstufen lässt („differenziertes Legalitätsprinzip").[481]

Soweit Gesetze beispielsweise in den Schutzbereich von Grundrechten eingreifen („eingriffsnahe Gesetze")[482], müssen die Eingriffstatbestände über das in Art. 18 Abs. 1 B-VG festgelegte Maß der

[473] Zu regeln sind das zuständige Organ, das einzuhaltende Verfahren und vor allem der Inhalt der von der Behörde zu treffenden Entscheidung, siehe *Berka*, Verfassungsrecht, Rz 500.

[474] Siehe dazu ua. VfSlg 2768/1954, 3027/1956, 8203/1977, 8813/1980, 10.275 und 10.313/1984, 10.737/1985, 11.455/1987, 12.133/1989, 12.679/1991, 13.785/1994, 14.850/1997, 15.177/1998, 15.888/2000.

[475] Zum differenzierten Legalitätsprinzip siehe *Novak*, Das "differenzierte Legalitätsprinzip" in der verfassungsgerichtlichen Rechtsprechung, in Funk /Adamovich (Hrsg), Staatsrecht und Staatswissenschaften in Zeiten des Wandels (1992). Dazu auch *Wimmer*, Materiales Verfassungsverständnis: ein Beitrag zur Theorie der Verfassungsinterpretation (1971), S. 116ff.

[476] *Arnold*, Rechtsstaat, demokratische Legitimation und Effizienz: Funktionen und Garanten eines sachgerecht flexiblen Legalitätsprinzips, in Arnold/Bundschuh-Rieseneder et al. (Hrsg), Recht, Politik, Wirtschaft, Dynamische Perspektiven (2008), S. 13.

[477] *Bachmann/Baumgartner/Feik et al.*, Besonderes Verwaltungsrecht[8] (2010).

[478] Vgl. etwa VfSlg. 13.785/1994.

[479] VfSlg 13.449/1993; 15.811/2000 ua. Siehe dazu auch *Novak* in Funk /Adamovich, Staatsrecht und Staatswissenschaften in Zeiten des Wandels, S. 494 ff.

[480] *Öhlinger*, Verfassungsrecht[7. Auflage] (2007), Rz 583 ff. *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11], Rz 570 f.

[481] Laut *Eberhard* steht dahinter die Überlegung, dass sich das Maß an inhaltlicher Determinierung des Verwaltungshandelns an der Stärke der Mitwirkung des vom entsprechenden Rechtsakt betroffenen Adressaten richtet und daher bei konsensualen Rechtsformen – wie dem hoheitlichen Vertrag – geringer sein kann - siehe *Eberhard*, Zeitschrift für öffentliches Recht (ZÖR), 2008, S. 88.

[482] Die Abhängigkeit des Determinierungsgrades von der Eingriffsnähe einer gesetzlichen Regelung ist in der Natur des Art. 18 B-VG enthalten, siehe *Arnold* in Arnold/Bundschuh-Rieseneder et al., Recht, Politik, Wirtschaft, Dynamische Perspektiven, S. 21.

Determinierung hinaus besonders genau umschrieben werden.[483] Dies gilt beispielsweise auch bei der Regelung von Straftatbeständen[484] und bei der Begründung behördlicher Zuständigkeiten[485].

Abgeschwächte Bestimmtheitserfordernisse bestehen insbesondere bei Regelungen künftiger, sich dynamisch entwickelnder Sachverhalte[486], bei der Vorgabe von im Wesentlichen technischen Standards und anderen Normierungen, beim schlichthoheitlichen Verwaltungshandeln und der inneren Organisation von Verwaltungsbehörden[487]. Im Gegenzug verlangt der VfGH im Rahmen der „finalen Determinierung" jedoch, dass der Regelung des Verfahrens besondere Aufmerksamkeit geschenkt wird („Legitimation durch Verfahren"). [488]

Im Hinblick auf die Formulierung des Betriebs von IKT-Lösungen ist festzustellen, dass nach dem Gesetzeswortlaut nicht eindeutig erkennbar ist, worum es sich bei diesen Einrichtungen handelt. Daran ändert auch die Legaldefinition der IKT-Lösungen im IKT-Konsolidierungsgesetz (siehe dazu Kapitel 7.3.1) nichts, die von der Gesamtheit aller informationstechnologischen Maßnahmen und technischen Mittel spricht, die erforderlich sind, um Nutzern Funktionen und Informationen automationsunterstützt zur Verfügung zu stellen. Grundsätzlich darf der Gesetzgeber unbestimmte Gesetzesbegriffe verwenden, wenn sich nur unter Ausschöpfung aller Interpretationsmethoden noch ein ausreichend bestimmter Regelungsgehalt ableiten lässt.[489] Bei unbestimmten Gesetzesbegriffen können auch Beispiele diese näher determinieren[490], wie dies in den Erläuternden Bemerkungen zum NIS-Gesetz der Fall ist.

Für ein abgeschwächtes Erfordernis der Bestimmtheit der Regelung spricht die dynamische Entwicklung von IKT-Lösungen, die zur Zielerreichung erforderlich sein können. Es kann wohl kaum vom Gesetzgeber verlangt werden, konkrete Lösungen zu nennen, die sich regelmäßig fortentwickeln und einer regelmäßigen gesetzlichen Anpassung bedürfen würden. Im Hinblick auf die somit zumindest geforderte Legitimität des Verfahrens hätte der Gesetzgeber jedoch umso mehr die konkreten Verfahrensbestimmungen regeln müssen, da – wie oben beschrieben – kaum Hinweise auf die datenschutzrechtliche Verarbeitung und insbesondere diesbezügliche Eingriffe zu finden sind.

---

[483] *Giese*, Sicherheitspolizeirecht, in Bachmann/Baumgartner et al. (Hrsg), Besonderes Verwaltungsrecht (2010), S. 10. siehe auch VfSlg 10.737/1985, 11.455/1987, 13.336/1993.
[484] VfSlg 14.153/1995, VfGH 25.09.2002, B 110/02 ua.
[485] VfSlg 13.021/1992, 13.816/1994.
[486] VfSlg 8280/1978, 14.041/1995, 17.345/2004.
[487] *Berka*, Verfassungsrecht, Rz 508.
[488] *Lienbacher*, Raumordnungsrecht, in Bachmann/Baumgartner et al. (Hrsg), Besonderes Verwaltungsrecht (2010), S. 443.
[489] VfSlg 11.499/1987, 13.785/1994, 15.447/1999.
[490] VfSlg 14.380/1995.

Darüber hinaus ist auch von einigermaßen eingriffsintensiven Maßnahmen auszugehen. Wenngleich Betreiber wesentlicher Dienste gem. Abs. 1 freiwillig an diesen IKT-Lösungen teilnehmen können, besteht keine Rechtssicherheit zu den Daten, die damit verarbeitet werden. Ebenso ist in Abs. 2 vom Betrieb von IKT-Lösungen durch den Bundesminister für Inneres zur Mustererkennung die Rede. Gerade im Hinblick auf die aktuelle Sensibilität von Eingriffen in Datenschutzrechte wäre hier mE eine konkrete Bestimmtheit verfassungsrechtlich vorgesehen.

Da somit einerseits aufgrund der datenschutzrechtlichen Problematik eingriffsintensive Regelungen vorliegen und darüber hinaus auch bei Verneinung dieser keine ausreichende verfahrensrechtliche Bestimmtheit (Legitimation durch Verfahren“) gegeben erscheint, widerspricht § 13 NISG mE dem Determinierungsgebot des Art. 18 B-VG.

7.4. Abschnitt 4 - Computer-Notfallteams

7.4.1. Aufgaben und Zweck der Computer-Notfallteams

7.4.1.1. Vorgaben der NIS-RL und aktuelle Situation in Österreich

Die NIS-RL sieht vor, dass jeder Mitgliedstaat ein oder mehrere CSIRTs (Computer-Notfallteams) benennen soll, die die vorgegebenen Anforderungen erfüllen und mindestens die in Anhang II der Richtlinie genannten Sektoren und die in Anhang III genannten Dienste abdecken (Art. 9). Sie sind dabei für die Bewältigung von Risiken und Vorfällen nach einem genau festgelegten Ablauf zuständig. Ziel ist, dass die Mitgliedstaaten über angemessene technische und organisatorische Fähigkeiten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen und auf Unionsebene effizient zusammenarbeiten können, insbesondere im Rahmen des CSIRTs-Netzwerks. [491]

Empfehlungen zur Einrichtung von Computer-Notfallteams gab es auf EU-Ebene bereits in vorhergehenden Strategien oder Mitteilungen. Die EU forderte die Mitgliedstaaten unter anderem 2009 im Rahmen der Strategie zum Schutz kritischer Informationsinfrastrukturen auf, nationale/staatliche Computer-Notfallteams einzurichten, die über gemeinsame Grundfähigkeiten

[491] ErwGr 34 NIS-RL.

verfügen.[492] Auch die Digitale Agenda für Europa aus 2010 sieht ein weit gespanntes Netz von Computer-Notfallteams in Europa vor.[493]

Dass die zunehmende Bedrohung aus dem Cyber-Raum die Bedeutung der Computer-Notfallteams hebt, zeigt die Anzahl der bei FIRST[494] akkreditierten CERTs. Waren es im Jahr 2007 erst 170 Mitglieder, sind es mittlerweile weltweit mehr als 300.[495] Bis vor kurzem wurden Computer-Notfallteams (deutscher Begriff zu Computer Emergency Response Teams – CSIRTs bzw. CERTs)[496] überwiegend privatrechtlich geführt[497], wobei dieser Ansatz in Österreich weiterhin verfolgt wird. Jedoch verschwimmt auch hier zunehmend die Grenze zwischen öffentlicher Gewalt und privaten Akteuren. [498]

Rechtlich problematisch war zum Inkrafttreten des NIS-Gesetzes, dass CERTs ursprünglich aus der Praxis zur Unterstützung bei IT-Sicherheitsvorfällen entstanden und ein rechtlicher Rahmen bisher unbestimmt[499] bzw. kaum vorhanden war.

In Österreich haben sich in den letzten Jahren verschiedenste Arten von Computer-Notfallteams etabliert[500], deren Aufgaben und Zuständigkeiten durch das NIS-Gesetz rechtlich verankert wurden.

Eine Definition des Computer-Notfallteams bzw. CERTs ist in der Österreichischen Strategie für Cybersicherheit (ÖSCS)[501] zu finden. Demnach ist Computer Emergency Response Team die Bezeichnung eines Notfallteams, das bei Sicherheitsvorfällen zur Abwehr und Wiederherstellung von IKT-Systemen bereitgehalten wird.[502]

Dabei ist insbesondere auf die Konstellation des Government Computer Emergency Response Team (GovCERT) in Verbindung mit dem (bisherigen) nationalen Computer-Notfallteam (CERT.at) zu achten. Das GovCERT ist organisatorisch im Bundeskanzleramt angesiedelt und steht in enger Verbindung (man könnte laut *Einzinger/Skopik/Fiedler* von einer Public Private Partnership

[492] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Writschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen, COM(2009) 149 final, S. 7.
[493] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Writschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine Digitale Agenda für Europa, COM(2010)245 final, S. 20.
[494] Forum of Incident Response and Security Teams (FIRST).
[495] *Huber/Helllwig/Quirchmayr*, Datenschutz und Datensicherheit - DuD, 2016, S. 163.
[496] Zur synonymen Verwendung der Begriff CERT und CSIRT siehe Kapitel 3.2.1.
[497] *Einzinger/Skopik*, Datenschutz und Datensicherheit - DuD, 2017, S. 572.
[498] *Bendiek*, SWP, 2012, S. 13.
[499] Tschohl et al., "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs," S. 1.
[500] *Huber*, Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation, S. 12.
[501] mehr dazu siehe Kapitel 3.2.
[502] *Bundeskanzleramt*, Österreichische Strategie für Cybersicherheit, 2013, S. 20.

sprechen) mit CERT.at, welches von der österreichischen Domain-Registrierungs-Gesellschaft nic.at und in Personal- und Arbeitsunion mit GovCERT betrieben wird. [503] CERT.at versteht sich dabei selbst als nationales CERT[504] und kann bei Sicherheitsvorfällen bereits bisher koordinierend und beratend aktiv werden.[505] Daneben existieren in Österreich CERTs in einzelnen Unternehmen (beispielsweise A1 Telekom oder Raiffeisen Informatik).[506]

7.4.1.2. Einrichtung von Computer-Notfallteams

Das NIS-Gesetz sieht die Einrichtung mehrerer Computer-Notfallteams vor. Einerseits sollen das nationale Computer-Notfallteam und sektorenspezifische Computer-Notfallteams Betreiber wesentlicher Dienste und Anbieter digitaler Dienste bei der Bewältigung von Risiken, Vorfällen und Sicherheitsvorfällen unterstützen (§ 14 Abs. 1 NISG). Für die Einrichtungen der öffentlichen Verwaltung erfüllt das Computer-Notfallteam der öffentlichen Verwaltung (GovCERT) diese Aufgabe. Das GovCERT (als Teil des Bundeskanzleramtes[507]) ist somit das einzige Computer-Notfallteam, welches konkret im NIS-Gesetz benannt bzw. mit seinen Aufgaben betraut wird.

Dies trifft auf das CERT.at, welches de facto seit Jahren die Aufgaben eines nationalen Computer-Notfallteams wahrnimmt, nicht zu. Denn die Eignung des nationalen Computer-Notfallteams als auch jene der sektorenspezifischen Computer-Notfallteams werden erst durch Bescheid des Bundeskanzlers im Einvernehmen mit dem Bundesminister für Inneres festgestellt (§ 15 Abs. 3). Das Gesetz spricht gar von einer Ermächtigung zur Aufgabenerfüllung (§ 15 Abs. 3) – was dies konkret hinsichtlich einer möglichen Beleihung bedeutet, ist in Kapitel 7.4.1.4 näher erläutert.

Unverständlich ist hier die Unterscheidung des Gesetzgebers, warum lediglich bei sektorenspezifischen Computer-Notfallteams ein Antrag[508] dem konstitutiven[509] Bescheid vorangehen muss, wohingegen dem Gesetzeswortlaut nach diese Feststellung beim nationalen Computer-Notfallteam ohne vorhergehenden Antrag stattfindet.[510] Womöglich hatte der

[503] *Einzinger/Skopik/Fiedler*, Datenschutz und Datensicherheit - DuD, 2015, S. 724.
[504] Zur eigenen Sichtweise von CERT.at als nationale Drehscheibe siehe *Huber/Helllwig/Quirchmayr*, Datenschutz und Datensicherheit - DuD, 2016, S. 163.
[505] *Hellwig*, Organisation, Rahmenbedingungen und Kommunikation bei CERTs, in Huber (Hrsg), Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation (2015), S. 23.
[506] Mehr zu den bisherigen nationalen Strukturen siehe Kapitel 3.2.1.
[507] § 14 Abs. 4 erster Satz NISG.
[508] Diesen Antrag hat jene Organisation zu stellen, welche die Aufgaben des Computer-Notfallteams wahrnehmen möchte.
[509] Siehe EB RV NIS-Gesetz, S. 17.
[510] Gem. § 15 Abs. 3 hat der Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres festzustellen, dass das nationale Computer-Notfallteam sowie über Antrag ein sektorenspezifisches Computer-Notfallteam die Anforderungen gemäß Abs. 1 erfüllen und geeignet sind, die Aufgaben gemäß § 14 Abs. 2 wahrzunehmen.

Gesetzgeber in diesem Fall das bereits bestehende CERT.at vor Augen und sieht vor, dass der Bundeskanzler lediglich die Eignung dieser bestehenden Einrichtung feststellen soll. Diese Konstruktion erscheint mehr als fragwürdig. ME hätte der Gesetzgeber CERT.at entweder konkret mit den Aufgaben des nationalen Computer-Notfallteams betrauen oder einen Antrag auch anderer Institutionen für diese Aufgabe vorsehen sollen.

Sowohl nach den Erläuternden Bemerkungen[511] als auch nach Ansicht *Anderl/Heußler/Mayer/Müller* dient das GovCERT als so genanntes „Auffang-CERT", falls ein nationales Computer-Notfallteam noch nicht eingerichtet sein sollte oder Betreiber wesentlicher Dienste das sektorenspezifische Computer-Notfallteam nicht unterstützen.

Diese Interpretation lässt sich mE nicht nachvollziehen. Gem. § 14 Abs. 1 NISG kommt dem Computer-Notfallteam der öffentlichen Verwaltung nur die Unterstützung von Einrichtungen der öffentlichen Verwaltung zu, eine Ausnahmeregelung dazu für den Fall des Nichtbestehens eines nationalen Computer-Notfallteams ist nicht zu finden. Aus diesem Grund wäre aufgrund der fehlenden Zuständigkeit und Aufgabe im Hinblick auf Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beispielsweise keine Verarbeitung personenbezogener Daten (§ 14 Abs. 7) zulässig, da dies nur für die Erfüllung der gem. Abs. 2 vorgesehenen Aufgaben gilt.

Darüber hinaus erscheint nicht ausreichend geregelt, an wen Betreiber wesentlicher Dienste Sicherheitsvorfälle melden sollen, sofern sie das sektorenspezifische Computer-Notfallteam nicht unterstützen. Dies ergibt sich mE lediglich aus einer systematischen Interpretation, da generell ein nationales Computer-Notfallteam eingerichtet wird und Betreiber für ihren Sektor ein sektorenspezifisches Computer-Notfallteam einrichten können, welches die Aufgaben gegenüber jenen Betreibern wahrnehmen, die es unterstützen (§ 14 Abs. 3). Aus dieser Formulierung geht jedoch nicht eindeutig hervor, dass die Betreiber in Fällen der Nichtunterstützung Meldungen an das nationale Computer-Notfallteam zu richten haben. Da sich an das Nichtmelden eines Sicherheitsvorfalles an das „für sie zuständige Computer-Notfallteam" (so die Formulierung in § 19 NISG (Meldepflicht)) verwaltungsstrafrechtliche Sanktionen knüpfen (§ 26 NISG), erscheint die Determinierung zur Zuständigkeit der Computer-Notfallteams im Lichte der Argumentation in Kapitel 7.3.2 (Das Determinierungsgebot (Art. 18 B-VG) im Zusammenhang mit dem Betrieb von IKT-Lösungen) unbestimmt. Aufgrund der doch einigermaßen schlüssigen möglichen Interpretation anhand der übrigen Gesetzesbestimmungen ist eine Verfassungswidrigkeit gem. Art. 18 B-VG jedoch mE nicht gegeben.

[511] EB RV NIS-Gesetz, S. 16.

Überlegenswert wäre meiner Meinung nach auch die Einrichtung des nationalen Computer-Notfallteams im Bundeskanzleramt (und damit eine Verbindung mit dem GovCERT) oder im Bundesministerium für Inneres gewesen. Gem. Art. 9 Abs. 1 NIS-RL kann ein CSIRT nämlich auch innerhalb einer zuständigen Behörde eingerichtet werden. Für die Einrichtung im Bundeskanzleramt hätte gesprochen, dass diesem nach den Bestimmungen des Bundesministeriengesetzes[512] die Koordination in Angelegenheiten der Telekommunikation, Informationstechnologien und Medien obliegt und eine gemeinsame Einrichtung mit dem GovCERT – auch aufgrund der bereits bestehenden Public Private Partnership zwischen diesen beiden Organisationen (siehe oben) – sinnvoll erschienen wäre.

Eine aufgrund der bereits bestehenden nationalen Rechtslage ebenso sinnvolle Lösung wäre die Einrichtung des nationalen Computer-Notfallteams im Bundesministerium für Inneres gewesen. [513] Den Sicherheitsbehörden obliegt gem. § 22 Abs. 1 Z 6 SPG bereits jetzt der vorbeugende Schutz von kritischen Infrastrukturen, worunter auch deren Netz- und Informationssysteme subsumiert werden können.[514] Insbesondere aufgrund der Einrichtung der operativ zuständigen Behörde beim Bundesminister für Inneres (§ 5) hätte eine gleichzeitige Einrichtung des nationalen Computer-Notfallteams bei dieser Behörde für große Synergien[515] und eine Vereinfachung der Meldewege gesorgt.[516]

Neben dem nationalen Computer-Notfallteam und dem GovCERT ist auch die Einrichtung sektorenspezifischer Computer-Notfallteams vorgesehen. Dem dadurch entstehenden Nachteil, dass nicht alle Vorfälle beim nationalen Computer-Notfallteam eingehen und somit dort gesammelt werden, stehen mehrere und meines Erachtens schwerer wiegende Vorteile gegenüber.

Einerseits hat die Praxis gezeigt, dass ein spezifisches Hintergrundwissen einen konkreten Sektor und die dort verwendeten Systeme betreffend für ein besseres Situationsbewusstsein und eine realistischere Lagebildbeurteilung wesentlich ist.[517] Darüber hinaus ist damit zu rechnen, dass sich die IT-Sicherheitsverantwortlichen bei den Betreibern und die Angestellten des sektorenspezifischen Computer-Notfallteams nach einiger Zeit der Zusammenarbeit persönlich

[512] Mehr dazu siehe Kapitel 4.2.1 sowie 7.2.1.
[513] Diese Möglichkeit wird auch angesprochen in *Einzinger/Skopik/Fiedler*, Datenschutz und Datensicherheit - DuD, 2015, S. 724
[514] Mehr zu dieser Aufgabe siehe Kapitel 4.2.2.
[515] Den Sicherheitsbehörden werden beispielsweise Auskunftsermächtigungen gegenüber Betreibern öffentlicher Telekommunikationsdienste und sonstigen Dienstanbietern gemäß E-Commerce Gesetz gewährt (SPG § 53 Abs. 3a).
[516] Gem. § 14 Abs. 2 Z 2 NISG hat das Computer-Notfallteam alle Meldungen über Sicherheitsvorfälle an den Bundesminister für Inneres weiterzuleiten.
[517] *Anderl et al.*, NISG::Kommentar, § 14, Rz 37.

kennen und Vertrauen erwiesenermaßen die wichtigste Voraussetzung für eine gute Kooperation darstellt.[518]

Als erstes und bisher einziges sektorenspezifisches Computer-Notfallteam wurde bisher das Austrian Energy CERT (AEC)[519] eingerichtet. Für alle anderen Sektoren, für die noch kein solches Computer-Notfallteam existiert, fallen die Aufgaben dem nationalen Computer-Notfallteam zu (§ 19 Abs. 2 NISG).

In diesem Zusammenhang ist auf die Anforderung für diese Notfallteams zu verweisen, einen Nachweis über die Unterstützung von Betreibern wesentlicher Dienste zu erbringen (§ 15 Abs. 1 Z 3). Demgemäß ist eine solche Unterstützung nur dann nachzuweisen, wenn es sich um ein Computer-Notfallteam gemäß § 14 Abs. 1 zweiter Satz handelt. In diesem zweiten Satz sind sowohl das nationale Computer-Notfallteam, als auch das sektorenspezifische und jenes der öffentlichen Verwaltung (GovCERT) aufgelistet.

Für das GovCERT sieht § 15 Abs. 2 („das GovCERT hat die Anforderungen mit Ausnahme von Z 3 zu erfüllen“) eine Ausnahme vor, nicht jedoch für das nationale Computer-Notfallteam (im Gegensatz dazu sprechen *Anderl/Heußler/Mayer/Müller* auch nur für die Notwendigkeit der Erbringung des Nachweises durch das sektorenspezifische Notfallteam[520] - dieser Ansicht ist nicht zu folgen).[521] Dementsprechend müsste letzteres einen Nachweis über die Unterstützung der Betreiber aller Sektoren erbringen, was wohl nicht Interesse des Gesetzgebers lag. Vielmehr wollte dieser die Unterstützung der Betreiber für das jeweils für sie zuständige sektorenspezifische Notfallteam erheben, nicht jedoch für das ohnedies für alle Betreiber zuständige nationale Computer-Notfallteam.

Für den von (zumindest) den sektorenspezifischen Computer-Notfallteams zu erbringenden Nachweis ist keine besondere Form vorgesehen, in der Praxis kann es sich dabei um eine Liste von Unterstützungserklärungen der Betreiber des Sektors handeln.[522] Offen lässt der Gesetzgeber dabei, von wie vielen Betreibern im Sektor das betroffene Notfallteam eine Unterstützung nachweisen muss. Ein Hinweis in den Erläuternden Bemerkungen sieht eine Unterstützung von zumindest zwei Betreibern vor, sofern im Sektor mehr als ein Betreiber wesentlicher Dienste

[518] Tschohl et al., "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs," S. 5. Zur Notwendigkeit der Vertrauensbasis siehe auch Kapitel 7.5.9 (Freiwillige Meldungen).
[519] *Anderl et al.*, NISG::Kommentar, § 14, Rz 37.
[520] *Anderl et al.*, NISG::Kommentar, § 15, Rz 4.
[521] § 15 Abs. 1 Z 3 sieht vor, dass ein Nachweis über die Unterstützung von Betreibern vorliegen muss, wenn es sich um ein Computer-Notfallteam gem. § 14 Abs. 1 zweiter Satz handelt. § 14 Abs. 1 zweiter Satz spricht jedoch sowohl vom nationalen als auch von den sektorenspezifischen Computer-Notfallteams.
[522] *Anderl et al.*, NISG::Kommentar, Rz 51.

identifiziert wurde.[523] Ebenso sehen die Erläuternden Bemerkungen vor, dass im Einzelfall zu beurteilen sein wird, ob die Unterstützung aus einem Sektor (bezogen auf die Anzahl der in diesem Sektor ermittelten Betreiber) ausreichend ist. Darauf, dass jene Betreiber eines Sektors, welche die Unterstützung verweigern, dem nationalen Computer-Notfallteam zugewiesen sind und Meldungen an dieses zu richten haben, wurde bereits weiter oben eingegangen.

Ob es sich um 10 %, 50 % oder um 90 % der Betreiber handeln muss, bleibt offen. Da es in einem Sektor stets nur ein sektorenspezifisches Computer-Notfallteam geben kann[524], wäre beispielsweise die Situation denkbar, dass kurz nach Inkrafttreten des Gesetzes ein sektorenspezifisches Notfallteam mit zwei Unterstützungserklärungen einen Antrag auf Feststellung seiner Eignung für diesen Sektor stellt und der Bundeskanzler diese Eignung mangels Alternativen (und trotz Vorliegens von lediglich zwei Unterstützungen) feststellt. Sofern einige Monate später eine andere Organisation für genau diesen Sektor die Feststellung seiner Eignung beantragt und die Unterstützung von mehr als diesen zwei Unterstützungserklärungen nachweist, müsste der Bundeskanzler dem bereits bestehenden Notfallteam möglicherweise die Eignung aberkennen und dem neuen Notfallteam zusprechen.

Wie schwierig diese gesamte Konstruktion ist, zeigt auch der Umstand, dass die sektorenspezifischen Computer-Notfallteams ihre Aufgaben nur für jene Betreiber wahrnehmen, die dieses unterstützen (siehe § 14 Abs. 3 1. Satz), da speziell in sicherheitsrelevanten Bereichen Vertrauen für den Wissens- und Informationsaustausch essentiell ist.[525] Soweit ein Betreiber ein sektorenspezifisches Computer-Notfallteam nicht unterstützt (bspw. weil dieses bei einem Konkurrenzunternehmen eingerichtet wurde oder eine sehr gute Kooperation mit einem solchen pflegt), fallen die Aufgaben für diesen Betreiber dem nationalen Computer-Notfallteam zu.[526] Durch diese womöglich in der Praxis entstehende Zersplitterung von Aufgaben (einerseits ist das nationale Computer-Notfallteam für einige Unternehmen aus einem Sektor zuständig, andererseits ein sektorenspezifisches Computer-Notfallteam) kann es zu unübersichtlichen Meldeflüssen und Lagebildern kommen.

Die gesamte Organisation der Computer-Notfallteams erscheint aus den nun genannten Gründen absurd und zur Zielerreichung nicht zweckmäßig. Denn wozu werden sektorenspezifische Computer-Notfallteams eingerichtet, wenn schlussendlich wieder jeder Betreiber selbst entscheiden kann, an welches Notfallteam er sich wendet. Das eigentliche Ziel der Erstellung

[523] EB RV NIS-Gesetz, S. 17.
[524] *Anderl et al.*, NISG::Kommentar, § 14, Rz 36.
[525] *Huber/Pospisil*, Wissensmanagement und Kommunikation bei CERTs, in Huber (Hrsg), Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation (2015), S. 110.
[526] *Anderl et al.*, NISG::Kommentar, § 14, Rz 36.

sektorenspezifischer Lagebilder und einheitlicher Meldeflüsse kann mit dieser Regelung jedenfalls nicht erreicht werden.

Aus diesem Grund ist zu untersuchen, ob die Regelung möglicherweise dem Sachlichkeitsgebot des Art. 7 B-VG widerspricht.[527] Nach Judikatur des VfGH ist es dem Sachlichkeitsgebot zufolge dem Gesetzgeber verwehrt, sachlich nicht begründbare Regelungen zu treffen.[528] Darunter sind jene Regelungen zu verstehen, denen kein adäquater Sinn zukommt, weil sie der Sachlogik und Vernunft entbehren.[529] Im Rahmen des Sachlichkeitsgebotes wird der Gleichheitssatz des Art. 7 B-VG nicht nur auf Gleich- und Ungleichbehandlungen angewendet; er wird auch herangezogen, um Regelungen für sich genommen als unsachlich zu verwerfen, ohne dass ein Vergleich mit anderen Regelungen gezogen wird.[530] Diese Erweiterung des VfGH wird in der Lehre durchaus kritisch gesehen, da der Anwendungsbereich des Art. 7 B-VG zu weit und nicht im ursprünglichen Sinne des Gleichheitsgrundsatzes ausgedehnt werde und der Umfang der Gesetzesprüfungskompetenz beträchtlich erweitert werde.[531]

Der VfGH betont in seiner Judikatur, dass der Gesetzgeber im Rahmen des Sachlichkeitsgebotes in der Wahl seiner Ziele und Mittel grundsätzlich frei sei. Ob eine Regelung zweckmäßig bzw. ob sie der optimale Weg zur Zielerreichung ist, habe der VfGH nicht zu beurteilen.[532] Der Gesetzgeber verletze das Sachlichkeitsgebot aber etwa dann, wenn er zur Zielerreichung völlig untaugliche Mittel einsetzt.[533]

Wenngleich die Regelungen zu den Computer-Notfallteams nicht stimmig erscheinen und wohl nicht der optimale Weg zur Zielerreichung sind, ist ein Verstoß gegen Art. 7 B-VG nicht erkennbar. Die dafür erforderliche „völlige Untauglichkeit“ und „Unsachlichkeit“ liegt mE nicht vor, da das System grundsätzlich funktionsfähig erscheint und wahrscheinlich lediglich einzelne Betreiber nicht systemkonform inkludiert sein werden.

---

[527] *Arnold* in Arnold/Bundschuh-Rieseneder et al., Recht, Politik, Wirtschaft, Dynamische Perspektiven, S. 11.
[528] so bspw VfSlg 11.369/1987 unter Hinweis auf VfSlg 8457/1978, 10064/1984, 10.084/1984; VfSlg 12.227/1989, 13.557/1993, 13.743/1994, 14.301/1995, 15.031/1997 ua.
[529] *Arnold* in Arnold/Bundschuh-Rieseneder et al., Recht, Politik, Wirtschaft, Dynamische Perspektiven, S. 11.
[530] *Pöschl*, Probleme des Gleichheitssatzes aus österreichischer Sicht, in Merten /Papier (Hrsg), Grundfragen der Grundrechtsdogmatik (2007), S. 109.
[531] Kritisch vor allem *Öhlinger*, Verfassungsrecht[7. Auflage], S. 336., *Pöschl* in Merten /Papier, Grundfragen der Grundrechtsdogmatik, S. 108f. Mit der Argumentation, dass beim Sachlichkeitsgebot trotzdem immer ein Vergleich von Regelungen stattfindet *Holoubek*, Die Sachlichkeitsprüfung des allgemeinen Gleichheitsgrundsatzes, ÖZW, 1991, S. 80 sowie *Hiebaum*, Gleichheit und Sachlichkeit, Zeitschrift für öffentliches Recht, 3/2009, S. 258ff.
[532] VfSlg 6541/1971, 7885/1976, 11.369/1987, 12.227/1989, 12.416/1990, 13.558/1993, 14.301/1995, 15.031/1997, 16.582/2002; VfGH 4.10.2006, G 9605.
[533] VfSlg 8457/1978, 11.369/1987, 12.227/1989, 12.486/1990, 16.582/2002.

7.4.1.3. Aufgaben der Computer-Notfallteams

Bei den Aufgaben von Computer-Notfallteams wird im Wesentlichen zwischen reaktiven (insbesondere Behandlung von Vorfällen) und proaktiven (bspw. Aussendung von Warnungen) Dienstleistungen sowie Qualitätsmanagement (unter anderem Schulungen) unterschieden. In welchem Ausmaß Dienstleistungen abgedeckt werden[534], hängt immer von der Größe, der Zielsetzung und den Anforderungen ab, die zu erfüllen sind.[535]

Die NIS-RL legt in ihrem Anhang I unter anderem die Mindestaufgaben der Computer-Notfallteams fest, die in der nationalen Umsetzung in § 14 Abs. 2 NISG zu finden sind. Dabei kommt den Computer-Notfallteams unter anderem die Entgegennahme von Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle und die Weiterleitung dieser Meldungen an den Bundesminister für Inneres zu (§ 14 Abs. 2 Z 1 und 2). Jedoch sind nicht alle dieser Meldungen in gleicher Weise weiterzuleiten. Wo Sicherheitsvorfälle (§ 19) sogleich weiterzuleiten sind, hat dies für freiwillige Meldungen (§ 23) nur in zusammengefasster Form zu erfolgen – diese Klarstellung ergibt sich aber erst aus den §§ 19 und 23 und nicht bereits eindeutig aus § 14 Abs. 2 Z 2.

Eine weitere Aufgabe der Computer-Notfallteams besteht in der Ausgabe von Frühwarnungen, Alarmmeldungen und Handlungsempfehlungen sowie Bekanntmachung und Verbreitung von Informationen über Risiken, Vorfälle oder Sicherheitsvorfälle (§ 14 Abs. 2 Z 3). Wie auch bereits bei den Aufgaben des Bundesministers für Inneres (§ 5 Abs. 1) diskutiert[536], ist die Abgrenzung zu diesen offen. Diesem obliegt nämlich die Erstellung und Weitergabe von zur Gewährleistung der Sicherheit von Netz- und Informationssystemen relevanten Informationen zur Vorbeugung von Sicherheitsvorfällen (§ 5 Abs. 1 Z 4).

Den Erläuternden Bemerkungen nach sind dies beispielsweise Warnungen oder Handlungsempfehlungen, die im Vorhinein weitergegeben werden können.[537] Anhand einer systematischen Interpretation könnte man bei den Alarmmeldungen und Handlungsempfehlungen des Computer-Notfallteams von solchen mit rein technischem Inhalt, bei jenen des Bundesministers für Inneres von allgemeiner Sensibilisierung und organisatorischen Empfehlungen

[534] Die ENISA beschreibt in ihrer Studie „Baseline Capabilities of National/Governmental CERTs: Updated Recommendations 2012“ die Minimalanforderungen, die ein nationales/Government-CERT erfüllen sollte. Siehe dazu *Hellwig* in Huber, Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation, S. 29.
[535] *Hellwig* in Huber, Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation, S. 28.
[536] Siehe Kapitel 7.2.3.
[537] EB RV NISG, S. 8.

ausgehen. In der praktischen Umsetzung wird es dabei mE höchstwahrscheinlich jedoch zu Doppelgleisigkeiten und Schwierigkeiten in der Abstimmung von Zuständigkeiten kommen.

Eine weitere Aufgabe der Computer-Notfallteams ist die erste allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall. Den Erläuternden Bemerkungen nach zu urteilen handelt es sich dabei um konkrete Handlungsanweisungen und Informationen, um den aktuellen Sicherheitsvorfall abzuwehren und die negativen Auswirkungen möglichst gering zu halten. Nur in Ausnahmefällen sollen Computer-Notfallteams auch vor Ort eine technische Unterstützung leisten, worauf die betroffene Einrichtung keinen Rechtsanspruch habe.[538]

Anderl/Heußler/Mayer/Müller begründen dies durch die begrenzten Ressourcen der Notfallteams.[539] Auch das Referenzdokument der Kooperationsgruppe spricht bei der technischen Unterstützung von relevanten Informationen zur effektiven Vorfallsbehebung, sofern die Umstände es erlauben.[540] Es kann sich dabei meines Erachtens aber nicht um die unmittelbare Abwehr einer Gefahr (bei der Gefahrenquelle) (§§ 21 ff SPG) oder um die Sicherung von Beweisen (§§ 98ff StPO) handeln, da dies Aufgaben der Sicherheitsbehörden bzw. der Kriminalpolizei sind.

Anzumerken ist dabei, dass auch der Bundesminister für Inneres nicht für eine reine technische Unterstützungsleistung vor Ort zuständig ist. Diesem kommen im Rahmen seiner Aufgaben und Befugnisse lediglich die Gefahrenabwehr (nach den Bestimmungen des SPG) sowie die strafprozessuale Ermittlung (nach den Bestimmungen der StPO) zu. Somit kann es nach einem erfolgten Angriff jedenfalls zur Sicherstellung von Daten vor Ort beim Betreiber kommen (StPO).

Die Gefahrenabwehr ist in diesem Fall komplexer zu sehen, da diese theoretisch auch dadurch erfolgen könnte, beim Betreiber vor Ort (gemeinsam mit dem Unternehmen) die IT-Systeme abzusichern und somit technisch zu unterstützen. Zur Frage eines möglichen „Gegenangriffs“ siehe Kapitel 7.6.2. (Mögliche Reaktion auf eine Cyberkrise). Eine Unterstützungsleistung per se, um dem Unternehmen beim Wiederaufbau seiner Systeme zu helfen, ist jedoch nicht denkbar und in Ausnahmefällen eben den Computer-Notfallteams vorbehalten.

Die in § 14 Abs. 2 Z 5 geregelte Aufgabe der Computer-Notfallteams zur Beobachtung und Analyse von Risiken, Vorfällen oder Sicherheitsvorfällen sowie die Lagebeurteilung ähnelt wiederum sehr stark der Aufgabe des Bundesministers für Inneres, Meldungen über Risiken, Vorfälle oder Sicherheitsvorfälle zu analysieren und regelmäßig ein Lagebild zu erstellen (§ 5 Abs. 1 Z 3). Genau

[538] EB RV NISG, S. 16.
[539] *Anderl et al.*, NISG::Kommentar, § 14, Rz 31.
[540] Reference document on Incident Notification for Operators of Essential Services, 2018, S. 8.

wie schon bei Z 3 ist weder dem Gesetz noch den Erläuternden Bemerkungen eine Differenzierung dieser Aufgaben zu entnehmen.

Nehmen die jeweiligen Organisationen ihre Aufgaben dementsprechend wahr, wird es zu einer Analyse des jeweiligen Sicherheitsvorfalles sowohl durch das betroffene Computer-Notfallteam als auch durch den Bundesminister für Inneres kommen.[541] Hier wird es notwendig sein, nähere Regelungen zu diesen Zuständigkeiten zu treffen, da das Gesetz selbst diese Fragen offenlässt. Von einer unzureichenden Determinierung (Art. 18 B-VG) ist jedoch nicht auszugehen, da es sich um Zuständigkeitsfragen handelt, die nicht in Rechte Dritter eingreifen und keine Auswirkungen auf die Betreiber selbst haben.

7.4.1.4. Rechtliche Stellung der Computer-Notfallteams

Da das NIS-Gesetz von der „Einrichtung" von Computer-Notfallteams spricht und diesen konkrete Aufgaben zuordnet, ist deren rechtliche Stellung zu untersuchen, insbesondere ob eine Beleihung, eine Inpflichtnahme, Indienstnahme bzw. Verwaltungshilfe oder keine dieser Formen vorliegt. Diese Frage kann mit einem Blick auf die durch die Computer-Notfallteams zu erfüllenden Aufgaben beantwortet werden, die bereits weiter oben dargestellt wurden.

Die Erläuternden Bemerkungen sprechen zumindest bei der Aufgabe der Entgegennahme von Meldungen durch Computer-Notfallteams (§ 14 Abs. 2 Z 1) von einer Beleihung, sofern es sich dabei um private Einrichtungen[542] handelt.[543] Wesentliches Merkmal einer Beleihung ist, dass der Private mit der Zuständigkeit zur Setzung von Hoheitsakten in eigener Organkompetenz und Verantwortung beliehen ist und die Kompetenz zu selbstständiger Entscheidung über die Erlassung bzw. den Inhalt von Hoheitsakten besteht.[544] Die Hoheitsverwaltung wird grundsätzlich durch das Gesetz konstituiert, wobei neben den „klassischen" Hoheitsakten[545] der Begriff der „schlichten Hoheitsverwaltung"[546] geprägt wurde.[547] Dabei handelt es sich um jenes Handeln, das mit den Kategorien der „Hoheitsakte" im engeren Sinn nicht zu erfassen war bzw. nicht „normativer" Art

[541] zu nicht nur reaktiven, sondern auch aktiven Gegenmaßnahmen der Behörden siehe Kapitel 7.6.2.
[542] beim GovCERT handelt es sich um eine Organisationseinheit des Bundeskanzleramtes und somit um Organe der öffentlichen Verwaltung – eine Beleihung oder andere Formen der Erfüllung hoheitlicher Aufgaben durch Private ist somit ausgeschlossen.
[543] Siehe EB RV NIS-Gesetz, S. 17; nähere Ausführungen zu den rechtlichen Hintergründen einer Beleihung sind auch Kapitel 7.5.5.1 zu finden.
[544] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.040.
[545] Bescheide, Verordnungen, Akte unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt; außerdem Weisungen und Vollstreckungsakte.
[546] auch „faktische Amtshandlungen", siehe OGH 30.09.2008 1 Ob 225/07f.
[547] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 696. Ausführlich dazu *Antoniolli/Koja*, Allgemeines Verwaltungsrecht[3] (1996). Siehe dazu auch *Korinek/Holoubek*, Grundlagen staatlicher Privatwirtschaftsverwaltung (1993).

ist, das aber jedenfalls „im Zusammenhang mit der Hoheitsverwaltung“ erfolgt.[548] Was sie zum hoheitlichen Handeln macht, ist also nicht das Handeln als solches, sondern der Kontext, in dem sie gesetzt werden.[549]

Da die Aufgaben der Computer-Notfallteams im Zusammenhang mit der Hoheitsverwaltung des Bundeskanzlers bzw. Bundesministers für Inneres stehen, kann von schlicht-hoheitlichem Handeln der Computer-Notfallteams ausgegangen werden. Dies gilt beispielsweise für die Aufgaben der Entgegennahme und Weiterleitung von Meldungen, die Ausgabe von Frühwarnungen, die allgemeine technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall und die Beobachtung von Risiken, Vorfällen oder Sicherheitsvorfällen (§ 14 Abs. 2 NISG).

Noch zu klären ist die Frage, ob es sich bei der schlicht-hoheitlichen Aufgabenerfüllung der Computer-Notfallteams um eine Beleihung[550] oder Indienstnahme bzw. Verwaltungshilfe[551] handelt. *Anderl/Heußler/Mayer/Müller* sehen keine Beleihung gegeben, da es sich bei den Aufgaben der Computer-Notfallteams um schlicht-hoheitliche Aufgaben handle und diese somit kein „imperium“ hätten.[552] Die Erläuternden Bemerkungen hingegen sehen die Computer-Notfallteams als Beliehene an, zumindest sofern es sich um die Aufgabe der Entgegennahme und Weiterleitung von Meldungen handelt.[553]

Gegen die Annahme einer Beleihung bei bloß schlicht-hoheitlichem Handeln spricht sich neben *Anderl/Heußler/Mayer/*Müller auch *Krajcsir* aus, der die Ermächtigung Privater zu schlicht-hoheitlichem Handeln nicht unter dem Begriff der Beleihung sieht, da sonst „strukturell verschiedene Sachverhalte in einem Begriff zusammengefasst und Differenzierungen verdeckt werden“.[554] Sofern Private zur Setzung von nur unselbstständigen Teilakten im Bereich der Hoheitsverwaltung berufen werden, keine selbstständige Entscheidungsbefugnis vorliegt und lediglich beschränkt hoheitliche Teilfunktionen wahrnehmen, liegt nach *Raschauer* keine Beleihung, sondern bloße Verwaltungshilfe bzw. Indienstnahme vor.[555]

---

[548] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 699.
[549] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 701.
[550] ausführliche zu den Formen der Beleihung siehe *Schäffer*, Erfüllung von Verwaltungsaufgaben durch Private (Beleihung und Inpflichtnahme) in Erfüllung von Verwaltungsaufgaben durch Privatrechtssubjekte, in Wirtschaft (Hrsg), Erfüllung von Verwaltungsaufgaben durch Privatrechtssubjekte (1972).
[551] Soweit die Heranziehung unabhängig von der Zustimmung des Betroffenen erfolgt, spricht man in diesem Zusammenhang auch von „Inpflichtnahme“, siehe *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.044.
[552] *Anderl et al.*, NISG::Kommentar, § 15 Rz 11.
[553] EB RV NISG, § 15, S. 17.
[554] *Krajcsir*, Staatliche Hoheitsverwaltung durch Private (1999), S. 128 f.
[555] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 119 ff.

Adamovic/Funk hingegen sehen die Beleihung als Kompetenz zu selbstständiger Entscheidung über die Erlassung bzw. den Inhalt von Hoheitsakten. Als Hoheitsakte kommen aus ihrer Sicht dabei insb. Verordnungen, Bescheide, verfahrensfreie Verwaltungsakte, aber auch Beurkundungen und Leistungsbeurteilungen in Betracht.[556] Schlicht-hoheitliches Handeln wäre demnach von deren Definition („verfahrensfreie Verwaltungsakte") umfasst. Nach *Rill* ist Beliehener jener, der mit „hoheitlichen Anordnungsbefugnissen (imperium) ausgestattet ist oder zu schlicht-hoheitlichem Handeln berufen ist, also einem Handeln in den Formen des öffentlichen Rechts, das in engem Zusammenhang mit der Ausübung von imperium steht".[557] Auch *Schön* geht davon aus, dass Beleihung auch dann vorliegt, wenn nicht nur förmliche Hoheitsakte gesetzt werden, sondern auch bei Realakten.[558]

Bei der bloßen Entgegennahme und Weiterleitung von Meldungen an den Bundesminister für Inneres kann meines Erachtens – der Formulierung in den Erläuternden Bemerkungen entgegnend – nur von einer bloßen Verwaltungshilfe bzw. Indienstnahme (und keiner Beleihung) in Form von schlicht-hoheitlichem Handeln ausgegangen werden, da es sich dabei um keine relevanten, selbstständigen Akte der Hoheitsverwaltung handelt.[559]

Ebenso handelt es sich bei der Aussendung von Frühwarnungen und der ersten technischen Unterstützung bei Sicherheitsvorfällen um Handlungen, die regelmäßig auch von privaten Sicherheitsdienstleistern erbracht werden und bereits vor Inkrafttreten des NIS-Gesetzes von CERT.at als privatem Verein geleistet wurden. Zwar ist aufgrund der Einrichtung durch Gesetz und den engen Zusammenhang zur Hoheitsverwaltung der Behörden im Rahmen der Netz- und Informationssystemsicherheit von schlicht-hoheitlichem Handeln auszugehen, eine Beleihung kann meines Erachtens jedoch nicht begründet werden.

7.4.1.5. Anforderungen an ein Computer-Notfallteam

Anhang I NIS-RL definiert unter anderem die Anforderungen, die in Umsetzung der NIS-RL von eingerichteten Computer-Notfallteams erfüllt werden müssen. Einerseits benötigen Computer-Notfallteams einen hohen Grad der Verfügbarkeit ihrer Kommunikationsdienste, wobei sie mehrere Kanäle bereitstellen sollen, damit sie jederzeit erreichbar bleiben und selbst Kontakt aufnehmen können.[560] Diese Voraussetzung ist hinsichtlich des ursprünglichen Ziels der Computer-

[556] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.040.
[557] *Rill*, Der Verwaltungsbegriff, in Ermacora (Hrsg), FS Antoniolli (1979), S. 51.
[558] *Schön*, Private Verwaltungshelfer: beliehene und inpflichtgenommene unter besonderer Berücksichtigung amtshaftungsrechtlicher Aspekte (1996), S. 105.
[559] Somit schließe ich mich der Meinung weiter oben Genannter an, wonach eine Beleihung nur bei förmlichen Hoheitsakten vorliegt und bei rein schlicht-hoheitlichem Handeln nicht begründet werden kann.
[560] Anhang I Z 1 lit. a NIS-RL.

Notfallteams, nämlich einen klar definierten „Point of Contact" darzustellen[561], wesentlich. Das NIS-Gesetz spricht hinsichtlich dieser Anforderung lediglich von der Verwendung sicherer Kommunikationskanäle (§ 15 Abs. 1 Z 5), die Bereitstellung mehrerer Kanäle ist indes nicht explizit vorgesehen.

In Umsetzung der Anforderung der NIS-RL, die Räumlichkeiten an sicheren Standorten einzurichten[562], sieht das NIS-Gesetz eine Erfüllung der in Art. 32 DSGVO festgelegten Standards vor (§ 15 Abs. 1 Z 1). Wie auch von *Anderl/Heußler/Mayer/Müller*[563] argumentiert bleibt offen, warum in diesem Zusammenhang nicht sogleich auf die von Betreibern wesentlicher Dienste zu erfüllenden Sicherheitsvorkehrungen (§ 17 Abs. 1 NISG iVm § 11 NISV[564]) verwiesen wurde. Die dort vorgesehenen Maßnahmen erfüllen eben genau den Zweck der Verfügbarkeit wesentlicher Dienste, die mit dem Zweck der Betriebskontinuität (von Computer-Notfallteams) vergleichbar ist.

Zur Gewährleistung ihrer Betriebskontinuität haben Computer-Notfallteams darüber hinaus durch Verwendung eines geeigneten Systems zur Verwaltung und Weiterleitung von Anfragen sowie durch eine personelle, technische und infrastrukturelle Ausstattung sicherzustellen, die eine ständige Bereitschaft und Verfügbarkeit gewährleistet (§ 15 Abs. 1 Z 2 lit. a und b).

Interessant ist in diesem Zusammenhang eine Regelung der NIS-RL. Demnach sollen die Mitgliedstaaten sicherstellen, dass ihre Computer-Notfallteams mit angemessenen Ressourcen ausgestattet sind, um ihre Aufgaben wirksam erfüllen zu können (Art. 9 Abs. 2) sowie sicherstellen, dass sie Zugang zu einer angemessenen, sicheren und robusten Kommunikations- und Informationsinfrastruktur auf nationaler Ebene haben (Art. 9 Abs. 3). Der nationale Gesetzgeber hat dies dadurch umgesetzt, dass es sich bei diesen Anforderungen um Voraussetzungen handelt, ohne deren Vorliegen die Eignung eines Computer-Notfallteams nicht festgestellt wird (§ 15 Abs. 3 iVm Abs. 1). Ob mit der Regelung in der Richtlinie nicht eher eine budgetäre Unterstützung – zumindest des nationalen Computer-Notfallteams – gemeint gewesen sein könnte, bleibt offen.

[561] *Pospisil et al.*, Datenschutz und Datensicherheit - DuD, 2017, S. 629.
[562] Anhang I Z 1 lit. b NIS-RL.
[563] *Anderl et al.*, NISG::Kommentar, § 15, Rz 2.
[564] Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssicherheitsverordnung – NISV), StF. BGBl. II Nr. 215/2019.

7.4.1.6. Sonstige Bestimmungen zu den Computer-Notfallteams

Empfehlungen zur Umsetzung der NIS-RL sehen vor, dass die Mitgliedstaaten es in Betracht ziehen können, den Aktionsbereich der CSIRT über die im Anwendungsbereich der RL erfassten Sektoren und Dienste hinaus zu erweitern.[565] Das bisherige nationale Computer-Notfallteam CERT.at ist wesentlicher Ansprechpartner im Bereich der IT-Sicherheit und betreut im Rahmen seiner Tätigkeit neben kleineren und mittleren Unternehmen auch die breitere Öffentlichkeit, die auch Privatpersonen umfasst, durch Warnungen und Tipps.[566] Diese Tätigkeit soll durch CERT.at auch weiterhin wahrgenommen werden können und damit in Zusammenhang stehende Datenverarbeitungen rechtlich verankert werden.[567] Im Rahmen einer richtlinienkonformen Interpretation ist der Aufgabenerfüllung zur Unterstützung der Betreiber wesentlicher Dienste und Anbieter digitaler Dienste aber jedenfalls Vorrang zu geben.

§ 14 Abs. 7 NISG ermächtigt Computer-Notfallteams, zur Aufgabenerfüllung personenbezogene Daten zu verarbeiten. Diese Ermächtigung gilt jedoch nur für die im Gesetz einzurichtenden Computer-Notfallteams. Jene Einrichtungen privater Unternehmen sind von dieser Regelung nicht umfasst und müssen sich nach den allgemeinen Bestimmungen der DSGVO richten.

Diese Bestimmung ist insofern wesentlich, als Nachrichten und Meldungen über sicherheitsrelevante Vorfälle erfahrungsgemäß immer personenbezogene Daten enthalten.[568] Beim Betrieb eines Computer-Notfallteams kommt es regelmäßig zur Verarbeitung personenbezogener Daten wie bspw. IP-Adressen oder Domain-Namen sowie zur Übermittlung dieser Informationen an Unternehmen im Rahmen ausgegebener Warnungen. [569]

Bemerkenswert ist daher, dass die NIS-RL eine solche datenschutzrechtliche Ermächtigung für die Computer-Notfallteams nicht regelt – dies gilt ebenso für die DSGVO und die Datenschutz-Richtlinie für die Strafverfolgung und Justiz (DSRL).[570] Lediglich ErwGr 49 DSGVO sieht vor, dass die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (CSERTs/CSIRTs), Betreiber von elektronischen Kommunikationsnetzen und –diensten sowie durch Anbieter von Sicherheitstechnologien und –diensten in dem Maße ein berechtigtes Interesse des

[565] COM(2017) 476 final S. 5.
[566] Siehe EB RV NIS-Gesetz, S. 16.
[567] Zu den bisher fehlenden Regelungen zur Datenverarbeitung durch Computer-Notfallteams siehe nächstes Unterkapitel (Datenverarbeitung durch Computer-Notfallteams).
[568] *Einzinger*, Datenschutz in Public-Private-Partnerships, in Skopik/Páhi et al. (Hrsg), Cyber Situational Awareness in Public-Private-Partnerships (2018), S. 181.
[569] Zum bisherigen Graubereich bei der Datenverarbeitung durch Computer-Notfallteams siehe *Einzinger/Skopik/Fiedler*, Datenschutz und Datensicherheit - DuD, 2015, S. 724.
[570] Siehe dazu auch *Einzinger* in Skopik/Páhi et al., Cyber Situational Awareness in Public-Private-Partnerships, S. 180.

jeweiligen Verantwortlichen darstellt, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist. Ein ErwGr stellt jedoch keine explizite Ermächtigung aus, sondern verweist auf ein berechtigtes Interesse des Verantwortlichen der Datenverarbeitung, welches in Verbindung mit Art. 6 Abs. 1 lit. f DSGVO die Verarbeitung und Übermittlung von personenbezogenen Daten in diesen Fällen als rechtmäßig anerkennt.[571]

7.5. Abschnitt 5 – Verpflichtungen für Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung

7.5.1. (Verfassungsrechtliche) Überlegungen zum Auferlegen von Verpflichtungen im Bereich der IT-Sicherheit

7.5.1.1. Staatliche Gewährleistungsverantwortung für die Daseinsvorsorge

Mehrfach wurde bereits auf den Umstand eingegangen, dass das Funktionieren kritischer Infrastrukturen für das Funktionieren des Staates insgesamt essentiell ist. Oftmals wird in der Literatur für die von kritischen Infrastrukturen erbrachten Leistungen der Begriff der Daseinsvorsorge verwendet, der von *Forsthoff*[572] geprägt wurde, zu dem es aber bis heute keine einheitliche geschweige denn nationale positivrechtliche Definition[573] gibt. *Adamovich* und *Funk*[574] sprechen in diesem Zusammenhang von der „Vorsorgeverwaltung“ und zählen hierzu Verkehrseinrichtungen, Bildungs- und Kultureinrichtungen, Krankenanstalten, Ver- und Entsorgungsanlagen sowie Kommunikationseinrichtungen.

Andere sehen den Begriff noch sehr viel weiter, wie beispielsweise *Wolff*[575], der beim Begriff der Daseinsvorsorge im juristischen Kontext von einer bestimmten Zielrichtung ausgeht, die wiederum eigentlich nicht juristisch, sondern politisch ist. „Mit Dasein sei das Dasein des einzelnen Menschen und mit Vorsorge die Bedingung gemeint, die dieser benötigt, um in einer Industriegesellschaft ein würdevolles Dasein zu fristen.“

[571] Siehe dazu *Einzinger/Skopik*, Datenschutz und Datensicherheit - DuD, 2017, S. 573.
[572] *Forsthoff*, Rechtsfragen der leistenden Verwaltung (1959).
[573] Zur Schwierigkeit einer rechtlichen Abgrenzung des Begriffes siehe *Knauff*, Der Gewährleistungsstaat: Reform der Daseinsvorsorge (2004), S. 46.
[574] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 44.015.
[575] *Wolff* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rz 6.

Binder[576] sieht die Daseinsvorsorge „generell als Antwort auf die Frage, welches übergeordnete Ziel die öffentliche Verwaltung verfolgt, welcher allgemeine Begriff die Vielzahl staatlicher Verwaltungsaufgaben umfassend beschreiben könnte".

