HAW HAMBURG

MASTER THESIS
Lars Kowoll

Information Security Incident Management an der HAW Hamburg

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Engineering and Computer Science
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Lars Kowoll

Information Security Incident Management an der HAW Hamburg

Masterarbeit eingereicht im Rahmen der Masterprüfung
im Studiengang *Master of Science Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachterin: Prof. Dr. Bettina Buth

Eingereicht am: 06. Dezember 2024

Lars Kowoll

Thema der Arbeit

Information Security Incident Management an der HAW Hamburg

Stichworte

Information Security Incident Management, Incident Handling, ISO/IEC 27035, BPMN

Kurzzusammenfassung

Die vorliegende Arbeit befasst sich mit der Implementierung eines Information Security Incident Managements an der HAW Hamburg. Das Ziel der Arbeit ist es einen Incident Handling Prozess auf Basis der ISO/IEC 27035 zu konzipieren. Um das Incident Handling zu modellieren, wurden im ersten Schritt die Meldepflichten sowie freiwillige Meldepraktiken der Hochschule betrachtet. Des Weiteren wurde in der vorliegenden Arbeit eine Methode entwickelt, um Information Security Incidents bezüglich ihrer Schweregrade zu kategorisieren. Die Kriterien *Ausmaß der Vorfallsart*, *Schutzbedarf* und *Wiederherstellungsaufwand* wurden dabei herangezogen.

Die Modellierung des Incident Handlings beginnt mit der Benennung der am Prozess beteiligten Rollen. Diese werden anschließend in Bezug zum *CSIRT Services Roles and Competencies* von *FIRST* gesetzt. Die Darstellung des Prozesses erfolgte in mehreren BPMN-Diagrammen. Die einzelnen Aktivitäten in den Phasen des Incident Handlings wurden mit Hilfe von RASCI-Matrizen den identifizierten Rollen zugeordnet. Dadurch sollte eine klare und eindeutige Zuordnung gewährleistet sowie Kompetenzkonflikten vorgebeugt werden. Des Weiteren wurde in der vorliegenden Arbeit untersucht, an welchen Stellen und aus welchem Grund von den Empfehlungen der ISO/IEC 27035 abgewichen wurde.

Die Evaluierung des Prozesses erfolgte anhand zweier exemplarischer Szenarien. Zum einen wurde eine Phishing Attacke untersucht, zum anderen Datenexfiltration über DNS Tunneling. Es konnte nachgewiesen werden, dass der Prozess eine geeignete und tragfähige Konzeption darstellt, um an der HAW Hamburg Incident Handling systematisch durchzuführen und zu implementieren. Im Rahmen der Evaluierung wurden jedoch auch mehrere Verbesserungspotenziale für den Incident Handling Prozess identifiziert, die bei der Implementierung umgesetzt werden müssen.

Lars Kowoll

Title of Thesis

Information Security Incident Management at the HAW Hamburg

Keywords

Information Security Incident Management, Incident Handling, ISO/IEC 27035, BPMN

Abstract

This thesis deals with the implementation of an Information Security Incident Management at the HAW Hamburg. The aim of the thesis is to design an incident handling process based on the ISO/IEC 27035. In order to model the incident handling process, the reporting obligations and voluntary reporting practices of the university were considered in the first step. Furthermore, a method was developed in this thesis to categorize information security incidents according to their severity. The criteria *type of incident*, *Schutzbedarf* and *recovery effort* were used.

The modeling of incident handling begins with naming the roles involved in the process. These are then set in relation to the *CSIRT Services Roles and Competencies* of *FIRST*. The process was visualized in several BPMN diagrams. The individual activities in the incident handling phases were assigned to the identified roles with the help of RASCI matrices. This was intended to ensure a clear and unambiguous assignment and prevent conflicts of competence. Furthermore, this thesis examined where and for what reason the requirements of ISO/IEC 27035 were deviated from.

