universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Methode zur Unterstützung der Reaktionsphase im NIST CSF bei Sicherheitsvorfällen“

verfasst von / submitted by

Dominik Klapec BSc

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

Master of Science (MSc)

Wien, 2021 / Vienna, 2021

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 066 926
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Wirtschaftsinformatik
Betreut von / Supervisor:	Univ.-Prof. Dipl.-Ing. Dr. Dr. Gerald Quirchmayr

Abstract

Die Masterarbeit fokussiert auf die Unterstützung der Reaktionsphase im NIST CSF, die mit Hilfe eines entwickelten Prototyps realisiert wird. Vor allem für betroffene Unternehmen ist es wichtig, entsprechend auf erfolgreiche Cyberangriffe wie APT, DDoS, Ransomware zu reagieren. Daher ist es für diese nützlich, mit Hilfe einer vorbereiteten Reaktionsphase die Reaktionszeit und den entstandenen Schaden zu reduzieren. Zusätzlich kann bei jedem Sicherheitsvorfall etwas Neues gelernt werden. Es wird in der Masterarbeit auf die einzelnen Phasen eines Incident Response Management näher eingegangen. Diese werden im Nachhinein für die Angriffsarten APT (Advanced Persistent Threat), DDoS (Distributed Denial of Service) und Ransomware unterstützt, um einem Unternehmen den Reaktionsablauf zu erleichtern. Dazu wird ein BPMN-Modell erstellt, das den kompletten Ablauf, angefangen von der Meldung eines Vorfalls bis hin zur Auswertung der Reaktion, darstellt. Nach der Beschreibung der Modelle wird auf die Entwicklung des Prototyps eingegangen, der unter anderem mit Hilfe der Beraterfunktion einige Phasen unterstützt. Anschließend wird anhand einer Case Study der Prototyp getestet und die Ergebnisse besprochen. Abschließend werden im Rahmen von Schlussfolgerungen auch Erweiterungsmöglichkeiten aufgezeigt.

The master thesis focuses on the support of the reaction phase in NIST CSF. It will be implemented in a prototype. Especially for effected enterprises it is important to correctly react to cyber-attacks like APT, DDoS, Ransomware. Therefore, it is useful for them to have a well-prepared reaction phase to reduce the reaction time and minimize the damage. Additionally, with every incident, something new can be learned. Different phases of an incident response management cycle will be discussed in more detail in the master's thesis. These will be supported for dealing with APT, DDoS and Ransomware to make it easier for enterprises to react. The BPMN-model will be constructed for representing the complete process starting from the incident and ending with the analysis of the reaction phase. After describing the models, the focus will be on the prototype development, which does for example put different phases through and advice function. Based on the case study the prototype will be tested and the results will be discussed. In the final section conclusion will be drawn and possible solution will be shown.

Keywords: Incident Response, Cyber Security Framework, Reaktionsphase, APT, DDoS, Ransomware

Contents

List of Figures

List of Tables

1 Einleitung

Der Fokus dieser Masterarbeit liegt in der Unterstützung der Reaktion auf Sicherheitsvorfälle, auch Incident Response Management genannt. Ein Sicherheitsvorfall reicht von einer aktiven Bedrohung über einen versuchten Angriff bis hin zu einer erfolgreichen Datenpanne [34]. Da Cyber-Bedrohungen immer mehr an Umfang und Komplexität gewinnen, wenden Unternehmen Praktiken an, die es ihnen ermöglichen, widerstandsfähiger gegen Angriffe zu sein und sich vor zukünftigen Vorfällen zu schützen. Das Ziel ist es die Vorfälle zu identifizieren, zu verwalten und zu analysieren. Ein Prozess zur Verwaltung von Sicherheitsvorfällen besteht aus verschiedenen Phasen. Dieser besteht aus einer "Prepare" Phase, einer "Reaction" Phase und einer "Post-Incident" Phase. [21][34][36]

Solch ein strukturierter Ansatz kann Vorteile mit sich bringen wie z.B.: [21][33][34]

- Eine allgemeine Verbesserung der Informationssicherheit
- Erkennen von Bedrohungen in einem frühen Stadium
- Geringere Auswirkung von Vorfällen
- Bessere Priorisierung der Sicherheitsmaßnahmen
- Bessere und aktuellere Risikobewertung der Informationen

Diese Masterarbeit konzentriert sich auf die "Reaction" Phase. Daher wurde eine Literaturanalyse im Bereich der "Reaction" Phase durchgeführt, die im NIST (National Institute of Standards and Technology) Cybersecurity Framework [42] näher beschrieben ist. Bei diesem Framework handelt es sich um einen risikobasierten Ansatz zum Management von Cybersicherheitsrisiken. Es hilft Unternehmen jeder Größe, das Cybersicherheitsrisiko besser zu verstehen, zu verwalten und ihre Netzwerke und Daten zu schützen. Elemente des Frameworks sind die Funktionen, mit den Phasen Identify, Protect, Detect, Response (Reaction) und Recover. Bei der "Reaction" Phase ist es unter anderem wichtig, im ersten Schritt den Sicherheitsvorfall zu identifizieren. Zusätzlich ist es notwendig, eine Analyse durchzuführen, um aus Fehlern zu lernen. In vielen Fällen ist das Sammeln von Beweismitteln und die forensische Analyse ein weiterer bedeutender Schritt. Bei der forensischen Analyse werden strafbare, rechtswidrige oder sozialschädliche Handlungen nachgewiesen, die mit Hilfe von digitalen Spuren untersucht werden. Weiters ist auch zu beachten, dass der Datenbestand nicht zerstört oder beschädigt wird und eine problemlose Wiederherstellung möglich ist, um frühestmöglich schnell betriebsbereit zu sein. [5][9][18][20][32][34][41][42][45][47][48]

Um die Art von Bedrohungen und das Einsatzumfeld einzugrenzen, fokussiert sich die Masterarbeit auf folgende drei Arten von Bedrohungen:

- APT: Advanced Persistent Threat (APT) ist, wie der Name sagt, nicht ein einfacher Angriff, sondern eine komplexe gezielte Attacke über einen längeren Zeitraum, die sich hauptsächlich gegen Einzelpersonen, bestimmte Organisation oder auch Branchen richtet. Als Ziel ist definiert, sensible oder hochwertige Daten zu stehlen oder Schäden zuzufügen. [7][36][44][50]

- DDoS: Distributed Denial of Service (DDoS) ist eine Angriffsart, bei der der Angreifer versucht, die Leistung des Servers oder Netzwerks zu beeinträchtigen, indem dieser zu viel Datenverkehr an das Ziel sendet, um die Ressourcen zu erschöpfen. Dies führt dazu, dass berechtigte Benutzer die Dienste/Services des Servers nicht nutzen können. Dieser Angriffstyp kommt häufig vor, da dafür Werkzeuge verfügbar sind, und da es nicht problemlos ist, ihn effektiv zu blocken. [27][29]

- Ransomware: Ransomware ist eine Art von Malware, die Daten eines Benutzers verschlüsselt oder den Zugriff auf das System, durch das Sperren des Systembildschirms, einschränkt. Anschließend wird ein Lösegeld verlangt, damit die Daten wieder entschlüsselt werden. Somit wird der Angegriffene dazu gezwungen, Geld zu übermitteln, um auf seine Daten wieder zugreifen zu können. Es können verschiedene Arten von Daten betroffenen sein, wie zum Beispiel wesentliche geldbezogene Informationen, Geschäftsunterlagen, Datenbanken oder auch persönliche Fotos. Es wird erwartet, dass sich Ransomware in naher Zukunft mit der steigenden Anzahl von Geräten, die mit dem Netzwerk verbunden sind, ausbreiten wird. Durch die zunehmende Nutzung von Smartphones, werden diese immer öfter zum Opfer eines Ransomware-Angriffs. [1][38][40]

Für die Unterstützung der Abwicklung der "Reaction" Phase werden im Laufe der Masterarbeit die diesbezüglichen Anforderungen definiert und es wird ein Modell erstellt. Daraufhin wird eine Methode entwickelt, die die einzelnen Schritte unterstützen soll. Anschließend wird dies im Rahmen einer Case Study getestet und die Ergebnisse werden diskutiert.

Diese Arbeit gliedert sich in den State of the Art in Literatur und Praxis, Beschreibung der Aufgabenstellung, Anforderungen an das zu entwickelnde System, Lösungsweg & Modellentwicklung, Implementierungsansatz für den Prototyp, Prototypentwicklung, Test des Prototyps im Rahmen einer Case Study, Diskussion der Ergebnisse sowie Schlussfolgerungen und Erweiterungsmöglichkeiten.

2 State of the Art in Literatur und Praxis

In der Literaturanalyse wird der Fokus auf drei Themenbereiche gelegt. Erstens werden allgemein die wichtigen Dokumente über Incident Response Management und über das NIST CSF [42], mit dem Fokus auf die "Reaction" Phase, die im Framework als Response Funktion beschrieben wird, betrachtet. Zweitens werden einige, bereits bestehende Ansätze, die die Reaktionsphase unterstützen, angeschaut. Drittens werden drei relevante Angriffsarten, und zwar APT, DDoS, Ransomware gewählt und genauer betrachtet.

2.1 Incident Response Management

Unter dem allgemeinem Begriff Incident Management versteht man alle Aktivitäten, die den gesamten Incident Lebenszyklus umfassen. Darunter fällt die Planung, Schulung und Bewusstseinsschaffung, aber auch das Erkennen, Reagieren auf und Lernen von Sicherheitsvorfällen. Das Ziel ist es, einen zuverlässigen und umfassenden Überblick über alle Sicherheitsprobleme in einer IT-Infrastruktur zu schaffen. [24][34]

Wie in [21] erwähnt, ist es für Unternehmen mit einer hohen IT-Abhängigkeit wichtig, auf Risiken pro-aktiv zu reagieren und ein Incident Response Management einzubauen. Incident Response Management kann als ein Ansatz definiert werden, bei dem man einen Sicherheitsvorfall erkennt, im weiteren Schritt versucht diesen anzuhalten oder abzuschwächen, gefolgt von einer Wiederherstellungsphase und anschließend von einer Post-Incident Analyse, um die Infrastruktur und die Prozesse zu verbessern [35]. Es ist für Unternehmen sinnvoll, einen Vorfallreaktionsplan (Incident Response Plan-IRP) zu haben, der aus einer Ansammlung von schriftlichen Anweisungen besteht [45]. Dieses Dokument soll dabei helfen, Sicherheitsvorfälle zu identifizieren und angemessen zu reagieren, um die Auswirkungen der Attacke zu mildern [45]. Wie in [30][35][45] erwähnt, besteht laut dem SANS Institute ein Vorfallreaktionsplan beziehungsweise ein Reaktionsablauf aus folgenden Phasen:

- Vorbereitungsphase: Es müssen zuerst die Vorfallreaktionsrichtlinien definiert werden, gefolgt vom Erstellen eines Reaktionsplans, sowie der Festlegung der Teamstruktur und der Kommunikationsrichtlinien. Zusätzlich ist es bedeutsam, die Anwender und die IT-Mitarbeiter rechtzeitig zu schulen, damit diese jederzeit auf einen Sicherheitsvorfall vorbereitet sind.

- Identifikationsphase: Bei dieser Phase soll zuerst geprüft werden, ob ein Vorfall tatsächlich stattfindet. Nachdem der Angriff identifiziert wurde, sollte mit der Bewertung und der Sammlung der Beweise fortgefahren werden. Diese Beweise müssen anschließend dokumentiert werden.

- Eindämmungsphase: Der verursachte Schaden wird begrenzt und die betroffenen Systeme werden getrennt, damit ein weiterer Schaden verhindert wird. Die Systemsicherung ist dabei erheblich. Das bedeutet, dass ein

forensisches Image vor dem Löschen erstellt wird. Dadurch können die Beweise gesichert werden, die bei Straftaten nützlich sind.

- Ausmerzungsphase: In dieser Phase soll der Auslöser des Sicherheitsvorfalls gefunden und die betroffenen Systeme aus der Umgebung entfernt werden. Anschließend wäre es sinnvoll die Verteidigungsmechanismen zu verbessern, damit erneute Angriffe nicht stattfinden können.

- Wiederherstellungsphase: Nachdem keine weiteren Bedrohungen mehr vorhanden sind, werden die betroffenen Systeme wieder in die Umgebung einbezogen. Daraufhin sollten die Systeme getestet, überwacht und validiert werden.

- Erkenntnisphase: Der Vorfall wird dokumentiert und bei einem Meeting analysiert, was man aus dem Sicherheitsvorfall lernen kann. Dadurch kann zukünftig eine rasche Reaktion ermöglicht werden.

Es ist bedeutsam, die Behandlung von Sicherheitsvorfällen im Vorhinein zu konzipieren und zu üben. Weiters ist es auch notwendig, die Sicherheitsvorfälle so schnell wie möglich zu bearbeiten, damit die Schäden begrenzt werden. Es ist hilfreich, ein vorher erprobtes Verfahren zu verwenden und so die Reaktionszeit zu minimieren. [20]

Ein Beispiel, das die Reaktionsphase unterstützt, ist das NIST Cybersecurity Framework [42] (CSF), das am 12 Februar 2014 von dem National Institute of Standard and Technology veröffentlicht wurde. Das Framework bietet eine gemeinsame Sprache zum Verständnis, zur Verwaltung und zum Ausdruck von Cybersecurity-Risiken, sowohl für interne als auch externe Stakeholder. Es kann zur Ermittlung und Priorisierung von Maßnahmen zur Verringerung des Sicherheitsrisikos verwendet werden. Dabei kann sich dies auf die ganze Organisation konzentrieren oder nur auf ausgewählte kritische Services innerhalb einer Organisation. Das NIST Cybersecurity Framework [42] könnte auch als ein Framework, das eine Reihe von Best Practices, Standards und Empfehlungen beinhaltet, die einer Organisation helfen, ihre Sicherheitsmaßnahmen zu verbessern, definiert werden. [9][41][42]

Das NIST CSF Framework [42] besteht aus drei Elementen: [5][9][41][42][46][48]

- Framework Core: Der Framework Core besteht aus einer Reihe von Sicherheitsaktivitäten, gewünschten Ergebnissen und anwendbaren Referenzen, die in kritischen Infrastruktursektoren üblich sind. Es beinhaltet Standards, Richtlinien und Praktiken, die die Kommunikation von Cybersecurity-Aktivitäten und -Ergebnissen im gesamten Unternehmen ermöglicht. Weiters besteht der Framework Core aus fünf gleichzeitigen, fortlaufenden Funktionen (Phasen) und zwar Identify, Protect, Detect, Respond, Recover. Betrachtet man Figure 1 gibt es noch zusätzlich folgende Elemente im Framework Core: Categories, Subcategories, Informative Sources.

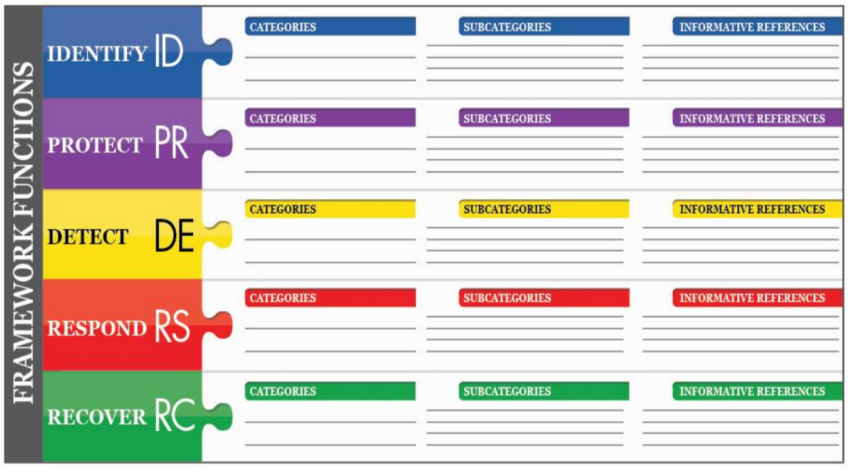

Figure 1: Framework Functions [42]

- Framework Implementation Tiers: Die Framework Implementation Tiers zeigen, wie eine Organisation das Sicherheitsrisiko und die Prozesse zur Steuerung dieses Risikos betrachtet. Dafür werden vier Stufen angeboten. Je höher die Stufe, desto besser ist das Unternehmen.

- Framework Profile: Das Framework Profile bezieht sich auf den aktuellen Status der Cybersecurity-Maßnahmen des Unternehmens, aber auch auf die Roadmaps, die für die Einhaltung der NIST CSF [42] Richtlinien benötigt werden. Weiters sollen Profiles Unternehmen ermöglichen, ihre Schwachstellen zu identifizieren.

Wie in der Einleitung erwähnt, liegt der Fokus der Masterarbeit auf der "Reaction" (Respond) Phase. Die "Reaction" Phase (Funktion) umfasst Aktivitäten im Zusammenhang mit der Entwicklung und Implementierung geeigneter Pläne und Prozesse, um Maßnahmen zu einem erkannten Cybersecurity-Ereignis oder Sicherheitsvorfall zu ergreifen. Hierbei handelt es sich um eine Post-Incident Funktion, die sich auf reaktive Aktivitäten konzentriert und die Fähigkeit der Abschwächung von Auswirkungen unterstützt. Aus Figure 1 können die Beispiele für Ergebniskategorien innerhalb dieser Funktion entnommen werden: Response Planung, Kommunikationen, Analyse, Schadensmilderung (Mitigation) und Verbesserungen. [9][26][41][42][47][48]

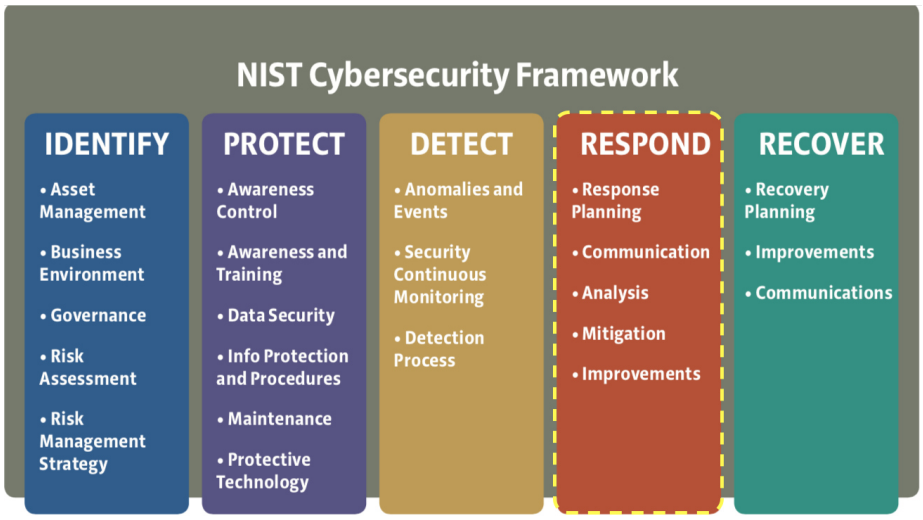

Figure 2: Reaktionsphase im NIST CSF [48]

Wie vorher erkannt und in Figure 2 sichtbar, ist eine der Aufgaben in der "Reaction" (Respond) Phase die Respond Planung beziehungsweise die Vorbereitung auf einen Sicherheitsvorfall. Dafür muss im ersten Schritt der Sicherheitsvorfall identifiziert werden. Dabei ist zu beachten, dass die IT-Mitarbeiter geschult sein sollten und jederzeit mit einem Sicherheitsvorfall rechnen müssen. Es wird daher empfohlen, einen Plan im Vorhinein so zu konzipieren und einzuüben. Dies kann eine rasche, effizientere Bearbeitung von Sicherheitsvorfällen ermöglichen und dabei helfen, Schäden zu begrenzen oder bestenfalls zu vermeiden. Somit kann die Reaktionszeit auch minimiert werden. Beim Plan selbst ist es notwendig, eine Vorgehensweise und die verantwortlichen Personen zur Behandlung von Sicherheitsvorfällen zu definieren. Anders gesagt, sollten eine Teamstruktur und Kommunikationsrichtlinien vorher definiert werden. Weiters ist es hilfreich festzulegen, in welcher Reihenfolge die Schäden des Sicherheitsvorfalls bearbeitet werden sollen. [6][20]

Im nächsten Schritt ist eine Analyse durchzuführen. Grundsätzlich sollte mit einer Erstanalyse begonnen werden. Diese soll dabei helfen, einen Vorfall zu bestätigen und den Umfang herauszufinden. Basierend darauf, können die Auswirkungen eingeschätzt und kann eine Priorisierung durchgeführt werden. Bei der Abwicklung einer genaueren Analyse kann eine forensische Analyse hilfreich sein, wo strafbare, rechtswidrige Handlungen nachgewiesen werden. Dabei werden digitale Spuren gesammelt und ausgewertet. Dazu können Formulare für die Dokumentation der sichergestellten Beweisspuren angewendet werden. Die genaue Vorgehensweise zur Beweissicherung sollte in einem Expertenteam abgeklärt werden. Ein Datenschutzbeauftragter kann auch miteinbezogen werden, damit die Fragen des Datenschutzes berücksichtigt werden. Solch eine Analyse kann dabei helfen, den Angreifer zu identifizieren, Beweise

für juristische Verfahren zu sichern und den entstandenen Schaden zu erkennen. [6][8][14][18][39]

Bei der Analyse sollte beachtet werden, dass es sich um eine fortlaufende Aktivität handelt, die nacheinander oder parallel zu anderen Aktivitäten erfolgen kann. Zusätzlich sollten alle betroffenen Stellen sowohl intern als auch extern über einen Sicherheitsvorfall informiert werden. Wenn die Notwendigkeit besteht, muss die Öffentlichkeit informiert werden. Daher kann es hier hilfreich sein vorher einzuplanen, wer und in welcher Ausführlichkeit benachrichtigt wird. Um einen Überblick der übermittelten Informationen zu erhalten, empfiehlt sich das Einsetzen einer Dokumentation. Normalerweise werden der Datenschutzbeauftragte, Interne Stellen, Externe Stellen, Öffentlichkeit und Sicherheitsgemeinde aufgeklärt. [8][20][39]

Folgende Stellen werden normalerweise aufgeklärt: [20]

- Datenschutzbeauftragter
- Interne Stellen
- Externe Stellen
- Öffentlichkeit
- Sicherheitsgemeinde

Ein weiterer bedeutender Schritt ist die Schadensmilderung des Sicherheitsvorfalls. Der Schaden des Sicherheitsvorfalls muss erkannt, abgeschätzt und gemildert werden, damit das Ausmaß des Schadens so gering wie möglich bleibt. Weiters muss eine Entscheidung getroffen werden, ob die Schadensmilderung gegenüber der Aufklärung Vorrang hat. Währenddessen sollte auf eine Dokumentation nicht vergessen werden. [6][8][20]

Betrachtet man die, im Vorfallreaktionsplan genannten Phasen, ist der nächste Schritt die Durchführung der Wiederherstellung des Betriebes. Aus Sicherheitsgründen sollten alle Daten von schreibgeschützten Datenträgern wiederhergestellt werden und auch alle sicherheitsrelevanten Konfigurationen und Patches miteingespielt werden. Bevor der reguläre Betrieb gestartet wird, sollten alle Passwörter geändert werden, und zwar nicht nur die der IT-Systeme, die vom Sicherheitsvorfall betroffen waren, sondern alle. Nachdem alles wiederhergestellt wurde, sollte überprüft werden, ob alles vollständig funktioniert. Zusätzlich sollten Überwachungswerkzeuge angewendet werden, die eine Logfileanalyse durchführen, da damit gerechnet werden kann, dass der Angreifer einen erneuten Angriff starten könnte. [6][8][20]

Es ist wichtig im letzten Schritt etwas über den Sicherheitsvorfall zu lernen. Dabei kann der zukünftige Umgang mit Sicherheitsvorfällen verbessert werden.

Auch die Sicherheitsmaßnahmen können ausgewertet und im Nachhinein aktualisiert werden. Dazu eignet sich ein Abschlussmeeting, wo ein Follow-up Bericht erstellt und die Wirksamkeit des Verfahrens überprüft werden kann. [6][8][20][39]

2.2 Bereits vorhandene Ansätze für die Unterstützung der Reaktionsphase

2.2.1 CenterTrack & PyFlag

Im Paper [31] wird eine forensische Methode für die Unterstützung der Reaktionsphase vorgeschlagen. Neben der vorgeschlagenen Teambildung und -vorbereitung, in der empfohlen wird, mehrere Schlüsselpersonen aus verschiedenen internen Abteilungen oder auch eine Strafverfolgungsbehörde einzubeziehen, ist es notwendig, eine forensische Analyse durchzuführen, um die digitalen Beweisspuren zu sammeln. Dafür werden hier die zwei Methoden CenterTrack und PyFlag vorgeschlagen. Die CenterTrack Methode beinhaltet spezielle Tracking Router, die ein autonomes Systemnetzwerk überwachen. Die Tracking Router befinden sich physisch oder virtuell an den Edge-Routern, die über IP-Tunnel mit dem zentralen Tracking-System verbunden sind und ein überlagerndes Netzwerk bilden. Der unerwünschte Datenverkehr wird somit an das zentrale Tracking-System weitergeleitet, das Rückwärtsrouten vom Router des Betroffenen auslöst. Die PyFlag Methode hingegen kann ermitteln, woher jedes Datenelement stammt. Es kann der Vorwärts- und Rückwärtsverkehr zwischen Quelle, Ziel und den DNS-Anfragen angezeigt werden. Im Nachhinein können mit Hilfe der zwei Methoden, die gehashten Beweisspuren analysiert und der Angriffsweg rekonstruiert werden. Bestenfalls kann die verantwortliche Person identifiziert und der Prozess verbessert werden. [31]

2.2.2 Security Coordination Model

Wie in Figure 3 sichtbar, wäre ein weiterer Vorschlag das Einsetzen eines Security Coordination Models, das eine Teilnehmerorganisation (PO), eine Koordinationsorganisation (CO) und externe Organisationen berücksichtigt. Dieses besteht aus einem Überwachungssystem (Monitoring System), das sich aus vier Komponenten zusammensetzt. Die Sensoren sind bei den Teilnehmerorganisationen installiert, damit die Sicherheitsfälle erkannt werden können. Nachdem Sicherheitsbedrohungen erkannt worden sind, werden diese an die Koordinationsorganisation übermittelt. Der Aggregator kann die Sicherheitsereignisse der Teilnehmerorganisation sammeln und der Monitor muss diese in Echtzeit überwachen. In diesem Prozess müssen die entdeckten Ereignisse im Protokollspeicher gespeichert werden. Das Reaktionssystem (Response System) besteht aus dem ersten Reaktionsmodul, dem Reaktionsmodul und dem Asset-Informationsspeicher. Das erste Reaktionsmodul sammelt erste Nachweise und verbreitet Warnungen zu Sicherheitsvorfällen. Das Reaktionsmodul isoliert die Cyberangriffe von der Teilnehmerorganisation und beseitigt die Ursache von Vorfällen.