Wimmer[577] bezeichnet damit (unter ausdrücklichem Verweis auf *Forsthoff*) die „Befriedigung menschlicher Grundbedürfnisse (wie Wohnen, Schlafen, Essen, Mobilität) bzw. die Schaffung entsprechender Voraussetzungen (Häuser, Wasserleitungen, Getreideverteilung, Feuerwehr, Straßen)", andere wiederum die „Sorge für die materiellen Existenzvoraussetzungen des Einzelnen oder die kollektive Vorsorge durch Schaffung von Infrastruktur und Leistungsbereitschaft der Verwaltung".[578]

Ob der offensichtlichen Bedeutung der Daseinsvorsorge stellt sich zwangsläufig die Frage, ob es sich dabei um eine Aufgabe des Staates handelt und wem selbige im Verwaltungsaufbau obliegt. Dass die Gewährleistung der Daseinsvorsorge bzw. des Gemeinwohls[579] im Interesse der gesamten Gesellschaft und somit im Interesse des Staates[580] liegt, ja nach Meinung *Forsthoffs*[581] sogar die bündigste Rechtfertigung für seine Existenz ist, die weit über die Interessen einzelner Unternehmen hinausgehen[582], scheint unumstritten. Die Leistungen des Staates im Bereich der Daseinsvorsorge machen den modernen Staat zum Sozialstaat, als solchen der Leistung[583] und Verteilung[584].

Das bundesstaatliche Prinzip (Art. 2 B-VG) und der Grundsatz der kommunalen Selbstverwaltung (Art. 115 ff B-VG) teilen den Staat in die Gebietskörperschaften Bund, Land und Gemeinde, jede Gebietskörperschaft führt die öffentliche Verwaltung und betreibt die Daseinsvorsorge im Rahmen ihres Kompetenzbereiches.[585] Anzumerken ist, dass die Gebietskörperschaften sowohl im Rahmen der Hoheitsverwaltung als auch im Rahmen der Privatwirtschaftsverwaltung tätig werden können

[576] *Binder*, Die Daseinsvorsorge der Gemeinde, in Gemeindebund (Hrsg), 40 Jahre Gemeindeverfassungsnovelle 1962 (2002), S. 105.
[577] *Wimmer*, Dynamische Verwaltungslehre (2010), S. 39.
[578] *Bull*, Daseinsvorsorge im Wandel der Staatsformen, Der Staat, 2008.
[579] Zum Begriff des Gemeinwohls siehe *Forsthoff*, Rechtsstaat im Wandel (1976), S. 39.
[580] Zur Daseinsvorsorge bzw. Regulierung zum Gemeinwohl als staatliche Aufgabe siehe *Walzel von Wiesentreu*, Die Wirtschaftsfreiheit der Gemeinde - Verfassungsdogmatische Anmerkungen zur Zulässigkeit der Ausgliederung von Gemeindeaufgaben, in Arnold/Bundschuh-Rieseneder et al. (Hrsg), Recht Politik Wirtschaft, Dynamische Perspektiven (2008), S. 628.
[581] *Forsthoff*, Rechtsstaat im Wandel, S. 39.
[582] *Bendiek*, SWP, 2012, S. 14.
[583] Zur Verwaltung als Leistungsträger siehe *Wimmer*, Dynamische Verwaltungslehre, S. 129.
[584] *Forsthoff*, Rechtsstaat im Wandel, S. 52.
[585] *Binder* in Gemeindebund, 40 Jahre Gemeindeverfassungsnovelle 1962, S. 105.

(Art. 17 B-VG) und im Rahmen der Privatwirtschaftsverwaltung nicht an das Kompetenzregime der Art. 10 bis 15 gebunden sind.[586]

Im Verwaltungsaufbau besteht die Daseinsvorsorge hauptsächlich[587] als Aufgabe der Gemeinde im eigenen Wirkungsbereich (Art. 118 Abs. 2 B-VG), wobei nach *Wimmer* das Prinzip des „kleinen Kreises" maßgeblich ist, welches von der Vorstellung getragen wird, dass bestimmte „Dienste", die der Bürger zum täglichen Leben braucht, auf der von ihm erreichbaren Ebene geschlossen zur Verfügung stehen müssen. [588]

Der dabei in den Verwaltungswissenschaften verwendete Begriff der „kommunalen Daseinsvorsorge" ist ein Bündel öffentlicher Verwaltungsaufgaben der Gemeinde und beschreibt jene Aufgaben, welche die Grundlagen des Lebens der Menschen vor Ort umsorgen und sichern (unter anderem die Wasserversorgung, Abwasserentsorgung, Energieversorgung).[589] Diese Aufgaben zählen zu jenen der Versorgungsaufgaben (im Gegensatz zu den Ordnungsaufgaben der Gemeinde), die in der Bereitstellung und Erbringung faktischer Leistungen der Daseinsvorsorge bestehen.[590]

Die Gemeinde kann als Selbstverwaltungskörper (Art. 116 Abs. 1 und 2 B-VG) dabei selbst entscheiden, welche konkreten öffentlichen Aufgaben sie im Rahmen der kommunalen Daseinsvorsorge wahrnehmen will, wobei sie nichtsdestotrotz als Teil der Verwaltung an Bundes- und Landesgesetze gebunden ist.[591]

Trotz eindeutigem Bestehen einer staatlichen Aufgabe kommt es seit Jahrzehnten[592] zu einer Entstaatlichung[593] öffentlicher Aufgaben bzw. der Daseinsvorsorge.[594] Dabei sollen vorab die damit verbundenen Begriffe definiert werden. Von einer Ausgliederung wird gesprochen, wenn bislang

---

[586] *Pürgy*, Dienstleistungen von allgemeinem Interesse in Österreich, in Krautscheid (Hrsg), Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl: Eine sektorspezifische Betrachtung (2009), S. 403.

[587] Betrifft den Bereich des „Örtlichen", der kommunalen Infrastruktur, um die es sich im Bereich der Daseinsvorsorge hauptsächlich handelt.

[588] *Wimmer*, Dynamische Verwaltungslehre, S. 140. Zur Daseinsvorsorge als Grundprinzip gesellschaftlichen Zusammenhalts, der zuallererst auf lokaler Ebene gebildet wird, siehe *Palmer*, Dasein oder Nichtsein - Der "Kampf um die Daseinsvorsorge" als exemplarischer Fall, in Hrbek /Nettesheim (Hrsg), Europäische Union und mitgliedstaatliche Daseinsvorsorge (2002), S. 12.

[589] *Binder* in Gemeindebund, 40 Jahre Gemeindeverfassungsnovelle 1962, S.107.

[590] *Kubin*, Die Gemeindeaufgaben und ihre Finanzierung (1972), S. 26.

[591] *Binder* in Gemeindebund, 40 Jahre Gemeindeverfassungsnovelle 1962, S. 106.

[592] Strömung der indirekten Lenkung, Deregulierung, Ausgliederung, Privatisierung, Non Profit Organisationen, Public Private Partnership etc. seit den 70 Jahren, siehe *Wimmer*, Dynamische Verwaltungslehre, S. 37.

[593] Entstaatlichung - Gefahr für den Rechtsstaat? (2002).

[594] *Wiater* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rz 13.

verwaltungseigene Tätigkeiten (zB der Betrieb von Verkehrseinrichtungen) auf einen – wenn auch staatseigenen – Rechtsträger übertragen werden. Eine echte Privatisierung liegt vor, wenn der betreffende Rechtsträger eine juristische Person privaten Rechts ist, eine unechte oder formelle Privatisierung, wenn der übertragenden Gebietskörperschaft Gesellschaftsanteile zur Gänze oder überwiegend gehören.[595]

Die Entstaatlichung bzw. insbesondere die Privatisierung[596] von Verwaltungsaufgaben war insbesondere von der Frage getragen, ob bestimmte Aufgaben nicht besser und billiger von der Privatwirtschaft erledigt werden sollten.[597]

Der Staat muss nach *Raschauer*[598] öffentliche Aufgaben nicht zu Staats- bzw. Verwaltungsaufgaben machen, wenn der private Sektor das als erforderlich erachtete Angebot bereithält. Einerseits wird versucht, durch Ausgliederungen[599] eine rationellere Wahrnehmung von Verwaltungsaufgaben zu erreichen[600], wobei die Gebietskörperschaften, die Geschäftsanteile an dieser Gesellschaft halten, diese in einer zivilrechtlichen Beauftragung verpflichtet, bestimmte Leistungen und Tätigkeiten zu erbringen (unechte Privatisierung).[601]

Oftmals behält sich der Staat im Rahmen der Ausgliederung auch Regulierungsbefugnisse vor, wodurch die Letztverantwortung über die Erfüllung öffentlicher Aufgaben bei ihnen verbleibt[602], oder agiert in Form von Public Private Partnership-Modellen[603]. Diese Entwicklungen haben zur Folge, dass staatliche Leistungsverantwortung abgebaut und durch Gewährleistungsverantwortung ersetzt wird.[604] Die Intensität der Regelung und Beaufsichtigung können somit variieren und es handelt sich zumindest um einen Zwischenbereich zwischen reiner Staatstätigkeit und freier Wirtschaft.[605] Dieses In-Pflicht-Bleiben des Staates wird zum Teil aus verfassungsrechtlichen Vorgaben abgeleitet.[606]

---

[595] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.047.
[596] Mehr zur Entwicklung der Privatisierung siehe *Wimmer*, Dynamische Verwaltungslehre, S. 107.
[597] *Binder* in Gemeindebund, 40 Jahre Gemeindeverfassungsnovelle 1962, S. 110.
[598] *Raschauer*, Allgemeines Verwaltungsrecht[3], S. 122.
[599] Hinzuweisen ist darauf, dass Ausgliederungen von Privatisierungen zu differenzieren sind.
[600] *Wimmer*, Dynamische Verwaltungslehre, S. 107.
[601] *Binder* in Gemeindebund, 40 Jahre Gemeindeverfassungsnovelle 1962, S. 110.
[602] Mit der zunehmenden Privatisierung gilt eine zunehmend geteilte Verantwortung für das Funktionieren kritischer Infrastruktur, siehe dazu *Wiater* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rz 16.
[603] *Pürgy* in Krautscheid, Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl: Eine sektorspezifische Betrachtung, S. 409.
[604] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.047.
[605] *Knauff*, Der Gewährleistungsstaat: Reform der Daseinsvorsorge, S. 52.
[606] *Walzel von Wiesentreu* in Arnold/Bundschuh-Rieseneder et al., Recht Politik Wirtschaft, Dynamische Perspektiven, S. 137.

Müller führt dazu aus, dass verfassungsrechtlich grundsätzlich nichts gegen die Ausgliederung staatlicher Aufgaben spreche und eine solche auch dem B-VG nicht zu entnehmen wäre. Dies gelte auch für so genannte staatliche Kernaufgaben[607] – sofern man sich überhaupt für deren (rechtliche) Existenz aussprechen sollte –, wobei den Staat hier zumindest eine Gewährleistungs- und Kontrollverantwortung treffe.[608]

Nicht unerwähnt bleiben sollen Überlegungen, ob es ein Grundrecht der Bürger auf eine funktionierende Daseinsvorsorge geben könnte. Dabei ist ein Blick auf Art. 6 der GRC[609] bzw. Art. 5 EMRK[610] zu werfen, die ein Recht auf Freiheit [611] und Sicherheit gewähren.[612] Eine weite Auslegung des Rechtes auf Sicherheit könnte dabei für ein Grundrecht auf eine funktionierende Daseinsvorsorge sprechen. Die herrschende Ansicht geht jedoch davon aus, dass es sich beim Begriff „Recht auf Freiheit und Sicherheit" um ein Begriffspaar handelt und dem Terminus der Sicherheit keine eigenständige Bedeutung zukomme. [613] Auch haben weder EuGH noch EGMR bisher klar festgestellt, dass Art. 5 Abs. 1 S. 1 EMRK (bzw. Art. 6 GRC) über ein bloßes Eingriffsrecht hinausgehe und die Staaten außerdem (positiv) dazu verpflichtet seien, die Sicherheit des Einzelnen durch konkrete Maßnahmen zu gewährleisten.[614]

Möglicherweise könnte sich auch durch das Grundrecht auf Leben und körperliche Unversehrtheit (Art. 2 EMRK[615]) ein subjektives Recht des Einzelnen auf die Erfüllung der Daseinsvorsorge des Staates ergeben. Art. 2 verpflichtet nach einschlägiger Rechtsprechung des EGMR über das Gebot, hoheitliche Eingriffe in das Recht auf Leben zu unterlassen, hinaus eine positive

---

[607] *Siehe dazu auch Lachmayer, Ausgliederungen und Beleihungen im Spannungsfeld der Verfassung, Juristische Blätter, 12/2007, S. 761*

[608] *Müller*, Das österreichische Regulierungsbehördenmodell (2010), S. 157.

[609] Europäische Grundrechtecharta, mehr dazu siehe Kapitel 7.5.2.3.

[610] Europäische Menschenrechtskonvention, mehr dazu siehe Kapitel 7.5.2.2.

[611] Das Recht auf persönliche Freiheit findet sich ebenso im österreichischen Verfassungsrecht verankert, siehe Art. 1 Abs. 1 Bundesverfassungsgesetz vom 29. November 1988 über den Schutz der persönlichen Freiheit, BGBl. I Nr. 2/2008.

[612] Art. 6 GRC entspricht dabei ungeachtet textlicher Abweichungen den materiellen und verfahrensrechtlichen Gewährleistungen des Art. 5 EMRK und zielt primär auf „klassische" Konstellationen von Freiheitsbeschränkungen ab, siehe *Bernsdorff*, Art. 6 GRC, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014), Rz 1.

[613] Zur kontroversiellen Diskussion zwischen Konventsmitgliedern, dass der Begriff „Sicherheit" für ein eigenes Rechtsgut stehen könnte sowie die Sicherheitsbehörden und damit auch die Polizei sehr weitgehend rechtlich binden könnte, siehe *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 7 u. 12. Für die Auslegung, dass mit Sicherheit die „Rechtssicherheit" in Bezug auf die persönliche Freiheit gemeint ist spricht auch die verbindliche französische Fassung, siehe *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte (2008), Rz 1097.

[614] *Peukert*, Art. 5 EMRK, in Frowein /Peukert (Hrsg), Europäische Menschenrechtskonvention: EMRK-Kommentar (2009), S. 75.

[615] In Kapitel 7.5.2.2 wird allgemein und näher auf die Europäische Menschenrechtskonvention eingegangen.

Gewährleistungspflicht des Staates.[616] Nach dem überwiegenden Teil der Lehre entstehen Schutzpflichten des Staates jedoch erst, wenn die Gefährdung des Lebens greifbar wird, dh mit größerer Wahrscheinlichkeit eintreten kann.[617] Bei der Daseinsvorsorge handelt es sich um die grundsätzliche Versorgung mit Energie, Wasser oder dem öffentlichen Verkehr. Diese Dienste sind für das Leben der Menschen in einem Staat notwendig und Voraussetzung dafür, eine Bedrohung mit dem Tod oder einer körperlichen Beeinträchtigung ist bei Unterlassen dieser Versorgung jedoch mE zumindest nicht unmittelbar erkennbar bzw. zwingend die Folge. Im Lichte der dargestellten Argumentation der Lehre ist somit von keiner aktiven Schutzpflicht des Staates gem. Art. 2 EMRK zur grundsätzlichen Versorgung auszugehen, da die geforderte Unmittelbarkeit der Gefährdung nicht vorliegt.

Festzuhalten bleibt, dass dem Staat eine Gewährleistungs- und Infrastrukturverantwortung obliegt[618] - er soll zwar viele Aufgaben nicht mehr selbst erfüllen, aber für ihre Erfüllung einstehen, was dem Konzept des Gewährleistungsstaates[619] entspricht.[620] [621]

7.5.1.2. Selbstverpflichtung der Wirtschaft vs. Auferlegen von Verpflichtungen

Als bisher herrschendes Prinzip im Rahmen des Schutzes kritischer Infrastruktur galt in Österreich jenes der Subsidiarität und Selbstverpflichtung[622] der Unternehmen, wonach sich diese in einer (freiwilligen) Selbstverpflichtung[623] zu einer erhöhten Resilienz bekennen sollen.[624] Der oftmals (auch im Österreichischen Programm zum Schutz kritischer Infrastruktur[625]) verwendete Begriff der

[616] EGMR, U 17.1.2002, Calvelli u. Ciglio gg Italien, Nr. 32967/96, Z 48. Siehe auch *Zacherl*, Leben gegen Leben? Lebensrecht des Einzelnen im Spannungsverhältnis zur Schutzpflicht des Staates gem. Art. 2 EMRK am Beispiel der Terrorismusbekämpfung (2010), S. 17.
[617] *Kopetzki*, Kommentierung zu Art. 2 EMRK, in Korinek /Holoubek (Hrsg), Bundesverfassungsrecht (2002), Rz 69.
[618] *Engels* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rz 12.
[619] Ausführlich zum Gewährleistungsstaat siehe *Knauff*, Der Gewährleistungsstaat: Reform der Daseinsvorsorge.
[620] *Bull*, Der Staat, 2008, S. 9
[621] Zum Begriff des „Risikosteuerungsstaates" durch Risiken bislang unbekannter Dimension, die insbesondere durch die technische Entwicklung herbeigeführt werden, siehe *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, S. 29.
[622] Bei Selbstverpflichtungen wird von Übereinkommen gesprochen, die von Unternehmen oder Branchenverbänden abgeschlossen werden. Sofern sie nicht ausnahmsweise in Vertragsform erfolgt, ist sie rechtlich unverbindlich. Häufig werden sie verwendet, um hoheitliche Rechtsetzung zu vermeiden. Mehr dazu siehe *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem (2010). *Knauff*, S. 247.
[623] sofern es sich dabei um öffentliche Aufgaben handelt, wird von einer Ausgliederung oder Privatisierung gesprochen, siehe dazu Kapitel 7.5.1.1.
[624] Österreichisches Programm zum Schutz kritischer Infrastruktur (APCIP), 2014, S. 8.
[625] Österreichisches Programm zum Schutz kritischer Infrastruktur (APCIP), 2014, S. 11.

„Public Private Partnership“ wird in diesem Zusammenhang wohl oft falsch genutzt[626], da es sich dabei um eine gleichberechtigte Beteiligung der privaten Wirtschaft an der Erfüllung öffentlicher Aufgaben handelt und die Beteiligten zu gleichen Teilen an den Chancen und Risiken dieser Partnerschaft partizipieren können.[627]

Binder verwendet den in der Verwaltungslehre genutzten Begriff der Public Private Partnership (PPP) beispielsweise in jenem Bereich, in denen die Gemeinden durch eigene Initiativen versuchen, die erforderlichen Leistungen der kommunalen Daseinsvorsorge zu gewährleisten, ohne selbst Leistungen organisieren und erbringen zu müssen.[628] Dies kann im Regelfall durch „Entkommunalisierung“ erfolgen, in dem die Gemeinde Formen der Zusammenarbeit mit Privaten sucht, die einerseits der Gemeinde die Entkommunalisierung erlauben, andererseits die neuen Leistungsträger an kommunale Rücksichten binden.[629]

In Bezug auf den Schutz kritischer Infrastruktur erscheint die Verwendung des Begriffes der „Governance“ passender, wonach diejenigen Formen der Steuerung verstanden werden, bei denen hierarchische staatliche Entscheidungen[630] nicht im Zentrum stehen, sondern das Zusammenwirken von staatlicher und privater Seite dominieren.[631] Es liegt damit eine Schwerpunktverlagerung von einseitig-hoheitlicher Anordnung zu Inklusion und freiwilliger Mitwirkung der Betroffenen vor,[632] wobei diese fortschreitende Vernetzung von Staat und Gesellschaft durch den zurückhaltenden staatlichen normativen Eingriff bei gleichzeitig erhöhtem Eigenverantwortlichkeitsanspruch an gesellschaftliche Akteure nicht zuletzt durch einen Kommunikationsprozess begleitet werden muss.[633]

---

[626] Zur Ansicht, dass es an einer klaren Definition von PPP seitens der Verwaltungswissenschaft bislang noch fehlt, siehe *Walzel von Wiesentreu* in Arnold/Bundschuh-Rieseneder et al., Recht Politik Wirtschaft, Dynamische Perspektiven, S. 687.

[627] *Wimmer*, Dynamische Verwaltungslehre, S. 117. Public Private Partnership beispielsweise als die Errichtung gemeinsamer Unternehmen mit Privaten (bspw. für Zwecke der Müllabfuhr oder der Abwasserentsorgung), siehe *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 331. Zur Ansicht, dass es sich bei einer PPP der Sache nach um nichts anderes als um die Heranziehung privater Unternehmen zur Wahrnehmung staatlicher Aufgaben handelt siehe *Walzel von Wiesentreu* in Arnold/Bundschuh-Rieseneder et al., Recht Politik Wirtschaft, Dynamische Perspektiven, S. 688.

[628] Wobei dies nichts anderes aus die Ausgliederung von Verwaltungsaufgaben darstellt.

[629] *Binder* in Gemeindebund, 40 Jahre Gemeindeverfassungsnovelle 1962, S. 106.

[630] Zur rechtspolitischen Frage, ob das Recht mit seinen Steuerungsinstrumenten den Risiken der IT-Sicherheit überhaupt Rechnung tragen kann siehe *Brisch*, Der Beitrag des Rechts zur IT-Sicherheit: Rechtsrahmen, Anforderungen, Grenzen, in Abolhassan (Hrsg), Security Einfach Machen (2017), S. 41.

[631] Zur Schwierigkeit der Definition von „Governance“ siehe *Schuppert*, Governance in einer sich wandelnden Welt, in Schuppert /Zürn (Hrsg), (2008), S. 24.

[632] *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, S. 15.

[633] *Weyand* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rz 5.

Die Herausforderung für das Funktionieren dieser Zusammenarbeit liegt jedenfalls darin, dass gesellschaftliche Ziele des Staates und ökonomische Ziele privater Unternehmen[634] in Einklang gebracht werden müssen, da im Bereich des Schutzes kritischer Infrastruktur der von staatlicher Seite an die Privatwirtschaft gerichtete Katalog an vorbeugenden Sicherheitsmaßnahmen auch solche umfasst, die nicht nur dem einzelnen Unternehmen nutzen, sondern gerade auf eine Verbesserung des gesamten Netzwerkes abzielen. [635]

Wo das Österreichische Programm generell von einer Selbstverpflichtung und Governance im Bereich des Schutzes kritischer Infrastruktur ausgeht, bestehen seit vielen Jahren aus oben genannten Gründen in Teilbereichen, in denen dies notwendig erscheint, trotz allem rechtliche Verpflichtung für private Unternehmen, wie dies beispielsweise in den Bereichen der Elektrizität[636], der Erdölvorsorge[637] oder dem Eisenbahnverkehr[638] ersichtlich ist.

Die zumindest partielle Kehrtwende[639] staatlicher Steuerung, die sich im Vergleich zum generellen Schutz kritischer Infrastruktur im Bereich der IT-Sicherheit durch die NIS-RL vollzogen hat, steht ebenso beispielhaft für die Problematik eines nicht vollständigen Gleichlaufs staatlicher und privater Interessen.[640] Beispielsweise weist auch die deutsche Bundesregierung in ihrem Gesetzesentwurf zum IT-Sicherheitsgesetz auf den Zustand hin, dass IT-Sicherheitsmaßnahmen in den verschiedenen Bereichen unterschiedlich stark entwickelt und die aus dem hohen Grad der Vernetzung resultierenden Interdependenzen zwischen den unterschiedlichen Bereichen kritischer Infrastrukturen nicht hinnehmbar sind.[641]

---

[634] Einer Erhebung von Forrester Research zufolge gibt ein durchschnittliches Unternehmen 0,0025 Prozent seines Umsatzes für IT-Sicherheit aus, siehe dazu *Könen*, Datenschutz und Datensicherheit - DuD, 2016, S. 13.

[635] Die Übernahme gemeinwohlrelevanter Zusatzkosten widerspricht dem Grundsatz individueller Rationalität der Marktteilnehmer, mehr dazu siehe *Wiater* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rz 23.

[636] Bundesgesetz, mit dem die Organisation auf dem Gebiet der Elektrizitätswirtschaft neu geregelt wird (Elektrizitätswirtschafts- und –organisationsgesetz 2010 – ElWOG 2010).

[637] Bundesgesetz über die Haltung von Mindestvorräten an Erdöl und Erdölprodukten (Erdölbevorratungsgesetz 2012 – EBG 2012).

[638] Bundesgesetz über Eisenbahnen, Schienenfahrzeuge auf Eisenbahnen und den Verkehr auf Eisenbahnen (Eisenbahngesetz 1957 – EisbG).

[639] Der Informationsaustausch zwischen staatlichen Behörden und betroffenen privatwirtschaftlichen Akteuren war bisher in den meisten Teilen Europas vor allem im Rahmen sogenannter Public Private Partnerships organisiert, siehe dazu *Klimburg*, Gesamtstaatliche Ansätze zur Cybersicherheit: Erfahrungen aus Österreich, Strategie und Sicherheit, S. 466.

[640] *Wiater* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rz 2.

[641] BT-Drs. 18/4096.

7.5.2. Eingriff in verfassungsrechtlich gewährleistete Rechte der Betreiber und Anbieter

7.5.2.1. Allgemeine Überlegungen

Durch die NIS-RL und deren Verpflichtungen zu Sicherheitsvorkehrungen und Meldepflichten soll schlussendlich ein höheres Maß an Sicherheit für jedermann entstehen. Diese Verpflichtungen bringen jedoch Einschränkungen für jene mit sich, die im Anwendungsbereich der Richtlinie liegen. Aus diesem Grund soll in den nachfolgenden Kapiteln untersucht werden, ob Regelungen der NIS-RL bzw. in weiterer Folge des NIS-Gesetzes in verfassungsrechtlich gewährleistete Rechte eingreifen und falls ja, ob diese Eingriffe rechtmäßig sind.

Im Rahmen dieser Untersuchung sind verschiedene Ebenen zu beleuchten. Einerseits müssen die Regelungen der NIS-RL als Rechtsakt der Europäischen Union in Übereinstimmung mit der Europäischen Grundrechtecharta (GRC) (und in diesem Zusammenhang mittelbar auch mit der Europäischen Menschenrechtskonvention (EMRK)) sein.[642] Dazu merkt die Richtlinie selbst in ihrem ErwGr 75 an, dass sie mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen, insbesondere der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang steht. Ebenso sieht sie im ErwGr vor, dass die Richtlinie im Einklang mit diesen Rechten und Grundsätzen umgesetzt werden sollte.[643]

Die nationale Umsetzung der Richtlinie im Form des NIS-Gesetzes obliegt dagegen einer so genannten doppelten Bindung.[644] Einerseits besagt dieser Grundsatz, dass bei der nationalen Gesetzgebung eine verfassungskonforme Lösung zu wählen ist, sofern eine Richtlinie dem nationalen Gesetzgeber bei der Umsetzung einen Spielraum und somit Raum für (eine nationale) verfassungskonforme Regelungen lässt.[645] Sofern hingegen kein Spielraum in der Umsetzung eines

[642] Siehe dazu Kapitel 7.5.2.3.
[643] ErwGr 75 NIS-RL.
[644] *Heißl*, Verhältnis der Grundrechtecharta zu nationalen Grundrechtsgewährleistungen und zur Europäischen Menschenrechtskonvention in Bezug auf Grundrechtskollisionen, in Kahl/Raschauer et al. (Hrsg), Grundsatzfragen der europäischen Grundrechtecharta (2013), S. 63. Zur Diskussion, ob der grundsätzliche Vorrang des europäischen Grundrechts zu einer weitgehenden Verdrängen (weitergehender) nationaler Grundrechte führen wird, siehe *Borowsky*, Allgemeine Bestimmungen über die Auslegung und Anwendung der Charta, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014), Rz 30.
[645] *Baumgartner*, Verfassungsgerichtliche Normenkontrolle und EU-Recht, Zeitschrift für öffentliches Recht, 3/2010, S. 298. Dies anerkennt erstmals der VfGH in VfSlg 15.215/1998.

EU-Rechtsaktes vorgesehen ist, bleiben nationale Grundrechte unangewendet und der Vorrang des Unionsrechts (in Form der Europäischen Grundrechtecharta) kommt zum Zug. [646]

In einer Grundsatzentscheidung vom 14. März 2012 stellte der VfGH fest, dass die von der Grundrechte-Charta garantierten Rechte als verfassungsgesetzlich gewährleistete Rechte Prüfungsmaßstab in Verfahren vor dem Verfassungsgerichtshof seien. Ebenso akzeptierte der VfGH bereits 1997 den Vorrang unmittelbar anwendbarer Vorschriften des Gemeinschaftsrechts vor einfachem nationalen Recht.[647]

Diese Parallelität der Grundrechteordnung führt insbesondere Art. 6 EUV näher aus, indem er drei selbstständige Säulen des Grundrechtsschutzes in der Union errichtet. Einerseits anerkennt die Union die Freiheiten und Grundsätze der Europäischen Grundrechtecharta (Art. 6 Abs. 1), die Grundrechte der Europäischen Menschenrechtskonvention (Art. 6 Abs. 3) sowie richterrechtlich entwickelte und auch künftig zu entfaltende unterschriebene europäische Grundrechte. [648]

Schwierigkeiten entstehen grundsätzlich dann, wenn sich Regelungen verschiedener Grundrechtskataloge widersprechen (beispielsweise Regelungen der GRC widersprechen nationalen Grundrechten), wobei sich EMRK und GRC in das bestehende Geflecht aus nationalen, europäischen und internationalen Grund- und Menschenrechten schonend einfügen, insbesondere ohne zu einer Anpassung nach unten zu führen.[649]

Auf diese möglichen Schwierigkeiten wird in den nächsten Kapiteln näher einzugehen sein.

7.5.2.2. Einleitende Anmerkungen zur Europäischen Menschenrechtskonvention (EMRK)

Die Konvention[650] zum Schutze der Grundfreiheiten und Menschenrechte (Europäische Menschenrechtskonvention – EMRK)[651] ist ein multilateraler völkerrechtlicher Vertrag, der vom Europarat verabschiedet[652] und in Österreich am 03. September 1958 in Verfassungsrang[653] ratifiziert[654] wurde.

---

[646] *Heißl* in Kahl/Raschauer et al., Grundsatzfragen der europäischen Grundrechtecharta, S. 63f.
[647] VfGH B877/86 v. 26.06.1997, VfSlg 14.886/1997.
[648] *Heißl* in Kahl/Raschauer et al., Grundsatzfragen der europäischen Grundrechtecharta, S. 61.
[649] *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar.
[650] Mittlerweile wurde die Konvention durch vierzehn Zusatzprotokolle ergänzt oder revidiert.
[651] Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl. Nr. 2010/1958 idF BGBl. III Nr. 139/2018.
[652] *Ehlers*, Allgemeine Lehren der EMRK, in Ehlers (Hrsg), Europäische Grundrechte und Grundfreiheiten (2014), Rz 7f.
[653] BGBl. 1964/59.
[654] Da die EMRK selbst keine Vorgaben über ihre Stellung enthält, haben Staaten diese in unterschiedlicher Rangordnung inkorporiert (Verfassungsrang, übergesetzlicher Rang, Rang einfacher Gesetze), siehe

Die Europäische Union sieht primärrechtlich einen Beitritt der EU zur EMRK vor (Art. 6 Abs. 2 EUV)[655], womit freilich keine unmittelbare Bindung der Union an die EMRK einhergeht.[656] Nichtsdestotrotz anerkennt Art. 6 Abs. 3 EUV die Grundrechte der EMRK sowie jene gemeinsamer Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze als Teil des Unionsrechts.[657]

Bevor die einzelnen Grundrechte und deren Betroffenheit näher beleuchtet werden, soll eingehend die Frage geklärt werden, ob die Hauptbetroffenen der NIS-RL – nämlich Unternehmen – überhaupt im Anwendungsbereich einer Konvention liegen können, die neben Grundfreiheiten von Menschenrechten spricht.

Gem. Art. 34 EMRK kann der Gerichtshof von jeder natürlichen Person, nichtstaatlichen Organisation oder Personengruppe, die behauptet, in einem der anerkannten Rechte verletzt zu sein, mit einer Beschwerde befasst werden. Durch die Beschwerdemöglichkeit nichtstaatlicher Organisationen kann davon ausgegangen werden, dass auch juristische Personen von den Rechten der EMRK erfasst sind. Diese Grundrechtsberechtigung soll nur dort nicht gegeben sein, wo das betreffende Recht seinem Wesen nach nicht auf die juristische Person anwendbar sein kann.[658]

Neben einigen absolut garantierten Grundrechten[659] enthält die EMRK hauptsächlich Grundrechte, hinsichtlich derer unter gewissen festgelegten Voraussetzungen Eingriffe möglich sind. Anders als die GRC enthält die EMRK keinen allgemeinen Gesetzesvorbehalt, sondern derer spezifische in den jeweiligen Bestimmungen selbst.[660]

Die grundsätzliche Systematik der Grundrechtsprüfung richtet sich nach der Prüfung des Schutzbereiches des Grundrechtes, dem Eingriff in diesen Schutzbereich durch eine konkrete Maßnahme und die Rechtfertigung dieses Eingriffes, wobei jeder Eingriff eine gesetzliche

---

Grabenwarter/Pabel, Europäische Menschenrechtskonvention (2012), § 3, Rz 1. *Ehlers* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 11.

[655] Der EuGH stellte in seinem Gutachten vom 18.12.2014 fest, dass das Beitrittsabkommen der EU zur EMRK aus mehreren Gründen unvereinbar mit dem Unionsrecht sei. Siehe „Gutachten nach Art. 218 Abs. 11 AEUV – Entwurf eines internationalen Übereinkommens – Beitritt der Europäischen Union zur Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten – Vereinbarkeit des Entwurfs mit dem EU-Vertrag und dem AEU-Vertrag“ in dem Gutachtenverfahren 2/13 betreffend einen Antrag auf Gutachten nach Art. 218 Abs. 11 AEUV, eingereicht am 4. Juli 2013 von der Europäischen Kommission.

[656] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 38.

[657] Die EMRK bilden für das Unionsrecht nur eine Rechtserkenntnisquelle, siehe *Ehlers* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 21.

[658] *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 17 Rz 5f. *Ehlers* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 44.

[659] Als Beispiel ist das Verbot der Folter (Art. 3 EMRK) anzuführen.

[660] *Ehlers* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 76.

Grundlage[661] haben, ein legitimes Ziel[662] verfolgen und dem Verhältnismäßigkeitsgrundsatz zu entsprechen hat.[663] Der Verhältnismäßigkeitsgrundsatz vereint dabei mehrere Bedingungen. Einerseits muss der Eingriff zur Zielerreichung geeignet sowie die eingreifende Maßnahme das gelindeste Mittel zur Zielerreichung sein.[664] Außerdem erfordert die Maßnahme einen Interessensausgleich zwischen dem Allgemeininteresse und dem Individualinteresse.[665]

Eine Anwendung dieser Grundsätze und allgemeinen Überlegungen erfolgt in den nachfolgenden Kapiteln zur spezifischen Prüfung der Rechtmäßigkeit von Eingriffen in die Grundrechte der EMRK durch die NIS-RL bzw. deren Umsetzung.

7.5.2.3. Einleitende Anmerkungen zur Charta der Grundrechte der Europäischen Union (GRC)

Die Charta der Grundrechte der Europäischen Union (GRC) [666] wurde am 7. Dezember 2000 in Nizza erstmals und am 12. Dezember 2007 in Straßburg in überarbeiteter Form feierlich proklamiert und kann als erster europäischer Grundrechtekatalog, der auf Initiative der EU-Mitgliedstaaten zu Stande gekommen ist, bezeichnet werden.[667] Tatsächliche Rechtswirkung entfaltete die Grundrechtecharta erst mit 01. Dezember 2009, als sie mit dem Vertrag von Lissabon in Kraft trat.[668]

Gem. Art. 6 Abs. 1 EUV erkennt die EU die Rechte, Freiheiten und Grundsätze an, die in der Charta der Grundrechte der EU vom 7. Dezember 2000 in der am 12. Dezember 2007 in Straßburg angepassten Fassung niedergelegt sind. Zusätzlich regelt Art. 6 Abs. 1 EUV, dass die Grundrechtecharta neben dem EU-Vertrag rechtlich gleichrangig (und somit primärrechtlich) existiert.[669]

---

[661] Gesetz im Sinn der EMRK sind auch untergesetzliche Normen mit Außenwirkung, nicht aber rein verwaltungsinterne Verwaltungsvorschriften (Gesetz im materiellen Sinn).
[662] Die legitimen Ziele sind meist in der jeweiligen Bestimmung des Grundrechts selbst zu finden.
[663] *Ehlers* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 67.
[664] *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 18 Rz 15.
[665] *Ehlers* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 80.
[666] Charta der Grundrechte der Europäischen Union, 2010/C 83/02.
[667] *Schwarze*, Der Grundrechtsschutz für Unternehmen in der Europäischen Grundrechtecharta, Europäische Zeitschrift für Wirtschaftsrecht, 17/2001, S. 517.
[668] *Jarass*, Charta der Grundrechte der Europäischen Union : Kommentar[2] (2013), Einleitung, Rz 2.
[669] Mit dem Vertrag von Lissabon (Art. 6 Abs. 1 EUV) hat die Charta mit 01.12.2009 erstmals formelle Geltung erlangt.

Sie gilt gem. Art. 51 Abs. 1 GRC unmittelbar nur für die Organe und Einrichtungen der Union[670] und für die Mitgliedstaaten bei der Durchführung des Unionsrechts[671]. Deshalb ist bei rein nationalen Sachverhalten von der Unanwendbarkeit der Grundrechtecharta auszugehen.[672] Wie bereits in Kapitel 7.5.2.1 angemerkt, gelten die Bestimmungen der Grundrechtecharta somit jedenfalls für die Regelungen der NIS-RL. Darüber hinaus ist auch von einer Anwendbarkeit für die Bestimmungen des NIS-Gesetzes auszugehen, da es sich dabei um eine Durchführung des Gemeinschaftsrechtes handelt. Sofern das NIS-Gesetz jedoch Regelungen enthält, die über jene der NIS-RL hinausgehen (siehe beispielsweise die Bestimmungen zum Sensornetzwerk, Kapitel 7.3.1), hat die Grundrechtecharta meines Erachtens unangewendet zu bleiben.[673]

Zum Verständnis der weiter unten angeführten konkreten Rechte der Grundrechtecharta ist auf deren Unterscheidung in Bestimmungen, die subjektive Rechte gewährleisten (die Mehrzahl) sowie jene Artikel, die objektivrechtliche Garantien[674] formulieren, hinzuweisen.[675]

Wie bereits weiter oben zur EMRK soll auch zur Grundrechtecharta einleitend die Frage beantwortet werden, ob sich Unternehmen als Hauptbetroffene der NIS-RL überhaupt im persönlichen Anwendungsbereich der Charta befinden.

Explizit finden sich juristische Personen nur in den Art. 42 bis 44 GRC vom persönlichen Anwendungsbereich erfasst. Doch auch in Grundrechten, die dies nicht explizit nennen, geht die Grundrechtsjudikatur des EuGH von der Einbeziehung juristischer Personen in den Anwendungsbereich aus. [676] Die Einbeziehung juristischer Personen ergibt sich dabei aus dem durch

[670] Von Anfang an war unbestritten, dass die Charta gerade die europäische Hoheitsgewalt binden, bändigen, begrenzen soll, siehe Verweis auf *Mock/Demuro/Cartabia*, Human Rights in *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 16.

[671] Dies ist insbesondere bei der Umsetzung von Richtlinien in das nationale Recht zu bejahen, siehe EuGH – X, C-74/95 u. C-129/95 – Slg. 1996, I-6609 Rz 25.

[672] EuGH Rs C-256/11 – Dereci. Dazu auch *Heißl* in Kahl/Raschauer et al., Grundsatzfragen der europäischen Grundrechtecharta, S. 63.

[673] In diesen Fällen sind nur die im nationalen Verfassungsrecht befindlichen Grundrechte (darunter insbesondere die Bestimmungen der EMRK) anzuwenden.

[674] Erkennbar durch Formulierungen, dass die darin gewährleisteten Rechte „anerkannt“ oder „geachtet“ werden.

[675] Diese Unterscheidung lässt eine abgestufte Intensität erkennbar werden, siehe *Schwarze*, Europäische Zeitschrift für Wirtschaftsrecht, 2001, S. 519. Eine Klarstellung erfolgt in Art. 52 Abs. 5 GRC, dass unter subjektiven Rechten einklagbare Rechte zu verstehen sind, während Grundsätze vollzugsbedürftige Prinzipien ohne prägenden subjektiv-rechtlichen Gehalt darstellen, so dass erst ein entsprechender Konkretisierungsakt subjektive Rechte begründen kann, siehe *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 33.

[676] *Schwarze*, Europäische Zeitschrift für Wirtschaftsrecht, 2001, S. 519. Siehe dazu EuGH 17.12.1998, C-185/95 P (Baustahlgewebe GmbH/Kommission); EuGH 26.06.1997, C-369/95 (Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH/Bauer Verlag); EuGH 11.07.1989, C-265/87 (Schräder GmbH & Co. KG/Hauptzollamt Gronau); ua.

Auslegung zu ermittelnden Schutzbereich des Grundrechts[677] - dies gilt insbesondere für die Garantien der Art. 15 (Berufsfreiheit), Art. 16 (unternehmerische Freiheit) und das Recht auf Schutz des Eigentums (Art. 17).

Im Gegensatz zur EMRK regelt die Charta selbst im letzten Teil (Art. 52 ff GRC) konkret Bedingungen und Voraussetzungen für die Rechtmäßigkeit von Eingriffen in deren Grundrechte. Art. 52 GRC enthält dabei eine Mischung aus Transfer- und Schrankenklauseln sowie Auslegungsregeln[678], die auf alle zuvor gewährleisteten Grundrechte anzuwenden sind.

Nachfolgende Systematik[679] der Eingriffsprüfung ist hierbei vorgesehen. Einerseits finden sich absolut bzw. einschränkungslos gewährleiste Grundrechte[680], in die selbsterklärend keinerlei Eingriff zulässig ist.

Daneben finden sich in der Charta einige Grundrechte, die aus der EMRK übernommen bzw. dieser entlehnt wurden. Dazu regelt Art. 52 Abs. 3, dass diese Rechte die gleiche Bedeutung und Tragweite haben sollen,[681] wie sie ihnen in der EMRK verliehen wird. Dies bedeutet in weiterer Folge, dass diese Grundrechte exakt den dort detailliert angeführten Schrankenregelungen unterworfen sein sollen.[682] Ein weitergehender Schutz von Rechten durch die Charta soll dadurch gleichzeitig nicht ausgeschlossen werden (Art. 52 Abs. 3 S 2 GRC).

Alle verbleibenden Rechte – also jene, die nicht absolut gelten und nicht die gleiche Bedeutung haben wie jene der EMRK – unterfallen der allgemeinen Einschränkungsklausel des Art. 52 Abs. 1 GRC. Für diese Rechte können sich über Art. 52 Abs. 4 zusätzliche Vorgaben für Einschränkungen ergeben, sofern sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ableiten. Diese Systematik der allgemeinen Einschränkungsklausel gilt auch für jene Rechte, bei

[677] *Stangl*, Der Anwendungsbereich der Grundrechtecharta, in Kahl/Raschauer et al. (Hrsg), Grundsatzfragen der europäischen Grundrechtecharta (2013), S. 2.
[678] *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Art. 52, Rz 12.
[679] *Bühler*, Einschränkung von Grundrechten nach der Europäischen Grundrechtecharta (2005), S. 235.
[680] Bspw. das Recht auf Menschenwürde gem. Art. 1 GRC.
[681] Präsidenten von EGMR und EuGH sprachen sich 2011 für eine parallele Auslegung aus der EMRK und der GRC aus, siehe„Joint Communication from Presidents Costa and Skouris“ v. 24.1.2011, https://www.echr.coe.int/Documents/UE_Communication_Costa_Skouris_ENG.pdf, abgerufen am 24.07.2019.
[682] Die Qualifikation eines Eingriffs richtet sich nach den Maßstäben der EMRK, und schließlich ist auch die Rechtfertigung nach den Maßstäben der Konventionsgarantie zu beurteilen, siehe *Vedder/Heintschel von Heinegg/Folz,* Europäischer Verfassungsvertrag in *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar., Rz 30.

denen der Grundrechtekonvent nicht ganz konsequent partielle Schranken bereits in den Text selbst aufgenommen hat.[683]

Im Rahmen der Eingriffsprüfung[684] muss somit in einem ersten Schritt geprüft werden, ob der Anwendungsbereich der Charta betroffen ist und eine Beeinträchtigung eines Grundrechts vorliegt. Die Rechtfertigung der Beeinträchtigung erfolgt in einem zweiten Schritt nach der jeweiligen Schrankenregelung (Art. 52 Abs. 3 im Falle von Rechten, die jenen der EMRK entsprechen bzw. die allgemeine Schrankenregelung des Art. 51 Abs. 1). Da die Eingriffsprüfung im Rahmen der EMRK bereits im vorhergehenden Kapitel dargestellt wurde, soll nun jene der Grundrechtecharta kurz beleuchtet werden.

Eine der Voraussetzungen des Eingriffs ist der Gesetzesvorbehalt (Art. 52 Abs. 1 S 1 GRC). Die Einschränkung kann neben dem unionalen Recht auch durch nationale Gesetze vorgesehen sein, soweit Handlungen eines Mitgliedstaates an den Chartarechten zu messen sind.[685]

Außerdem muss die Einschränkung erforderlich sein und den von der Union anerkannten[686], dem Gemeinwohl dienen Zielsetzungen oder Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen (Art. 52 Abs. 1 S 2 GRC). Diese Zielsetzungen umfassen auch (primär mitgliedstaatliche) Interessen der nationalen Sicherheit bzw. der Aufrechterhaltung der öffentlichen Ordnung, die die Union selbst mangels Kompetenz nicht verfolgen dürfte.[687]

Der Grundsatz der Wesensgehaltgarantie[688] (Art. 52 Abs. 1 S 1 GRC) besagt als weitere Bedingung, dass grundlegende Bestandteile eines Rechts nicht völlig missachtet werden dürfen.[689]

Außerdem ist bei jeder Eingriffsprüfung der Grundsatz der Verhältnismäßigkeit zu beachten (Art. 52 Abs. 1 S 2 GRC). Die gesetzlich vorgesehenen Einschränkungen müssen danach zur Erreichung der legitimer Weise verfolgten Ziele geeignet, erforderlich und angemessen sein.[690] Nach ständiger Rechtsprechung des EuGH dürfen Handlungen der Unionsorgane nicht die Grenzen dessen

[683] Diese spezifischen Schranken stellen Ausformungen des Grundsatzes der Verhältnismäßigkeit dar, siehe *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 15a.
[684] Zum Prüfungsschema siehe auch *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 701.
[685] *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 20.
[686] Zielsetzung des Funktionierens des Binnenmarktes gem. EUV.
[687] *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 21.
[688] Mehrwert der eigenständigen Prüfung der Wesensgehaltsgarantie ist in der Rechtsprechung des EuGH (ABNA ua – C-453/03, Slg. 2005, I-10423, Rz 87) sowie in Teilen der Lehre umstritten, siehe *Bühler*, Einschränkung von Grundrechten nach der Europäischen Grundrechtecharta, S. 257. Eine eigenständige Bedeutung der Wesensgehaltsgarantie argumentiert bspw *Häberle*, Europäische Verfassungslehre (2011), S. 637.
[689] Vgl. EuGH – Kommission/Belgien, C-408/3, Slg. 2006, I-2647 Rz 68.
[690] *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 22b.

überschreiten, was zur Erreichung der mit der fraglichen Regelung zulässigerweise verfolgten Ziele geeignet und erforderlich ist, wobei zu beachten ist, dass dann, wenn mehrere geeignete Maßnahmen zur Auswahl stehen, die am wenigsten belastende zu wählen ist und die verursachten Nachteile nicht außer Verhältnis zu den angestrebten Zielen stehen dürfen.[691]

7.5.2.4. Recht auf Privatsphäre von Unternehmen (Art. 8 EMRK, Art. 7 GRC, Art. 9, 10, 10a StGG)

Der Schutz der Privatsphäre von Personen hat im Rahmen der Grundrechte einen hohen Stellwert. Dieser Umstand wird insbesondere dadurch unterstrichen, dass sich grundrechtliche Gewährleistungen zum Schutze dieses Rechtes im Völkerrecht (Art. 8 EMRK), im Europarecht (Art. 7 GRC) sowie im nationalen Verfassungsrecht (Art. 9, 10, 10a StGG[692]) widerspiegeln.

Gem. Art. 8 EMRK hat jedermann Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seiner Korrespondenz. Dabei sind die Konventionsstaaten nicht nur abwehrrechtlich zum Unterlassen rechtswidriger Eingriffe, sondern auch leistungsrechtlich zum Erbringen positiver Schutzmaßnahmen verpflichtet.[693] Ähnlich erfolgt die Regelung in Art. 7 GRC, wonach jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation[694] hat.[695] Auch hier sind Organe und Einrichtungen der Union als auch die Mitgliedstaaten verpflichtet, Eingriffe zu unterlassen und den positiven Schutz der Privatsphäre durch Gesetzgebung, Rechtsprechung und Verwaltung sicherzustellen.[696]

Die grundsätzliche Feststellung, dass sich der Anwendungsbereich des Art. 8 EMRK und Art. 7 GRC auch auf juristische Personen erstreckt, wurde bereits in den Kapiteln 7.5.2.2 und 7.5.2.3 getroffen. Die weitgehende Gleichstellung juristischer Personen mit natürlichen ist in Art. 7 GRC schon durch

[691] EuGH – Sky Österreich, C-283/11, Rz 50, EuGH – Afton Chemical, C-343/09 – Slg. 2010, I-7027, Rz 45, ua.
[692] Staatsgrundgesetz vom 21. December 1867, über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder, StF RGBl. Nr. 142/1867 idF BGBl. Nr. 684/1988.
[693] *Gusy/Eichenhofer*, Die Einzelnen im Recht der Zivilen Sicherheit, in Gusy/Kugelmann et al. (Hrsg), Rechtshandbuch Zivile Sicherheit (2017), Rz 20.
[694] Um der technischen Entwicklung Rechnung zu tragen, wurde der Begriff „Korrespondenz“ durch „Kommunikaiton“ ersetzt, siehe Erläuterungen zur Charta der Grundrechte, ABl. C 303/17
[695] Aus den Erläuterungen des Präsidiums zu Art. 7 wird deutlich, dass die Vorschrift Art. 8 EMRK nachgebildet ist und auch (nur) deren Bedeutung und Tragweite haben soll (Art. 52 Abs. 3 S. 1).
[696] *Frowein*, Art. 8 EMRK, in Frowein /Peukert (Hrsg), Europäische Menschenrechtskonvention: EMRK-Kommentar (2009), S. 338, 42ff, 49f, 59f und 62.

die Eingangsformulierung „jede Person“ abgesichert[697], während Art. 8 EMRK mit „jedermann“ beginnt.[698]

7.5.2.4.1. Schutz des Privatlebens

Zum einen schützen Art. 8 EMRK als auch Art. 7 GRC das Privatleben, wobei der Schutz personenbezogener Daten als ein spezifisch ausgestalteter Teilbereich dieses Rechts angenommen wird. [699] Auf mögliche Eingriffe in das Recht auf den Schutz personenbezogener Daten (welches insbesondere durch die lex spezialis in Art. 8 GRC näher ausformuliert wird) wird in Kapitel 7.5.2.7 (Eingriff in das Recht des Schutzes personenbezogener Daten) näher eingegangen.

7.5.2.4.2. Schutz der Wohnung

Zum zweiten schützen Art. 8 EMRK und Art. 7 GRC die Wohnung bzw. das Hausrecht.[700] Durch die Rechtsprechung des EGMR[701] (EMRK) als auch des EuGH[702] (GRC) wurde der Begriff der Wohnung mittlerweile auf Betriebs- und Geschäftsräume ausgedehnt. [703]

Ein möglicher Eingriff in dieses Grundrecht besteht durch § 17 Abs. 4 NISG, wonach der Bundesminister für Inneres zur Kontrolle der Einhaltung der Anforderungen nach § 17 Abs. 1 NISG (Treffen geeigneter Sicherheitsvorkehrungen) Einschau in die Netz- und Informationssysteme nehmen kann. Zu diesem Zweck ist er nach vorangegangener Verständigung berechtigt, Örtlichkeiten zu betreten, in denen Netz- und Informationssysteme gelegen sind (§ 17 Abs. 4 S 2). Ob diese Bestimmungen alleine nach den Grundsätzen nationaler Verfassungsbestimmungen (ua. EMRK) oder aber auch nach den Bestimmungen der Grundrechtecharta zu messen ist, richtet sich nach der Frage, ob damit Richtlinientext umgesetzt wurde.

Die NIS-RL selbst regelt dazu in Art. 15 Abs. 1, dass die Mitgliedstaaten sicherzustellen haben, dass die zuständigen Behörden über Befugnisse und Mittel verfügen, die erforderlich sind, um zu

---

[697] Träger des Art. 7 GRC sind vor allem natürliche Personen. Ist die Schutzbedürftigkeit natürlicher und juristischer Personen funktionell vergleichbar, so können auch juristische Personen aus Art. 7 berechtigt sein. Siehe *Guradze*, Die Europäische Menschenrechtskonvention : Konvention zu Schutze der Menschenrechte und Grundfreiheiten nebst Zusatzprotokollen; Kommentar (1968), Art. 8 Rz 5, 14, 24. *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 25.

[698] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 1174.

[699] *Breitenmoser*, Der Schutz der Privatsphäre gemäß Art. 8 EMRK (1986), S. 245. So auch *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 1173. *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 22 Rz 4.

[700] Auf den Schutz des Hausrechts durch Art. 9 StGG bzw. das Gesetz zum Schutze des Hausrechtes wird in dieser Arbeit nicht näher eingegangen.

[701] EGMR, 16.12.1992 – Niemitz/Deutschland – Nr. 72/1991/324/396, Serie A/251B = EGRZ 1993, 65.

[702] EuGH, Rs C-94/00, Slg. 2002, I-9011 (9054, Rz 29) – Roquette Freres.

[703] *Ehlers* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 44. Die Rechtsprechung des EuGH (EuGH, Slg 1989, 2919, Rz 18), die in dieser Frage hinter dem Schutzstandard der EMRK zurückblieb, ist damit nicht aufgegriffen worden, siehe dazu *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 23.

bewerten, ob die Betreiber ihren Pflichten nachkommen. Insbesondere sollen Behörden dabei von Betreibern verlangen können, dass sie Informationen (Art. 15 Abs. 2 lit. a) sowie Nachweise über Ergebnisse durchgeführter Sicherheitsüberprüfungen (Art. 15 Abs. 2 lit. b) zur Verfügung stellen.

Trotz der offensichtlichen Tatsache, dass ein Betreten von Örtlichkeiten im Richtlinientext selbst nicht vorgesehen ist, kann meines Erachtens trotzdem von einer Anwendbarkeit der Charta (neben der Anwendbarkeit von nationalem Verfassungsrecht) ausgegangen werden, da es sich um die grundsätzliche Umsetzung von Unionsrecht in Form des Art. 15 NIS-RL handelt, wenngleich möglicherweise überschreitend.[704]

Das Recht auf Privatsphäre bzw. Achtung der Wohnung wird vor allem aufgrund von Durchsuchungen beeinträchtigt.[705] Eine Durchsuchung ist in diesem Fall nicht vorgesehen, sondern lediglich das Betreten der Örtlichkeiten nach vorangegangener Verständigung. Da das NISG in diesem Zusammenhang lediglich die Anordnungsmöglichkeit der Behörde zum Betreten der Örtlichkeit und keine daran anschließenden Zwangsbefugnisse regelt, stellt sich die Frage, ob der Bundesminister für Inneres die Betriebsräumlichkeiten bei Nichtgewähren des Zutritts auch zwangsweise betreten dürfte. *Adamovich/Funk* führen dazu aus, dass Befehlsgewalt als verfahrensfreier Verwaltungsakt in verschiedenen Formen auftreten kann. Die Durchsetzung mit Zwangsgewalt sei nur zulässig, wenn dies auch gesetzlich geregelt ist. Eine andere Form verfahrensfreier Anordnungen seien jene, deren Nichtbefolgung lediglich mit Verwaltungsstrafe bedroht seien[706], wie dies auch in gegenständlichem Fall zutrifft. Stimmt der Betreiber somit dem Betreten der Räumlichkeiten nicht zu, besteht für die Behörde keine Möglichkeit, diese zwangsweise zu betreten. [707]

Trotz fehlender Regelung einer (heimlichen) Durchsuchungsermächtigung oder einer zwangsweisen Durchsuchung kann von einem Eingriff in die Achtung der Privatsphäre von Unternehmen ausgegangen werden, insbesondere da die Verweigerung der Einschau durch den Betreiber eine Verwaltungsstrafe gem. § 26 Abs. 1 Z 3 NISG zur Folge hat.

Da es sich bei Art. 7 GRC um ein aus der EMRK (Art. 8 EMRK) entlehntes Recht handelt,[708] ist das Eingriffsschema der EMRK anzuwenden (Art. 52 Abs. 3 GRC). Die geforderte gesetzliche Grundlage findet sich wie besprochen in § 17 Abs. 4 NISG. Die legitimen Ziele für Eingriffe in das Hausrecht sind in Art. 8 Abs. 2 EMRK taxativ geregelt, wobei die Ziele der nationalen Sicherheit sowie die

[704] Zu den Ausführungen zur Anwendbarkeit der GRC bei nationalen Sachverhalten siehe Kapitel 7.5.2.3.
[705] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 1331.
[706] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 50.052.
[707] Siehe dazu auch Kapitel 7.5.4.5.
[708] Siehe RL (EU) 2007/2007/C 303/02; Erläuterungen zur Charta der Grundrechte, Art. 7 GRC.

öffentliche Ruhe und Ordnung in Betracht kommen. Das Betreten der Örtlichkeiten dient der Einschau, ob die festgelegten Sicherheitsstandards von Betreibern wesentlicher Dienste eingehalten werden. Deren Einhaltung dient grundsätzlich dem Zweck, das Funktionieren dieser Dienste zu gewährleisten und mögliche schwerwiegende Auswirkungen auf die Gesellschaft zu verhindern, die auch Folgen für die öffentliche Ruhe und Ordnung sowie die nationale Sicherheit generell haben können.[709]

Als dritte Voraussetzung des Eingriffes in das Grundrecht ist der Verhältnismäßigkeitsgrundsatz zu beachten. § 17 Abs. 4 S 3 NISG sieht dazu vor, dass die Einschau in dem unbedingt erforderlichen Ausmaß zu erfolgen hat und unter möglichster Schonung der Rechte der betroffenen Einrichtung und Dritter sowie des Betriebes auszuüben ist.