The process was evaluated using two exemplary scenarios. Firstly, a phishing attack was examined, and secondly, data exfiltration via DNS tunneling. It was demonstrated that the process is a suitable and viable concept for systematically carrying out and implementing incident handling at HAW Hamburg. However, the evaluation also identified several potential improvements to the incident handling process that need to be realized during implementation.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungen

BPMN *Business Process Model and Notation.*

BSI *Bundesamt für Sicherheit in der Informationstechnik.*

CC *Coordination Center.*

CERT *Computer Emergency Response Team.*

CISA *Cybersecurity and Infrastructure Security Agency.*

CISO *Chief Information Security Officer.*

CSIRT *Computer Security Incident Response Team.*

DDoS *Distributed Denial of Service.*

DNS *Domain Name System.*

DORA *Digital Operational Resilience Act.*

DSGVO *Datenschutz-Grundverordnung.*

ENISA *Agentur der Europäischen Union für Cybersicherheit.*

FH *Fachhochschule.*

FHH *Freien und Hansestadt Hamburg.*

FIRST *Forum of Incident Response and Security Teams.*

HAW *Hochschule für Angewandte Wissenschaften.*

IDS *Intrusion Detection System.*

IEC *International Electrotechnical Commission.*

ISIM *Information Security Incident Management.*

ISMS *Information Security Management System.*

ISO *International Organization for Standardization.*

ITIL *Information Technology Infrastructure Library.*

ITSC *Informationstechnik Service Center.*

ITSM *IT-Service-Management.*

NCISS *National Cyber Incident Scoring System.*

NIS *Network and Information Security.*

NIST *National Institute of Standards and Technology.*

SIEM *Security Information and Event Management.*

SP *Special Publication.*

SQL *Structured Query Language.*

1 Einleitung

Die zunehmende Digitalisierung führt zu einer Vergrößerung der Angriffsfläche von Unternehmen, Behörden und wissenschaftlichen Einrichtungen, damit steigen auch die Angriffsvektoren, die von den Angreifern genutzt werden können [8]. Hochschulen sehen sich dabei mit einer besonderen Herausforderung konfrontiert, da sie, bedingt durch ihren Lehre- und Forschungsbereich, über stark heterogene Systemlandschaften verfügen [58]. Deutlich wird das mit der Aussage von Prof. Dr. Sebastian Schinzel[1], der im Rahmen des Cyberangriffs auf die *Fachhochschule* (FH) Münster Folgendes sagte:

> *„Als Hochschule können wir unsere IT nicht wasserdicht abschotten wie beispielsweise eine Bank. Forschung und Lehre leben davon, dass wir uns zu einem gewissen Grad öffnen [33].“*

Wie häufig Hochschulen Ziel von Angriffen werden, zeigt sich bei der Betrachtung der Website von Dr. Andreas Heil[2]. Die Website führt erfolgreiche Angriffe auf Hochschulen in Deutschland auf, wenn sie in der Presse Erwähnung finden. Der erste Eintrag erfolgte am 20.06.2018, bis heute waren 33 weitere Hochschulen betroffenen. Auch die *Hochschule für Angewandte Wissenschaften* (HAW) Hamburg ist auf der Website vertreten, hier wurde am 29.12.2022 ein umfassender Cyberangriff detektiert [2]. Dabei sind Hochschulen auch einer Vielzahl von Angriffsversuchen oder sicherheitsrelevanten Ereignissen ausgesetzt, ohne dass sie seitens der Hochschule öffentlich bekanntgegeben oder systematisch erfasst werden. Schon bei einem Verdacht oder einer Warnmeldung von Systemen, sollte eine systematische Aufarbeitung erfolgen, um möglichst frühzeitig reagieren zu können. Dadurch besteht die Möglichkeit, den zeitlichen Ausfall von Systemen zu minimieren und den Informationsabfluss, im Falle eines erfolgreichen Angriffs, zu verringern oder sogar ganz zu unterbinden [16].

Eine solche systematische Aufarbeitung von Verdachtsmomenten bzw. Events oder Sicherheitsvorfällen bzw. Incidents, wird unter dem Namen *Information Security Incident*

[1] IT-Sicherheitsbeauftragter der FH Münster
[2] https://aheil.de/edusec/

Management (ISIM) zusammengefasst. Im Rahmen der vorliegenden Arbeit erfolgt eine Betrachtung von Incidents immer aus der Perspektive der Informationssicherheit. Sofern Incidents im Sinne der *Information Technology Infrastructure Library* (ITIL), also als Geschäftsvorfall, betrachtet werden, wird dies explizit erwähnt.

1.1 Motivation

Die Arbeit ist im Rahmen des Projekt InSights entstanden. Das Projekt hat das Ziel die Informationssicherheit der HAW Hamburg zu verbessern. Dabei werden Aspekte des IT-Grundschutzes betrachtet, wie z. B. Härtung von Systemen, Tests im Rahmen der IT-Sicherheit und Security Awareness. Der Fokus des Projekts liegt dabei auf dem *Informationstechnik Service Center* (ITSC), dem zentralen IT-Systembetreiber der HAW Hamburg. Ein zentrales Ziel des Projekts ist hierbei die Einführung eines Information Security Incident Managements auf Basis der ISO/IEC 27001.