Der Asset-Informationsspeicher speichert die Asset-Informationen von der Teilnehmerorganisation, um den Schadensgrad zu berechnen. Das forensische System besteht aus Beweissammler, Analysator, Reporter und Beweisspeicherung. Der Beweissammler sammelt und behandelt Beweise forensisch und der Analysator untersucht die Ursache von Sicherheitsvorfällen und rekonstruiert diese. Der Reporter erstellt forensisch verschiedene Vorfälle und verbreitet Sicherheitsvorfälle ohne vertrauliche Informationen. [26]

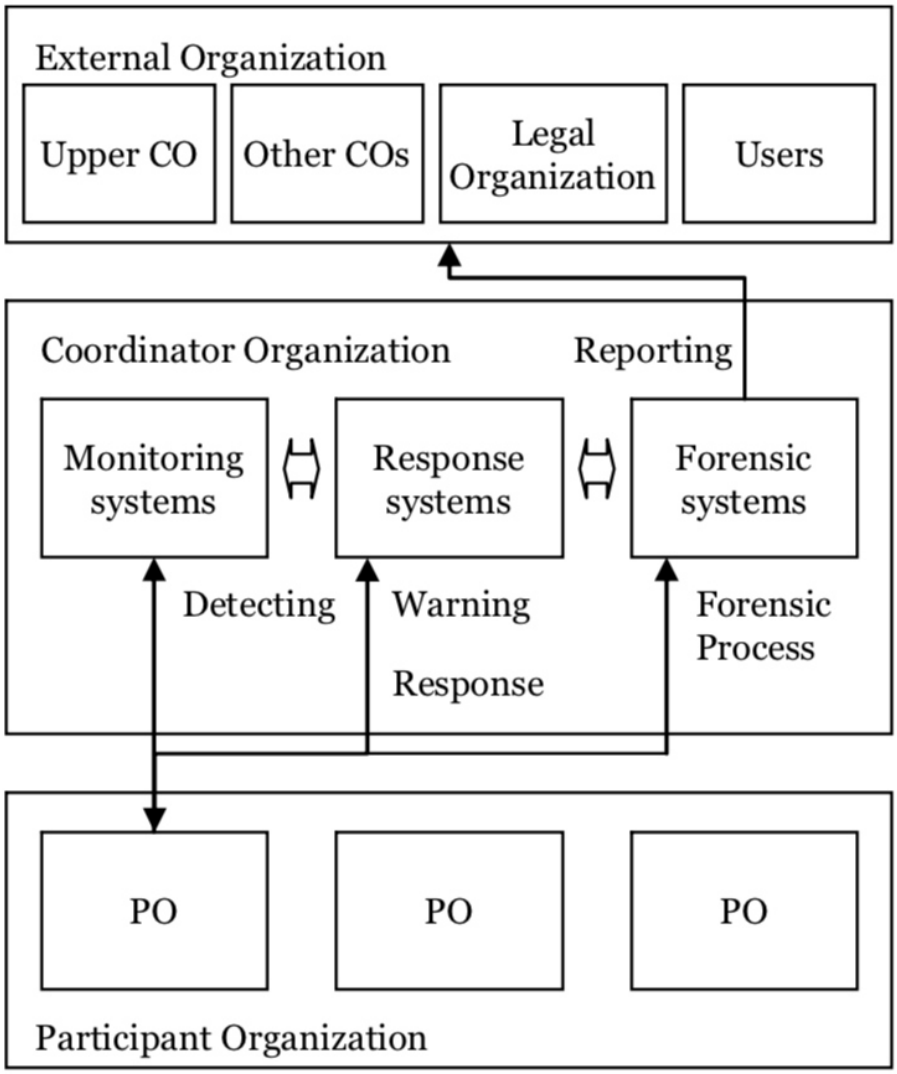

Figure 3: Security Coordination Model [26]

2.2.3 Response Strategy Model

Eine weitere Möglichkeit ist ein Response Strategy Model (RSM), das eine Beziehung zwischen Vorfällen und verschiedenen Arten von Reaktionsoptionen mit unterschiedlichen Prioritätsstufen schafft. Dabei werden Response Planung und das Zeitmanagementkonzept bei der Betrachtung des Angriffs berücksichtigt. Darüber hinaus wird eine Reaktionsstrategie angeboten, in der Vorfälle nach ihrer Priorität in einer ähnlichen Gruppe gesammelt werden, damit dann eine gleichzeitige Reaktion ermöglicht werden kann. Das verwendete Zeitmanagementkonzept besteht aus vier Kategorien von Aufgaben, Q1: kritisch und dringend, Q2: kritisch, aber nicht dringend, Q3: nicht kritisch, aber dringend, Q4: nicht wichtig und nicht kritisch. Weiters wird noch eine Risiko Response Planung mit folgenden Strategien verwendet: Vermeidung, Übertragung, Milderung und Akzeptanz. Dies wird innerhalb einer Tabelle dargestellt, in der Vermeidung die erste Option ist, gefolgt von Übertragung, Minderung und Akzeptanz. Die Tabelle besteht demzufolge aus einer Kombination von Risiko Response Planung, den Quadranten Q1-Q4 und den Reaktionsoptionen. In Figure 4 sieht man ein Beispiel, wie solch eine Tabelle mit den ersten zwei Quadranten dargestellt werden kann. [3]

Risk Response Planning (Threshold)	**Quadrants**	**Response options**
Avoidance (0.75-1.00)	1st Quadrant: Urgent incident and for a critical asset	• Block users, processes or network traffic in preventing future attacks. • Adjust users, processes or network traffic configuration in minimising impacts but maintain system's performances.
Mitigation (0.50-0.75)	2nd Quadrant: Not an urgent incident but for a critical asset	• Collaborate with other appliances by limiting users, processes or network traffic for delaying the process of attacks (Example: using access control, firewall, enabling other countermeasures or antivirus). • Terminate users, processes or network traffic in preventing continuous attacks (Example: locking OS, resetting connection, dropping user and killing process).

Figure 4: Response Strategy Planning [3]

2.2.4 Incident Response System

Ein weiteres Beispiel wäre das IRSS (Incident Response Support System), das sich mit der Reaktion und der automatischen Response Plan Erstellung beschäftigt. Dieses sollte in anderen Sicherheitstools integriert werden. Grundsätzlich wird

hier zuerst der Angriff identifiziert und im Nachhinein die Angriffsbeschreibung ausgegeben. Danach wird ein entsprechender Reaktionsplan vorgeschlagen. [22]

2.2.5 Case-Based Reasoning

Ein anderer Ansatz wäre das Decision Support System, basierend auf Case-based reasoning (CBR) und Ontologie. Dies hilft bei der Erkundung von erfolgreichen Erfahrungen aus der Vergangenheit und beim Aufbau der formalen Repräsentation, damit diese gespeichert und weitergegeben werden können. Das CBR und die Ontologie werden für die Erfüllung der genannten Aufgaben verwendet. [22]

2.2.6 Artificial Model

Auch das Anwenden von Künstlicher Intelligenz kann helfen, das Wissen aus früheren Studien angemessen zu nutzen. Dazu wird ein Modell, siehe Figure 5, vorgeschlagen, das im ersten Schritt die Daten des Sicherheitsvorfalls in der Datenbank speichert und gruppiert, um Beziehungen zwischen zuvor gelösten Straftaten herauszufinden. Wenn ein neuer Fall aufgetreten ist, dann passt das System die entsprechende Straftat an und lernt von selbst, was im Nachhinein bei zukünftigen Analysen verwendet werden kann. [22]

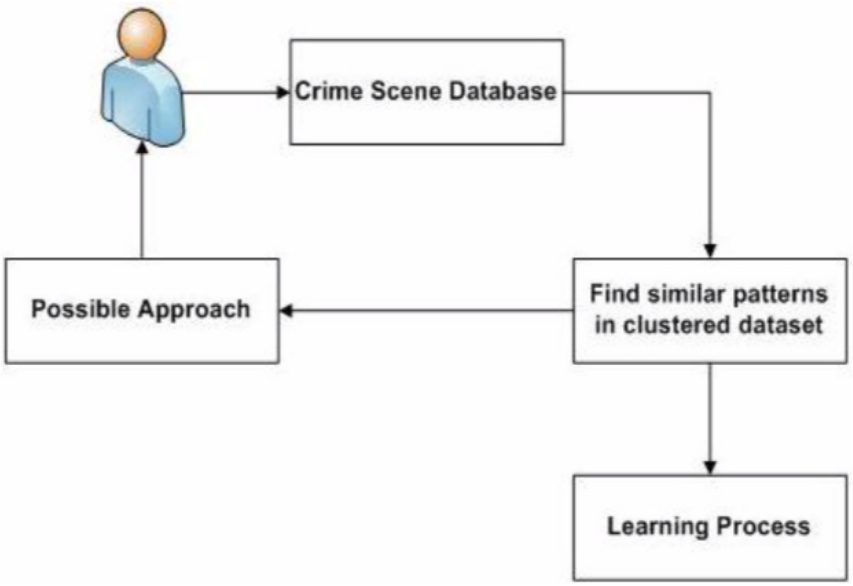

Figure 5: Artificial Model System [22]

2.2.7 Graph based technique

Ein weiterer Ansatz beschäftigt sich mit der Erfassung und Verarbeitung von Eingabedaten, der Quantifizierung von Modellparametern, der Sicherheitsbewertung und der Auswahl der Gegenmaßnahmen auf der Grundlage der Menge von Sicherheitsmetriken. Die vorgeschlagene Technik ermöglicht die Auswahl der Sicherheitsmaßnahmen, die das Risiko im statischen Systembetriebsmodus auf ein akzeptables Niveau verringern und ebenso die Gegenmaßnahmen gegen die erkannten Angriffe im dynamischen Systembetriebsmodus. Die vorgeschlagene Technik ist anpassungsfähig. Daraus folgt, dass die Algorithmen zur Auswahl der Gegenmaßnahmen von den verfügbaren Daten abhängen. Dies ermöglicht es, zu jedem Zeitpunkt Ergebnisse der ausgewählten Gegenmaßnahmen zu erhalten und diese unter Verwendung neu gewonnener Daten zu korrigieren. In Figure 6 sieht man ein Beispiel eines dynamischen Ablaufs. [10]

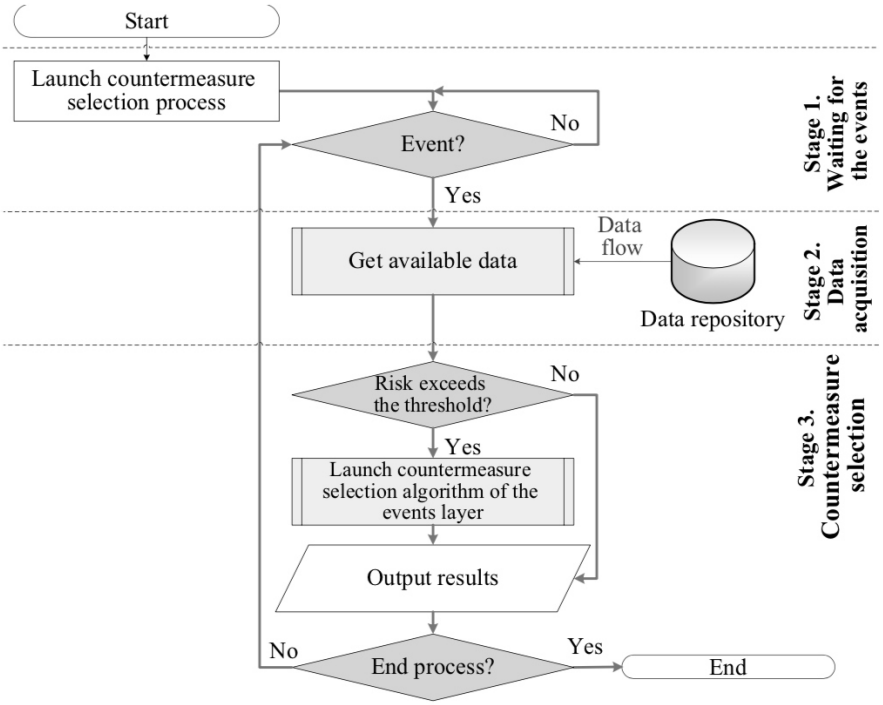

Figure 6: Dynamic Mode [10]

2.2.8 IE-IRS

Eine andere Option wäre IE-IRS, ein Modell für die Reaktionsselektion. Beim IE-IRS werden verschiedene Firewall-Konfiguration als Reaktion auf einen bestimmten Angriff gewählt. Diese Firewall-Konfigurationen werden hinsichtlich ihrer Wirksamkeit bewertet. Daher werden hier die Abhängigkeiten zwischen

Netzwerkdiensten, Systembenutzer, Netzwerktopologien und Firewall-Regeln berücksichtigt. Diese Abhängigkeiten werden als Abhängigkeitsbaum modelliert. [43]

2.2.9 CS-IRS

Weiters gibt es das CS-IRS, wo davon ausgegangen wird, dass Reaktionsmaßnahmen zu positiven und negativen Auswirkungen führen können. Es soll dabei den Schaden des Angriffs und die negativen Auswirkungen der Reaktionsbereitstellung minimieren. Im CS-IRS werden die Reaktionskosten und die Einbruchskosten anhand von zwei Faktoren bewertet: Betriebskosten und Auswirkungen auf die Systemressourcen. Es wird für jede Reaktion ein Parameter für die Erfolgsrate definiert. Wenn die Reaktion erfolgreich war, dann wird der Erfolgsfaktor um 1 erhöht. Ansonsten wird der Ausfallfaktor der Reaktion erhöht. [43]

2.2.10 TVA

Ein anderer Ansatz wäre TVA, bei der es sich um einen Modellierungs- und Simulationsansatz handelt. Dieser stützt sich auf die vorhandenen Sicherheitstools, um die erforderlichen Informationen über die Schwachstellen sowohl aus internen als auch externen Quellen und Netzwerkkonfigurationen zu sammeln. TVA berücksichtigt auch die Angreifer-Perspektive, um alle Angriffspfade innerhalb eines Netzwerks zu ermitteln. [43]

2.2.11 REASSESS

Schlussendlich wird noch ein REASSESS Modell vorgeschlagen, das auf CS-IRS und IE-IRS basiert. Im Gegensatz zum CS-IRS betrachtet REASSESS die negativen Auswirkungen einer Reaktion als Einschätzung des Ausmaßes der negativ betroffenen legitimen Serviceanforderungen aufgrund der Reaktionsbereitstellung. Darüber hinaus werden die negativen Auswirkungen eines Angriffs, ohne dass darauf reagiert wird, anhand der Priorität einer Warnung modelliert. Im Gegensatz zum IE-IRS werden bei REASSESS Strafkosten als Service Level Agreement (SLA) – Verletzungskosten im Zusammenhang mit der Wichtigkeit eines bereitgestellten Dienstes betrachtet. Es besteht aus fünf Stufen: Eingabe und Konfiguration, Alarmverarbeitung, Reaktionsauswahl, Reaktionsausführung und Dokumentation. [43]

2.3 Angriffsarten, die im Rahmen der Masterarbeit adressiert werden sollen

2.3.1 APT

Der dritte Themenbereich der Literaturanalyse befasst sich mit den drei Angriffsarten APT, DDoS und Ransomware. Unter APT versteht man einen fortgeschrittenen (Advanced) Cyberangriff (Threat), der sich über einen längeren

Zeitraum (Persistent), dies können ein Monat oder auch Jahre sein, auf ein bestimmtes Ziel fokussiert. Dies betrifft in den meisten Fällen Organisationen, in denen der Angreifer versucht, sensible Daten zu stehlen oder bestimmte Schäden zuzufügen. Die Anwender von APTs verwenden unterschiedliche Techniken und Technologien für die Intrusionsphase. Dafür werden häufig mehrere Methoden, Werkzeuge zusammengeführt, um ihr Ziel zu erreichen und anschließend darauf zuzugreifen. [7][44]

Wie in [2][49] beschrieben, hat jedes Wort in APT eine Bedeutung:

- Advanced: Der Angreifer verfügt über technische Fähigkeiten, um Schwachstellen beim Ziel ausnützen zu können, indem dieser mehrere Bedrohungsvektoren wie Malware, Spear Phishing, Social Engineering verwendet.
- Persistent: APTs treten häufig über einen längeren Zeitraum hinweg in mehreren Schritten auf. Dies umfasst die Ermittlung der Schwachstellen der Organisation, die Ausnutzung der Schwachstellen, Erweiterung der Kontrolle nach dem Zugang und einen kontinuierlichen Angriff.
- Threat: Der Angreifer ist motiviert einen Angriff durchzuführen, da dieser so zu Vermögenswerten wie Geld oder anderen wichtigen Informationen/Daten von Finanzinstituten oder auch anderen Organisation gelangen kann.

Ein APT hat folgende Merkmale: [44][50]

- Beständig über die Zeit
- Phasen
- Einzelquelle (gleiche Schlüsselakteure)
- Jeder ist eine Bedrohung
- Ungewöhnlich (Muster kann bei einer ungewöhnlichen Tageszeit wiederholt werden)
- Nicht offensichtlich

Wie erwähnt, besteht ein APT-Angriff aus mehreren Phasen. Dabei können folgende fünf Phasen identifiziert werden (siehe Figure 7): [2]

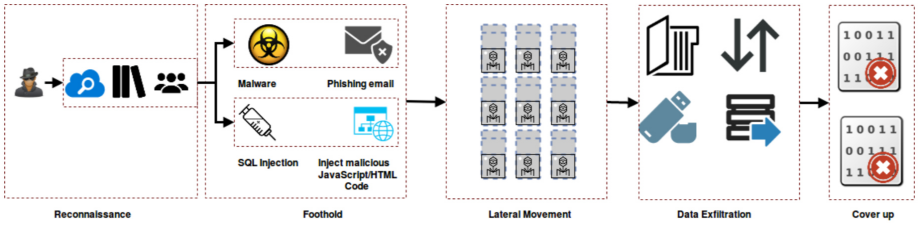

Figure 7: APT-Attack [2]

1. Erkundung (Reconnaissance): Beim ersten Schritt soll etwas über das Ziel gelernt werden. Je mehr gelernt wird, desto höher ist die Erfolgsquote.

2. Halt aufbauen (Establish Foothold): Diese Phase steht für den erfolgreichen Einstieg in den Computer und/oder das Computernetzwerk des Betroffenen.

3. Seitliche Fortbewegung (Lateral Movement): Sobald ein Zugang zum System besteht, müssen anschließend die Knoten gefunden werden, die sensible Daten enthalten.

4. Exfiltration: Wenn das Ziel die Organisationsdaten ist, dann geht es um das Abrufen und Senden der Daten an das Kontrollzentrum des Angreifers.

5. Vertuschung (Cover Up): In dieser Phase versucht der Angreifer alle Beweise, die eine Identifikation ermöglichen könnten, zu entfernen.

Es gibt Technologien wie z.B. Sandboxing und Honeyspot, die ein Unternehmen bei der APT-Erkennung unterstützen können. Sandbox wird verwendet, um einen verdächtigen Inhalt in einer isolierten Umgebung auszuführen und so dessen Verhalten zu beobachten und zu analysieren. Honeyspot zielt darauf ab, mehr Informationen über die eingesetzte Angriffsmethode zu sammeln. Dies soll dabei helfen, die Verbreitung zu stoppen und neue Exploits und Bedrohungen zu identifizieren. [36]

2.3.2 DDoS

Die zweite Angriffsart ist DDoS (Distributed Denial of Service). Bei einem DDoS-Angriff sendet der Angreifer zu viel Datenverkehr an die Zielseite und versucht, die Leistung des Server-Netzwerks zu beeinträchtigen, sodass der Server keinen Dienst mehr für die Benutzer bereitstellen kann. Diese Art ist seit langem bekannt und ist eine der schwerwiegendsten Angriffstypen, da diese über eine einfache Angriffsmethode und ein Werkzeug, das überall leicht zu finden ist, verfügt. Demzufolge kommt es auch häufig vor, besonders im E-Commerce, wo finanzielle Verluste verursacht werden können. Sie ist oft nicht einfach effektiv zu blocken. Weiters ist es normalerweise schwer, den Verkehr von DDoS-Angriffen und normalen Diensten zu unterscheiden. Somit kann es passieren, dass ein normales Paket als ein DDoS-Paket klassifiziert wird. Um die Verluste durch DDoS zu vermeiden und diesen Angriffen entgegenzuwirken, sind effiziente Mechanismen erforderlich. [27][29]

Wie in Figure 8 dargestellt sendet der Angreifer bei einem DDoS-Angriff die Pakete an den kompromittierten Knoten, der Master genannt wird. Diese werden dann vom Master an die Slaves gesendet. Als Quell-IP-Adresse wird eine gefälschte IP-Adresse eingefügt, damit der Angreifer nicht identifiziert werden kann und als Zieladresse wird die IP-Adresse des Betroffenen angegeben. Danach wird der Verkehr in Richtung der Zielmaschine erhöht. [29]

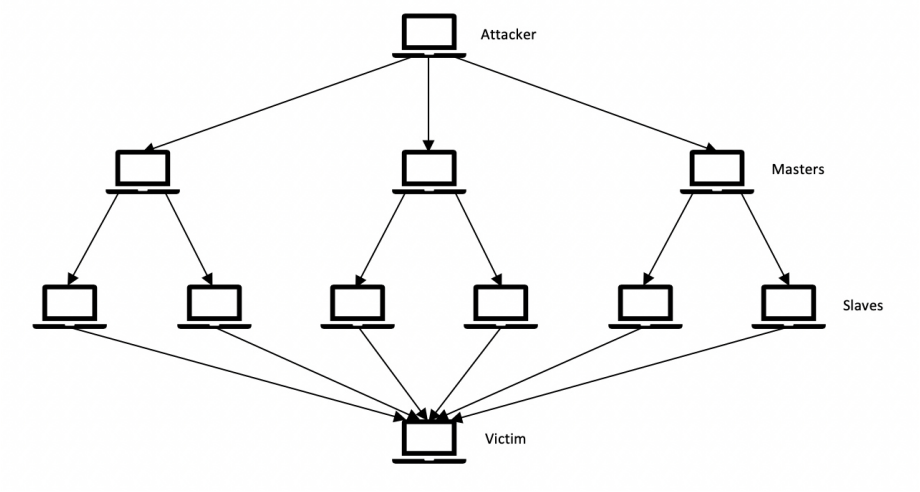

Figure 8: DDoS-Attack [29]

Durch die zunehmende Häufigkeit von DDoS-Attacken wurden viele Erkennungstechnologien entwickelt, um den Angriff zu bekämpfen. Unter anderem gibt es dafür die Egress Filterung, die zum Verwerfen von Paketen mit gefälschten IP-Adressen dient. Diese Art der Filterung erfolgt am Rand eines Netzwerks, an den Firewalls und an den Grenzroutern. Ein weiteres Beispiel wären Paketmarkierungsmechanismen, wo die Zwischenrouter bei der Paketweiterleitung die Pakete markieren. Diese Markierungsinformationen identifizieren den Router, der das Paket weiterleitet, eindeutig. Der Angegriffene kann diese dann verwenden, um die wahre Angriffsquelle zu finden. [29]

2.3.3 Ransomware

Die dritte Angriffsart ist Ransomware, die eine Art von Malware ist. Bei Ransomware handelt es sich um eine Methode zur Erpressung von Geld durch den Angreifer. Dabei werden die Benutzerdaten des Betroffenen verschlüsselt und ein Lösegeld vom Angreifer verlangt, welches oft als elektronische Währung verlangt wird, zum Bespiel als Bitcoin. Ransomware kann wie in [40] beschrieben als Malware, die den Zugriff von Benutzern auf das System verhindert oder einschränkt, entweder durch das Sperren des Systembildschirms oder der Benutzerdaten, bezeichnet werden. [1][38][40]

Es gibt verschieden Typen von Ransomware wie z.B. CryptoLocker oder WannaCry. Beim CryptoLocker handelt es sich um eine Datenverschlüsselungs-Ransomware, die mit Hilfe des RSA 2048 Schlüssels die privaten Datensätze verschlüsselt. Anschließend wird ein Hinweis angezeigt, der den Benutzer auffordert, ein Lösegeld zu zahlen, damit seine Daten entschlüsselt werden. WannaCry ist eines der neuesten Ransomware, die im Mai 2017 ausgeführt wurde. Diese richtet sich hauptsächlich gegen Windows Betriebssysteme. [1]

Um sich einen Überblick über das Ausmaß von WannaCry zu verschaffen und die Ziele in Europa zu berücksichtigen, kann die nachfolgende Grafik (Figure 9) betrachtet werden: [11]

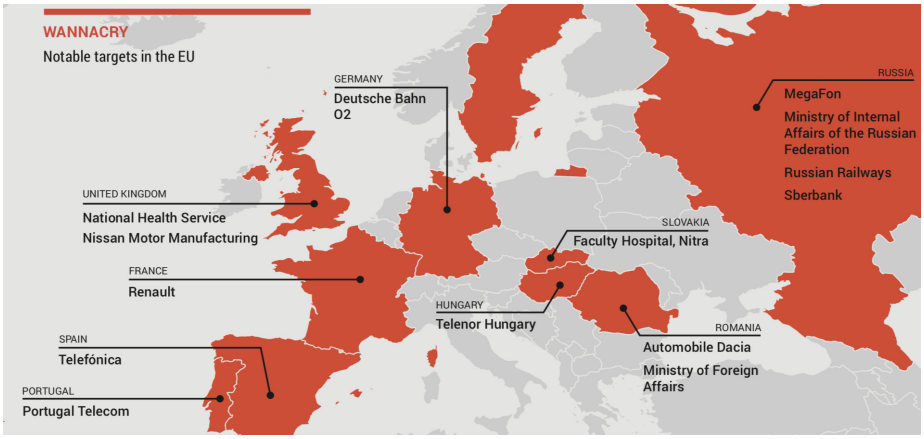

Figure 9: WannaCry [11]

Die Funktionsweise einer Ransomware kann in folgenden Schritten zusammengefasst werden: [1]

1. Der Benutzer erhält eine E-Mail mit einem Link, der von einem legitimen Absender gesendet wurde, wie z.B. vom Chef.
2. Der Benutzer wird zu dem Link einer Webseite geleitet, der authentisch erscheint.
3. Wenn die Website geladen ist, nutzt der Server das Kit, das mit dem Zielsystem interagiert.
4. Das Kit versucht die Sicherheitsanfälligkeit auszunutzen.
5. Alle Prozesse, einschließlich der Sicherheitskopie, werden multipliziert.
6. Es wird eine PowerShell verwendet, um die Kopien von sich selbst im Dateisystem zu verbreiten.
7. Die powershell.exe generiert drei Kopien von der ursprünglichen Malware-Binärdatei, zuerst im AppData-Verzeichnis, dann im Startverzeichnis und schließlich im C-Verzeichnis.
8. Wenn die Daten des Betroffenen komplett verschlüsselt sind, leitet die Malware den verschlüsselten Schlüssel an den Steuerungsserver weiter.
9. Der Server leitet dann die Nachricht an das Ziel weiter, dass ein Lösegeld zu bezahlen ist.