Dies reicht jedoch meines Erachtens nicht aus. Einerseits scheitert der Eingriff bereits an der Eignung zur Zielerreichung. Das Betreten von Örtlichkeiten, an denen Netz- und Informationssysteme gelegen sind, kann kaum darüber Auskunft geben, ob diese die geforderten Sicherheitsstandards gem. § 17 Abs. 1 NISG erfüllen. Dies kann möglicherweise noch für die physische Sicherheit gelten, bei denen es sich jedoch nur um eine von elf zu überprüfenden Kategorien handelt.[710] Für andere Maßnahmen, wie eine Risikoanalyse, Personalwesen, Umgang mit Dienstleistern oder die Systemadministration, gilt dies keineswegs.

Das geeignetere und auch im Rahmen der Verhältnismäßigkeitsprüfung gelindere Mittel wäre in diesem Fällen die Einschau in die Unterlagen der Betreiber. Erschwerend kommt in diesen Fällen noch hinzu, dass vom Betreten oftmals Dritte (externe IT-Dienstleister) betroffen sein werden, deren Dienstleistung von Betreibern wesentlicher Dienste in Anspruch genommen werden und in deren Betriebsräumlichkeiten somit die Überprüfung erfolgt. Darüber hinaus erfolgt die Überprüfung der Vorkehrungen ohnedies durch qualifizierte Stellen (§ 18 NISG).[711] Warum der Bundesminister für Inneres hier trotzdem nochmals selbst und anlassunabhängig Einschau halten möchte, ist wohl nur durch eine abermalige eigenständige Kontrollmöglichkeit zu erklären und mE als unverhältnismäßig zu werten.

Somit kann aus meiner Sicht festgehalten werden, dass die in § 17 Abs. 4 NISG geregelte Maßnahme der Einschau in Örtlichkeiten bei Betreibern durch den Bundesminister für Inneres aus oben dargestellten Gründen der Unverhältnismäßigkeit gegen Art. 8 EMRK, und sofern eine Anwendbarkeit der Grundrechtecharta angenommen wird, gegen Art. 7 GRC verstößt.

---

[709] Durch den längeren Ausfall der Stromversorgung kann es zu Plünderungsdiebstählen, durch den längeren Ausfall des öffentlichen Verkehrs kann der Straßenverkehr zum Erliegen kommen, etc.
[710] Siehe Anlage 1 Netz- und Informationssystemsicherheitsverordnung (NISV), Punkt 7.
[711] Zur Überprüfung durch qualifizierte Stellen siehe Kapitel 7.5.5.

Eine darüberhinausgehende Prüfung der Bestimmungen des Staatsgrundgesetzes unterbleibt hier.

7.5.2.4.3. Schutz der Korrespondenz/Kommunikation

Art. 8 EMRK bzw. Art. 7 GRC schützen außerdem die Korrespondenz bzw. die Kommunikation als Teil des Privatlebens. Diese Begriffe sind entsprechend weit auszulegen.[712] Aufgrund der technischen Entwicklung[713] sind daher nicht mehr nur der Briefverkehr und Telefonie, sondern auch Kommunikation per Email sowie Internettelefonie vom Grundrecht umfasst. [714] Im persönlichen Anwendungsbereich befinden sich – wie bereits in Kapitel 7.5.2.2 (Einleitende Anmerkungen zur EMRK) grundsätzlich angemerkt - auch juristische Personen. [715] Der Schutz greift nach herrschender Lehre nur für heimliche Überwachungsmaßnahmen. [716]

Vom Grundrecht erfasst ist der Schutz privater Kommunikation, der die Kontaktaufnahme und den Informationsaustausch mit anderen beinhaltet. [717] Im Falle juristischer Personen ist somit die geschäftliche Kommunikation geschützt. Darüber hinaus sind bei Unternehmen selbstverständlich auch von Mitarbeitern vom Arbeitsplatz verschickte (private) Emails (als Teil von deren Privatleben) umfasst.[718]

Ein Eingriff in gegenständliches Grundrecht könnte möglicherweise durch den Betrieb von IKT-Lösungen zur Vorbeugung von Sicherheitsvorfällen (§ 13 NISG) vorliegen. Da sich im Richtlinientext selbst keine gleichlautende Bestimmung findet und es sich bei dieser nationalen Regelung somit nicht annähernd um Umsetzung von Unionsrecht handelt, ist von einer Anwendung der Charta meines Erachtens abzusehen,[719] wenngleich selbstverständlich eine Anwendbarkeit des nationalen Verfassungsrechtes (Art. 8 EMRK sowie Art. 10, 10a StGG) bestehen bleibt.

Gem. § 13 NISG kann der Bundesminister für Inneres IKT-Lösungen betreiben, um Risiken oder Vorfälle frühzeitig zu erkennen, wobei Betreiber wesentlicher Dienste an diesen IKT-Lösungen teilnehmen und dabei festlegen können, welche Daten an die Behörde übermittelt werden. Wie

---

[712] *Breitenmoser*, Der Schutz der Privatsphäre gemäß Art. 8 EMRK, S. 307. *Frowein* in Frowein /Peukert, Europäische Menschenrechtskonvention: EMRK-Kommentar, Art. 8 Rz 48. *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 22 Rz 24f.

[713] *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 24.

[714] *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 22 Rz 25.

[715] Für eine Zurückschneidung des Begriffes auf die reine Kommunikation unter Privatpersonen besteht aufgrund der offenen Formulierung kein Anlass, siehe *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 1173.

[716] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 1348 u. 248.

[717] *Kugelmann* in *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, S. 13.

[718] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 1248.

[719] Siehe dazu Kapitel 7.5.2.3.

bereits in Kapitel 7.3.1 (Betrieb von IKT-Lösungen) dargelegt, handelt es sich bei dieser Bestimmung um die Einrichtung eines Sensornetzwerks.

Da eine Teilnahme von Unternehmen lediglich auf freiwilliger Basis vorgesehen ist, kann nicht von einem Eingriff in Art. 8 EMRK ausgegangen werden. Nichtsdestotrotz soll kurz auf das Eingriffspotenzial dieser Bestimmung eingegangen werden, insbesondere, weil nicht ausgeschlossen werden kann, dass der Gesetzgeber bei unzureichender freiwilliger Beteiligung eine gesetzliche Verpflichtung der Teilnahme regeln könnte.

Die Funktionsweise des Sensornetzwerks kann im dies betreffenden Kapitel 7.3.1 (Betrieb von IKT-Lösungen) nochmals nachgelesen werden. Zusammenfassend sei festgestellt, dass ein Sensor (eine IKT-Lösung) vor dem Netz des Betreibers installiert werden soll, um den gesamten Datenverkehr auf mögliche Bedrohungen (bspw. Schadsoftware) zu untersuchen. Diese Untersuchung erfolgt nur anhand der Metadaten der durchlaufenden IP-Pakete.

Einen Eingriff in das Grundrecht bildet nur jede Art von Kontrolle, Zensur, Anhalten oder verzögerter Weitergabe von Kommunikation[720] – hierunter fallen das Öffnen[721], Lesen[722] und Kopieren[723] sowie Verzögerungen bei der Übermittlung.[724]

Bei der Überprüfung der Metadaten im Rahmen des Sensornetzwerks kommt es gerade nicht zum Öffnen[725], Lesen, Verarbeiten oder gar Analysieren der Daten. Ebenso wenig ist eine Verzögerung bei der Übermittlung anzunehmen, da es sich bei diesem Vorgang wohl nur um (im Rahmen der Datenverarbeitung übliche) wenige Millisekunden handeln wird.

Frenz[726] sieht gar im einzelnen IP-Paket selbst keine Korrespondenz, da eine Nachricht, die eine hinter dem Kommunikationsvorgang stehende natürliche Person[727] senden möchte, eben nicht in dem einzelnen IP-Paket bestünde. Dem kann man sich wohl nur insoweit anschließen, als der Eingriff selbst nur ein einzelnes IP-Paket betrifft. Würde der gesamte Datenstrom – und somit mehrere zusammenhängende IP-Pakete – verarbeitet, wäre meines Erachtens sehr wohl von einem Eingriff auszugehen, da daraus auf den Kommunikationsvorgang selbst geschlossen werden kann.

[720] Ursprünglich von Briefen.
[721] EGMR, 19.4.2001, Peers/GRE, Nr. 28524/95, Z. 81.
[722] EGMR, 25.3.1992, Campbell/GBR, Nr. 13590/88, Z. 33.
[723] EGMR, 20.6.2000, Foxley/GBR, Nr. 33274/96, Z. 30.
[724] *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, Rz 27.
[725] Insbesondere eine Entschlüsselung der Kommunikation ist nicht vorgesehen.
[726] *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, S. 17.
[727] Dies betrifft gleichwohl juristische Personen.

Darüber hinaus ist festzuhalten, dass die Schutzfunktion des Grundrechts grundsätzlich für alle übertragenen Daten gelten soll, [728] da es während des Übermittlungsvorgangs technisch nicht möglich ist, zwischen Datenströmen, die Individualkommunikation übertragen, und anderen Datenströmen zu unterscheiden.[729]

Gegenständliches Sensornetzwerk ist wohl nicht mit dem vom britischen Geheimdienst verwendeten Programm TEMPORA[730] zu vergleichen, welches Datenströme mit dem Ziel abfängt, auf Inhalte von Emails, Verbindungsdaten etc. zuzugreifen und dabei direkt auf die transatlantischen Glasfaserverbindungen zugreift, die Knotenpunkte des Internets darstellen.[731]

Aus bereits weiter oben genannten Gründen der Freiwilligkeit, aber auch des fehlenden Eingriffes durch tatsächlichen Zugriff auf Inhaltsdaten ist von keinem Eingriff in gegenständliches Grundrecht auszugehen.

7.5.2.5. Recht auf Freiheit des Eigentums (Art. 1 ZP Nr. 1 EMRK, Art. 17 GRC, Art. 5 StGG)

Neben Art. 1 1. Zusatzprotokoll EMRK[732] schützt auch Art. 17 GRC das Eigentumsrecht[733], bei dem es sich um eines der wirtschaftlichen Grundrechte der Grundrechtecharta handelt.[734] Das Eigentumsrecht umfasst nicht nur den Bestand der Eigentumsposition, sondern auch die Befugnis, sie zu nutzen und darüber zu verfügen.[735]

Art. 1 1. ZP EMRK erwähnt ausdrücklich juristische Personen als Grundrechtsträger. Da in den Erläuterungen zu Grundrechtecharta explizit darauf hingewiesen wurde, dass Art. 17 aufgrund Art. 52 Abs. 3 GRC die gleiche Bedeutung und Tragweite wie Art. 1 1. ZP EMRK haben soll, gilt dies auch für die Bestimmung der GRC. [736]

---

[728] *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, S. 113.
[729] EGMR stellte einen Eingriff in Recht auf Achtung der Korrespondenz fest, ohne einen konkreten Nachweis zu verlangen, dass Korrespondenz zumindest auch betroffen war, siehe EGMR, 16.10.2007, 74336/01 (Wieser und Bicos Beteiligungen GmbH/AUT, Rz 45; EGMR, 14.3.2013, 24117/08 (Bernh Larsen Holding AS ua/NOR), Rz 105.
[730] EGMR, 7.1.2014, 58170/13 (Big Brother Watch ua/UK).
[731] *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, S. 111.
[732] BGBl. 1958/2010.
[733] Das Eigentumsrecht ist tief in der Rechtsgeschichte der europäischen Rechtsfamilie verwurzelt und hat in allen Mitgliedstaaten – mit Ausnahme Großbritanniens – Verfassungsrang, siehe *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2778.
[734] Ö ratifizierte das 1. Zusatzprotokoll 1958.
[735] *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 16.
[736] RL (EU) 2007/2007/C 303/02; Erläuterungen zur Charta der Grundrechte. Siehe dazu auch *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2806. EuGH, Slg 1979, 3727 Rz 14ff ua.

Durch die weite Fassung des Schutzbereichs werden grundsätzlich auch wirtschaftliche Interessen, die den Betrieb eines Unternehmens betreffen, durch die Eigentumsfreiheit geschützt.[737] Der EGMR vertritt neuerdings auch die Auffassung, der Schutz des Eigentums in Art. 1 ZP Nr. 1 zur EMRK umfasse auch das Recht, Verträge zu schließen, und unter bestimmten Voraussetzungen das Recht, ein Unternehmen zu betreiben.[738] Auch vom Schutzbereich des Eigentums erfasst werden die geschäftlichen Beziehungen, die sich ein Unternehmen oder ein Unternehmer in der Vergangenheit erarbeitet hat und die den Vermögenswert des Geschäfts über den reinen Substanzwert hinaus beeinflussen.[739]

Ein Eingriff in das Grundrecht auf Eigentum durch die NIS-RL bzw. das NISG kommt einerseits insofern in Betracht, als Betreiber die (zumeist in ihrem Eigentum stehende) Netz- und Informationssysteme umrüsten müssen, sodass diese den in Art. 14 NIS-RL bzw. § 17 Abs. 1 NISG vorgesehenen technischen und organisatorischen Sicherheitsvorkehrungen entsprechen.

Ein Eingriff[740] in das Grundrecht auf Eigentum liegt vor, wenn eine eigentumsfähige Position entzogen oder ihre Nutzung, Verfügung oder Verwertung Beschränkungen[741] unterworfen wird.[742] Ebenso ist das Eigentumsgrundrecht beeinträchtigt, wenn die Nutzung der Produktionsstätten und –anlagen des Gewerbebetriebes unmittelbar betroffen ist.[743] Einen Eingriff stellen auch Nutzungsregelungen in Form hoheitlicher Maßnahmen dar, die einen bestimmten Gebrauch des Eigentums gebieten oder untersagen.[744]

Ein Eingriff in das Eigentumsrecht könnte durch die hoheitliche Anordnung des Treffens bestimmter Maßnahmen hinsichtlich der Netz- und Informationssysteme begründet werden. Der Betreiber als juristische Person kann seine Systeme (bzw. als sein Eigentum) nicht in der ihm gewünschten Form nutzen, sondern hat sich nach den Beschränkungen und Auflagen der Behörden zu richten.

---

[737] *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 26 Rz 31.
[738] Urt. V. 25.3.1999 – Iatridis/Griechenland – Appl. Nr. 31107/96;
[739] EGMR, EuGRZ 1988, 35ff – van Marke; siehe auch *Wegener*, § 5 Wirtschaftsgrundrechte, in Ehlers (Hrsg), Europäische Grundrechte und Grundfreiheiten (2014), Rz 11.
[740] Art. 1 1. ZP EMRK unterscheidet drei Arten von Eingriffen in die Eigentumsgarantie: Enteignungen, Nutzungsregelungen und sonstige Eingriffe.
[741] Einschränkung der Nutzung kann zeitlich, räumlich oder sachlich erfolgen.
[742] *Calliess*, § 20 Eigentumsgrundrecht, in Ehlers (Hrsg), Europäische Grundrechte und Grundfreiheiten (2014), Rz 25.
[743] *Calliess* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 21.
[744] *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 25 Rz 12. *Calliess* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 3.

Da es sich um einen Eingriff in den Schutzbereich des Grundrechts handelt, ist dieser auf seine Rechtmäßigkeit hin zu prüfen.[745] Bloße Nutzungsbeschränkungen des Eigentums sind nach ständiger Rechtsprechung des EuGH rechtmäßig, wenn sie tatsächlich dem Gemeinwohl dienenden Zielen der Gemeinschaft entsprechen und nicht einen im Hinblick auf die verfolgten Ziele unverhältnismäßigen, nicht tragbaren Eingriff darstellen, der die so gewährleisteten Rechte in ihrem Wesensgehalt[746] antastet[747].

Wie bereits mehrmals in der Arbeit dargestellt, erscheinen die vorgesehenen Sicherheitsvorkehrungen nicht nur aus gesellschaftlichen, der öffentlichen Ruhe und Ordnung dienen Gründen erforderlich. Es liegt wohl auch im eigenen Interesse der Unternehmen, Netz- und Informationssysteme zu betreiben, deren Ausfall nicht zu Betriebs- oder Produktionsstillständen führt. Eine tatsächliche Nutzungsbeschränkung oder Entziehung des Eigentums als schwerwiegender Eingriff ist gerade nicht vorgesehen.

Aus diesem Grund kann meines Erachtens von einem rechtmäßigen Eingriff in das Recht auf Eigentum ausgegangen werden.

Eine weitere Bestimmung mit Potenzial zum Eingriff in das Grundrecht auf Eigentum stellt die Veröffentlichung von Sicherheitsvorfällen dar, auf die nochmals in den Ausführungen zum Schutz personenbezogener Daten (Kapitel 7.5.2.7 [Schutz personenbezogener Daten]) einzugehen sein wird.

Gem. Art. 14 Abs. 6 NIS-RL bzw. § 10 Abs. 1 NISG können die Behörden nach Anhörung des vom Sicherheitsvorfall betroffenen Betreibers Informationen darüber veröffentlichen, um die Öffentlichkeit über Sicherheitsvorfälle zu unterrichten, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von Sicherheitsvorfällen erforderlich ist, oder die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt (§ 10 Abs. 1 NISG).

[745] Art. 1 Abs. 1 S. 2 und Abs. 2 ZP Nr. 1 zur EMRK enthalten sachgebietsbezogene Ausformungen des Verhältnismäßigkeitsgrundsatzes, sodass Art. 52 Abs. 3 S. 1 zur Anwendung gelangt und der Rückgriff auf die allgemeine Einschränkungsregelung des Art. 52 Abs. 1 versperrt ist. Dies ist aber umstritten, siehe *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 19.

[746] Unberührt bleibt der Wesensgehalt, wenn die Maßnahme nur die Modalitäten der Ausübung (des Eigentumsrechts) betrifft, ohne dessen Bestand selbst zu gefährden, siehe EuGH, Slg 1994, I-5555, Rz 24 – SMW Winzersekt;

[747] Ständige Rechtsprechung des EuGH, siehe bspw. EuGH, Slg 1998, I-1953, Rz 21 – Metronome Musik; Slg 1998, I-7976, Rz 79 – Generics.

Nach Rechtsprechung des EGMR stellen Maßnahmen, die negative Auswirkungen auf den Firmenwert haben, ebenso einen Eingriff in die Eigentumsgarantie dar.[748] Auch Beeinträchtigungen des Goodwill sowie des Kundenstamms eines Unternehmens sind Eingriffe in das Eigentumsrecht,[749] jedoch nur dann, wenn das Unternehmen in seiner Substanz betroffen oder zumindest bedroht ist.[750] Andere Meinungen sprechen davon, dass bereits jede Beeinträchtigung der Rentabilität oder des Wertes des Unternehmens eine Beeinträchtigung eigentumsrechtlicher Positionen darstellt.[751]

Die Veröffentlichung von Sicherheitsvorfällen kann immense Auswirkungen auf den Wert von Unternehmen haben, sofern dadurch Rückschlüsse auf deren Angreifbarkeit, verwundbare Systeme und sorgloser Umgang mit Sicherheit bzw. dem Schutz von Kundendaten gezogen werden können bzw. gezogen werden. Somit liegt meines Erachtens jedenfalls ein Eingriff in den Schutzbereich des Eigentumsrechts vor.

Als legitimes Ziel des Eingriffes kann die Verhinderung von strafbaren Handlungen sowie die öffentliche Ruhe und Ordnung genannt werden. Die Maßnahme erscheint auch zur Zielerreichung geeignet. Durch die Sensibilisierung der breiten Öffentlichkeit, insbesondere auch anderer Unternehmen, können diese sich auf mögliche auch sie betreffende Angriffe und Vorfälle vorbereiten und diesen insofern vorbeugen.

So stellt sich abschließend noch die Frage der Verhältnismäßigkeit bzw. des gelindesten Mittels. Diese kann nur als gegeben betrachtet werden, sofern die namentliche Nennung des vom Vorfall betroffenen Unternehmens möglichst unterbleibt (freilich wäre in diesem Fall der Unternehmenswert nicht von einer Beeinträchtigung betroffen, da das Unternehmen nicht bekannt werden würde) und ausschließlich nur für jene Fälle erfolgt, sofern dies aus oben genannten Gründen unbedingt erforderlich ist. Diese Verhältnismäßigkeit wird im Einzelfall zu beurteilen sein.

Zusammenfassend lässt sich somit feststellen, dass es weder durch die Regelungen im Richtlinientext als auch in der nationalen Umsetzung zu Eingriffen in das Recht auf Eigentum kommt.

[748] EGMR, 7.7.1989, Tre Traktörer Aktiebolag/SWE, Nr. 10873/84, Z. 53.
[749] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2847.
[750] *Jarass*, Charta der Grundrechte der Europäischen Union : Kommentar[2], § 22 Rz 13. EuGH, Rs C-363/01, Slg. 2003, I-11893 (11937) – Flughafen Hannover ua.
[751] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2848.

7.5.2.6. Recht auf unternehmerische Freiheit, Erwerbsausübungsfreiheit und Berufsfreiheit (Art. 16 GRC, Art. 6, 18 StGG)

Das Recht auf unternehmerische Freiheit, das systematisch eine Klammer zwischen der Berufsfreiheit (Art. 15 GRC – dazu weiter unten) und dem Eigentumsrecht (Art. 17 GRC – vorhergehendes Kapitel) schafft, wird unionsrechtlich anerkannt.[752] Vom Schutzbereich erfasst wird jede selbstständige wirtschaftliche Betätigung, ohne Rücksicht auf Art und Umfang, Rechtsform und Finanzierung des Unternehmens.[753] Mitumfasst vom Schutzbereich ist nach Rechtsprechung des EuGH auch der Schutz von Geschäftsgeheimnissen[754] und Geschäftsunterlagen[755]. Dass sich juristische Personen im persönlichen Schutzbereich des Grundrechts befinden, ist somit unbestritten. [756]

Hinzuweisen ist auf die Abgrenzung zu Art. 15 GRC (Berufsfreiheit). Durch die Schaffung der unternehmerischen Freiheit in Art. 16 wurde der persönliche Anwendungsbereich des Art. 15 Abs. 1 auf unselbstständig beruflich Tätige beschränkt,[757] der ursprünglich natürliche und juristische Personen betrifft.[758] Es liegt nahe, Art. 16 GRC in Bezug auf die unternehmerische Freiheit als lex specialis zu Art. 15 zu sehen.[759] Die Berufsfreiheit (Art. 15) umfasst das Recht, zu arbeiten und einen frei gewählten oder angenommenen Beruf auszuüben, während die unternehmerische Freiheit auf die Ausübung einer Wirtschafts- oder Geschäftstätigkeit gerichtet ist und zudem die Vertragsfreiheit sowie die Freiheit des Wettbewerbs beinhaltet.[760]

In der EMRK finden sich kein derartiges Grundrecht, wobei Einschränkung bislang mitunter auf das Eigentumsrecht (Art. 1 1. ZP EMRK) gestützt wurden. [761]

---

[752] Zur frühzeitigen Anerkennung der wirtschaftlichen Betätigungsfreiheit siehe EuGH, Rs 4/73, Slg. 1974, 491 – Nold; Rs 230/78, Slg. 1979, 279 – Eridania, Rs C-317/00 P®, Slg. 2000, I-9541 – Invest, ua. Zur frühzeitigen Anerkennung der Unternehmensfreiheit siehe EuGH, Rs C-143/88 u. 92/89, Slg. 1991, I-415 – Süderdithmarschen.

[753] *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Art. 16 Rz 10a.

[754] EuGH, Rs C-450/06, EuGRZ 2008, 136 (138) – Varec.

[755] EuGH, Rs C-435/02 u. 103/03, Slg. 2004, I-8663 (8683) – Axel Springer Verlag. Folgerichtig, da der Schutz von Betriebsgeheimnissen und Geschäftsunterlagen die Erhaltung marktwirtschaftlich erarbeiteter Wettbewerbsvorteile sichert, siehe *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2722.

[756] *Ruffert*, § 19 Berufsfreiheit und unternehmerische Freiheit, in Ehlers (Hrsg), Europäische Grundrechte und Grundfreiheiten (2014), Rz 25.

[757] *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Art. 15 Rz 13.

[758] EuGH, Rs C-280/93, Slg. 1994, I-4973 – Bananen; so auch *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2534.

[759] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2505.

[760] *Schwarze*, Europäische Zeitschrift für Wirtschaftsrecht, 2001, S. 519

[761] EGMR, Urt. V. 25.3.1999, Nr. 31107/96 (Rz 55), EuGRZ 1999, 316 (317) – Iatridis/Griechenland.

Art. 16 GRC steht als Ausdruck des Prinzips freien Wettbewerbs grundsätzlich Regelungen entgegen, die den freien Wettbewerb einschränken, ebenso Einschränkungen im Bereich von Erzeugungs- und Produktionsvorschriften.[762]

Ein Eingriff durch Bestimmungen der NIS-RL bzw. des NIS-Gesetzes sind durch die zwingende Überprüfung der eigenen Sicherheitsvorkehrungen durch qualifizierte Stellen denkbar. Wo die Richtlinie den Nachweis der Sicherheitsvorkehrungen sehr offen formuliert und keine konkreten Maßnahmen vorsieht (Art. 14 NIS-RL), regelt das NIS-Gesetz den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen (§ 17 Abs. 3 NISG).

Wie bereits in Kapitel 7.5.5 erläutert, können nach wörtlicher Interpretation des § 17 Abs. 3 NISG Sicherheitsvorkehrungen entweder durch Zertifizierungen, wo solche bestehen, oder durch Überprüfungen durch qualifizierte Stellen erfolgen. Da Zertifizierungen nicht für alle Kategorien der Sicherheitsvorkehrungen laut NISV[763] existieren, haben Betreiber jedenfalls (auch) auf qualifizierte Stellen zurückzugreifen. Dabei handelt es sich um (eine begrenzte Anzahl) juristischer Personen, die gewisse Voraussetzungen zu erfüllen haben (§ 18 NISG) und vom Bundesminister für Inneres per Bescheid als solche anerkannt werden.

Durch diese Regelung könnte in das Recht auf unternehmerische Freiheit eingegriffen werden. Ein Teilaspekt der unternehmerischen Freiheit ist auch die Vertragsfreiheit[764], welche die Wahl des Geschäftspartners als essentielle Garantie einer offenen Marktwirtschaft mit freiem Wettbewerb umfasst.[765] Obwohl der Gedanke im ersten Moment weit hergeholt erscheint, soll der Vollständigkeit halber geprüft werden, ob möglicherweise in die Freiheit des Betreibers eingegriffen wird, frei zu entscheiden, welches Unternehmen er mit der Überprüfung seiner Systeme beauftragt, indem lediglich eine begrenzte Zahl von durch die Behörden dazu anerkannten Unternehmen zur Verfügung steht, soll im nächsten Schritt die Rechtfertigung dieses möglichen Eingriffes[766] überprüft werden.[767]

[762] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2745.
[763] Anhang I NISV.
[764] RL (EU) 2007/2007/C 303/02; Erläuterungen zur Charta der Grundrechte.
[765] *Ganglbauer*, Das Grundrecht der unternehmerischen Freiheit gem. Art. 16 GRC, in Kahl/Raschauer et al. (Hrsg), Grundsatzfragen der europäischen Grundrechtecharta (2013), S. 211.
[766] Art. 16 kann einer Vielzahl von Eingriffen der öffentlichen Gewalt unterworfen sein, siehe EuGH – Sky Österreich, C-283/11, Rz 36ff., 47.
[767] Die grundsätzliche Anwendbarkeit der GRC ist unproblematisch, da es sich bei der Überprüfung von Sicherheitsvorkehrungen um Umsetzung des Art. 14 NIS-RL und somit Gemeinschaftsrecht handelt.

Auffallend ist, dass Art. 16 GRC einen (eigenen) Vorbehalt zugunsten des Unionsrechts sowie einzelstaatlicher Rechtsvorschriften und Gepflogenheiten enthält.[768] Da keine gleichlautende Bestimmung der EMRK existiert (Art. 52 Abs. 3), kommt zusätzlich die allgemeine Schrankenregelung des Art. 52 Abs. 1 GRC[769] hinzu („doppelte Schranken") zum Tragen.[770]

Die bestehende Gesetzesgrundlage ist mit § 17 Abs. 3 NISG gegeben. Zusätzlich muss die Beschränkung tatsächlich dem Gemeinwohl dienenden Zielen entsprechen und nicht einen im Hinblick auf den verfolgten Zweck unverhältnismäßigen, nicht tragbaren Eingriff darstellen, der die unternehmerische Freiheit in ihrem Wesensgehalt antastet.[771] Die Verhältnismäßigkeit wird wie bereits bei den Grundrechten zuvor mit Vorliegen der Eignung, Erforderlichkeit und Angemessenheit bewertet.

Dass jene Stellen, die die Überprüfung von (im NIS-Gesetz bzw. der NIS-Verordnung) neu definierten Sicherheitsvorkehrungen vornehmen, selbst gewisse Voraussetzungen erfüllen sollten, liegt meines Erachtens auf der Hand. Da die staatlichen Stellen eben nicht selbst diese Überprüfungen vornehmen, sondern sich dabei auf die so genannten qualifizierten Stellen verlassen, sollten für diese Stellen eben auch gewisse Voraussetzungen – wie fachspezifische Kenntnisse/Ausbildungen, eigene sichere Systeme etc.[772] – gelten. Da darüber hinaus jedes Unternehmen die Möglichkeit hat, einen Antrag auf Anerkennung als qualifizierte Stelle beim Bundesminister für Inneres zu stellen, erscheinen die vertraglichen Möglichkeiten für Betreiber wesentlicher Dienste auch entsprechend weit. Die geforderte Wesensgehaltsgarantie wird darüber hinaus nur verletzt, wenn dem Betroffenen seine unternehmerische Tätigkeit zur Gänze versagt wird,[773] wovon im gegenständlichen Fall nicht ausgegangen werden kann.

In diesem Zusammenhang sollen auch die nationalen Grundrechte der Erwerbsausübungsfreiheit (Art. 6 StGG) sowie der Berufsfreiheit (Art. 18 StGG) Erwähnung finden. Art. 6 ermöglicht es jedem Staatsbürger, unter den gesetzlichen Bedingungen jeden Erwerbszweig auszuüben. Dabei wird jede

[768] Hier sollte offenbar dem Subsidiaritätsprinzip Rechnung getragen werden, siehe *Schwarze*, Europäische Zeitschrift für Wirtschaftsrecht, 2001

[769] Zur Diskussion eines unterschiedlichen Verständnisses der Schrankenregelung in Art. 16 GRC siehe *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2660ff.

[770] Ein Teil der Lehre sieht diesen Vorbehalt als Ausgestaltungs- und Regelungsvorbehalt an, ein anderer Teil nimmt die Existenz einer grundrechtlichen unternehmerischen Freiheitssphäre an, wobei Art. 16 GRC als neben die Schrankenregelung des Art. 52 GRC tretende Beschränkungsmöglichkeit tritt, siehe dazu *Ganglbauer* in Kahl/Raschauer et al., Grundsatzfragen der europäischen Grundrechtecharta, S. 218.

[771] Ständige Rechtsprechung ua. EuGH, Rs C-184 u. 223/02, Slg. 2004 I-7789 (7847) – Spanien u. Finnland.

[772] Verordnung des Bundesministers für Inneres zur Festlegung der Erfordernisse und besonderer Kriterien für qualifizierte Stellen nach dem Netz- und Informationssystemsicherheitsgesetz (Verordnung über qualifizierte Stellen – QuaSteV), StF: BGBl. II Nr. 226/2019.

[773] *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 2765.

Tätigkeit geschützt, die auf wirtschaftlichen Erfolg gerichtet ist und damit jede Art, Vermögen zu erwerben.[774] Das Grundrecht kann nach der jüngeren Judikatur des VfGH[775] verfassungsrechtlich einwandfrei eingeschränkt werden, solange dadurch nicht der Wesensgehalt des Grundrechts berührt oder in anderer Weise gegen einen den Gesetzgeber bindenden Verfassungsgrundsatz verstoßen wird.[776] Im Rahmen dessen kann der Gesetzgeber eine Regelung der Ausübung der Berufe vornehmen, eine solche Berufsausübung nur unter bestimmten Voraussetzungen gestatten und alle Personen, die diese Voraussetzungen nicht erfüllen, von der Berufsausübung ausschließen.[777] Beschränkungen sind nach der ständigen Rechtsprechung des VfGH jedoch nur zulässig, wenn sie durch ein öffentliches Interesse geboten, zur Zielerreichung geeignet, adäquat und auch sonst sachlich zu rechtfertigen sind.[778] Zur Zulässigkeit einer möglichen Einschränkung wird auf die Diskussion oben zu den Bestimmungen der GRC verwiesen.

Die Berufsfreiheit gem. Art. 18 StGG kommt für gegenständliche Diskussion ohnedies nicht in Frage, da diese nur natürlichen Personen zusteht.[779]

7.5.2.7. Schutz personenbezogener Daten (Art. 16 AEUV, Art. 7, 8 GRC, DSGVO, Art. 8 EMRK, § 1 DSG)

Das Grundrecht auf Datenschutz findet sich in den verschiedensten Rechtsmaterien. Dies ist nur ein Indiz dafür, dass es sich um einen sehr komplexen Themenbereich handelt.

Im Folgenden soll hauptsächlich die Anwendbarkeit des Rechts auf Datenschutz für juristische Personen untersucht, die Regelungsbereiche der verschiedenen den Datenschutz betreffenden Grundrechte abgegrenzt sowie mögliche Eingriffe durch Bestimmungen der NIS-RL und des NIS-Gesetz untersucht werden. Nicht eingegangen werden soll dabei auf die grundsätzlichen behördlichen Datenverarbeitungsbestimmungen des NIS-Gesetzes (§§ 10ff NISG).[780]

---

[774] Siehe etwa *Grabenwarter/Holoubek*, Verfassungsrecht - Allgemeines Verwaltungsrecht[2] (2014), Rz 497. *Bezemek*, Die Erwerbsfreiheit im StGG - Schutzgegenstand und Stellung, Juristische Blätter, 8/2014, S. 477

[775] VfGH 4.10.1984, G70/84, S. 21f; 7.3.1985, B251/83, S. 12.

[776] VfSlg 10932/1986.

[777] VfSlg 4011/1961.

[778] VfGH 5.3,.1987 G174/86; 1.3.1988, G79/87.

[779] VfSlg 8967/1980.

[780] Eine eingehende Untersuchung der Bestimmungen zur Datenverarbeitung (§§ 10, 11, 12 NISG) würde den Umfang einer eigenständigen wissenschaftlichen Arbeit darstellen. Der Fokus soll vielmehr auf jene Bestimmungen gelegt werden, die Betreiber wesentlicher Dienste „unmittelbarer“ betreffen.

Bereits in ihren Schlussfolgerungen stellte die Europäische Datenschutzbeauftragte fest, dass die NIS-RL wesentlich zur Wahrung der Rechte natürlicher Personen auf Schutz der Privatsphäre und Datenschutz in der Online-Umgebung beitragen könne.[781]

Zur Anwendbarkeit des Grundrechts auf Datenschutz auf juristische Personen ist grundsätzlich anzumerken, dass diese aufgrund der oft vorhandenen Gegeninteressen unter Umständen einem abgestuften Schutz unterliegen.[782] *Anderl* argumentiert gar, dass seit Inkrafttreten der Geheimnisschutzrichtlinie[783], die das berechtigte Geheimhaltungsinteresse an Unternehmens-Know-how regelt, faktisch kein Bedarf an einem strengen Datenschutz für Daten juristischer Personen mehr bestünde.[784] Diesem Gedanken kann man sich grundsätzlich anschließen, wenngleich dies nichts an einem möglicherweise bestehenden Grundrecht auf Datenschutz auch für juristische Personen ändert.

Zum einen legt Art. 16 AEUV das Recht auf Schutz personenbezogener Daten fest, wobei in Art. 16 Abs. 2 der Schutz auf natürliche Personen eingeschränkt wird.[785] Interessant ist, dass diese Bestimmung gleichlautend mit dem in Art. 8 GRC vorgesehenen Grundrecht auf den Schutz personenbezogener Daten geregelt ist,[786] wobei die beiden Bestimmungen gem. Art 6 EUV rechtlich gleichrangig zu betrachten sind.[787] In der Lehre wird hierbei davon ausgegangen, dass Art. 16 AEUV bloß Programmnorm- bzw. Grundsatzcharakter hat[788] und erst durch Art. 8 GRC seine nähere Ausgestaltung genießt.[789] Dieser Meinung kann man sich aufgrund der generellen Systematik von AEUV und EUV nur anschließen.

---

[781] Zusammenfassung der Stellungnahme der Europäischen Datenschutzbeauftragten zur Gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik zur "Cybersicherheitsstrategie der Europäischen Union" und zum Vorschlag der Kommission für eine richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, ABl. C 32/19, Schlussfolgerung 75.

[782] *Berka*, Die Grundrechte: Grundfreiheiten und Menschenrechte in Österreich (1999), S. 273ff.

[783] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl 2016, L 157/1.

[784] So auch *Anderl/Hörlsberger/Tlapak et al.*, Kein Schutz von Daten juristischer Personen nach der DSGVO, Dorda Presse, 2018, zu finden unter https://www.dorda.at/publications/kein-schutz-von-daten-juristischer-personen-nach-der-dsgvo, abgerufen am 03.08.2019.

[785] Ein Verweis auf einen Beschluss zur Festlegung von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten findet sich auch in Art. 39 EUV.

[786] Der einzige Unterschied ist die offensichtlich schrankenlose Regelung des Rechts in Art. 16 AEUV, wohingegen in Art. 8 Abs. 2 GRC Schranken festgelegt sind.

[787] Art. 6 Abs. 1 EUV: die Charta der Grundrechte und die Verträge sind rechtlich gleichrangig.

[788] *Raschauer*, Europäisches Datenschutzrecht - quod vadis?, in Raschauer (Hrsg), Datenschutzrecht 2010 (2011), S. 92. *Spitzbart*, Grundrecht auf Datenschutz für juristische Personen (Dissertation) (2014), S. 93.

[789] Im dazu bekannten Urteil EuGH 09.10.2010, C-92/09 und C-93/09 (Schecke/Land Hessen) findet nur Art. 8 GRC, jedoch nicht Art. 16 AEUV Erwähnung.

Der bereits erwähnte Art. 8 Abs. 1 GRC sieht das Recht jeder Person auf den Schutz der sie betreffenden personenbezogenen Daten vor. Die herrschende Meinung der Lehre[790] geht bei Art. 8 GRC von einer lex-specialis-Regelung zu Art. 7 GRC (Achtung des Privat- und Familienlebens)[791] aus,[792] wohingegen der EuGH die beiden Bestimmungen in vergangener Rechtsprechung undifferenziert anwandte. [793]

Zum persönlichen Anwendungsbereich des Art. 8 GRC ist festzustellen, dass dieser möglicherweise nur natürliche Personen berechtigt. Dies ergibt sich aus dem Umstand, dass Sekundärrechtsakte[794] bereichsspezifische Konkretisierungen des Art. 52 Abs. 2 GRC darstellen und aus diesem Grund zur Auslegung des Primärrechts heranzuziehen sind.[795] Die Datenschutzgrundverordnung (DSGVO) als zentraler Sekundärrechtsakt den Datenschutz betreffend[796] berechtigt ausschließlich natürliche Personen.[797]

Weiters findet sich in den Erläuterungen zur Grundrechtecharta der Verweis auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen, von der ebenso nur natürliche Personen erfasst sind.[798]

Mittlerweile hat der EuGH anerkannt, dass sich auch juristische Personen dann auf den durch Art. 8 GRC vermittelten Schutz berufen können, wenn ihr (Firmen-)Name eine oder mehrere natürliche Personen bestimmt bzw. nennt.[799] In der Literatur gibt es unterschiedliche Meinungen, ob daraus im Umkehrschluss zu schließen sei, dass juristische Personen nicht in den Schutzbereich fallen, sofern kein Name einer natürlichen Person Teil des Namens der juristischen Person ist.[800]

---

[790] *Jarass*, Charta der Grundrechte der Europäischen Union : Kommentar[2], Art. 7 Rz 5. *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Art. 8 Rz 13. Näheres zu dieser Diskussion *Spitzbart*, Grundrecht auf Datenschutz für juristische Personen (Dissertation), S. 105.

[791] Siehe dazu Kapitel 7.5.2.4.1.

[792] Nach Frenz kommt es darauf an, ob eher die technische Seite durch den Eingriff berührt (Art. 8 GRC) oder das Eindringen in die Privatsphäre den Schwerpunkt bildet (Art. 7 GRC), siehe *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 1184.

[793] EuGH – Schecke, C-92/09 u. C-93/09, Slg. 2010, I-11063.

[794] Zur Tatsache, dass hier das einschlägige Sekundärrecht (wie die DSGVO) zu beachten ist, siehe *Borowsky* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Rz 26.

[795] *Raschauer* in Raschauer, Datenschutzrecht 2010, S. 99f. *Frenz* sieht Unternehmensdaten von Art. 8 GRC nicht, jedoch ggf von Art. 16, 17 umfasst, siehe *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 1367.

[796] ErwGr 1 DSGVO bezieht sich konkret auf Art. 16 AEUV und Art. 8 GRC.

[797] Siehe Art. 1 DSGVO.

[798] RL (EU) 2007/2007/C 303/02; Erläuterungen zur Charta der Grundrechte, Art. 8 GRC.

[799] EuGH – Schecke, C-92/09 u. C-93/09, Slg. 2010, I-11063.

[800] Für diesen Umkehrschluss spricht sich bspw aus *Ennöckl*, EuGH zur Veröffentlichung von EU-Agrarbeihilfen: (vorläufiges) Ende der Transparenz, Österreichische Juristenzeitung (ÖJZ), 21/2011. Dagegen *Spitzbart*, Grundrecht auf Datenschutz für juristische Personen (Dissertation), S. 97f. sowie *Stangl* in Kahl/Raschauer et al., Grundsatzfragen der europäischen Grundrechtecharta, S. 3. *Jarass* spricht sich für eine

Teile der Lehre sprechen sich dafür aus, berufsbezogene Daten oder Geschäftsinformationen hauptsächlich Art. 15 GRC (Berufsfreiheit), Art. 16 GRC (unternehmerische Freiheit) und Art. 17 GRC (Eigentumsrecht) zuzurechnen und dass Art. 7 und 8 GRC zusätzlich gelten. [801]

Eine Änderung der Auslegung könnte sich durch die EMRK ergeben. Aufgrund der Regel des Art. 52 Abs. 3 GRC ist jedenfalls dann die EMRK als Auslegungshilfe heranzuziehen, sofern ein dort garantiertes Recht einem solchen der GRC entspricht. [802] Dies könnte möglicherweise auf Art. 8 EMRK zutreffen, der das Recht auf Achtung des Privat- und Familienlebens regelt und das Recht auf Datenschutz inkludiert.[803]

Zu Art. 8 EMRK entschied der EGMR bereits mehrmals, dass auch juristische Personen und somit Wirtschaftsdaten davon erfasst sind.[804] Dort, wo das Grundrecht seinem Wesen nach auch für juristische Personen relevant sein kann, wird eine Anwendbarkeit des Art. 8 EMRK auch in der Literatur[805] angenommen. Dies wird insbesondere auch für den Datenschutz bejaht.[806] Zu verweisen ist hier auch noch auf die grundsätzliche Rechtsprechung des EGMR, dass die EMRK ein „living instrument" sei, das „in light of the present day conditions"[807] ausgelegt werden muss (dynamische Auslegung) – die technischen Entwicklungen der letzten Jahre, die Datenerhebungen und -sammlungen mit kleinem Aufwand in großem Ausmaß ermöglichen, ist als eine solche Entwicklung zu sehen, wodurch der Begriff „personenbezogene Daten" eben auch auf Daten mit Bezug zu juristischen Personen beziehen sollte.[808]

Einbeziehung, jedoch nur insoweit aus, als Daten auf eine Privatperson zurückzuführen sind, siehe *Jarass*, Charta der Grundrechte der Europäischen Union : Kommentar[2], Art. 8 Rz 7.

[801] *Bernsdorff* in Meyer, Charta der Grundrechte der Europäischen Union::Kommentar, Art. 8 Rz 13. *Jarass*, Charta der Grundrechte der Europäischen Union : Kommentar[2], Art. 8 Rz 4. *Knecht*, Die Charta der Grundrechte der Europäischen Union (2005).

[802] Art. 8 EMRK und Art. 7 GRC werden gleich ausgelegt. Zusätzlich muss der EuGH in seinen Entscheidungen die Rechtsprechung des (schon länger existierenden) EGMR zu Art. 8 EMRK mitberücksichtigen und umgekehrt, siehe dazu *Becker*, Art. 52 GRC, in Schwarze (Hrsg), EU-Kommentar (2019), Rz 16.

[803] Siehe dazu Kapitel 7.5.2.4.1. Siehe auch RL (EU) 2007/2007/C 303/02; Erläuterungen zur Charta der Grundrechte, Art. 8 GRC.

[804] Der EGMR erkannte an, dass sich eine juristische Person ebenso wie eine natürliche Person auf Art. 8 EMRK berufen könne und verwies auf die Tatsache, dass sich der Schutzumfang des Art. 8 EMRK in gleicher Weise auf „berufliche und geschäftliche Tätigkeiten erstreckt", siehe EGMR 16.12.1992, 13710/88 – Niemitz/Deutschland. Ebenso EGMR 16.4.2002, 37971/97 (Societé Colas Est and others); EGMR 28.01.2003, 44647/98 (Peck gg Vereinigtes Königreich); siehe außerdem die Ausführungen zu Art. 8 EMRK;

[805] Siehe beispielsweise *Winkler*, Die Grundrechte der Europäischen Union : System und allgemeine Grundrechtslehren (2006), S. 353. *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 22 Rz 4.

[806] *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, S. 57. *Grabenwarter/Pabel*, Europäische Menschenrechtskonvention, § 22 Rz 4.

[807] *Ehlers* in Ehlers, Europäische Grundrechte und Grundfreiheiten, Rz 41.

[808] *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, S. 60.

Wenngleich somit festzustellen ist, dass Art. 8 EMRK den Schutz von Daten juristischer Personen umfasst, hat dies keinerlei Auswirkung auf Art. 8 GRC, da bereits die Erläuterungen zur GRC feststellen, dass Art. 8 GRC der EMRK nicht entlehnt ist und somit Art. 52 Abs. 3 nicht zur Anwendung kommt.[809]

Somit kommt statt der Auslegungsregel des Art. 52 Abs. 3 GRC (GRC hat Tragweite der gleichlautenden Bestimmung der EMRK) jene des Art. 52 Abs. 2 GRC zum Tragen, wonach die Ausübung der durch die Charta anerkannten Rechte, die in den Verträgen geregelt sind, im Rahmen der in den Verträgen festgelegten Bedingungen und Grenzen erfolgt. Wie weiter oben bereits erläutert, liegt mit der DSGVO eine sekundärrechtliche Konkretisierung des primärrechtlichen Art. 16 AEUV (bezieht sich auf natürliche Personen) vor, wodurch durch die Verträge wohl nur ein Schutz natürlicher Personen vorgesehen ist. Somit steht meines Erachtens klar fest, dass der Anwendungsbereich des Art. 7 GRC jedenfalls auf natürliche Personen[810] beschränkt bleibt. [811]

Neben den Regelungsbereichen der EMRK[812] und der Charta soll schlussendlich der persönliche Anwendungsbereich der nationalen Verfassungsbestimmung des Schutzes personenbezogener Daten in § 1 Datenschutzgesetz (DSG) in den Untersuchungsbereich mitaufgenommen werden.

Nach nationalem Verfassungsrecht hat jedermann, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht (§ 1 Abs. 1 DSG). Das DSG wurde durch das nationale Datenschutz-Änderungsgesetz 2018[813] novelliert, wodurch die DSGVO in einzelnen Punkten konkretisiert und ergänzt wurde. Die Verfassungsbestimmungen (§§ 1-3 DSG) wurden aus dem DSG 2000 übernommen bzw. nicht geändert.[814]

Bis zu dieser Novellierung nannte § 4 Z 3 DSG unter dem Begriff der vom DSG Betroffenen neben natürlichen auch juristische Personen[815], wodurch von § 1 Abs. 1 DSG („Jedermann“) iVm § 4 Z 3 DSG auch juristische Personen vom Schutzbereich erfasst waren, sofern ein schutzwürdiges

[809] RL (EU) 2007/2007/C 303/02; Erläuterungen zur Charta der Grundrechte.
[810] Juristische Personen nur insofern, als der Name einer natürlichen Person im Unternehmensnamen aufscheint, siehe EuGH-Entscheidung weiter oben.
[811] Siehe zur damaligen Auslegung gem. DatenschutzRL 95/46/EG auch *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 1361.
[812] Ähnlich dazu siehe Art. 53 GRC
[813] Bundesgesetz, mit dem das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) geändert wird, BGBl. I Nr. 23/2018.
[814] zur damaligen realpolitischen Situation, dass der Gesetzgeber nicht die erforderliche Zweidrittelmehrheit für die Verfassungsbestimmungen erzielen konnte, siehe *Knyrim/Tretzmüller*, Die wichtigsten Regelungen des DSG (neu), Datenschutz konkret, 4/2017, S. 79.
[815] Zur Diskussion, inwieweit § 4 DSG zur Auslegung der Verfassungsbestimmung des § 1 DSG herangezogen warden kann, siehe *Spitzbart*, Grundrecht auf Datenschutz für juristische Personen (Dissertation).

Geheimhaltungsinteresse[816] bestand.[817] Geheimhaltung bei juristischen Personen im Sinne des § 1 Abs. 1 DSG betrifft Geschäfts- oder Betriebsgeheimnisse. Dies sind Tatsachen kommerzieller oder technischer Art, die nur einer bestimmten und begrenzten Anzahl von Personen bekannt und anderen nicht oder nur schwer zugänglich sind, nach dem Willen des Berechtigten nicht über den Kreis der Eingeweihten hinaus dringen sollen und an deren Geheimhaltung der Unternehmensinhaber ein wirtschaftliches Interesse hat.[818]

Diese Klarstellung des persönlichen Anwendungsbereiches existiert seit der Novelle nicht mehr. Vielmehr regelt § 4 Abs. 1 DSG für den Anwendungsbereich nun, dass das Bundesgesetz für die Verarbeitung personenbezogener Daten natürlicher Personen gelte. Von einer Geltung für juristische Personen findet sich nichts mehr.

Trotzdem argumentierte *Riedl* kürzlich – im Gegensatz zu *Anderl*[819] der den Schutz nunmehr auf natürliche Personen beschränkt sieht - , dass der Datenschutz für juristische Personen aufgrund der weiterhin bestehenden Verfassungsbestimmung des § 1 DSG bestehen bleibe.[820] Diese Argumentation kann insofern nachvollzogen werden, als es sich bei § 4 DSG, in dem nunmehr nur von natürlichen Personen die Rede ist, um eine einfachgesetzliche Bestimmung handelt, die den Anwendungsbereich der Verfassungsbestimmung des § 1 DSG nicht ohne Weiteres reduzieren kann, sofern man bei § 1 (ohne die Verbindung mit dem ehemaligen § 4 für dessen Auslegung unbedingt für notwendig zu erachten) weiterhin vom weiten Anwendungsbereich ausgeht.

Anzumerken ist hinsichtlich dieser Auslegung einleitend, dass der Langtitel des DSG mit der Novelle in „Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)“ umbenannt wurde und somit für sich auf eine Einbeziehung nur natürlicher Personen schließen lässt.

Darüber hinaus könnte man aufgrund des Vorranges des Unionsrechtes (Grundrechtecharta und als deren Konkretisierung die DSGVO), die lediglich vom Schutz natürlicher Personen ausgeht, von einem eindeutig reduzierten Anwendungsbereich ausgehen. Dem kann entgegnet werden, dass Art. 53 GRC bestimmt, dass keine Bestimmung der Charta als eine Einschränkung oder Verletzung

[816] Das Geheimhaltungsinteresse ist nicht gegeben, wenn Daten wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind (§ 1 Abs. 1 DSG).
[817] Der VfGH stellte erstmals im Erkenntnis VfSlg 12.228/1989 fest, dass Wirtschaftsdaten personenbezogene Daten eines Betroffenen sein können und unter den sachlichen Anwendungsbereich des § 1 DSG subsumiert werden können.
[818] *Pollirer/Weiss/Knyrim et al.*, Datenschutzgesetz (DSG)[4] (2019), Anhang V/1/D § 11 Anm. 1. Auch *Schramböck*, Der Schutz von Geschäfts- und Betriebsgeheimnissen; Praxishandbuch (2002), S. 6.
[819] *Anderl et al.*, Dorda Presse, 2018. Allgemeiner *Anderl* zur DSGVO siehe auch *Anderl/Tlapak*, Die (zukünftige) Zulässigkeit der Einbindung datenschutzrechtlicher Zustimmungen in AGB, ecolex, 7/2016.
[820] *Riedl*, Der Datenschutz für die juristischen Personen bleibt bestehen, Datenschutz konkret, 4/2017, S. 74.

der Menschenrechte auszulegen ist, die durch die Verfassungen der Mitgliedstaaten anerkannt werden.[821] Sofern somit weiterhin vom weiten Anwendungsbereich des § 1 DSG ausgegangen wird, kann Art. 8 GRC (trotz grundsätzlichem Vorrang von Unionsrecht) diesen meines Erachtens nicht auf natürliche Personen einschränken bzw. verdrängen.

Nicht vergessen werden darf außerdem auf das Gebot EU-rechtskonformer Interpretation. Dieses besagt, dass die innerstaatlichen Stellen verpflichtet sind, das nationale (auch Verfassungs-)Recht unionsrechtskonform auszulegen, wenn und soweit ein entsprechender Interpretationsspielraum besteht.[822] Eine EU-rechtskonforme Auslegung spricht aus oben genannten Gründen meines Erachtens eindeutig für eine Einschränkung des Anwendungsbereichs auf natürliche Personen.

Als Gegenargument könnte theoretisch noch ins Treffen geführt werden, dass der nationale Gesetzgeber ursprünglich mit der Datenschutz-Novelle den § 1 DSG auf natürliche Personen einschränken wollte, dies jedoch an der notwendigen Verfassungsmehrheit scheiterte. Nun könnte argumentiert werden, dass dies möglicherweise nicht notwendig gewesen wäre, wäre der Anwendungsbereich ohnedies durch das Inkrafttreten der DSGVO auf natürliche Personen beschränkt.

Die vermeintlichen Absichten des Gesetzgebers sind jedoch wohl kein rechtliches Argument, die eine Einbeziehung juristischer Personen in den Anwendungsbereich bestätigen oder auch nicht. Aus den oben genannten Gründen, insbesondere aus Gründen der systematischen Interpretation des § 1 DSG anhand des Langtitels des Bundesgesetzes sowie in Verbindung mit dem neuen § 4 DSG, als auch aufgrund einer EU-rechtskonformen Interpretation ist meines Erachtens im Fall von § 1 DSG ab dem Zeitpunkt der Novellierung 2018 entgegen der Position von *Riedl* lediglich von einem Schutz von Daten natürlicher Personen auszugehen.

Da unabhängig vom persönlichen Anwendungsbereich des § 1 DSG jedenfalls Art. 8 EMRK als nationales Verfassungsrecht Geltung hat und dieses wie oben beschrieben juristische Personen miteinschließt, sind mögliche Eingriffe durch das NIS-Gesetz zu prüfen.

Dabei fällt einerseits die mögliche Veröffentlichung von Sicherheitsvorfällen durch die Behörden (§ 10 Abs. 1 NISG) ins Auge. Auf diese Bestimmung wurde bereits in Kapitel 7.5.2.5 zum Eigentumsrecht und möglichen Minderung des Unternehmenswertes durch Reputationsschäden näher eingegangen. Nach Rechtsprechung des EGMR hat der Grundrechtsträger das Recht, dass

[821] Der VfGH sprach sich in Bezug auf die VorratsdatenspeicherungsRL dafür aus, dass Garantien der Grundrechtecharta so auszulegen sind, dass der Grundrechtsstandard der mitgliedstaatlichen Verfassungen nicht unterschritten wird, siehe VfGH 28.11.2012, G47/12 ua.
[822] *Baumgartner*, Zeitschrift für öffentliches Recht, 2010, S. 301.

seine personenbezogenen Daten nicht an die Öffentlichkeit weitergegeben werden, wenn staatliche Stellen von ihnen Kenntnis haben. Dies gilt für sensible Daten und für normale personenbezogene Daten.[823] Darüber hinaus beinhaltet das Recht auf Geheimhaltung vor der Öffentlichkeit auch das Recht, nicht vom Staat gezwungen zu werden, bestimmte Informationen offenzulegen.[824] Genau das ist in § 10 Abs. 1 NISG jedoch für Anbieter digitaler Dienste vorgesehen, sofern sie von einem Sicherheitsvorfall betroffen sind. Eine Veröffentlichung personenbezogener Daten ist insbesondere deshalb von besonderer Bedeutung, als ein Eingriff nicht wieder rückgängig gemacht werden kann.

In Bezug auf das legitime Ziel ist auf die Ausführungen zum Eingriff in das Eigentumsrecht zu verweisen. Wie auch dort ist jedenfalls zu prüfen, ob die Anonymisierung der Daten einer Erreichung der Ziele entgegengestanden hätte.[825] Anhand dieser Prüfung im Einzelfall wird zu beurteilen sein, ob es sich um einen unrechtmäßigen Eingriff in das Grundrecht auf Art. 8 EMRK handelt.

Ein weiterer Eingriff in das Grundrecht auf Privatleben gem. Art. 8 EMRK könnte die Einrichtung eines Sensornetzwerks gem. § 13 NISG darstellen. Auf diese Bestimmung wurde bereits im Kapitel 7.5.2.4.3 (Eingriff in das Recht auf Korrespondenz/Kommunikation gem. Art. 8 EMRK) näher eingegangen. Somit bleibt auch hier der Verweis auf die dortigen Ausführungen, dass es sich gerade nicht um die Verarbeitung personenbezogener Daten handelt.[826]

7.5.3. Ermittlung der Betreiber wesentlicher Dienste

7.5.3.1. Kriterien zur Ermittlung der Betreiber wesentlicher Dienste

Im Zentrum der Regelungen rund um die NIS-RL stehen die Betreiber, deren höherer Standard an Verfügbarkeit und Resilienz eigentliches Ziel der Richtlinie ist. Dementsprechend ist es erforderlich, die betroffenen Betreiber zu identifizieren. Die Richtlinie sieht vor, dass die Mitgliedstaaten für jeden in Anhang II genannten Sektor und Teilsektor die Betreiber wesentlicher Dienste in ihrem Hoheitsgebiet ermitteln (Art. 5 NIS-RL) und definiert Kriterien, anhand derer diese Ermittlung erfolgen soll (Art. 5 Abs. 2).