1.2 Zielsetzung

Das Ziel der Arbeit ist es einen generischen Incident Handling Prozess zu konzipieren, welcher die Anforderungen der HAW Hamburg erfüllt. Basierend auf den Anforderungen der HAW Hamburg und den rechtlichen Anforderungen, die sich aus dem IT-Grundschutz des *Bundesamt für Sicherheit in der Informationstechnik* (BSI) ergeben, wurde in einer vorherigen Arbeit die ISO/IEC 27035 als am besten geeignetes Rahmenwerk identifiziert. Darauf aufbauend soll in dieser Arbeit der Incident Handling Prozess erarbeitet werden.

Bisher werden Incidents an der HAW Hamburg unsystematisch behandelt, die Bearbeitungsweise ist dabei abhängig von den jeweiligen Mitarbeitern, die je nach Erfahrung stark variieren kann. Der Prozess soll den Mitarbeitern ermöglichen, systematisch auf Incidents zu reagieren und ihnen Handlungssicherheit bei der Bearbeitung von Incidents geben. Um den Erfolg des Prozesses beurteilen zu können, soll eine Evaluierung durchgeführt werden.

Die HAW Hamburg verfügt über begrenzte personelle Ressourcen, daher soll ebenfalls ein Rollenkonzept erarbeitet werden, welches mit hoher Effizienz und Flexibilität funktioniert. Darüber hinaus soll sichergestellt werden, dass die angemessenen Ressourcen bei der Behandlung von Incidents eingesetzt werden können. Aus diesem Grund soll eine

Methode entwickelt werden, um Incidents zu kategorisieren. Diese beiden Aspekte sollen sich dabei auch im Incident Handling Prozess widerspiegeln.

1.3 Aufbau der Arbeit

In Kapitel 2 wird eine Einführung in das Thema ISIM gegeben. Dafür werden zunächst die Begrifflichkeiten Event, Potential Incident und Incident voneinander abgegrenzt. Weiterhin erfolgt eine Einordnung des Begriffs Information Security Incident Management. Außerdem wird in diesem Kapitel die Auswahl für das Rahmenwerk für die Modellierung des Incident Handlings Prozess erläutert.

In Kapitel 3 werden die Meldepflichten und freiwilligen Meldepraktiken der HAW Hamburg untersucht und erläutert. Darüber hinaus werden auch die Auswirkungen von der *Network and Information Security* (NIS)2-Richtlinie und der Verordnung *Digital Operational Resilience Act* (DORA) betrachtet.

In Kapitel 4 wird eine Methode entwickelt, um den Schweregrad bei Incidents zu bestimmen. Dabei werden Kriterien erarbeitet, die bei der Bestimmung des Schweregrads herangezogen werden.

Das Kapitel 5 behandelt die Modellierung des Incident Handlings an der HAW Hamburg. Zunächst werden die Rollen definiert und mit dem *Computer Security Incident Response Team (CSIRT) Services Roles and Competencies* von *Forum of Incident Response and Security Teams* (FIRST) verglichen. Es erfolgt eine Vorstellung der einzelnen Phasen des Incident Handlings. Mit Hilfe von RASCI-Matrizen werden die Phasen den identifizierten Rollen zugewiesen. Am Ende des Kapitels wird rekapituliert, an welchen Punkten von der ISO/IEC 27035 abgewichen wurde.

Das Kapitel 6 befasst sich mit der Evaluierung des Incident Handlings. Dafür werden zwei Szenarien betrachtet, zum einen eine Phishing Attacke, zum anderen eine Datenexfiltration über DNS Tunneling. Basierend auf den Szenarien wird der Incident Handling Prozess durchlaufen.

In Kapitel 7 erfolgt eine Zusammenfassung der Arbeit. Außerdem werden Verbesserungspotenziale, basierend auf der Evaluierung, aufgeführt und erläutert.

2 Grundlagen

In dem folgenden Kapitel wird zunächst eine terminologische Abgrenzung der Begriffe Events, Potential Incidents und Incidents vorgenommen. Danach wird ein Überblick über Incident Taxonomien gegeben. Außerdem werden wichtige Begriffe des Information Security Incident Management vorgestellt. Am Ende des Kapitels erfolgt ein kurzer Abschnitt zur Auswahl eines geeigneten Rahmenwerkes für ein ISIM an der HAW Hamburg.