Zusätzlich noch ein zusammengefasster Ablauf (Figure 10) einer Ransomware Attacke grafisch dargestellt: [37]

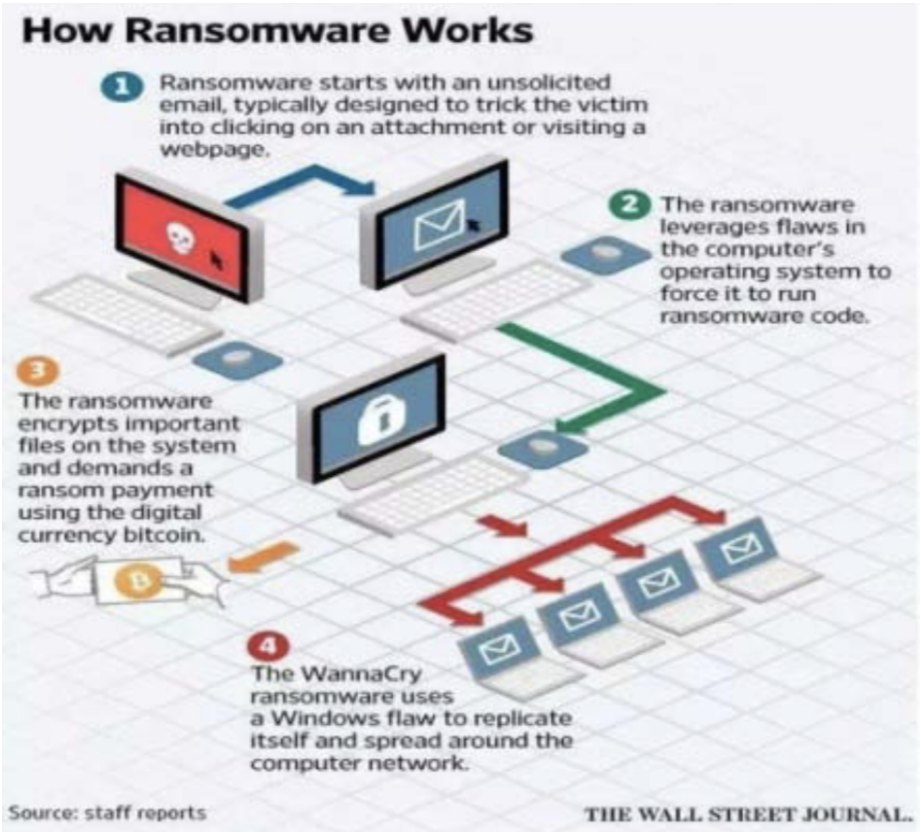

Figure 10: Ransomware [37]

Es gibt einige Präventionsmaßnahmen, die hilfreich gegen Ransomware-Attacken sein können. In [1] wird folgendes empfohlen:

- Spam-Filter, um verdächtige E-Mails zu erkennen
- Verwenden eines Exploit-Ausführungsschutzmoduls
- Wenn der Angriff vor der Verschlüsselung gestoppt wird, hat der Benutzer die Möglichkeit einen Dateiverschlüsselungsschlüssel in einem Dateisystem oder Speicher abzulegen
- Um Ransomware zu blockieren, wenn dieser mit der Verschlüsselung beginnt, wird empfohlen zusätzliche Vertrauensgrenzen im Betriebssystem zu definieren, die Krypto-Schließfächer beim Zugriff auf freigegebene Ordner und Netzlaufwerke zu blockieren

Weiters gibt es auch einige Empfehlungen zur Minimierung der Auswirkungen von Ransomware: [1]

- Entwicklung und Ausführung eines Plans für ein Endbenutzer-Bewusstseinsprogramm
- Überprüfung der Server-Sicherungsprozesse
- Überprüfung der Netzwerklaufwerksberechtigungen, um die Auswirkungen eines einzelnen Benutzers auf die Endbenutzerprivilegien zu minimieren
- Dokumentation des Vorfallreaktionsplans für Ransomware

2.4 Ergebnisse der Literaturanalyse

Wie im vorigen Kapitel erwähnt wurden in der Literarturanalyse drei Teilbereiche näher analysiert. Da es bei der Masterarbeit um die Unterstützung der Reaktion auf Sicherheitsvorfälle geht, ist Incident Response Management ein wichtiges Thema, das aus folgenden Schritten besteht: [30][35]

- Im ersten Schritt wird versucht, den Sicherheitsvorfall zu erkennen.
- Im zweiten Schritt wird versucht, den Sicherheitsvorfall anzuhalten oder abzuschwächen.
- Im nächsten Schritt folgt die Wiederherstellungsphase.
- Im letzten Schritt eine Post-Incident Analyse, um die Infrastruktur und die Prozesse zu verbessern.

Dafür wird ein Vorfallreaktionsplan, auch Incident Response Plan-IRP genannt, empfohlen, wo schriftliche Anweisungen gesammelt sind. Dieses Dokument hilft bei der Identifikation von Sicherheitsvorfällen und anschließend bei der Reaktion, um die Auswirkungen des Sicherheitsvorfalls zu schwächen. Laut SANS beinhaltet dieser Plan eine: [30][35][45]

- Vorbereitung
- Identifikation
- Eindämmung
- Ausmerzung
- Wiederherstellung
- Erkenntnis

Vergleicht man die Phasen, die vom SANS Institute [30] vorgeschlagen wurden mit der "Reaction" (Respond) Funktion oder Phase, die im Framework Core vom NIST Cybersecurity Framework [42], das dem Unternehmen hilft, ihre Sicherheitsmaßnahmen zu verbessern, zur Verfügung stehen, sieht man zwar Unterschiede in der Anzahl der Schritte, jedoch wird praktisch dasselbe angeboten. Die Response Planung und Analyse kann mit der Vorbereitungs- und Identifikationsphase des SANS Institute [30] gleichgestellt werden. Weiters kann die Schadensmilderung (Mitigation) mit der Eindämmungs- und Ausmerzungsphase gleichgesetzt werden. Zusätzlich wird die Wiederherstellungsphase beim SANS Institute [30] vorgeschlagen, die als vorletzte Funktion beim NIST CSF [42] empfohlen wird. Des Weiteren gibt es den Lerneffekt, der als Erkenntnisphase bezeichnet wird. Somit kann festgestellt werden, dass beim Vorfallreaktionsplan die letzten zwei Funktionen des NIST CSF [42] als eines gesehen werden. [35][41][42][45]

Wie im vorigen Kapitel besprochen, besteht die Reaktionsphase aus mehreren Schritten: [6][8][14][18][20][41][42]

- Response Planung: Zuerst sollte der Sicherheitsvorfall identifiziert werden. Um eine rasche Bearbeitung zu ermöglichen, sollte vorher ein Plan festgelegt werden, wo die Vorgehensweise, verantwortliche Personen und die Reihenfolge der Schadensbearbeitung beschrieben ist.

- Analyse: Für die Erstanalyse und in weiterer Folge die genauere Analyse empfiehlt sich eine forensische Analyse. Dabei ist es sinnvoll, eine Vorgehensweise im Expertenteam festzulegen. Zusätzlich sollten nach der Erstanalyse die Auswirkungen eingeschätzt und eine Priorität vergeben werden. Des Weiteren sollte eine Dokumentation zu den gesammelten Spuren durchgeführt werden. Diese Analyse soll helfen, die Schwachstellen zu identifizieren, die Schadenshöhe zu ermitteln oder den Angreifer herauszufinden. Notwendig ist auch das Informieren der betroffenen internen und externen Stellen, sowie der Öffentlichkeit und Sicherheitsgemeinde.

- Schadensmilderung: Hier geht es grundsätzlich um die Minderung des Schadens, damit dieser so gering wie möglich bleibt. Dabei sollte eine Dokumentation durchgeführt werden. Diese kann helfen, einen Überblick über Ursachen, Folgen und Maßnahmen zu erhalten, ein Problem ersichtlich zu machen und bei zukünftigen ähnlichen Problemen die Bearbeitungszeit zu verringern.

- Wiederherstellung: Bei der Wiederherstellung ist zu beachten, dass alle Daten von schreibgeschützten Datenträgern wiederhergestellt werden. Auch das Ändern aller Passwörter ist ein wichtiger Aspekt. Nach der Wiederherstellung sollte geprüft werden, ob alles ordnungsgemäß funktioniert.

- Lerneffekt: Hier soll etwas über den Sicherheitsvorfall gelernt werden. Es wird unter anderem die Reaktionszeit, Eskalationsstrategie, Unter-

suchungseffektivität, Motivation des Täters oder auch die Handlungsanweisungsentwicklung betrachtet.

Wie im vorigen Kapitel herausgefunden, gibt es mehrere Ansätze, die die Reaktionsphase unterstützen soll. Einer der Ansätze beschreibt eine forensische Methode, die bei der Analyse der Beweisspuren und im Nachhinein bei der Rekonstruktion des Angriffsweges helfen soll. Dafür wird CenterTrack und PyFlag vorgeschlagen. Eine andere Möglichkeit wäre, das Einsetzen eines Security Coordination Models, bei dem es eine Teilnehmerorganisation (PO), eine Koordinationsorganisation (CO) und externe Organisationen gibt. Zusätzlich wird hier noch ein Überwachungssystem, ein Reaktionssystem und ein forensisches System verwendet. Eine andere Option wäre ein Response Strategy Model (RSM), bei dem eine Beziehung zwischen Vorfällen und den Reaktionsoptionen mit verschiedenen Prioritätsstufen geschaffen wird. Das Ganze wird in einer Tabelle dargestellt, die aus einer Kombination von Risiko Response Planung, den Quadranten Q1-Q4 und den Reaktionsoptionen besteht. Weitere drei Ansätze wären: IRSS, das sich mit der Reaktion und der automatischen Response Plan Erstellung beschäftigt, Decision Support System, das auf Case-based reasoning und Ontologie basiert und ein Modell, das Künstliche Intelligenz verwendet und das Wissen aus früheren Studien angemessen nutzen kann. Ein weiterer Ansatz beschäftigt sich mit der Erfassung und Verarbeitung von Eingabedaten, der Quantifizierung von Modellparametern, der Sicherheitsbewertung und der Auswahl der Gegenmaßnahmen auf der Grundlage der Menge von Sicherheitsmetriken. Es sind auch noch vier Response Selection Modelle bekannt. Das IE-IRS Modell wählt verschiedene Firewall-Konfiguration als Reaktion auf einen bestimmten Angriff. Das CS-IRS hingegen geht davon aus, dass es Reaktionsmaßnahmen mit positiven und negativen Auswirkungen gibt. Dabei wird bei einer erfolgreichen Reaktion der Erfolgsfaktor um 1 erhöht, ansonsten der Ausfallfaktor um 1 erhöht. Beim TVA handelt es sich um einen Modellierungs- und Simulationsansatz. Die Informationen über die Schwachstellen werden sowohl aus internen als auch externen Quellen und Netzwerkkonfigurationen gesammelt. Schlussendlich gibt es noch das REASSESS Modell, das eine Kombination aus IE-IRS und CS-IRS ist. [3][10][22][26][31][43]

Der dritte Teil der Literaturanalyse konzentriert sich auf die drei Angriffsarten APT, DDoS und Ransomware. Wie im vorigen Kapitel dargestellt, versteht man unter APT (Advanced Persistent Threat) einen fortgeschrittenen Cyberangriff, der sich auf bestimmte Ziele über einen längeren Zeitraum konzentriert. Das Hauptziel dabei ist das Ausspionieren von sensiblen Daten oder entsprechende Schäden zu verursachen. Eines der Merkmale einer APT-Attacke ist das Verwenden von mehreren Phasen, die Erkundung, Halt aufbauen, Seitliche Fortbewegung, Exfiltration und Vertuschung genannt werden. Bei einem Distributed Denial of Service (DDoS) Angriff versucht der Angreifer das Server-Netzwerk des Ziels zu überlasten, indem dieser eine große Menge Datenverkehr sendet. Folglich kann der Server keine Dienste mehr für die Benutzer zur Verfügung stellen. Genauer beschrieben, werden die Pakete an den Master geschickt, der

diese dann an die Slaves weiterschickt. Danach wird der Verkehr in Richtung der Zielmaschine erhöht. Ransomware hingegen ist eine Art von Malware, in der versucht wird, Geld vom Betroffenen zu erpressen. Meistens werden dabei die Daten des Angegriffenen verschlüsselt und ein Lösegeld gefordert, damit die Daten wieder entschlüsselt werden. Ein Beispielablauf dieser Attacke besteht aus 9 Schritten, die im Unterkapitel "Ransomware" genauer beschrieben wurden. [1][2][7][29][38][40][44]

2.5 Verwendung der Ergebnisse als Basis für die Masterarbeit

Für die Masterarbeit sind auf der einen Seite die Ergebnisse des Incident Response Managements und der "Reaction" (Respond) Phase des NIST Cybersecurity Framework [42] bedeutsam. Da das Hauptaugenmerk auf der Unterstützung der Reaktionsphase im NIST CSF [42] bei Sicherheitsvorfällen liegt, kann es hier hilfreich sein, die einzelnen Schritte bei einem Incident Response Management und den Vorfallreaktionsplan (Incident Response Plan-IRP) zu beachten. Zusätzlich ist es essenziell, die "Reaction" (Respond) Phase im NIST CSF [42] zu berücksichtigen, die aus weniger Schritten besteht als der vorgeschlagene Vorfallreaktionsplan vom SANS Institute [30]. Im Endeffekt können die Respond Funktion und der Vorfallreaktionsplan gleichgesetzt werden. Dafür können die Ergebnisse des genau beschriebenen Ablaufs hilfreich sein. Weiters sind die Ergebnisse der bereits bestehenden Ansätze bedeutend, vor allem beim Definieren der Anforderungen und beim Erstellen des Modells für die Masterarbeit. Auf der anderen Seite wird es unerlässlich sein, die Eigenschaften beziehungsweise Vorgehensweise der drei gewählten Angriffsarten APT, DDoS und Ransomware zu kennen. Dies wird vor allem bei der Ausarbeitung der Reaktion auf die drei Angriffstypen notwendig sein.

2.6 Conclusio

Die Literaturanalyse konzentriert sich auf drei Themenbereiche: Incident Response Management inklusive Reaktionsphase im NIST Cybersecurity Framework [42], bereits vorhandene Ansätze für die Unterstützung der Reaktionsphase und auf drei Angriffsarten (APT, DDoS, Ransomware). Die Reaktionsphase besteht aus mehreren Schritten, die sowohl im Vorfallreaktionsplan des SANS Institute [30] als auch in der "Reaction" (Respond) Phase des NIST CSF [42] beschrieben sind. Bei der Reaktion auf einen Sicherheitsvorfall ist es wichtig, nachdem der Vorfall bestätigt wurde, eine Analyse, wo die digitalen Beweisspuren sichergestellt werden, durchzuführen. Im Nachhinein wird der entstandene Schaden minimiert und die Wiederherstellung des Betriebes durchgeführt. Abschließend kann aus jedem Sicherheitsvorfall etwas Neues gelernt werden und vorherige Fehler beziehungsweise Probleme können zukünftig vermieden werden. Allgemein sollte ein Unternehmen im Vorhinein darauf vorbereitet sein, dass ein Sicherheitsvorfall jederzeit eintreffen kann. Daher ist es wichtig, Reaktionen auf Sicherheitsvorfälle, wie APT, DDoS und Ransomware,

vorher einzuplanen und zu testen, um somit die Reaktionszeit zu verbessern und den Schaden so gering wie möglich zu halten.

3 Beschreibung der Aufgabenstellung

In diesem Kapitel wird auf den Hintergrund und die Motivation näher eingegangen. Anschließend werden die Vorgehensweise und der methodische Ansatz für das Schaffen einer Lösung genauer beschrieben.

3.1 Hintergrund & Motivation

In letzter Zeit häufen sich Sicherheitsvorfälle. Das kann eine aktive Bedrohung, ein versuchter Angriff oder ein erfolgreicher Verlust von Daten sein. Es kann beobachtet werden, dass immer öfter namhafte Unternehmen betroffen sind. Der Grund für die zunehmende Anzahl von Cyber-Angriffen kann unterschiedlich sein, jedoch kann man davon ausgehen, dass die Attacken effektiv sein können und die Verfolgung und Identifizierung des Täters schwierig ist. Durch den Einsatz von kontinuierlich verbesserten Techniken und Werkzeugen, die für die Angreifer problemlos zugänglich sind, ist es einfach einen erfolgreichen Angriff durchzuführen. Es kann festgestellt werden, dass die Durchführung von Cyber-Attacken auf ein Unternehmen nicht zufällig geschieht, sondern diese auf ein, vorher eingeplantes, Ziel gerichtet werden. Immer wieder gibt es Versuche, die Bundesverwaltung oder Finanzinstitute anzugreifen. Solch gelungene Attacken können bei Unternehmen zu fatalen Folgen führen, da damit gerechnet werden kann, dass sensible Daten gestohlen werden können. Diese Auswirkungen können sowohl für das betroffene Unternehmen als auch für die Verbraucher inakzeptabel sein und enormen Schaden herbeiführen. Somit sollte sich ein Unternehmen folgende Ziele setzen:

- Informationssicherheit schaffen
- frühes Erkennen von Bedrohungen
- Schadensminimierung
- gute Risikobewertung der Informationen

Deshalb empfiehlt es sich für Unternehmen, sich mit der Prävention von Sicherheitsvorfällen, der frühzeitigen Erkennung und der Reaktion auf Vorfälle zu beschäftigen. Je früher eine entsprechende Reaktion auf angewendete Angriffsmethoden, wie z.B. APT, DDoS und Ransomware erfolgt, desto höhere Chancen bestehen, den Schaden gering zu halten und die Reaktionszeit zu minimieren. Aus diesem Grund scheint es für ein Unternehmen sinnvoll zu sein, nicht erst nach einem bereits vorhandenen Angriff ohne Vorbereitung zu reagieren, sondern vorher einzuplanen, wie man bei bestimmten Attacken reagiert und wer die zuständigen Personen für die jeweiligen Aufgaben sind. Hierfür bietet sich eine schriftliche Dokumentation an, die im Nachhinein helfen kann, die durchgeführten

Schritte auszuwerten und den zukünftigen Umgang mit Sicherheitsvorfällen zu verbessern. Zusätzlich kann aus jedem Sicherheitsvorfall etwas Neues gelernt und die vorher definierte Vorgehensweise aktualisiert werden.

3.2 Vorgehensweise und methodischer Ansatz

Der methodische Ansatz zur Unterstützung der Reaktionsphase baut auf den entsprechenden Anforderungen zur Behandlung von Sicherheitsvorfällen im NIST CSF [42] auf. Als Ausgangspunkt dafür soll die, im Kapitel 2 "State of the Art in Literatur und Praxis" ausgearbeitete, Literaturanalyse dienen. Diese beschäftigt sich unter anderem mit dem Incident Response Management, mit den bereits verfügbaren Ansätzen für die Unterstützung der Reaktionsphase und den drei gewählten Angriffsarten. Anschließend wird eine Methode entwickelt, die die Reaktionsphase und die einzelnen vorkommenden Schritte, unterstützen soll. Dabei ist es grundlegend zu erwähnen, dass die komplette Phase der Reaktion auf Sicherheitsvorfälle verstärkt werden soll und nicht die einzelnen Teile davon betroffen sind. Zusätzlich ist zu beachten, dass eine Reaktion auf folgende drei Angriffsarten ausgearbeitet werden soll:

- APT
- DDoS
- Ransomware

Als Grundlage dafür wird die ausgearbeitete Literatur der drei Cyber-Angriffe herangezogen, wobei unter anderem die Vorgehensweise und die Eigenschaften ausgeforscht wurden. Es ist nötig, den kompletten Ablauf beziehungsweise die ausgearbeitete Methode zu testen. Um dies zu untersuchen, wird eine Case Study verwendet, die es ermöglicht, alles zu kontrollieren. Die daraus resultierenden Ergebnisse werden diskutiert.

Der Fokus der Modellerstellung liegt auf der Unterstützung der Reaktionsphase. Im ersten Schritt sollen die Anforderungen definiert werden, gefolgt von einem Modell und einer entsprechenden Methode, um die einzelnen Schritte zu fördern. Der Vorteil der Unternehmen liegt dabei, den Schaden und die Reaktionszeit reduzieren zu können.

4 Anforderungen an das zu entwickelnde System

Um eine nützliche Methode für die Unterstützung der Reaktionsphase im NIST CSF [42] bei Sicherheitsvorfällen zu entwickeln, sollten zuerst Anforderungen festgelegt werden, um Klarheit über die zu erledigenden Aufgaben zu schaffen. Daher beschäftigt sich dieses Kapitel mit der Diskussion und der Definition der Anforderungen. Auf der einen Seite wird auf die Anforderungen der Reaktionsphase, genauer gesagt auf die einzelnen Schritte und auf der anderen Seite auf die Anforderungen bezüglich der adressierten Angriffsarten eingegangen.

4.1 Anforderungen für die Unterstützung der Reaktionsphase

Zuerst werden die Anforderungen der einzelnen Schritte der Reaktionsphase im NIST CSF [42] beleuchtet. Hierbei unterscheidet man zwischen fünf Phasen. Diese werden als Response Planung, Analyse, Schadensmilderung, Wiederherstellung und Lerneffekt bezeichnet.

Beginnend mit der ersten Phase Response Planung werden folgende Anforderungen definiert:

- Es soll ein Plan mit einer definierten Vorgehensweise für die gewählten Angriffsarten erstellt werden, damit eine gewisse Vorbereitung besteht und eine raschere, effizientere Bearbeitung ermöglicht wird. Dies soll unter anderem die Reaktionszeit minimieren, was in der Folge zu einer Schadensbegrenzung führen kann.
- Es sollen die verantwortlichen Personen bestimmt werden, die für die Bearbeitung des jeweiligen Sicherheitsvorfalls zuständig sind. Dabei muss genau festgelegt werden, wer für welche Aufgaben bei der Behandlung des Vorfalls zuständig ist.
- Es soll die Reihenfolge der verschiedenen Schritte festgelegt werden, damit beim Eintreffen eines Sicherheitsvorfalls klar ist, welche Schritte wann und durch wen durchzuführen sind.

Der allgemeine Reaktionsplan für einen APT-Angriff soll folgende Schritte einbeziehen: [15][16]

1. Es soll das Reaktionsteam, das aus IT-Sicherheitsmitarbeitern, Sicherheitsmanager und Security Analyst besteht, einberufen werden. Bei der Sitzung sollen die durchzuführenden Maßnahmen besprochen und die eingeteilten Personen zugewiesen werden.
2. Anfangs muss eine Erstbegutachtung durchgeführt werden, um herauszufinden, welche Systeme betroffen sind, ob es eine Beteiligung einer Malware gibt, ob der Angreifer noch aktiv ist und über welche Zugriffe dieser

verfügt. Zusätzlich sollte geprüft werden, welche Monitoring-Tools eingesetzt werden und es soll entschieden werden, ob neue eingesetzt werden.

3. Ein Anwalt und eine Anzeige bei der Polizei sollten in Betracht gezogen werden.
4. Die Personen, die sich mit der Presse beschäftigen, sollten Informationen über den Sicherheitsvorfall vorbereiten, falls eine Stellungnahme veröffentlicht werden soll.
5. Weiters sollten die internen und externen Partner informiert und weitere Maßnahmen abgestimmt werden.
6. Der APT-Angriff muss dem Computer-Notfallteam (wie z.B. CERT.at) mitgeteilt werden.
7. Mit Hilfe des Analyseplans sollen die Beweisspuren festgehalten werden.
8. Eine Schadensmilderung soll durchgeführt und die Schritte dokumentiert werden.
9. Im nächsten Schritt kann mit der Wiederherstellung des Systems begonnen werden. Zunächst muss eine Neuinstallation des infizierten Systems durchgeführt werden und anschließend kann die Wiederherstellung der Daten erfolgen.
10. Abschließend soll ein Fragebogen über den Sicherheitsvorfall ausgefüllt werden, um zu prüfen, ob Aktualisierungen an der Reaktionsphase notwendig sind.

Der allgemeine Reaktionsplan für einen DDoS-Angriff wird folgende Schritte beinhalten: [16]

1. Es muss das zugewiesene Reaktionsteam gebildet werden, bestehend aus IT-Sicherheitsmitarbeitern, Sicherheitsmanager, Security Analyst und Personen, die für Presse und Öffentlichkeit zuständig sind. Hier sollen die Maßnahmen besprochen und die verantwortlichen Personen zugewiesen werden.
2. Der Vorfall muss dem Management bekannt gegeben werden.
3. Es sollte der Internet-Service-Provider frühzeitig eingebunden werden.
4. Ein Anwalt sollte kontaktiert und eine Anzeige bei der Polizei eingereicht werden.
5. Die zuständigen Personen für Presse und Öffentlichkeit müssen eine Auskunft zur Verfügung stellen, damit auf Anfragen geantwortet werden kann.
6. Weiters sollten die Kunden und Partner informiert werden.

7. Der DDoS-Angriff muss dem zuständigen Computer-Notfallteam gemeldet werden. Die kann in Österreich das CERT.at sein.

8. Basierend auf dem Analyseplan, sollen die Beweisspuren gesammelt und dokumentiert werden.

9. Es soll der Schaden gemildert und die durchgeführten Schritte dokumentiert werden.

10. Weiters soll das komplette System wiederhergestellt werden. Beginnend mit der neuen Installation des infizierten Systems, abschließend mit der Wiederherstellung der Daten aus vertrauenswürdigen Datenträgern.

11. Zum Schluss soll ein Fragebogen, der sich auf die Bearbeitung des Sicherheitsvorfalls bezieht, ausgefüllt werden. Dabei soll unter anderem festgestellt werden, ob eine Aktualisierung des Ablaufs der Reaktionsphase überarbeitet werden muss.

Der allgemeine Reaktionsplan für einen Ransomware-Angriff beinhaltet folgende Schritte: [16][17]

1. Es sollte auf keinen Fall das Lösegeld bezahlt werden. Stattdessen muss das Reaktionsteam berufen werden, das aus IT-Sicherheitsmitarbeitern, Sicherheitsmanager und Security Analyst besteht. Dabei sollten alle weiteren Maßnahmen besprochen werden.

2. Zunächst ist es wichtig, eine Strafanzeige bei der Polizei zu erstatten, damit eine genauere Untersuchung durchgeführt werden kann.

3. Um den Schaden gering zu halten, sollten infizierte Systeme rasch vom Netz getrennt werden, indem die Netzwerkkabel von den Computern gezogen werden, beziehungsweise der WLAN Adapter ausgeschaltet wird. Zur Sicherheit können alle Geräte vom Netzwerk getrennt werden, da die Gefahr besteht, dass anfangs nicht alle infizierten Systeme bereits erkannt wurden.

4. Es sollten die Logdaten geprüft werden, in denen die Zugriffe auf Netzlaufwerke erkannt werden können. Auch die Metadaten, an denen ersichtlich ist, welche Nutzer welche Daten erstellt haben, können ein infiziertes System andeuten.

5. Um Presseanfragen zu beantworten, sollten gewisse Informationen zum Sicherheitsvorfall zur Verfügung gestellt werden.

6. Der Ransomware-Angriff muss beim zuständigen Notfallteam, welches in Österreich z.B. CERT.at sein kann, gemeldet werden.

7. Anhand des Analyseplans sollen die Beweisspuren gesammelt und dokumentiert werden.

8. Eine Schadensmilderung soll durchgeführt und anschließend dokumentiert werden.

9. Der nächste Schritt ist die Durchführung der Wiederherstellung des Systems. Zuerst sollte eine Neuinstallation des infizierten Systems durchgeführt werden und daraufhin eine Wiederherstellung der vorher gesicherten Daten erfolgen.

10. Abschließend soll ein Fragebogen ausgefüllt werden, damit ausgewertet werden kann, ob eine Aktualisierung der, zu dieser Zeit angewendeten, Schritte notwendig ist.

Im Bereich der Analyse, genauer gesagt bei der forensischen Analyse, sind folgende Anforderungen von Bedeutung:

- Der Benutzer soll bei der Erstanalyse unterstützt werden, indem eine Beraterfunktion mit den, zu überprüfenden, Schritten und den Stellen, die genauer zu betrachten sind, angeboten wird. Folglich soll es möglich sein, den Verdacht eines Angriffs auszuschließen oder zu bestätigen. Bei einer Bestätigung soll die Phase des Angriffs eingeschätzt werden.

- Es soll möglich sein, die Auswirkungen des Angriffs zu bewerten. Dazu soll der Benutzer in der Lage sein, die funktionale Auswirkung, die Informationsauswirkung, die Wiederherstellbarkeit einzuschätzen und anhand dieser eine Priorisierung durchzuführen.

- Weiters soll der Benutzer bei der genaueren Analyse mit Hilfe einer Beraterfunktion, in der die, zu untersuchenden Punkte vorgeschlagen werden, unterstützt werden. Zusätzlich soll eine allgemeine Vorgehensweise für die Angriffsarten APT, DDoS, Ransomware spezifiziert werden, sodass die Analyse der digitalen Spuren effizient und genau durchgeführt werden kann.

- Es soll eine Dokumentation durchgeführt werden, indem die einzelnen digitalen Spuren, die bei der Erstanalyse und Analyse identifiziert wurden, festgehalten werden. Solch eine Dokumentation kann bei juristischen Verfahren als Beweis dienen. Zusätzlich soll vorgeschlagen werden, welche Punkte zu dokumentieren sind und in welcher Form die Dokumentation durchgeführt werden sollte. Abschließend soll die durchgeführte Dokumentation als pdf-Datei generiert werden.