[823] EGMR, 17.7.2003, 63737/00 (Perry/UK), Rz 38; EGMR, 12.12.2013, 20383/04 (Khmel/RUS), Rz 41.
[824] *Paefgen*, Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, S. 84.
[825] EGMR, 28.1.2003, 44647/98 (Peck/UK), Rz 80f; EGMR, 15.4.2014, 50073/07 (Radu/MOL), Rz 30f.
[826] Siehe die Ausführungen in Kapitel 7.5.2.4.3, wonach es lediglich zu einem Abgleich der Metadaten von IP-Paketen handelt und gerade nicht um die unverschlüsselte Verarbeitung personenbezogener Daten.

In diesem Zusammenhang bedarf es einer Ausführung zum grundsätzlichen Verständnis eines Betreibers wesentlicher Dienste. Die NIS-RL sieht einen Bottom-Up-Ansatz vor, in dem zuerst wesentliche Dienste gesellschaftlicher und/oder wirtschaftlicher Tätigkeit (Art. 5 Abs. 2 NIS-RL) identifiziert und die Unternehmen, die diese Dienste zur Verfügung stellen, als Betreiber wesentlicher Dienste identifiziert werden sollen. Es kann und wird daher durchaus der Fall sein, dass Einrichtungen sowohl wesentliche als auch unwesentliche Dienste erbringen.[827]

Die näheren Kriterien zur Ermittlung (Art. 5 Abs. 2 NIS-RL) legt der nationale Gesetzgeber durch VO fest. Gem. § 16 Abs. 2 kann der Bundeskanzler[828] nähere Regelungen zu den in § 2 genannten Sektoren bestimmen, insbesondere Teilsektoren, Bereiche, die dazugehörigen wesentlichen Dienste sowie Arten von Einrichtungen nennen. Dabei sollen bestimmte Faktoren berücksichtigt werden (§ 16 Abs. 2 Z 1-6). In dieser Verordnung[829] werden zu jedem dieser Sektoren (§ 2) die Teilsektoren (im Sektor Energie bspw. die Teilsektoren Elektrizität, Erdöl und Erdgas) sowie gegebenenfalls die Bereiche (im Teilsektor Elektrizität bspw. die Bereiche Stromerzeugung, Stromverteilung und Stromübertragung) angeführt. Zu jedem dieser Bereiche werden Schwellenwerte definiert, welche Dienste als wesentliche Dienste im Sinne des § 16 Abs. 2 NISG gelten (§§ 4ff NISV) Dabei wird – abhängig vom jeweiligen Sektor, Teilsektor oder Bereich – entweder auf die Zahl der Nutzer (bspw. im Flugverkehr[830]) oder sektorenspezifische Kriterien (Erzeugungsleistung in der Stromerzeugung[831]) – Bezug genommen.

Näher untersucht werden soll die Frage, ob die in der nationalen Umsetzung vorgesehenen Kriterien der NISV mit jenen der NIS-RL übereinstimmen. Einerseits soll berücksichtigt werden, dass die Einrichtung einen Dienst bereitstellt, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist (Art. 5 Abs. 2 lit. a NIS-RL). Da in der NISV ohnedies nur auf jene Teilsektoren und Einrichtungen Bezug genommen wird, die in Anhang II NIS-RL geregelt wurden und somit im Anwendungsbereich liegen, war in Bezug darauf kein weiteres Kriterium erforderlich.

---

[827] Beispiel des Flughafens, der mit seinem Start- und Landebahn-Management einen wesentlichen Dienst und mit dem Betrieb von Einkaufsbereichen unwesentliche Dienste erbringt, siehe dazu auch ErwGr 22 NIS-RL.

[828] Im Einvernehmen mit dem Bundesminister für Inneres.

[829] Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV).

[830] § 5 Abs. 1 lit. b NISV.

[831] § 4 Abs. 1 Z 1 lit. aa NISV.

Das Kriterium der Abhängigkeit von Netz- und Informationssystemen für die Bereitstellung dieses Dienstes (Art. 5 Abs. 2 lit. b NIS-RL) wurde in der Definition des wesentlichen Dienstes (§ 3 Z 9) berücksichtigt, auf den sich die Ermittlung der Betreiber wesentlicher Dienste gem. § 16 Abs. 1 NISG bezieht.

Einzubeziehen ist nach den Regelungen der Richtlinie überdies, dass ein Sicherheitsvorfall[832] erhebliche Störungen bei der Bereitstellung dieses Dienstes bewirken würde (Art. 5 Abs. 2 lit. c NIS-RL). Die Erwägungsgründe der Richtlinie nennen hier als Beispiel die Menge der erzeugten Energie, die tägliche Fördermenge an Öl oder die Anzahl jährlich versorgter Patienten.[833] ME handelt es sich bei diesen Beispielen jedoch vielmehr um die Kritikalität des Dienstes für die Gesellschaft. Das Kriterium der Bedeutung des Sicherheitsvorfalles für die Bereitstellung des Dienstes wird meines Erachtens bereits durch die Voraussetzung der Abhängigkeit des Dienstes von Netz- und Informationssystemen (Art. 5 Abs. 2 lit. b NIS-RL) abgedeckt. Ein Sicherheitsvorfall im Sinne dieses Gesetzes ist eine Störung der Netz- und Informationssysteme. Sofern eine Abhängigkeit von diesen Systemen gegeben ist, bewirkt eine Störung dieser Netz- und Informationssysteme auch eine Störung des Dienstes selbst. Der nationale Gesetzgeber selbst sah dies offenbar ähnlich und berücksichtigte diese Voraussetzung nicht als separates Kriterium im NIS-Gesetz.

In Kapitel 7.1.2 (Gegenstand und Ziel des Gesetzes) wurde bereits auf die ungewöhnliche Konstruktion der Definition des wesentlichen Dienstes (§ 3 Z 9) im Zusammenhang mit der Nennung von Sektoren in § 2 näher eingegangen. Diese legistische Konstruktion ist auch in Kombination mit § 16 Abs. 2 nicht nachvollziehbar. Die NISV definiert die wesentlichen Dienste konkret durch das Anführen dieser Dienste inkl. Schwellenwerten. Warum der wesentliche Dienst zusätzlich einer Definition in § 3 Z 9 bedurfte, die überdies Bereiche der wesentlichen Dienste auslässt (bspw. Bankwesen) bzw. nicht mit den Teilsektoren der NISV übereinstimmt, ist nur aus den bereits in Kapitel 7.1.2 erwähnten Gründen zu erklären.

7.5.3.2. Rechtliche Möglichkeiten zur nationalen Umsetzung der Ermittlung Betreiber wesentlicher Dienste

Die Richtlinie sieht vor, dass Mitgliedstaaten nationale Maßnahmen erlassen, in denen bestimmt wird, welche Einrichtungen den Pflichten im Zusammenhang mit Netz- und Informationssystemen unterliegen.[834] In der nationalen Umsetzung kamen dafür mehrere Varianten in Betracht, deren theoretische Anwendbarkeit und Wirksamkeit untersucht werden soll.

[832] Der Sicherheitsvorfall wird in Kapitel 7.5.6.2 näher erläutert.
[833] ErwGr 28 NIS-RL.
[834] ErwGr 25 NIS-RL.

Im deutschen IT-Sicherheitsgesetz wurde der Ansatz einer Selbstermittlung durch die Betreiber gewählt. Dabei sieht § 10 BSI-Gesetz[835] eine Rechtsverordnung vor, in der Einrichtungen, Anlagen oder Teile davon als kritische Infrastruktur im Sinne dieses Gesetzes bestimmt werden sollen. Die auf Grund des § 10 Abs. 1 BSI-Gesetz erlassene Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz[836] bzw. die erste Verordnung zur Änderung der BSI-Kritisverordnung[837] legen ebenso wie die NISV Schwellenwerte[838] für die verschiedenen Sektoren, Teilsektoren und Bereiche fest.

Unternehmen müssen in weiterer Folge selbst bestimmen, ob ihre Anlagen die definierten Schwellenwerte erreichen und gegebenenfalls binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung dem BSI[839] eine Kontaktstelle benennen (§ 8b Abs. 3 BSI-Gesetz). Die Regelung kommt somit einer Selbstermittlung[840] der Betreiber wesentlicher Dienste gleich, die sich bei Erreichen der Schwellenwerte selbst beim BSI zu melden haben.[841] Das BSI entledigt sich somit der Aufgabe, die aufwändige Ermittlung selbst vorzunehmen. *Grudzien* sieht darin einen gangbaren Weg des Gesetzgebers[842], *Heinickel/Feiler* würden sich aus verfassungsrechtlichen Gründen eine Definition des Begriffes der kritischen Infrastruktur im BSI-Gesetz selbst, und nicht erst durch Verordnung, wünschen.[843]

In diesem Zusammenhang stellt sich die Frage, ob diese Lösung in der österreichischen Rechtsordnung einer verfassungswidrigen formalgesetzlichen Delegation (Art. 18 B-VG)[844] gleichkommen würde, da die Entscheidungsgewalt (vom Gesetzgeber) an die Verwaltung (als Verordnungsgeber) übertragen würde. Nach ständiger Rechtsprechung des VfGH darf eine Verordnung bloß präzisieren, was in den wesentlichen Konturen bereits im Gesetz selbst vorgezeichnet wurde.[845] Nach dem Prinzip der Vorausbestimmung des Verordnungsinhalts durch das Gesetz müssen aus dem Gesetz alle wesentlichen Merkmale der beabsichtigten Regelung

[835] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), zuletzt geändert durch Art. 1 G v. 23.6.2017 I 1885.
[836] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016, BGBl. I Nr. 20/2016.
[837] Erste Verordnung zur Änderung der BSI-Kritisverordnung vom 21. Juni 2017, BGBl. I Nr. 40/2017.
[838] Als Regelschwellwert wurde eine Anzahl von 500.000 betroffenen Personen festgelegt, siehe dazu auch *Brisch* in Abolhassan, Security Einfach Machen, S. 46.
[839] Bundesamt für Sicherheit in der Informationstechnik (BSI)
[840] *Dürig/Fischer*, Cybersicherheit in Kritischen Infrastrukturen, Datenschutz und Datensicherheit - DuD, 4/2018, S. 212.
[841] Siehe dazu auch Schutz kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS, 2017.
[842] *Grudzien*, Datenschutz und Datensicherheit - DuD, 2016, S. 31.
[843] Siehe dazu *Heinickel/Feiler*, Computer und Recht, 2014, S. 714.
[844] *Berka*, Verfassungsrecht, Rz 495.
[845] VfSlg. 7945/1976, 9226/1981, 9227/1981, 10296/1984 ua.

ersehen werden können.[846] Die Grenze zwischen einer noch ausreichenden materiellen Bestimmtheit des Gesetzes und einer formalen Delegation wird nicht immer leicht zu bestimmen sein, wobei das Entscheidungskriterium stets die Frage sei, ob die im Verordnungsweg getroffene (Durchführungs-)Regelung auf ihre inhaltliche Gesetzmäßigkeit überprüft werden kann.[847] § 10 BSI-Gesetz verweist auf § 2 Abs. 10 BSI-Gesetz, in dem kritische Infrastrukturen und die dazugehörigen Sektoren (ähnlich wie in § 2 NISG) legal definiert sind (weshalb die Kritik von *Heinickel/Feiler* (siehe oben) nicht nachvollzogen werden kann). An den Verordnungsgeber delegiert wird lediglich die Regelung von spezifischen Dienstleistungen und Schwellwerten in den genannten Sektoren, wie dies auch im NIS-Gesetz iZm der NISV umgesetzt wurde. Die Verordnung präzisiert somit lediglich die Bestimmung des Gesetzgebers, weshalb (auch in der österreichischen Umsetzung) keine verfassungswidrige formalgesetzliche Delegation vorliegt.

Die Lösung der Selbstermittlung durch die Unternehmen ist meines Erachtens aufgrund verschiedener Gesichtspunkte schwierig. Die Mitgliedstaaten sind verpflichtet, Betreiber wesentlicher Dienste zu ermitteln (Art. 5 Abs. 1 NIS-RL). Zwar könnte argumentiert werden, dass eine solche Ermittlung in Deutschland durch den Empfang von Kontaktstellen der sich selbst ermittelnden Betreiber erfolgt. Die genannte Regelung der NIS-RL könnte mit dieser Formulierung aber wohl einen aktiveren Ansatz in Auge gefasst haben.

Merkwürdig erscheint meines Erachtens auch die Konstruktion per se, da das BSI ohnedies selbst eine Ermittlung vornehmen und eine entsprechende Liste mit betroffenen kritischen Infrastrukturen wird führen müssen. § 14 BSI-Gesetz sieht eine Ordnungswidrigkeit vor, wer eine Kontaktstelle nicht oder nicht rechtzeitig benennt, obwohl er als kritische Infrastruktur dazu verpflichtet gewesen wäre (§ 14 Abs. 1 Z 3 BSI-Gesetz). Darüber hinaus bestehen auch Übertretungen für die Nichterfüllung der Sicherheitsvorkehrungen (§ 14 Abs. 1 Z 1 BSI-Gesetz) sowie für Nichterfüllung der Meldepflicht (§ 14 Abs. 1 Z 4 BSI-Gesetz). Das Vorliegen einer solchen Ordnungswidrigkeit kann einem logischen Schluss zufolge wohl nur festgestellt werden, wenn dem BSI bekannt ist, dass ein Unternehmen die Schwellenwerte einer kritischen Infrastruktur erreicht, sich aber rechtswidrig nicht meldet.

Außerdem sind die Mitgliedstaaten verpflichtet, der Kommission alle zwei Jahre die Zahl der Betreiber wesentlicher Dienste, die in jedem der in Anhang II genannten Sektoren ermittelt wurden, zu übermitteln. Hier stellt sich die Frage, ob das BSI hierbei die Liste der sich meldenden

[846] VfSlg. 4139/1962, 462/1964, 5373/1966, 7945/1976.
[847] VfSlg. 1932/1950, 2294/1952, 4072/1961, 10296/1984.

Unternehmen oder jene Liste übermittelt, die sie (aus oben genannten Gründen) selbst ermittelt haben.

Wenngleich das System der Selbstermittlung Rechtsunsicherheit für die Unternehmen schafft, widerspricht dies mE nicht EU-Recht und dem Grundsatz der Rechtssicherheit. [848] Nach stRsp des EuGH ist es wichtig, dass jeder Mitgliedstaat die Richtlinien in einer Weise durchführt, die dem Erfordernis der Rechtssicherheit voll entspricht.[849] Die Angabe von Schwellenwerten zur eigenständigen Ermittlung durch den Betroffenen widerspricht an und für sich diesem Gedanken wohl dann nicht, wenn diese Schwellenwerte und die Auslegung selbiger durch den Betroffenen eindeutig ist. Nach österreichischer Rechtslage wäre bei der Angabe konkreter Schwellenwerte ebenso von keiner Verfassungswidrigkeit gem. Art. 18 B-VG (Rechtssicherheit)[850] auszugehen, wie auch der VfGH kürzlich in seiner Entscheidung zum Heumarkt-Projekt (und in diesem Zusammenhang vorgesehenen Schwellenwerten im UVP-Verfahren) in einem ähnlich gelagerten Fall begründete.[851]

Der Rechtssicherheit trägt die mit dem NIS-Gesetz vorgesehene Regelung der Ermittlung von Betreibern wesentlicher Dienste per Bescheid Rechnung. Dabei handelt es sich rechtlich um einen Gestaltungsbescheid[852], da dieser ex nunc wirkt und das Rechtsverhältnis, nämlich das Vorliegen eines Betreibers wesentlicher Dienste, erst begründet.[853] *Anderl/Heußler/Mayer/Müller* sprechen in diesem Zusammenhang von einem „state driven approach", wohingegen in Deutschland ein „provider driven approach" vorliegt. [854]

Als dritte Option käme die Identifizierung der Betreiber per Verordnung in Betracht. In dieser Verordnung könnten die einzelnen Sektoren, Teilsektoren und gegebenenfalls Bereiche sowie die darunterfallenden Betreiber wesentlicher Dienste angeführt werden.

„Die Abgrenzung zwischen Bescheid und Verordnung richtet sich üblicherweise nach dem Adressatenkreis: richtet sich ein Rechtsakt einer Verwaltungsbehörde an einen individuellen

[848] Im EU-Recht gilt ein allgemeiner Grundsatz der Rechtssicherheit, siehe *Öhlinger/Potacs*, EU-Recht und staatliches Recht[6], S. 6.
[849] EuGH Rs 239/85 (Kommission/Belgien), Slg 1986, 3645 Rz 7.
[850] *Arnold* in Arnold/Bundschuh-Rieseneder et al., Recht, Politik, Wirtschaft, Dynamische Perspektiven., S. 47.
[851] VfGH 1.10.2019, E1643/2019.
[852] Gem. EB RV NIS-Gesetz kommt dem Bescheid für die Eigenschaft als Betreiber wesentlicher Dienste konstitutive Wirkung zu (S. 18). Zur Statusentscheidung der Gestaltungsbescheide siehe auch *Leeb*, Bescheidwirkungen und ihre subjektiven Grenzen nach dem AVG (2010), S. 39.
[853] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 900.
[854] *Anderl et al.*, NISG::Kommentar, § 16, Rz 61.

Adressaten, so sei dieser Rechtsakt ein Bescheid; richtet sich der Rechtsakt an einen generellen Adressatenkreis, sei er eine Verordnung.“[855]

Raschauer sieht dann die Vorsehung einer Verordnung, „wenn ein bestimmter Hoheitsakt unzweideutig Rechtswirkungen für eine unbestimmte bzw. nur nach Gattungsmerkmalen bestimmte Vielzahl auslösen oder überhaupt die generelle Rechtslage gestalten soll.“[856] Nach *Antoniolli* richtet sich der „Bescheid immer an eine oder mehrere individuell bestimmte Personen, während sich die Verordnung an eine generell bestimmte Mehrheit wendet.“[857] Nach *Walter* kommt „der Verordnung keine Erkenntnis-, Feststellungs- und Exekutivfunktion zu sondern beschränkt sich darauf, etwa den vom Gesetz aufgestellten Tatbestand präziser zu umreißen. „[858]

Da der Rechtsakt genau die Stellung eines individuellen Unternehmens als Betreiber wesentlicher Dienste festlegen bzw. gestalten soll und es sich um einen bestimmbaren Personenkreis handelt, wäre die Identifizierung per Verordnung mE unzulässig. Darüber hinaus wären mit einer Verordnung die Rechtsschutzmöglichkeiten beschränkt, da dem VfGH alleine nach Art. 139 B-VG ein Prüfungsmonopol bei Verordnungen zukommt[859], und darüber hinaus einer Verordnungsanfechtung keine aufschiebende Wirkung zuerkannt werden kann.[860]

Generell wird in der Lehre und Rechtsprechung in solchen Fällen von janusköpfigen Verwaltungsakten gesprochen.[861] Diese Rechtsakte haben sowohl die Wirkung einer generellen Regelung (Verordnung) als auch die Wirkung eines Individualaktes (zB Bescheid), sind jedoch aufgrund ihrer unterschiedlichen Bedingungen der Erzeugung, der Kundmachung, des Rechtschutzes und der Bestandskraft (wie auch oben angeführt) in der Lehre strittig.[862] Der VfGH erachtet dies in seiner Rechtsprechung als zulässig und ging dahingehend schon mehrfach von unterschiedlichen Wirkungen dieser Rechtsakte für ein Individuum (Bescheid) sowie für einen unbestimmten Personenkreis (Verordnung) aus.[863]

---

[855] *Herbst*, Die Abgrenzung von Bescheid und Verordnung (2017), S. 41.; *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 749.
[856] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 750.; VfSlg 17018/2003.
[857] *Antoniolli/Koja*, Allgemeines Verwaltungsrecht[3], S. 72.
[858] *Walter*, Der Aufbau der Rechtsordnung: eine rechtstheoretische Untersuchung auf Grundlage der reinen Rechtslehre[2] (1974), S. 42f.
[859] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 809.
[860] *Aichlreiter*, Österreichisches Verordnungsrecht: ein systematisches Handbuch[2] (1988), S. 118.
[861] *Raschauer* verweist darauf, dass es janusköpfige Verwaltungsakte als eigenständigen Verwaltungsakttypus nicht gibt, siehe *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 753.
[862] *Adamovich et al.*, Österreichisches Staatsrecht, S. 135.
[863] VfSlg. 9.221/1981, 10.313/1984, 10.502/1985, 14295/1995, 17.338/2004, Siehe auch *Walter/Mayer*, Grundriss des österreichischen Verwaltungsverfahrensrecht[5] (1991), Rz 380.

Neben der rechtlichen Begründung sprechen abschließend auch sicherheitspolitische Kriterien gegen ein Verordnungsverfahren. Die Veröffentlichung der Betreiber wesentlicher Dienste, die mit der Publizität[864] der Verordnung einhergehen würde, würde dem Gedanken des NIS-Gesetzes, für die Sicherheit dieser Betreiber zu sorgen, wohl zuwiderlaufen.

7.5.3.3. Konsultation mit anderen Mitgliedstaaten bei der Ermittlung von Betreibern

Sofern eine Einrichtung einen wesentlichen Dienst in zwei oder mehr Mitgliedstaaten anbietet, sollten diese Mitgliedstaaten zur Ermittlung des Betreibers untereinander bilaterale oder multilaterale Beratungen aufnehmen, um die kritische Rolle des Betreibers im Hinblick auf grenzüberschreitende Auswirkungen zu beurteilen.[865] Im Gegensatz zu den eben genannten Erwägungsgründen sieht der Richtlinientext selbst sogar eine Verpflichtung einer solchen Konsultation vor, bevor eine Entscheidung über die Ermittlung getroffen wird (Art. 5 Abs. 4 NIS-RL).

Auch die nationale Umsetzung im NIS-Gesetz regelt, dass eine Entscheidung, ob ein Betreiber wesentlicher Dienste gem. § 16 Abs. 1 zu ermitteln ist, erst nach erfolgter Konsultation mit dem oder den anderen Mitgliedstaaten der Europäischen Union getroffen werden kann, sofern ein Betreiber einen Dienst noch in einem oder mehreren Mitgliedstaaten der Europäischen Union bereitstellt (§ 16 Abs. 4 NISG).

Die zentrale Anlaufstelle wäre nach Empfehlungen der Kooperationsgruppe[866] die geeignete Stelle zur Aufnahme dieser Konsultation, kann aber auch bei anderen zuständigen Behörden etabliert werden. In Österreich kommt diese Aufgabe dem Bundeskanzler als zuständige Stelle für die Ermittlung der Betreiber zu (§ 16 Abs. 4 Z 2).

In diesem Zusammenhang unstimmig ist meines Erachtens der in ErwGr 24 genannte Zweck dieser Konsultation, nämlich die Beurteilung der kritischen Rolle des Betreibers im Hinblick auf grenzüberschreitende Auswirkungen. Sowohl die Kriterien der NIS-RL als auch jene des NIS-Gesetzes für die Ermittlung von Betreibern wesentlicher Dienste sprechen lediglich von der nationalen Bedeutung des jeweiligen Dienstes, nicht von einer grenzüberschreitenden Kritikalität. Diese Information kann lediglich dann an Bedeutung gewinnen, wenn ein nationaler Sicherheitsvorfall (§ 3 Z 6) eintritt und die nationalen Behörden jene Mitgliedstaaten der Europäischen Union informieren sollen, die von diesem Vorfall ebenso betroffen sein könnten (§

[864] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 730.
[865] ErwGr 24 NIS-RL.
[866] Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact, 2018, S. 9.

19 Abs. 4). Für die Ermittlung selbst hat diese Information jedoch keinerlei Bedeutung, weshalb mE unverständlich bleibt, warum diese Konsultation vor der nationalen Ermittlung verpflichtend[867] (§ 16 Abs. 4 Z 2) zu erfolgen hat.

7.5.3.4. Bekanntgabe einer Kontaktstelle durch Betreiber

Betreiber wesentlicher Dienste haben dem Bundeskanzler innerhalb von zwei Wochen nach Zustellung des Bescheids eine Kontaktstelle für die Kommunikation mit den öffentlichen Stellen zu nennen (§ 16 Abs. 3 NISG). Die Erläuternden Bemerkungen nennen als Beispiele für Kontaktstellen eine Telefonnummer und eine E-Mail-Adresse.[868] Das Bundeskanzleramt und das Bundesministerium für Inneres haben im Jänner 2019 in einer veröffentlichten Leitlinie („NIS Fact-Sheet“[869] die Kontaktstellen von Betreibern wesentlicher Dienste näher beschrieben.[870]

Diese beschreiben nähere Umstände zur Einrichtung der Kontaktstelle, die aus dem Gesetz selbst nicht erkennbar sind. Beispielsweise kommt als Kontaktstelle auch ein externer IT-Dienstleister in Frage[871], wobei jedoch jedenfalls darauf zu achten ist, dass eine „Kommunikation in der Staatssprache Deutsch möglich ist“. [872] In Kapitel 7.5.4.2 wird näher auf die Frage eingegangen, ob das Fact-Sheet zu den IKT-Sicherheitsstandards[873] als Verordnung zu qualifizieren ist. Was dort als Grenzfall eher verneint wurde, soll aus dort genannten Gründen auch für gegenständliche Leitlinien gelten. Dies insbesondere deshalb, da im NIS-Gesetz nähere Regelungen zu Kontaktstellen per Verordnung nicht vorgesehen sind.[874]

Dies hat jedoch auch zur Folge, dass die im Fact-Sheet genannten Voraussetzungen, die sich weder aus dem Gesetz noch aus den Erläuternden Bemerkungen ergeben, keine Rechtsfolgen nach sich ziehen und für die Betreiber wesentlicher Dienste keine Verpflichtung zur Umsetzung besteht.

---

[867] Zur Konsultation als Ermittlungs- und somit Verfahrenserfordernis siehe *Anderl et al.*, NISG::Kommentar, § 16, Rz 75.
[868] EB RV NIS-Gesetz, S. 18.
[869] *Bundeskanzleramt/Inneres*, NIS Fact Sheet 01/2019, Kontaktstellen von Betreibern wesentlicher Dienste, 2019.
[870] Zur Frage der Rechtsqualität dieses Fact-Sheet siehe Kapitel 7.5.4.2
[871] Siehe dazu auch *Anderl et al.*, NISG::Kommentar, § 16, Rz 68.
[872] *Bundeskanzleramt/Inneres*, NIS Fact Sheet 01/2019, Kontaktstellen von Betreibern wesentlicher Dienste, 2019.
[873] *Bundeskanzleramt*, NIS Fact Sheet 08/2018, Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices, 2018.
[874] dies alleine lässt nicht auf das Nicht-Vorliegen einer Verordnung schließen, wenngleich diese dann als rechtswidrig zu qualifizieren wäre. Siehe dazu *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 725.

7.5.4. Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste

Gem. Art. 14 Abs. 1 NIS-RL stellen die Mitgliedstaaten sicher, dass Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.

Gem. Abs. 2 stellen die Mitgliedstaaten überdies sicher, dass die Betreiber wesentlicher Dienste geeignete Maßnahmen ergreifen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit der von ihnen für die Bereitstellung dieser wesentlichen Dienste genutzten Netz- und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.

7.5.4.1. Sicherheitsvorkehrungen nach dem Stand der Technik (Standards, Normen)

In der nationalen Umsetzung werden Betreiber wesentlicher Dienste verpflichtet, in Hinblick auf die von ihnen betriebenen wesentlichen Dienste geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zur Gewährleistung der Sicherheit von Netz- und Informationssystemen zu treffen, wobei der Stand der Technik zu berücksichtigen ist und diese dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein haben (§ 17 Abs. 1 NISG).

Wesentlich ist hier die Einschränkung auf jene Netz- und Informationssysteme, die die Betreiber für die Bereitstellung des wesentlichen Dienstes nutzen, die in dieser Form zwar nicht in Art. 14 NIS-RL, jedoch im ErwGr 22 der Richtlinie zu finden ist. Einrichtungen können demnach sowohl wesentliche als auch unwesentliche Dienste erbringen, wobei als Beispiel im Bereich der Luftfahrt das Start- und Landebahn-Management als wesentlicher bzw. die Bereitstellung der Einkaufsbereiche im Flughafengebäude als unwesentlicher Dienst genannt werden. Die identifizierten Einrichtungen sollen nur in Bezug auf die wesentlich geltenden Dienste – die gemäß § 16 Abs. 2 NISG ermittelt werden – die spezifischen Sicherheitsanforderungen erbringen müssen. Da die Aufrechterhaltung genau jener Dienste Ziel der Richtlinie ist, folgt diese Einschränkung der grundsätzlichen Systematik der Richtlinie, wie später auch hinsichtlich der Meldepflicht[875] zu sehen sein wird. [876]

[875] Siehe dazu Kapitel 7.5.6.
[876] So auch *Anderl et al.*, NISG::Kommentar, § 17, Rz 4.

Der Hinweis auf verhältnismäßige sowie dem Risiko angemessene Sicherheitsvorkehrungen bildet insbesondere den im Bereich der Netz- und Informationssicherheit praktizierten „risikobasierten Ansatz“ ab.[877] Dieser risikobasierte Ansatz findet insbesondere auch in der Datenschutz-Grundverordnung seine Anwendung.[878] Auch die NIS-RL selbst spricht von Sicherheitsvorkehrungen, die dem bestehenden Risiko angemessen sind (Art. 14 Abs. 1). Diese erforderliche Angemessenheit im Verhältnis zu den Risiken wird damit begründet, dass Betreibern wesentlicher Dienste keine unverhältnismäßigen finanziellen und administrativen Belastungen entstehen.[879]

Die Betreiber haben darüber hinaus dem Stand der Technik entsprechende Sicherheitsvorkehrungen zur Gewährleistung der Netz- und Informationssystemsicherheit zu treffen. Auf den Stand der Technik wird in zahlreichen Normen verwiesen, insbesondere auch in der DSGVO (Art. 32 Abs. 1) sowie im TKG (§ 16a Abs. 2).[880]

Unter dem "Stand der Technik" ist nach den heute inhaltlich weitgehend übereinstimmenden Legaldefinitionen der auf den einschlägigen wissenschaftlichen Erkenntnissen beruhende Entwicklungsstand fortschrittlicher technologischer Verfahren, Einrichtungen und Betriebsweisen, deren Funktionstüchtigkeit erprobt und erwiesen ist, zu verstehen, wobei insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen sind. Maßgeblich ist der internationale, anlagenspezifische Stand der Technik. Das Tatbestandsmerkmal "erprobt und erwiesen" ist der entscheidende Ansatzpunkt im Rahmen der verschiedenen Legaldefinitionen des Begriffes "Stand der Technik".[881]

Die DIN EN 45020 definiert den Stand der Technik als ein zu einem bestimmten Zeitpunkt bewährtes und in der Praxis erprobtes Stadium von Maßnahmen, die auf den diesbezüglichen gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung basieren.[882]

In § 8a BSI-Gesetz in Deutschland wird ebenso auf den Stand der Technik – in diesem Fall konkret hinsichtlich der Netz- und Informationssystemsicherheit - Bezug genommen, wobei darunter laut Gesetzesbegründung „der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder

[877] EB RV NIS-Gesetz, S. 19.
[878] Siehe beispielsweise die vergleichbare Bestimmung in Art. 32 DSGVO (Sicherheit der Verarbeitung), mehr zum risikobasierten Ansatz auch *Buchner*, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, Datenschutz und Datensicherheit - DuD, 3/2016, S. 157.
[879] ErwGr 53 NIS-RL.
[880] Siehe dazu Kapitel 5.2 sowie 5.5.
[881] VwGH 2008/05/0115; siehe auch Saria (Hg.), Stand der Technik, S. 34f.
[882] *Michaelis*, Der "Stand der Technik im Kontext regulatorischer Anforderungen", Datenschutz und Datensicherheit - DuD, 2016, ebenso DIN EN 45020.

Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt“ verstanden wird.[883]

Das NIS-Gesetz geht – im Gegensatz zu den beiden genannten Rechtsmaterien DSGVO und TKG – näher auf die Erfordernisse ein, was unter dem Begriff des Standes der Technik im Regelungskontext zu verstehen ist. Gemäß § 4 Abs. 2 Z 3 NISG kann der Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres Sicherheitsvorkehrungen, die jedenfalls[884] zur Gewährleistung der Anforderungen nach Abs. 1 geeignet sind, durch Verordnung festlegen.

Darüber hinaus können Betreiber wesentlicher Dienste gemeinsam mit Sektorenverbänden sektorenspezifische Sicherheitsvorkehrungen zur Gewährleistung der Anforderungen nach Abs. 1 vorschlagen (Abs. 2), wobei der Bundesminister für Inneres auf Antrag feststellt, ob diese geeignet sind, die Anforderungen zu erfüllen. Der Grund für die Verwendung dieses unbestimmten Begriffes und Verweis auf Verordnungen liegt im Umstand, dass der Gesetzgeber, hätte er tatsächlich einmal eine detaillierte Regelung getroffen, diese laufend auf den jeweils neuesten Stand bringen müsste.[885] Ein Zweck der Verwendung des Begriffes „Stand der Technik“ ist es also, die Regelung dynamisch zu halten, um die Weiterentwicklung einerseits zu berücksichtigen, andererseits aber die getroffene Regelung nachhaltig zu fassen.[886] Aus diesem Grund handelt es sich auch nicht um eine verfassungswidrige formalgesetzliche Delegation (näheres dazu siehe auch Kapitel 7.5.3.2 [Rechtliche Möglichkeiten zur Umsetzung der Ermittlung von Betreibern wesentlicher Dienste]).

Im Richtlinientext findet sich eine weitere Bestimmung zur möglichen Auslegung des Standes der Technik. Demnach sollen die Mitgliedstaaten gemäß Art. 19 Abs. 1 NIS-RL ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen fördern.

Im Rahmen dessen soll die ENISA Leitlinien zu den technischen Bereichen erlassen, die in Bezug auf Abs. 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen – einschließlich der nationalen Normen der Mitgliedstaaten -, mit denen diese Bereiche abgedeckt werden können

[883] *Michaelis*, Datenschutz und Datensicherheit - DuD, 2016, S. 460 bzw. BT-Drs. 18/4096, S. 26.
[884] EB RV NISG, S. 19.
[885] Siehe dazu auch BVerfGE 49, 89 (135 f) (Beschluss vom 8.8.1978).
[886] *Knopp*, Stand der Technik, Ein alter Hut oder eine neue Größe?, Datenschutz und Datensicherheit - DuD, 11/2017, S. 666.

(Abs. 2). Die Harmonisierung[887] solcher Anforderungen würde die Einhaltung durch oftmals in mehreren Mitgliedstaaten wesentliche Dienste zur Verfügung stellende Betreiber wesentlich vereinfachen.[888]

Die Leitlinien wurden im Februar 2018 von der Kooperationsgruppe mit dem „Reference document on security measures for Operators of Essential Services"[889] veröffentlicht, wobei im Dokument auf keine international anerkannten Normen Bezug genommen wird. Da es sich bei diesen Leitlinien weder um eine nach Art. 288 AEUV verbindliche noch um eine der genannten unverbindlichen Rechtsformen (Empfehlung, Stellungnahme)[890] handelt, besteht für den nationalen Gesetzgeber grundsätzlich keine Verpflichtung, sich an diesen Leitlinien zu orientieren.

Nach der Rechtsprechung des EuGH[891] sind die nicht verbindlichen Empfehlungen und Stellungnahmen „nicht als rechtlich völlig wirkungslos anzusehen, sondern von innerstaatlichen Gerichten bei der Entscheidung über bei ihnen anhängige Rechtsstreitigkeiten zu berücksichtigen".[892] Nach Rechtsprechung des VwGH[893] kommen Empfehlungen (im Vergleich zu sonstigen „soft law"-Instrumenten[894]) insbesondere dann höhere Bedeutung zu, wenn in der Richtlinie selbst spezifisch und eng determiniert die Kommission mit der Erlassung dieser Empfehlung beauftragt wird und ausdrücklich ein Berücksichtigungsgebot für die nationale Behörde, verbunden mit Verfahrensvorschriften für den Fall des Abweichens, festgelegt wird.

Dies könnte nach *Müller*[895] deshalb problematisch sein, weil Leitlinien, Richtlinien, Mitteilungen und Empfehlungen von Gemeinschaftsorganen, denen innerstaatlich weder Verordnungs- noch Bescheidqualität zukommt, der Kontrolle der Gerichtshöfe des öffentlichen Rechts entzogen sind, was zu wesentlichen Rechtsschutzdefiziten führen würde, käme ihnen Normativität zu. Der VwGH akzeptierte bereits 2003 in seinem grundlegenden Erkenntnis, dass die belangte Behörde im angefochtenen Bescheid von einer Explanatory Note der EU-Kommission abwich, ihr also

[887] Viele Praktiker verweisen mittlerweile auf internationale Koordination, Kooperation und gemeinsame Ausrichtung anstatt einer regulatorischen Harmonisierung, siehe *Marchant/Allenby*, Soft law: New tools for governing emerging technologies, Bulletin of the Atomic Scientists, 04 March 2017, Vol.73(2), p.108-114,
[888] COM(2017) 476 final ; siehe auch *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, S. 300.
[889] Siehe https://ec.europa.eu/digital-single-market/en/nis-cooperation-group, abgerufen am 28.04.2019.
[890] *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, S. 297.
[891] Urteil vom 13. Dezember 1989, Rs C-322/88, Grimaldi, Slg 1989, 4407.
[892] *Calliess* in Calliess /Ruffert, EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar.
[893] VwSlg 17136 A/2007.
[894] Zur Einstufung von Empfehlungen als ein Quelle von Soft Law siehe *Köndgen*, Europäische Methodenlehre, in Riesenhuber (Hrsg), de Gruyter Handbuch (2015).
[895] *Müller*, Das österreichische Regulierungsbehördenmodell, S. 437.

offensichtlich keine innerstaatliche Rechtserheblichkeit zumaß.[896] Er wies darauf hin, dass auf Empfehlungen der EU-Kommission Bedacht zu nehmen wäre, ohne sie allerdings als verbindliche Anordnungen zu verstehen. Auch im gegenständlichen Fall kommt genannter Leitlinie eben keine Normativität zu, weshalb der fehlende Rechtsschutz nicht weiter problematisch erscheint.

Obwohl in Art. 19 NIS-RL spezifisch auf durch die ENISA zu erlassenden Leitlinien[897] verwiesen wird, werden die oben genannten Voraussetzungen – insbesondere die Rechtsform der Empfehlung – nicht erfüllt, weshalb es sich bei den Leitlinien keinesfalls um verpflichtend umzusetzende Vorgaben handelt.

In Anlehnung an den ersten Satz des Art. 19 Abs. 1 NIS-RL würde in der nationalen Gesetzgebung – anstatt des Verweises auf den Stand der Technik oder auch das Referenzdokument der Kooperationsgruppe - konkret die Bezugnahme auf die internationale Norm DIN[898] ISO[899]/IEC 27001 auf der Hand liegen.[900] Unter einer Norm ist nach DIN EN 45020 ein Dokument zu verstehen, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt.[901]

Derartige Regelungen werden von privaten Standardisierungsorganisationen wie Austrian Standards[902], dem Deutschen Institut für Normung e.V. (DIN) oder der International Organization for Standardization (ISO) erlassen und sind unbestritten aus sich selbst heraus rechtlich unverbindlich.[903] Die ISO/IEC 27001 ist eine internationale Norm für Informationssicherheit in privaten, öffentlichen oder gemeinnützigen Organisationen und beschreibt die Anforderungen für das Einrichten, Realisieren, Betreiben und Optimieren eines dokumentierten Informationssicherheits-Managementsystems.[904]

Möchte man in Rechtsakten auf diese von privaten Organisationen herausgegebenen technischen Normen verweisen, stellt sich die Frage der Zulässigkeit solcher Verweise. Dabei muss zwischen

---

[896] VwGH 18.11.2003, 2002/03/0284. Ebenso der VwGH in einer Entscheidung vom 8.9.2004, 2003/03/0119.
[897] ErwGr 38 NIS-RL.
[898] Deutschen Institut für Normung e.V. (DIN).
[899] International Organization for Standardization (ISO).
[900] Zur Eignung der ISO 27000-Normenreihe siehe auch *Kipker/Pfeil*, IT-Sicherheitsgesetz in Theorie und Praxis, 12/2016, S. 810.
[901] Siehe DIN EN 45020.
[902] https://www.austrian-standards.at/home/, abgerufen am 29.09.2018.
[903] *Zubke-von Thünen*, Technische Normung in Europa (1999), S. 312.
[904] Mehr zur ISO 27001 siehe *Kersten/Klett/Reuter et al.*, IT-Sicherheitsmanagement nach der neuen ISO 27001 (2016).

statischen und dynamischen Verweisen durch den Gesetzgeber unterschieden werden.[905] Da Normen laufend weiterentwickelt werden und die Aktualität der Norm den Zweck des Verweises auf Selbige erfüllt, ist zuerst an einen dynamischen Verweis auf die technische Norm zu denken.

Verfassungsrechtliche Bedenken bestehen hier insbesondere deshalb, da diese technischen Normen durch private Institutionen fortentwickelt werden. Beispielsweise werden die Österreichischen Normen (ÖNormen) vom Österreichischen Normungsinstitut, einem privatrechtlich konstituierten Verein, herausgegeben.[906] Der Gesetzgeber könnte die künftige Entwicklung der Bezugsnorm nicht selbst bestimmen und würde damit seine Rechtsetzung indirekt auf Private übertragen.[907]

Die statische Verweisung auf technische Normen bringt den Nachteil mit sich, dass diese möglicherweise inhaltlich überholt und durch neue Regeln ersetzt wurden[908]. Grundsätzlich kommt Normen der Charakter einer generellen Norm zu, sofern sie durch Rechtsvorschriften für verbindlich erklärt wurden, sonst sind sie nur Richtlinien.[909] Damit ist in der Rechtsordnung jedenfalls eine Mitbestimmung nichthoheitlicher Maßstabsgebung[910] gegeben, auch wenn gerade kein Verweis in einer Rechtsvorschrift vorliegt. Diese Lösung wird oftmals dann herangezogen, wenn die Schaffung von Recht auf unüberwindbare politische Hürden trifft.[911]

7.5.4.2. Sicherheitsvorkehrungen gem. § 4 Abs. 2 Z 3, die jedenfalls dem Stand der Technik entsprechen und zum Begriff des Soft Law

Der Bundeskanzler kann im Einvernehmen mit dem Bundesminister für Inneres Sicherheitsvorkehrungen, die jedenfalls zur Gewährleistung der Anforderungen nach § 17 Abs. 1 geeignet sind, durch Verordnung festlegen (§ 4 Abs. 2 Z 3).[912] Bei dieser Verordnung handelt es sich um die Netz- und Informationssystemsicherheitsverordnung (NISV). Gemäß Art. 19 Abs. 1 NIS-RL sollen die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer oder international anerkannter Normen

[905] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 19.073, 27.34.
[906] OGH 26.06.2001 5 Ob 70/01g.
[907] *Hübner*, Wie wirken Standards und Normen im Recht?, Datenschutz und Datensicherheit - DuD, 2011, S. 56.
[908] *Hartlieb*, Verweisung auf technische Normen in Rechtsvorschriften (1982), S. 15.
[909] 1 Ob 359/98w, 7 Ob 265/00x.
[910] *Wolff* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rz 33.
[911] *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, S. 248.
[912] § 17 Abs. 1 NISG spricht lediglich davon, dass der Bundeskanzler mit Verordnung Sicherheitsvorkehrungen festlegen kann. Die EB ergänzen diese Bestimmung insofern, als damit jene Sicherheitsvorkehrungen festgelegt werden, die jedenfalls zur Gewährleistung der Anforderungen nach Abs. 1 geeignet sind, siehe EB RV NIS-Gesetz, S. 19.

und Spezifikationen für die Sicherheit von Netz- und Informationssystemen fördern. Im Rahmen dessen soll die ENISA Leitlinien zu den technischen Bereichen erlassen, die in Betracht zu ziehen sind, wobei die Kommission die Mitgliedstaaten anregt, den entwickelten Leitlinien genau zu folgen, sodass sich nationale Bestimmungen über die Sicherheitsanforderungen soweit wie möglich daran ausrichten. Diese Leitlinien wurden im Februar 2018 von der Kooperationsgruppe[913] mit dem „Reference document on security measures for Operators of Essential Services"[914] veröffentlicht und beinhalten allgemeine Vorkehrungen in den Bereichen Governance und Eco-Systeme, Schutz, Verteidigung und Resilienz.[915] Die in der nationalen Umsetzung in der NISV festgelegten Vorkehrungen orientieren sich an dieser Leitlinie.[916]

Um für die Betreiber wesentlicher Dienste ein höheres Maß an „Rechtssicherheit"[917] zur Umsetzung der Sicherheitsvorkehrungen zu gewährleisten[918], wurde anhand der in der Verordnung definierten (sehr allgemein gehaltenen) Vorkehrungen durch den Bundeskanzler und den Bundesminister für Inneres ein Leitfaden erstellt, der die in Anhang 1 der NISV vorgesehenen Sicherheitsvorkehrungen bestehenden Normen und Standards beschreibt, zuordnet („Mapping")[919] und Anwendungsbespiele sowie sektorenspezifische Standards anführt. Grundsätzlich wäre es denkbar gewesen, die genaue Beschreibung direkt in der Verordnung zu regeln. Dies würde der Regelungstechnik einer Legaldefinition des „Standes der Technik" gleichkommen, wodurch es gerade zur Vernichtung jener Spielräume kommt, die mittels Rückgriffs auf den „Stand der Technik" erst geschaffen werden sollen.[920]

Untersucht werden soll, ob der vom Bundeskanzler und vom Bundesminister für Inneres entwickelte Leitfaden als Verordnung zu qualifizieren ist. *Raschauer*[921] beschreibt mehrere Voraussetzungen für das Vorliegen einer Verordnung. Urheber des Aktes muss eine Verwaltungsbehörde sein, der eine Ermächtigung zu hoheitlichem Handeln zukommt und es muss ein Mindestmaß an Publizität[922] erlangt werden. Außerdem muss ein normativer Inhalt in der

---

[913] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group, abgerufen am 10.05.2019.

[914] https://circabc.europa.eu/sd/a/c5748d89-82a9-4a40-bd51-44292329ed99/reference_document_security_measures_OES.pdf, abgerufen am 10.05.2019.

[915] „Governance and Ecosystem", „Protection", „Defense", „Resilience".

[916] Netz- und Informationssystemsicherheits-Verordnung (NISV), Anhang I.

[917] Zur Kritik der Rechtsunsicherheit in Deutschland siehe *Kipker/Pfeil*, 2016, S. 811.

[918] *Anderl et al.*, NISG::Kommentar, § 17, Rz 9.

[919] Zur Möglichkeit der Implementierung internationaler Standards im nationalen Recht durch Soft Law siehe *Kwiatkowski*, Soft Law in International Governance, Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza, 2017, Vol.7(1), pp.93-103, S. 95.

[920] *Saria*, Grundsätzliches zum "Stand der Technik" aus rechtswissenschaftlicher Sicht, in Saria (Hrsg), Der "Stand der Technik" (2007), S. 33.

[921] Für alle dargestellten Voraussetzungen siehe *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 729ff.

[922] Vgl zB VfSlG 16281/2001, VfGH 13.12.2007, V56/07.

Gestaltung oder verbindlichen Feststellung der Rechtslage zu sehen sein, wobei auch generell-abstrakte „Feststellungen“ normativ wirken können. Auf die Bezeichnung des Aktes kommt es jedenfalls nicht an bzw. existiert für Verordnungen keine verfassungsrechtliche Bezeichnungspflicht.

Festzustellen ist, dass § 4 Abs. 2 Z 3 NISG den Bundeskanzler und den Bundesminister für Inneres zur Festlegung der Sicherheitsvorkehrungen nach § 17 Abs. 1 mit Verordnung ermächtigt. Dazu ist anzumerken, dass es für die Möglichkeit der Erlassung einer Durchführungsverordnung durch eine Verwaltungsbehörde keiner expliziten Verordnungsermächtigung bedarf, da sich dies unmittelbar aus Art. 18 Abs. 2 B-VG ergibt, sofern die Verordnung bestehende gesetzliche Regelungen bloß konkretisiert.[923] Sofern der Verordnungsgeber jedoch ermächtigt werden soll, die Rechtslage (im Verhältnis zur Gesetzeslage) zu „gestalten“, muss dies gesetzlich ausdrücklich vorgesehen werden.[924] Im Fall der Sicherheitsvorkehrungen handelt es sich mE lediglich um eine Konkretisierung jener gesetzlichen Regelung, welche die Betreiber dazu verpflichtet, technische und organisatorische Sicherheitsvorkehrungen zu treffen (§ 17 NISG), weshalb § 4 Abs. 2 Z 3 NISG grundsätzlich obsolet gewesen wäre. Die Ermächtigung macht jedoch insofern Sinn, um dadurch festzulegen, welche Verwaltungsbehörde für die Erlassung dieser Verordnung – nämlich im gegenständlichen Fall der Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres – zuständig ist. Eine Verpflichtung für den Verordnungsgeber, eine solche Verordnung zu erlassen, ergibt sich dadurch nicht.[925]

Die aufgrund dieser Bestimmung ergehende Verordnung ist zwar primär die NISV. Dies schließt mE jedoch die Kundmachung einer weiteren, diesen Bereich regelnden Verordnung per se nicht aus.

Raschauer nennt als zentrales Kriterium der Untersuchung, ob eine Verordnung vorliegt, welchen Akt der Gesetzgeber für ein bestimmtes Verwaltungshandeln vorgesehen hat.[926] Bezeichnet werden die Leitlinien als „NIS Fact Sheet – Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices“, wobei dies wie oben dargestellt für die Qualifikation als Verordnung irrelevant ist. Als Herausgeber sind das Bundeskanzleramt und das Bundesministerium für Inneres angeführt, denen einerseits der Charakter einer Verwaltungsbehörde und andererseits die grundsätzliche Ermächtigung zur Ausübung von Hoheitsgewalt[927] im Bereich der Netz- und Informationssystemsicherheit zukommt.

---

[923] Siehe dazu bspw VfSlg 11653/1988.
[924] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 782.
[925] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 777.
[926] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 726.
[927] Wenngleich der Behördencharakter lediglich dem Bundeskanzler und dem Bundesminister für Inneres (anstatt dem Bundeskanzleramt und dem Bundesministerium für Inneres) zukommt, schadet dies der Qualifizierung mE nicht.

Ergeht ein genereller Akt in einem „Bereich“, der nach seiner gesetzlichen Ausgestaltung als Teil der Hoheitsverwaltung zu werten ist, dann ist dies ein Indiz für den Verordnungscharakter des Aktes.[928] Das Fact-Sheet wird auf der Website des Bundeskanzleramtes publiziert und erreicht damit auch das geforderte Maß an Veröffentlichung. Die zentrale Frage ist darin zu sehen, ob es sich dabei um einen normativen Inhalt in Form einer Gestaltung oder verbindlichen Feststellung der Rechtslage handelt. Dabei können auch generell-abstrakte Feststellungen normativ wirken, da nach der Feststellung andere Regeln anwendbar sind als vor der Feststellung – Akte mit bloß informativer (und nicht normativer) Qualität fallen hingegen nicht darunter.[929] Nach Auffassung von *Zeder* führe dann, wenn ein Dokument[930] einer Verwaltungsbehörde generell-abstrakte Normen enthalte, welche sich an den Rechtsunterworfenen richten, kein Weg daran vorbei, dieses als Rechtsverordnung iSd Art. 18 Abs. 2 B-VG zu sehen.[931] Dem entgegnet *Raschauer,* dass eine der Behördentransparenz entsprechende Information der Öffentlichkeit – durch Kundmachung im Internet – diese nicht zu einer Verordnung mache, sondern dem Dokument vielmehr selbstbindende Wirkung zukomme.[932]

Diese selbstbindende Wirkung[933] ergibt sich unmittelbar aus dem verfassungsrechtlichen Vertrauensschutzprinzip, das unter anderem einen eng begrenzten Schutz von begründeten Erwartungshaltungen und damit in Zusammenhang stehenden Dispositionen und Investitionen bei sonstigen Rechtsänderungen verbürgt.[934] *Feiel*[935] begründete in ähnlichen Fällen im TKG, dass eine bestimmte Vertrauenslage betreffend die Anwendung oder Auslegung von Rechtsvorschriften gegenüber den Rechtsunterworfenen geschaffen werde, ohne dass diese aber daran gebunden wären. Ein Abweichen davon in einer Entscheidung der Behörde ohne sachliche Rechtfertigung

[928] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 736.

[929] Grenzfälle bilden zT auf Transparenz des Behördenverhaltens abzielende Kundmachungen der Rechtsauffassung, siehe dazu *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 764.

[930] In diesem Fall ging es um ein gem. § 11 Abs. 3 WettbG im Internet veröffentlichtes Handbuch der Bundeswettbewerbsbehörde.

[931] *Zeder*, Die österreichischen Kartellbußen am Maßstab des Kriminalrechts, Juristische Blätter, 8/2007, S. 483.

[932] *Raschauer* begründete dies damit, dass eine derartige Deutung nicht nur zu erheblichen rechtlichen Problemen führen würde, sondern auch die Rechtsdogmatik, seit dem Betritt Österreichs zur EU, vorsichtiger geworden sei, weil man sich immer wieder mit Phänomenen konfrontiert sehe, die nicht in die traditionellen Lehrbuchkategorien passen würden. *Raschauer*, Die Bundeswettbewerbsbehörde und Art. 6 EMRK, Österreichische Zeitschrift für Wirtschaftsrecht, 2/2008, S. 37f.

[933] Selbst praktische Verwaltungsabläufe, die in hohem Maße durch Verwaltungsbrauch bestimmt sind, können unter Gesichtspunkten des Vertrauensschutzes zu rechtserheblichen Selbstbindungen führen, siehe *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 467.

[934] *Berka*, Verfassungsrecht, Rz 1692.

[935] *Feiel*, Telekomrecht als Regulierungsrecht, in Raschauer (Hrsg), Aktuelles Telekommunikationsrecht (2005), S. 33.

würde demnach einem Akt der Willkür nicht unähnlich und daher mit einem in die Verfassungssphäre reichenden Mangel behaftet sein können.

Der Rechtsunterworfene muss im gegenständlichen Fall somit darauf vertrauen können, dass die Verwaltungsbehörde den von ihr veröffentlichten Leitfaden auch anwendet.

Ein Blick in das Fact-Sheet selbst ergibt, dass dieses „im Sinne der guten Kooperation" erstellt und „als Hilfestellung bzw. zur Vorbereitung" zur Verfügung gestellt wurde. Darüber hinaus wird darauf hingewiesen, dass Änderungen des Fact Sheets vorbehalten sind.[936] Durch den dadurch nach außen in Erscheinung tretenden Staatswillen (der nach *Raschauer* für die Qualifizierung maßgeblich sein soll)[937] wird von keiner Verordnung auszugehen sein, wenngleich es sich mE um einen Grenzfall handelt.

Der vom Bundeskanzler und Bundesminister für Inneres entwickelte Leitfaden könnte eher unter den mittlerweile üblichen Begriff des „Soft Law"[938] subsumiert werden, wenngleich Regelungen vom Soft Law-Geber selbst kaum je als solches bezeichnet werden.[939]
Beim Begriff des Soft Law handelt es sich um einen Oberbegriff[940] für eine Vielzahl von Regelungsformen, in seiner engeren Auslegung um von Hoheitsträgern bzw. mit der Ausübung von Hoheitsgewalt befassten Stellen geschaffene verhaltensbezogene Regelungen, die über keine oder nur eine auf die Innensphäre des Regelungsgebers bezogene Rechtsverbindlichkeit verfügen und die ihre Steuerungswirkungen auf außerrechtlichem Wege erzielen.[941]

Ziel dieses Leitfadens ist die (technische) Konkretisierung der Gesetzes- bzw. Verordnungsbestimmungen[942], wenngleich dem Leitfaden keine unmittelbare Rechtswirkung zukommt. Die Betreiber wesentlicher Dienste erfüllen die Sicherheitsvorkehrungen jedenfalls, wenn den Erfordernissen der gemäß § 4 Abs. 2 Z 2 NISG erlassenen Verordnung nachgekommen wird. Der Leitfaden bildet an die allgemein gehaltene Verordnung anknüpfend und darauf basierend eine Handlungsanleitung, mit deren Nichtbefolgung jedoch keine Rechtsfolgen verbunden sind.

---

[936] *Bundeskanzleramt*, NIS Fact Sheet 08/2018, Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices, 2018, S. 3.
[937] *Raschauer*, Allgemeines Verwaltungsrecht[3].
[938] *Kempen/Hillgruber*, Völkerrecht[2] (2012).; *Schweisfurth*, Völkerrecht (2006). Siehe auch *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, S. 211.
[939] *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, S. 214.
[940] *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, S. 224.
[941] *Knauff*, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem, S. 228.
[942] Zur Schaffung von "Rechtssicherheit" durch Soft Law siehe *Abbott/Snidal*, Hard and Soft Law in International Governance, International Organization, 3/2003, S. 455; siehe dazu auch Empfehlung Soft Law durch den Rat der Europäischen Union in Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society, S. 194.