2.1 Definition und Abgrenzung von Events, Potential Incidents und Incidents

Im Folgenden wird untersucht, was unter dem Begriff Incident zu verstehen ist und wie er entsteht. Ein Incident entsteht nicht ad hoc, sondern setzt beim Angegriffenen stets die Detektion eines Events voraus. Die Detektion von Events kann durch verschiedene Akteure oder von Werkzeugen, wie z. B. Meldungen von einem *Intrusion Detection System* (IDS), erfolgen [42]. In der *International Organization for Standardization* (ISO)/*International Electrotechnical Commission* (IEC) 27035 werden Events folgendermaßen definiert: *"Occurrence indicating a possible breach of information security or failure of controls"* [42]. Im Anschluss an die Erzeugung eines Events muss eine initiale Analyse erfolgen, um zu überprüfen, ob die potenzielle Verletzung der Informationssicherheit, wie sie in der Definition des Events beschrieben wird, tatsächlich eine potenzielle Verletzung ist und kein Fehlalarm [44]. Sollte dies bestätigt werden, wird ein Potential Incident ausgerufen. Ein Potential Incident ist demnach in seiner Aussagekraft in einer potenziellen Verletzung über ein Event, aber unter einem Incident zu stellen. Im Rahmen einer umfassenden Analyse wird durch einen Experten überprüft, ob tatsächlich eine Einstufung als Incident erforderlich ist. Ist dies der Fall, wird damit bestätigt, dass eine Verletzung der Informationssicherheit stattgefunden hat [46]; [47]. Incidents definiert die ISO/IEC 27035 wie folgt: *"One or multiple related and identified information security*

events that can harm an organization's assets or compromise its operations" [42]. In dieser Arbeit werden die Definitionen der ISO/IEC für Events und Incidents verwendet.

In der Abbildung 2.1 werden die Begriffe Event, Potential Incident und Incident in Beziehung zueinander gesetzt. Als Ausgangspunkt dient die wiederholte Falscheingabe eines Passworts. Ein *Security Information and Event Management* (SIEM) könnte dies als einen Brute-Force-Angriff interpretieren und ein Information Security Event erzeugen. Hierbei ist zu beachten, dass nicht jedes Event detektiert wird. Weiterhin führt nicht jedes Event zwangsläufig zu einem Potential Incident und ebenso wenig führt jeder Potential Incident zu einem Incident, da Fehlalarme oder falsche Analyseergebnisse auftreten können. Die Verjüngung des Trichterdiagramms dient der verstärkenden Darstellung der aussortierten Ereignisse. Dabei ist die Grafik in ihrem Verhältnis nicht als maßstabsgetreu zu interpretieren.

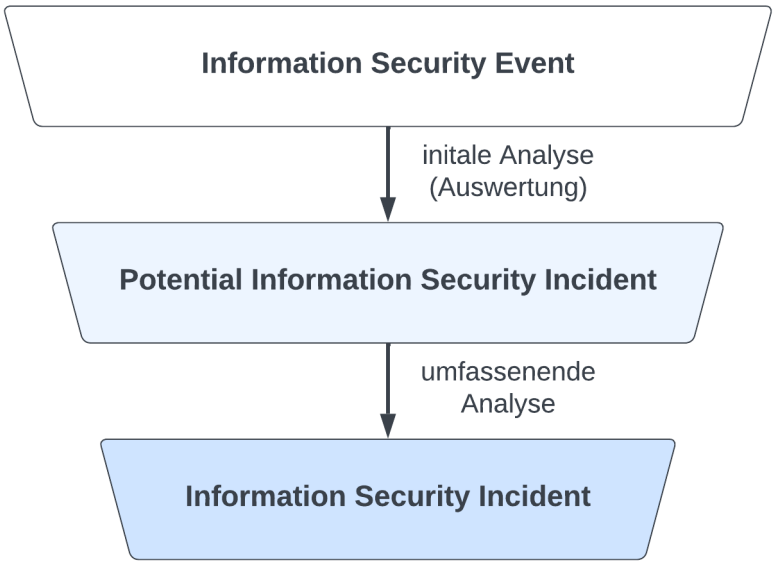

Abbildung 2.1: Beziehung zwischen Information Security Events, Information Security Potential Incidents und Information Security Incidents, eigene Darstellung