- Je nach Sicherheitsvorfall sollen die betroffenen internen, externen Stellen als auch Öffentlichkeit und Sicherheitsgemeinde informiert werden. Dabei soll beachtet werden, wer und in welcher Genauigkeit benachrichtigt wird.

Für die allgemeine Vorgehensweise bei einem APT-Angriff werden folgende Schritte für die Analyse angeboten: [15]

1. Die Analyse eines APT-Angriffs hat drei Aspekte. Es kann damit begonnen werden, dass die Malware, die das System befallen hat, in einer gesicherten Umgebung analysiert wird. Dadurch sollte bestimmt werden, wie hoch der Schadensgrad ist, welche Systeme/Komponenten betroffen sind, welche Indikatoren es gibt und woher die Malware stammt. Bestenfalls kann auch die Herkunft des Angriffs bestimmt werden.

2. Anschließend können die Systeme, die vom Sicherheitsvorfall betroffen sind, durch das Einsetzen von Host-Forensik untersucht werden.

3. Um Daten, die im Nachhinein analysiert werden können, zu bekommen, müssen IT-forensische Abbilder des Hauptspeichers, der Festplatten und anderer Speichermedien gemacht werden. Es sollten alle Datenträger, vollständige Systeme, Protokolldaten und Datensicherungen sichergestellt werden.

4. Wenn die Entschlossenheit besteht, ein Gerichtverfahren einzuleiten, dann müssen bei der Datenerfassung Maßnahmen getroffen werden. Dabei ist die Durchführung einer ausführlichen Dokumentation nicht zu vergessen.

5. Grundsätzlich sollten folgende Fragen beantwortet worden sein:

   - Wie schaut der Weg der Infektion aus?
   - Welche Systeme und Nutzerkonten sind vom Sicherheitsvorfall betroffen?
   - Welches Muster wurde bei der Vorgehensweise angewendet?
   - Wie schaut der Datenfluss aus?
   - Welche Nachweise gibt es für die Herkunft des Angriffs?

6. Die nächste Möglichkeit wäre das Beobachten des Netzwerkverkehrs. Für die Netzwerkforensik können Protokollierungssystem, Beobachtungssysteme und Netzwerkprotokolldaten hilfreich sein.

7. Es können dieselben Fragen wie bei der Host-Forensik beantwortet werden. Zusätzlich besteht die Möglichkeit, zwei weitere Fragestellungen zu formulieren:

   - Wie schaut die aktuelle Vorgehensweise des Angreifers aus?
   - Welche Spuren wurden nach einem erneut durchgeführten Angriff, beim Verwenden der ersten definierten Maßnahmen, hinterlassen?

Bei der allgemeinen Analyse eines DDoS-Angriffs empfiehlt es sich, solchermaßen vorzugehen: [16][19]

1. Es sollte damit begonnen werden, eine 1:1 Kopie beziehungsweise ein forensisches Abbild des, zu dieser Zeit eingesetzten Systems zu generieren, damit in Ruhe alle Beweisspuren gesammelt werden können.

2. Anschließend kann mit der Analyse des Netzwerkverkehrs gestartet werden. Diese kann dabei helfen die Angriffsmethode zu bestimmen um entsprechend dazu die Gegenmaßnahmen definieren zu können.

3. Im nächsten Schritt kann mit der Aufzeichnung der IP-Adresse begonnen werden. Dabei sollten folgende Adressen dem zuständigen Provider übermittelt werden:

   - IP-Adresse des Angreifenden
   - Zeitstempel und Zeitzone
   - IP-Adresse des Geschädigten

4. Der Provider sollte kontaktiert werden und die Informationen sollten übermittelt werden. Zu beachten ist dabei, dass dies nicht hinausgezögert werden sollte, da die Provider Logdaten der letzten 7 Tage zur Verfügung haben.

Die allgemeine Vorgehensweise für die Analyse der digitalen Spuren eines Ransomware-Angriffs wird folgendermaßen aussehen: [19]

1. Damit eine möglichst genaue Analyse durchgeführt werden kann, muss im ersten Schritt ein forensisches Abbild, genauer gesagt eine 1:1 Kopie des aktuellen Systems geschaffen werden. Diese Aktion ermöglicht das Sichern der Beweisspuren.

2. Zunächst kann das System ausgeschaltet werden. Dabei sollte dieses nicht heruntergefahren werden, da dadurch Daten überschrieben werden können. Daher ist das Ziehen des Stromsteckers die optimalste Variante.

3. Nachdem alles gesichert wurde, kann mit der Analyse gestartet werden. Eines der wichtigsten Aufgaben ist das Auswerten der Logdaten, die beim Identifizieren der betroffenen Systeme und beim Schätzen des Ausmaßes helfen können. Daher ist es wichtig, regelmäßig Logs zu erzeugen und zu speichern.

4. Der Security Analyst sollte sich folgende Logs genauer anschauen:

   - HTTP-Proxy Logs, um den HTTP-Datenverkehr zurückverfolgen zu können
   - E-Mail Server Logs
   - Logs der Firewall
   - Logs der Active-Directory, um verdächtige Zugriffe zu erkennen

5. Um den aktuellen Angriff zu analysieren, empfiehlt sich das Full-Packet-Capturing. Dies ermöglicht das Analysieren von Inhalten, sodass z.B. Befehle, die vom Angreifer durchgeführt wurden, nachvollziehbar sind. Zu beachten ist, dass ein Datenschutzbeauftragter eingebunden werden sollte.

6. Es empfiehlt sich das Einsetzen von Tools wie z.B. TCPDump oder Wireshark, die beim Aufzeichnen und Auswerten hilfreich sein können.

Beim nächsten Schritt der Schadensmilderung, wo versucht wird, den Schaden so gering wie möglich zu halten, ist es bedeutsam, folgende Punkte zu beachten:

- Der Benutzer soll bei der Durchführung der Schadensmilderung unterstützt werden, indem eine Beraterfunktion mit den durchzuführenden Schritten, die den Schaden abschwächen können, angeboten wird.
- Es soll eine Dokumentation durchgeführt werden, bei der die einzelnen Schritte, die bei der Milderung des Schadens ausgeführt wurden, festgehalten werden. Anschließend soll eine pdf-Datei generiert werden.
- Es soll ein Überblick über die Ursachen, Folgen und Maßnahmen geschaffen werden, die bei der zukünftigen Bearbeitung hilfreich sind und die Bearbeitungszeit verringern können.

In der nächsten Phase geht es um die Wiederherstellung des regulären Betriebes. Dafür werden folgende Anforderungen gesetzt:

- Es sollen in regelmäßigen festgelegten Abständen Backups durchgeführt werden.
- Der Benutzer soll in der Lage sein, sich die, zuletzt durchgeführten, Backups einzublenden und anhand dieser herauszufinden, welcher als sicher eingestuft werden können.
- Die Daten sollen aus schreibgeschützten Datenträgern wiederhergestellt und alle Passwörter geändert werden, nicht nur die, die vom Sicherheitsvorfall betroffen sind.
- Es sollen Überwachungswerkzeuge, die eine Logfileanalyse durchführen, eingesetzt werden.
- Schließlich soll es möglich sein, die Wiederherstellungsschritte zu dokumentieren. Zusätzlich soll die durchgeführte Dokumentation als pdf-Datei generiert werden.

Ein Wiederherstellungsplan könnte folgende Punkte beinhalten: [15][17][19]

1. Nachdem alle infizierten Systeme forensisch gesichert wurden, kann mit der Neuinstallation begonnen werden. Zu beachten ist, dass das verwendete System aus einem glaubwürdigen Datenträger hereingespielt wird.
2. Nicht zu vergessen ist, dass nach dem Aufsetzen das System aktualisiert und bei Bedarf gehärtet werden sollte, da erneute Angriffe gestartet werden können.
3. Anschließend kann mit der Wiederherstellung der Systeme begonnen werden. Dabei können Backups für die Wiedereinspielung der Daten verwendet werden.

4. Abschließend sollten alle Passwörter geändert werden.

Im letzten Schritt geht es um den Lerneffekt, das heißt, man dokumentiert, was aus jedem Sicherheitsvorfall gelernt werden kann. Dafür werden folgende Anforderungen berücksichtigt:

- Der Benutzer soll bei der Auswertung mit Hilfe der vorher erstellten Dokumentation der Erstanalyse, Analyse, Schadensmilderung und Wiederherstellung unterstützt werden.
- Die Auswertung soll sowohl auf zeitlichen Faktoren, die für die Bearbeitung des Vorfalls gebraucht wurden, als auch auf einer objektiven Bewertung basieren.
- Zusätzlich soll es die Möglichkeit geben, einen Abschlussbericht zu erstellen. Dabei soll der Benutzer bei der Durchführung mit vorgegebenen Fragen unterstützt werden.

4.2 Anforderungen betreffend der Abwehrmaßnahmen gegen ausgewählte Angriffe

Wie bereits angesprochen, ist es notwendig, zusätzlich zu den oben genannten Punkten der Reaktionsphase die Anforderungen an die Abwehr gegen die einzelnen gewählten Angriffsarten zu berücksichtigen. Hierfür wurden folgende drei Angriffsarten gewählt:

- APT - Advanced Persistent Threat
- DDoS - Distributed Denial of Service
- Ransomware

Die darauffolgenden Anforderungen beziehen sich auf die oben genannten Angriffsarten, jedoch zeigt es sich, dass ein gewisses Zusammenspiel mit den davor gestellten Anforderungen der Reaktionsphase besteht. Für die Bekämpfung der Angriffsarten wurden folgende Anforderungen definiert:

- Es sollen für jedes der drei Angriffsarten Beratungsschritte für die Erstanalyse, Analyse und Schadensmilderung festgelegt werden, die dabei helfen können den Sicherheitsvorfall zu beheben. Dafür sollten unter anderem die Eigenschaften oder auch die Vorgehensweise der Angriffstypen berücksichtigt werden.
- Es sollen drei Reaktionspläne erstellt werden, jeweils einer pro Angriffsart, damit eine vordefinierte Vorgehensweise besteht und beim Eintreten einer der drei Angriffstypen Zeit gespart werden kann.
- Es soll eine klare Reihenfolge eingeplant werden, wo pro Angriffsart jeweils beschrieben ist, welche Schritte von wem und zu welchem Zeitpunkt durchgeführt werden.

- Es sollen drei Templates erstellt werden, jeweils eines pro Angriffsart, für die Dokumentation der einzelnen Spuren, die bei der Erstanalyse und Analyse festgehalten werden. Zusätzlich soll dabei vorgeschlagen werden, welche Punkte unbedingt zu berücksichtigen sind.
- Es soll die Schadensmilderung der drei Sicherheitsvorfälle mit den einzelnen durchgeführten Schritten dokumentiert werden.
- Nach jedem Sicherheitsvorfall sollen die vorher definierten Maßnahmen für die jeweiligen Angriffstypen ausgewertet und bei Bedarf aktualisiert werden, falls Ergänzungen oder Verbesserungen notwendig sind.

Die hier definierten Anforderungen werden im Anschluss unter anderem für das BPMN-Modell und die Anwendungsfälle (Use Cases) bedeutsam sein.

5 Lösungsweg & Modellentwicklung

In diesem Kapitel wird auf den Lösungsweg für die Methode zur Unterstützung der Reaktionsphase im NIST CSF [42] bei Sicherheitsvorfällen näher eingegangen. Dabei werden unter anderem zwei BPMN-Modelle vorgestellt, die einerseits die Vorbereitungsphase und andererseits die Reaktionsphase unterstützen. Weiters werden die notwendigen Funktionen, die für die Erstellung der Methode benötigt werden, grafisch in einem Use Case Diagramm dargestellt und beschrieben. Darauffolgend wird eine Modellentwicklung durchgeführt, beginnend mit den Akteuren, die schlussendlich Gebrauch von der Methode machen. Im weiteren Schritt werden die Elemente definiert und deren Beziehungen zueinander geklärt. Schließlich wird ein Modell entwickelt, das die einzelnen Elemente und die Verbindungen grafisch darstellt.

5.1 BPMN Diagramme

5.1.1 BPMN Diagramm Vorbereitungsphase

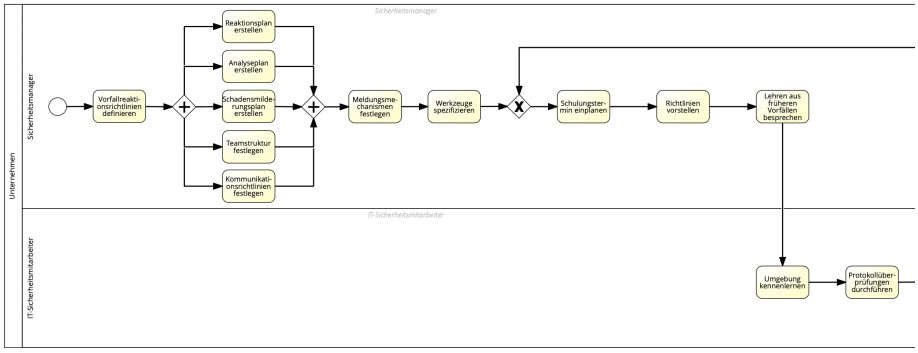

Figure 11: BPMN-Vorbereitungsphase (Teil 1)

Um den Ablauf der Reaktionsphase zu verbessern, ist es wichtig sich als gesamtes Team auf die verschiedenen Angriffsarten vorzubereiten. Daher ist es notwendig eine Vorbereitungsphase einzuplanen, um die Vorgehensweise bei diversen Vorfällen zu üben. Dies sollte auch in gewissen Abständen wiederholt werden, um die Effizienz zu erhöhen. Das in Figure 11 und Figure 12 dargestellte BPMN-Modell wurde auf Basis der vorher durchgeführten Literaturanalyse erstellt. Aus Übersichtlichkeitsgründen wurde das Modell in zwei Teile geteilt. Dabei ist zu beachten, dass in diesem Diagramm der Security Analyst auch als IT-Sicherheitsmitarbeiter gesehen wird.

Wie in Figure 11 zu sehen, beginnt der Prozess der Vorbereitungsphase mit dem Definieren der Vorfallreaktionsrichtlinien durch den Sicherheitsmanager (Security Manager). Anschließend müssen einige Pläne erstellt und Aspekte definiert werden, die im Nachhinein den Reaktionsablauf unterstützen sollen. Darunter zählen unter anderem das Erstellen eines:

- Reaktionsplans
- Analyseplans
- Schadensmilderungsplans

Zusätzlich muss folgendes festgelegt werden:

- Teamstruktur
- Kommunikationsrichtlinien

Darauffolgend muss der Sicherheitsmanager die Mechanismen für die Meldung des Vorfalls festlegen und die Werkzeuge spezifizieren, die während des Reaktionsablaufs verwendet werden. Nachdem dies alles eingeplant wurde, ist es notwendig, einen Schulungstermin einzuplanen. Die Schulung selbst soll mit dem Vorstellen der Richtlinien und der Lehren aus früheren Vorfällen beginnen. Anschließend kann mit der Einschulung der IT-Sicherheitsmitarbeiter (Security Employee, Security Analyst) begonnen werden. Zuerst muss der IT-Sicherheitsmitarbeiter die Umgebung kennenlernen, um mit den Protokollüberprüfungen fortzufahren.

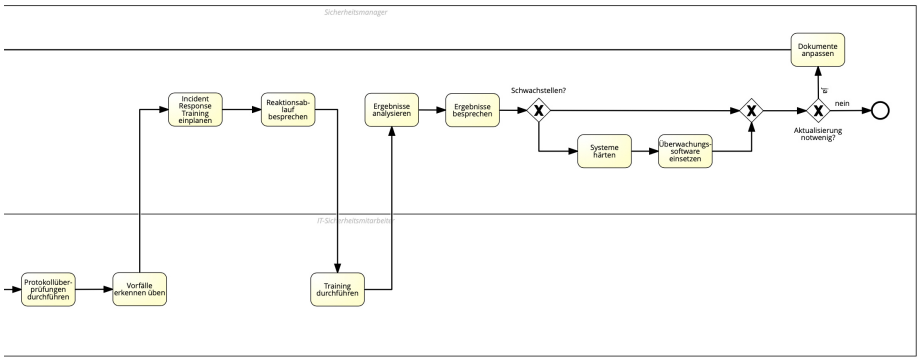

Figure 12: BPMN-Vorbereitungsphase (Teil 2)

Nach der Protokollüberprüfung, wie in Figure 12 zu sehen, muss der IT-Sicherheitsmitarbeiter üben, die Vorfälle zu erkennen. Danach ist es von Vorteil, ein Incident Response Training einzuplanen, das vom IT-Sicherheitsmanager durchgeführt werden soll. Zu Beginn des Trainings muss zuerst der Reaktionsablauf besprochen werden, um anschließend das Training mit den IT-Sicherheitsmitarbeitern durchzuführen. Abschließend soll der Sicherheitsmanager die Ergebnisse analysieren und besprechen. Wenn dabei Schwachstellen erkannt wurden, ist es notwendig, die Systeme zu härten und Überwachungswerkzeuge einzusetzen. Am Ende der Vorbereitungsphase muss überlegt werden, ob eine Aktualisierung der Dokumente erforderlich ist. Sobald dies der Fall ist, muss eine Anpassung der Dokumente durchgeführt werden.

5.1.2 BPMN Diagramm Reaktionsphase

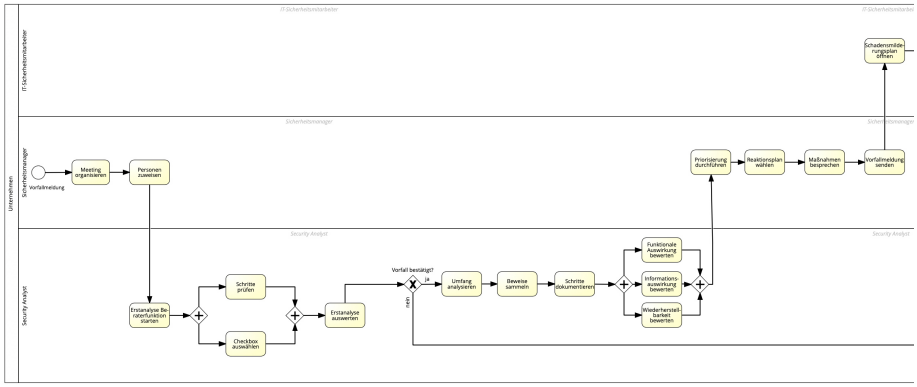

Figure 13: BPMN-Reaktionsphase (Teil 1)

Das, in Figure 13 dargestellte BPMN-Modell stellt die Reaktionsphase dar, die nach der Meldung eines Verdachts auf einen Vorfall beginnt. An diesem Diagramm werden sich die darauffolgenden Anwendungsfälle und der Prototyp orientieren. Um die Übersichtlichkeit zu erhöhen, wurde das Diagramm in drei Teile (Figure 13-15) geteilt. Das Prozessmodell wurde ebenfalls auf Basis der vorher durchgeführten Literaturanalyse erstellt.

Im BPMN-Modell wird zwischen Sicherheitsmanager (Security Manager), IT-Sicherheitsmitarbeiter (Security Employee) und Security Analyst unterschieden. Der Prozess startet beim Sicherheitsmanager, nachdem ein bestimmter Angriff gemeldet wurde. Der erste Schritt, den der Manager durchführt, ist das Organisieren eines Meetings, um den vermuteten Angriff zu besprechen und die Personen, die bei der Reaktion tätig sein werden, zuzuweisen. Anschließend muss der Security Analyst eine Erstanalyse durchführen, indem dieser die Beraterfunktion verwendet. Dabei müssen die einzelnen vorgeschlagenen Schritte, die jeweils einzeln angezeigt werden, geprüft und eine Frage beantwortet werden. Nachdem alle Beratungsschritte erkundet wurden, wird die Erstanalyse ausgewertet. Wenn der Vorfall nicht bestätigt wird, dann endet der Prozess. Bei einem Schadensfall sind die nächsten Schritte das Analysieren des Umfangs, das Sammeln und Dokumentieren von Beweisen, die ebenfalls vom Security Analyst durchgeführt werden. Abschließend muss dieser noch die folgenden drei Auswirkungen bewerten:

- Funktionale Auswirkung
- Informationsauswirkung
- Wiederherstellbarkeit

Fortgeführt wird das BPMN-Diagramm mit dem Sicherheitsmanager, der anhand der Auswirkungen eine Prioritätsstufe für den Angriff vergeben soll. Daraufhin soll ein entsprechender Reaktionsplan für die Angriffsart gewählt und

sollen Maßnahmen mit dem Reaktionsteam besprochen werden. Abschließend wird der Vorfall bei den internen und externen Partnern gemeldet.

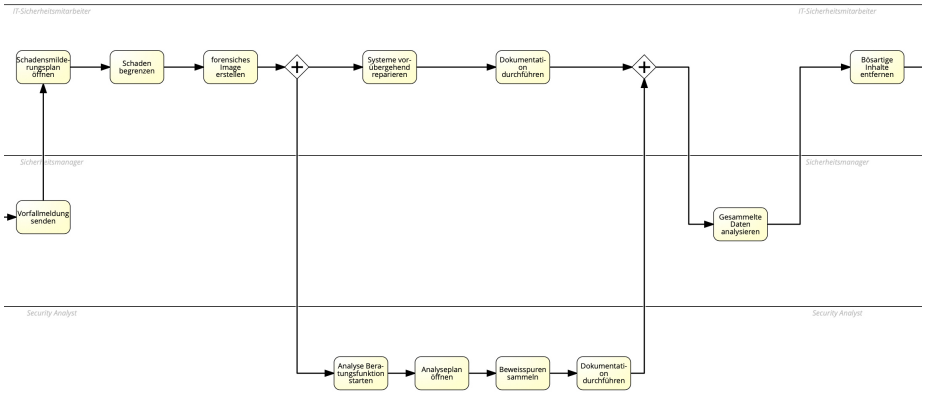

Figure 14: BPMN-Reaktionsphase (Teil 2)

Wie in Figure 14 zu sehen ist, beginnt der Sicherheitsmitarbeiter (Security Employee) mit dem Öffnen des Schadensmilderungsplans gegen den spezifischen Angriff. Daraufhin wird der Schaden begrenzt und ein forensisches Image erstellt, um im Nachhinein einen reibungslosen Analyseablauf zu ermöglichen. Anschließend wird auf der einen Seite das System vom IT-Sicherheitsmitarbeiter vorübergehend repariert und eine Dokumentation der durchgeführten Schritte erstellt. Auf der anderen Seite wird vom Security Analyst eine genauere Analyse mit Hilfe der Beratungsfunktion und des Analyseplans durchgeführt, die darauffolgend dokumentiert wird. Nachdem beide ihre Aufgaben erledigt haben, müssen die gesammelten Daten nochmals vom Sicherheitsmanager analysiert werden. Danach wird der Prozess durch den IT-Sicherheitsmanager fortgeführt, indem die gefährlichen Inhalte entfernt werden.

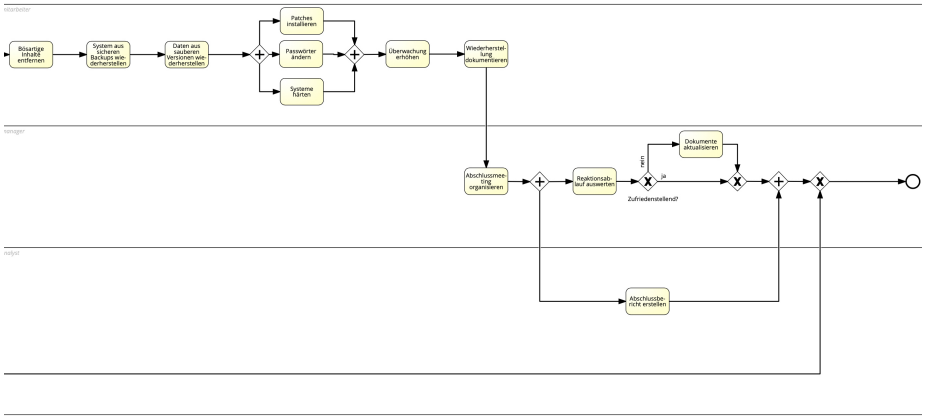

Figure 15: BPMN-Reaktionsphase (Teil 3)

Daraufhin muss der IT-Sicherheitsmitarbeiter das System aus sicheren Backups und die Daten aus sauberen Versionen wiederherstellen, wie in Figure 15 zu sehen ist. Es sollte Folgendes durchgeführt werden:

- Patches installieren
- Passwörter ändern
- Systeme härten

Anschließend muss die Überwachung erhöht und die Wiederherstellungsschritte dokumentiert werden. Danach wird durch den Sicherheitsmanager ein Abschlussmeeting organisiert, um den Reaktionsablauf auszuwerten und einen Abschlussbericht zu erstellen. Dabei führt der Sicherheitsmanager die Reaktionsablauf-Auswertung durch und der Security Analyst beschäftigt sich mit der Erstellung des Abschlussberichts. Zum Schluss werden die Dokumente entweder aktualisiert oder nicht, je nachdem ob die Auswertung zufriedenstellend ist oder nicht. Danach ist der Prozess der Reaktionsphase erfolgreich beendet.

Basierend auf diesem Modell der Reaktionsphase werden die Anwendungsfälle definiert. Im Nachhinein wird der Prototyp erstellt.

5.2 Architekturdiagramm

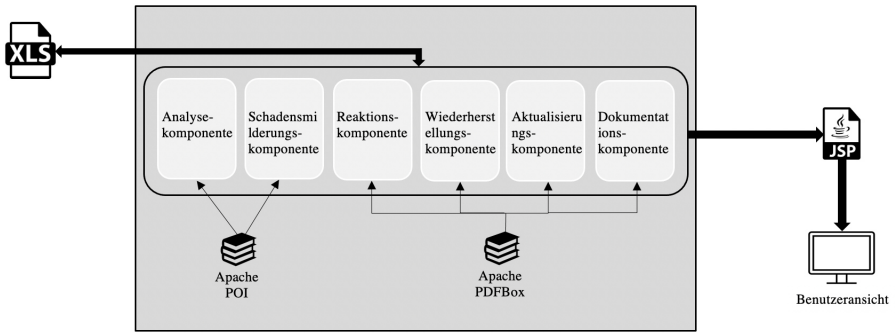

Figure 16: Architekturdiagramm

Im Architekturdiagramm wird die allgemeine Struktur des Systems gezeigt. Dieses beinhaltet sechs Komponenten, die für die Unterstützung der Reaktionsphase benötigt werden:

- Analysekomponente
- Schadensmilderungskomponente
- Reaktionskomponente
- Wiederherstellungskomponente
- Aktualisierungskomponente
- Dokumentationskomponente

Des Weiteren enthält das Architekturdiagramm folgende Elemente:

- Programmierbibliotheken: Apache POI [13] wird verwendet, um die Daten aus einem excel-File auszulesen oder zu schreiben. Apache PDFBox [12] wird für die Erstellung eines pdf-Dokuments, sowie für das Auslesen der Daten aus einer pdf-Datei, benötigt.
- Excel-Files: Es gibt mehrere excel-Files, die unter anderem die Daten für die Beratungsschritte, die für einige Schritte relevant sind, enthalten. Weiters wird die Zeit, die in den einzelnen Schritten gebraucht wird, festgehalten.
- Benutzeransicht: Die Ergebnisse aus den unterschiedlichen Komponenten werden mit Hilfe von Java Server Pages (jsp-Dateien) dem Anwender auf der Benutzeroberfläche angezeigt.

Im Anschluss werden die Komponenten und deren Beziehungen detaillierter beschrieben.