Der Begriff des „Soft Law“ ist jedoch innerhalb der österreichischen Rechtsordnung aufgrund des in der herrschenden Lehre[943] und Rechtsprechung[944] anerkannten geschlossenen Rechtsquellensystems schwierig. Dieses besagt, dass der einfache Gesetzgeber keine „neuen“ Rechtsquellen erfinden darf und wird durch das System des Rechtsschutzes vor den Gerichtshöfen des öffentlichen Rechts untermauert, das einen Rechtsschutz nur gegenüber bestimmten Rechtsakten eröffnet.[945] Die primären Anknüpfungspunkte für die Beschwerdezulassung sind nicht das Rechtsverhältnis und die daraus resultierenden Ansprüche, sondern das Vorliegen eines bekämpfbaren Aktes.[946] Konsequenterweise meint *Mayer* daher, dass Verwaltungsakte, die erhebliche Rechtswirkungen haben, nicht als unbekämpfbare Verwaltungsakte konstruiert werden dürfen, weil das verfassungsgesetzliche Rechtsschutzsystem sonst leer laufen würde.[947]

Müller spricht in diesem Zusammenhang wie ein Teil der Lehre[948] von einem bloß „relativ“ geschlossenen Rechtsquellensystem; demnach seien atypische Rechtsquellen dann zulässig, sofern ein angemessenes Niveau von Rechtsschutz zur Verfügung steht und eine besondere sachliche Rechtfertigung vorliegt.[949]

Wie weiter oben bereits erläutert, soll es sich bei den Leitlinien aus Sicht der Behörde eben nicht um einen formellen Rechtsakt mit normativem Charakter, sondern bloß um eine Konkretisierung und Information an die Betreiber handeln. *Raschauer* bezeichnet Akte, die verhaltenssteuernde Appelfunktion gegenüber Unternehmen entfalten und „knapp unterhalb“ der Schwelle der Normativität angesiedelt seien (als Beispiele werden Leitlinien, Empfehlungen und Standards namentlich genannt) als „subnormative Akte“.[950] Es handle sich dabei um Darstellungen der behördlichen Rechtsauffassung, die nicht imperativ-verhaltenssteuernd konzipiert wären. Gegen derartige Auslegungshilfen und Mitteilungen der Rechtsansicht der Behörde bestehen keine verfassungsrechtlichen Bedenken.[951]

Problematisch und verfassungswidrig seien solche Leitlinien nach den Ausführungen von *Müller* dann, wenn diese selbst als Rechtsgrundlage für Bescheide herangezogen werden würden und den

[943] *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11], Rz 167.
[944] VfSlg. 7593/1975, 11.196/1986, 12.682/1991, 13.223/1992, 17.137/2004 ua.
[945] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 464.
[946] *Eberhard*, Der verwaltungsrechtliche Vertrag (2002), S. 333.
[947] *Mayer*, Gleichbehandlungsgesetz und Rechtsschutzstaat, zeitschrift für Arbeits- und Sozialrecht (ZAS), 1/1992, S. 39.
[948] siehe ua. *Griller*, Die Übertragung von Hoheitsrechten auf zwischenstaatliche Einrichtungen (1989), Rz 118.
[949] *Müller*, Das österreichische Regulierungsbehördenmodell, S. 427.
[950] *Raschauer*, Subnormative Verhaltenssteuerungen, in Akyürek /Schäffer (Hrsg), Staat und Recht in europäischer Perspektive (2006), S. 685ff.
[951] Der VfGH brachte bereits mehrmals zum Ausdruck, dass keine Verordnung vorliege, wenn die Behörde bloß ihre Rechtsansicht mitteile – siehe VfSlg 5.300/1966, 5799/1968.

Rechtsunterworfenen ihrer Rechtsschutzmöglichkeiten zur Anfechtung dieser Leitlinien berauben würden.[952] Dies ist bei gegenständlichen Leitlinien nicht der Fall. Das NIS-Gesetz selbst verweist in § 4 Abs. 2 Z 3 darauf, dass Sicherheitsvorkehrungen nach § 17 Abs. 1 mit Verordnung festgelegt werden können, was durch die NISV umgesetzt wurde. Die NISV regelt in ihrem § 11 sowie mit Verweis auf Anlage 1 der NISV die Sicherheitsvorkehrungen in generischer Form, auf die sich das weitere verwaltungsstrafrechtliche Verfahren beziehen würde. Genannte Leitlinien stellen tatsächlich nur eine Auslegungshilfe für die Betreiber dar, auf die sich ein möglicher verwaltungsstrafrechtlicher Bescheid aber nicht beziehen wird dürfen. Sohin dürfte ein Abweichen von diesen Leitlinien – bei gleichzeitiger Erfüllung der generischen gesetzlichen Bestimmungen des NISG und der NISV – per se keine Rechtswidrigkeit durch die Betreiber begründen.[953]

7.5.4.3. Sektorenspezifische Sicherheitsvorkehrungen

Betreiber wesentlicher Dienste können gemeinsam mit ihren Sektorenverbänden im Rahmen des Rechtskonstrukts der Partizipation[954] eigene Sicherheitsvorkehrungen vorschlagen, mit denen die Anforderungen des Abs. 1 gewährleistet werden können und beantragen, dass die Eignung dieser Vorkehrungen durch den Bundesminister für Inneres bescheidmäßig festgestellt wird (§ 17 Abs. 2).[955] Diese Möglichkeit besteht auch für Teilsektoren.[956]

Ziel dieser Bestimmung ist es, auf sektorenspezifische Gegebenheiten bzw. in einzelnen (Teil-) Sektoren existierende Standards[957] Bezug nehmen zu können, da diese womöglich besser für diesen Bereich geeignet sind als die allgemein durch Verordnung vorgegebenen Sicherheitsvorkehrungen gemäß § 4 Abs. 2 Z 3 NISG.[958]

Unter dem Begriff Sektorenverbände könnten jene juristischen Personen zu verstehen sein, die in diversen Bereichen gegenüber dem Staat vertretend für die Betreiber in diesem Sektor auftreten (beispielsweise Interessensvertretungen) oder auch sonst Regelwerke veröffentlichen, die für

[952] *Müller*, Das österreichische Regulierungsbehördenmodell, S. 433.
[953] *Müller*, Das österreichische Regulierungsbehördenmodell, S. 433.
[954] Unter einer Partizipation versteht man die Mitwirkung von Betroffenen oder deren Interessensvertretungsorganisationen an Verwaltungsentscheidungen, siehe auch *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.046.
[955] Zur Regelung der Branchenstandards im ITSiG in Deutschland siehe *Gitter/Meißner/Spauschus*, Das IT-Sicherheitsgesetz, Datenschutz und Datensicherheit - DuD, 1/2016, S. 8.
[956] Siehe EB RV NIS-Gesetz, § 17.
[957] Sektorenspezifische Sicherheitsanforderungen sind bspw. auch in der ISO/IEC TR 27019 (Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry) zu finden, siehe auch Informationssicherheit im Smart Grid, Datenschutz und Datensicherheit - DuD, 11/2013.
[958] So auch *Anderl et al.*, NISG::Kommentar, § 17, Rz 10.

Betreiber – wenn auch nur auf freiwilliger Basis – Geltung finden.[959] Dabei stellt sich die Frage, welche Verbände diese Aufgabe für die Betreiber wesentlicher Dienste wahrnehmen könnten. Relevante Sektorenverbände gemäß Abs. 2 in Österreich sind meines Erachtens etwa Oesterreichs Energie[960] im Teilsektor Elektrizität, die Österreichische Vereinigung für das Gas- und Wasserfach[961] im Sektor Gas und der Trinkwasserversorgung oder der Verein Internet Service Providers Austria[962] für einen Teil der Digitalen Infrastrukturen.

Da das Recht auf Vorschlag von sektorenspezifischen Sicherheitsvorkehrungen primär dem Betreiber, und nur gemeinsam mit dem Sektorenverband, zukommt, wird dieser bei Fehlen eines solchen Verbandes (bspw. im Bereich der Gesundheitsversorgung) mE auch einzeln und selbstständig Sicherheitsvorkehrungen vorschlagen bzw. dies auch im Zusammenwirken mit anderen Betreibern aus diesem Sektor veranlassen können.

Der Rechtsgestaltungs-Bescheid[963] des Bundesministers für Inneres zur Feststellung der Eignung muss mE immer unmittelbar an die betroffenen Betreiber wesentlicher Dienste ergehen, nicht an den Sektorenverband. Dies erschließt sich aus der Tatsache, dass nicht der Verband, sondern der Betreiber zur Umsetzung der Sicherheitsvorkehrungen verpflichtet ist und es sich bei gegenständlichem Bescheid um eine Feststellung handelt, dass durch die vorgeschlagenen Vorkehrungen die (vom Betreiber zu erfüllenden) Anforderungen gemäß Abs. 1 erfüllt werden.

7.5.4.4. Unmittelbare Umsetzung der Sicherheitsvorkehrungen nach Zustellung des Bescheides

Betreiber wesentlicher Dienste haben die Erfüllung der Sicherheitsanforderungen dem BMI nachzuweisen (§ 17 Abs. 3 NISG). Die Betreiber haben dazu eine Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen zu übermitteln. Eine Überprüfung durch qualifizierte

[959] Zur Definition siehe *Anderl et al.*, NISG::Kommentar, § 17, Rz 11. Eine andere Definition definiert Sektorverbände insofern, als diese die Sektoren gegenüber dem Staat vertreten und Dienstleistungen für Unternehmen erbringen, siehe *Teuber*, Interessenverbände und Internationalisierung: Dachverbände, Automobilindustrie und Einzelhandel in der Europäischen Union (2009), S. 41.

[960] „Oesterreichs Energie ist die Interessensvertretung der österreichischen E-Wirtschaft. Sie vertritt die gemeinsam erarbeiteten Brancheninteressen gegenüber Politik, Verwaltung und Öffentlichkeit, siehe auch https://oesterreichsenergie.at/ueber-uns.html, abgerufen am 06.10.2018.

[961] „Die Österreichische Vereinigung für das Gas- und Wasserfach unterstützt bereits seit dem 19. Jahrhundert das Ziel einer Versorgung nach dem letzten Stand der Technik. Sie vertritt die Interessen ihrer Mitglieder aus beiden Branchen und sorgt mit ihrem Regelwerk für einheitliche, anerkannte Richtlinien“, siehe auch https://www.ovgw.at/oevgw/, abgerufen am 06.10.2018.

[962] „Die ISPA vertritt als freiwillige Interessensvertretung mehr als 200 Mitglieder aus allen Bereichen rund um das Internet“, siehe auch https://www.ispa.at/ueber-ispa/ueber-ispa.html, abgerufen am 06.10.2018.

[963] Die Rechtslage wird insofern abgeändert, als die Betreiber dieses Sektors ex nunc die sektorenspezifischen Sicherheitsvorkehrungen anstatt jener der NISV umzusetzen haben.

Stellen ist mE somit dann nicht zwingend erforderlich, sofern die durch Verordnung vorgegebenen Sicherheitsanforderungen bereits per durchgeführter Zertifizierungen nachgewiesen werden können. Eine andere Möglichkeit als der Nachweis per Zertifizierung oder Überprüfung einer qualifizierten Stelle – beispielsweise durch eine lediglich interne Überprüfung im Unternehmen -- kommt jedenfalls nicht in Betracht.[964]

Da es sich bei den vorgeschriebenen Sicherheitsvorkehrungen um eine für Betreiber ressourcenmäßig und vor allem zeitlich aufwändige Implementierung handelt[965], stellt sich die Frage nach einer Legisvakanz[966] hinsichtlich der Umsetzung. Die NIS-RL selbst sieht eine solche nicht vor, legt sie doch eine Erlassung und Veröffentlichung von nationalen Rechts- und Verwaltungsvorschriften bis zum 09. Mai 2018, eine Anwendung der Maßnahmen ab 10. Mai 2018 (Art. 25 NIS-RL) sowie keine Übergangsmaßnahmen (Art. 24 NIS-RL) vor. Bei entsprechend offener Formulierung würde eine richtlinienkonforme Interpretation somit dazu führen, dass Betreiber theoretisch bereits ab Zustellung des Bescheides die Sicherheit ihrer Netz- und Informationssysteme im Sinne des § 17 Abs. 1 gewährleisten, diese jedoch nur alle drei Jahre (aktiv) nachweisen müssen (§ 17 Abs. 3).[967]

In der nationalen Umsetzung haben die Betreiber die Sicherheitsvorkehrungen mindestens alle drei Jahre nach Zustellung des Bescheides (§ 16 Abs. 4 Z 1) nachzuweisen (§ 17 Abs. 3) und somit grundsätzlich drei Jahre Zeit, die Vorkehrungen zu implementieren. Darüber hinaus hat der Bundesminister für Inneres jedoch die Möglichkeit, die Einhaltung der Anforderungen gemäß Abs. 1 (jederzeit) durch Einschau vor Ort zu kontrollieren (§ 17 Abs. 4), wobei sich hier keine zeitliche Beschränkung dieser Befugnis findet. Außerdem kann der Bundesminister für Inneres unabhängig davon auch (jederzeit) Empfehlungen aussprechen und die Befolgung bescheidmäßig anordnen (§ 17 Abs. 5).

Einer teleologischen Interpretation[968] folgend wäre eine Einschau sowie das Aussprechen von Empfehlungen Hand in Hand mit dem geregelten dreijährigen Nachweis und somit nach erstmaliger Erbringung des Nachweises durchzuführen, da dies andernfalls die Bestimmung des § 17 Abs. 3 (und somit die dreijährige Frist) unterlaufen würde.

---

[964] Siehe *Anderl et al.*, NISG::Kommentar, § 17, Rz 18.
[965] Siehe dazu die Auflistung der Vorkehrungen und deren breites Spektrum laut NISV.
[966] Zu grundlegenden Ausführungen zur Legisvakanz siehe *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 533.
[967] Zur Kritik an der zu kurzen Frist gem. § 8a BSIG, demnach Betreiber die Sicherheitsvorkehrungen spätestens zwei Jahre nach Inkrafttreten zu treffen haben, siehe *Heinickel/Feiler*, Computer und Recht, 2014, S. 712.
[968] Zu den verschiedenen Aspekten der Gesetzesinterpretation siehe auch *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 555.

Dagegen spricht eine (den Vorrang zu gebende)[969] strenge richtlinienkonforme Interpretation[970] [971], wonach für Betreiber kein Umsetzungsspielraum vorgesehen ist und diese die Sicherheit ihrer Netz- und Informationssysteme bereits ab Bescheidzustellung gewährleisten müssen. Demnach wäre es mE dem Bundesminister jederzeit bzw. bereits vor Ablauf der ersten drei Jahre möglich, den Betreibern bescheidmäßig die Befolgung bzw. Empfehlungen anzuordnen (§ 17 Abs. 5). Tatsächlich wird der Betreiber mE mit Zustellung des Bescheids mit der Umsetzung der Sicherheitsmaßnahmen beginnen und diese spätestens nach Ablauf von drei Jahren implementiert haben müssen.

Diese (im Sinne der richtlinienkonformen Interpretation angenommene) Pflicht zum unmittelbaren und sofortigen Beginn der Umsetzung der Sicherheitsvorkehrungen wirft theoretisch die Frage nach einer Verletzung des Vertrauensschutzprinzips[972] auf, da ein gravierender, nicht vorhersehbarer staatlicher Eingriff in Rechtspositionen in Situationen eines gerechtfertigten Vertrauen-Dürfens mit dem verfassungsrechtlichen Gleichheitssatz unvereinbar sein kann.[973] Zwar verbürgt der verfassungsrechtliche Vertrauensschutz unter anderem auch begründete Erwartungshaltungen und damit in Zusammenhang stehende Dispositionen und Investitionen bei Rechtsänderungen, beschränkt dies jedoch auf Fälle, in denen der Gesetzgeber durch vorheriges Handeln einen besonderen Vertrauenstatbestand geschaffen hat oder wenn es sich um besonders intensive Eingriffe in schutzwürdige Interessen handelt.[974]

Nach der Judikatur des VfGH genießt das Vertrauen auf den unveränderten Fortbestand der gegebenen Rechtslage keinen besonderen verfassungsrechtlichen Schutz.[975] Somit widerspricht es diesem Verfassungsprinzip natürlich nicht, Verpflichtungen einzuführen, die davor nicht geregelt werden. Hinsichtlich des Vertrauens der Betreiber kann außerdem argumentiert werden, dass die Einrichtung geeigneter, verhältnismäßiger, dem Stand der Technik entsprechender Sicherheitsvorkehrungen einerseits nicht unvorhersehbar war, da die gleichlautende Formulierung bereits aus dem im Jahr 2016 kundgemachten Richtlinientext ersichtlich war. Darüber hinaus waren Betreiber auch bisher nach anderen Rechtsgrundlagen verpflichtet, grundlegende, dem Stand der

[969] Zur Möglichkeit des BMI, schon vor Ablauf der dreijährigen Nachweispflicht Einschau in vorhandene Nachweise zu nehmen siehe *Anderl et al.*, NISG::Kommentar, § 17, Rz 20.
[970] Zur richtlinienkonformen Interpretation siehe *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 479.
[971] Zu nennen ist hier grundsätzlich auch die europarechtskonforme Auslegung, deren Ziel eine umfassende Sicherstellung der Europarechtskonformität ist. Der EuGH verwendet die Begriffe der richtlinien- und europarechtskonformen Auslegung synonym. Siehe *Frenz*, Handbuch Europarecht, Band 5, Wirkungen und Rechtsschutz.
[972] Zum Vertrauensgrundsatz als Bestandteil der Gemeinschaftsverfassung im Sinne des primären Gemeinschaftsrechts siehe auch EuGH Rs C-264/90, Wehrs, Slg 1992, I-6285, Rz 15.
[973] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 656.
[974] *Berka*, Verfassungsrecht, Rz 1692.
[975] VfSlg 13.461, 13.657/1993. Zu ähnlich lautenden Entscheidungen des EuGH zum Vertrauensschutzprinzip (bezogen auf die EMRK) siehe *Frenz*, Handbuch Europarecht, Band 4, Europäische Grundrechte, Rz 3012.

Technik entsprechende Vorkehrungen zu treffen, wobei hier generell an das Unternehmensgesetzbuch[976], das Aktiengesetz[977], das Börsegesetz[978] und insbesondere an das bisherige Datenschutzgesetz[979] zu denken ist.

Der verhältnismäßig größere Aufwand für Betreiber entsteht durch das Erbringen des Nachweises durch Zertifizierungen oder Überprüfungen durch qualifizierte Stellen, für den jedoch drei Jahre[980] Zeit bleiben (§ 17 Abs. 3).

7.5.4.5. Befugnis der Einschau durch den Bundesminister für Inneres

Zur Kontrolle der Einhaltung der Sicherheitsanforderungen kann der Bundesminister für Inneres auch Einschau in die Netz- und Informationssysteme und diesbezügliche Unterlagen der Betreiber wesentlicher Dienste nehmen (§ 17 Abs. 4 NISG). Unter der Einschau in Netz- und Informationssysteme ist die Überprüfung beim Betreiber (oder einem externen IT-Dienstleister) vor Ort gemeint und bezieht sich insbesondere auf jene Maßnahmen[981], die durch eine physische Einschau überhaupt erst überprüft werden können. Dazu ist der Bundesminister auch berechtigt, nach vorangegangener Verständigung Örtlichkeiten zu betreten, in welchen Netz- und Informationssysteme gelegen sind (§ 17 Abs. 4). Auch unter der Befugnis zur Einsicht in diesbezügliche Unterlagen[982] wird eine Einsicht vor Ort gemeint sein, da andernfalls die Einsicht in

[976] Gem. § 243 Unternehmensgesetzbuch müssen die wesentlichen Risiken, denen das Unternehmen ausgesetzt ist, beschrieben werden.
[977] Gem. § 84 Abs. 1 Aktiengesetz haben Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden, wobei hier auch die Umsetzung gewisser Security –Richtlinien argumentiert werden könnte, wodurch Unternehmen ein Schaden entsteht.
[978] Gemäß § 9 Börsegesetz hat das Unternehmen über angemessene Vorkehrungen und Systeme zur Ermittlung aller für seinen Betrieb wesentlichen Risiken zu verfügen und wirksame Maßnahmen zur Begrenzung dieser Risiken zu treffen.
[979] Bis zur Umsetzung der Datenschutzgrundverordnung mit 25. Mai 2018 war hier § 14 Abs. 1 DSG anzuwenden, wonach Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt werden mussten.
[980] Der Grund, warum die Betreiber die Anforderungen grundsätzlich (ohne direktes Verlangen der Behörde) alle drei Jahre erbringen müssen, liegt womöglich in den Zyklen anderer Zertifizierungen im Bereich der IT-Sicherheit (bspw. ISO 27.001), siehe dazu *Anderl et al.*, NISG::Kommentar, § 17, Rz 18.
[981] Die Domänen der Sicherheitsmaßnahmen sind in der NISV aufgelistet. Bei jenen, die insbesondere durch Einschau vor Ort (beispielsweise in Log-Dateien oder bestehende Zugriffsrechte) überprüft werden können, handelt es sich mE um die IT-Sicherheitsarchitektur, die IT-Sicherheitsadministration, das Identitäts- und Zugriffsmanagements, die IT-Sicherheitswartung und die Erkennung von Anomalien.
[982] Bei jenen Sicherheitsmaßnahmen, die durch Einsicht in Unterlagen (und nicht durch Einschau in Systeme) überprüft werden können, handelt es sich mE insbesondere um Maßnahmen zur Information System Security Governance und Risikomanagement, zum Ecosystem Management, zur Bewältigung von Sicherheitsvorfällen, zur Betriebskontinuität und zum Krisenmanagement, da diese organisatorischer Natur sind, deren Erfüllung durch Einschau in entsprechende Dokumente überprüft werden kann.

den vom Betreiber übermittelten Nachweis gemäß § 17 Abs. 3 zweiter Satz ausreichen würde und der Gesetzgeber hier offenbar eine Unterscheidung treffen wollte. [983]

Wie weiter oben bereits ausgeführt kann die Einschau durch den Bundesminister für Inneres ohne konkreten Anlass und unabhängig davon erfolgen, ob spezifische Verdachtsmomente vorliegen. Die Regelung in § 17 Abs. 3, wonach der Nachweis erstmals innerhalb von drei Jahren zu erbringen ist, ändert – wie bereits oben dargestellt – nichts daran, dass eine Einschau bereits früher stattfinden kann.

Anderl/Heußler/Mayer/Müller hinterfragen darüber hinaus die grundsätzliche Verfassungskonformität einer solchen Einschau durch den BMI. Die Auditierungen erfolgen grundsätzlich durch so genannte qualifizierte Stellen (siehe Kapitel 7.5.5 [Überprüfung der Sicherheitsvorkehrungen durch qualifizierte Stellen]), wodurch eine zusätzliche Einschau durch den Bundesminister zu einem sachlich nicht begründbaren Mehraufwand ohne erkennbaren Nutzen führen könnte.[984]

Dieser Ansicht lässt sich wohl für unbegründete, anlasslose Vornahmen einer Einschau durch den Bundesminister folgen. Sofern ein stattgefundener Sicherheitsvorfall oder sonstige Verdachtsmomente jedoch auf fehlende Sicherheitsvorkehrungen schließen lassen, wäre mE eine selbstständige Einschau durch den BMI nichtsdestotrotz zulässig.

Im Rahmen der Befugnisse des Bundesministers zur Einschau ist jedenfalls die Verhältnismäßigkeit zu beachten. Dies bedeutet, dass die Ausübung der Einschau nur in dem unbedingt erforderlichen Ausmaß und unter möglichster Schonung der Rechte der betroffenen Einrichtung und Dritter sowie des Betriebs erfolgen darf (§ 17 Abs. 4).

7.5.4.6. Der Betrieb von Netz- und Informationssystemen bei externen Dienstleistern im In- und (EU)-Ausland

Eine in der Vollziehung relevante Frage stellt sich ob der Tatsache, dass zu überprüfende Netz- und Informationssysteme österreichischer Betreiber wesentlicher Dienste oftmals bei sowohl im Inland, als auch in anderen EU-Mitgliedsstaaten und in Drittstaaten angesiedelten externen Dienstleistern eingerichtet sind bzw. von diesen betrieben werden.[985]

[983] Siehe dazu *Anderl et al.*, NISG::Kommentar, § 17, Rz 20.
[984] Ausführlicher dazu *Anderl et al.*, NISG::Kommentar, § 17, Rz 22.
[985] *Willcocks/Fitzgerald/Feeny*, Outsourcing IT: The Strategic Implications, Long Range Planning, 5/1995. *Burnett*, Outsourcing IT, the legal aspects (2009).

In den Erwägungsgründen der Richtlinie findet sich dazu die Regelung, dass Sicherheitsanforderungen jedenfalls für die einschlägigen Betreiber wesentlicher Dienste unabhängig davon gelten sollen, ob sie ihre Netz- und Informationssysteme intern (durch internes IT-Personal) verwalten oder diese Aufgabe ausgliedern. Damit hat der Betreiber selbst (beispielsweise vertraglich) zu gewährleisten, dass die Anforderungen durch den Dritten erfüllt werden.[986]

Befinden sich die Netz- und Informationssysteme bei einem externen Dienstleister im Inland**,** hat der Betreiber wesentlicher Dienste die Erfüllung der Anforderungen selbst durch Zertifizierungen oder durchgeführte Überprüfungen durch qualifizierte Stellen nachzuweisen, wenngleich die Zertifizierung bzw. Überprüfung beim externen IT-Dienstleister stattfinden wird müssen. Auch die mögliche Einschau des Bundesministers für Inneres (§ 17 Abs. 4) in die Netz- und Informationssysteme kann nur beim externen IT-Dienstleister stattfinden, insbesondere da diese Befugnis nicht auf die Betriebsörtlichkeit des Betreibers wesentlicher Dienste selbst einschränkt ist.[987]

Da ein externer IT-Dienstleister oftmals die Systeme verschiedenster Unternehmen betreibt ist hier jedenfalls zu beachten, dass im Rahmen der Einschau tatsächlich nur jene Systeme überprüft werden, die für den betroffenen Betreiber wesentlicher Dienste betrieben werden.

Anderes gilt, sofern die Netz- und Informationssysteme eines österreichischen Betreibers wesentlicher Dienste von einem IT-Dienstleister in einem anderen EU-Mitgliedsstaat[988] betrieben werden. Beim regelmäßigen Nachweis der Erfüllung der Sicherheitsanforderungen ist zu beachten, dass diese durch Überprüfungen von in Österreich anerkannten qualifizierten Stellen oder sonstige Zertifizierungen nachgewiesen werden müssen. Die (durch den Bundesminister für Inneres gemäß § 18 NISG anerkannte) qualifizierte Stelle mit Niederlassung im Inland wäre daher vom österreichischen Betreiber wesentlicher Dienste zu beauftragen und müsste die Überprüfung der Systeme beim externen IT-Dienstleister im Ausland durchführen. Eine andere Möglichkeit wäre mE die Anerkennung von Überprüfungsmechanismen in anderen EU-Mitgliedstaaten als Nachweis durch Zertifizierungen (§ 17 Abs. 3)[989], da der Begriff legal nicht näher definiert ist.

---

[986] ErwGr 52 NIS-RL.

[987] § 17 Abs. 4 NISG spricht von betroffenen Einrichtungen und Dritten.

[988] Betrifft die tatsächliche physische Lokation der Systeme im EU-Ausland, nicht beispielsweise nur die Hauptniederlassung des externen IT-Dienstleisters im Ausland.

[989] § 17 Abs. 3 NISG ermöglicht den Nachweis der Sicherheitsvorkehrungen durch Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen.

Jedenfalls wäre im Sinne des eigentlichen Zwecks der NIS-RL, nämlich das Funktionieren des Binnenmarktes, mE eine (unions-)rechtliche Möglichkeit[990] anzudenken, die diese Überprüfungsprozesse vereinfachen könnte.

Neben dem soeben beschriebenen regelmäßigen Nachweis soll der Bundesminister für Inneres auch selbst Einschau in die Netz- und Informationssysteme und diesbezügliche Unterlagen nehmen können (§ 17 Abs. 4). Befinden sich diese Systeme jedoch in einem andere EU-Mitgliedsstaat, kann wohl nur auf eine Behördenkooperation zurückgegriffen werden, die sich entweder in einem völkerrechtlichen Abkommen oder in einem Gemeinschaftsrechtsakt widerspiegeln müsste.[991]

Auf das üblicherweise für den Bundesminister für Inneres in seinem Vollzugsbereich anwendbare Polizeikooperationsgesetz[992] kann aufgrund des zu engen Anwendungsbereiches[993] nicht zurückgegriffen werden, wodurch auf völkerrechtliche Abkommen mit den jeweils in Frage kommenden Staaten abgestellt werden muss. Beispielsweise kommt dafür der Vertrag zwischen der Republik Österreich und der Bundesrepublik Deutschland über Amts- und Rechtshilfe in Verwaltungssachen[994] in der Kooperation zwischen Österreich und Deutschland in Betracht, erscheint in seinem Anwendungsbereich jedoch ebenfalls zu eng, da lediglich Amts- und Rechtshilfe durch Ermittlungen einschließlich Beweisaufnahmen, die Anhörung Beteiligter und Vernehmung Beschuldigter/Betroffener, die Erteilung von Auskünften einschließlich solcher aus dem Strafregister oder die Übersendung von Schriftstücken (Artikel 5 Abs. 1) in Frage kommen.

Die Verweigerung der Einschau in seine Netz- und Informationssysteme zieht eine Verwaltungsstrafe – sowohl für den Betreiber wesentlicher Dienste als auch, sofern sich die Netz- und Informationssysteme dort befinden, für den externen IT-Dienstleister - nach sich.[995]

7.5.4.7. Empfehlungen durch den Bundesminister für Inneres

Zur Herstellung der Sicherheitsanforderungen ist der Bundesminister für Inneres ermächtigt, Empfehlungen auszusprechen (§ 17 Abs. 5 NISG). Dabei stellt sich die Frage, in welchen Fällen diese Empfehlungen ausgesprochen werden können. Einerseits können diese Empfehlungen wohl

[990] Zu denken wäre beispielsweise an einen EU-Durchführungsrechtsakt, der die Einschau durch die jeweils zuständige Behörde im anderen Mitgliedsstaat regelt.
[991] Siehe auch *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 425. Dazu auch *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, S. 509ff.
[992] Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz – PolKG), BGBl. I Nr. 104/1997 idF BGBl. I Nr. 32/2018.
[993] Die internationale polizeiliche Kooperation erfolgt gemäß § 1 Abs. 1 PolKG für Zwecke der Sicherheitspolizei, der Kriminalpolizei, des Paßwesens, der Fremdenpolizei und der Grenzkontrolle.
[994] Vertrag zwischen der Republik Österreich und der Bundesrepublik Deutschland über Amts- und Rechtshilfe in Verwaltungssachen, BGBl. Nr. 526/1990.
[995] Mehr zu den Verwaltungsstrafbestimmungen siehe Kapitel 7.7.1.

ergehen, sofern die Einschau in die Netz- und Informationssysteme bzw. die diesbezüglichen Unterlagen Mängel ergeben haben und konkrete Empfehlungen den gesetzmäßigen Zustand herstellen sollen. Darüber hinaus sind diese Empfehlungen wohl auszusprechen, sofern durch die Überprüfung der qualifizierten Stellen Sicherheitsmängel aufgedeckt und dem Bundesminister für Inneres durch den Betreiber übermittelt wurden (§ 17 Abs. 3).

Ein Aussprechen von Empfehlungen in jenen Fällen, in denen weder die Übermittlung eines Nachweises (durch Zertifizierungen oder durchgeführte Überprüfungen durch qualifizierte Stellen) noch eine Einschau in die Netz- und Informationssysteme erfolgt ist, scheint nicht in Frage zu kommen.

Wird den Empfehlungen nicht innerhalb der gesetzten angemessenen Frist nachgekommen, kann die Befolgung mit Bescheid angeordnet werden.

7.5.5. Überprüfung der Sicherheitsvorkehrungen durch qualifizierte Stellen

7.5.5.1. Rechtsstellung der qualifizierten Stellen im Rahmen der Überprüfung

Art. 15 NIS-RL sieht vor, dass die zuständigen Behörden der Mitgliedstaaten von Betreibern wesentlicher Dienste Nachweise für die wirksame Umsetzung der Sicherheitsmaßnahmen verlangen können, wie etwa die Ergebnisse einer von einem qualifizierten Prüfer durchgeführten Sicherheitsüberprüfung.

In der nationalen Umsetzung haben Betreiber wesentlicher Dienste die Erfüllung der Sicherheitsanforderungen anhand von Zertifizierungen oder durchgeführten Überprüfungen durch so genannte qualifizierte Stellen nachzuweisen (§ 17 Abs. 3). Bei einer qualifizierten Stelle im Sinne des NIS-Gesetzes handelt es sich um eine Einrichtung mit Niederlassung in Österreich (§ 3 Z 11), deren Eignung durch Bescheid des Bundesministers für Inneres (§ 18) festgestellt wurde. Da somit eine wesentliche Aufgabe durch (private) Einrichtungen übernommen wird[996], stellt sich die Frage der Rechtsform dieser Aktivitäten bzw. das Vorliegen einer Beleihung.

In Zeiten der Privatisierung und Deregulierung ist die Besorgung der Aufgaben der öffentlichen Verwaltung durch Private verstärkt der Fall.[997] Insbesondere in Bereichen der Auditierungen und Zertifizierungen mit Fokus auf Informationstechnologien erscheint es durchaus zweckmäßig, die

[996] Anhand der Definition in § 3 Z 11 könnten auch Gebietskörperschaften als qualifizierte Stellen festgestellt werden.
[997] *Fuchs*, Verwaltungshilfe, in Fuchs/Merli et al. (Hrsg), Staatliche Aufgaben, private Akteure (2017), S. 95ff; *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.039.

Aufgaben an mit dieser Expertise und dem entsprechenden Personal ausgestatteten juristischen Personen auszulagern[998], wobei sich Auslagerungen immer auch am Effizienzgebot der Verfassung zu orientieren haben.[999]

Hauptgesichtspunkt einer Beleihung ist die Übertragung von hoheitlichen Aufgaben von der Staatsverwaltung auf private Rechtssubjekte.[1000] Wesentlich ist die Betrauung Privater mit der Zuständigkeit zur Setzung von Hoheitsakten in eigener Organkompetenz und Verantwortung, wobei die Funktion des Beliehenen über die unselbstständige Stellung eines Verwaltungshelfers hinausgeht und die Kompetenz zu selbstständiger Entscheidung über die Erlassung bzw. den Inhalt von Hoheitsakten (insb. Verordnungen, Bescheide, verfahrensfreie Verwaltungsakte, aber auch Beurkundungen und Leistungsbeurteilungen) besteht.[1001]

Auch wenn die qualifizierten Stellen – wie im Falle von Beleihungen üblich durch Bescheid oder Verordnung – durch Hoheitsakt[1002] zu solchen erklärt werden, liegt in diesem Fall mE keine Beleihung vor.

Zuerst ist die Frage nach einem Vorliegen der Hoheitsverwaltung im Bereich der Überprüfung der Erfüllung der Sicherheitsanforderungen gemäß § 17 NISG zu klären. Von Hoheitsverwaltung wird dort gesprochen, wenn der Staat imperium einsetzt, speziell mit Hilfe bestimmter Formen (z. B. Bescheidform) oder Symbole (z. B. Einschreiten uniformierter Organe) und wenn Befehl und Zwang als Formen einseitiger Herstellung rechtlicher Verbindlichkeit oder deren tatsächliche Umsetzung potenziell oder aktuell maßgeblich sind.[1003] Da der Bundesminister für Inneres Empfehlungen aussprechen, angemessene Fristen setzen und die Befolgung bescheidmäßig anordnen kann, liegt im genannten Bereich jedenfalls hoheitliches Handeln vor.

Die Rolle der qualifizierten Stellen in diesem Verfahren ist mit der Durchführung von Überprüfungen bei Betreibern wesentlicher Dienste und der Erstellung eines Berichts, inklusive aufgedeckter Sicherheitsmängel, beschränkt (§ 17 Abs. 3). Dieser Bericht entfaltet für sich selbst keine unmittelbare (hoheitliche) Rechtswirkung, sondern wird lediglich an den Betreiber selbst übergeben, der diesen (als Nachweis) dem Bundesminister für Inneres übermittelt.

---

[998] Zur Gewährleistung eines höheren Maßes an aufgabenspezifischer Effizienz und Flexibilität siehe auch *Funk*, Allgemeine Probleme, in Funk (Hrsg), Die Besorgung öffentlicher Aufgaben durch Privatrechtssubjekte (1981), S. 29.

[999] *Korinek*, Verfassungsrechtliche Grenzen von Ausgliederungen, Beleihung und Inpflichtnahme, in Duschanek (Hrsg), Beiträge zur Ausgliederungsdiskussion (2002), S. 37.

[1000] Siehe auch *Berka*, Verfassungsrecht, Rz 773.

[1001] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.040.

[1002] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 116.

[1003] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 49.003.

Erst die Behörde entscheidet[1004] nach Durchsicht dieses Berichtes, ob der Nachweis damit erbracht wurde, da nur ihm die Aufgabe zukommt, anhand dessen (im Rahmen der Hoheitsverwaltung) Empfehlungen auszusprechen, Fristen zu setzen und die Befolgung bescheidmäßig anzuordnen (§ 17 Abs. 3 letzter Satz). Keine Beleihung liegt darüber hinaus vor, wenn Private privatrechtsspezifische Befehls- und Zwangsakte setzen, wie dies bei in der Wirtschaft üblichen Audits, Zertifizierungen oder Wirtschaftsprüfungen üblicherweise der Fall ist.[1005]

Die Tätigkeit der qualifizierten Stelle könnte vielmehr als Verwaltungshilfe[1006] verstanden werden, bei der es sich um eine bloß unterstützende und verwaltungsentlastende Tätigkeit handelt und eine Kompetenz zur Setzung von Hoheitsakten kraft eigenen Entschlusses damit nicht verbunden ist.[1007] Sofern Private (auch per Bescheid) eben nur zur Setzung von unselbstständigen Teilakten im Bereich der Hoheitsverwaltung berufen werden und mangels jeglicher selbstständiger Entscheidungsbefugnis bzw. der jedenfalls bei der Behörde verbleibenden Letztentscheidungsbefugnis auch nicht als „Beliehene" anzusehen sind, wird von so genannten „Verwaltungshelfern"[1008], bei „einem höheren Grad an Selbstständigkeit bzw. eigenständigem Tätigwerden" von einem „verlängerten Arm der Behörde"[1009] gesprochen.[1010]

Der Terminus des Verwaltungshelfers an sich kommt insofern nicht in Betracht, da dieser nicht in ein eigenes, aufgabenbezogenes Rechtsverhältnis zu dem von der Aufgabenwahrnehmung betroffenen Dritten tritt[1011], was bei den qualifizierten Stellen jedoch jedenfalls der Fall sein wird.

Auch das Agieren als „verlängerter Arm der Behörde" ist fraglich, da auch dort der Private für eine Behörde handelt.[1012] Die im Rahmen des § 17 Abs. 3 vorgesehene Konstellation, dass die Betreiber die vorhandenen Sicherheitsvorkehrungen entweder durch den Nachweis von (nicht zwangsläufig durch qualifizierte Stelle ausgestellten) Zertifizierungen oder durchgeführten Überprüfungen durch

---

[1004] Zur Diskussion einer „Quasi-Beleihung" siehe auch *Funk/Marx*, Ziviltechnikerurkunden im Verwaltungsverfahren, ÖJZ, 14-15/2002.

[1005] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 117.

[1006] Zur Abgrenzung zur Indienstnahme und Inpflichtnahme siehe *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 121. Zu einer klaren Trennung und Unterscheidung zwischen den Begriffen der Indienstnahme, Inpflichtnahme sowie Verwaltungshilfe siehe auch *Fuchs* in Fuchs/Merli et al., Staatliche Aufgaben, private Akteure, S. 99. Siehe dagegen die Indienstnahme als Überbegriff für Verwaltungshilfe in *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.044.

[1007] *Adamovich et al.*, Österreichisches Staatsrecht, Rz 46.044.

[1008] Siehe *Fuchs* in Fuchs/Merli et al., Staatliche Aufgaben, private Akteure, Rz 108.

[1009] Der Begriff des verlängerten Armes spricht den Privaten einen höheren Grad an „Selbstständigkeit" zu, weil auch „eigenständiges Tätigwerden" vorgesehen ist und unterscheidet ihn vom Verwaltungshelfer, der zur Gänze unselbstständig handelt.

[1010] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 120.

[1011] *Fuchs* in Fuchs/Merli et al., Staatliche Aufgaben, private Akteure, S. 122.

[1012] Zur Unterscheidung der beiden Begriffe „Verwaltungshelfer" und „verlängerter Arm" siehe auch *Fuchs* in Fuchs/Merli et al., Staatliche Aufgaben, private Akteure, S. 109.

qualifizierte Stellen nachweisen können, spricht mE gegen die Annahme, die qualifizierten Stellen würden für die Behörde handeln (da eben auch andere Zertifizierungen in Betracht kommen). Darüber hinaus wird das Resultat der Überprüfung dem Betreiber und nicht der Behörde übermittelt.

Zusammenfassend lässt sich feststellen, dass die Eignung qualifizierter Stellen zwar durch Bescheid des Bundesministers für Inneres festgestellt[1013] wird, ihnen wesentliche Aufgaben in der Vollziehung des NIS-Gesetzes zukommen und außerdem entsprechende Feststellungen[1014] der Eignung, Überprüfungen/Kontrollen und Entziehungsmöglichkeiten der Eignung vorgesehen sind. Da ihre Rolle jedoch eine gänzlich selbstständige ist und die Behörde lediglich auf Ergebnisse ihrer Überprüfungen – wie auch auf Ergebnisse sonstiger Zertifizierungen – zurückgreift, kann mE von keiner (verwaltungsrechtlich relevanten) Beteiligung am hoheitlichen Handeln ausgegangen werden.

Eine ähnliche Vorgehensweise zum NIS-Gesetz hinsichtlich der Überprüfung von Betreibern sieht das Telekommunikationsgesetz[1015] vor. Gemäß § 16a Abs. 4 TKG kann die Regulierungsbehörde Betreiber öffentlicher Kommunikationsnetze und –dienste in bestimmten Fällen verpflichten, sich einer Sicherheitsüberprüfung durch die Regulierungsbehörde oder durch eine von ihr beauftragte qualifizierte unabhängige Stelle zu unterziehen, wobei darüber hinaus keine näheren Erfordernisse zu den Voraussetzungen dieser qualifizierten Stellen zu finden sind.[1016]

Statt der bescheidmäßigen Ernennung der qualifizierten Stellen durch den Bundesminister für Inneres wäre auch ein Rückgriff auf die Akkreditierung von Konformitätsbewertungsstellen (insbesondere Prüf-, oder Zertifizierungsstellen) im Sinne des Akkreditierungsgesetzes 2012[1017] möglich gewesen. Voraussetzung für ein solches Akkreditierungsverfahren ist das Vorliegen entsprechender Normen und/oder spezifischer Anforderungen und Regeln (§ 6 Abs. 3 AkkG), die in Form der durch Verordnung festgelegten Sicherheitsanforderungen im NIS-Gesetz vorgelegen wären. Darüber hinaus hätten die jeweils zuständigen Gebietskörperschaften dafür Sorge zu tragen, dass sie die spezifischen Voraussetzungen für die Akkreditierung der Akkreditierungsstelle vorlegen (§ 6 Abs. 3 AkkG). Die Erteilung der Akkreditierung erfolgt dabei mittels Bescheid (§ 8

[1013] Feststellungsbescheiden kann die Wirkung von Gestaltungsbescheiden zukommen (konstitutive Feststellung), siehe dazu *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 901., sowie *Leeb*, Bescheidwirkungen und ihre subjektiven Grenzen nach dem AVG, S. 38ff.
[1014] Zum Vorliegen eines bloß feststellenden Bescheids siehe auch *Anderl et al.*, NISG::Kommentar, § 18.
[1015] Näheres zum TKG und seiner Abgrenzung zum NIS-Gesetz siehe Kapitel 5.5.
[1016] *Pachinger*, § 16a, in Riesz /Schilchegger (Hrsg), Telekommunikationsgesetz (2016), Rz 11.
[1017] Bundesgesetz über die Akkreditierung von Konformitätsbewertungsstellen (Akkreditierungsgesetz 2012 – AkkG 2012), BGBl. I Nr. 28/2012 idF BGBl. I Nr. 40/2014.

AkkG). Grund dafür, dass nicht auf dieses bereits vorhandene System der Akkreditierung zurückgegriffen wurde, könnte evtl. die sehr lange Verfahrensdauer zur Schaffung einer für die Sicherheitsanforderungen nach dem NIS-Gesetz geeigneten Akkreditierungsstelle sowie daran anknüpfende Akkreditierung von Konformitätsbewertungsstellen gewesen sein, die eine fristgerechte Richtlinienumsetzung nicht ermöglicht hätte.[1018]

7.5.6. Meldepflicht für Betreiber wesentlicher Dienste

Die Häufigkeit und die Auswirkungen von IT-Sicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar.[1019] In Österreich kam es hinsichtlich strafbarer Handlungen im Bereich der Computerkriminalität im Jahr 2017 im Vergleich zum Vorjahr zu einem Anstieg von 28,2 %.[1020] Da insbesondere von Angriffen auf Netz- und Informationssystemen oftmals eine Vielzahl von (natürlichen und juristischen) Personen betroffen sind, ist es wichtig, bei Bekanntwerden bestimmter Arten von Angriffen so rasch als möglich potenzielle weitere Opfer zu informieren[1021], damit diese ihre Systeme entsprechend sichern bzw. darauf vorbereiten können.

Die NIS-RL verpflichtet die Mitgliedstaaten sicherzustellen, dass Betreiber wesentlicher Dienste der zuständigen Behörde oder dem CSIRT Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten Dienste haben, unverzüglich melden (Art. 14 Abs. 3 NIS-RL).

In der nationalen Umsetzung haben Betreiber wesentlicher Dienste einen Sicherheitsvorfall, der einen von ihnen bereitgestellten wesentlichen Dienst betrifft, unverzüglich an das für sie zuständige Computer-Notfallteam zu melden (§ 19 Abs. 1). Dabei gilt als Sicherheitsvorfall eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat (§ 3 Z 6).

7.5.6.1. Störung von Netz- und Informationssystemen

Wesentlich ist in diesem Zusammenhang einerseits die Beschränkung der Meldepflicht auf eine tatsächliche Einschränkung oder einen tatsächlichen Ausfall der Netz- und Informationssysteme,

[1018] *Anderl et al.*, NISG::Kommentar, § 18, Rz 3.
[1019] ErwGr 2 NIS-RL.
[1020] Bundeskriminalamt, Lagebericht Cyber Crime 2017.
[1021] Zur Notwendigkeit der Vorgabe von Kommunikationspflichten siehe auch *Weyand* in Gusy/Kugelmann et al., Rechtshandbuch Zivile Sicherheit, Rz 3.

wo in anderen Mitgliedstaaten[1022], beispielsweise in Deutschland[1023], darüber hinausgehend auch jene Störungen als meldepflichtig gelten, die zu Beeinträchtigungen führen hätten können.[1024]

Eine Definition der Störung ist in den Erläuternden Bemerkungen zum NIS-Gesetz nicht zu finden. Nach den Erläuternden Bemerkungen zum IT-Sicherheitsgesetz in Deutschland liegt eine Störung dann vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken.[1025]

Anzumerken ist, dass bei der Störung selbst auf alle vier Merkmale der Netz- und Informationssystemsicherheit (Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit)[1026] abgestellt wird, bei der Auswirkung selbst jedoch lediglich auf die Verfügbarkeit (Einschränkung der Verfügbarkeit oder Ausfall des betriebenen Dienstes).

Auch die NIS-RL selbst gibt vor, dass nur Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit haben, meldepflichtig sein sollen (Art. 14 Abs. 3). Dies bedeutet in weiterer Folge, dass Vorfälle mit Folgen für die Integrität, Authentizität oder Vertraulichkeit, die die Verfügbarkeit des Dienstes nicht betreffen, nach den Bestimmungen des NIS-Gesetzes nicht meldepflichtig sind. Als Beispiel dafür ist der Diebstahl oder die Manipulation von Daten zu nennen, die einerseits die Verfügbarkeit, andererseits die Integrität einschränken würden.[1027]

Nichtsdestotrotz ist das Abstellen in der Definition der Störung beim Sicherheitsvorfall auf diese vier Merkmale insofern korrekt, als auch eine Störung der Datenintegrität (ua Richtigkeit der Daten) für den betroffenen Dienst, beispielsweise einen Gesundheitsdienst, so wesentlich ist, dass der Betreiber die Verfügbarkeit einschränken muss, bis die Integrität wieder gewährleistet ist.[1028]

Bei einer solchen Störung muss es sich jedoch nicht zwangsläufig um Angriffe, sondern kann es sich auch um Naturereignisse, Stromausfälle oder Fehlverhalten eigener Mitarbeiter handeln.[1029] Somit kann es sich bei einem in der Praxis sehr häufigen Szenario, nämlich dem versehentlichen

[1022] COM(2017) 476 final S. 11.
[1023] Betreiber kritischer Infrastruktur haben gemäß § 8b Abs. 4 BSI-Gesetz erhebliche Störungen […], die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder geführt haben […] zu melden.
[1024] So auch *Anderl et al.*, NISG::Kommentar, § 19, Rz 6.
[1025] BT-Drs. 18/4096, S. 29.
[1026] Auf die vier Merkmale der Netz- und Informationssystemsicherheit wird in Kapitel 7.1.2 näher eingegangen.
[1027] In diesem Fällen kann bei Betroffenheit von personenbezogenen Daten jedoch eine Meldepflicht nach der DSGVO vorliegen.
[1028] Als Beispiel ist die Möglichkeit einer Verfälschung von Patientendaten (Integrität) zu nennen. Bei einer dahingehenden Unsicherheit wird der Betreiber des wesentlichen Gesundheitsdienstes wohl die Dienstleistung einschränken, um sich nicht dem Risiko von Fehlbehandlungen auszusetzen.
[1029] EB RV NISG, S. 4.

Durchtrennen eines Erdkabels durch Bauarbeiten (z. B. durch einen Bagger), bei dadurch verursachten Ausfällen der Netz- und Informationssysteme ebenso um einen meldepflichtigen Sicherheitsvorfall handeln.

Auffällig bei der Definition des Sicherheitsvorfalles ist außerdem, dass auf die Einschränkung oder den Ausfall des betriebenen Dienstes (§ 3 Z 6) abgestellt wird und nicht – wie in Bezug auf die Sicherheitsvorkehrungen (§ 17 Abs. 1) – nur auf den *wesentlichen* Dienst (§ 3 Z 9). Dies liegt wohl daran, dass § 17 nur die Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste regelt, die Definition des Sicherheitsvorfalles in § 3 Z 6 darüber hinaus jedoch auch für Anbieter digitaler Dienste und Einrichtungen des Bundes gilt, für die keine „wesentlichen Dienste" definiert werden. In den Erläuternden Bemerkungen[1030] ist diesbezüglich auch klar festgelegt, dass es sich bei dem betriebenen Dienst um einen wesentlichen Dienst (§ 3 Z 9), einen digitalen Dienst (§ 3 Z 12) oder einen wichtigen Dienst einer Einrichtung des Bundes handeln kann.

Die Begriffe des Ausfalls und der Einschränkung der Verfügbarkeit werden in § 3 NISV näher definiert. Unter dem Ausfall ist demnach die Unverfügbarkeit für Nutzer (§ 3 Z 1), unter einer Einschränkung die signifikant geminderte Verfügbarkeit des Dienstes in qualitativer Dimension für Nutzer (§ 3 Z 2) zu verstehen. Eine Beschränkung lediglich auf die qualitative (und nicht auch quantitative) Dimension kann nur so erklärt werden, als letztere ohnedies durch die Zahl der betroffenen Nutzer abgedeckt ist, die einen Parameter zur Bewertung der Erheblichkeit darstellt.

Offen bleibt die Frage, was unter einer signifikant geminderten Verfügbarkeit zu verstehen ist. Wo eine Determinierung im quantitativen Bereich (Zahl betroffener Nutzer) für den Verordnungsgeber möglich ist, erscheint dies im qualitativen Spektrum durchaus schwierig. Zu überlegen wäre in diesem Zusammenhang ein Verstoß gegen das Determinierungsgebot gem. Art. 18 Abs. 1 B-VG, auf welches im Rahmen dieser Arbeit bereits mehrfach eingegangen wurde (umfangreich dazu siehe Kapitel 7.3.2 [Das Determinierungsgebot im Zusammenhang mit dem Betrieb von IKT-Lösungen]).

Da sich an eine falsche Auslegung des Betreibers und eine daran anknüpfende Nichtmeldung des Sicherheitsvorfalls konkrete verwaltungsstrafrechtliche Sanktionen knüpfen, erscheint der verfassungsrechtliche Determinierungsbedarf dieser Regelung mE doch verhältnismäßig hoch. Diesem Anspruch werden die diesbezüglichen Regelungen der NISV nicht gerecht, da sich kein Hinweis darauf findet, wann eine „signifikante" Minderung einer Verfügbarkeit vorliegt. Aus diesem Grund ist mE von einem Verstoß gegen Art. 18 Abs. 1 B-VG und damit einer Verfassungswidrigkeit der Regelungen zu den Sicherheitsvorfällen in der NISV auszugehen.

[1030] EB RV NISG, S. 4.

7.5.6.2. Erheblichkeit des Sicherheitsvorfalles

Das wohl wesentlichste Merkmal der Definition des Sicherheitsvorfalles (§ 3 Z 6) sind die erheblichen Auswirkungen, die als Folge der Störung[1031] auftreten. Bei der Erheblichkeit ist insbesondere auf die Zahl der betroffenen Nutzer, die Dauer des Sicherheitsvorfalles, die geografischen Auswirkungen und die Auswirkung auf wirtschaftliche und gesellschaftliche Tätigkeiten abzustellen (§ 3 Z 6), wobei in Art. 14 Abs. 4 NIS-RL in Bezug auf die Meldepflicht von Betreibern wesentlicher Dienste lediglich die ersten drei dieser vier Parameter angeführt sind.

Der vierte Parameter stammt aus der Definition der Erheblichkeit von Vorfällen bei Anbietern digitaler Dienste (Art. 16 Abs. 4 lit. e NIS-RL). Da im NIS-Gesetz der Sicherheitsvorfall nicht spezifisch für Betreiber wesentlicher Dienste, Anbieter digitaler Dienst und Einrichtungen der öffentlichen Verwaltung, sondern für alle gemeinsam definiert wurde, finden sich in den angeführten Parametern zur Bestimmung der Erheblichkeit gesammelt auch alle Parameter der NIS-RL für alle Organisationen im Anwendungsbereich.

Da das Abstellen auf lediglich diese sehr allgemeinen Parameter alleine unzureichend erscheint, sieht die NIS-RL vor, dass im Rahmen der Kooperationsgruppe die zuständigen Behörden Leitlinien zu den Umständen ausarbeiten können, unter denen die Betreiber wesentlicher Dienste Sicherheitsvorfälle melden müssen, wobei dies auch für die Parameter zu den Auswirkungen (Art. 14 Abs. 4) gilt (Art. 14 Abs. 7). Darüber hinaus werden die Mitgliedstaaten dazu angehalten, diesen entwickelten Leitlinien genau zu folgen, um grenzüberschreitend tätigen Betreibern wesentlicher Dienste Rechtsunsicherheit, komplizierte Verfahren und erhebliche Verwaltungskosten zu ersparen.[1032]

Genannte Leitlinien wurden von der EU-Kooperationsgruppe erstmals im Februar 2018 als „Reference document on Incident Notification for Operators of Essential Services“[1033] sowie im Juli 2018 als „Guidelines on notification of Operators of Essential Services Incidents“[1034] veröffentlicht.

Im Folgenden soll untersucht werden, ob die Empfehlungen dieser Leitlinien im NIS-Gesetz bzw. der darauf basierenden Verordnung umgesetzt wurden und welche Konsequenzen dies für die nationale Rechtslage haben könnte.

[1031] Zum Begriff der Störung siehe auch *Leisterer/Schneider*, Der überarbeitete Entwurf für ein IT-Sicherheitsgesetz, Computer und Recht, 9/2014, S. 577.
[1032] COM(2017) 476 final .
[1033] Reference document on Incident Notification for Operators of Essential Services, 2018.
[1034] Guidelines on notification of Operators of Essential Services incidents, 2018.

In Bezug auf die Parameter zur Bestimmung der Erheblichkeit eines Sicherheitsvorfalles (§ 3 Z 6) weisen die Leitlinien darauf hin, dass aufgrund der Unterschiede in den betroffenen Sektoren neben der Zahl der Nutzer, der geografischen Auswirkung sowie der Dauer des Vorfalles auch andere bzw. weitere Parameter herangezogen werden können und die Mitgliedstaaten die Parameter daher diesen Umständen entsprechend festlegen sollen.[1035]

Für die Festlegung der Kriterien existieren im Grunde drei Zugänge.[1036] Die Mitgliedstaaten können einen allgemeinen Schwellenwert für alle Sektoren (bspw. die Betroffenheit von 100.000 Nutzern) festlegen, unterschiedliche Schwellwerte für die verschiedenen Sektoren oder aber überhaupt keinen Schwellwert festlegen, sondern eine Meldepflicht für alle Vorfälle vorsehen. Österreich hat sich in diesem Zusammenhang für die zweite Variante entschieden.

Die Kriterien zur Beurteilung der Erheblichkeit eines Sicherheitsvorfalles werden in der NISV sektorenspezifisch (§ 2 NISG) näher konkretisiert, wobei auf die Zahl der vom Sicherheitsvorfall betroffenen Nutzer (§ 3 Z 3 NISV), auf die Dauer des Sicherheitsvorfalles (§ 3 Z 4 NISV), auf die geografische Ausbreitung (§ 3 Z 5 NISV) sowie auf die Auswirkung auf wirtschaftliche und gesellschaftliche Tätigkeiten (§ 3 Z 6 NISV) Bezug genommen wird.

Die Parameter zur Beurteilung der Erheblichkeit eines Sicherheitsvorfalles werden folglich je nach Sektor unterschiedlich verwendet. Wesentlichster Parameter scheint hier das Produkt der Zahl der Nutzer mit der Dauer des Sicherheitsvorfalles (Nutzerstunden, § 3 Z 7 NISV) zu sein, da die Erheblichkeit eines Vorfalles mit der Zahl der betroffenen Nutzer als auch mit der Dauer des Vorfalles steigt. Weniger betroffene Nutzer über eine lange Dauer werden dadurch gleich gewichtet wie eine hohe Zahl betroffener Nutzer über eine kürzere Dauer.[1037] Eine ähnliche Vorgehensweise wurde auch von der RTR für die Meldepflicht gem. § 16a TKG gewählt.[1038]

Ebenso fällt auf, dass in den verschiedenen Sektoren die Dauer des Ausfalls/der Einschränkung unterschiedlich in Bezug auf die Erheblichkeit des Sicherheitsvorfalles gewertet wird.

Beispielsweise ist in der Stromerzeugung ein Vorfall jederzeit bzw. sofort zu melden, im Bereich Stromübertragung nach Ablauf von drei Stunden oder im Teilsektor Erdöl erst nach 24 Stunden. Die unterschiedliche Bewertung ist mE auf die differenzierte Kritikalität der einzelnen Dienste

[1035] COM(2017) 476 final sowie Reference document on Incident Notification for Operators of Essential Services, S. 8.
[1036] Reference document on Incident Notification for Operators of Essential Services, 2018, S. 15. Ausführungen dazu auch in *Anderl et al.*, NISG::Kommentar, § 19, Rz 8.
[1037] Die Nutzung des Parameters der Nutzerstunden unterstützt einen praktikableren und realistischeren Ansatz, siehe dazu Reference document on Incident Notification for Operators of Essential Services, 2018, S. 19.
[1038] Siehe dazu https://www.rtr.at/de/tk/Netzsicherheit, abgerufen am 19.02.2019.

zurückzuführen.[1039] Wirkt sich der Ausfall der Stromerzeugung und –übertragung unmittelbar auf die Bevölkerung aus, so ist der Ausfall von Anlagen zur Erdölförderung wohl erst sehr viel später spürbar.[1040]

Das Treffen dieser Unterscheidung ist mE differenziert zu sehen. Einerseits ist es insofern zu befürworten, als die NIS-RL bzw. das NIS-Gesetz auf die Versorgungssicherheit abzielt und einen Ausfall von wesentlichen Versorgungsleistungen für die Bevölkerung verhindern möchte. Die Guideline zur Meldepflicht der Kooperationsgruppe spricht davon, dass die Definition der Erheblichkeit zwischen den Mitgliedstaaten unterschiedlich sein kann und abhängig vom Sektor, dem wesentlichen Dienst, nationalen Umständen etc. ist.[1041] Eine Differenzierung nach der Kritikalität des jeweiligen Dienstes für die Bevölkerung ist insofern nachvollziehbar.

Auf der anderen Seite verfolgt die Meldepflicht – im Gegensatz zum Treffen von Sicherheitsvorkehrungen (§ 17) – nicht den Zweck, den Ausfall des jeweiligen Dienstes zu verhindern, sondern Bedrohungen rasch zu erkennen und andere wesentliche Dienste gegebenenfalls rechtzeitig davor warnen zu können. Muss ein Betreiber den Vorfall jedoch erst nach einer Dauer von 24 Stunden melden, vergeht wertvolle Zeit, um andere potenziell betroffene Unternehmen (mit einer höheren Kritikalität) davon informieren zu können. Dementsprechend wäre es mE wirkungsvoller gewesen, eine Meldepflicht unabhängig von der Kritikalität des jeweils betroffenen Dienstes entstehen zu lassen.

Ein weiterer Parameter, auf den hier kurz eingegangen werden soll, ist die Zahl der betroffenen Nutzer. Dies ist die Zahl der von einem Sicherheitsvorfall betroffenen natürlichen und juristischen Personen, mit denen ein Vertrag über die Bereitstellung des Dienstes abgeschlossen wurde, oder die Zahl der betroffenen Nutzer, die den Dienst im Zeitpunkt des Sicherheitsvorfalles genutzt haben oder für die voraussichtliche Dauer des Sicherheitsvorfalls nutzen würden (§ 3 Z 3 NISV).

Die erste Kategorie (Nutzer, mit denen ein Vertrag abgeschlossen wurde) umfasst insbesondere jene wesentlichen Dienste, im Rahmen derer es üblicherweise zu vertraglichen Vereinbarungen über eine langfristige Verfügbarkeit bestimmter Dienste kommt oder ein Vertrag über eine konkrete Leistung vorliegt. Die beiden weiteren Kategorien (Nutzer, die den Dienst im Zeitpunkt des Vorfalles genutzt haben oder für die voraussichtliche Dauer des Sicherheitsvorfalles nutzen werden) sind für die Betreiber wohl schwieriger zu ermitteln, stellen jedoch nichtsdestotrotz ein wesentliches Kriterium für das Entstehen der Meldepflicht dar. Als Beispiel ist der wesentliche Dienst der Gesundheitsversorgung zu nennen, wo die Zahl der Patienten, die für die Dauer des

[1039] So auch *Anderl et al.*, NISG::Kommentar, § 19, Rz 11.
[1040] Siehe dazu auch ErwGr 27 NIS-RL.
[1041] Siehe Guidelines on notification of Operators of Essential Services incidents, 2018, S. 9.

Vorfalles eine stationäre oder ambulante Behandlung in der Krankenanstalt benötigen, noch nicht bekannt ist. In diesem Zusammenhang müssen Betreiber wohl auf statistische Werte bzw. Prognosen zurückgreifen, die aufgrund der Notwendigkeit einer ökonomischen Unternehmens-/Betriebsführung ohnedies vorliegen sollten.[1042]

7.5.6.3. Zeitpunkt der Meldung

Ziel des gesamten Melderegimes ist neben der Erstellung eines umfassenden Lagebildes durch die Behörden[1043] insbesondere die möglichst rasche Kenntnis von Sicherheitsvorfällen, um andere potenziell betroffene Betreiber rechtzeitig vor Bedrohungen oder Schwachstellen in IT-Systemen warnen zu können. Dementsprechend sieht die NIS-RL eine unverzügliche Meldung von Sicherheitsvorfällen vor (Art. 14 Abs. 3 NIS-RL). Gleichzeitig besteht jedoch das behördliche Interesse an einer möglichst breiten Information über die Art des Vorfalles, betroffene Systeme, den Auslöser und vieles mehr. Diese Informationen liegen dem Betreiber jedoch zumeist nicht sofort vor, sondern erfordern intensive Recherchen im eigenen System.

Dementsprechend verwenden die meisten Mitgliedstaaten ein zwei- oder drei Phasen Reporting.[1044] Im NIS-Gesetz nimmt der Gesetzgeber auf eine Erstmeldung, Nachmeldungen und eine Abschlussmeldung Bezug (§ 19 Abs. 3 NISG). Die Erstmeldung (Phase 1) muss unverzüglich nach Vorliegen eines Sicherheitsvorfalles an das zuständige Computer-Notfallteam ergehen (§ 19 Abs. 3 1. Satz).[1045] Danach haben regelmäßig Zwischenberichte bzw. Nachmeldungen (Phase 2) ohne unangemessene weitere Verzögerung zu erfolgen, sofern beim Unternehmen neue Informationen über den Sicherheitsvorfall vorliegen (§ 19 Abs. 3 2. Satz). Letztendlich ist ein umfassender Gesamtbericht bzw. Abschlussbericht (Phase 3) – ebenso ohne unangemessene Verzögerung – zu übermitteln, wobei daran zu denken ist, dass bis zum Vorliegen aller relevanten Informationen zum Sicherheitsvorfall auch Monate vergehen können.[1046] Durch die Regelung der verschiedenen Phasen wird die rechtliche Schwierigkeit umgangen, mit einer Meldung eine einerseits unverzügliche, andererseits aber auch vollständige Meldung zu fordern.

In Bezug auf die Erstmeldung muss festgestellt werden, dass eine Meldepflicht erst nach Ablauf der gem. NISV für den jeweiligen wesentlichen Dienst festgelegten Dauer entsteht. Dies kann zu Szenarien führen, dass die breite Öffentlichkeit (durch mediale Berichterstattung) bereits von Ausfällen wesentlicher Dienste informiert ist, eine Meldung über den Sicherheitsvorfall jedoch erst

[1042] Zu den gesamten Ausführungen zu betroffenen Nutzern siehe *Anderl et al.*, NISG::Kommentar, § 19, Rz 10.
[1043] Reference document on Incident Notification for Operators of Essential Services, 2018, S. 6.
[1044] Reference document on Incident Notification for Operators of Essential Services, 2018, S. 9.
[1045] Eine frühzeitige Meldung hat demnach Vorrang vor einer vollständigen Meldung.
[1046] Reference document on Incident Notification for Operators of Essential Services, 2018, S. 9.

nach 24 Stunden ergeht, da ein *Sicherheitsvorfall* ex lege (siehe dazu bspw. § 4 Abs 2 NISV) erst mit Überschreitung dieser Dauer vorliegt und gem. § 19 NISG Betreiber wesentlicher Dienste *Sicherheitsvorfälle* zu melden haben (§ 19 Abs. 1 NISG).

Aus genannten Gründen wäre das sofortige Entstehen einer Meldepflicht zu befürworten gewesen, wofür zwei Optionen in Frage kommen: Einerseits könnte jede Störung der Netz- und Informationssysteme, die zu einem Ausfall oder zu einer Einschränkung der Verfügbarkeit für eine bestimmte Zahl an Nutzern führt, unabhängig von der Dauer eine Meldepflicht begründen. Dem könnte jedoch entgegnet werden, dass damit eine ungebührliche und unverhältnismäßige Meldepflicht einhergehen würde, da bspw. jede kurzfristige Einschränkung im Schienenverkehr oder beim Online-Banking (hervorgerufen durch Software-Updates) zu melden wäre. Dafür würde sprechen, dass der Bundesminister für Inneres tatsächlich über jede Störung informiert werden würde und dadurch ein umfassendes Lagebild und eine rechtzeitige Information an weitere potenziell gefährdete Betreiber veranlassen könnte.

Die zweite Option wäre zwar die Beibehaltung der (Mindest-)Dauer, jedoch das Entstehen der Meldepflicht bereits schon zu dem Zeitpunkt, zu dem für den betroffenen Betreiber erkennbar ist, dass zumindest die Einschränkung der Verfügbarkeit voraussichtlich länger als die definierte Dauer anhalten wird. Dadurch käme es einerseits zu einem früheren Entstehen der Meldepflicht, auf der anderen Seite jedoch zu einer sehr unspezifischen Verpflichtung und daran anknüpfenden Verwaltungsübertretung bei Nichteinhalten der Bestimmung, die wohl dem Determinierungsgebot (Art. 18 B-VG) widersprechen würde.

Ein kurzer Vergleich soll hinsichtlich des Zeitpunkts der Meldung noch zu den Bestimmungen der DSGVO gezogen werden. Dort ist eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden an die zuständige Aufsichtsbehörde zu melden, nachdem dem Verantwortlichen die Verletzung bekannt wurde (Art. 33 DSGVO).

7.5.6.4. Inhalt und Art der Meldung

Die Meldung muss sämtliche relevante Angaben zum Sicherheitsvorfall und den technischen Rahmenbedingungen[1047] enthalten, insbesondere die vermutete oder tatsächliche Ursache, die betroffene Informationstechnik, die Art der betroffenen Einrichtung oder Anlage (§ 19 Abs. 3 NISG). Dabei muss es sich gerade um jene Informationen handeln, aufgrund derer eine Einschätzung der Bedrohung für andere Betreiber wesentlicher Dienste aufgrund erkannter Angriffsmuster oder Schwachstellen ermöglicht wird. In diesem Zusammenhang ist an die Pflicht zur Unterrichtung der

[1047] Zum wenig präzisen Begriff der technischen Rahmenbedingungen siehe auch *Leisterer/Schneider*, Computer und Recht, 2014, S. 575.

zentralen Anlaufstellen anderer Mitgliedstaaten zu denken, sofern ein Sicherheitsvorfall Betreiber wesentlicher Dienste anderer Mitgliedstaaten betrifft (§ 19 Abs. 5).

§ 19 Abs. 3 geht auch darauf ein, dass die (unverzüglich zu erstattende) Erstmeldung alle Angaben enthalten muss, die zu diesem Zeitpunkt bekannt sind. Dabei ist bspw. an die Ursache des Ausfalls oder die Einschränkung des Dienstes zu denken, die mitunter erst nach umfangreichen Untersuchungen („Root Cause Analysis")[1048] im System bekannt sein wird. Nichtsdestotrotz können auch zu diesem Zeitpunkt bereits Vermutung vorliegen, bspw. sofern am Vortag ein umfangreiches Software-Update installiert wurde.

Der Meinung in *Anderl/Heußler/Mayer/Müller*[1049] folgend sollte seitens des für die Kontrolle der Einhaltung der Meldepflicht zuständigen Bundesministers für Inneres ein standardisiertes elektronisches Formular zur Verfügung gestellt werden. Dadurch ist die einheitliche Qualität, die rasche Bearbeitbarkeit durch den Betreiber, eine unverzügliche Reaktionsfähigkeit sowie eine effiziente Möglichkeit einer nachfolgenden Zusammenführung/Analyse verschiedenster Meldungen gewährleistet. Die Guideline der Kooperationsgruppe[1050] empfiehlt verschiedene Methoden der Meldung, nämlich einen einfachen Telefonanruf (mit dem Nachteil, dass dies in Krisen unübersichtlich werden könnte), (verschlüsseltes) Email oder Online-Formulare.

Meiner Einschätzung nach sollte das elektronische Formular bestenfalls anhand eines Web-Services eingerichtet werden, um durch die Nutzung eine rasche Weiterbearbeitung sowie Auswertung der relevanten Angaben zu erzielen.

7.5.6.5. Inanspruchnahme eines Anbieters digitaler Dienste in Bezug auf die Meldepflicht

§ 19 Abs. 4 NISG regelt die Meldepflicht, sofern von einem Sicherheitsvorfall sowohl ein Anbieter digitaler Dienste als auch ein Betreiber wesentlicher Dienste betroffen sind. Der Absatz regelt den Fall, dass ein Betreiber wesentlicher Dienste einen Anbieter digitaler Dienste in Anspruch nimmt, bei dem es zu einem Sicherheitsvorfall kommt und aufgrund dessen erhebliche Auswirkungen auf die Verfügbarkeit des Betreibers wesentlicher Dienste die Folge sind. In diesem Fall hat nämlich der Betreiber wesentlicher Dienste den Vorfall zu melden.

Die in *Anderl/Heußler/Mayer/Müller*[1051] vertretene Ansicht, dass die Meldepflicht des Anbieters digitaler Dienste davon unberührt bleibt, ist zumindest zu diskutieren. Die Kooperationsgruppe

[1048] *Anderl et al.*, NISG::Kommentar, § 19, Rz 19.
[1049] *Anderl et al.*, NISG::Kommentar, § 19, Rz 21.
[1050] Guidelines on notification of Operators of Essential Services incidents, 2018, S. 13.
[1051] *Anderl et al.*, NISG::Kommentar, § 19, Rz 25.

geht in ihrem *Reference Document* nämlich vom Gegenteil aus („Consequently, it is the responsibility of the OES[1052], and not of the DSP[1053], to notify the incident to the competent authority").[1054] Dem ist jedoch zu entgegnen, dass in der Bestimmung zur Meldepflicht für Anbieter digitaler Dienste (§ 21 Abs. 2) keine Ausnahmeregelung dafür definiert ist und somit auch vom Anbieter jeder Sicherheitsvorfall gem. den Vorgaben des § 21 Abs. 2 zu melden ist.

Interessant erscheint hier die Formulierung, dass der Betreiber „jede erhebliche Auswirkung auf die Verfügbarkeit des wesentlichen Dienstes" zu melden hat (§ 19 Abs. 4 2. Halbsatz). Diese Definition geht weit über jene des Sicherheitsvorfalles (§ 3 Z 6) hinaus, wodurch eine neue Meldepflicht entstehen könnte. Dem ist jedoch zu entgegnen, dass der Gesetzgeber hier wohl bloß den Richtlinientext des Art. 16 Abs. 5 NIS-RL übernommen hat und keine Unterscheidung, sondern eine Klarstellung der Zuständigkeit zur Meldepflicht treffen wollte. Im Sinne einer teleologischen Interpretation wäre auch nicht zu erkennen, worum in diesen Fällen eine weitergehende Meldung von Vorfällen vorgesehen sein sollte, als bei sonstigen Ursachen des Ausfalls oder der Einschränkung von wesentlichen Diensten.

7.5.6.6. Meldung an das Computer-Notfallteam bzw. Weiterleitung an den Bundesminister für Inneres

Sicherheitsvorfälle sind von Betreibern wesentlicher Dienste an das zuständige Computer-Notfallteam zu melden, das die Meldung unverzüglich an den Bundesminister für Inneres weiterleitet (§ 19 Abs. 1 NISG). Zuständig ist demnach das sektorenspezifische Computer-Notfallteam, falls ein solches eingerichtet ist und der betroffene Betreiber dieses unterstützt (§ 19 Abs. 2). Sektorenspezifische Computer-Notfallteams können von Betreibern wesentlicher Dienste für ihren Sektor (§ 2) eingerichtet werden und dieses unterstützen. Dies gilt jedoch nur für jene Betreiber dieses Sektors, die dieses Computer-Notfallteam auch unterstützen (§ 14 Abs. 3 1. Satz).[1055]

Dieser Zusatz ist meines Erachtens insofern von Relevanz, als die Voraussetzung für insbesondere freiwillige Meldungen ein Vertrauensverhältnis zwischen dem Betreiber und dem Computer-Notfallteam ist. Theoretisch könnte ein Betreiber des Sektors bei sich das sektorenspezifische Computer-Notfallteam einrichten und hätte so Zugang zu allen Risiken, Vorfällen und Sicherheitsvorfällen der anderen (möglicherweise Konkurrenz-) Unternehmen im Sektor. Um dies zu verhindern, sollen nur jene Betreiber an das jeweilige sektorenspezifische Computer-

[1052] Operators of Essential Services (OES) steht für Betreiber wesentlicher Dienste.
[1053] Digital Service Provider (DSP) steht für Anbieter digitaler Dienste.
[1054] Siehe Reference document on Incident Notification for Operators of Essential Services, 2018, S. 17.
[1055] Mehr zur Einrichtung sektorenspezifischer Computer-Notfallteams siehe Kapitel 7.4.1.2.

Notfallteam melden können, die dieses auch unterstützen – in allen anderen Fällen an das nationale (unabhängige) Computer-Notfallteam.

Der Meinung in *Anderl/Heußler/Mayer/Müller*[1056], wonach sich bereits aus der Meldung an das Computer-Notfallteam eindeutig ergeben muss, dass ein (meldepflichtiger) Sicherheitsvorfall und keine freiwillige Meldung eines Vorfalles vorliegt, kann man sich vollinhaltlich anschließen. Nur der Betreiber selbst kann bewerten, ob die Kriterien für das Vorliegen eines Sicherheitsvorfalles vorliegen. Sollte das Computer-Notfallteam bei einer freiwilligen Meldung das Vorliegen der Kriterien eines Sicherheitsvorfalles bemerken, wäre der jeweilige Betreiber darüber in Kenntnis zu setzen, eine formelle Meldung eines Sicherheitsvorfalles zu veranlassen.[1057]

Basiert der Sicherheitsvorfall auf einer gerichtlich strafbaren Handlung (bspw. § 126a StGB), trifft Behörden oder öffentliche Dienststellen eine Anzeigepflicht gem. § 78 StPO. Der Bundesminister für Inneres hat diesen im Rahmen seiner (noch weitergehenden) Ermittlungspflicht jedenfalls – grundsätzlich unabhängig von der Zustimmung des Betreibers[1058] (Ausnahme Ermächtigungs- bzw. Privatanklagedelikte) – als Kriminalpolizei gem. § 2 iVm § 99 StPO von Amts wegen in einem Ermittlungsverfahren aufzuklären.

Die sich aus solchen Meldungen möglicherweise ergebende Anzeigepflicht an die Staatsanwaltschaft für Computer-Notfallteams wird in Kapitel 7.5.9.2 (Prinzip der Anzeigepflicht für Computer-Notfallteams) eingehend beleuchtet.

7.5.6.7. Weiterleitung der Meldungen an Dritte

Daten, die dem Bundesminister für Inneres aus der Meldepflicht bekannt werden, können und (teilweise) müssen an verschiedene Stellen weitergeleitet werden.

Eine Kann-Bestimmung findet sich in § 10 Abs. 2 NISG (Datenübermittlung), wonach Informationen an militärische Organe und Behörden für Zwecke der militärischen Landesverteidigung gem. Art. 79 Abs. 1 B-VG, an Sicherheitsbehörden für Zwecke der Sicherheitspolizei und Strafrechtspflege, an Staatsanwaltschaften und ordentliche Gerichte für Zwecke der Strafrechtspflege sowie an sonstige inländische Behörden übermittelt werden können, soweit dies eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist (§ 10 Abs. 2).

Damit könnte bspw. die Datenschutzbehörde (DSB) gemeint sein[1059], sofern für den Bundesminister für Inneres im Zuge der Meldung eines Sicherheitsvorfalles erkennbar ist, dass auch eine Verletzung

[1056] *Anderl et al.*, NISG::Kommentar, § 19 Rz 13.
[1057] Eine (gesetzliche) Verpflichtung dazu für das Computer-Notfallteam existiert freilich nicht.
[1058] *Schmoller*, § 2, in Fuchs /Ratz (Hrsg), Wiener Kommentar zur Strafprozessordnung (2016), Rz 6.
[1059] *Anderl et al.*, NISG::Kommentar, § 19, Rz 15.

des Schutzes personenbezogener Daten (Art. 33 DSGVO) vorliegt. Es handelt sich dabei jedoch nicht um die primäre Zielrichtung des NIS-Gesetzes, die Verletzung des Schutzes personenbezogener Daten der Datenschutzbehörde anzuzeigen.

Eine dahingehende, eigeninitiative Prüfung durch den Bundesminister für Inneres hat mE dahingehend nicht zu erfolgen. Zu denken wäre bspw. an die Konstellation, in der ein Sicherheitsvorfall medial öffentlich wird und die Datenschutzbehörde beim Bundesminister für Inneres nachfragt, ob Informationen dazu vorliegen. Weitere inländische Stellen, die ein gesetzlich begründbares Interesse an entsprechenden Meldungen über Sicherheitsvorfälle haben könnten, sind die Aufsichtsbehörden der Betreiber.

Weiters kann der Bundesminister für Inneres Informationen über Sicherheitsvorfälle an Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie sonstige Einrichtungen übermitteln, wenn diese von einem Risiko, Vorfall oder Sicherheitsvorfall betroffen sind (§ 10 Abs. 3). Trotz des Umstandes, dass es sich hierbei um eine Kann-Bestimmung handelt, könnte sich eine Verpflichtung der Übermittlung von Informationen aus dem Sicherheitspolizeigesetz ergeben.

Hat die Sicherheitsbehörde[1060] Grund zur Annahme, es stehe ein gefährlicher Angriff gegen Leben, Gesundheit, Freiheit oder Vermögen bevor, so hat sie die betroffenen Menschen hiervon nach Möglichkeit in Kenntnis zu setzen (§ 22 Abs. 4 SPG). Sofern der Bundesminister für Inneres über Informationen zu Risiken, Vorfällen oder Sicherheitsvorfällen verfügt und erkennen kann, dass (ähnliche) gefährliche Angriffe[1061] auch bei anderen Einrichtungen bevorstehen, hat er diese Informationen im Rahmen des SPG weiterzuleiten.

Fraglich ist hier mE nur, wie weit diese Verpflichtung gehen kann. Daraus kann sich nämlich wohl kein Rechtsanspruch jedes Unternehmens und jedes Bürgers in Österreich ergeben, jederzeit von Risiken informiert zu werden, um dadurch evtl. gegen sie gerichtete Angriffe verhindern zu können. Dementsprechend muss dem Bundesminister für Inneres mE eine konkrete, mögliche Betroffenheit eines Dritten bekannt sein, um eine Pflicht zur Weitergabe von Informationen nach dem SPG entstehen zu lassen. Die gleichlautende Befugnis zur Übermittlung personenbezogener Daten, um diese Informationspflicht erfüllen zu können, findet sich in § 56 Abs. 1 Z 4 SPG, wonach die Sicherheitsbehörden Daten an einen Menschen übermitteln dürfen, dessen Rechtsgut durch einen gefährlichen Angriff bedroht ist, soweit dies für seine Kenntnis von Art und Umfang der Bedrohung erforderlich ist.

[1060] Der BMI ist gem. § 4 Abs. 1 oberste Sicherheitsbehörde.
[1061] Wie bspw. Datenbeschädigung (§ 126a StGB), Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) etc.

Eine Pflicht zur Weiterleitung von Informationen über Meldungen findet sich bei grenzüberschreitendem Bezug[1062] in § 19 Abs. 5 NISG. Demnach hat die zentrale Anlaufstelle die zentrale Anlaufstelle eines anderen Mitgliedstaates über einen Sicherheitsvorfall zu unterrichten, sofern der Vorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in jenem Mitgliedstaat hat (siehe dazu auch Art. 14 Abs. 5 NIS-RL). Die Übermittlungsbefugnis von personenbezogenen Daten an andere Mitgliedstaaten findet sich in § 10 Abs. 5 NISG.

National nicht umgesetzt erscheint die Bestimmung in Art. 10 Abs. 3 NIS-RL[1063], wonach die zentrale Anlaufstelle der Kooperationsgruppe jährlich einen zusammenfassenden Bericht über die eingegangenen Meldungen, einschließlich der Zahl der Meldungen und der Art der gemeldeten Sicherheitsvorfälle vorzulegen hat.[1064] Die Verpflichtung zur Vorlage dieses Berichtes findet sich weder in der Bestimmung zur zentralen Anlaufstelle (§ 6) noch zur Meldepflicht (§ 19). § 6 regelt lediglich die Aufgabe der zentralen Anlaufstelle als operative Verbindungsstelle zur Gewährleistung der Zusammenarbeit mit der Kooperationsgruppe. Eine generelle (jedoch keine oben genannte konkrete) Befugnis zur Datenübermittlung an Organe der Europäischen Union (als welches die Kooperationsgruppe fungiert) findet sich in § 10 Abs. 4 NISG.

7.5.6.8. Unterrichtung der Öffentlichkeit

Da von Vorfällen beim Betrieb von Netz- und Informationssystemen neben den im Anwendungsbereich der NIS-RL liegenden Betreibern wesentlicher Dienste und Anbietern digitaler Dienste insbesondere auch kleine und mittlere Unternehmen[1065] betroffen sein können, regelt die Richtlinie eine Unterrichtung der Öffentlichkeit über einzelne Sicherheitsvorfälle, sofern dies zur Sensibilisierung oder Bewältigung erforderlich ist (Art. 14 Abs. 6 NIS-RL).

Ein weiterer Zweck der Meldepflicht kann die Schaffung von mehr Transparenz gegenüber der Marktgegenseite (den Kunden des Betreibers) sein.[1066] Bereits in der Richtlinie wird auf die Interessensabwägung Bezug genommen, da vor einer Veröffentlichung jedenfalls der meldende Betreiber wesentlicher Dienste angehört werden muss (Art. 14 Abs. 6 1. Satz NIS-RL). Die

[1062] Zum berechtigten Kritikpunkt, dass dafür keine Kriterien vorliegen, siehe auch Reference document on Incident Notification for Operators of Essential Services, 2018, S. 16.
[1063] Guidelines on notification of Operators of Essential Services incidents, 2018, S. 10.
[1064] Siehe dazu auch Kapitel 7.2.3.
[1065] ErwGr 40 NIS-RL.
[1066] *Heinickel/Feiler*, Computer und Recht, 2014, S. 710.

diesbezüglichen Erwägungsgründe[1067] sprechen von einer sorgfältigen Abwägung des Interesses der Öffentlichkeit gegen einen möglichen wirtschaftlichen Schaden bzw. Imageschaden. [1068]

Die nationale Umsetzung in § 10 Abs. 1 NISG legt als Zweck der Veröffentlichung ebenso die Sensibilisierung der Öffentlichkeit zur Verhütung oder zur Bewältigung von Sicherheitsvorfällen oder ein sonstiges öffentliches Interesse fest und verpflichtet die veröffentlichende Behörde (Bundeskanzler oder Bundesminister für Inneres) zu einer Interessensabwägung bezüglich der Auswirkungen auf die datenschutzrechtlich Betroffenen.

Zu hinterfragen ist die Abgrenzung der Zuständigkeit zur Veröffentlichung von Vorfällen. Wo die Pflicht zur Unterrichtung über einzelne Sicherheitsvorfälle dem Bundesminister für Inneres zukommt (§ 5 Abs. 1 Z 7 NISG), soll der Bundeskanzler die Öffentlichkeit über Sicherheitsvorfälle informieren, die mehrere der in § 2 genannte Sektoren betreffen (§ 4 Abs. 1 Z 5 NISG). Diese Unterscheidung kann sich wohl nur auf die eigentliche Koordinierungsaufgabe des Bundeskanzlers[1069] stützen, die bei Betroffenheit mehrerer Sektoren aus Sicht des Gesetzgebers eher zu begründen ist als bei Auswirkungen in nur einem Sektor.

Besser wäre aus meiner Sicht eine Differenzierung nach der Ursache des Vorfalles gewesen. Wo dem Bundeskanzler aufgrund seiner strategischen Ausrichtung die grundsätzliche Veröffentlichung von Vorfällen zukommen hätte können, hätte diese Zuständigkeit dann auf den Bundesminister für Inneres übergehen können, sofern es sich bei der Ursache des Vorfalles um einen (gerichtlich strafbaren) Angriff auf IT-Systeme handelt.[1070]

Interessant ist hier auch die getroffene Unterscheidung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste. Über Sicherheitsvorfälle bei ersteren informieren die Behörden selbst, von Anbietern digitaler Dienste kann der Bundesminister für Inneres verlangen, die Unterrichtung selbst vorzunehmen (§ 10 Abs. 1 letzter Satz).

Die Differenzierung stammt aus der NIS-RL selbst, die die Möglichkeit der selbstständigen Veröffentlichung den Anbietern digitaler Dienste einräumt (Art. 16 Abs. 7). Warum dies indes nur vom Bundesminister für Inneres (und nicht vom Bundeskanzler) verlangt werden kann, bleibt offen.

[1067] ErwGr 59 NIS-RL.

[1068] Zum allgemeinen Verhältnismäßigkeitsgrundsatz staatlicher Eingriffsakte siehe ua *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 640. Zur Liste zu beachtender Rechtsgebiete wie Wirtschaftsgeheimnisse, zivilrechtliche Schutzbestimmungen, wettbewerbsrechtliche Vorschriften sowie medienrechtliche Vorschriften siehe *Schweighofer/Heußler/Hötzendorfer*, Informations- und Meldepflichten in PPPs, in Skopik/Páhi et al. (Hrsg), Cyber Situational Awareness in Public-Private-Partnerships (2018), S. 129.

[1069] Aufgabe der Koordination der öffentlich-privaten Zusammenarbeit gem. § 4 Abs. 1 Z 3 NISG.

[1070] Und somit die Zuständigkeit des BMI als Sicherheitsbehörde gem. SPG oder Kriminalpolizei gem. StPO gegeben ist. Die grundsätzlich im gerichtlichen Strafrecht zuständige Staatsanwaltschaft hat im NISG keine Aufgaben oder Befugnisse.

Offen bleibt darüber hinaus, warum eine Veröffentlichung von Sicherheitsvorfällen bei Einrichtungen des Bundes nicht vorgesehen ist (Art. 10 Abs. 1).

Da durch die Veröffentlichung eines solchen Vorfalles schutzwürdige Geheimhaltungsinteressen des meldenden Betreibers oder Anbieters betroffen sein könnten, ist darüber hinaus die Frage des diesbezüglichen Rechtsschutzes zu stellen. *Anderl/Heußler/Mayer/Müller* gehen hier von einem zweistufigen Verfahren aus, bei dem das Verlangen an den Anbieter digitaler Dienste ein bloß schlicht-hoheitliches „Ersuchen" ist und der Bundesminister für Inneres im Fall der Nichtbefolgung die Veröffentlichung bescheidmäßig anordnet.[1071]

Dem ist insbesondere deshalb zu folgen, da Akte unmittelbarer Befehls- und Zwangsgewalt im Allgemeinen nur von Organen des öffentlichen Sicherheitsdienstes[1072], vereinzelt von Organen der öffentlichen Aufsicht sowie in Einzelfällen von so genannten zuständigen „Behörden"[1073] und Verwaltungshelfern getroffen werden dürfen.[1074]

Nicht eingegangen wird auf die Rechtsform der selbstständigen Veröffentlichung des Bundeskanzlers oder des Bundesministers für Inneres im Falle von Sicherheitsvorfällen bei Betreibern wesentlicher Dienste, wobei es sich eben – im Gegensatz zu Vorfällen bei Anbietern digitaler Dienste – um kein zweistufiges Verfahren handelt.

Berka sieht staatliche Informationsakte grundsätzlich unterhalb der Schwelle der „Normativität". Werden behördliche Warnmeldungen erlassen oder wird die Allgemeinheit über Gefahren informiert, stellt dies aus seiner Sicht keinen Akt unmittelbarer Befehls- und Zwangsgewalt dar.[1075] *Müller* hingegen sieht in der Veröffentlichung von Pressemitteilungen durch die Regulierungsbehörde zu „Verfehlungen" von Unternehmen einen solchen verfahrensfreien Verwaltungsakt und eine dementsprechende Rechtsschutzmöglichkeit gegeben.[1076]

Aufgrund der fehlenden Normativität solcher Mitteilungen stellen solche Informationen mE dennoch bloß schlicht-hoheitliches Handeln dar, für das – im Gegensatz zu den förmlichen Verwaltungsakten - kein verfassungsunmittelbarer Rechtsschutz vorgesehen ist.[1077] Dies ist insofern bedenklich, da ein einmal veröffentlichter Vorfall die Reputation des Unternehmens

[1071] *Anderl et al.*, NISG::Kommentar, § 10, Rz 5.
[1072] Zu Organen des öffentlichen Sicherheitsdienstes siehe § 5 SPG.
[1073] Nach *Raschauer* sind Akte unmittelbarer Befehls- und Zwangsgewalt von Bediensteten von Behörden eher die Ausnahme, siehe Rz 959.
[1074] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 1000.
[1075] *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 988.
[1076] Eine detaillierte Auseinandersetzung zur Einordnung derartiger Informationen als Akt unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt, Bescheid oder Verordnung siehe *Müller*, Pressearbeit als (regulierungs-)verwaltungsbehördliche Handlungsform, Zeitschrift für Verwaltung (ZfV), 4/2010, S. 21.
[1077] Zur Anwendbarkeit des AHG siehe *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 706.

irreversibel schädigt und ein Eingriff in die Grundrechte des Unternehmens vorliegen kann (mehr dazu siehe in Kapitel 7.5.2.5 [Recht auf Freiheit des Eigentums] und 7.5.2.7 [Schutz personenbezogener Daten]).

Da hier möglicherweise eine Rechtsschutzlücke vorhanden ist, sollen die dahingehenden Rechtsschutzmöglichkeiten für Betreiber näher untersucht werden.

Art. 130 Abs. 2 B-VG eröffnet grundsätzlich die Möglichkeit für Verwaltungsgerichte, über Beschwerden wegen Rechtswidrigkeit eines Verhaltens einer Verwaltungsbehörde in Vollziehung der Gesetze zu erkennen. Darunter wäre beispielsweise schlicht-hoheitliches Handeln zu subsumieren. Dies muss jedoch explizit gesetzlich geregelt werden – eine solche explizite Rechtsschutzmöglichkeit findet sich im NIS-Gesetz jedoch nicht.

Ein solches Beispiel findet sich im Sicherheitspolizeigesetz, das die Möglichkeit der Beschwerde gegen schlicht-hoheitliches Handeln im Rahmen der Besorgung der Sicherheitsverwaltung regelt (§ 88 Abs. 2 SPG). Kann der Beschwerdeführer argumentieren, dass die Veröffentlichung im Rahmen der Vorbeugung von gefährlichen Angriffen (§ 22 Abs. 2 iVm § 22 Abs. 4 SPG) erfolgt ist[1078], stünde ihm zumindest diese Beschwerdemöglichkeit offen.

Der VfGH entschied 2009 im Zusammenhang mit der Veröffentlichung von Warnmeldungen[1079] gem. § 4 Abs. 7 S 1 BWG[1080] durch die Finanzmarktaufsichtsbehörde (FMA), dass sowohl das Sachlichkeitsgebot des Gleichheitssatzes als auch das Rechtsstaatsprinzip verletzt seien, wenn eine solche, ein einzelnes Unternehmen betreffende Information veröffentlicht werden darf, ohne dass diesem Unternehmen von der Rechtsordnung ein adäquates Instrumentarium zur Verfügung gestellt würde, die Information auf ihre Berechtigung überprüfen, eventuell öffentlich korrigieren sowie allfällige Folgen einer rechtswidrigen Information beseitigen lassen zu können.[1081] § 4 Abs. 7 BWG wurde mittlerweile novelliert[1082] und sieht ein bescheidmäßiges Überprüfungsverfahren samt Widerrufsanspruch vor.

Die Veröffentlichung im NIS-Gesetz ist aus diesen Gründen mE mit einer Verfassungswidrigkeit belastet, solange nicht auch ähnlich wie im BWG ein bescheidmäßiges Überprüfungsverfahren angeschlossen wird.

[1078] Nähere Ausführungen dazu finden sich einige Absätze weiter oben.
[1079] Der Gerichtshof qualifizierte solche Investorenwarnungen weder als Bescheide noch als AuvBZ, sondern ordnete sie offensichtlich als Rechtsakte sui generis ein, für die kein Verwaltungsrechtsschutz zur Verfügung steht.
[1080] Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG), BGBl. Nr. 532/1993 idF BGBl. Nr. 17/2018.
[1081] VfSlg 18747/2009.
[1082] BGBl. I 2009/66.

Denkbar ist unabhängig davon als sekundärer Rechtsschutz ein schadenersatzrechtlicher Anspruch[1083] nach den Bestimmungen des Amtshaftungsgesetzes[1084]. Demnach haftet der Bund[1085] nach den Bestimmungen des bürgerlichen Rechts für den Schaden am Vermögen oder an der Person, den die als ihre Organe handelnden Personen in Vollziehung der Gesetze durch ein rechtswidriges Verhalten wem immer schuldhaft zugefügt haben (§ 1 AHG). Das Problem dieses Rechtsschutztypus liegt im gegenständlichen Fall darin, dass nach den Bestimmungen des AHG der Schaden lediglich in Geld zu ersetzen ist, dies dem Betreiber aufgrund des möglicherweise durch die Veröffentlichung entstandenen Reputationsschadens aber nicht wirklich hilft. Dies ist laut *Müller* aus Gründen der Gewaltentrennung gar nicht anders möglich, zumal ein Zivilgericht einer hoheitlich handelnden Verwaltungsbehörde keine Leistungen (im konkreten Fall den Widerruf) auftragen kann.[1086]

Die Betreiber können somit bei Rechtswidrigkeit keinen Widerruf durch die Behörde geltend machen (im Schadenersatzrecht des ABGB durch § 1330 ABGB selbstverständlich), da das AHG einen solchen nicht vorsieht.[1087] Auch im oben genannten Fall (BWG) erachtete der VfGH das Amtshaftungsrecht als kein ausreichendes Instrumentarium.

Abschließend ist festzuhalten, dass die Veröffentlichung von Sicherheitsvorfällen dem Verhältnismäßigkeitsgrundsatz folgend mE nur in Ausnahmefällen den Namen des betroffenen Betreibers enthalten muss, da die bezweckte Sensibilisierung wohl eher Angriffsmuster und Schwachstellen und weniger das betroffene Unternehmen darstellen wird müssen. Nichtsdestotrotz wird zu befürchten sein, dass auch bei Unterlassung der namentlichen Nennung Rückschlüsse auf das betroffene Unternehmen möglich sein werden.

Hinzuweisen ist in Bezug auf die Veröffentlichung auf eine ähnlich lautende Bestimmung der DSGVO, wonach der Verantwortliche die betroffene Person von einer Verletzung des Schutzes ihrer personenbezogenen Daten unverzüglich zu benachrichtigen hat (Art. 34 Abs. 1 DSGVO). Sollte der Verantwortliche dieser Verpflichtung noch nicht nachgekommen sein, kann die Aufsichtsbehörde von dem Verantwortlichen verlangen, dies nachzuholen (Art. 34 Abs. 4 DSGVO).

[1083] Siehe dazu auch OGH 26.11.1975, 1 Ob 171/75; OGH 21.02.1990, 1 Ob 47/89 ua.
[1084] Bundesgesetz über die Haftung der Gebietskörperschaften und der sonstigen Körperschaften und Anstalten des öffentlichen Rechts für in Vollziehung der Gesetze zugefügte Schäden (Amtshaftungsgesetz – AHG), StF BGBl. Nr. 20/1949 idF BGBl. I Nr. 122/2013.
[1085] dies gilt ebenso für die übrigen Gebietskörperschaften, sonstigen Körperschaften und Anstalten des öffentlichen Rechts.
[1086] *Müller*, Zeitschrift für Verwaltung (ZfV), 2010, S. 24.
[1087] Eingehend dazu *Kletecka*, Schutz gegen "hoheitliche Kreditgefährdung"?, ecolex, 1993, S. 441 ff

7.5.6.9. Sonstige Meldepflichten aufgrund anderer Rechtsgrundlagen

Eine ähnliche Regelung der Meldepflicht findet sich in der sogenannten „Data Breach Notification Duty“ nach Art. 33 DSGVO. Der Unterschied zur Meldepflicht des NIS-Gesetzes liegt in der Auswirkung des Vorfalles. Wo die Meldepflicht gem. DSGVO durch eine Verletzung des Schutzes personenbezogener Daten entsteht, kommt es im NIS-Regime nur bei Ausfall oder Einschränkung wesentlicher Dienste zu einer dementsprechenden Verpflichtung. Häufig können jedoch beide Tatbestände erfüllt sein und somit eine doppelte Meldepflicht – einerseits an die Datenschutzbehörde, andererseits an das Computer-Notfallteam – entstehen.

Nicht im Anwendungsbereich des NIS-Gesetzes sind Betreiber öffentlicher Kommunikationsdienste, für die eine spezielle Informationsverpflichtung bei Verletzung des Schutzes personenbezogener Daten besteht (§ 95a Abs. 1 TKG). Darüber hinaus haben diese Betreiber der Regulierungsbehörde Sicherheitsverletzungen oder einen Verlust der Integrität mitzuteilen, sofern dadurch beträchtliche Auswirkungen auf den Netzbetrieb oder die Dienstebereitstellung eingetreten sind (§ 16a Abs. 5 TKG). Die Regulierungsbehörde hat diese Mitteilung daraufhin unverzüglich an den Bundesminister für Inneres weiterzuleiten, der diese Information in das zu erstellende Lagebild aufnimmt (§ 16a Abs. 5a TKG).

Für den Finanzsektor bzw. die Zahlungsdienstleister regelt das Zahlungsdienstegesetz (ZaDiG)[1088] (Umsetzung der Zahlungsdiensterichtlinie[1089]) eine Meldeverpflichtung für schwerwiegende Betriebs- oder Sicherheitsvorfälle an die Finanzmarktaufsicht (FMA) (§ 86 Abs. 1 ZaDiG).

Ferner ist die Meldepflicht nach dem Produktsicherheitsgesetz (PSG)[1090] zu nennen, wonach der Inverkehrbringende unverzüglich eine der zuständigen Behörden zu informieren hat, wenn er aufgrund der vorliegenden Informationen weiß oder wissen muss, dass ein Produkt für die Verbraucher eine Gefahr darstellt (§ 7 Abs. 4 PSG).[1091]

[1088] Bundesgesetz über die Erbringung von Zahlungsdiensten 2018 (Zahlungsdienstegesetz 2018 – ZaDiG 2018), BGBl. I Nr. 17/2018.
[1089] Siehe dazu Kapitel 5.3.
[1090] Bundesgesetz zum Schutz vor gefährlichen Produkten (Produktsicherheitsgesetz 2004 – PSG 2004), BGBl. I Nr. 16/2005 idF BGBl. I Nr. 32/2018.
[1091] Siehe dazu *Schweighofer/Heußler/Hötzendorfer* in Skopik/Páhi et al., Cyber Situational Awareness in Public-Private-Partnerships, S. 143.

Eine Linie zwischen allen Meldepflichten zu ziehen ist theoretisch möglich, praktisch kann ein Vorfall aber immer unter verschiedene Kategorien und Zuständigkeit verschiedenster Behörden fallen. [1092]

7.5.7. Ausnahmen von der Verpflichtung für Betreiber wesentlicher Dienste

Durch die horizontale[1093] Geltung der NIS-RL hinsichtlich der Rechtsetzung zu Cybersicherheit sind davon auch Bereiche betroffen, deren Sicherheit von Netz- und Informationssystemen oder Meldepflicht zu sicherheitsrelevanten Vorfällen[1094] bereits durch andere EU-Rechtsakte geregelt sind.

Art. 1 Abs. 3 NIS-RL sieht dementsprechend vor, dass die in der Richtlinie vorgesehenen Sicherheitsanforderungen und Meldepflichten nicht für Unternehmen gelten, die den Anforderungen der Art. 13a und 13b der Richtlinie 2002/21/EG unterliegen. [1095] Gleiches gilt für Vertrauensdiensteanbieter, für die die Anforderungen des Art. 19 der Verordnung (EU) Nr. 910/2014 gelten.[1096]

Darüber hinaus regelt Art. 1 Abs. 7 NIS-RL in einer weiteren lex-spezialis-Bestimmung, dass jene einschlägigen sektorenspezifischen Rechtsakte anzuwenden sind[1097], die für Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste die Gewährleistung der Sicherheit ihrer Netz- und Informationssysteme oder die Meldung von Sicherheitsvorfällen vorsehen und diese Anforderungen in ihrer Wirkung den in der NIS-RL enthaltenen Pflichten mindestens gleichwertig sind.

Die Erwägungsgründe führen hier als Beispiel die Regulierung und Aufsicht in den Sektoren der Banken und Finanzmarktinfrastrukturen an, die auf Unionsebene in hohem Maße harmonisiert sind und ein hohes Maß an Anforderungen für ihre Systeme aufweisen.[1098] Zu dieser Erkenntnis kommt auch die Europäische Kommission in ihrer Mitteilung, die bestehende, gleichwertige Regelungen auf Unionsebene derzeit im Finanzsektor, insbesondere in den Sektoren Bankwesen und

[1092] Reference document on Incident Notification for Operators of Essential Services, 2018, S. 13.
[1093] Siehe *Anderl et al.*, NISG::Kommentar, § 20, Rz 1.
[1094] Hier wird bewusst nicht der Begriff der „Sicherheitsvorfall“ verwendet, da dieser in der NIS-RL bzw. im NISG legal definiert ist und andere Rechtsakte sicherheitsrelevante Vorfälle anders bezeichnen bzw. definieren (siehe bspw. § 86 Zahlungsdienstegesetz).
[1095] Mehr zur nationalen Umsetzung der Rahmen-Richtlinie siehe in Kapitel 5.5.
[1096] Siehe dazu Kapitel 5.6.
[1097] In diesen Fällen sollten ausschließlich die Bestimmungen der einschlägigen Unionsrechtsakte und ihre Anwendung in den Mitgliedstaaten berücksichtigt werden, siehe ErwGr 9 NIS-RL.
[1098] ErwGr 12 und 13 NIS-RL.

Finanzmarktinfrastrukturen gegeben sieht.[1099] Als Beispiele werden die Zweite Zahlungsdiensterichtlinie (Payment Services Directive 2)[1100], die Verordnung (EU) Nr. 648/2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister[1101] sowie die Richtlinie 2014/65/EU über Märkte für Finanzinstrumente[1102] angeführt.

Interessant ist die Tatsache, dass der nationale Gesetzgeber für genannte Betreiber lediglich eine Ausnahme der Sicherheitsvorkehrungen und der Meldepflicht vorsieht (§ 20 Abs. 1 NISG), nicht jedoch für die Ermittlung der Betreiber selbst (§ 16). Wenngleich die NIS-RL in ihren Erwägungsgründen festhält, dass für genannte Unternehmen das Verfahren zur Ermittlung der Betreiber nicht durchzuführen ist[1103], regelt das NIS-Gesetz eine solche Ausnahme nicht.

§ 16 sieht die Ermittlung der Betreiber wesentlicher Dienste für jeden der in § 2 genannten Sektoren vor, der mit dem Bankwesen (§ 2 Z 3) und den Finanzmarktinfrastrukturen (§ 2 Z 4) jene beiden Sektoren umfasst, für die sektorenspezifische Regelungen iSd § 20 vorliegen.

Anderl/Heußler/Mayer/Müller begründen dies mit dem Umstand, dass solche Einrichtungen somit auch sektorenspezifische Computer-Notfallteams einrichten (§ 14), in die OpKoord (§ 7) und den Koordinationsausschuss (§ 25) einbezogen werden sowie an einer IKT-Lösung zur Vorbeugung von Sicherheitsvorfällen (§ 13 Abs. 1) teilnehmen können.[1104] Dies ist auch insofern richtlinienkonform, da es sich bei den Bestimmungen zu Betreibern wesentlicher Dienste um eine Mindestharmonisierung handelt (Art. 3 NIS-RL).

Wichtig ist in diesem Zusammenhang die Regelung, dass Meldepflichten im Rahmen des NIS-Gesetzes erhalten bleiben, sofern andere, speziellere Normen nicht zumindest gleichwertig sind. Ein gutes Beispiel dafür sind die Meldepflichten nach Art. 33 DSGVO im Falle einer Verletzung des Schutzes personenbezogener Daten. Die damit zu meldenden Vorfälle sind nicht mit den

[1099] Anhang der Mitteilung der Kommission an das Europäische Parlament und den Rat - Bestmögliche Netz- und Informationssicherheit - hin zu einer wirksamen Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, COM(2017) 476 final, Annex 1, S. 40.
[1100] RL (EU) 2015/2366; PSD 2; mehr zur nationalen Umsetzung dieser Richtlinie siehe Kapitel 5.3.
[1101] RL (EU) 2012/648; Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister.
[1102] RL (EU) 2014/61; Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU.
[1103] ErwGr 9 NIS-RL.
[1104] *Anderl et al.*, NISG::Kommentar, § 20, Rz 7.

Sicherheitsvorfällen im NIS-Regime gleichzusetzen[1105], weshalb die DSGVO keine lex spezialis zur NIS-RL darstellt.[1106]

Die Ausnahmen von Verpflichtungen gem. § 20 Abs. 1 legt der Bundeskanzler im Einvernehmen mit dem Bundesminister für Inneres mit Verordnung fest (§ 4 Abs. 3).[1107]

7.5.8. Sicherheitsvorkehrungen und Meldepflicht für Einrichtungen des Bundes

Anhang II NIS-RL regelt die Sektoren, Teilsektoren und Bereiche, die in den Anwendungsbereich der Richtlinie fallen, worunter die Einrichtungen der öffentlichen Verwaltung nicht zu finden sind. Die Erwägungsgründe sprechen in diesem Zusammenhang von der Verantwortung der Mitgliedstaaten für die Gewährleistung der Sicherheit von Netz- und Informationssystemen der öffentlichen Verwaltung, die eben nicht in den Anwendungsbereich dieser Richtlinie fallen.[1108]

Der nationale Gesetzgeber greift diese Möglichkeit auf und inkludiert die so genannten Einrichtungen der öffentlichen Verwaltung (§ 3 Z 19) in den Anwendungsbereich des NIS-Gesetzes (§ 2). Dazu zählen unter anderem die Einrichtungen des Bundes, die in § 3 Z 18 legal definiert werden. Auf die Frage, warum die in § 3 Z 18 genannten Einrichtungen in den Anwendungsbereich aufgenommen wurden, wird in Kapitel 7.1.2 näher eingegangen.

Der wesentliche Unterschied zur Umsetzung der Sicherheitsvorkehrungen und Meldepflichten der Betreiber wesentlicher Dienste (und Anbieter digitaler Dienste) liegt darin, dass bei Nichtbefolgung keine verwaltungsstrafrechtliche Sanktionierung (§ 26 NISG) vorgesehen ist.[1109] Dies kann damit begründet werden, dass im nationalen Rechtsrahmen eine verwaltungsstrafrechtliche Verantwortlichkeit eines obersten Verwaltungsorgans[1110] für Handlungen im Rahmen des hoheitlichen Gesetzesvollzugs nicht in Betracht kommt[1111] und der Betrieb von Netz- und

[1105] Zur Abgrenzung der Meldepflichten siehe auch Kapitel 7.5.6.
[1106] EB RV NIS-RL, S. 21.
[1107] VO war zum Zeitpunkt der Erstellung gegenständlicher Arbeit noch nicht veröffentlicht.
[1108] Teilweise könnten öffentliche Verwaltungen als Betreiber wesentlicher Dienste identifiziert werden, sofern sie bspw. für die Trinkwasser- oder Energieversorgung zuständig sind. Siehe auch ErwGr 45 NIS-RL.
[1109] Die Gewährleistung der Einhaltung geeigneter Vorkehrungen ist nichtsdestotrotz eine gesetzliche Verpflichtung und kann bei (rechtswidrigen und schuldhaften) Versäumnissen und darauf basierenden Schäden zu entsprechenden Amtshaftungsansprüchen führen, siehe auch *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, Rz 3.
[1110] Gem. Art. 19 B-VG zählen die Bundesminister zu den obersten Organen der Vollziehung, siehe dazu auch *Barfuß*, Ressortzuständigkeit und Vollzugsklausel, Eine verfassungs- und verwaltungsrechtliche Untersuchung zur Zuständigkeit der Bundesminister, S. 28.
[1111] VwGH 21.10.1992, 92/10/0111 sowie VfSlg 19.988/2015.

Informationssystemen zur Gewährleistung wichtiger Dienste der Hoheitsverwaltung als Teil der Hoheitsverwaltung gesehen werden kann.[1112]

§ 22 NISG unterscheidet grundlegend zwischen Verpflichtungen für Einrichtungen des Bundes und der Länder. Einrichtungen des Bundes haben in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung wichtiger Dienste nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Hier verwendet der Gesetzgeber den Begriff der „wichtigen Dienste", wohingegen bei Betreibern wesentlicher Dienste auf deren „wesentliche Dienste" abgestellt wird (§ 17 Abs. 1 NISG).

Ein Blick auf die Legaldefinition der „wesentlichen Dienste" (§ 3 Z 9 NISG) zeigt, dass davon nur Dienste der in § 2 genannten Sektoren (Energie, Gesundheit etc.), nicht aber Einrichtungen der öffentlichen Verwaltung umfasst sind. Aus diesem Grund musste der Gesetzgeber wohl eine andere Begrifflichkeit verwenden. Offen bleibt trotzdem, um welche Dienste es sich dabei handelt. Die wesentlichen Dienste der Betreiber kann der Bundeskanzler in einer Verordnung regeln (§ 16 Abs. 1), für die wichtigen Dienste der Einrichtungen der öffentlichen Verwaltung besteht eine solche Möglichkeit nicht. Somit bleibt für diese Einrichtungen wohl nur die Möglichkeit, diese selbst zu definieren, wobei im Sinne einer systematischen Interpretation auch hier von jenen Diensten auszugehen sein wird, denen eine wesentliche Bedeutung in der Aufrechterhaltung wichtiger gesellschaftlicher Funktionen im Rahmen der öffentlichen Verwaltung zukommt.[1113]

Darüber hinaus haben Einrichtungen des Bundes einen Sicherheitsvorfall, der einen von ihnen bereitgestellten wichtigen Dienst betrifft, unverzüglich zu melden (§ 22 Abs. 2 NISG). Ähnlich wie bei den Sicherheitsvorkehrungen sind darüber hinaus, insbesondere hinsichtlich möglicher Meldeschwellenwerte, keine weiteren Regelungen getroffen. Einzig die Definition des Sicherheitsvorfalles (§ 3 Z 6) gibt Aufschluss darüber, welche Vorfälle davon umfasst sein könnten.

Zu melden sind demnach nur erhebliche Vorfälle, wobei hier insbesondere die Zahl der vom Vorfall betroffenen Nutzer, die Dauer des Vorfalles, die geografische Ausbreitung sowie die Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten zu berücksichtigen sind. Wo für Betreiber wesentlicher Dienste mit Verordnung (§ 4 Abs. 2 Z 1 NISG) nähere Kriterien für diese Parameter festgelegt werden, bleibt dies für Einrichtungen des Bundes offen. Nicht nur *Anderl/Heußler/Mayer/Müller* hätten sich hier eine Aufnahme der Schwellwerte in der NISV gewünscht.[1114]

[1112] *Anderl et al.*, NISG::Kommentar, § 22, Rz 3.
[1113] *Anderl et al.*, NISG::Kommentar, Rz 4.
[1114] *Anderl et al.*, NISG::Kommentar, Rz 6.

Obwohl Einrichtungen der öffentlichen Verwaltung nicht vom Anwendungsbereich der NIS-RL umfasst sind, sind deren Sicherheitsvorfälle nach den nationalen Bestimmungen im NIS-Gesetz im Wege der zentralen Anlaufstelle (SPoC) an die zentrale Anlaufstelle in anderen Mitgliedstaaten zu übermitteln, sofern diese davon betroffen sind (§ 22 Abs. 4 NISG). Diese Regelung erscheint jedenfalls sinnvoll, wenngleich die Weiterleitung an mögliche betroffene Stellen in diesen Mitgliedstaaten fragwürdig erscheint.

Da Einrichtungen der öffentlichen Verwaltung in anderen Mitgliedstaaten nicht vom Meldeprozess umfasst bzw. möglicherweise auch keine Kontaktdaten bekannt sind, ist mE fraglich, ob die bei der zentralen Anlaufstelle des anderen Mitgliedstaates eingehende Meldung zeitgerecht an die geeigneten Stellen dieses Mitgliedstaates weitergeleitet werden können.