5.3 Use Case Diagramm für das zu entwickelnde System

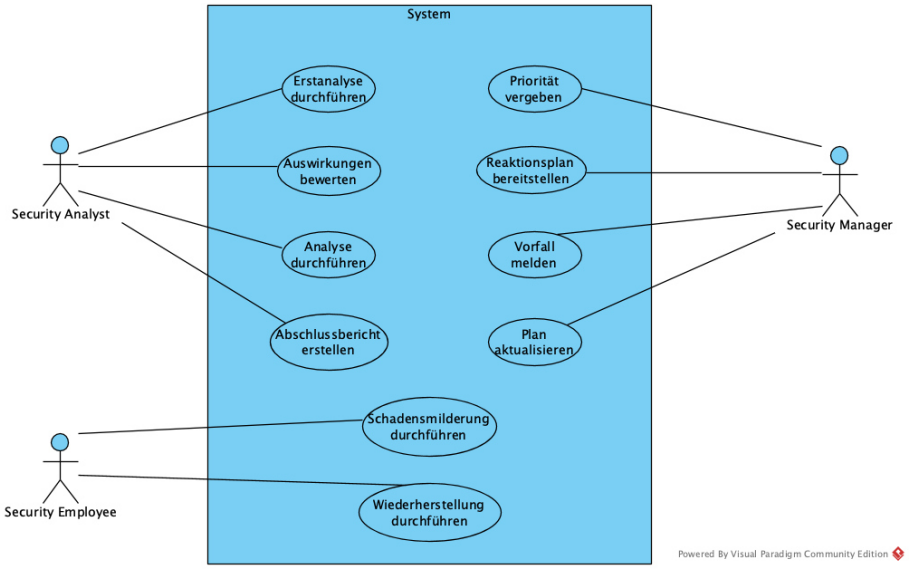

Figure 17: Use Case Diagramm

Grundsätzlich ist zu beachten, dass bei der Methode nicht nur einzelne ausgewählte Phasen wie z.B. die Analyse Phase unterstützt werden sollen, sondern alle vorher im Kapitel 2.1 (Incident Response Management) beschriebenen Reaktionsphasen. Daher soll ein sogenanntes Gesamtpaket geschaffen werden, das bei der Abarbeitung der Respond Planung bis hin zur Lernphase hilfreich ist. Um dies realisieren zu können, werden daher folgende Funktionen (siehe Figure 17: Use Case Diagramm) vonnöten sein:

1. **Erstanalyse durchführen:** Eine essenzielle Funktion zur Unterstützung der Reaktionsphase ist das Durchführen der Erstanalyse, die dabei helfen soll den Angriff zu bestätigen und die Phase, in der sich der Vorfall befindet, herauszufinden. Wie mehrmals erwähnt, liegt der Fokus auf drei Angriffsarten. Daher muss der Security Analyst am Anfang wählen, welcher Typ von Angriff vermutet wird. Anschließend wird dem Benutzer eine Beratungsfunktion angeboten, wo einzelne Schritte vorgeschlagen werden, die ihm bei der Durchführung der Erstanalyse helfen sollen. Zusätzlich wird jeweils am Ende des vorgeschlagenen Schrittes eine Frage gestellt, die mit "Ja" oder "Nein" zu beantworten ist, je nachdem ob etwas gefunden wurde oder nicht. Anschließend wird anhand der Fragen ausgewertet, ob ein Angriff stattfindet und in welcher Phase sich dieser befindet oder ob es sich um eine Falschmeldung handelt. Letztlich wird dem Security Analyst eine Dokumentationsseite zur Verfügung gestellt, wo die einzelnen Schritte dokumentiert werden sollen und die gemachten Screenshots hinzugefügt werden können. Nach der Durchführung wird automatisch eine pdf-Datei generiert. Um sich dies genauer vorstellen zu können, wird dazu ein Anwendungsfall, der vom Security Analyst bedient wird, in tabellarischer Form beschrieben.

Titel:	Erstanalyse durchführen
Kurzbeschreibung:	Es soll eine Erstanalyse durchgeführt und ausgewertet werden.
Akteure:	Security Analyst
Vorbedingungen:	Die Beratungsschritte müssen vorher zur Verfügung stehen.
Ablauf:	(a) Der Akteur wählt "Erstanalyse durchführen" und die Angriffsart, die vermutet wird, aus. (b) Das System liest das Erstanalyse excel-File und zeigt die Beratungsschritte an. (c) Der Akteur prüft die einzelnen Schritte und beantwortet die Fragen. (d) Das System speichert die Antworten im excel-File, wertet die beantworteten Fragen aus und zeigt eine Bestätigung des Vorfalls mit der entsprechenden Phase an. (e) Der Akteur klickt auf "Weiter". (f) Das System zeigt eine Dokumentationsseite mit den Hinweisen, in welcher Form die Dokumentation durchgeführt werden soll, an. (g) Der Akteur führt die Dokumentation durch, wählt die Screenshots aus und klickt auf "Weiter". (h) Das System generiert aus der Dokumentation eine formatierte pdf-Datei und zeigt eine Bestätigung an.
Alternativablauf:	(a) Der Akteur wählt "Erstanalyse durchführen" und die Angriffsart, die vermutet wird, aus. (b) Das System zeigt die Beratungsschritte an. (c) Der Akteur prüft die einzelnen Schritte und beantwortet die Fragen. (d) Das System speichert die Antworten im excel-File, wertet die beantworteten Fragen aus und zeigt eine Bestätigung der Falschmeldung an. (e) Der Akteur klickt auf "Home". (f) Das System zeigt die Home-Seite an.
Auswirkungen:	Die Erstanalyse wurde erfolgreich durchgeführt.

Table 1: Use Case: Erstanalyse durchführen

2. **Auswirkungen bewerten:** Weiters sind die Auswirkungen anhand der Erstanalyse zu bewerten. Dabei wird zwischen Funktionaler Auswirkung, Informationsauswirkung und Wiederherstellbarkeit unterschieden. Daher wird dem Security Analyst eine Seite mit den drei vorher genannten Auswirkungen angezeigt. Der Benutzer kann bei der Funktionalen Auswirkung zwischen folgenden Auswahlmöglichkeiten wählen:

   - Keine
   - Niedrig
   - Mittel
   - Hoch

   Bei der Informationsauswirkung kann folgendes gewählt werden:

   - Keine
   - Datenschutzverletzung
   - Proprietäre Verletzung
   - Integritätsverlust

   Bei der Wiederherstellbarkeit kann folgendes gewählt werden:

   - Regulär
   - Ergänzend
   - Erweitert
   - Nicht Wiederherstellbar

   Abschließend wird eine pdf-Datei mit den Auswirkungen generiert. Um sich dies genauer vorstellen zu können, wird dazu ein Anwendungsfall, der vom Security Analyst bedient wird, in tabellarischer Form beschrieben.

Titel:	Auswirkungen bewerten
Kurzbeschreibung:	Es sollen die Auswirkungen bewertet werden.
Akteure:	Security Analyst
Vorbedingungen:	Es muss vorher eine Erstanalyse durchgeführt worden sein.
Ablauf:	(a) Der Akteur wählt "Auswirkungen bewerten" aus. (b) Das System zeigt die zu bewertenden Auswirkungen an. (c) Der Akteur klickt den Auswahlbreich für die "Funktionale Auswirkung" an. (d) Der Akteur wählt "Niedrig" aus. (e) Der Akteur klickt den Auswahlbreich für die "Informationsauswirkung" an. (f) Der Akteur wählt "Keine" aus. (g) Der Akteur klickt den Auswahlbreich für die "Wiederherstellbarkeit" an. (h) Der Akteur wählt Regulär aus und klickt auf "Weiter". (i) Das System generiert eine pdf-Datei mit den gewählten Auswirkungen und zeigt eine Bestätigung an.
Alternativablauf:	/
Auswirkungen:	Die Auswirkungen wurden erfolgreich eingeschätzt und gespeichert.

Table 2: Use Case: Auswirkungen bewerten

3. **Priorität vergeben:** Eine weitere Funktion ist das Vergeben einer Priorität für den Sicherheitsvorfall basierend auf der vorher durchgeführten Bewertung der Auswirkungen. Daher wird dem Benutzer nach der Auswahl des entsprechenden Angriffs eine Priorisierungsseite angezeigt, wo die Angriffsart, Funktionale Auswirkung, Informationsauswirkung und die Wiederherstellbarkeit aus der Auswirkungsbewertung dargestellt sind. Zusätzlich wird dem Benutzer anhand der vorher bewerteten Auswirkungen automatisch eine Prioritätsstufe vorgeschlagen. Der Security Manager kann den Vorschlag annehmen oder eine andere Priorität setzen. Anschließend wird die pdf-Datei mit den Auswirkungen und mit der vergebenen Prioritätsstufe aktualisiert. Um sich dies genauer vorstellen zu können, wird dazu ein Anwendungsfall, der vom Security Manager bedient wird, in tabellarischer Form beschrieben.

Titel:	Priorität vergeben
Kurzbeschreibung:	Es soll eine Priorität für den Vorfall vergeben werden.
Akteure:	Security Manager
Vorbedingungen:	Es muss vorher die Auswirkung bewertet worden sein.
Ablauf:	(a) Der Akteur wählt "Priorisierung" und die Angriffsart aus. (b) Das System wertet die vorher durchgeführte Auswirkungsbewertung aus. (c) Das System zeigt die Priorisierungsseite mit der vorgeschlagenen Prioritätsstufe und den restlichen Informationen der Auswirkungen an. (d) Der Akteur übernimmt die vorgeschlagene Priorität und klickt auf "Weiter" (e) Das System aktualisiert die Auswirkungs-pdf mit der Prioritätsstufe.
Alternativablauf:	(a) Der Akteur wählt "Priorisierung" und die Angriffsart aus. (b) Das System wertet die vorher durchgeführte Auswirkungsbewertung aus. (c) Das System zeigt die Priorisierungsseite mit der vorgeschlagenen Prioritätsstufe und den restlichen Informationen der Auswirkungen an. (d) Der Akteur wählt eine andere Priorität aus und klickt auf "Weiter" (e) Das System aktualisiert die Auswirkungs-pdf mit der Prioritätsstufe.
Auswirkungen:	Der Angriff wurde erfolgreich priorisiert.

Table 3: Use Case: Priorität vergeben

4. **Reaktionsplan bereitstellen:** Eine weitere bedeutsame Funktion für die Unterstützung der Reaktionsphase ist das Anzeigen von Plänen. Dies kann vor allem bei der Reaktion auf eintretende Sicherheitsvorfälle hilfreich sein, da unter anderem damit die Reaktionszeit minimiert oder der Schaden begrenzt werden kann. Wie mehrmals erwähnt, liegt der Fokus auf drei Angriffsarten (APT, DDoS, Ransomware). Daher werden drei Pläne zur Verfügung stehen, die je nach Vorfall generiert werden. Der Reaktionsplan selbst wird aus vorher definierten Maßnahmen bestehen, die in einer bestimmten Reihenfolge angeordnet sind, damit eine gewisse Vorgehensweise definiert ist. Um sich dies genauer vorstellen zu können, wird dazu ein Anwendungsfall, der vom Security Manager bedient wird, in tabellarischer Form beschrieben.

Titel:	Reaktionsplan bereitstellen
Kurzbeschreibung:	Es soll der vorher erstellte Reaktionsplan angezeigt werden.
Akteure:	Security Manager
Vorbedingungen:	Ein Plan muss vorher zur Verfügung stehen und die Priorisierung muss durchgeführt worden sein.
Ablauf:	(a) Der Akteur wählt "Reaktionsplan" aus, nachdem die Priorisierung durchgeführt wurde. (b) Das System wählt den Reaktionsplan für den entsprechenden Angriff (APT, DDoS oder Ransomware) aus. (c) Das System zeigt den Reaktionsplan mit der beschriebenen Vorgehensweise an.
Alternativablauf:	/
Auswirkungen:	Der gewünschte Reaktionsplan für den entsprechenden Sicherheitsvorfall wird angezeigt.

Table 4: Use Case: Reaktionsplan bereitstellen

5. **Vorfall melden:** Die nächste Funktion ist das Melden des Vorfalls an die internen und externen Partner. Dabei wird dem Security Manager ein rasches Melden des Vorfalls ermöglicht, indem ihm eine E-Mail Seite zur Verfügung gestellt wird mit dem entsprechenden Betreff, den Partnern, die vom Benutzer gewählt werden können und einem vordefinierten Text zur Verständigung. Der Text kann entweder übernommen oder bearbeitet werden. Anschließend wird die E-Mail automatisch an die gewählten Partner gesendet. Um sich dies genauer vorstellen zu können, wird dazu ein Anwendungsfall, der vom Security Manager bedient wird, in tabellarischer Form beschrieben.

Titel:	Vorfall melden
Kurzbeschreibung:	Es soll eine E-Mail mit der Information über einen Angriff an die gewählten Partner gesendet werden.
Akteure:	Security Manager
Vorbedingungen:	Es muss vorher der Reaktionsplan angezeigt worden sein.
Ablauf:	(a) Der Akteur wählt "Vorfallmeldung" aus, nachdem der Reaktionsplan eingeblendet wurde. (b) Das System zeigt die Vorfallmeldungsseite an. (c) Der Akteur gibt den Betreff an. (d) Der Akteur wählt die Partner aus, an die die E-Mail gesendet werden soll. (e) Der Akteur übernimmt den vorher definierten Text und klickt auf "Senden". (f) Das System sendet die E-Mail an die gewählten Partner. (g) Das System zeigt eine Bestätigung an.
Alternativablauf:	(a) Der Akteur wählt "Vorfallmeldung" aus, nachdem der Reaktionsplan eingeblendet wurde. (b) Das System zeigt die Vorfallmeldungsseite an. (c) Der Akteur gibt den Betreff an. (d) Der Akteur wählt die Partner aus, an die die E-Mail gesendet werden soll. (e) Der Akteur bearbeitet den vorher definierten Text und klickt auf "Senden". (f) Das System sendet die E-Mail an die gewählten Partner. (g) Das System zeigt eine Bestätigung an.
Auswirkungen:	Die internen und externen Partner wurden über den Angriff informiert.

Table 5: Use Case: Vorfall melden

6. **Schadensmilderung durchführen:** Weiters ist es notwendig, eine Schadensmilderung durchzuführen, die den Schaden minimieren soll. Der Fokus liegt auf den drei Angriffsarten, daher muss der Security Employee zuerst wählen, um welche Angriffsart es sich handelt. Daraufhin wird dem Benutzer eine Beratungsfunktion angeboten, wo einzelne Schritte vorgeschlagen werden, die dabei helfen sollen, den Schaden zu mildern. Zusätzlich wird jeweils am Ende des vorgeschlagenen Schrittes eine Checkbox zur Verfügung gestellt, die der Benutzer auswählen kann, wenn der Schritt erledigt wurde. Anschließend wird ein Standardschadensmilderungsplan angezeigt. Zu guter Letzt wird dem Security Employee eine Dokumentationsseite zur Verfügung gestellt, wo die einzelnen Schritte dokumentiert werden sollen. Nachdem die Dokumentation abgeschlossen wurde, wird diese als formatierte pdf-Datei gespeichert. Um sich dies genauer vorstellen zu können, wird dazu ein Anwendungsfall, der vom Security Employee bedient wird, in tabellarischer Form beschrieben.

Titel:	Schadensmilderung durchführen
Kurzbeschreibung:	Es soll eine Schadensmilderung durchgeführt werden.
Akteure:	Security Employee
Vorbedingungen:	Es muss vorher die Vorfallsmeldung abgeschlossen sein.
Ablauf:	(a) Der Akteur wählt "Schadensmilderung" und die entsprechende Angriffsart aus. (b) Das System liest das Schadensmilderung excel-File und zeigt die Beratungsschritte an. (c) Der Akteur führt die vorgeschlagenen Schritte aus und klickt die Checkbox an. (d) Das System speichert den Wert der Checkbox in das Schadensmilderung excel-File. (e) Der Akteur klickt auf "Weiter". (f) Das System zeigt den Standardschadensmilderungsplan an. (g) Der Akteur betrachtet den Plan und klickt auf "Weiter". (h) Das System zeigt eine Dokumentationsseite an. (i) Der Akteur führt die Dokumentation durch und klickt auf "Weiter". (j) Das System generiert aus der Dokumentationsseite eine pdf-Datei und zeigt eine Bestätigung an.
Alternativablauf:	/
Auswirkungen:	Die Schadensmilderung wurde erfolgreich durchgeführt.

Table 6: Use Case: Schadensmilderung durchführen

7. **Analyse durchführen:** Ein weiterer Anwendungsfall ist die Durchführung der Analyse, die dabei helfen soll, die einzelnen Spuren zu sammeln und eine entsprechende Dokumentation zu erstellen, die bei juristischen Verfahren hilfreich sein kann. Um die Analyse effizient durchführen zu können, werden jeweils pro Angriffsart Beratungsschritte vorgeschlagen. Zusätzlich wird jeweils am Ende des vorgeschlagenen Schrittes eine Checkbox zur Verfügung gestellt, die der Security Analyst auswählen kann, wenn der Schritt erledigt wurde. Daraufhin wird ein Analyseplan angezeigt und ein Template für die Dokumentation vorgeschlagen, wo die einzelnen Spuren dokumentiert werden können. Abschließend wird eine formatierte pdf-Datei generiert. Um sich dies genauer vorstellen zu können, wird dazu ein Anwendungsfall, der vom Security Analyst bedient wird, in tabellarischer Form beschrieben.

Titel:	Analyse durchführen
Kurzbeschreibung:	Es sollen die einzelnen Spuren gesammelt und dokumentiert werden.
Akteure:	Security Analyst
Vorbedingungen:	Analyse Beratungsschritte, ein Analyseplan muss zur Verfügung stehen und ein forensisches Image muss erstellt sein.
Ablauf:	(a) Der Akteur wählt "Analyse durchführen" aus, nachdem die vorherigen Schritte durchgeführt wurden. (b) Das System liest die Analyse excel-Datei und zeigt die Beratungsschritte für die Analyse an. (c) Der Akteur prüft den vorgeschlagenen Schritt, klickt die Checkbox an, wenn dies erledigt wurde, und drückt auf "Weiter". (d) Das System speichert den Checkbox Wert in dem excel-File mit den Beratungsschritten. (e) Das System zeigt den allgemeinen Analyseplan und ein Template zum Dokumentieren an, nachdem alle Beratungsschritte angezeigt wurden. (f) Der Akteur dokumentiert die Beweisspuren und wählt die Bilder/Screenshots aus, die bei der Analyse gemacht wurden. (g) Der Akteur speichert das fertige Template mit den Beweisspuren ab. (h) Das System speichert das Template als pdf-Datei und zeigt eine Bestätigung an.
Alternativablauf:	/
Auswirkungen:	Alle Beweisspuren wurden erfolgreich festgehalten.

Table 7: Use Case: Analyse durchführen

8. **Wiederherstellung durchführen:** Ein weiterer Punkt ist die Wiederherstellung des normalen Betriebes. Dafür wird ein Dokument erstellt, wo die einzelnen Backups inklusive Datum der Durchführung notiert sind. Diese Backups werden dem Security Employee entweder grün oder rot markiert, je nachdem ob das Backup sicher ist. Dies kann dabei helfen, mit Hilfe des Datums und der Analyse der Beweisspuren herauszufinden, welches Backup nicht von dem Sicherheitsvorfall betroffen ist. Zusätzlich wird es eine Dokumentationsseite geben, wo die einzelnen durchgeführten Schritte eingefügt werden sollen. Anschließend wird dieses Dokument als formatierte pdf-Datei gespeichert. Um sich dies genauer vorstellen zu können, wird dazu ein Anwendungsfall, der vom Security Employee bedient wird, in tabellarischer Form beschrieben.

Titel:	Wiederherstellung durchführen
Kurzbeschreibung:	Es sollen die einzelnen Backups angezeigt werden und die durchgeführten Schritte dokumentiert werden.
Akteure:	Security Employee
Vorbedingungen:	Es muss vorher eine Backupliste erstellt werden.
Ablauf:	(a) Der Akteur wählt "Wiederherstellung" aus. (b) Das System zeigt die Backupliste an. (c) Der Akteur analysiert die vorhandenen Backups und klickt auf "Weiter". (d) Das System zeigt die Dokumentationsseite an. (e) Der Akteur dokumentiert die einzelnen durchgeführten Schritte der Wiederherstellung. (f) Der Akteur speichert die fertige Dokumentation als pdf-Datei ab. (g) Das System speichert die Dokumentation und zeigt eine Bestätigung an.
Alternativablauf:	/
Auswirkungen:	Die Wiederherstellung des Betriebes wurde erfolgreich abgeschlossen.

Table 8: Use Case: Wiederherstellung durchführen

9. **Plan aktualisieren:** Eine weitere essenzielle Funktion ist das Lernen aus jedem Sicherheitsvorfall. Daher ist die vorletzte Funktion das Aktualisieren der vorher eingeplanten und durchgeführten Strategien, das durch den Security Manager abgewickelt wird. Um dies leichter zu bewerten, wird die automatische Auswertung unter anderem mit Hilfe der vorher erstellten Dokumentation der Erstanalyse, Analyse, Schadensmilderung und Wiederherstellung unterstützt. Dabei wird einerseits die Zeit, die für die Bearbeitung des Vorfalls gebraucht wurde, betrachtet und andererseits eine objektive Bewertung des Vorfalls durchgeführt. Anschließend wird dem Security Manager bei Bedarf eine Aktualisierungsseite mit dem aktuellen Reaktionsplan angezeigt. Daraufhin kann der Benutzer diesen Plan aktualisieren und speichern. Um sich dies genauer vorstellen zu können, wird dazu ein Anwendungsfall, der vom Security Manager bedient wird, in tabellarischer Form beschrieben.

Titel:	Plan aktualisieren
Kurzbeschreibung:	Es sollen die eingesetzten Pläne ausgewertet und falls nötig aktualisiert werden.
Akteure:	Security Manager
Vorbedingungen:	Es müssen alle vorherigen Schritte abgeschlossen sein.
Ablauf:	(a) Der Akteur wählt "Plan aktualisieren" aus. (b) Das System zeigt die drei Angriffsarten (APT, DDoS, Ransomware) an. (c) Der Akteur wählt die Angriffsart aus und klickt auf "Auswerten". (d) Das System wertet die vorher durchgeführten Dokumentationen anhand zeitlicher und objektiver Faktoren aus und gibt dem Benutzer eine Rückmeldung, ob eine Aktualisierung des Plans notwendig ist. (e) Der Akteur bearbeitet den Plan. (f) Der Akteur speichert den Plan ab. (g) Das System speichert den Plan und zeigt eine Bestätigung mit dem neuen Plan an.
Alternativablauf:	(a) Der Akteur wählt "Plan aktualisieren" aus. (b) Das System zeigt die drei Angriffsarten (APT, DDoS, Ransomware) an. (c) Der Akteur wählt die Angriffsart aus und klickt auf "Auswerten". (d) Das System wertet die vorher durchgeführten Dokumentationen anhand zeitlicher und objektiver Faktoren aus und gibt dem Benutzer eine Rückmeldung, ob eine Aktualisierung des Plans notwendig ist. (e) Das System informiert den Akteur, dass keine Aktualisierung notwendig ist.
Auswirkungen:	Der Reaktionsplan wurde erfolgreich aktualisiert.

Table 9: Use Case: Plan aktualisieren

10. **Abschlussbericht erstellen:** Schließlich ist es möglich, einen Abschlussbericht zu erstellen, wo unter anderem einige Fragen vom Security Analyst beantwortet werden sollen, um nochmals den Sicherheitsvorfall durchzugehen und Verbesserungsmöglichkeiten zu erkennen. Weiters kann eine Chronologie von Ereignissen und eine Schätzung der Höhe des, durch den Vorfall verursachten, Schadens dokumentiert werden. Anschließend wird der Abschlussbericht als formatierte pdf-Datei gespeichert.

Titel:	Abschlussbericht erstellen
Kurzbeschreibung:	Es soll ein Abschlussbericht mit den beantworteten Fragen erstellt werden.
Akteure:	Security Analyst
Vorbedingungen:	Es müssen alle vorherigen Schritte abgeschlossen sein.
Ablauf:	(a) Der Akteur wählt "Abschlussbericht" aus. (b) Das System zeigt die drei Angriffsarten (APT, DDoS, Ransomware) an. (c) Der Akteur wählt die Angriffsart aus und beantwortet die gestellten Fragen. (d) Der Akteur klickt auf "Weiter". (e) Das System speichert eine formatierte pdf-Datei aus dem vorher durchgeführten Abschlussbericht. (f) Das System zeigt die Home-Seite an.
Alternativablauf:	/
Auswirkungen:	Es wurde ein Abschlussbericht erstellt.

Table 10: Use Case: Abschlussbericht erstellen

5.4 Modellentwicklung

Für die Modellentwicklung sind zum einen die Akteure, die mit dem System beziehungsweise mit dem Modell interagieren, festzulegen. Zum anderen wird das Definieren der einzelnen Modellelemente von Bedeutung sein. Diese sollen die Bereitstellung der im Unterkapitel "Use Case Diagramm für das zu entwickelnde System" genannten Funktionen ermöglichen. Zusätzlich kann ein Element mit anderen Elementen zusammenarbeiten. Anders gesagt, es kann eine Beziehung zwischen den einzelnen Komponenten bestehen.

5.4.1 Akteure

Angefangen mit den Akteuren, die für das Modell beziehungsweise System relevant sind, kann, wie oben angedeutet, festgelegt werden, dass drei Zielgruppen zu berücksichtigen sind. Da es sich hier um die Reaktion auf Sicherheitsvorfälle handelt, ist es nicht ausreichend IT-Mitarbeiter einzusetzen, sondern es werden spezielle IT-Sicherheitsmitarbeiter (Security Employee) vonnöten sein. Zusätzlich wird es einen Security Analyst geben, der für die Durchführung der Analyse zuständig ist. Weiters zu beachten sind die Sicherheitsmanager (Security Manager), die diverse wichtige Entscheidung treffen können wie z.B. die Priorisierung des Angriffes oder die Durchführung von Planänderungen.

5.4.2 Modellelemente

Um die Funktionen, die im Unterkapitel "Use Case Diagramm für das zu entwickelnde System" genannt werden, zu unterstützen, werden folgende Elemente beziehungsweise Komponenten festgelegt:

1. Analysekomponente: Zu Beginn soll die Analysekomponente bei der Erstanalyse helfen, indem diese die einzelnen Schritte, die durchzuführen sind, vorschlägt. Anschließend unterstützt es mit der Bestätigung des Vorfalls. Weiters hilft diese bei der Bewertung der Auswirkungen und bei der Vergabe der Priorität. Ebenso soll die Analysekomponente bei der Sammlung der Spuren behilflich sein, die daraufhin als Beweismittel bei Gerichtsverfahren dienen können. Um die Analyse zu unterstützen, werden eine Beratungsfunktion mit den durchzuführenden Schritten und ein Analyseplan für jede Angriffsart angeboten.

2. Reaktionskomponente: Dieses Element ist für die Auswahl und das Anzeigen des entsprechenden Plans zuständig. Nachdem erkannt wird, um welchen Sicherheitsvorfall es sich handelt - in unserem Fall wird zwischen APT, DDoS, Ransomware unterschieden - wird der vorher erstellte Reaktionsplan mit den Maßnahmen angezeigt. Zusätzlich unterstützt diese Komponente das Informieren der internen und externen Partner, indem eine E-Mail-senden Funktion bereitgestellt wird.

3. Schadensmilderungskomponente: Diese Komponente soll dabei helfen, die Schadenshöhe zu mildern. Dafür wird eine Beratungsfunktion zur Ver-

fügung gestellt, die mit den einzelnen Schritten helfen soll, den aktuellen Schaden und den möglichen zukünftigen, zu verringern. Die Beratungsschritte werden jeweils an die Angriffsart (APT, DDoS, Ransomware) angepasst.

4. Wiederherstellungskomponente: Dieses Element soll bei der Durchführung der Wiederherstellung des normalen Betriebes hilfreich sein. Es wird unter anderem für das Anzeigen aller Backups in Form eines Dokumentes zuständig sein. Dies kann dabei helfen, sich einen Überblick zu verschaffen und die Wiederherstellung erfolgreich abzuschließen.