Die bisherigen Ausführungen zu Sicherheitsvorkehrungen und Meldepflichten finden lediglich für Einrichtungen des Bundes Geltung. Ein Land kann durch Landesgesetz diese Pflichten auch in Hinblick auf die von seinen Einrichtungen erbrachten wichtigen Dienste für anwendbar erklären, wovon die Ämter der Landesregierungen und weitere Dienststellen der Länder und Gemeinden umfasst sind (§ 22 Abs. 5 NISG). Ähnlich findet sich eine Ausrollung auf Länder und Gemeinden auch im Österreichischen Programm zum Schutz kritischer Infrastruktur. Demnach sollen die Bundesländer eigene Programme zum Schutz ihrer regionalen kritischen Infrastrukturen entwickeln und auch die Städte und Gemeinden motivieren, lokale Programme zu schaffen.[1115]

7.5.9. Freiwillige Meldungen

Das Melderegime der NIS-RL verfolgt den allgemeinen Zweck, den Behörden die Möglichkeit eines Lagebildes über aktuelle Sicherheitsvorfälle und sonstige Risiken zu geben, um auf Basis dessen beispielsweise Empfehlungen aussprechen und so die Sicherheit insgesamt erhöhen zu können.[1116] Klar ist, dass dieses Lagebild umfassender und gesamtheitlicher erstellt werden kann, wenn eine höhere Zahl an Informationen über Vorfälle und Risiken vorliegt. Dies ist umso mehr der Fall, da die Schwellenwerte für die verpflichtenden Meldungen von Sicherheitsvorfällen relativ hoch angesetzt zu sein scheinen.[1117]

Art. 20 NIS-RL regelt dementsprechend die Möglichkeit von freiwilligen Meldungen, die über die verpflichtende Meldung von Sicherheitsvorfällen hinausgehen. Demnach können Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden und keine Anbieter digitaler Dienste sind, auf freiwilliger Basis Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die

[1115] *Bundeskanzleramt*, Österreichisches Programm zum Schutz kritischer Infrastruktur, 2014, S. 7.
[1116] Zu näheren Hintergründen der Meldepflicht im Rahmen des NISG siehe Kapitel 7.5.6.
[1117] Siehe Schwellenwerte der einzelnen Sektoren der NISV, wonach beispielsweise jeweils zehntausende Menschen vom Vorfall betroffen sein müssen, um eine Meldepflicht entstehen zu lassen.

Verfügbarkeit der von ihnen angebotenen Dienste haben (Abs. 1). Eine Bearbeitung dieser Sicherheitsvorfälle von Unternehmen, die eigentlich nicht im Anwendungsbereich der Richtlinie liegen, soll nur dann erfolgen, wenn dies keinen unverhältnismäßigen oder ungebührlichen Aufwand für die betreffenden Mitgliedstaaten darstellt. [1118]

Die nationale Umsetzung geht sogar noch weiter. Wo die Richtlinie eine freiwillige Meldung lediglich für jene Einrichtungen vorsieht, die weder Betreiber wesentlicher Dienste noch Anbieter digitaler Dienste sind, schafft das NIS-Gesetz die Möglichkeit freiwilliger Meldungen auch für die im Anwendungsbereich liegenden Unternehmen, sofern noch kein Sicherheitsvorfall vorliegt. § 23 NISG unterschiedet somit zwischen freiwilligen Meldungen von Risiken und Vorfällen, die von Betreiber wesentlicher Dienste oder Anbietern digitaler Dienste gemeldet werden (und noch keine meldepflichtigen Sicherheitsvorfälle darstellen) (Abs. 1) und freiwilligen Meldungen von Risiken, Vorfällen und Sicherheitsvorfällen durch Einrichtungen, die nicht als Betreiber wesentlicher Dienste ermittelt wurden und keine Anbieter digitaler Dienste oder Einrichtungen des Bundes sind (Abs. 2).

Bei den Begriffen Risiko, Vorfall und Sicherheitsvorfall handelt es sich nach den Legaldefinitionen (§ 3) um eine Abstufung[1119] von Ereignissen, die Netz- und Informationssysteme betreffen. Wo das „Risiko“ noch von allen Umständen oder Ereignissen, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben (§ 3 Z 8 NISG), ausgeht, spricht der „Vorfall“ bereits von allen Ereignissen, die tatsächlich nachteilige Auswirkungen auf die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen haben und kein Sicherheitsvorfall sind (§ 3 Z 7 NISG). Der Sicherheitsvorfall als schwerster Eingriff ist eine tatsächliche Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- und Informationssystemen, die zu einer Einschränkung der Verfügbarkeit oder zu einem Ausfall des betriebenen Dienstes mit erheblichen Auswirkungen geführt hat (§ 3 Z 6).

Tschohl geht auch bei der NIS-RL davon aus, dass Betreiber wesentlicher Dienste und Anbieter digitaler Dienste freiwillig Vorfälle melden können, auch wenn sie die Erheblichkeitsschwelle nicht überschreiten, da sich dies aus einem Größenschluss und dem Normzweck ergäbe.[1120] Unabhängig davon können die Mitgliedstaaten im Sinne einer Mindestharmonisierung der NIS-RL ein höheres

[1118] ErwGr 67 NIS-RL.

[1119] Siehe dazu auch *Anderl et al.*, NISG::Kommentar, § 3, Rz 22.

[1120] Demnach sind Vorfälle bei Betreibern wesentlicher Dienste und Anbietern digitaler Dienste, die noch keine erheblichen Auswirkungen auf die Verfügbarkeit dieser Dienste haben, für die gesamte Cybersicherheitslage mindestens so bedeutsam, wie Vorfälle, die keine wesentlichen Dienste bzw. digitalen Dienste betreffen, siehe dazu Tschohl et al., "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs," S. 7.

Sicherheitsniveau erlassen (Art. 3 NIS-RL), weshalb die nationale, über die Bestimmung im Richtlinientext hinausgehende Regelung unionsrechtlich unproblematisch ist.

Hinzuweisen ist dabei auch auf einen Erwägungsgrund der Durchführungsverordnung 2018/151/EU, wonach Anbieter digitaler Dienste angehalten werden, jeglichen Sicherheitsvorfall freiwillig zu melden, der ihnen zuvor unbekannte Merkmale wie neue Exploits, Angriffsvektoren oder Angreifer, Anfälligkeiten und Gefahren aufweist. [1121]

ME nicht so recht ersichtlich ist der konkrete Anreiz für Einrichtungen, die keine Betreiber wesentlicher Dienste, Anbieter digitaler Dienste oder Einrichtungen des Bundes sind, Risiken, Vorfälle oder Sicherheitsvorfälle zu melden.[1122] Grundsätzlich ist davon auszugehen, dass Unternehmen Vorfälle, die ihre eigenen Systeme betreffen, nicht melden bzw. (bei Vorliegen eines Angriffes) nicht zur Anzeige[1123] bringen, da oftmals Angst vor einem Reputationsverlust besteht.[1124] Maßgeblich für einen Informationsaustausch mit Stellen außerhalb des eigenen Unternehmens ist das Vertrauen, dass die bereitgestellten Informationen über Vorfälle nicht an Dritte weitergegeben werden. [1125]

Ein Anreiz zur Meldung von Vorfällen kann einerseits sein, dass die Einrichtungen der Ansicht sind, dass es im öffentlichen Interesse liegt, das Auftreten derartiger Sicherheitsvorfälle zu melden.[1126] Dieser Anreiz wird wohl dadurch verstärkt werden können, dass die meldenden Unternehmen selbst in weiterer Folge von Unterstützungsleistungen des Computer-Notfallteams oder von einem ganzheitlichen und vollständigen Lagebild der Behörden profitieren. Der Bundesminister für Inneres kann nämlich an Betreiber wesentlicher Dienste, Anbieter digitaler Dienste sowie alle anderen Einrichtungen relevante Informationen („Daten“) übermitteln, wenn diese von einem Risiko, Vorfall oder Sicherheitsvorfall betroffen sind (§ 10 Abs. 3 NISG).

[1121] Zur freiwilligen Meldung insgesamt siehe auch *Schweighofer/Heußler/Hötzendorfer* in Skopik/Páhi et al., Cyber Situational Awareness in Public-Private-Partnerships, S. 153.

[1122] *Anderl et al.*, NISG::Kommentar, § 23, Rz 2.

[1123] Angesichts der Möglichkeit, dass die Vertraulichkeit eines Geschäftsgeheimnisses im Verlauf von Gerichtsverfahren nicht gewährt bleibt, schrecken die rechtmäßigen Inhaber von Geschäftsgeheimnissen häufig davor zurück, zum Schutz ihrer Geschäftsgeheimnisse ein Gerichtsverfahren einzuleiten; siehe dazu ErwGr 27 RL (EU) 2016/943; Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.

[1124] *Huber/Pospisil* in Huber, Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation, S. 116.; zu negativer Publizität und Schäden für die Reputation des Unternehmens, wie bspw. Berichte über internes Versagen oder unzureichende IT-Absicherung siehe auch *Anderl et al.*, NISG::Kommentar, § 23, Rz 7.

[1125] *Klimburg*, Strategie und Sicherheit, 2012, S. 466.

[1126] ErwGr 67 NIS-RL.

Dies hat er jedoch unabhängig davon zu tun, ob Einrichtungen bereits freiwillig Vorfälle gemeldet haben. Jedenfalls profitieren mE jedoch alle Unternehmen und Einrichtungen von einer gut informierten Behörde, die aufgrund des Vorliegens umfassender Information über bisherige Risiken und Vorfälle ihre Abwehrmaßnahmen besser und gezielter steuern wird können, um dadurch die IT-Sicherheit in Österreich insgesamt und für alle Unternehmen und Einrichtungen zu erhöhen.

Ein wesentlicher Anreiz für die Durchführung freiwilliger Meldungen ist die Möglichkeit einer anonymen Meldung[1127] (§ 23 Abs. 4 NISG), sowie die Übermittlung der Meldung an ein (sektorenspezifisches und privates) Computer-Notfallteam anstatt einer direkten Meldung an die (Sicherheits-)Behörde (§ 23 Abs. 1 und 2).

7.5.9.1. Prinzip der Amtswegigkeit im Zusammenhang mit der Meldung von Vorfällen

Wenn Einrichtungen ein Risiko, einen Vorfall oder einen Sicherheitsvorfall an das Computer-Notfallteam melden, hat dieses die Meldungen – im Gegensatz zum meldepflichtigen Sicherheitsvorfall – „zusammengefasst“ an den Bundesminister für Inneres weiterzuleiten (§ 23 Abs. 1 NISG). Diese Weiterleitung hat auch nicht – wie beim meldepflichtigen Sicherheitsvorfall - unverzüglich zu erfolgen, sondern kann mit einer gewissen zeitlichen Verzögerung weitergeleitet werden.[1128]

Der Grund für diese Regelung in § 23 liegt offenbar in der Schaffung eines Anreizes[1129] für Meldungen, da dadurch das Auslösen der Ermittlungspflicht des Bundesministers für Inneres (§ 99 Abs. 1 StPO) verhindert werden soll.[1130] Die Sicherheitsbehörden sind bei Vorliegen eines Anfangsverdachtes verpflichtet, von sich aus und amtswegig Ermittlungen einzuleiten.[1131] Ein Anfangsverdacht liegt vor, wenn auf Grund bestimmter Anhaltspunkte angenommen werden kann, dass eine Straftat begangen wurde (§ 1 Abs. 3 StPO). Bei dieser Straftat kann es sich in Bezug auf Netz- und Informationssysteme beispielsweise um eine Datenbeschädigung (§ 126a StGB), eine

[1127] Die Anonymität ist für die Erstellung eines Lagebildes insofern kein Nachteil, da dies auch ohne Kenntnis von der Identität des betroffenen Betreibers möglich ist. Dazu und zur in Deutschland anfangs umstrittenen Möglichkeit der anonymen Meldung siehe *Leisterer/Schneider*, Computer und Recht, 2014, S. 576.

[1128] EB RV NIS-Gesetz, S. 22.

[1129] Amtswegige Ermittlungen der Kriminalpolizei widersprechen dem Interesse des Betroffenen an Diskretion, denn in einem Strafverfahren wird der jeweilige Sicherheitsvorfall offengelegt, siehe auch Tschohl et al., "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs," S. 5.

[1130] *Anderl et al.*, NISG::Kommentar, § 23, Rz 5.

[1131] Das Prinzip der Amtswegigkeit besteht bereits im Vorfeld eines Strafverfahrens bzw. für jene Verfahrensschritte, die dem Anfangsverdacht vorgelagert sind, siehe dazu *Schmoller* in Fuchs /Ratz, Wiener Kommentar zur Strafprozessordnung, Rz 9.

Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) oder einen Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB) handeln.

In diesem Zusammenhang stellt sich die Frage, in welchen Fällen der Bundesminister für Inneres amtswegig Ermittlungen einzuleiten hat, sofern ihm eine freiwillige Meldung über eine Straftat vom zuständigen Computer-Notfallteam weitergeleitet wird und ihm dadurch zur Kenntnis kommt.

Dabei sollen drei (theoretische) Fälle unterschieden werden:

Fall 1 wäre die unmittelbare Weiterleitung der freiwilligen Meldung[1132] inkl. Nennung der betroffenen Einrichtung durch das Computer-Notfallteam an den Bundesminister für Inneres (wie dies auch bei meldepflichtigen Sicherheitsvorfällen der Fall ist). Da in diesem Fall die genauen Informationen des Vorfalles sowie der betroffenen Einrichtung aufliegen, hätte der Bundesminister für Inneres jedenfalls amtswegig Ermittlungen einzuleiten, sofern es sich um eine Straftat handelt. Dies trifft im Grunde auf jeden meldepflichtigen Sicherheitsvorfall zu, da dieser in jedem Fall und unverzüglich vom Computer-Notfallteam an den Bundesminister für Inneres weiterzuleiten ist.[1133]

Fall 2 wäre die unmittelbare Weiterleitung der freiwilligen Meldung ohne Nennung der betroffenen Einrichtung an den Bundesminister für Inneres. Auch hier muss vom Vorliegen eines Anfangsverdachtes ausgegangen werden, da auf Grund bestimmter Anhaltspunkte – nämlich der übermittelten Informationen - angenommen werden kann, dass eine Straftat begangen wurde.[1134] Die Nennung des Opfers ist dabei mE nicht erforderlich. Im Rahmen der amtswegig einzuleitenden Ermittlungen hätte die Kriminalpolizei in diesen Fällen wohl Ermittlungen beim zuständigen Computer-Notfallteam durchzuführen, um an die Informationen über die betroffene Einrichtung zu gelangen.

Da auch dies nicht im Interesse des Gesetzgebers lag, wurde eine Konstellation gewählt (Fall 3), in der keine Ermittlungspflicht durch die Kriminalpolizei entstehen soll. Dabei sollen freiwillige Meldungen nur zusammengefasst an den Bundesminister für Inneres weitergeleitet werden (§ 23 Abs. 1 NISG).

Eine zusammengefasste Meldung könnte beispielsweise Statistiken, gängige Angriffsmuster oder Analyseergebnisse von Angriffen enthalten.
Nach *Markel* in *Fuchs/Ratz* darf „ein Anfangsverdacht nur auf Grund konkreter Anhaltspunkte angenommen werden, aus den Umständen muss sich jedoch noch keine genaue Tatkonkretisierung

[1132] Dieser Fall ist im NISG nicht vorgesehen, soll aber trotzdem kurz dargestellt werden.
[1133] Siehe dazu Kapitel 7.5.6.
[1134] *Anderl et al.*, NISG::Kommentar, § 23, Rz 17.

ergeben. Bestimmte Anhaltspunkte setzen voraus, dass zumindest nach der sich bietenden Sachlage die Annahme einer verfolgbaren Tat indiziert ist. Es muss im Gesamtbild aller Faktoren nach kriminalistischer Erfahrung als möglich erscheinen, dass eine verfolgbare Straftat vorliegt."[1135]

Schmoller geht darüber hinaus davon aus, dass „eine Ermittlungspflicht nicht erst mit Entstehen eines Anfangsverdachtes, sondern bereits für jene Verfahrensschritte gilt, die dem vorgelagert sind (insb. Prüfung, ob sich ein Anfangsverdacht ergibt)".[1136]

Entsprechend diesen Ausführungen genügt eine zusammenfassende Darstellung mE jedenfalls nicht, um der Ermittlungspflicht zu entgehen.[1137] Auch wenn im Bericht lediglich Statistiken, beispielsweise das Vorliegen von fünf Angriffen im Zeitraum der letzten 14 Tage, oder Analyseergebnisse von Angriffen angeführt werden, bei denen der Bundesminister für Inneres (als Sicherheitsbehörde und somit Kriminalpolizei) weiß, dass diese auf freiwilligen Meldungen beruhen und somit tatsächlich vorgefallen sind, wird vom Entstehen eines Anfangsverdachtes oder zumindest einer Ermittlungspflicht zur Prüfung, ob sich ein Anfangsverdacht ergibt, auszugehen sein.

Darüber hinaus sprechen die Erläuternden Bemerkungen davon, dass im Rahmen der zusammengefassten Meldungen die namentliche Nennung des (freiwilligen) Melders auf dessen Verlangen entfallen kann.[1138] Aufgrund dieser Formulierung wäre davon auszugehen, dass der Namen des Melders in der zusammengefassten Meldung inkludiert wird, sofern dieser nicht aktiv seine Nichtnennung verlangt. Diese Idee widerspricht mE dem grundsätzlichen Gedanken. Durch die Nennung konkret Betroffener erfolgt eine Konkretisierung einer Straftat und somit jedenfalls das Entstehen eines Anfangsverdachtes.

Eine zusätzliche Schwierigkeit ergibt sich auch durch die in den Erläuternden Bemerkungen angeführte und einem „zusammenfassenden" Bericht immanenten Möglichkeit, einen Vorfall erst „nach einer gewissen zeitlichen Verzögerung"[1139] dem Bundesminister für Inneres zu übermitteln. Diese verspätete Übermittlung führt möglicherweise dazu, dass öffentliche Stellen nicht mehr rechtzeitig reagieren und zeitnahe die notwendigen Schlüsse ziehen können.[1140]

[1135] *Markel*, § 1, in Fuchs /Ratz (Hrsg), Wiener Kommentar zur Strafprozessordnung (2015), Rz 26.
[1136] *Schmoller* in Fuchs /Ratz, Wiener Kommentar zur Strafprozessordnung, Rz 9.
[1137] Anders hier *Anderl/Heußler/Mayer/Müller*, die durch die Zusammenfassung von keinem Vorliegen einer Ermittlungspflicht ausgehen, *Anderl et al.*, NISG::Kommentar, § 23, Rz 17.
[1138] EB RV NIS-Gesetz, S. 22.
[1139] EB RV NIS-Gesetz, S. 22.
[1140] *Anderl et al.*, NISG::Kommentar, § 23, Rz 11.

7.5.9.2. Prinzip der Anzeigepflicht für Computer-Notfallteams

Unabhängig von der Fragestellung, ob das Amtswegigkeitsprinzip der Sicherheitsbehörde vorliegt, ist die Frage zu stellen, ob es seitens der Computer-Notfallteams selbst bei Einlangen freiwilliger Meldungen zu Straftaten bereits zu einer Anzeigepflicht kommt. Wäre dies der Fall, könnte dies eine Kooperation der Unternehmen verhindern, da wiederum Ermittlungen und somit ein (öffentliches) Strafverfahren ausgelöst werden würden. „Der so gesetzte Fehlanreiz kann langfristig gesehen mehr Schaden anrichten, als eine Anzeigepflicht nutzt.“[1141]

Eine Behörde oder öffentliche Dienststelle ist zur Anzeige an Kriminalpolizei oder Staatsanwaltschaft verpflichtet, sofern ihr der Verdacht einer Straftat bekannt wird, die ihren gesetzmäßigen Wirkungsbereich betrifft (§ 78 Abs. 1 StPO).

Die Anzeigepflicht gilt für Computer-Notfallteams nur insoweit, als es sich dabei um Behörden und nicht um Private handelt. Dabei wird zwischen einem organisatorischen und einem funktionalen Behördenbegriff differenziert. [1142]. Das GovCERT als Teil des Bundeskanzleramtes und somit einer Behörde im organisatorischen Sinn unterliegt der Anzeigepflicht, wohingegen das nationale Computer-Notfallteam oder sektorenspezifische Computer-Notfallteams dieser Anzeigepflicht nicht unterliegen. Selbst wenn man davon ausgeht, dass die (privaten) Computer-Notfallteams für bestimmte Aufgaben beliehen und damit als Behörde im funktionalen Sinne zu qualifizieren seien, würden für sie nach *Schwaighofer* die Anzeigepflicht keine Wirkung entfalten. [1143]

Zusammenfassend ist somit festzustellen, dass unter den bereits eingerichteten[1144] Computer-Notfallteams lediglich das beim Bundeskanzleramt organisatorisch verankerte GovCERT anzeigepflichtig ist[1145]; alle anderen Notfallteams (CERT.at, Energie-CERT)[1146] unterliegen dieser Anzeigepflicht nicht.[1147]

[1141] Tschohl et al., "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs," S. 5.
[1142] mehr zum GovCERT siehe Kapitel 7.4.1.
[1143] Zur Verwendung des organisatorischen statt eines funktionalen Behördenbegriffs siehe *Schwaighofer*, § 78, in Fuchs /Ratz (Hrsg), Wiener Kommentar zur Strafprozessordnung (2017), Rz 6 u. 9.
[1144] Stand Februar 2019.
[1145] Zur Behördeneigenschaft des Bundeskanzleramtes siehe *Schwaighofer* in Fuchs /Ratz, Wiener Kommentar zur Strafprozessordnung, Rz 4.
[1146] Mehr zu den Computer-Notfallteams in Kapitel 7.4.
[1147] Mehr zur Anzeige- und Ermittlungspflicht in Kapitel 7.5.9.

7.5.9.3. Veröffentlichung freiwillig gemeldeter Vorfälle

Art. 20 Abs. 2 NIS-RL regelt, dass einem freiwillig meldenden Unternehmen keine Pflichten entstehen dürfen, die es sonst nicht gehabt hätte. Außerdem wird in dieser Bestimmung der Richtlinie geregelt, dass freiwillige Meldungen nach dem in Art. 14 für verpflichtende Meldungen festgelegten Verfahren zu behandeln sind.

Tschohl folgert daraus, dass auch eine freiwillige Meldung zu der in Art. 14 Abs. 6 NIS-RL vorgesehenen Unterrichtung der Öffentlichkeit führen kann, wenn dies für die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist.[1148]

Dies kann mE womöglich für den Richtlinientext, nicht jedoch für die nationale Umsetzung gelten, da die Veröffentlichung im Rahmen des NIS-Gesetzes klar auf von einem *Sicherheitsvorfall*[1149] betroffene Betreiber wesentlicher Dienste oder Anbieter digitaler Dienste beschränkt ist (§ 10 Abs. 1).

7.6. Abschnitt 6 - Strukturen und Aufgaben im Falle der Cyberkrise

7.6.1. Der Begriff der Cyberkrise und einzurichtende Strukturen in Österreich

Im sechsten Abschnitt des NIS-Gesetzes kommt es zur Regelung eines Bereiches, der zwar im Kontext der Cybersicherheit relevant, nicht jedoch Teil des Richtlinientextes ist.[1150]. Im Gegensatz zur NIS-RL werden im NIS-Gesetz in den §§ 24 und 25 Strukturen und Aufgaben im Falle der Cyberkrise geregelt.

Eine (von der NIS-RL unabhängige) EU-Empfehlung für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und –krisen sieht im EU-rechtlichen Kontext eine Krise dann als gegeben, wenn die durch den Vorfall verursachte Störung zu umfangreich ist, als dass ein betroffener Mitgliedstaat sie alleine bewältigen könnte, oder wenn sie in zwei oder mehr Mitgliedstaaten zu so

[1148] Tschohl et al., "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs," S. 7.
[1149] Der gesetzlich klar von einem (freiwillig zu meldenden) Vorfall oder Risiko getrennt ist.
[1150] Entsprechend einer (nicht im unmittelbaren Zusammenhang mit der NIS-RL stehenden) Empfehlung der Kommission sollten die MS sicherstellen, dass sie mit ihren nationalen Krisenmanagementmechanismen angemessen auf Cybersicherheitsvorfälle reagieren können und die notwendigen Verfahren für eine Zusammenarbeit auf EU-Ebene innerhalb des EU-Rahmens schaffen, siehe Empfehlung der Kommission vom 13.9.2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen, C(2017) 6100 final, S. 6.

weitreichenden Auswirkungen von technischer oder politischer Bedeutung führt, dass eine zeitnahe Koordinierung und Reaktion auf der politischen Ebene der Union erforderlich ist.[1151]

Darüber hinaus wird grundsätzlich betont, dass in erster Linie die Mitgliedstaaten selbst für die Reaktion auf große Cybersicherheitsvorfälle oder –krisen, von denen sie betroffen sind, zuständig sind und den EU-Institutionen dann beispielsweise eine wichtige Rolle zukommt, wenn sich Vorfälle oder Krisen auf die Wirtschaftstätigkeit im Binnenmarkt auswirken.[1152]

Das NIS-Gesetz definiert die Cyberkrise als einen oder mehrere Sicherheitsvorfälle, die eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellen und schwerwiegende Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen können (§ 3 Z 22 NISG). Dabei scheint es sich um die erste Definition des Begriffes einer Krise in der österreichischen Rechtsordnung zu handeln.[1153]

Wenngleich der Begriff der Krise nicht definiert ist, regelt die nationale Rechtsordnung doch Zuständigkeiten zum grundsätzlichen Krisenmanagement. Das Bundesministeriengesetz[1154] weist dem Bundeskanzleramt die anlassbezogene Koordination innerstaatlicher Maßnahmen zur Bewältigung überregionaler oder internationaler Krisen und Katastrophen[1155], dem Bundesministerium für Inneres die Koordination in Angelegenheiten des staatlichen Krisenmanagements und des staatlichen Katastrophenschutzmanagements[1156] zu.[1157] Die eigentliche Zuständigkeit zur Bewältigung von Krisen und Katastrophen liegt gem. Art. 15 B-VG bei den Ländern, die sich in der Gesetzgebung in den einzelnen Katastrophenschutzgesetzen der Länder[1158] manifestiert.

Die Österreichische Cybersicherheitsstrategie legt fest, dass sich das Cyberkrisenmanagement in seiner Zusammensetzung und Arbeitsweise am staatlichen Krisen- und Katastrophenmanagement

[1151] Empfehlung der Kommission vom 13.9.2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen, C(2017) 6100 final, Nr. 2.
[1152] Empfehlung der Kommission vom 13.9.2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen, C(2017) 6100 final, Nr. 14.
[1153] Siehe auch *Anderl et al.*, NISG::Kommentar, § 24, Rz 1.
[1154] Mehr zum BMG siehe Kapitel 4.2.1.
[1155] BMG, Anlage zu § 2, Teil 2 A.
[1156] BMG, Anlage zu § 2, Teil 2 H.
[1157] Mehr zur aktuellen SKKM-Strategie des Bundesministeriums für Inneres siehe *Inneres*, SKKM Strategie 2020, 2009.
[1158] Siehe bspw Wiener Katastrophenhilfe und Krisenmanagementgesetz, LGBl. Nr. 60/2003 idF LGBl. Nr. 57/2018.

(SKKM) orientiert und im Sinne der inneren Sicherheit für übergreifende Bedrohungen der Cyber Sicherheit das Bundesministerium für Inneres die Federführung übernimmt.[1159]

Den Zuständigkeitsregelungen im BMG folgend obliegt dem Bundesminister für Inneres auch in Vollziehung des NIS-Gesetzes die Entscheidung über das Vorliegen einer Cyberkrise (§ 24), wobei zu seiner Beratung in Bezug auf diese Entscheidung und zu operativen Maßnahmen zur Bewältigung einer Cyberkrise ein Koordinationsausschuss eingerichtet wird (§ 25 Abs. 1).

Dabei handelt es sich um ein interministerielles Gremium, welches vom Generaldirektor für die öffentliche Sicherheit geleitet wird und sich aus dem Chef des Generalstabs, dem Generalsekretär des Bundeskanzleramtes und dem Generalsekretär für auswärtige Angelegenheiten zusammensetzt (§ 25 Abs. 2 1. Satz).[1160] Dabei handelt es sich um die hochrangigsten Vertreter auf Beamtenebene[1161] jener Bundesministerien, die auch im IKDOK (§ 7) vertreten sind.

Der Ausschuss kann um weitere Vertreter, insbesondere Betreiber wesentlicher Dienste[1162], Computer-Notfallteams sowie Einsatzorganisationen erweitert werden, wenn dies zur Bewältigung der Cyberkrise erforderlich ist (§ 25 Abs. 2 2. Satz). Dies ist mE deshalb wichtig, da durch einen Sicherheitsvorfall eine umfassende Krise ausgelöst werden kann, die sich auf Tätigkeitsbereiche jenseits der Netz- und Informationssysteme und Kommunikationsnetze auswirkt[1163] und angemessene Reaktionen sich sowohl auf Cyber-Maßnahmen als auch auf andere Maßnahmen zur Eindämmung der Folgen stützen müssen.[1164]

Offen bleibt aus meiner Sicht die Frage, warum nicht Anbieter digitaler Dienste oder Einrichtungen der öffentlichen Verwaltung auch in den Koordinationsausschuss eingebunden werden können, insbesondere sofern sie von einem Sicherheitsvorfall betroffen sind bzw. dieser die Ursache für eine Cyberkrise darstellt.

[1159] *Bundeskanzleramt*, Österreichische Strategie für Cybersicherheit, 2013.

[1160] Zur Rolle des Bundesministers für Landesverteidigung und der Bundesministerin für Europa, Internationales und Äußeres siehe Kapitel 7.2.5.

[1161] Eine Ausnahme bilden hier der Generaldirektor für die öffentliche Sicherheit sowie der Chef des Generalstabs, denen jeweils (Stand April 2019) auf Beamtenebene noch Generalsekretäre übergeordnet sind.

[1162] Bereits die im Jahr 2013 erstellte ÖSCS sieht vor, dass Betreiber von kritischen Infrastrukturen bei Prozessen des nationalen Cyber Krisenmanagements eingebunden werden sollen. Mehr zur ÖSCS siehe Kapitel 3.2.1.

[1163] Ein durch einen Sicherheitsvorfall ausgelöster Ausfall des Stromnetzes in Österreich führt zu zahlreichen weiteren Ausfällen (bspw. von Tankstellen, Aufzügen, Wasserversorgung etc.), die in einem herkömmlichen Krisenmanagement abzuhandeln sein werden.

[1164] Empfehlung der Kommission vom 13.9.2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen, C(2017) 6100 final, S. 2.

Nicht unerwähnt bleiben soll, dass eine Cyberkrise auch einen Fall der militärischen Landesverteidigung (Art. 79 Abs. 1 B-VG) darstellen kann, sofern ein Angriff von außen durch ein anderes Völkerrechtsubjekt erfolgt, der auf die Souveränität der Republik Österreich abzielt.[1165] Näheres dazu regelt das NIS-Gesetz jedoch nicht.

7.6.2. Mögliche Reaktion auf eine Cyberkrise

Wenngleich die Regelung von Strukturen und Prozessen im Cyberkrisenmanagement im nationalen Rechtsrahmen positiv zu bewerten ist, wirken die Bestimmungen doch unvollständig, da sich an die Entscheidung über das Vorliegen einer Cyberkrise – außer der Einrichtung eines Koordinationsausschusses – keinerlei weiteren Befugnisse knüpfen. So kommen den Behörden – insbesondere dem Bundesminister für Inneres als Sicherheitsbehörde – keine zusätzlichen Maßnahmen zu, die möglicherweise notwendig wären, um eine Cyberkrise beenden zu können.

Grundsätzlich festzustellen ist, dass die Reaktion auf Cybersicherheitsvorfälle und speziell –krisen vielfältige Formen annehmen kann. Im Rahmen des NIS-Gesetzes als Möglichkeiten zu nennen sind hier beispielsweise die technische Unterstützung vor Ort und Untersuchung der technischen Ursachen des Sicherheitsvorfalles durch die Computer-Notfallteams[1166], die Auswertung von Ergebnissen aus dem vom Bundesminister für Inneres betriebenen IOC-basierten Frühwarnsystem[1167], die Veröffentlichung von Erkenntnissen für die Bevölkerung[1168] sowie die Übermittlung wichtiger Handlungsempfehlungen zur Verhinderung des weiteren Ausbreitens der Krise an Betreiber wesentlicher Dienste[1169].

Nicht geregelt sind eingreifende Maßnahmen, um gegebenenfalls die (böswillige) Quelle der Cyberkrise, beispielsweise ein angreifendes System, außer Betrieb nehmen zu können. Auch wenn das NIS-Gesetz selbst keine derartigen Befugnisse vorsieht, kennt die österreichische Rechtsordnung doch Regelungen, die auch in diesen Fällen zur Anwendung gebracht werden können.

[1165] Mehr zum Cyberkrieg sowie zur Abgrenzung der Cyberkrise vom Verteidigungsfall siehe *Anderl et al.*, NISG::Kommentar, Rz 15ff.
[1166] Siehe dazu Kapitel 7.4.1.
[1167] Siehe dazu Kapitel 7.3.1.
[1168] Siehe dazu Kapitel 7.5.6.
[1169] Siehe dazu Kapitel 7.2.3.

Zu denken ist beispielsweise an die Aufgaben und Befugnisse des Sicherheitspolizeigesetzes (SPG)[1170], welche die Sicherheitsbehörden (Bundesminister für Inneres als oberste Sicherheitsbehörde) verpflichten, gefährlichen Angriffen[1171] ein Ende zu setzen (§ 21 Abs. 2 SPG).

Die §§ 34 ff SPG regeln besondere Befugnisse zur Erfüllung dieser Aufgabe, beispielsweise das Platzverbot (§ 36), die Wegweisung (§ 38), die Durchsuchung (§ 40) oder die Sicherstellung von Sachen (§ 42). Eine besondere Befugnis zur Abwehr von Angriffen auf Netz- und Informationssysteme findet sich nicht, sieht man von der generellen Möglichkeit einer Durchsuchung von Räumen oder Sicherstellung (bspw. von Servern, von denen Angriffe ausgehen), ab.[1172]

Neben den besonderen Befugnissen findet sich jedoch auch eine allgemeine Befugnis zur Beendigung gefährlicher Angriffe, wonach Organe des öffentlichen Sicherheitsdienstes ermächtigt sind, einem gefährlichen Angriff durch Ausübung von unmittelbarer Befehls- und Zwangsgewalt[1173] ein Ende zu setzen (§ 33 SPG).

Nun stellt sich die Frage, ob darunter auch besondere Maßnahmen zur Abwehr von Cyberangriffen gesetzt werden können. Nach höchstgerichtlicher Entscheidung[1174] handelt es sich bei § 33 um eine Generalklausel, woraus sich keine näheren Beschränkungen – außer bspw. jener des Art. 3 EMRK – ergeben. „Innerhalb dieser Grenzen haben die Organe das in § 33 umschriebene Ziel, nämlich das Ende des gefährlichen Angriffs, zu erreichen – was für die Beendigung eines gefährlichen Angriffs in Betracht kommt, hänge demnach von den konkreten Umständen des Einzelfalls ab."

Davon ist nach *Pürstl/Zirnsack* auch der Eingriff in Rechtsgüter unbeteiligter Dritter umfasst.[1175] Zu denken ist dabei an die Anweisung an einen unbeteiligten Dritten[1176] (bspw. Telekomanbieter),

[1170] Allgemeines zu den Bestimmungen im SPG siehe Kapitel 4.2.2.
[1171] Ein gefährlicher Angriff ist die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Verlangen eines Verletzten verfolgt wird (§ 16 Abs. 2 SPG).
[1172] *Anderl et al.*, NISG::Kommentar, § 24, Rz 12.
[1173] Da eine Definition von Zwang im Gesetz nicht enthalten ist, muss der Begriff durch Auslegung näher bestimmt werden. Nach dem allgemeinen Sprachgebrauch kann daher grundsätzlich jede Maßnahme als Zwangsmaßnahme verstanden werden, die geeignet ist, die in der konkreten Situation zulässige Befugnis auch gegen den Willen des Betroffenen durchzusetzen, siehe *Maier*, § 50 SPG, in Thanner /Vogl (Hrsg), Sicherheitspolizeigesetz, Kommentar (2013), Anm. 6.
[1174] VwGH 8.3.1999, 98/01/0096.
[1175] *Pürstl/Zirnsack*, Sicherheitspolizeigesetz[2] (2011), § 33, Anm. 8.
[1176] Hinzuweisen ist freilich darauf, dass der gefährliche Angriff primär durch Eingriff in die Rechtsgüter des Angreifers beendet werden muss.

einen Server vom Netz zu nehmen, der sich in dessen Eigentum befindet und von dem ohne Wissen und Einfluss des Dritten (ferngesteuert) Angriffe ausgehen.[1177]

Neben den Aufgaben des SPG kommen den Sicherheitsbehörden als Kriminalpolizei[1178] auch die Aufgaben und Befugnisse der StPO[1179] zu, wenn auf Grund bestimmter Anhaltspunkte angenommen werden kann, dass eine Straftat begangen wurde (§ 1 Abs. 3 StPO). Bei so genannten „Cyberangriffen" ist an die Verwirklichung der Straftaten gem. § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem), § 126a StPO (Datenbeschädigung" oder auch § 126b StPO (Störung der Funktionsfähigkeit eines Computersystems) zu denken, die gerichtlich strafbare Tatbestände abbilden. Eine der möglichen Befugnisse der Kriminalpolizei im Rahmen der StPO ist jene der Sicherstellung von Gegenständen. Eine solche ist grundsätzlich aus Beweisgründen zulässig (§ 110 Abs. 1 Z 1 StPO) und kann von der Kriminalpolizei von sich aus durchgeführt werden, wenn ein Gegenstand am Tatort aufgefunden wurde und zur Begehung der strafbaren Handlung verwendet oder dazu bestimmt worden sein könnte (§ 110 Abs. 3 Z 1 lit. c StPO). Somit besteht auch die Möglichkeit, Server, von denen Angriffe ausgehen, sicherzustellen, auch wenn sich diese im Eigentum Dritter – beispielsweise von Telekomanbietern – befinden.[1180]

Die Befugnisse der österreichischen Sicherheitsbehörden und Kriminalpolizei gelten selbstverständlich nur für im Inland befindliche Server. Schwierigkeiten entstehen im Regelfall des Cyberangriffs, nämlich, dass die Angriffe im Ausland ihren Ursprung haben. Die Sicherheitsbehörden stoßen hier neben den Beschränkungen des völkerrechtlichen Souveränitätsprinzips[1181] auf die zumeist vorhandene Unmöglichkeit, die tatsächliche Ursprungs-Quelle der Angriffe zu bestimmen.[1182]

Unabhängig von der zweiten genannten Problematik bestünde für die Sicherheitsbehörden die rechtliche Möglichkeit, als Kriminalpolizei gem. § 1 Abs 1 Z 1 lit. b EU-JZG[1183] (Sicherstellung von Gegenständen) ein Rechtshilfeersuchen an die jeweilige Strafverfolgungsbehörde des fremden Staates zu richten. Bei Betroffenheit eines Staates außerhalb der Europäischen Union kann ein Rechtshilfeersuchen an die Strafverfolgungsbehörde eines fremden Staates gem. dem Budapester

[1177] Das Nutzen im Eigentum Dritter stehender Server ist der Regelfall bei großflächigen Angriffen.
[1178] Die Kriminalpolizei obliegt den Sicherheitsbehörden (§ 18 Abs. 2 StPO).
[1179] Strafprozessordnung 1975 (StPO), StF BGBl. Nr. 631/1975 idF BGBl. I Nr. 70/2018.
[1180] Die StPO beschränkt die Sicherstellung von Gegenständen nicht auf solche im Eigentum von Verdächtigen oder Beschuldigten.
[1181] *Mayer*, Kriminalpolizeiliche Befugnisse im Lichte neuer Technologien (2017), S. 48.
[1182] *Süptitz/Utz/Eymann*, State-of-the-Art: Ermittlungen in der Cloud, Datenschutz und Datensicherheit - DuD, 2013, S. 311.
[1183] Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (EU-JZG), StF BGBl. I Nr. 36/2004 idF BGBl. I Nr. 28/2018.

Übereinkommen über Computerkriminalität (CyCC) gerichtet werden, welches 2012 in Österreich ratifiziert wurde.[1184] Das Übereinkommen formuliert innerstaatlich zu treffende Maßnahmen betreffend die Strafbarkeit von Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und –systemen (Art. 2 ff) sowie verfahrensrechtliche Bestimmungen (Art. 14 ff).

Darüber hinaus werden allgemeine Grundsätze der gegenseitigen Rechtshilfe geregelt (Art. 25 ff), wobei die zuständige Behörde in Österreich im gegenständlichen Fall den betroffenen Vertragsstaat um Sicherstellung eines konkret identifizierten Computersystems[1185] ersuchen könnte.

Neben den sicherheitsbehördlichen bzw. kriminalpolizeilichen Maßnahmen kommen auch Befugnisse im Rahmen der militärischen Landesverteidigung in Betracht, sofern es sich um einen Fall der Cyberverteidigung („Cyberkrieg"[1186]) handelt (mehr zu den Voraussetzungen dafür siehe Kapitel 4.1.2 [Schutz kritischer Infrastruktur als Aufgabe des Österreichischen Bundesheeres]).

Dieser Befugnis widmet sich bereits die geplante Novelle des Militärbefugnisgesetzes, mehr dazu siehe Kapitel 4.2.4 (Militärbefugnisgesetz).

7.7. Abschnitt 7 - Strafbestimmungen

7.7.1. Verwaltungsstrafbestimmungen

Die Mitgliedstaaten sollen Vorschriften über Sanktionen für Verstöße erlassen und alle erforderlichen Maßnahmen treffen, um die Anwendungen der Bestimmungen der NIS-RL sicherzustellen. Die dabei vorgesehenen Sanktionen müssen wirksam, angemessen und abschreckend sein (Art. 21 NIS-RL).

Die nationale Umsetzung sieht Verwaltungsstrafbestimmungen in § 26 Abs. 1 vor, wobei die mangelnde Bekanntgabe einer Kontaktstelle (Z 1), die Nicht-Erbringung eines Nachweises der Sicherheitsvorkehrungen (Z 2), die Verweigerung der Einschau (Z 3), die Nichtumsetzung bescheidmäßig ergangener Anordnungen (Z 4) sowie die Unterlassung einer verpflichtenden Meldung (Z 5) sanktioniert werden. Dass zugehörige Verwaltungsstrafbestimmungen nach dem Adhäsionsprinzip ebenso wie die materiellen Kompetenzbestimmungen vom Bundesgesetzgeber geregelt werden können, ist unstrittig.[1187]

[1184] Übereinkommen über Computerkriminalität, StF BGBl. III Nr. 140/2012 idF BGBl. III Nr. 45/2019.
[1185] Die verfahrensrechtliche Maßnahme dazu wird in Art. 19 Abs. 3 lit. a geregelt.
[1186] *Ischinger* in Abolhassan, Security Einfach Machen, S. 17.
[1187] Nach dem Adhäsionsprinip sind die nach Kompetenzartikeln zugewiesenen Bereiche weiter, als dies zunächst erscheint; dh dass die Kompetenz zur Regelung eines ausdrücklich genannten – meist materiellen – Sachbereiches die Kompetenz zur Regelung weiterer, nicht ausdrücklich angeführter Bereiche nach sich zieht.

Hinsichtlich der Höhe der möglichen Geldstrafen (50.000 Euro, im Wiederholungsfall bis zu 100.000 Euro) drängt sich ein Vergleich mit den Sanktionsmechanismen der DSGVO auf. Diese sieht ein Bußgeld bis zu 20 Mio. Euro oder im Fall eines Unternehmens bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes[1188] des vorangegangenen Geschäftsjahres – je nachdem, welcher der Beträge höher ist - vor (Art. 83 Abs. 5 DSGVO).[1189]

Da in mehreren Kapiteln zuvor[1190] bereits ein Vergleich mit den Vorschriften der DSGVO[1191] gezogen und die Ähnlichkeit – insbesondere hinsichtlich der Erbringung von Sicherheitsvorkehrungen sowie bei der Meldepflicht – betont wurde, stellt sich die Frage, warum die Höhe der Geldbuße bei Zuwiderhandeln so unterschiedlich ausgefallen ist. Dazu ist festzustellen, dass die Entscheidung für niedere Strafsätze vom nationalen Gesetzgeber getroffen wurde, da die NIS-RL selbst lediglich von „wirksamen, angemessenen und abschreckenden" Sanktionen spricht (Art. 21 NIS-RL). Möglicherweise hat sich der nationale Gesetzgeber auch an den Vorschriften des BSI-Gesetzes[1192] orientiert, welches ebenso Bußgelder in der Höhe von 50.000 Euro bzw. 100.000 Euro vorsieht (§ 14 BSI-Gesetz).[1193]

Die Richtlinienkonformität bei nationaler Festlegung derart geringer Strafhöhen ist mE zumindest in Frage zu stellen, da dies für große Unternehmen, die größtenteils von der Richtlinie betroffen sein werden (Unternehmen der Sektoren Bankwesen, Finanzmarktinfrastrukturen, Energie sowie bspw. Anbieter digitaler Dienste) – im Gegensatz zu den Sanktionen der DSGVO – keine abschreckende Wirkung erzielen wird können.

Ursprünglich strittig war die Verfassungskonformität derart hoher Geldstrafen im nationalen Verwaltungsstrafrecht[1194]. Diese Verfassungskonformität wurde erst 2017 vom VfGH in seiner Entscheidung zu den Strafhöhen im Finanzwesen bestätigt.[1195] In diesem Verfahren hatte ein

---

Dies bezieht sich beispielsweise auf das Verfahrensrecht, die Verwaltungspolizei sowie die Festsetzung von Strafen. Siehe *Mayer/Kucsko-Stadlmayer/Stöger*, Bundesverfassungsrecht[11], Rz 259.

[1188] Die Abhängigkeit vom Unternehmensumsatz stammt ursprünglich aus dem Kartellrecht, siehe *Bergt*, Sanktionierung von Verstößen gegen die Datenschutz-Grundverordnung, Datenschutz und Datensicherheit - DuD, 2017, S. 555.

[1189] *Eckhardt/Menz*, Bußgeldsanktionen der DS-GVO, Datenschutz und Datensicherheit - DuD, 2018, S. 139.

[1190] Siehe Kapitel 7.5.2.5, Kapitel 7.5.4, Kapitel 7.5.6.

[1191] Anzumerken ist, dass eine parallele Strafbarkeit gem. Art. 83 Abs. 4 lit a DSGVO und § 54 DSG aufgrund unterschiedlicher Schutzzwecke denkbar ist, siehe *Anderl et al.*, NISG::Kommentar, § 26, Rz 2.

[1192] Umsetzung der NIS-RL in Deutschland.

[1193] *Grudzien*, Datenschutz und Datensicherheit - DuD, 2016, S. 31.

[1194] Das gerichtliche Strafrecht sieht in Österreich max. 180 Tagsätze zu je max. 10.000 Euro (dh max. 1,8 Mio. Euro) vor. Zur Unterscheidung zwischen justiziellem und Verwaltungsstrafrecht siehe ua. *Michels*, Strafbare Handlung und Zuwiderhandlung::Versuch einer materiellen Unterscheidung zwischen Kriminal- und Verwaltungsstrafrecht (1963); *Grof*, Die Trennung zwischen Justiz- und Verwaltungsstrafrecht aus national- und europarechtlichem Blickwinkel (2017).

[1195] VfSlg 20.231/2017.

Kreditinstitut gegen ein Straferkenntnis der Finanzmarktaufsicht Rechtsmittel erhoben, in dem gegen das Kreditinstitut aufgrund mehrerer Übertretungen des BWG eine Geldstrafe in Höhe von insgesamt EUR 953.700,-- verhängt wurde. Der pro Übertretung höchstmögliche Strafrahmen war von der Finanzmarktaufsichtsbehörde in Bezug auf das betroffene Kreditinstitut mit EUR 3.135.494,83 errechnet worden. Der VfGH erkannte, seine bisherige Rechtsprechung nicht aufrecht erhaltend[1196], dass es nicht überzeuge, die Zuständigkeitsabgrenzung zwischen Verwaltungsstrafrecht und gerichtlichem Strafrecht ausschließlich nach dem Kriterium der Strafdrohung zu treffen. Verwiesen wurde in diesem Zusammenhang auch auf die Einräumung der richterlichen Garantien der neu geschaffenen Verwaltungsgerichte erster Instanz, die sich grundsätzlich von den zuvor bestehenden Rechtsschutzeinrichtungen in Gestalt der Unabhängigen Verwaltungssenate unterscheiden würden.

Nichtsdestotrotz soll nochmals auf den Umstand eingegangen werden, dass Verstöße gegen den Schutz personenbezogener Daten nunmehr bis zu 100-fach höher sanktioniert werden, als die Mechanismen zum Schutz der Daseinsvorsorge wie der lebenswichtigen Stromversorgung oder Gesundheitsdienstleistungen. Dies kann mE dadurch begründet werden, dass letzteres – nämlich das Funktionieren der eigenen Systeme und somit des für den Unternehmensgewinn wesentlichen Geschäftsbetriebes – im eigenen Interesse der Unternehmen liegt. Die Betreiber werden somit – unabhängig von den Vorschriften des NIS-Gesetzes – aus Gründen der Betriebskontinuität Maßnahmen setzen, um das Funktionieren ihrer Netz- und Informationssysteme zu gewährleisten. Gänzlich anders stellt sich dies wohl beim Schutz personenbezogener Daten dar, an dem Unternehmen an und für sich aus eigenem kein großes Interesse haben.[1197]

7.7.2. Verbandsverantwortlichkeit und Opportunitätsprinzip

Das österreichische Verwaltungsstrafrecht kennt grundsätzlich keine Verantwortlichkeit juristischer Personen für Verwaltungsübertretungen[1198] - verwaltungsstrafrechtlich verantwortlich sind bei juristischen Personen und bei eingetragenen Personengesellschaften, wenn nichts anderes vorgesehen ist, die zur Vertretung nach außen berufenen Organe (Organwalter) (§ 9 VStG[1199]).[1200]

[1196] VfSlg 12151/1989, 19960/2015.
[1197] Der Vollständigkeit halber soll dazu angemerkt werden, dass sich dieses Interesse in den letzten Jahren wohl auch erhöht hat, da die Sensibilität der Kundinnen und Kunden diesbezüglich massiv gestiegen ist.
[1198] Bisher war eine Verantwortlichkeit juristischer Personen in § 370 Abs. 1a und 1b GewO, § 99d BWG und § 30 iVm § 62 DSG im österreichischen Verwaltungsstrafrecht vorgesehen, siehe *Anderl et al.*, NISG::Kommentar, § 26, Rz 6.
[1199] Verwaltungsstrafgesetz 1991 – VStG, BGBl. Nr. 52/1991 idF BGBl. I Nr. 58/2018.
[1200] Siehe dazu *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 132.

Das NIS-Gesetz regelt das Prinzip einer (nicht vom Schuldprinzip abhängigen)[1201] Verbandsverantwortlichkeit[1202] und orientiert sich dabei an der DSGVO, die dem Modell der originären Verbandshaftung folgt, mit dem Sanktionen unmittelbar gegen den Rechtsträger verhängt werden, bei Unternehmen also regelmäßig gegen die juristische Person, ohne dass eine Zurechnung von Handlungen natürlicher Personen erforderlich wäre.[1203]

Grundgedanke ist, dass jedes Unternehmen verpflichtet ist, sich so zu organisieren, dass Rechtsverstöße ausbleiben, dass jedes Unternehmen das Tun seiner Mitarbeiter kennen muss und dass kein Unternehmen sich darauf berufen kann, dass seine interne Organisation nicht fehlerfrei funktioniert hat. [1204] Im nationalen Recht orientiert[1205] sich die Verbandsverantwortlichkeit des NIS-Gesetzes an der Verwaltungsstrafbestimmung des § 99d BWG bzw. entspricht ihr nahezu wortgleich.

Gleichlautend mit den Regelungen des § 99d BWG ist auch die Bestimmung in § 26 Abs. 6 NISG, die einem Opportunitätsprinzip[1206] folgend ein Absehen von der Bestrafung einer natürlichen Person nach § 9 VStG ermöglicht, wenn für denselben Verstoß bereits eine Verwaltungsstrafe gegen die juristische Person verhängt wurde. § 30 Abs. 3 DSG sieht dazu sogar vor, dass die Datenschutzbehörde bei der Bestrafung der juristischen Person von der Bestrafung einer natürlichen Person nach § 9 VStG abzusehen *hat*.[1207] Aus Art. 83 Abs. 2 DSGVO ergibt sich wiederum, dass die Aufsichtsbehörde sowohl in Bezug auf das Ob eines Bußgeldes, als auch in Bezug auf dessen Höhe ein Ermessen hat.[1208]

Im Verwaltungsstrafverfahren zuständig sind die Bezirksverwaltungsbehörden, wobei sich die örtliche Zuständigkeit nach der Hauptniederlassung des Unternehmens, in Ermangelung einer solchen im Inland nach dem Sitz des Vertreters richtet (§ 26 Abs. 2).

Eine Zuständigkeit der Bezirksverwaltungsbehörden im Verwaltungsstrafverfahren war bis zur letzten Novelle in Umsetzung der DSGVO auch im Datenschutzrecht vorgesehen.[1209] Nunmehr liegt die Verhängung von Geldbußen in der Zuständigkeit der Datenschutzbehörde (§ 30 Abs. 1 DSG) als

[1201] *Anderl et al.*, NISG::Kommentar, § 26, Rz 6.
[1202] Prinzip, dass normwidriges Organ- oder Vertreterverhalten dem Verband als eigenes und schuldhaftes Verhalten zugrechnet wird, siehe dazu *Wagner*, § 99d, in Dellinger (Hrsg), Bankwesengesetz : Kommentar (2016), Rz 4.
[1203] *Bergt*, Datenschutz und Datensicherheit - DuD, 2017, S. 555.
[1204] *Bergt*, Datenschutz und Datensicherheit - DuD, 2017, S. 555.
[1205] So auch EB RV NISG, S. 23.
[1206] Zum Ermessen als abwägungsgebundene Rechtsanwendung im Verwaltungsrecht siehe *Raschauer*, Allgemeines Verwaltungsrecht[3], Rz 573ff.
[1207] Siehe dazu *Anderl et al.*, NISG::Kommentar, § 26, Rz 13.
[1208] *Eckhardt/Menz*, Datenschutz und Datensicherheit - DuD, 2018, S. 141.
[1209] Siehe § 52 Abs. 5 DSG, BGBl. Nr. 165/1999 idF BGBl. I Nr. 120/2017.

Behörde mit vorhandener Expertise in Rechtsfragen des Datenschutzes. Auch im NIS-Regime hätte demnach mE die Zuständigkeit im Verwaltungsstrafverfahren für den Bundesminister für Inneres als Organe mit Expertise geschaffen werden können, dem ohnedies die Aufsichtsfunktionen zu Sicherheitsvorkehrungen (§ 17) und Meldepflicht (§ 19) zukommen.

8. Zusammenfassung der Ergebnisse und Ausblick

Legistische Maßnahmen zur Steigerung der Sicherheit jener Systeme, von denen heutige Gesellschaften mehr denn je abhängig sind, könnten nicht dringlicher sein, wenn man daran denkt, dass die Digitalisierung bereits seit mehr als zehn Jahren unaufhaltsam voranschreitet und den einzelnen Bürger von Jahr zu Jahr stärker betrifft. Auch wenn (mittlerweile hauptsächlich private) Betreiber dieser Systeme eigentlich selbst ausreichend Veranlassung dazu sehen sollten, für eine ausreichende Sicherheit ihrer Dienstleistungen zu sorgen und dementsprechende Maßnahmen zu treffen, so haben Vorfälle und Studien der letzten Jahre das Gegenteil bewiesen. Kostspielige Investitionen in Sicherheit werden oft erst dann getätigt, wenn Unternehmen bereits von Sicherheitsvorfällen betroffen waren. Informationen zu Vorfällen werden nur in den seltensten Fällen an potenziell ebenso gefährdete Organisationen oder Behörden weitergegeben.

Aus diesem Grund waren in Bezug auf Dienste der Daseinsvorsorge immer wieder umfangreiche Privatisierungs- und Ausgliederungsakte des Staates durchaus kritisch zu sehen, wobei rechtlich nichts dagegen einzuwenden ist, auch so genannte Kernaufgaben des Staates auszulagern. Dem Staat obliegt für diese Aufgaben jedoch zumindest eine Gewährleistungs- und Infrastrukturverantwortung, denen er beispielsweise durch Regulierungsbehörden nachkommt.[1210]

Dem Thema der Gewährleistung eines hohen Niveaus der Sicherheit von Netz- und Informationssystemen und somit der Daseinsvorsorge nahm sich im Jahr 2013 die Kommission der Europäischen Union an. Dies mündete im Jahr 2016 in eine Richtlinie und wurde in Österreich (verspätet) mit Dezember 2018 mit dem Bundesgesetz zur Sicherheit von Netz- und Informationssystemen (NIS-Gesetz) umgesetzt.

Nach Kundmachung des NIS-Gesetzes wurde im November 2019 vom Verlag Manz ein Kurzkommentar zum NIS-Gesetz veröffentlicht, an dem die Verfasserin der gegenständlichen Dissertation als eine von vier AutorInnen mitwirkte. Fokus des Kurzkommentars war eine praktische Hilfestellung für die Anwender des NIS-Gesetzes, wohingegen sich gegenständliche Arbeit mit (verfassungs-)rechtlichen Fragen der nationalen Umsetzung der NIS-Richtlinie auseinandersetzt.

Ziel der Arbeit war somit die Untersuchung der verfassungsrechtlichen und einfachgesetzlichen Rechtslage in Bezug auf den Schutz kritischer Infrastruktur und insbesondere den neuen Aufgabenbereich der Cybersicherheit, wobei insbesondere die Gesetzgebungs- und Vollziehungskompetenzen im EU-Primärrecht und österreichischen Verfassungsrecht berücksichtigt wurden. In diesem Zusammenhang spielten auch die Zuständigkeit der

[1210] Siehe Kapitel 7.5.1.1 (Staatliche Gewährleistungsverantwortung des Staates)

Sicherheitsbehörden sowie des Österreichischen Bundesheeres und die Kriterien der Abgrenzung zueinander eine wichtige Rolle.