5. Dokumentationskomponente: Diese Komponente ist für das Festhalten von Dokumentationen jeder Art zuständig. Dies beinhaltet das Dokumentieren der Spuren, die bei der Erstanalyse und Analyse festgehalten wurden. Weiters ist die Dokumentationskomponente für das Speichern der Auswirkungen inklusive Priorität, das Dokumentieren der Schadensmilderung und der Wiederherstellung zuständig. Zusätzlich hilft es bei der Festhaltung des Abschlussberichts. Aus all diesen Dokumentationen wird mit Hilfe der Komponente jeweils eine formatierte pdf-Datei generiert.

6. Aktualisierungskomponente: Das letzte Modellelement ist für die Bearbeitung beziehungsweise Aktualisierung der zurzeit eingesetzten Pläne bestimmt. Um herauszufinden, ob ein Bedarf auf eine Überarbeitung besteht, werden zeitliche und objektive Faktoren einbezogen und basierend darauf eine Auswertung durchgeführt. Bei einem negativen Ergebnis wird anschließend der Reaktionsplan zur Abänderung angezeigt. Am Schluss werden die neuen Dokumente von der Aktualisierungskomponente gespeichert.

5.4.3 Beziehungen zwischen Modellelementen

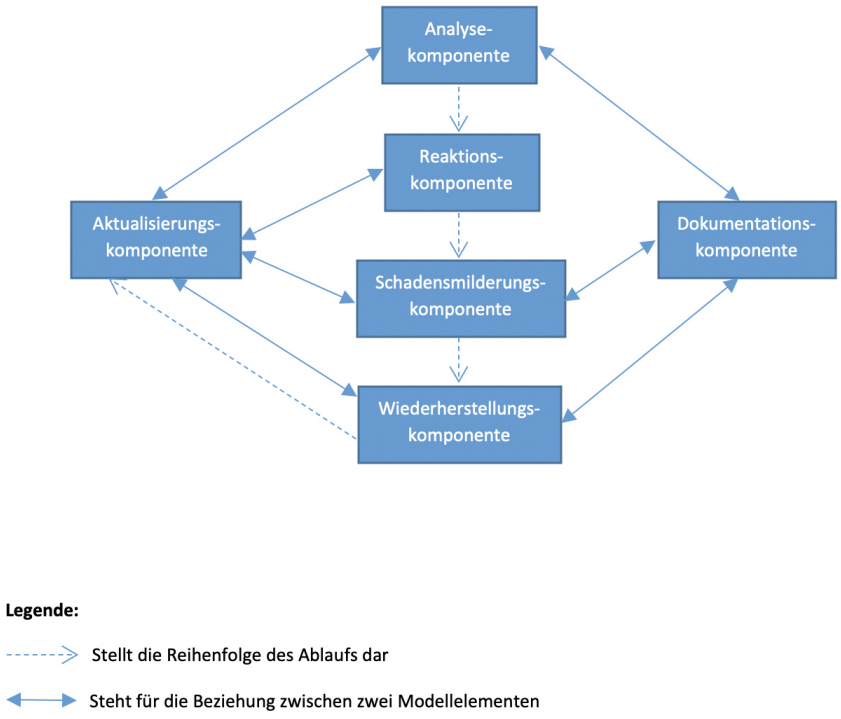

Figure 18: Komponentenmodell und deren Beziehungen

- Grundsätzlich besteht eine Verbindung zwischen der jeweils aktuellen Komponente und der darauffolgenden Komponente, wie z.B. Analysekomponente → Reaktionskomponente oder Reaktionskomponente → Schadensmilderungskomponente. Diese sind durch eine gestrichelte Linie mit einem Pfeil am Ende gekennzeichnet und stellen die Reihenfolge des Ablaufs dar (siehe Figure 18: Modell). Angefangen mit der Analyse, fortgesetzt mit der Reaktion, Schadensmilderung, Wiederherstellung und abschließend mit der Aktualisierung.

- Analyse-, Schadensmilderungs-, Wiederherstellungskomponente ⇔ Dokumentationskomponente: Zwischen den Komponenten Analyse und Dokumentation besteht eine Beziehung. Die Spuren, die bei der Erstanalyse und Analyse gesammelt werden, werden anschließend dokumentiert. Weiters besteht eine Verbindung zwischen Schadensmilderungskomponente und Dokumentationskomponente, die die durchgeführten Schritte als formatierte pdf-Datei speichert. Es besteht auch eine Beziehung zwischen Wiederherstellungskomponente und Dokumentationskomponente. All diese Beziehungen werden mit einem Doppelpfeil verbunden.

- Analyse-, Reaktions-, Schadensmilderungs-, Wiederherstellungskomponente ⇔ Aktualisierungskomponente: Weiters besteht eine Verbindung zwischen der Reaktionskomponente und der Aktualisierungskomponente. Die vorgeschlagenen Pläne für die drei Angriffsarten können durch die Aktualisierungskomponente ergänzt beziehungsweise aktualisiert werden. Dasselbe gilt für die drei restlichen Relationen Analyse ⇔ Aktualisierung, Schadensmilderung ⇔ Aktualisierung und Wiederherstellung ⇔ Aktualisierung. Diese wirken auch auf die Überarbeitung des Reaktionsplans ein. All diese Beziehungen werden mit einem Doppelpfeil verbunden.

6 Implementierungsansatz für den Prototyp

In diesem Kapitel wird etwas genauer auf den Implementierungsansatz für den Prototyp eingegangen. Dabei wird bis auf kleine Ausnahmen fast alles besprochen, angefangen mit der Vorbereitung, in der zuerst überlegt wurde, wie die vorher definierten Anforderungen erfüllt werden können, dann mit den Daten, die benötigt werden, um die Beratungsfunktionen zur Verfügung zu stellen. Darauf folgt die Auswertung der Erstanalyse des Angriffs, um herauszufinden, ob ein Angriff stattfindet und in welcher Phase sich dieser befindet. Weiters werden die Auswirkungen betrachtet und die Vergabe der Priorität definiert. Nun wird der Prozess mit der Unterstützung der Schadensmilderung, Analyse und Wiederherstellung weitergeführt. Fortgesetzt wird mit der Unterstützung der Dokumentationen und der Aktualisierungsauswertung, in der vorher durchgeführte Schritte bewertet werden. Zusätzlich wird noch anhand eines Beispiels auf eine dynamischere Form des Hereinladens von Daten in ein excel-File eingegangen.

6.1 Vorbereitung auf die Technologieauswahl

Um die definierten Anforderungen abzudecken und die modellierten Anwendungsfälle unterstützen zu können, wurde für die Prototyprealisierung ein entsprechender Technologie-Stack gewählt. Abzudecken dabei waren die Programmiersprache sowie die Technologiebasis für den Server. Als Programmiersprache wurde Java und für die Gestaltung der grafischen Benutzeroberfläche wurde Bootstrap gewählt. Das Backend basiert auf folgenden, von Apache Tomcat zur Verfügung gestellten Technologien:

- Java Servlets: Diese sind für das Entgegennehmen und das Beantworten der Benutzeranfragen zuständig.
- Java Server Pages: Diese sind für die grafische Darstellung der einzelnen Seiten zuständig, die anhand von HTML angezeigt werden.

Die Bereitstellung und der Zugriff auf jene Daten, die für die einzelnen Arbeitsschritte nötig waren, stellten eine zentrale Herausforderung dar. Daher wurde daraufhin das Aussehen der Beraterfunktion und der Durchführung der Erstanalyse spezifiziert. Anschließend wurden die Auswirkungen, die zu bewerten sind und die Priorität, die zu vergeben ist, herausgearbeitet. Abschließend

wurde noch die Unterstützung der Dokumentationen und die Abwicklung der Aktualisierung überlegt. Genauer beschrieben wird dies in den darauffolgenden Unterkapiteln.

6.2 Vorbereitung der Inputdaten für die Beratungsfunktion

Damit der Prototyp den Reaktionsablauf von drei verschiedenen Angriffsarten (APT, DDoS, Ransomware) unterstützen kann, mussten anfänglich Daten zu diesen gesammelt werden. Um diese in einer bestimmten Form als Input zur Verfügung zu stellen, wurde das MITRE ATT&CK Framework [4] gewählt. MITRE ATT&CK Framework bietet eine globale Wissensbasis der Taktiken und Techniken an, die von Angreifern verwendet werden [4]. Auf dieser Seite befinden sich unter dem Reiter Techniques → Enterprise eine Vielzahl an Informationen über die Techniken der Angreifer. Basierend auf der Vorgehensweise der drei Angriffe, die in der Literaturanalyse beschrieben wurde, wurden die Informationen der verschiedenen Techniken in den unterschiedlichen Phasen ausgearbeitet. Der Fokus der Masterarbeit liegt auf den drei Angriffstypen APT, DDoS und Ransomware, daher wurden jeweils pro Angriff Datensätze erstellt. Dadurch, dass die Datenmenge überschaubar ist, wurde entschieden, ein excel-File zu verwenden, das folgendermaßen aussieht:

ErstID	Angriffsart	Text	Frage	Antwort
1	APT	Prüfen Sie zunächst, ob es in letzter Zeit zu mehreren Ablehnungen von der Firewall für einzelne Ports von ein und demselben Host gekommen ist. Falls dies der Fall ist, halten Sie die verdächtige IP-Adresse in einer Liste fest.	Konnten Sie Ablehnungen feststellen?	
2	APT	Betrachten Sie die TCP Verbindungen auf Port 443, die SSL/TLS verschlüsselt, genauer. Versuchen Sie einen internen Host mit externen IP-Adresse zu finden, die vorher auf der Liste der verdächtigen IP-Adressen gelandet ist. Schauen Sie sich zusätzlich das Volumen pro Mitarbeiter pro Host an. Wenn dieses sich in einem bestimmten Zeitraum verändert, könnte das auch ein Anzeichen auf einen Angriff sein.	Konnten Sie eine verdächtige IP-Adresse bzw. ein höheres Volumen finden?	
3	APT	Verwenden Sie die Prozessüberwachung, um die Ausführung von CMSTP.exe zu erkennen und zu prüfen. Vergleichen Sie die letzten Aufrufe von CMSTP.exe mit der Vorgeschichte geladener Dateien, um Anomalien festzustellen. Prüfen Sie zuletzt durchgeführte Befehlszeilen- und Skriptaktivitäten. Auch das Laden von Modulen sollten Sie überprüfen. Überwachen Sie Prozesse auf abnormales Verhalten, das auf DDE-Missbrauch hinweist, z. B. Microsoft Office-Anwendungen, die DLLs laden, und andere Module, die normalerweise nicht mit der Anwendung verknüpft sind, oder diese Anwendungen, die ungewöhnliche Prozesse hervorrufen (z. B. cmd.exe). Prüfen Sie DLL-Ladevorgänge (z.B. kernel32.dll, advapi32.dll, user32.dll, gdi32.dll) auf abnormale oder potenzielle böswillige Prozesse.	Konnten Sie etwas verdächtiges Erkennen?	
4	APT	Suchen Sie auch nach Verhalten auf dem Endpunktsystem, das auf einen erfolgreiche Kompromittierung hinweist, z. B. abnormales Verhalten des Browsers oder der Office-Prozesse. Überprüfen Sie Prozesse, die mit COM-Objekten verknüpft sind, insbesondere die von einem anderen Benutzer als aktuell angemeldeten aufgerufen werden. Verwenden Sie die Prozessüberwachung, um die Ausführung von mshta.exe zu überwachen. Suchen Sie in der Befehlszeile nach mshta.exe, die ein unformatiertes oder verschleiertes Skript ausführt.	Konnten Sie ein abnormales Verhalten erkennen?	
5	APT	Untersuchen Sie SQL-Server-Instanzen und zwar prüfen Sie die IP-Adressen am Port 1433. Schauen Sie sich auch den Port 135 und 139 für die Netzwerkfreigaben an. Sie können zusätzlich mit Hilfe einer Echtzeitanalyse feststellen, ob sich ein VPN-Account in einer unrealistischen Zeitspanne von zwei verschiedenen geografischen Standorten anmeldet.	Konnten Sie etwas verdächtiges Erkennen?	
6	APT	Prüfen Sie, ob in folgenden Startordnern ein Programm hinzugefügt wurde: C:\Users\Username1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	Konnte etwas Auffälliges entdeckt werden?	

Figure 19: excel-Tabelle

Hierbei handelt es sich um das excel-File (erstanalyse_*angriffsart*.xlsx) der Erstanalyse, die aus einer ID, Angriffsart, Text, Frage und einer Antwort besteht. Der Text beinhaltet die einzelnen Beratungsschritte, die dem Benutzer pro Angriff in der Erstanalyse, Analyse, Schadensmilderung nach der Reihe angezeigt werden und die Unterstützung ermöglichen. Im Vergleich zu den anderen, gibt es bei der Erstanalyse eine Frage, die gestellt wird, und eine Antwort. Bei

der Analyse und Schadensmilderung hingegen befindet sich nach dem Text eine Abgehakt Spalte. Mit Hilfe dieser Daten wird bei den weiteren Schritten gearbeitet.

6.3 Auswertung der Erstanalyse

Um eine Auswertung der Erstanalyse durchführen zu können, muss vorher der Benutzer die Angriffsart wählen, die Beratungsschritte durchgehen und die gestellten Fragen beantworten. Daher müssen zunächst die Schritte für den bestimmten Angriff aus dem excel-File (erstanalyse_*angriffsart*.xlsx) herausgelesen werden. Dafür wurde die Java Programmierbibliothek Apache POI [13] gewählt, die auf der einen Seite das Lesen aus einem excel-File und auf der anderen Seite das Schreiben in ein excel-File ermöglicht. Nachdem alle Beratungsschritte dem Benutzer angezeigt und die Antworten im excel-File (erstanalyse_*angriffsart*.xlsx) geschrieben wurden, kann mit der Auswertung der Erstanalyse weitergemacht werden. Für die Auswertung werden demnach folgende Schritte durchgeführt:

- Angriffsart wählen: Zuerst muss die vermutete Angriffsart gewählt werden.
- Text herauslesen: Es werden die Beratungsschritte mit der dazugehörigen Frage als String array herausgelesen und dem Benutzer angezeigt.
- Antwort speichern: Dann wird der Antwortwert des Benutzers als String übergeben und im excel-File gespeichert.
- Antworten herauslesen: Danach werden die Antworten des Benutzers als String herausgelesen und für die Auswertung der Erstanalyse bereitgestellt.
- Erstanalyse auswerten: Die Antworten werden begutachtet und aufgrund der, daraus gewonnenen, Erkenntnisse wird ein Angriff entweder bestätigt oder nicht. Wenn es beispielsweise nur Nein-Antworten gibt, dann handelt es sich um eine Fehlermeldung. Zusätzlich wird auch das Herausfinden der Phase unterstützt, da die Reihenfolge der Beratungsschritte an die Phasen angepasst ist. Anders gesagt, betrifft zum Beispiel der erste Schritt die erste Phase eines Angriffs.

6.4 Auswirkungen bewerten & Priorität vergeben

Damit die Auswirkungen eingeschätzt werden können, muss zuerst überlegt werden, anhand welcher Kategorien diese bewertet werden sollten. Dazu wurde das NIST Dokument [8] zur Hand genommen, wo unter anderem drei Kategorien vorgeschlagen werden. Dabei wird zwischen drei Auswirkungen unterschieden: [8]

- Funktionale Auswirkung
- Informationsauswirkung

- Wiederherstellbarkeit

Kategorie	Funktionale Auswirkung
Keine	Keine Auswirkung auf die Dienste, die Benutzern zur Verfügung gestellt werden
Niedrig	Minimaler Effekt, es können weiterhin alle Dienste zur Verfügung gestellt werden, aber es gibt einen Verlust an Effizienz
Mittel	Das Unternehmen hat die Fähigkeit verloren, einer Untergruppe von Systembenutzern einen Dienst bereitzustellen
Hoch	Das Unternehmen ist nicht in der Lage einige wichtige Dienste für Benutzer bereitzustellen

Kategorie	Informationsauswirkung
Keine	Es wurden keine Informationen exfiltriert, geändert, gelöscht oder auf andere Weise kompromittiert
Datenschutz-verletzung	Es wurde auf personenbezogene Daten zugegriffen oder sie wurden herausgefiltert
Proprietäre Verletzung	Es wurde auf nicht klassifizierte proprietäre Informationen wie z.B. geschützte kritische Infrastrukturinformationen zugegriffen oder sie wurden herausgefiltert
Integritäts-verlust	Vertrauliche oder geschützte Informationen wurden geändert oder gelöscht

Kategorie	Wiederherstellbarkeit
Regulär	Die Zeit bis zur Wiederherstellung mit den vorhandenen Ressourcen ist vorhersehbar
Ergänzend	Die Zeit bis zur Wiederherstellung ist mit zusätzlichen Ressourcen vorhersehbar
Erweitert	Die Zeit zur Wiederherstellung ist unvorhersehbar, Zusätzliche Hilfe von außen ist notwendig
Nicht Wiederher-stellbar	Eine Wiederherstellung ist nicht möglich (z.B. vertrauliche Daten, die herausgefiltert und veröffentlicht wurden), Untersuchungen einleiten

Table 11: Auswirkungen

Wie den Tabellen zu entnehmen ist, wurden, basierend auf dem NIST Dokument [8] jeweils pro Auswirkung mehrere Kategorien zugeordnet. Aus diesen Kategorien muss der Benutzer die Auswirkungen bewerten. Anschließend wird anhand dieser Bewertung die Priorisierung des Angriffs durchgeführt.

Um das Priorisieren zu unterstützen, wird mit Hilfe der bewerteten Auswirkungen dem Security Manager eine Prioritätsstufe (Niedrig, Mittel, Hoch) wie in [25] vorgeschlagen. Welche Auswirkungen für die Bewertung in Betracht gezogen werden, hängt von der Angriffsart ab. Bei einem APT-Angriff wird der Fokus auf die Informationsauswirkung gelegt, da der Angreifer das Ziel verfolgt, sensible Daten eines Unternehmens zu stehlen. Wird hingegen ein DDoS-Angriff

betrachtet, dann ist es wichtiger, die Funktionale Auswirkung einzubeziehen, da es bei dieser Attacke darum geht, einen hohen Datenfluss zu generieren, um die Serverleistung zu beeinträchtigen und somit die angebotenen Dienste für den Benutzer stark einzuschränken. Je höher die Funktionale Auswirkung ist, desto höher ist die Priorität. Bei einem Ransomware-Angriff werden sowohl die Funktionalen- als auch die Informationsauswirkungen berücksichtigt, da es sowohl zu einem vorübergehenden, möglicherweise dauerhaften Verlust der Daten des Unternehmens als auch zu einem kompletten Abschalten des Betriebs (Funktionalität beeinträchtigt) kommen kann. Allgemein ist zu beachten, dass der Security Manager die Priorität vergeben kann und somit nicht unbedingt den Vorschlag annehmen muss.

6.5 Unterstützung der Schadensmilderung & Analyse

Um die Schadensmilderung und die Analyse zu unterstützen, werden, ähnlich wie bei der Erstanalyse, Beratungsschritte angeboten. Es werden ebenfalls die Schritte für den bestimmten Angriff aus dem excel-File (banalyse_*angriffsart*.xlsx oder schaden_*angriffsart*.xlsx) gelesen. Hierfür wurde auch die Java-Programmierbibliothek Apache POI [13] gewählt, die das Auslesen und Schreiben in ein excel-File ermöglicht. Die einzelnen Beratungsschritte werden sowohl bei der Schadensmilderung als auch bei der Analyse dem Benutzer angezeigt und nach der Überprüfung vom Benutzer als geprüft markiert. Der geprüft-Wert wird anschließend in das excel-File geschrieben. Bei der Schadensmilderung und Analyse werden folgende Schritte benötigt:

- Text herauslesen: Zuerst werden die Beratungsschritte der entsprechenden Angriffsart als String array herausgelesen und dem Benutzer angezeigt. Hier wird ein Array verwendet, um den geprüft-Wert zu erfassen, der angezeigt wird, falls ein Benutzer zu einem Schritt zurückkehrt, der vorher von ihm durchgeführt wurde.
- Geprüft-Wert speichern: Anschließend wird jeweils pro Beratungsschritt der Wert der Checkbox als String übergeben und in das entsprechende excel-File gespeichert.

6.6 Wiederherstellung

Bei der Wiederherstellung wurde darauf geachtet, dem Benutzer die Auswahl des richtigen Backups zu erleichtert. Es wurde die Entscheidung getroffen, die letzten fünf Backups mit Namen, Datum und der verlinkten Backup-Datei anzuzeigen. Zusätzlich werden die Backups, die als sicher gesehen werden, in grüner Textfarbe dargestellt und die unsicheren mit Rot gekennzeichnet. Um dies zu ermöglichen, muss im ersten Schritt eine pdf-Datei mit Hilfe von Apache PDFBox [12] herausgelesen werden, die die Backups mit Datum und der Uhrzeit in Tabellenform beinhalten. Daraus werden die letzten fünf herausgenommen und basierend auf der Vorfallzeit wird entschieden, ob sie grün oder rot angezeigt werden.

6.7 Unterstützung der Dokumentation

Bei der Dokumentation wurde die Entscheidung getroffen, alle Formulare zu vereinfachen, indem dem Benutzer erstens ein Textfeld angeboten wird, bei dem keine Formatierungsaspekte beachtet werden müssen und zweitens automatisch ein pdf-Dokument daraus erstellt wird. Zu beachten ist nur, dass nach einem Schritt beziehungsweise nach einem Absatz ein Strichpunkt (;) gesetzt wird, damit erkannt wird, wann ein Zeilenumbruch zu machen ist. Zusätzlich gibt es die Möglichkeit, die gemachten Screenshots auszuwählen. Anschließend wird daraus eine formatierte pdf-Datei mit dem Text und den Screenshots erstellt. Für das Generieren und im Nachhinein für das Auslesen der pdf-Datei wurde die Apache PDFBox [12] Bibliothek verwendet. Um ein formatiertes Dokument zu erstellen, werden folgende Schritte benötigt:

- Im ersten Schritt muss der Text, der vom Benutzer hinzugefügt wurde, übergeben werden, inklusive Angriffsart, Ersteller und optional der Filename des Screenshots.
- Anschließend wird berechnet, wie viele Zeilen gebraucht werden, indem der übergebene String text auf die Länge geprüft wird und zusätzlich die Strichpunkte (;) beachtet werden.
- Danach wird der Text gesplittet, sodass jedes Wort als ein Element betrachtet wird.
- Daraufhin werden die Wörter in ein Array eingefügt bis die Zeilenlänge erreicht ist, und dann wird auf das nächste Arrayelement gesprungen.
- Abschließend wird noch geprüft, wie viele Seiten aufgrund der Arraylänge und der maximalen Zeilenanzahl der pdf-Seite gebraucht werden.
- Zu guter Letzt wird das pdf-Dokument mit dem Inhalt generiert.
- Wahlweise werden noch die Screenshots auf einer neuen Seite der pdf-Datei hinzugefügt, falls welche ausgewählt wurden.

Manche pdf-Dateien wie z.B. Angriffsart_Erstanalyse_Datum.pdf wurden mit einem Passwort versehen. Um die pdf-Datei anzusehen, muss als Passwort "test" eingegeben werden.

Zusätzlich ist bei der Dokumentation des Abschlussberichts anzumerken, dass dem Benutzer Fragen zum Beantworten angeboten werden. Diese wurden anhand von [8] ausgearbeitet.

6.8 Aktualisierung

Um die Entscheidung der Aktualisierung zu unterstützen, wurde überlegt, den Reaktionsablauf mit Hilfe von zeitlichen und objektiven Faktoren automatisch auszuwerten. Bei der automatischen Auswertung anhand der Zeit werden folgende Faktoren basierend auf [8] berücksichtigt:

- Gesamtaufwand für den Vorfall (Gesamtzeit)
- Verbrauchte Zeit vom Beginn des Vorfalls bis zur Entdeckung des Vorfalls, bis zur anfänglichen Folgenabschätzung, bis zu jeder Phase des Vorfallbehandlungsprozesses (Schadensmilderung, Wiederherstellung)
- Zeit, wie lange das Team für die Reaktion auf den Vorfall gebraucht hat, um auf den ersten Bericht über den Vorfall zu reagieren
- Zeit, wie lange es gedauert hat, den Vorfall dem Management und den externen Stellen zu melden

Bei der Unterstützung der automatischen Auswirkung, anhand der objektiven Bewertung, werden folgende Faktoren basierend auf [8] einbezogen:

- Überprüfen von Berichten beziehungsweise Dokumentationen auf Einhaltung der festgelegten Richtlinien und Verfahren zur Reaktion auf Vorfälle.
- Ermitteln, welche Indikatoren des Vorfalls aufgezeichnet wurden, um festzustellen, wie effektiv der Vorfall protokolliert und identifiziert wurde.

Alle Zeiten, von Anfang bis zum Ende, werden aufgezeichnet und die Dokumentation wird mit Hilfe von Pattern, Matcher geprüft ob alles ordnungsgemäß eingehalten wurde. Um die Einhaltung der Zeit zu prüfen, wurde folgende Tabelle basierend auf [28] erstellt:

Prioritäts-stufe	Erstreaktions-zeit	Reaktionszeit Erstanalyse	Meldung an externe Stellen	Reaktionszeit Eindämmung	Reaktions-zeit Wieder-herstellung	Gesamt-reaktions-zeit
Niedrig	Max. 4h	Max. 8h	Max. 12h	Max. 16h	Max. 20h	Max. 24h
Mittel	Max. 1h	Max. 2.5h	Max. 4h	Max. 5.5h	Max. 7h	Max. 8h
Hoch	Max. 10 min	Max. 1h	Max. 1.5h	Max. 2h	Max. 3h	Max. 4h

Table 12: Bewertung der Zeit

Wie in dieser Tabelle zu erkennen ist, werden die drei Prioritätsstufen Niedrig, Mittel, Hoch angeboten. Weiters gibt es für jede Phase eine maximale Zeit pro Prioritätsstufe, die nicht überschritten werden darf. Wenn sowohl die Zeit als auch die objektive Bewertung in Ordnung ist, wird keine Aktualisierung vorgeschlagen.

6.9 Dynamische Wartung - Umwandlung der Daten in Tabellen

Um eine gewisse Dynamik einzubauen, können Daten, die in einem HTML-Dokument gespeichert sind, herausgelesen und in ein excel-File geschrieben werden. Dies wird anhand eines Beispiels dargestellt. Als Java-Bibliothek wurde dafür Jsoup [23] verwendet, die das Extrahieren von Daten aus HTML-Dokumenten ermöglicht. Dabei kann auf DOM (Document Object Model) zugegriffen werden. Wie oben, in "Vorbereitung der Daten an die Beratungsfunktion", erwähnt, wurde das MITRE ATT&CK Framework [4] für die Sammlung der Informationen über die Angriffstechniken verwendet.

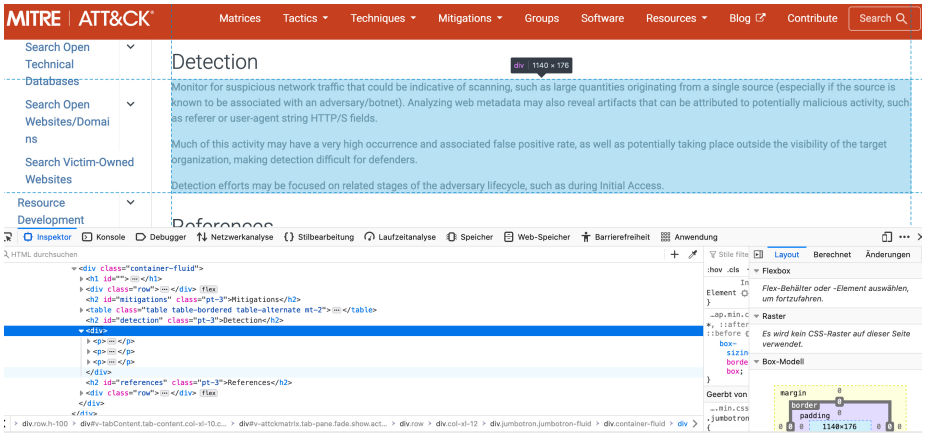

Figure 20: Firefox-Inspektor/MITRE ATT&CK Framework [4]

Wie in Figure 20 zu erkennen ist, muss im ersten Schritt, nach dem Aufrufen der Seite, analysiert werden, wie sich die Struktur des HTML-Dokuments darstellt. Dazu kann in Firefox der Inspektor (Extras → Web-Entwickler → Inspektor oder F12) verwendet werden. Anschließend kann die DOM-Eigenschaft angezeigt werden, indem zuerst der HTML-Tag gewählt wird, der die Daten zur Verfügung stellt und danach Rechtsklick → "DOM-Eigenschaften" anzeigen ausgewählt wird.

Basierend auf dem DOM kann mit Hilfe eines select-Statements auf die Daten des HTML-Dokuments zugegriffen werden. Als Beispiel werden hier die Daten einer Angriffstechnik für die Erstanalyse herausgelesen. Dafür wird folgendes select benötigt:

- Elements e = doc.select("h2#detection").first().nextElementSibling().select("div p");
- Mit Hilfe dieser Zeile wird zuerst der h2-Tag mit der detection-id gewählt, damit danach nicht die falsche div Box ausgesucht wird. Anschließend wird der darauffolgenden div-Tag, der die p-Tags mit dem Text enthält, selektiert.

ErstID	Angriffsart	Text	Frage	Antwort
1	APT	Monitor for suspicious network traffic that could be indicative of scanning, such as large quantities originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields. Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders. Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.	Did you find suspicious network traffic?	

Figure 21: excel-Tabelle mit Daten aus HTML-Dokument

Diese Daten werden daraufhin im excel-File in der Text-Spalte gespeichert und können anschließend dem Benutzer nach dem Herauslesen angezeigt werden.

6.10 Importierung des Projektes

In diesem Unterkapitel wird auf die Anforderungen eingegangen, denen man sich stellen muss, um den implementierten Prototyp zum Laufen zu bringen. Um diesen zu testen, müssen grundsätzlich Java und ein Tomcat Server auf dem Rechner installiert sein. Weiters muss ein Programmierwerkzeug wie z.B. Eclipse, IntelliJ IDEA, NetBeans IDE etc. verwendet werden. Anschließend ist es notwendig, das zur Verfügung gestellte Prototypprojekt zu importieren. Für das Einfügen des Projektes am Beispiel von Eclipse, werden folgende Schritte textuell beschrieben als auch grafisch dargestellt:

- Schritt 1: Der Projektordner muss in den vorhandenen workspace Ordner von Eclipse kopiert werden.

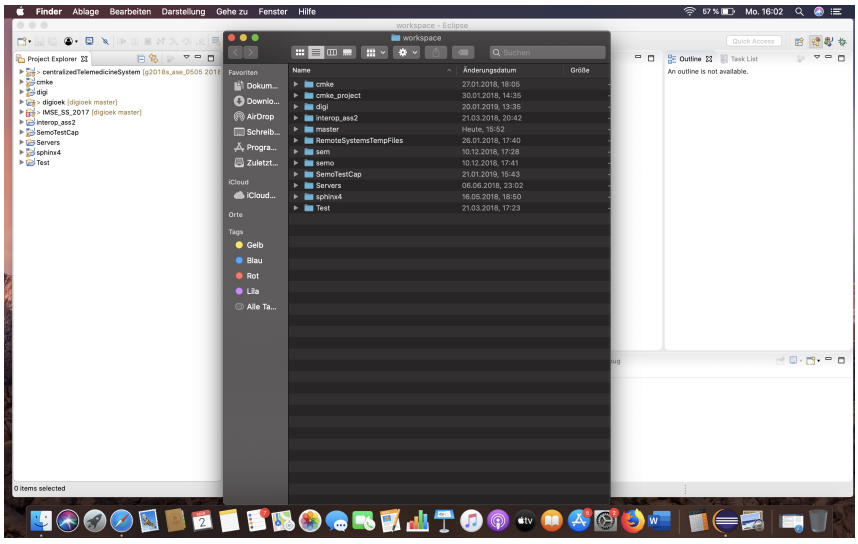

Figure 22: Schritt 1

- Schritt 2: Man wählt File ⇒ Import ⇒ Existing Projects into Workspace ⇒ Next ⇒ Select root directory: workspace ↪ Projektfoldername ⇒ OK ⇒ Finish

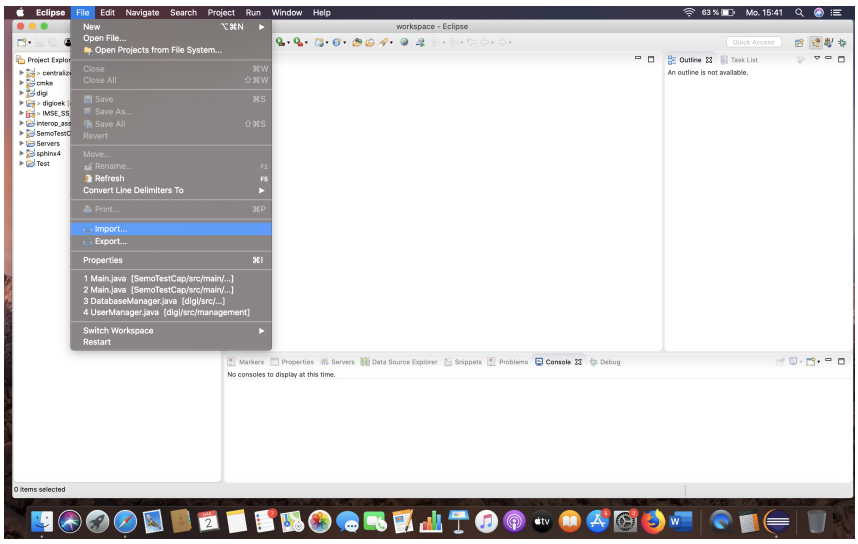

Figure 23: Schritt 2-1

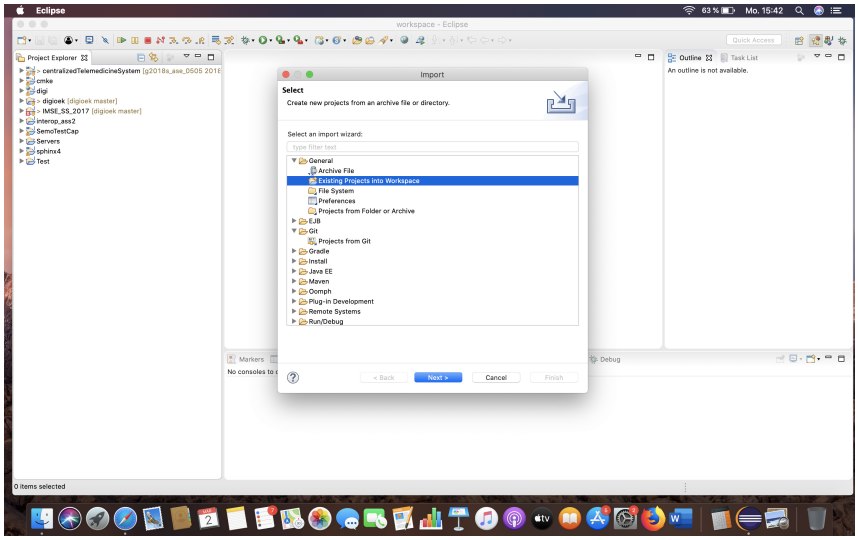

Figure 24: Schritt 2-2

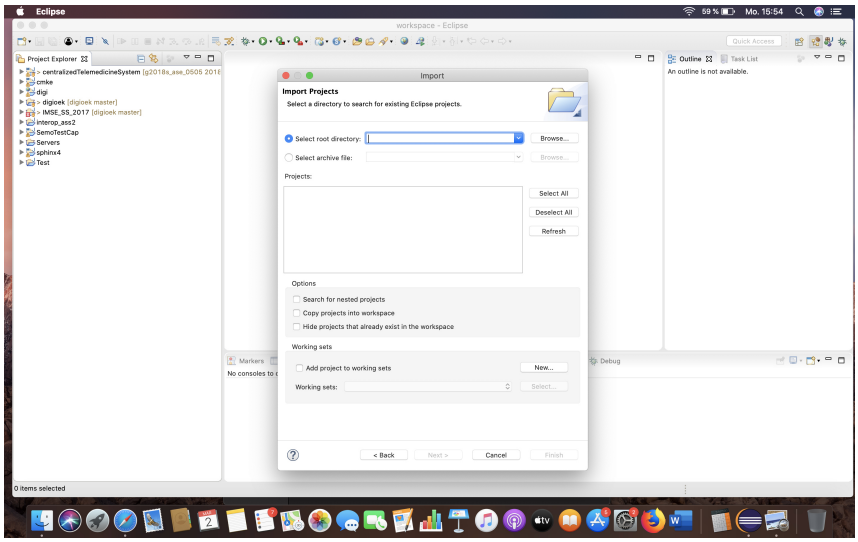

Figure 25: Schritt 2-3

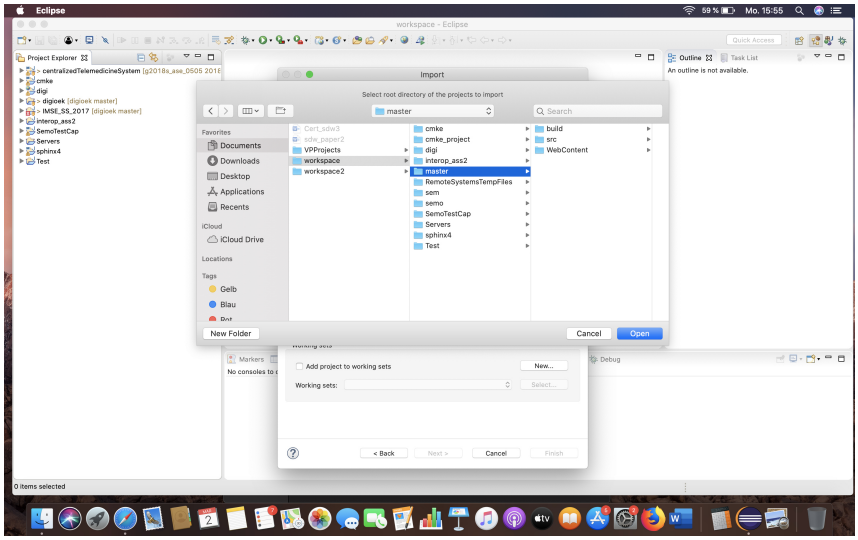

Figure 26: Schritt 2-4

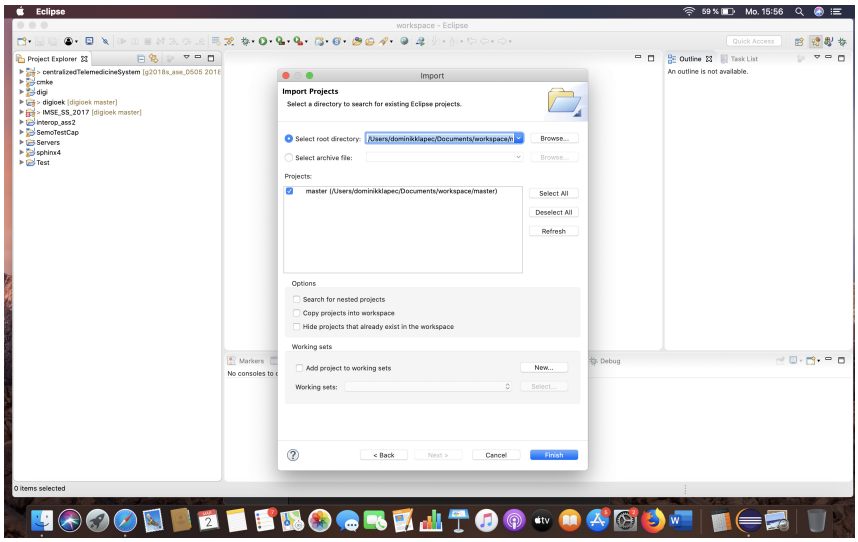

Figure 27: Schritt 2-5

- Schritt 3: In Eclipse Rechtsklick auf Projektfolder ⇒ Run As ⇒ Run on Server ⇒ Finish

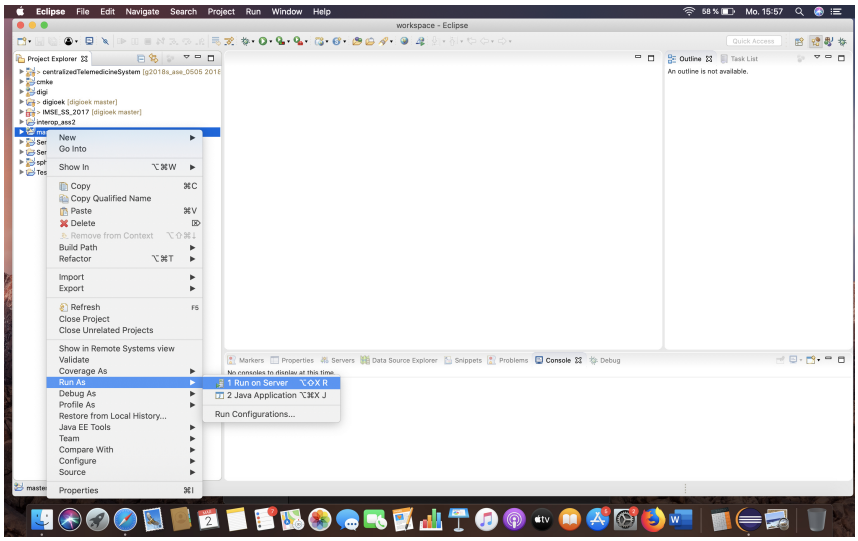

Figure 28: Schritt 3-1

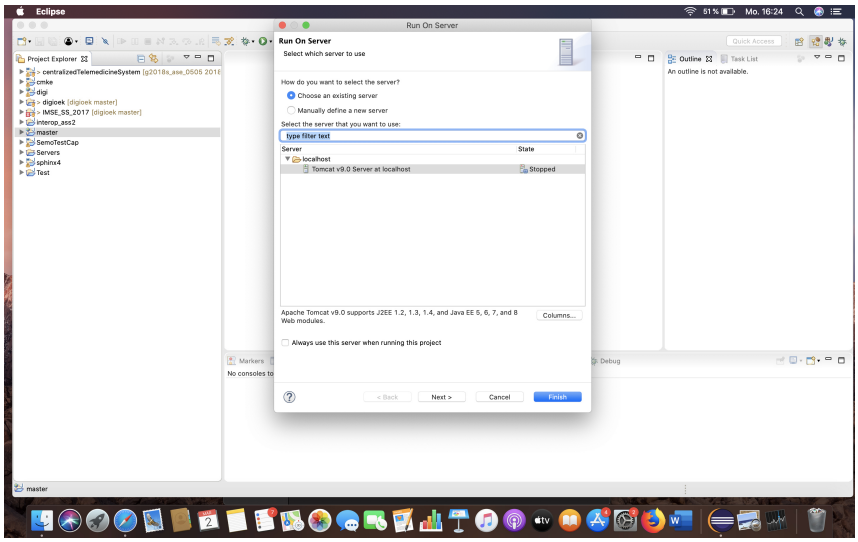

Figure 29: Schritt 3-2

7 Prototypentwicklung

Dieses Kapitel befasst sich mit der Beschreibung der Funktionsweise des Prototyps. Hier wird erklärt, was im Prototyp zur Verfügung steht und wie dieser zu bedienen ist.

7.1 Rollen des Prototyps

Die, im Prototyp zur Verfügung gestellten, Rollen umfassen den Security Analyst, Security Manager und den Security Employee. Dadurch werden ohne weitere Probleme alle zur Verfügung gestellten Funktionen abgedeckt.

7.2 Beschreibung des Prototyps

Der erste Schritt, der durchgeführt werden muss, um die angebotenen Funktionen des Prototyps zu verwenden, ist das Einloggen. Um dies durchzuführen, müssen ein entsprechender Benutzername und ein dazugehöriges Passwort eingegeben werden. Wie im Unterkapitel "Rollen des Prototyps" erwähnt, gibt es drei Arten von Rollen (Security Manager, Security Analyst, Security Employee) und somit jeweils ein Benutzerkonto pro Rolle. Dafür müssen folgende Login Daten verwendet werden:

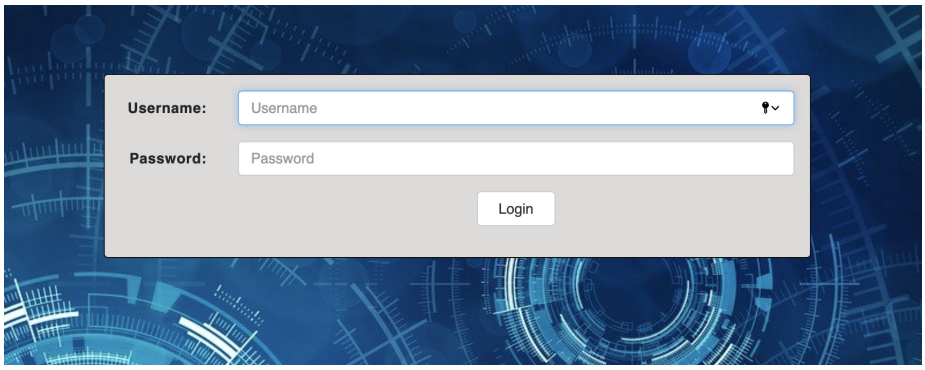

Figure 30: Login Ansicht

1. Security Analyst:
   (a) Benutzername: secanalyst
   (b) Passwort: secana123!
2. Security Manager:
   (a) Benutzername: secmanager
   (b) Passwort: secman123!

3. Security Employee:

   (a) Benutzername: secemployee

   (b) Passwort: secemp123!

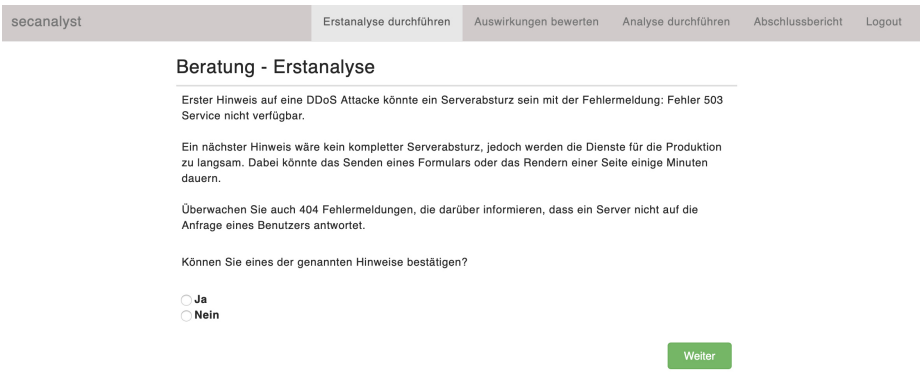

Figure 31: Security Analyst Ansicht (Angriffsart ausgewählt)

Je nachdem, welcher Benutzer eingeloggt wird, gibt es drei verschiedene Ansichten. Der Security Analyst wird nach der Anmeldung auf eine Seite weitergeleitet, auf der die entsprechende Angriffsart ausgewählt werden kann. Nachdem die eingetroffene Angriffsart (APT, DDoS, Ransomware) gewählt wurde, wird die Erstanalyseansicht mit den Beratungsschritten angezeigt. Abschließend wird dem Security Analyst angezeigt, ob ein Angriff stattfindet und in welcher Phase sich dieser befindet.

Nach der Erstanalyse werden dem Security Analyst die Auswirkungen angezeigt, die durch den Akteur eingeschätzt werden sollen. Daraufhin werden die Auswirkungen als pdf-Datei gespeichert.

Anschließend werden dem Security Analyst die Beratungsschritte für die Analyse angezeigt. Der Akteur kann die Checkbox markieren, wenn der entsprechende Beratungsschritt durchgeführt wurde. Darauffolgend wird die Dokumentationsseite für die Analyse angezeigt und nach dem Ausfüllen als pdf-Datei gespeichert.

Der Security Analyst kann noch einen Abschlussbericht erstellen. Dies sollte jedoch erst am Ende des kompletten Prozesses geschehen.

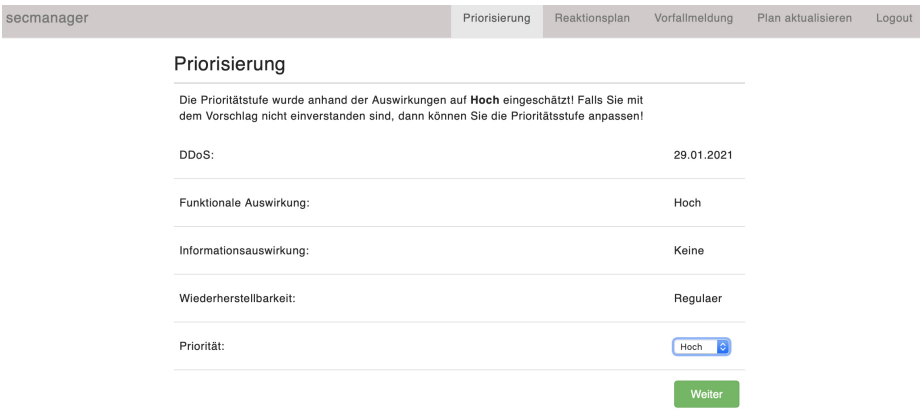

Figure 32: Security Manager Ansicht (Angriffsart ausgewählt)

Dem Security Manager wird nach der Anmeldung und der Auswahl der Angriffsart die Priorisierungsseite angezeigt, wo die Priorität für den Angriff anhand der vorher bewerteten Auswirkungen vergeben werden soll.

In der Folge wird dem Security Manager der Reaktionsplan für die entsprechende Angriffsart angezeigt.

Im Anschluss kann der Vorfall gemeldet werden, indem der Security Analyst einen Text verfasst oder den bereits vorhandenen verwendet und die Partner auswählt, die kontaktiert werden sollten.

Zuletzt kann der Plan vom Security Manager aktualisiert werden. Es wird dem Akteur - basierend auf der Auswertung der vorigen Schritte - angezeigt, ob eine Aktualisierung notwendig ist. Dabei ist zu beachten, dass dies erst nach der Wiederherstellung durchgeführt werden sollte.

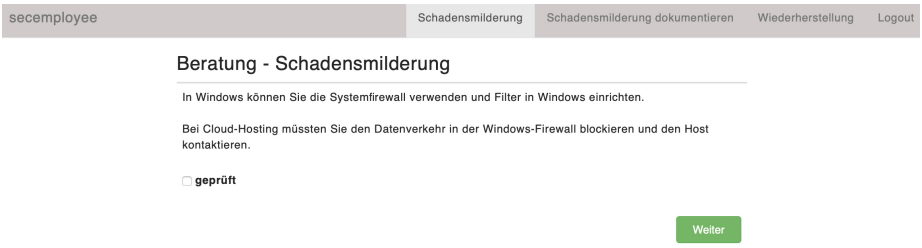

Figure 33: Security Employee Ansicht (Angriffsart ausgewählt)

Dem Security Employee steht nach dem Anmelden das Dokumentieren der Schadensmilderung zur Verfügung. Hier muss auch die Angriffsart gewählt werden. Daraufhin wird die Beratungsansicht für die Schadensmilderung angezeigt.

Der Akteur kann die Checkbox markieren, wenn der entsprechende Beratungsschritt durchgeführt wurde.

Anschließend wird die Dokumentationsseite angezeigt, auf der die Schritte der Schadensmilderung dokumentiert werden können. Diese werden daraufhin als formatierte pdf-Datei gespeichert.

Der Security Employee kann sich auch das Wiederherstellungsdokument anzeigen lassen, das eine Backupliste beinhaltet. Anhand dieser kann festgestellt werden, wann ein Backup zuletzt durchgeführt wurde. Nachfolgend kann eine Dokumentation der einzelnen Schritte durchgeführt werden.

7.3 Implementierung des Prototyps

In diesem Unterkapitel wird nicht auf die komplette Entwicklung des Prototyps eingegangen, da diese viele Klassen und Methoden beinhaltet.

```
public String [] readErstAnalyseData(int r, int c, int c2, String angart) {
    XSSFWorkbook wobo = null;
    String [] arr = new String[2];
    try {
        FileInputStream file=new FileInputStream("/Users/dominikklapec/Documents/
        wobo = new XSSFWorkbook(file);
    } catch (Exception e) {
        e.printStackTrace();
    }
    XSSFSheet sh = wobo.getSheetAt(0);

    System.out.println("letzte Reihe:" + sh.getLastRowNum());

    if(r > sh.getLastRowNum()) {
        arr[0] = "";
        arr[1] = "";
        return arr;
    } else {
        Row row = sh.getRow(r);
        Cell cell = row.getCell(c);
        Cell cell2 = row.getCell(c2);
        arr[0] = cell.getStringCellValue();
        arr[1] = cell2.getStringCellValue();
        System.out.println("text:" + arr[0]);
        System.out.println("frage:" + arr[1]);

        return arr;
    }
}
```

Figure 34: Implementierung Erstanalyse (1)

Der erste Codeabschnitt (Figure 34) bezieht sich auf die Durchführung der Erstanalyse. Genauer gesagt wird hier einer der Beratungsschritte mit der dazugehörigen Frage für die entsprechende Angriffsart aus einem excel-File gele-

sen und anschließend dem Benutzer angezeigt. Um welchen Beratungsschritt es sich handelt, wird anhand des übergebenen int r Werts bestimmt.

```
public void writeData(int counter, String s, String angart) throws FileNotFoundException, IOException {
    try {
        FileInputStream file = new FileInputStream(new File("/Users/dominikklapec/Documents/workspace/mast

        XSSFWorkbook wobo = new XSSFWorkbook(file);
        XSSFSheet sh = wobo.getSheetAt(0);
        Cell c = sh.getRow(counter).getCell(4);
        c.setCellValue(s);

        file.close();

        FileOutputStream fileout = new FileOutputStream(new File("/Users/dominikklapec/Documents/workspace
        wobo.write(fileout);
        fileout.close();
        wobo.close();

    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

Figure 35: Implementierung Erstanalyse (2)

Bei diesem Abschnitt (Figure 35) wird das Schreiben der Antworten der Beratungsschritte in das excel-File gezeigt. Dafür wird unter anderem ein int counter benötigt, um die Reihe bestimmen zu können. Weiters werden noch der Antwortwert (Ja/Nein), der vom Benutzer ausgewählt wurde, und die entsprechende Angriffsart, übergeben.

```
public String readAntwort(String angart) {
    String antwort = "";

    try {
        FileInputStream file = new FileInputStream(new File("/Users/dominikklapec/Documents/

        XSSFWorkbook wobo = new XSSFWorkbook(file);
        XSSFSheet sh = wobo.getSheetAt(0);
        Cell cell = null;

        for(int i = 1; i <= sh.getLastRowNum(); i++) {
            cell = sh.getRow(i).getCell(4);
            antwort += cell.getStringCellValue() + ",";
        }

        file.close();
        wobo.close();
    } catch (Exception e) {
        e.printStackTrace();
    }

    return antwort;
}
```

Figure 36: Implementierung Erstanalyse (3)

In diesem Codeabschnitt werden die Antworten der Beratungsschritte aus dem excel-File des Angriffs herausgelesen, um im Nachhinein auszuwerten, ob der vermutete Angriff stattfindet und in welcher Phase sich dieser befindet. Dabei

wird mit Hilfe einer for-Schleife auf alle Reihen zugegriffen und der Antwortwert herausgelesen.