Die NIS-Richtlinie stützt sich kompetenzrechtlich mit dem Ziel des Funktionierens des Binnenmarktes auf Art. 114 AEUV und ist sowohl mit dem EU-rechtlichen Prinzip der begrenzten Einzelermächtigung als auch mit den Prinzipien der Subsidiarität und Verhältnismäßigkeit vereinbar. Ebenso ist kein Widerspruch zum Vorbehalt zu Regelungen zur Aufrechterhaltung der öffentlichen Ordnung und dem Schutz der inneren Sicherheit sowie dem Vorbehalt für Regelungen der Daseinsvorsorge im EU-Primärrecht erkennbar.[1211] Innerstaatlich stützt sich die Materie der Netz- und Informationssicherheit kompetenzrechtlich überwiegend auf Art. 10 B-VG. Da sie als Querschnittsmaterie jedoch auch Landeszuständigkeiten in (Ausführungs-)gesetzgebung und Vollziehung betrifft, sieht das NIS-Gesetz mit einer Kompetenzdeckungsklausel in Verfassungsrang eine alleinige Zuständigkeit des Bundes vor, um damit die Umsetzung zu vereinfachen.[1212]

Ziel der Arbeit war außerdem die Untersuchung der Umsetzungsmöglichkeiten der Richtlinie anhand der nationalen Rechtsordnung, insbesondere in Zusammenschau mit verfassungsgesetzlich gewährleisteten Rechten, dem geschlossenen Rechtsquellensystem sowie nationalen Möglichkeiten der Einbindung privater in hoheitliche Rechtsakte.

Der Anwendungsbereich setzt sich laut Richtlinientext aus Betreibern wesentlicher Dienste und Anbietern digitaler Dienste zusammen, wobei dieser innerstaatlich auf Einrichtungen der öffentlichen Verwaltung ausgedehnt wurde. Zu kritisieren ist in diesem Zusammenhang, dass sowohl die Richtlinie als auch die nationale Umsetzung die Branchen der Lebensmittelversorgung und der Abwasserentsorgung ausklammern. Wenngleich die Abhängigkeit von IT-Systemen, die als notwendige Voraussetzung von Betreibern wesentlicher Dienste gem. NIS-RL gilt, möglicherweise noch nicht so weit fortgeschritten zu sein scheint wie in den anderen Bereichen, so ist auch hier die Digitalisierungsoffensive nicht aufzuhalten. Der Gesetzgeber hätte hier zukunftsorientierter denken und alle Bereiche der Daseinsvosorge bzw. kritischen Infrastruktur aufnehmen sollen.[1213]

Die Richtlinie lässt die Identifizierung der Betreiber wesentlicher Dienste offen, wobei sich der nationale Gesetzgeber für die Identifizierung per Gestaltungsbescheid („state driven approach“) entschied. Ein anderer Zugang hätte die Selbstermittlung der Betreiber durch festgesetzte Schwellenwerte vorgesehen („provider driven approach“, wie bspw in Deutschland), oder auch die

[1211] Siehe Kapitel 6.2 (Kompetenzgrundlage der Europäischen Union).
[1212] Siehe Kapitel 7.1.1 (Kompetenzdeckungsklausel).
[1213] Siehe Kapitel 7.1.2 (Gegenstand und Ziel des Gesetzes).

Identifizierung mit Verordnung als janusköpfigem Verwaltungsakt mit jedoch beschränkten Rechtsschutzmöglichkeiten.[1214]

Wo der Richtlinientext generisch Verantwortlichkeiten einer nationalen zuständigen Behörde und einer zentralen Anlaufstelle regelt, weist das innerstaatliche NIS-Gesetz diese Aufgaben dem Bundeskanzler und dem Bundesminister für Inneres sowie (meist privaten) Computer-Notfallteams zu. Diese Aufgabenzuweisungen hätten besser gelöst werden können, da sie sich teilweise überschneiden und im Vollzug die Schwierigkeit auftreten wird, dass einzelne Tätigkeiten von mehr als einer Organisation umgesetzt werden. Oft machen Bestimmungen – wie beispielsweise die Analyse von Vorfällen durch den Bundesminister für Inneres und Computer-Notfallteams oder die Vertretung Österreichs nach außen durch Bundeskanzler und Bundesminister für Inneres – den Eindruck, als hätte sich der Gesetzgeber nicht entscheiden können und somit diverse Aufgaben mehrfach verteilt.[1215]

Abweichend vom Richtlinientext regelt das NIS-Gesetz den Betrieb von IKT-Lösungen, konkret den Betrieb eines Sensornetzwerkes und von Honeypots, die jedoch im Gesetz selbst nicht so bezeichnet werden. Diese sensiblen Aufgaben erscheinen aufgrund ihrer hohen potenziellen Eingriffsintensität unzureichend determiniert und verfassungswidrig.[1216]

Kritik muss außerdem am unklaren Regelungssystem zu den im Vollzug bedeutsamen Computer-Notfallteams geübt werden, die an der Hoheitsverwaltung zwar durch schlicht-hoheitliches Handeln, jedoch nicht in Form einer Beleihung eingebunden sind. Grundsätzlich erscheint der vom Gesetzgeber gewählte Ansatz, sektorenspezifische Notfallteams einzurichten und Risiken branchenweise zu identifizieren bzw. Vorfälle zu analysieren, durchaus sinnvoll und zielführend. Umgesetzt wurde diese Idee jedoch in einer Form, die in der Praxis noch Schwierigkeiten mit sich bringen wird, wenngleich eine Prüfung des Sachlichkeitsgebotes gem. Art 7 B-VG keine Verfassungswidrigkeit der Regelung ergab.[1217]

Ein zentraler Untersuchungsbereich dieser Arbeit war der potenzielle Eingriff in verfassungsrechtlich gewährleistete Rechte durch Bestimmungen des NIS-Gesetzes in Umsetzung der Richtlinie, wobei Eingriffe in Rechte der Europäischen Menschenrechtskonvention (EMRK), der Charta der Grundrechte der Europäischen Union (GRC) sowie in nationales Verfassungsrecht wie

[1214] Siehe Kapitel 7.5.3.2 (Rechtliche Möglichkeiten der Umsetzung der Ermittlung von Betreibern wesentlicher Dienste).
[1215] Siehe Kapitel 7.2 (Abschnitt 2 – Aufgaben und Strukturen).
[1216] Siehe Kapitel 7.3.2 (Das Determinierungsgebot (Art. 18 B-VG) im Zusammenhang mit dem Betrieb von IKT-Lösungen).
[1217] Siehe Kapitel 7.4.1.2 (Einrichtung von Computer-Notfallteams).

das Staatsgrundgesetz oder das Datenschutzgesetz untersucht wurden. Dabei ist einleitend jeweils zu prüfen, ob Unternehmen als juristische Personen unter den Anwendungsbereich des jeweiligen Grundrechtes fallen, was nicht immer der Fall war.[1218]

Als unverhältnismäßiger und damit verfassungswidriger Eingriff in das Hausrecht gem. Art. 8 EMRK und Art. 7 GRC, welche auch auf Betriebs- und Geschäftsräume anzuwenden sind, wurde die Möglichkeit des Bundesministers für Inneres erkannt, anlassunabhängig Örtlichkeiten von Unternehmen zu betreten, um die Umsetzung der Sicherheitsvorkehrungen zu überprüfen. Begründend wurde ausgeführt, dass diese Einschau ohnedies bereits von zu beauftragenden qualifizierten Stellen durchgeführt werde und kein sachlicher Grund dafür bestünde, diese Einschau – die eine Mehrbelastung für Betreiber darstellt – nochmals durch den Bundesminister selbst zu wiederholen.[1219] Keinen Eingriff in das Recht auf Schutz der Korrespondenz und Kommunikation als Form des Rechtes auf Privatsphäre gem. Art. 8 EMRK/Art. 7 GRC stellt der Betrieb des Frühwarnsystems in Form von IKT-Lösungen dar, da die Teilnahme auf freiwilliger Basis vorgesehen ist.[1220]

Ebenso verneint wurde ein Eingriff in das Recht auf Freiheit des Eigentums gem. Art. 1 ZP Nr. 1 EMRK, Art. 17 GRC und Art. 5 StGG. Zwar sind wirtschaftliche Interessen, die den Betrieb eines Unternehmens betreffen, durch die Eigentumsfreiheit geschützt und könnten durch die verpflichtende Umrüstung der IT-Systeme einen Eingriff darstellen. Dieser kann jedoch zweifelsohne als erforderlich und verhältnismäßig angesehen werden.[1221]

Strittiger ist dieser Eingriff in Bezug auf die Veröffentlichung von Sicherheitsvorfällen durch die Behörden zu sehen, die eine negative Auswirkung auf den Firmenwert haben könnten, der ebenso durch das Eigentumsrecht geschützt ist. Hier ist einerseits vorzusehen, dass diese Veröffentlichung möglichst ohne Nennung des Namens des Unternehmens erfolgt. Außerdem beinhaltet die Veröffentlichung von Sicherheitsvorfällen durch die Behörde eine Rechtsschutzlücke, da sie nicht als Akt unmittelbarer Befehls- und Zwangsgewalt gilt und damit kein Rechtsschutz vorgesehen ist. In diesem Zusammenhang wird der Gesetzgeber dazu aufgerufen sein, eine solche Möglichkeit zu schaffen, beispielsweise durch ein daran anknüpfendes bescheidmäßiges Überprüfungsverfahren.[1222]

[1218] Siehe Kapitel 7.5.2.1 (Allgemeine Überlegungen).
[1219] Siehe Kapitel 7.5.2.4.2 (Schutz der Wohnung).
[1220] Siehe Kapitel 7.5.2.4.3 (Schutz der Korrespondenz/der Kommunikation).
[1221] Siehe Kapitel 7.5.2.5 (Schutz der Freiheit des Eigentums).
[1222] Siehe Kapitel 7.5.6.8 (Unterrichtung der Öffentlichkeit).

Durch diese Veröffentlichung kann auch ein Eingriff in das Recht auf den Schutz personenbezogener Daten gem. Art. 8 EMRK vorliegen, sofern keine Anonymisierung erfolgt, obwohl diese möglich gewesen wäre. Strittig war in diesem Zusammenhang der Anwendungsbereich des nationalen Datenschutzgesetzes seit der Novelle 2018 mit dem Datenschutz-Änderungsgesetz, dessen Anwendungsbereich juristische Personen wohl nicht mehr berücksichtigt. Zu untersuchen war in diesem Zusammenhang auch der Eingriff durch die Einrichtung eines Sensornetzwerkes, wobei festgestellt wurde, dass es dabei zu keiner Verarbeitung personenbezogener Daten kommt.[1223]

Die verpflichtende Umsetzung von Sicherheitsvorkehrungen und Meldung von Vorfällen stehen im Mittelpunkt sowohl der Richtlinie als auch des Bundesgesetzes. Zu untersuchen war hier einerseits die Form des Rechtsaktes so genannter Leitlinien, die vom Bundeskanzler und Bundesminister für Inneres zur Konkretisierung und Information herausgegeben wurden. Dabei wurde festgestellt, dass es sich zwar nicht um den Rechtstyp einer Verordnung handle, nichtsdestotrotz jedoch eine selbstbindende Wirkung für die Behörde entstehe, ohne dass die Rechtsunterworfenen daran gebunden wären (subnormativer Akt). Im Rahmen dessen wurde auch der Begriff des Soft Law einer Überprüfung im Zusammenhang mit dem geschlossenen Rechtsquellensystem sowie dem nationalen Rechtsschutzsystem unterzogen.[1224]

Schwierigkeiten bestehen in Bezug auf die Sicherheitsvorkehrungen durch eine unklare Regelung in Bezug auf die Legisvakanz und Fristen zur Implementierung der Sicherheitsvorkehrungen durch die Unternehmen, als auch in jenen Fällen, in denen sich IT-Dienstleister von Betreibern wesentlicher Dienste im EU-Ausland oder in Drittstaaten befinden. Hier wären zumindest für den europäischen Raum Regelungen wünschenswert gewesen, die eine Anerkennung von Überprüfungsmechanismen in anderen Ländern vorstehen.[1225]

Überprüft werden sollen die Sicherheitsvorkehrungen durch so genannte qualifizierte Stellen, die weder in Form einer Beleihung noch der Verwaltungshilfe tätig werden, da ihre Rolle eine gänzlich selbstständige ist und die Behörden lediglich auf Ergebnisse ihrer Überprüfungen zurückgreifen.[1226]

Ein Verstoß gegen das Determinierungsgebot gem. Art. 18 B-VG ist in den Regelungen zur Meldepflicht von Betreibern wesentlicher Dienste zu sehen, die eine Pflicht zur Meldung eines Vorfalles für die Einschränkung der Verfügbarkeit vorsieht, die wiederum als „signifikant geminderte Verfügbarkeit des Dienstes in qualitativer Dimension“ legal definiert ist. Darüber hinaus

[1223] Siehe Kapitel 7.5.2.7 (Schutz personenbezogener Daten).
[1224] Siehe Kapitel 7.5.4.1 (Sicherheitsvorkehrungen nach dem Stand der Technik).
[1225] Siehe Kapitel 7.5.4.4 (Unmittelbare Umsetzung der Sicherheitsvorkehrungen nach Zustellung des Bescheides).
[1226] Siehe Kapitel 7.5.5 (Überprüfung der Sicherheitsvorkehrungen durch qualifizierte Stellen).

findet sich kein Hinweis für den Rechtsunterworfenen, wann eine solche geminderte Verfügbarkeit vorliegt, obwohl sich verwaltungsstrafrechtliche Sanktionen daran knüpfen und ein dementsprechend hoher Determinierungsgrad vorzusehen gewesen wäre.[1227]

Analysiert wurde im Rahmen der Meldepflicht auch das Bestehen einer Ermittlungspflicht des Bundesministers für Inneres als Sicherheitsbehörde sowie einer Anzeigepflicht der Computer-Notfallteams, die jeweils dem Ziel von insbesondere freiwilligen Meldungen der Unternehmen zu Vorfällen zuwiderlaufen würden, da diese deren Reputation in Gefahr sehen könnten. Dabei wurde eine Ermittlungspflicht in allen Fällen bejaht, wohingegen die Anzeigepflicht für (private) Computer-Notfallteams verneint wurde, auch wenn man von einer Beleihung selbiger ausgehen würde.[1228]

Bei Verstoß gegen die Vorschriften zu Sicherheitsvorkehrungen und Meldepflichten sieht die Richtlinie wirksame, angemessene und abschreckende Sanktionen vor, die im NIS-Gesetz mit Geldstrafen in der Höhe von bis zu EUR 50.000 und im Wiederholungsfall bis zu EUR 100.000 umgesetzt wurden. Diese geringen Strafhöhen sind insofern beachtlich, als die Datenschutz-Grundverordnung für ähnliche Übertretungen (Sicherheitsvorkehrungen und Meldepflicht) Strafhöhen bis zu EUR 20 Mio oder bis zu 4 % des weltweit erzielten Jahresumsatzes vorsieht. Die Verfassungskonformität derart hoher Strafen im Verwaltungsrecht war ursprünglich strittig, wurde jedoch erst 2017 vom VfGH bestätigt.[1229]

Bleibt schlussendlich die Frage, wie der Staat auf Angriffe auf Netz- und Informationssysteme reagieren bzw. diese abwehren kann. Konkrete Befugnisse sieht das NIS-Gesetz dazu leider nicht vor. Möglichkeiten dazu bestehen bereits jetzt teilweise (und nicht konkret auf IT-Angriffe abzielend) für die Sicherheitsbehörden im Sicherheitspolizeigesetz, für die Kriminalpolizei in der Strafprozessordnung sowie für das Österreichische Bundesheer im Militärbefugnisgesetz. All diese Bestimmungen haben jedoch grundsätzlich andere Arten von Angriffen im Sinn und können in ihrer Auslegung - und das auch nur beschränkt - für Angriffe auf Netz- und Informationssysteme herangezogen werden.[1230]

Wünschenswert wären daher konkrete Aufgaben und Befugnisse für die zuständigen Behörden in den unterschiedlichen Rechtsmaterien, um die Art von Angriffen, die in den letzten Jahren immer häufiger wurden und welche die innere Sicherheit auch in Zukunft gefährden werden, abwehren oder verhindern zu können.

[1227] Siehe Kapitel 7.5.6.2 (Erheblichkeit des Sicherheitsvorfalles).
[1228] Siehe Kapitel 7.5.9 (Freiwillige Meldungen).
[1229] Siehe Kapitel 7.7.1 (Verwaltungsstrafbestimmungen).
[1230] Siehe Kapitel 7.6.2 (Mögliche Reaktion auf eine Cyberkrise).

Abstract (Deutsch)

Die Lebensadern unserer Gesellschaft, wie die Versorgung mit Strom, Trinkwasser, Geldmitteln und Gesundheitsdienstleistungen, sind im Rahmen umfassender Digitalisierungstendenzen mehr denn je von Informations- und Kommunikationssystemen (IKT) abhängig. Um innerhalb der Europäischen Union ein einheitliches Mindestmaß an Sicherheit und Resilienz dieser Systeme, die auch für den Binnenmarkt von hoher Bedeutung sind, sicherstellen zu können, wurde im Juli 2016 die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL) beschlossen und in Österreich Ende 2018 durch das Bundesgesetz zur Sicherheit von Netz- und Informationssystemen (NISG) umgesetzt.

In der gegenständlichen Arbeit wurde die nationale Umsetzung der Richtlinie untersucht, insbesondere im Hinblick auf zu berücksichtigende nationale und europäische Rechtsakte im Zusammenhang mit dem Schutz kritischer Infrastruktur und der Cybersicherheit. Ein grundlegender Untersuchungsgegenstand waren zu Beginn der Arbeit EU-rechtliche sowie verfassungsrechtliche Gesetzgebungs- und Vollziehungskompetenzen in Bezug auf die durch die NIS-RL zu regelnden Aufgaben sowie ein Exkurs in die grundsätzliche Gewährleistungsverantwortung des Staates in Bezug auf die nationale Daseinsvorsorge. Kritisch betrachtet wurde das in diesem Zusammenhang offenkundig weitreichende Regelungsinteresse der EU, welches sich kompetenzrechtlich auf das Funktionieren des Binnenmarktes gem. Art. 114 AEUV stützte, dabei jedoch sehr weitreichende Verpflichtungen implementiert wurden.

Untersucht wurden außerdem vom NISG abweichende, möglicherweise effektivere Alternativen der Umsetzung der Richtlinie in nationales Recht und deren verfassungsrechtliche Zulässigkeit. Als zentraler Gegenstand der Arbeit galt die Prüfung potenzieller Eingriffe in verfassungsrechtlich gewährleistete Rechte durch Bestimmungen des NISG, beispielsweise durch den Betrieb so genannter Honeypots und Sensornetzwerke, durch möglicherweise nicht ausreichend determinierte Meldepflichten, durch die Pflicht zur Veröffentlichung von Sicherheitsvorfällen und durch die eventuell unverhältnismäßige Überprüfung von Sicherheitsvorkehrungen in Unternehmen. Abschließend wurde die rechtliche Möglichkeit des Staates, auf Angriffe gegen Netz- und Informationssysteme zu reagieren, beleuchtet, da die NIS-RL bzw. das NISG selbst dazu keine Befugnisse regeln. Ein (nicht ausreichend zufriedenstellender) rechtlicher Rückgriff kann dabei teilweise auf bestehende Rechtsgrundlagen im Sicherheitspolizeigesetz, in der Strafprozessordnung sowie im Militärbefugnisgesetz erfolgen. Das Ergebnis der Arbeit zeigt jedoch, dass die NIS-RL sowie die nationale Umsetzung dieser nicht die letzten Rechtsakte zum Zukunftsthema der Cybersicherheit gewesen sein dürften.

Abstract (English)

The lifelines of our society, such as the supply of electricity, drinking water, funds and health services, are more dependent than ever on information and communication systems (ICT) in the context of comprehensive digitization trends. In order to be able to ensure a uniform minimum level of security and resilience of these systems within the European Union, which are also of great importance for the internal market, Directive (EU) 2016/1148 on security of network and information systems (NIS Directive) was adopted in July 2016. The Directive was implemented in Austria in December 2018 by the Federal Law on Security of Network and Information Systems (NISG).

In the present thesis, the national implementation of the Directive was examined, especially with regard to the national and European legal acts to be taken into account in connection with the protection of critical infrastructure and cybersecurity. At the beginning of the thesis, a primary object of investigation were competences in legislation and enforcement in EU primary law as well as national constitutional law with regard to the tasks to be regulated by the NIS Directive. Followed by an excursus into the governmental responsibility for guaranteeing public services. A critical analysis referred to the evidently far-reaching regulatory interest of the EU in this context, which in terms of competence relates to the functioning of the internal market in accordance with Art. 114 TFEU and at first seemingly to go far beyond this competence.

In addition, different and possibly more effective alternatives to the implementation of the directive into national law and its constitutional admissibility were examined. The central subject of the thesis was the analysis of potential interferences with constitutionally guaranteed rights by provisions of the NISG, e.g. by the operation of so-called honeypots and sensor networks, by possibly not sufficiently determined reporting obligations, by the obligation to publish security incidents and by the possibly disproportionate review of security measures in companies.

Finally, the legal possibility of the government to react to attacks against network and information systems was examined, since the NIS Directive and the NISG itself do not regulate any powers. A (not sufficiently satisfactory) recourse can partially be based on existing legal bases in the Security Police Act (SPG), the Code of Criminal Procedure (StPO) and the Military Authorization Act (MBG). However, the result of the thesis shows that the NIS Directive and its national implementation were probably not the last legal acts on the future topic of cybersecurity.

Quellen- und Literaturverzeichnis

EU-Rechtsakte und -Quellen

"Anhang der Mitteilung der Kommission an das Europäische Parlament und den Rat - Bestmögliche Netz- und Informationssicherheit - hin zu einer wirksamen Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union." 2017.

"Charta der Grundrechte der Europäischen Union." ABl. C 83/389, 2010.

"Cyber-Sicherheitsstrategie für Deutschland." Berlin: Bundesministerium des Inneren, 2016.

"Empfehlung der Kommission vom 13.9.2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen." EU Publications, 2017.

Entstaatlichung - Gefahr für den Rechtsstaat?(Wien Graz 2002).

Erläuterungen zur Charta der Grundrechte, ABl. C 303/17.

"Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Cybersicherheitsstrategie der Europäischen Union - ein offener, sicherer und geschützter Cyberraum." 2013.

"Guidelines on notification of Operators of Essential Services incidents." Brussels: EU Cooperation Group, 2018.

"Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact." Brussels: EU Cooperation Group, 2018.

"Informationen der Organe, Einrichtungen und sonstigen Stellen der Europäischen Union, Europäischer Rat, Das Stockholmer Programm - Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger." 2010.

Mitteilung "Leistungen der Daseinsvorsorge" vom 20.09.2000, COM (2000) 580, ABl. EG C 17/4.

"Mitteilung der Kommission an das Europäische Parlament und den Rat - Bestmögliche Netz- und Informationssicherheit - hin zu einer wirksamen Umsetzung der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union." 2017.

"Mitteilung der Kommission an das Europäische Parlament und den Rat, EU-Strategie der inneren Sicherheit: Fünf Handlungsschwerpunkte für mehr Sicherheit in Europa." 2010.

"Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen, Eine allgemeine Politik zur Bekämpfung der Internetkriminalität." 2007.

"Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen, "Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität"." 2009.

"Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine Digitale Agenda für Europa." 2010.

"Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Writschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen." 2009.

"Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Writschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine Digitale Agenda für Europa." 2010.

"Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine Strategie für eine sichere Informationsgesellschaft - "Dialog, Partnerschaft und Delegation der Verantwortung"." 2006.

"Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz." 2001.

"Mitteilung der Kommission über ein Europäisches Programm für den Schutz kritischer Infrastrukturen." 2006.

Protokoll (Nr. 2) über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit, ABl 2008 C 115/206.

Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme, ABl 2005, L 69/67.

"Reference document on Incident Notification for Operators of Essential Services." Brussels: EU Cooperation Group, 2018.

Richtlinie 98/83/EG des Rates vom 3. November 1998 über die Qualität von Wasser für den menschlichen Gebrauch, ABl. 1998, L 330/32.

Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl 2002 L 108/33.

Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl 2008 L 345/75.

Richtlinie 2009/140/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste, der Richtlinie 2002/19/EG über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung und der Richtlinie 2002/20/EG über die Genehmigung elektronischer Kommunikationsnetze und -dienste, ABl 2009 L 337/37.

Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung, ABl. 2011, L 88/45.

Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl 2013 L 218/8.

Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU, ABl 2014 L 173/349.

Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, ABl 2015 L 337/35.

Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl 2016, L 157/1.

Richtlinie (EU) 2016/1145 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl 2016 L 194/1.

Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl L 194/1.

RL 2009/72/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG, ABl. 2009, L 211/55.

"State of the Union 2017 - Factsheet Cybersecurity." Brussels: European Commission, 2017.

"Strategie für einen digitalen Binnenmarkt für Europa." Brüssel: Europäische Kommission, 2015.

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl 2016, L 119/1.

Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Euopäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004, ABl L 165/41.

Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012., ABl. 2013, L 176/1.

Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister., ABl 2012, L 201/1.

Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl 2014, L 257/73.

"Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit")." 2017.

Zusammenfassung der Stellungnahme der Europäischen Datenschutzbeauftragten zur Gemeinsamen Mitteilung der Kommission und der Hohen Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik zur "Cybersicherheitsstrategie der Europäischen Union" und zum Vorschlag der Kommission für eine richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, ABl. C 32/19.

Monographien/Kommentare/Lehrbücher/Artikel

Abbott/Snidal, Hard and Soft Law in International Governance, International Organization, 3/2003,

Abolhassan, Security Einfach Machen, IT-Sicherheit als Sprungbrett für die Digitalisierung (2017).

Adamovich/Funk et al., Österreichisches Staatsrecht (Vienna 2009).

Aichlreiter, Österreichisches Verordnungsrecht: ein systematisches Handbuch[2] (Wien 1988).

Amann, Bedeutung von Produktionskompetenz im Supply Chain Management : Entwicklung einer marktorientierten Steuerungskonzeption am Beispiel der Lebensmittelindustrie(Wiesbaden 2009).

Anderl/Heußler et al., NISG::Kommentar (2019).

Anderl/Tlapak, Die (zukünftige) Zulässigkeit der Einbindung datenschutzrechtlicher Zustimmungen in AGB, ecolex, 7/2016, 563.

Antoniolli/Koja, Allgemeines Verwaltungsrecht[3] (Wien 1996).

Arnold, Rechtsstaat, demokratische Legitimation und Effizienz: Funktionen und Garanten eines sachgerecht flexiblen Legalitätsprinzips, in Arnold/Bundschuh-Rieseneder *et al.* (Hrsg), Recht, Politik, Wirtschaft, Dynamische Perspektiven (2008).

Bachmann/Baumgartner et al., Besonderes Verwaltungsrecht[8] (Wien 2010).

Barfuß, Ressortzuständigkeit und Vollzugsklausel, Eine verfassungs- und verwaltungsrechtliche Untersuchung zur Zuständigkeit der Bundesminister(1968).

Baumgartner, Verfassungsgerichtliche Normenkontrolle und EU-Recht, Zeitschrift für öffentliches Recht, 3/2010, S. 295.

Becker, Art. 52 GRC, in Schwarze (Hrsg), EU-Kommentar (Wien 2019).

Bedner/Ackermann, Schutzziele der IT-Sicherheit, Datenschutz und Datensicherheit - DuD, 5/2010,

Bendiek, Digitale Agenda und Cybersicherheit, in Weidenfeld /Wessels (Hrsg), Jahrbuch der Europäischen Integration 2016 (2016).

Bendiek, Europäische Cybersicherheitspolitik, SWP, 2012,

Bendiek. "Gemeinsame Außen- und Sicherheitspolitik der EU: von der Transformation zur Resilienz." edited by (SWP). Berlin, 2017.

Bendiek, Kritische Infrastruturen, Cybersicherheit und Datenschutz: die EU schlägt Pföcke für digitale Standortpolitik ein, SWP-Aktuell, 35/2013, 1.

Bergt, Sanktionierung von Verstößen gegen die Datenschutz-Grundverordnung, Datenschutz und Datensicherheit - DuD, 2017,

Berka, Die Grundrechte: Grundfreiheiten und Menschenrechte in Österreich(Wien 1999).

Berka, Verfassungsrecht(Vienna 2012).

Bernsdorff, Art. 6 GRC, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014).

Bernsdorff, Art. 8 GRC, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014).

Bernsdorff, Art. 15 GRC, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014).

Bernsdorff, Art. 16 GRC, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014).

Bernsdorff, Art. 17 GRC, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014).

Bezemek, Die Erwerbsfreiheit im StGG - Schutzgegenstand und Stellung, Juristische Blätter, 8/2014,

Binder, Die Daseinsvorsorge der Gemeinde, in Gemeindebund (Hrsg), 40 Jahre Gemeindeverfassungsnovelle 1962 (Wien 2002), VI, 187 S.

Biner/Trauner, Lehrbuch öffentliches Recht - Grundlagen[4] (Wien 2016).

Bock, Terrorismus(München 2009).

Bock/Meissner, Datenschutz-Schutzziele im Recht, Datenschutz und Datensicherheit - DuD, 6/2012,

Borowsky, Allgemeine Bestimmungen über die Auslegung und Anwendung der Charta, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014).

Borowsky, Art. 51, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014).

Borowsky, Art. 52, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014).

Borowsky, Art. 53, in Meyer (Hrsg), Charta der Grundrechte der Europäischen Union::Kommentar (2014).

Breitenmoser, Der Schutz der Privatsphäre gemäß Art. 8 EMRK(Basel 1986).

Brisch, Der Beitrag des Rechts zur IT-Sicherheit: Rechtsrahmen, Anforderungen, Grenzen, in Abolhassan (Hrsg), Security Einfach Machen (Wiesbaden, [Germany] : 2017), 1 online resource (XIII, 142 S.).

Buchner, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, Datenschutz und Datensicherheit - DuD, 3/2016,

Bühler, Einschränkung von Grundrechten nach der Europäischen Grundrechtecharta(Berlin 2005).

Bull, Daseinsvorsorge im Wandel der Staatsformen, Der Staat, 2008,

Burnett, Outsourcing IT, the legal aspects(2009).

Calliess, § 20 Eigentumsgrundrecht, in Ehlers (Hrsg), Europäische Grundrechte und Grundfreiheiten (Berlin 2014).

Calliess, EUV Art. 5, in Calliess /Ruffert (Hrsg), EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar (München 2011).

Chovancová/Ádám et al., Securing Distributed Computer Systems Using An Advanced Sophisticated Hybrid Honeypot Technology, Computing and Informatics, 1/2017,

Davy/Davy, Gezähmte Polizeigewalt? Aufgaben und Neuordnung der Sicherheitspolizei in Österreich(Wien 1991).

Dürig/Fischer, Cybersicherheit in Kritischen Infrastrukturen, Datenschutz und Datensicherheit - DuD, 4/2018, 209.

Eberhard, Das Legalitätsprinzip im Spannungsfeld von Gemeinschaftsrecht und nationalem Recht, Zeitschrift für öffentliches Recht (ZÖR), 1/2008,

Eberhard, Der verwaltungsrechtliche Vertrag(Wien 2002).

Eckhardt/Menz, Bußgeldsanktionen der DS-GVO, Datenschutz und Datensicherheit - DuD, 2018, 139.

Ehlers, Allgemeine Lehren der EMRK, in Ehlers (Hrsg), Europäische Grundrechte und Grundfreiheiten (Berlin 2014).

Einzinger, Datenschutz in Public-Private-Partnerships, in Skopik/Páhi *et al.* (Hrsg), Cyber Situational Awareness in Public-Private-Partnerships (2018).

Einzinger/Skopik, Über die datenschutzrechtliche Problematik in CERTs/CSIRTs-Netzwerken, Datenschutz und Datensicherheit - DuD, 09/2017, 572.

Einzinger/Skopik et al., Keine Cyber-Sicherheit ohne Datenschutz, Datenschutzrechtliche Herausforderungen bei der Etablierung von nationalen CERTs, Datenschutz und Datensicherheit - DuD, 11/2015, 723.

Engels, Zivile Sicherheit in Kritischen Infrastrukturen - Öffentliche Netze, in Gusy/Kugelmann *et al.* (Hrsg), Rechtshandbuch Zivile Sicherheit (Heidelberg 2017).

Ennöckl, EuGH zur Veröffentlichung von EU-Agrarbeihilfen: (vorläufiges) Ende der Transparenz, Österreichische Juristenzeitung (ÖJZ), 21/2011, S. 955.

Feiel, Telekomrecht als Regulierungsrecht, in Raschauer (Hrsg), Aktuelles Telekommunikationsrecht (Wien 2005).

Feiler/Forgó, EU-DSGVO(Wien 2017).

Fichtenbauer, Freiheitliche Vorstellungen zur Landesverteidigung, Strategie und Sicherheit, 1/2013, S. 515.

Forsthoff, Rechtsfragen der leistenden Verwaltung(Stuttgart 1959).

Forsthoff, Rechtsstaat im Wandel(München 1976).

Frenz, Handbuch Europarecht, Band 4, Europäische Grundrechte(Berlin 2008).

Frenz, Handbuch Europarecht, Band 5, Wirkungen und Rechtsschutz(Berlin 2010).

Frenz, Handbuch Europearecht, Band 6, Institutionen und Politiken(Berlin 2011).

Frowein, Art. 8 EMRK, in Frowein /Peukert (Hrsg), Europäische Menschenrechtskonvention: EMRK-Kommentar (Kehl am Rhein 2009).

Fuchs, Verwaltungshilfe, in Fuchs/Merli *et al.* (Hrsg), Staatliche Aufgaben, private Akteure (Wien 2017), XXIV, 273 Seiten.

Funk, Allgemeine Probleme, in Funk (Hrsg), Die Besorgung öffentlicher Aufgaben durch Privatrechtssubjekte (Wien 1981), XVIII, 406 S.

Funk/Marx, Ziviltechnikerurkunden im Verwaltungsverfahren, ÖJZ, 14-15/2002, 532.

Ganglbauer, Das Grundrecht der unternehmerischen Freiheit gem. Art. 16 GRC, in Kahl/Raschauer *et al.* (Hrsg), Grundsatzfragen der europäischen Grundrechtecharta (Wien 2013).

Giese, Sicherheitspolizeirecht, in Bachmann/Baumgartner *et al.* (Hrsg), Besonderes Verwaltungsrecht (Wien 2010).

Gitter/Meißner et al., Das IT-Sicherheitsgesetz, Datenschutz und Datensicherheit - DuD, 1/2016, 7.

Gordon, Official (ISC) Guide to the CISSP CBK[4] (2015).

Grabenwarter/Holoubek, Verfassungsrecht - Allgemeines Verwaltungsrecht[2] (2014).

Grabenwarter/Pabel, Europäische Menschenrechtskonvention(Wien 2012).

Griller, Die Übertragung von Hoheitsrechten auf zwischenstaatliche Einrichtungen(Wien 1989).

Grof, Die Trennung zwischen Justiz- und Verwaltungsstrafrecht aus national- und europarechtlichem Blickwinkel(Wien 2017).

Grudzien, IT-Sicherheitsgesetz - Gedanken zur Implementierung, Datenschutz und Datensicherheit - DuD, 1/2016, 29.

Guizani/Rayes et al., Network Modeling and Simulation, A Practical Perspective(2010).

Guradze, Die Europäische Menschenrechtskonvention : Konvention zu Schutze der Menschenrechte und Grundfreiheiten nebst Zusatzprotokollen; Kommentar(Berlin 1968).

Gusy/Eichenhofer, Die Einzelnen im Recht der Zivilen Sicherheit, in Gusy/Kugelmann *et al.* (Hrsg), Rechtshandbuch Zivile Sicherheit (Heidelberg 2017).

Häberle, Europäische Verfassungslehre(Baden-Baden 2011).

Hartlieb, Verweisung auf technische Normen in Rechtsvorschriften(Berlin [u.a.] 1982).

Hauer/Keplinger, Sicherheitspolizeigesetz[4] (Wien 2011).

Hauer/Keplinger, Sicherheitspolizeigesetz(Wien 2005).

Heinickel/Feiler, IT-SiG-E - europarechtlicher Kontext und die Bedürfnisse der Praxis, Computer und Recht, 11/2014, 708.

Heißl, Verhältnis der Grundrechtecharta zu nationalen Grundrechtsgewährleistungen und zur Europäischen Menschenrechtskonvention in Bezug auf Grundrechtskollisionen, in Kahl/Raschauer *et al.* (Hrsg), Grundsatzfragen der europäischen Grundrechtecharta (Wien 2013).

Hellwig, Organisation, Rahmenbedingungen und Kommunikation bei CERTs, in Huber (Hrsg), Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation (2015).

Henninger/Scheuermann *et al.* "Zurechenbarkeit von Aktionen in virtuellen Welten, Schlussbericht." edited by Gesellschaft: Bundesministerium für Bildung und Forschung (BMBF), 2004.

Herbst, Die Abgrenzung von Bescheid und Verordnung(Wien 2017).

Hiebaum, Gleichheit und Sachlichkeit, Zeitschrift für öffentliches Recht, 3/2009,

Hiessl, Alternativen der kommunalen Wasserversorgung und Abwasserentsorgung(Heidelberg 2003).

Hofer/Hofmann et al., Management der Filiallogistik im stationären Einzelhandel: Eine ressourcenorientierte Betrachtung, Marketing: Zeitschrift für Forschung und Praxis, 2/2009,

Holoubek, Die Sachlichkeitsprüfung des allgemeinen Gleichheitsgrundsatzes, ÖZW, 1991,

Huber, Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation(2015).

Huber/Helllwig et al., Wissensaustausch und Vertrauen unter Computer Emergency Response Teams - eine europäische Herausforderung, Datenschutz und Datensicherheit - DuD, 3/2016, 162.

Huber/Pospisil, Wissensmanagement und Kommunikation bei CERTs, in Huber (Hrsg), Sicherheit in Cyber-Netzwerken; Computer Emergency Response Teams und ihre Kommunikation (2015).

Hübner, Wie wirken Standards und Normen im Recht?, Datenschutz und Datensicherheit - DuD, 2011,

Hummer, Neueste Entwicklungen im Zusammenspiel von Europarecht und nationalem Recht der Mitgliedstaaten(Wien 2010).

Informationssicherheit im Smart Grid, Datenschutz und Datensicherheit - DuD, 11/2013, 747.

Ischinger, Sicherheitspolitik: Regeln für den Cyberraum, in Abolhassan (Hrsg), Security Einfach Machen (2017).

Jarass, Charta der Grundrechte der Europäischen Union : Kommentar^{2} (2013).

Jensen, Zur Messbarkeit von Schutzzielen, Datenschutz und Datensicherheit - DuD, 1/2018,

Kahl, AEUV Art. 114, in Calliess /Ruffert (Hrsg), EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar (München 2011).

Kempen/Hillgruber, Völkerrecht^{2} (2012).

Keplinger/Kutschera et al., Polizeiliches Staatsschutzgesetz(Linz 2016).

Kersten/Klett et al., IT-Sicherheitsmanagement nach der neuen ISO 27001(Wiesbaden 2016).

Kipker/Pfeil, IT-Sicherheitsgesetz in Theorie und Praxis, 12/2016, 810.

Klein-Hennig/Schmidt, Zurück auf Los - Die IT-Sicherheit zurück in der Steinzeit, Datenschutz und Datensicherheit - DuD, 2017,

Kletecka, Schutz gegen "hoheitliche Kreditgefährdung"?, ecolex, 1993, S. 441.

Klett/Ammann, Gesetzliche Initiativen zur Cybersicherheit, Computer und Recht, 2/2014, 93.

Klimburg, Gesamtstaatliche Ansätze zur Cybersicherheit, Strategie und Sicherheit, 1/2012,

Klimburg, Gesamtstaatliche Ansätze zur Cybersicherheit: Erfahrungen aus Österreich, Strategie und Sicherheit,

Klimburg/Tirmaa-Klaar. "Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for action within the EU." edited by European Parliament. Brussels, 2011.

Knauff, Der Gewährleistungsstaat: Reform der Daseinsvorsorge(Berlin 2004).

Knauff, Der Regelungsverbund: Recht und Soft Law im Mehrebenensystem(2010).

Knecht, Die Charta der Grundrechte der Europäischen Union(Stuttgart 2005).

Knopp, Stand der Technik, Ein alter Hut oder eine neue Größe?, Datenschutz und Datensicherheit - DuD, 11/2017, 663.

Knyrim/Tretzmüller, Die wichtigsten Regelungen des DSG (neu), Datenschutz konkret, 4/2017, S. 79.

Köndgen, Europäische Methodenlehre, in Riesenhuber (Hrsg), de Gruyter Handbuch (Berlin : 2015), 1 online resource (li, 663 pages).

Könen, IT-sicherheit gesetzlich geregelt, Datenschutz und Datensicherheit - DuD, 1/2016, 12.

Kopetzki, Kommentierung zu Art. 2 EMRK, in Korinek /Holoubek (Hrsg), Bundesverfassungsrecht (Wien 2002).

Korinek, Verfassungsrechtliche Grenzen von Ausgliederungen, Beleihung und Inpflichtnahme, in Duschanek (Hrsg), Beiträge zur Ausgliederungsdiskussion (Wien 2002), 268 S.

Korinek/Holoubek, Grundlagen staatlicher Privatwirtschaftsverwaltung(Graz 1993).

Krajcsir, Staatliche Hoheitsverwaltung durch Private(Wien 1999).

Krajewski, Aktuelle Rechtsprechung des Gerichtshofs der Europäischen Union zu öffentlichen Dienstleistungen, Zeitschrift für öffentliche und gemeinwirtschaftliche Unternehmen, 1/2011, 81.

Kriesel/Kriesel, Cyberwar - relevant für Sicherheit und Gesellschaft? Eine Problemanalyse, Zeitschrift für Außen- und Sicherheitspolitik (ZFA), 4/2011,

Kubin, Die Gemeindeaufgaben und ihre Finanzierung(Wien München 1972).

Kwiatkowski, Soft Law in International Governance, Przegląd Prawniczy Uniwersytetu im. Adama Mickiewicza, 2017, Vol.7(1), pp.93-103,

Lachmayer, Ausgliederungen und Beleihungen im Spannungsfeld der Verfassung, Juristische Blätter, 12/2007,

Leeb, Bescheidwirkungen und ihre subjektiven Grenzen nach dem AVG(2010).

Leisterer, Zivile Cybersicherheit in Europa: Entwicklung des Bereichs der Netz- und Informationssicherheit im Unionsrecht, in Gusy/Kugelmann *et al.* (Hrsg), Rechtshandbuch Zivile Sicherheit (Heidelberg 2017).

Leisterer/Schneider, Der überarbeitete Entwurf für ein IT-Sicherheitsgesetz, Computer und Recht, 9/2014, 574.

Leuschner, Sicherheit als chartarechtliches Gewährleistungsziel in der EU, in Gusy/Kugelmann *et al.* (Hrsg), Rechtshandbuch Zivile Sicherheit (Heidelberg 2017).

Lienbacher, Raumordnungsrecht, in Bachmann/Baumgartner *et al.* (Hrsg), Besonderes Verwaltungsrecht (Wien 2010).

Linder, Daseinsvorsorge in der Verfassungsordnung der Europäischen Union(2004).

Maier, § 50 SPG, in Thanner /Vogl (Hrsg), Sicherheitspolizeigesetz, Kommentar (Wien 2013).

Marchant/Allenby, Soft law: New tools for governing emerging technologies, Bulletin of the Atomic Scientists, 04 March 2017, Vol.73(2), p.108-114,

Markel, § 1, in Fuchs /Ratz (Hrsg), Wiener Kommentar zur Strafprozessordnung (Wien 2015).

Mayer, Gleichbehandlungsgesetz und Rechtsschutzstaat, zeitschrift für Arbeits- und Sozialrecht (ZAS), 1/1992, S. 37.

Mayer, Kriminalpolizeiliche Befugnisse im Lichte neuer Technologien(Wiener Neustadt 2017).

Mayer/Kucsko-Stadlmayer et al., Bundesverfassungsrecht[11] (2015).

Mayerhofer, Artikel 12 Abs 1 Z 5 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (Wien 2015).

McGuire/Downling. "Cyber Crime: a review of the evidence." 2013.

Michaelis, Der "Stand der Technik im Kontext regulatorischer Anforderungen", Datenschutz und Datensicherheit - DuD, 2016, 458.

Michels, Strafbare Handlung und Zuwiderhandlung::Versuch einer materiellen Unterscheidung zwischen Kriminal- und Verwaltungsstrafrecht(Berlin 1963).

Mitterer, Terrorismus - Der Krieg des 21. Jahrhunderts(Wien 2014).

Möstl, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union(2002).

Müller-Graff, Artikel 14 AEUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (Baden-Baden 2012).

Müller-Graff, Artikel 106 AEUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (Baden-Baden 2012).

Müller, Artikel 10 Abs 1 Z 8 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (Wien 2015).

Müller, Das österreichische Regulierungsbehördenmodell(Wien 2010).

Müller, Daseinsvorsorge und die EU: Anmerkungen zu einem alten Streit und jüngeren Entwicklungen, in Bos /Dieringer (Hrsg), Die Genese einer Union der 27, Die Europäische Union nach der Osterweiterung (2008).

Müller, Pressearbeit als (regulierungs-)verwaltungsbehördliche Handlungsform, Zeitschrift für Verwaltung (ZfV), 4/2010, S. 17.

Muzak, Artikel 11 Abs 1 Z 6 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (Wien 2012).

Novak, Das "differenzierte Legalitätsprinzip" in der verfassungsgerichtlichen Rechtsprechung, in Funk /Adamovich (Hrsg), Staatsrecht und Staatswissenschaften in Zeiten des Wandels (Wien 1992).

Öhlinger, Verfassungsrecht[7] (Wien 2007).

Öhlinger/Potacs, EU-Recht und staatliches Recht[6] (2017).

Pachinger, § 16a, in Riesz /Schilchegger (Hrsg), Telekommunikationsgesetz (Wien 2016), 1 Online-Ressource (XXXIX, 1738 Seiten).

Paefgen, Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet(Heidelberg 2016).

Palmer, Dasein oder Nichtsein - Der "Kampf um die Daseinsvorsorge" als exemplarischer Fall, in Hrbek /Nettesheim (Hrsg), Europäische Union und mitgliedstaatliche Daseinsvorsorge (Baden-Baden 2002).

Pernthaler, Umfassende Landesverteidigung(Wien 1970).

Perthold-Stoitzner, Verfassungsrecht(Wien 2015).

Peukert, Art. 5 EMRK, in Frowein /Peukert (Hrsg), Europäische Menschenrechtskonvention: EMRK-Kommentar (Kehl am Rhein 2009).

Pohlmann, Zur Entwicklung einer IT-Sicherheitskultur, Datenschutz und Datensicherheit - DuD, 1/2016, S. 38.

Pollirer/Weiss et al., Datenschutzgesetz (DSG)[4] (2019).

Pöschl, Probleme des Gleichheitssatzes aus österreichischer Sicht, in Merten /Papier (Hrsg), Grundfragen der Grundrechtsdogmatik (Heidelberg 2007).

Pospisil/Gusenbauer et al., Cyber-Sicherheitsstrategien - Umsetzung von Zielen durch Kooperation, Datenschutz und Datensicherheit - DuD, 2017,

Potacs/Rogatsch, in Holoubek /Potacs (Hrsg), Öffentliches Wirtschaftsrecht I (2013).

Pürgy, Dienstleistungen von allgemeinem Interesse in Österreich, in Krautscheid (Hrsg), Die Daseinsvorsorge im Spannungsfeld von europäischem Wettbewerb und Gemeinwohl: Eine sektorspezifische Betrachtung (Wiesbaden 2009), 41.

Pürstl/Zirnsack, Sicherheitspolizeigesetz[2] (2011).

Raschauer, Allgemeines Verwaltungsrecht[3] (Vienna 2009).

Raschauer, Artikel 10 Abs 1 Z 5 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (Wien 2011).

Raschauer, Artikel 10 Abs 1 Z 10 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (Wien 2011).

Raschauer, Die Bundeswettbewerbsbehörde und Art. 6 EMRK, Österreichische Zeitschrift für Wirtschaftsrecht, 2/2008, S. 30.

Raschauer, Europäisches Datenschutzrecht - quod vadis?, in Raschauer (Hrsg), Datenschutzrecht 2010 (Wien 2011).

Raschauer, Subnormative Verhaltenssteuerungen, in Akyürek /Schäffer (Hrsg), Staat und Recht in europäischer Perspektive (Wien 2006).

Reindl-Krauskopf, PStSG Polizeiliches Staatsschutzgesetz(Wien 2016).

Resch, Artikel 11 Abs 1 Z 4 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (Wien 2012).

Riedl, Der Datenschutz für die juristischen Personen bleibt bestehen, Datenschutz konkret, 4/2017, S. 74.

Rill, Der Verwaltungsbegriff, in Ermacora (Hrsg), FS Antoniolli (Wien 1979).

Robrahn/Bock, Schutzziele als Optimierungsgebote, Datenschutz und Datensicherheit - DuD, 1/2018,

Rosenau/Petrus, Artikel 72 AEUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (Baden-Baden 2012).

Rossi, AEUV Art. 72, in Calliess /Ruffert (Hrsg), EUV / AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtescharta, Kommentar (München 2011).

Rossi, Artikel 114 AEUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (Baden-Baden 2012).

Rost, Die Ordnung der Schutzziele, Datenschutz und Datensicherheit - DuD, 2018,

Rost/Pfitzmann, Datenschutz-Schutzziele - revisited, Datenschutz und Datensicherheit - DuD, 6/2009,

Ruffert, § 19 Berufsfreiheit und unternehmerische Freiheit, in Ehlers (Hrsg), Europäische Grundrechte und Grundfreiheiten (Berlin 2014).

Saria, Grundsätzliches zum "Stand der Technik" aus rechtswissenschaftlicher Sicht, in Saria (Hrsg), Der "Stand der Technik" (Graz 2007).

Schäffer, Erfüllung von Verwaltungsaufgaben durch Private (Beleihung und Inpflichtnahme) in Erfüllung von Verwaltungsaufgaben durch Privatrechtssubjekte, in Wirtschaft (Hrsg), Erfüllung von Verwaltungsaufgaben durch Privatrechtssubjekte (1972).

Schmoller, § 2, in Fuchs /Ratz (Hrsg), Wiener Kommentar zur Strafprozessordnung (Wien 2016).

Schön, Private Verwaltungshelfer: beliehene und inpflichtgenommene unter besonderer Berücksichtigung amtshaftungsrechtlicher Aspekte(Wien 1996).

Schöndorf-Haubold, Das Recht der Zivilen Sicherheit an der Schnittstelle von nationaler, europäischer und internationaler Zuständigkeit, in Gusy/Kugelmann *et al.* (Hrsg), Rechtshandbuch Zivile Sicherheit (Heidelberg 2017).

Schramböck, Der Schutz von Geschäfts- und Betriebsgeheimnissen; Praxishandbuch(Wien 2002).

Schuppert, Governance in einer sich wandelnden Welt, in Schuppert /Zürn (Hrsg), (Wiesbaden 2008).

Schwaighofer, § 78, in Fuchs /Ratz (Hrsg), Wiener Kommentar zur Strafprozessordnung (Wien 2017).

Schwarze, Daseinsvorsorge im Lichte des europäischen Wettbewerbsrechts, Europäische Zeitschrift für Wirtschaftsrecht, 11/2001, 334.

Schwarze, Der Grundrechtsschutz für Unternehmen in der Europäischen Grundrechtecharta, Europäische Zeitschrift für Wirtschaftsrecht, 17/2001, S. 517.

Schweighofer/Heußler et al., Informations- und Meldepflichten in PPPs, in Skopik/Páhi *et al.* (Hrsg), Cyber Situational Awareness in Public-Private-Partnerships (2018).

Schweisfurth, Völkerrecht(2006).

Seidel, Präventive Rechtsangleichung im Bereich des Gemeinsamen Marktes, Europarecht, 1/2006, 26.

Simon/Moucha, Verwundbarkeitsprüfungen mit Shodan, Datenschutz und Datensicherheit - DuD, 2016,

Skopik/Fiedler et al., Cyber Attack Information Sharing, Datenschutz und Datensicherheit - DuD, 4/2014, 251.

Sparenberg/Pohlmann, Cybersecurity made in EU, Datenschutz und Datensicherheit - DuD, 4/2018, 220.

Spitzbart, Grundrecht auf Datenschutz für juristische Personen (Dissertation)(Wien 2014).

Stangl, Der Anwendungsbereich der Grundrechtecharta, in Kahl/Raschauer *et al.* (Hrsg), Grundsatzfragen der europäischen Grundrechtecharta (Wien 2013).

Süptitz/Utz et al., State-of-the-Art: Ermittlungen in der Cloud, Datenschutz und Datensicherheit - DuD, 2013, 307.

Teuber, Interessenverbände und Internationalisierung: Dachverbände, Automobilindustrie und Einzelhandel in der Europäischen Union(Wiesbaden 2009).

Toufar, IT-Recht, in Hofmann /Schmidt (Hrsg), Masterkurs IT-Management, Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker (2010).

Tschohl/Hötzendorfer *et al.* "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs." In *ResearchGate*, 2017.

Tschohl/Hötzendorfer *et al.* "Die NIS-Richtlinie und der rechtliche Rahmen von CERTs." In *ResearchGate*, edited by Institute, 2017.

Vedder, Artikel 4 EUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (Baden-Baden 2012).

Vedder, Artikel 5 EUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (Baden-Baden 2012).

Vedder, Artikel 222 AEUV, in Vedder /Heintschel von Heinegg (Hrsg), Europäisches Unionsrecht, EUV/AEUV/Grundrechte-Charta, Handkommentar (Baden-Baden 2012).

Vogelgesang/Möllers et al., Auf der Jagd nach Schwachstellen - Eine strafrechtliche Bewertung von Portscans, Datenschutz und Datensicherheit - DuD, 8/2017, 501.

Voigt/Von dem Bussche, EU-Datenschutz-Grundverordnung (DSVO) : Praktikerhandbuch(Berlin 2018).

Voitel, Sind Hash-Werte personenbezogene Daten?, Datenschutz und Datensicherheit - DuD, 11/2017, 686.

Wagner, § 99d, in Dellinger (Hrsg), Bankwesengesetz : Kommentar (Wien 2016).

Wallnöfer, Artikel 10 Abs 1 Z 9 B-VG, in Kneihs /Lienbacher (Hrsg), Rill-Schäffer-Kommentar Bundesverfassungsrecht (Wien 2015).

Walter, Der Aufbau der Rechtsordnung: eine rechtstheoretische Untersuchung auf Grundlage der reinen Rechtslehre[2] (Wien 1974).

Walter/Mayer, Grundriss des österreichischen Verwaltungsverfahrensrecht[5] (Wien 1991).

Walzel von Wiesentreu, Die Wirtschaftsfreiheit der Gemeinde - Verfassungsdogmatische Anmerkungen zur Zulässigkeit der Ausgliederung von Gemeindeaufgaben, in Arnold/Bundschuh-Rieseneder *et al.* (Hrsg), Recht Politik Wirtschaft, Dynamische Perspektiven (Vienna 2008).

Wegener, § 5 Wirtschaftsgrundrechte, in Ehlers (Hrsg), Europäische Grundrechte und Grundfreiheiten (Berlin 2014).

Weyand, Demokratie und Sicherheit: Zum Kommunikationsprozess Staat - Gesellschaft im Kontext der Zivilen Sicherheit, in Gusy/Kugelmann *et al.* (Hrsg), Rechtshandbuch Zivile Sicherheit (Heidelberg 2017).

Wiater, Bürger und Unternehmen als Akteure der Zivilen Sicherheit, in Gusy/Kugelmann *et al.* (Hrsg), Rechtshandbuch Zivile Sicherheit (Heidelberg 2017).

Wiederin, § 5, in Fuchs /Ratz (Hrsg), Wiener Kommentar zur Strafprozessordnung (Wien 2013).

Willcocks/Fitzgerald et al., Outsourcing IT: The Strategic Implications, Long Range Planning, 5/1995, 59.

Wimmer, § 22 SPG, in Thanner /Vogl (Hrsg), Sicherheitspolizeigesetz, Kommentar (Wien 2013).

Wimmer, Dynamische Verwaltungslehre(Vienna 2010).

Wimmer, Materiales Verfassungsverständnis: ein Beitrag zur Theorie der Verfassungsinterpretation(Wien 1971).

Winkler, Die Grundrechte der Europäischen Union : System und allgemeine Grundrechtslehren(Wien 2006).

Wolff, Zivile Sicherheit als Infrastrukturgewährleistung und Daseinsvorsorge, in Gusy/Kugelmann *et al.* (Hrsg), Rechtshandbuch Zivile Sicherheit (Heidelberg 2017).

Zacherl, Leben gegen Leben? Lebensrecht des Einzelnen im Spannungsverhältnis zur Schutzpflicht des Staates gem. Art. 2 EMRK am Beispiel der Terrorismusbekämpfung(Wien 2010).

Zeder, Die österreichischen Kartellbußen am Maßstab des Kriminalrechts, Juristische Blätter, 8/2007, 477.

Zubke-von Thünen, Technische Normung in Europa(Berlin 1999).

Sonstige Quellen

Anderl/Hörlsberger et al., Kein Schutz von Daten juristischer Personen nach der DSGVO, Dorda Presse, 2018,

"Arbeitsprogramm der österreichischen Bundesregierung 2013-2018." 2013.

BMLVS. "Teilstrategie Verteidigungspolitik 2014." Wien, 2014.

Bundeskanzleramt. "NIS Fact Sheet 08/2018, Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices." 2018.

Bundeskanzleramt. "Österreichische Sicherheitsstrategie." Wien, 2013.

Bundeskanzleramt. "Österreichische Strategie für Cybersicherheit." Wien, 2013.

Bundeskanzleramt. "Österreichisches Programm zum Schutz kritischer Infrastruktur." Wien, 2014.

Bundeskanzleramt. "Österreichisches Programm zum Schutz kritischer Infrastruktur." Wien, 2008.

Bundeskanzleramt/Inneres. "NIS Fact Sheet 01/2019, Kontaktstellen von Betreibern wesentlicher Dienste." 2019.

EBA. "Leitlinien für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie (EU) 2015/2366 (PSD2)." 2017.

EBA. "Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationallen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 (PSD2)." 2018.

Inneres. "SKKM Strategie 2020." Wien, 2009.

Kleines Lexikon der Politik, Band 1145(Bonn 2011).

"Österreichisches Programm zum Schutz kritischer Infrastruktur (APCIP)." 2014.

"Schutz kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS." Bundesamt für Sicherheit in der Informationstechnik, 2017.