```
public String erstapt(String antwort) {
    antwort = antwort.replaceAll(",", " ");
    String [] s = antwort.split("\\s+");
    String ausgabe = "";
    String ausgabe2 = "";
    int count = 0;

    if(s[0].equals("nein") && s[1].equals("nein") && s[2].equals("nein") && s[3].equals("nein") && s[4].equal
        ausgabe = "Der Verdacht eines APT-Angriffs kann anhand der Erstanalyse nicht bestätigt werden.";
    } else {
        String [] phase = {"Reconnaissance", "Initial Access", "Execution", "Execution oder Lateral Movement"
        for (int i = 0; i < s.length; i++) {
            if(s[i].equals("ja")) {
                ausgabe2 = phase[i];
                count++;
            }
        }
        if(count >= 5) {
            ausgabe = "Der Verdacht eines APT-Angriffs kann anhand der Erstanalyse bestätigt werden. "
                    + "Es wird vermutet, dass der Angriff sich in der " + ausgabe2 + "-Phase befindet.";
        } else {
            ausgabe = "Der Verdacht eines APT-Angriffs kann anhand der Erstanalyse zwar nicht eindeutig bestä
                    + "jedoch wird eine weitere Behandlung und Analyse des Vorfalls vorgeschlagen. "
                    + "Es wird vermutet, dass der Angriff sich in der " + ausgabe2 + "-Phase befindet.";
        }
    }

    return ausgabe;
}
```

Figure 37: Implementierung Erstanalyse (4)

Im letzten Codeabschnitt wird gezeigt, wie ausgewertet wird, ob ein Angriff bestätigt wird oder nicht. Bei diesem Fall handelt es sich um die Erstanalyse eines APT-Angriffs. Um diesen Schritt durchführen zu können, müssen die vorher gelesenen Antworten übergeben werden.

8 Test des Prototyps im Rahmen einer Case Study

In diesem Kapitel wird der Prototyp getestet und beurteilet. Dabei werden die, im Kapitel "Anforderungen an das zu entwickelnde System" definierten, Anforderungen geprüft. In dieser Case Study wird davon ausgegangen, dass einem Unternehmen ein Sicherheitsvorfall gemeldet wurde. Es deutet auch alles daraufhin, dass der Angriff sich in einem fortgeschrittenen Zustand befindet und bedeutsame firmenspezifische Daten herausgefiltert wurden beziehungsweise werden. Präzisiert wird heute Morgen um 09:12 ein APT-Angriff gemeldet. Der Security Manager organisiert sofort ein Meeting und weist die zuständigen Personen für den Sicherheitsvorfall zu.

8.1 Erstanalyse

Nachdem die Angriffsart APT vom Security Analyst gewählt wurde, werden die einzelnen Beratungsschritte der Erstanalyse, die vorher ausgearbeitet wurden, nacheinander angezeigt und beantwortet. Aus Übersichtlichkeitsgründen wird hier die Beschreibung der einzelnen Schritte nicht angezeigt, sondern es wird nur hingewiesen, zu welcher Phase sie gehört. Dies kann bei Bedarf im excel-File erstanalyse_*angriffsart*.xslx angesehen werden. Es wurden alle Schritte durch den Security Analyst durchgeführt und folgende Antworten bei den einzelnen Beratungsschritten ausgewählt:

- Beratungsschritt 1:
  - Phase: Reconnaissance
  - Antwort: Ja
- Beratungsschritt 2:
  - Phase: Initial Access
  - Antwort: Ja
- Beratungsschritt 3:
  - Phase: Execution
  - Antwort: Ja
- Beratungsschritt 4:
  - Phase: Execution oder Lateral Movement
  - Antwort: Ja
- Beratungsschritt 5:
  - Phase: Discovery
  - Antwort: Ja

- Beratungsschritt 6:
  - Phase: Persistence
  - Antwort: Ja
- Beratungsschritt 7:
  - Phase: Persistence
  - Antwort: Ja
- Beratungsschritt 8:
  - Phase: Persistence
  - Antwort: Nein
- Beratungsschritt 9:
  - Phase: Priviledge Escalation
  - Antwort: Ja
- Beratungsschritt 10:
  - Phase: Defense Evasion
  - Antwort: Ja
- Beratungsschritt 11:
  - Phase: Discovery
  - Antwort: Ja

Basierend darauf wurde folgende Rückmeldung angezeigt: **Der Verdacht eines APT-Angriffs kann anhand der Erstanalyse bestätigt werden. Es wird vermutet, dass der Angriff sich in der Discovery-Phase befindet.**

Daraufhin werden die wichtigsten Aspekte, die gesammelt wurden, vom Security Analyst dokumentiert. Anschließend wird daraus eine formatierte pdf-Datei erstellt, die sich folgendermaßen darstellt:

1. Umfang: Fast komplettes System betroffen
2. Status: Fortgeschritten

8.2 Auswirkungsbewertung & Prioritätsvergabe

Basierend auf dem letzten Schritt bewertet der Security Analyst die drei angebotenen Auswirkungskategorien folgendermaßen:

- Funktionale Auswirkung: Keine
- Informationsauswirkung: Datenschutzverletzung
- Wiederherstellbarkeit: Regulär

Mit Hilfe der vorher bewerteten Auswirkungen wird im nächsten Schritt die Prioritätsstufe vergeben. Dabei wird dem Security Manager Folgendes vorgeschlagen: **Die Prioritätsstufe wurde anhand der Auswirkungen auf Hoch eingeschätzt! Falls Sie mit dem Vorschlag nicht einverstanden sind, dann können Sie die Prioritätsstufe anpassen!**

Der Security Manager entscheidet sich dafür, die vorgeschlagene Priorität zu übernehmen und meldet den Vorfall bei den internen und externen Partnern.

8.3 Schadensmilderung

Nachdem der Vorfall gemeldet wurde, kann mit dem nächsten Schritt, der Schadensmilderung, begonnen werden. Dabei werden dem Security Employee die einzelnen Beratungsschritte für die Schadensmilderung angezeigt. Der Security Employee führt fast alle vorgeschlagenen Schritte durch und markiert die Checkboxen. Aus Übersichtlichkeitsgründen wird hier die Beschreibung der einzelnen Schritte nicht angezeigt. Dies kann bei Bedarf im excel-File schaden_*angriffsart*.xslx angesehen werden. Es wurden folgende Beratungsschritte geprüft:

- Beratungsschritt 1: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 2: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 3: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 4: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 5: nicht geprüft
  - Checkbox-Wert: Nein
- Beratungsschritt 6: nicht geprüft

  - Checkbox-Wert: Nein

Daraufhin werden zuerst die durchgeführten Schritte vom Security Employee dokumentiert und im Nachhinein wird daraus eine formatierte pdf-Datei generiert.

8.4 Analyse

Anschließend kann der Security Analyst mit der genaueren Analyse fortfahren. Dabei werden wie bei der Schadensmilderung die Beratungsschritte für die Analyse angezeigt. Der Security Analyst führt die Analyseschritte durch und klickt die geprüft-Checkbox an. Auch hier wird aus Übersichtlichkeitsgründen nicht die Beschreibung der einzelnen Schritte angezeigt. Dies kann bei Bedarf im excel-File banalyse_*angriffsart*.xslx angesehen werden. Es wurden folgende Beratungsschritte geprüft:

- Beratungsschritt 1: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 2: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 3: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 4: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 5: nicht geprüft
  - Checkbox-Wert: Nein
- Beratungsschritt 6: nicht geprüft
  - Checkbox-Wert: Nein
- Beratungsschritt 7: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 8: geprüft
  - Checkbox-Wert: Ja
- Beratungsschritt 9: nicht geprüft
  - Checkbox-Wert: Nein

Abschließend werden die gesammelten Aspekte vom Security Analyst dokumentiert und die gemachten Screenshots ausgewählt. Daraufhin wird daraus eine formatierte pdf-Datei erstellt, die folgendes beinhaltet:

1. IP-Adresse des Betroffenen: 192.168.12.1
2. OS des Betroffenen: Windows
3. IP-Adresse des Angreifers: 200.10.110.177
4. Land des Angreifers: Austria
5. Stadt des Angreifers: Vienna

8.5 Wiederherstellung

Nachfolgend kann der Security Employee die Wiederherstellung des normalen Betriebes fortführen. Zur Hilfe wird die angebotene Funktion des Systems, das die einzelnen Backups mit Datum und Uhrzeit anzeigt, verwendet. Dabei werden die letzten fünf Backups dargestellt, die entweder grün sind, wenn diese als sicher gelten, oder rot, wenn diese als unsicher zu betrachten sind. Dem Security Employee wurde Folgendes angezeigt:

- back_v1.3
  - Textfarbe: grün
- back_v1.4
  - Textfarbe: grün
- back_v1.5
  - Textfarbe: grün
- back_v1.6
  - Textfarbe: grün
- back_v1.7
  - Textfarbe: rot

Der Security Employee verwendet das letzte sichere Backup "back_v1.6" und führt die Systemwiederherstellung durch. Nachdem alles erneuert im Betrieb ist, werden die Patches installiert, alle Passwörter geändert und das System gehärtet. Zusätzlich wird auch die Überwachung erhöht. Abschließend werden alle durchgeführten Schritte dokumentiert und es wird eine pdf-Datei daraus generiert.

8.6 Aktualisierung & Abschlussbericht

Zum Schluss kann der Security Manager den Reaktionsablauf auswerten. Dafür verwendet dieser die Aktualisierungsfunktion. Hier wählt der Benutzer die Angriffsart APT aus und wertet den Ablauf aus. Nach der automatischen Auswertung wird folgende Rückmeldung angezeigt: **Die Gesamtreaktionszeit wurde nicht überschritten. Die Dokumentationsvorgaben wurden nicht eingehalten. Die Schadensmilderungsschritte sollten genauer beachtet werden, da diese die Schadenshöhe des Angriffs reduzieren oder auch zukünftige Angriffe vermeiden können.**

Anschließend wird der, darunter angezeigte, Reaktionsplan vom Security Manager aktualisiert und gespeichert.

Zum Schluss wird beim Abschlussmeeting ein Bericht vom Security Analyst erstellt. Dieser beantwortet folgende angezeigte Fragen:

1. Was genau ist passiert und zu welchem Zeitpunkt?
   - Heute Morgen um 09:12 wurde ein Verdacht eines APT-Angriffs gemeldet.
2. Wie gut sind Mitarbeiter und Management mit dem Vorfall umgegangen?
   - Im Großen und Ganzen wurde der Vorfall gut bearbeitet, jedoch muss mehr Wert auf die Einhaltung der Dokumentationsvorgaben und Schadensmilderungsschritte gelegt werden.
3. Welche Informationen werden früher benötigt?
   - Bei diesem Punkt wurde kein Verbesserungsbedarf erkannt.
4. Wurden Schritte oder Maßnahmen ergriffen, die die Wiederherstellung möglicherweise behindert haben?
   - Nein, die Wiederherstellung wurde nicht behindert.
5. Was würden Mitarbeiter und Management beim Auftreten eines ähnlichen Vorfalls anders machen?
   - Die Mitarbeiter sollten mehr Acht auf die Schadensmilderungsschritte geben. Allgemein müssen alle auch darauf achten, die Dokumentationsvorgaben einzuhalten.
6. Wie könnte der Informationsaustausch mit anderen Organisationen verbessert werden?
   - Mit Hilfe der aktuell verwendeten E-Mail Unterstützung ist der Informationsaustausch ausreichend gut organisiert.

Aus diesen Antworten wird ein Abschlussbericht als pdf-Datei generiert. Der Prozess wurde somit vom Reaktionsteam um 12:05 erfolgreich abgeschlossen.

9 Diskussion der Ergebnisse

In diesem Kapitel werden die Ergebnisse diskutiert, die sich aus dem vorherigen Kapitel "Test des Prototyps im Rahmen einer Case Study" ergeben. Dabei wird auf Erstanalyse, Auswirkungsbewertung, Prioritätsvergabe, Schadensmilderung, Analyse, Wiederherstellung, Aktualisierung und Abschlussbericht eingegangen.

Bei der Erstanalyse kann beobachtet werden, dass die Angriffsart APT anhand der Beratungsschritte bestätigt wurde. Zusätzlich wurde dabei noch die Discovery-Phase eingeschätzt. Bei der genaueren Betrachtung der Antworten kann festgestellt werden, dass fast alle Beratungsschritte, außer Beratungsschritt 6, mit Ja beantwortet wurden. Somit ist die Bestätigung der Angriffsart APT korrekt, da mindestens ein Beratungsschritt nicht mit einem Nein-Wert versehen ist. Auch die eingeschätzte Phase, in der sich der Angriff befindet, kann als angemessen betrachtet werden, da der letzte Beratungsschritt, der mit Ja beantwortet wurde, sich in der Discovery-Phase befindet. Wie früher erwähnt, entspricht jeder Schritt einer bestimmten Phase eines Angriffs, was unter anderem die Erstellung einer Vermutung leichter macht. Weiters wurde eine formatierte pdf-Datei mit den wichtigsten Aspekten der Erstanalyse erstellt. Im Prototyp wurde vor der Dokumentation vorgeschlagen, welche Punkte auf jeden Fall beachtet werden sollen. Die pdf-Datei sollte außer dem Umfang, Status, die in dieser Dokumentation angegeben wurden, noch die Schwachstellen und die Schritte beschreiben. Wie zu erkennen ist, wurden die zwei letzten Punkte nicht beachtet, was bedeutet, dass die Dokumentation nicht ordnungsgemäß durchgeführt wurde.

Bei der Auswirkungsbewertung und Prioritätsvergabe kann festgestellt werden, dass die anfängliche Bewertung korrekt durchgeführt wurde, da der Angriff fortgeschritten ist und sich in der Discovery-Phase befindet. Die Phase kann ein Anzeichen dafür sein, dass bedeutsame Daten aus dem Unternehmen ausspioniert werden. Daher wird die Informationsauswirkung korrekterweise als Datenschutzverletzung gesehen. Da keine funktionalen Auswirkungen erkannt wurden und die Wiederherstellbarkeit regulär durchgeführt werden kann, wurden die Standardwerte übernommen. Bei der Vergabe der Priorität, die anhand der Auswirkungen eingeschätzt wird, wurde die Stufe Hoch vergeben und vom Security Manager übernommen. Das Ergebnis des Prototyps kann als korrekt gesehen werden, da es sich hier um eine Datenschutzverletzung handelt, die auf jeden Fall als hoch einzuschätzen ist.

Der Prozess wird mit der Schadensmilderung weitergeführt, wobei die Beratungsschritte zu sehen sind, die vom Security Employee geprüft wurden. Dabei kann beobachtet werden, dass vier von sechs Beratungsschritten geprüft wurden. Basierend auf den Checkbox-Werten, wird bei der Aktualisierung entschieden, ob die Schadensmilderung genügend gut durchgeführt wurde. Abschließend wurde noch eine korrekt formatierte pdf-Datei mit den abgewickelten Schritten generiert.

Weiters kommt es zu einer genaueren Analyse des Angriffs, wobei die Beratungsschritte, die geprüft wurden, zu betrachten sind. Dabei ist zu erkennen, dass sechs von neun Schritten durchgeführt wurden, das heißt die Beratungsschritte 5, 6, 9 wurden nicht kontrolliert. Diese werden, wie auch die Beratungsschritte der Schadensmilderung, einen Einfluss bei der Entscheidung, ob eine Aktualisierung notwendig ist, haben. Zusätzlich wurde eine formatierte pdf-Datei mit den gesammelten Spuren erstellt. Dafür wurde dem Security Analyst vorher angezeigt, welche Punkte unbedingt dokumentiert werden sollten. Wie zu sehen ist, beinhaltet die erstellte pdf-Datei die IP-Adresse des Betroffenen, OS des Betroffenen, IP-Adresse des Angreifers, Land des Angreifers und Stadt des Angreifers. Im Vergleich zu den vorgeschlagenen Punkten fehlt der Hostname sowohl des Betroffenen als auch des Angreifers. Dies wird auch auf die Aktualisierung des Reaktionsplans Einfluss haben.

Es folgt die Wiederherstellung, bei der dem Security Employee die Backups vorgeschlagen wurden, die als sicher zu betrachten sind. Wie zu sehen ist, werden die letzten fünf Backups angezeigt, die entweder mit einer grünen oder roten Textfarbe gekennzeichnet sind. Nachdem geprüft wurde, wann der Vorfall gemeldet und wann die Backups durchgeführt wurden, werden die sicheren Backups im Prototyp korrekt in der Farbe Grün angezeigt. Schließlich wurde ein formatiertes pdf-Dokument mit den Wiederherstellungsschritten erfolgreich erstellt.

Zum Schluss kommt es zur Aktualisierung und dem Abschlussbericht. Dabei wird auf der einen Seite geschaut, ob eine Aktualisierung notwendig ist, auf der anderen Seite wird ein Bericht erstellt, der die Antworten auf gestellte Fragen beinhaltet. Bei der Auswertung des Reaktionsablaufs wurde dem Security Manager korrekterweise folgende Meldung angezeigt: Die Gesamtreaktionszeit wurde nicht überschritten. Die Dokumentationsvorgaben wurden nicht eingehalten. Die Schadensmilderungsschritte sollten genauer beachtet werden, da diese die Schadenshöhe des Angriffs reduzieren oder auch zukünftige Angriffe vermeiden können.

Wie zu sehen ist, wurde die Gesamtreaktionszeit eingehalten, da bei der Prioritätsstufe Hoch eine Gesamtreaktionszeit von 4 Stunden vorgesehen ist, die hier nicht überschritten wurde. Zusätzlich wurden die maximalen Zeiten zu den einzelnen Phasen nicht überstiegen. Andernfalls würde der Benutzer eine Rückmeldung bekommen, in welcher Phase die Zeit überschritten wurde. Die Dokumentationsvorgaben wurden aufgrund der vorher erstellten pdf-Dateien der Erstanalyse und Analyse nicht ausreichend genug eingehalten. Auch die Schadensmilderungsschritte wurden anhand der Beratungsschritte nicht angemessen durchgeführt. Bei dem Abschlussbericht wurden sechs von acht Fragen, die den Reaktionsablauf betreffen, durch den Security Analyst beantwortet und erfolgreich in Form eines formatierten pdf-Dokuments gespeichert.

10 Schlussfolgerungen und Erweiterungsmöglichkeiten

Es ist enorm wichtig, sich genug Zeit für die Vorbereitung auf einen Sicherheitsvorfall zu nehmen. Dazu zählt das Definieren von Vorfallsrichtlinien, das Erstellen von Plänen, das Einschulen von Mitarbeitern, das Durchführen eines Incident Response Trainings und das Auswerten der Ergebnisse. Dabei ist das regelmäßige Wiederholen des Vorbereitungsprozesses notwendig. Dies ist ein Grundbaustein für die effiziente Durchführung des Reaktionsablaufs bei einem erfolgreichen Angriff. In Bezug auf die Angriffsarten liegt der Fokus der Masterarbeit auf APT, DDoS und Ransomware, die als weit verbreitet zu sehen sind. Vor allem für Unternehmen können sie großen Schaden anrichten, da sie zu Ausspionierung von Daten oder auch zu finanziellem Schaden führen können. Daher ist es wichtig, den kompletten Reaktionsablauf von der Identifikation- bis zur Lessons Learned-Phase zu unterstützen und so den Schaden so gering wie möglich zu halten. Dahingehend unterstützen die erstellten Modelle, die den Ablauf der Reaktionsphase darstellen. Der, basierend darauf, entwickelte Prototyp unterstützt den Benutzer bei der Bearbeitung des Vorfalls unter anderem mit Hilfe einer Beraterfunktion, wobei die Erstanalyse, Analyse und Schadensmilderung erleichtert werden oder er hilft bei der automatischen Auswertung des Reaktionsablaufs. Die Daten selbst, die als Input verwendet werden, basieren auf dem MITRE ATT&CK Framework [4].

Es gibt auch Erweiterungsmöglichkeiten, die die Unterstützung der Reaktionsphase verbessern können. Eine Option kann das Ändern der Speicherart der Inputdaten sein. Da die Menge der Daten, die für die Beraterfunktionen der Erstanalyse, Schadensmilderung und Analyse benötigt werden, zurzeit überschaubar ist, werden diese in einem excel-File gespeichert und herausgelesen. Es kann jedoch überlegt werden, bei einer größeren Anzahl von Daten auf eine Datenbank umzusteigen. Ein anderer Erweiterungspunkt kann im Bereich der Dokumentation festgestellt werden. Bei dem aktuellen Prototyp wird der Benutzer bei der Durchführung der Dokumentationen darauf hingewiesen, in welcher Form dies zu tun ist. Zukünftig kann dafür ein gewisser Standard von Dokumentationsvorgaben zur Verfügung stehen, mit dem der Prototyp erweitert werden kann.

References

[1] Najla Aldaraani and Zeenat Begum. Understanding the impact of ransomware: A survey on its evolution, mitigation and prevention techniques. IEEE, 2018.

[2] Adel Alshamrani, Sowmya Myneni, Ankur Chowdhary, and Dijiang Huan. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE, 2015.

[3] Nor Badrul Anuar, Maria Papadaki, Steven Furnell, and Nathan Clarke. A response strategy model for intrusion response systems. Springer, 2012.

[4] MITRE ATT&CK. Mitre att&ck framework. `https://attack.mitre.org/`, Accessed: 2020-12-16.

[5] Reza Barkhi, Elizabeth T. Schwartz, and Stephen J. Seifert. Denistifying cybersecurity: An internal mis and it audit self-assessment tool. ProQuest, 2016.

[6] Pauline Bowen, Joan Hash, and Mark Wilson. Information security handbook: A guide for managers. NIST Special Publication 800-100, 2006.

[7] Saranya Chandran, Hrudya P, and Prabaharan Poornachandran. An efficient classification model for detecting advanced persistent threat. IEEE, 2015.

[8] Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone. Computer security incident handling guide. NIST Special Publication 800-61 Revision 2, 2012.

[9] Adenekan Dedeke. Cybersecurity framework adoption: Using capability levels for implementation tiers and profiles. IEEE, 2017.

[10] Elena Doynikova and Igor Kotenko. The multi-layer graph based technique for proactive automatic response against cyber attacks. IEEE, 2018.

[11] Europol. Internet organised crime threat assessment (iocta). European Cybercrime Centre (EC3), 2018.

[12] THE APACHE SOFTWARE FOUNDATION. Apache pdfbox. `https://pdfbox.apache.org`, Accessed: 2020-06-27.

[13] THE APACHE SOFTWARE FOUNDATION. Apache poi. `https://poi.apache.org`, Accessed: 2021-01-12.

[14] Bundesamt für Sicherheit in der Informationstechnik. Studie zur itsicherheit in kleinen und mittleren unternehmen. `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile`, 2011.

[15] Bundesamt für Sicherheit in der Informationstechnik. Auswahlkriterium für quaifizierte atp-response-dienstleister. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Auswahlkriterien_APT-Response_Dienstleister.pdf, 2017.

[16] Bundesamt für Sicherheit in der Informationstechnik. Abwehr von ddos-angriffen. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_002.pdf?__blob=publicationFile&v=1, 2018.

[17] Bundesamt für Sicherheit in der Informationstechnik. Ransomware: Bedrohungslage, prävention & reaktion 2019. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf, 2019.

[18] Bundesamt für Sicherheit in der Informationstechnik. Der.2.2: Vorsorge für die it-forensik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/05_DER_Detektion_und_Reaktion/DER_2_2_Vorsorge_fuer_die_IT_Forensik_2020.pdf?__blob=publicationFile&v=1, 2020.

[19] Bundesamt für Sicherheit in der Informationstechnik. Erste hilfe bei einem schweren it-sicherheitsvorfall version 1.1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf, 2020.

[20] Bundesamt für Sicherheit in der Informationstechnik. Der.2.1: Behandlung von sicherheitsvorfällen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2021.pdf?__blob=publicationFile&v=2, 2021.

[21] Schutzwerk GmbH. Incident response management. https://www.schutzwerk.com/de/40/Incident-Response-Management.html, Accessed: 2020-02-01.

[22] Raza Hasan, Salman Mahmood, Akshyadeep Raghav, and M. Asim Hasan. Artificial intelligence based model for incident response. IEEE, 2011.

[23] Jonathan Hedley. jsoup html parser. https://jsoup.org, Accessed: 2021-01-25.

[24] Cathrine Hove, Marte Tarnes, Maria B. Line, and Karin Bernsmed. Information security incident management: Identified practice in large organizations. IEEE, 2014.

[25] Yadigar Imamverdiyev. An information security incident prioritization method. IEEE, 2013.

[26] Kimoon Jeong, Junhyung Park, Minsoo Kim, and Bongnam Noh. A security coordination model for an inter-organizational information incidents response supporting forensic process. IEEE, 2008.

[27] Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim. Ddos flooding attack detection through a step-by-step investigation. IEEE, 2011.

[28] Stefan Kempter. Checkliste incident-priorität. `https://wiki.de.it-processmaps.com/index.php/ITIL-Checklisten`, 2020.

[29] Md Khamruddin and Ch. Rupa. A rule based ddos detection and mitigation technique. IEEE, 2012.

[30] Patrick Kral. Incident handler's handbook. Sans Institute Information Security Reading Room, 2020.

[31] Trevor Lamis. A forensic approach to incident response. ACM, 2010.

[32] Shen Lei and Scitech Lawyer. The nist cybersecurity framework: Overview and potential impacts. ProQuest, 2014.

[33] Maria B. Line, Inger Anne Tondel, and Martin G. Jaatun. Information security incident management: Planning for failure. IEEE, 2014.

[34] Nate Lord. What is security incident management? `https://digitalguardian.com/blog/what-security-incident-management-cybersecurity-incident-management-process`, 2018.

[35] Kevin Mepham, Panos Louvieris, Gheorghita Ghinea, and Natalie Clewley. Dynamic cyber-incident response. IEEE, 2014.

[36] Brahim ID Messaoud, Karim Guennoun, Mohamed Wahbi, and Mohamed Sadik. Advanced persistent threat: new analysis driven by life cycle phases and their challenges. IEEE, 2016.

[37] Savita Mohurle and Manisha Patil. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 2017.

[38] Sharma Divya Mukesh. An analysis technique to detect ransomware threat. IEEE, 2018.

[39] NASA. Information security handbook. Incident Response Management: NASA Information Security Incident Management, 2011.

[40] Daniel F Netto, Shony K M, and Elizabeth Rose Lalso. An integrated approach for detecting ransomware using static and dynamic analysis. IEEE, 2018.

[41] NIST. Cybersecurity framework version 1.0. https://www.nist.gov/cyberframework/framework, 2014.

[42] NIST. Cybersecurity framework version 1.1. https://www.nist.gov/cyberframework/framework, 2018.

[43] Sven Ossenbu, Jessica Steinberger, and Harald Baier. Towards automated incident handling: How to select an appropriate response against a network-based attack? IEEE, 2015.

[44] Faisal Quader, Vandana Janeja, and Justin Stauffer. Persistent threat pattern discovery. IEEE, 2015.

[45] Margaret Rouse. Vorfallreaktionsplan – incident response plan (irp). https://www.computerweekly.com/de/definition/Vorfallreaktionsplan-Incident-Response-Plan-IRP, Accessed: 2020-02-01.

[46] Scott J. Shackelford, Andrew A. Proia, Brenton Martell, and Amanda N. Craig. Toward a global cybersecurity standard of care: Exploring the implications of the 2014 nist cybersecurity framework on shaping reasonable national and international cybersecurity practices. HeinOnline, 2015.

[47] Nuno Teodoro, Luis Goncalves, and Carlos Serrao. Nist cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements. IEEE, 2015.

[48] Darnell Washington. Cybersecurity assessments: An overview. ProQuest, 2018.

[49] Zeti Suhana Zainudin and Nurul Nuha Abdul Molok. Advanced persistent threats awareness and readiness: A case study in malaysian financial institutions. IEEE, 2018.

[50] Qingyun Zhang, Huan Li, and Jinsong Hu. A study on security framework against advanced persistent threat. IEEE, 2017.