2.2 Incident Taxonomie

Um eine einheitliche Verwendung von Begriffen in einem bekannten Kontext zu gewährleisten, ist die Anwendung einer Taxonomie oft hilfreich. Eine Taxonomie stellt ein System zur Klassifikation von Objekten dar, welches in Form einer Baumstruktur organisiert ist. Die Anzahl der Verzweigungen ist abhängig von der Anzahl der Kategorien, welche erforderlich sind, um das Objekt taxonomisch zu beschreiben. In der Biologie werden beispielsweise sechs Kategorien verwendet, um Lebewesen zu beschreiben. Die Taxonomie umfasst die folgenden Hierarchieebenen: Reich, Stamm, Klasse, Ordnung, Familie und Gattung [5]. Im Folgenden werden die Anforderungen an eine Taxonomie dargestellt, die erfüllt sein müssen, damit sie sinnvoll eingesetzt werden kann, entnommen aus [36]:

- Sich gegenseitig ausschließend: Kategorien sollen sich nicht überlappen
- Vollständig: Alle Möglichkeiten sollen in der Taxonomie berücksichtigt werden
- Eindeutig: Es besteht keine Unsicherheit bei der Zuordnung
- Wiederholbar: Wiederholte Anwendung führt stets zum gleichen Ergebnis
- Anerkannt: Die Taxonomie ist allgemein anerkannt
- Nützlich: Ermöglicht Einblicke in den Untersuchungsbereich

Taxonomien werden nicht nur in der Biologie zur Klassifikation eingesetzt, sondern auch in der Informationssicherheit. Eine Taxonomie fördert hier die Vergleichbarkeit und den Austausch in der Informationssicherheit, indem über Organisationsgrenzen hinweg eine gemeinsame Sprache gesprochen wird [36]. Des Weiteren führt sie zu einer erhöhten Automatisierbarkeit der Incident Handling Prozesse [28].

Es existiert eine Vielzahl unterschiedlicher Taxonomien in der Informationssicherheit mit unterschiedlichen Schwerpunkten. Während Taxonomien existieren, die speziell zur Klassifikation von *Distributed Denial of Service* (DDoS) Angriffen konzipiert wurden, gibt es auch solche, die den gesamten Angriff sowie die entsprechende Verteidigungsstrategie klassifizieren [57]. Ein Beispiel für die letztgenannte Möglichkeit stellt AVOIDIT dar. Das Wort ist ein Akronym und besteht aus den Wörtern: Attack Vector, Operational Impact, Defense, Information Impact and Target. Die Wörter geben gleichzeitig die Kategorien der Taxonomie wieder. In Tabelle 2.1 wird ein Angriff mit AVOIDIT klassifiziert.

Dazu wurde ein beispielhafter Angriff durch *Structured Query Language* (SQL) Slammer[1] simuliert [57]. Der Angriff umfasst zwei Phasen. Zunächst überprüft die Schadsoftware, ob das Zielsystem verwundbar ist. Sollte dies der Fall sein, wird in der entsprechenden Anwendung ein Buffer Overflow ausgelöst[50].

Attack Vector	Operational Impact	Information Impact	Defense	Target
Misconfiguration	Installed Malware: Worm: Network Aware	Discovery	Mitigation: Whitelisting CAN-2002-0649	Network
Buffer Overflow	Installed Malware: Worm: Network Aware	Distort	Remediation: Patch System	Application

Tabelle 2.1: Taxonomische Darstellung des Angriffs durch SQL Hammer mit AVOIDIT, in Anlehnung an [57]

Im Gegensatz zu AVOIDIT, bei dem der gesamte Angriff im Vordergrund steht, fokussiert sich die Reference Security Incident Taxonomy von *Agentur der Europäischen Union für Cybersicherheit* (ENISA) lediglich auf die Art des Incidents. Die Taxonomie umfasst zwei Kategorien, den Klassifikationstyp und den spezifischen Incident. Die zuletzt genannte Kategorie stellt eine optionale Ergänzung dar, wird von den Autoren allerdings empfohlen, um eine vollständige Darstellung zu gewährleisten [28]. In Tabelle 2.2 wird ein Ausschnitt aus der Taxonomie präsentiert, welcher die Klassifikationstypen Malicious Code und Information Gathering umfasst.

Die Taxonomie umfasst insgesamt zehn Klassifikationstypen sowie einem Test-Klassifikationstyp. Die Motivation für die Entwicklung einer Incident Taxonomie bestand in der Definition europaweit einheitlicher Begriffe, welche die Kommunikation zwischen CSIRTs erleichtern sollten. Das für die Festlegung der Taxonomie zuständige Konsortium setzt sich daher überwiegend aus europäischen CSIRTs zusammen [28]. Im Rahmen dieser Arbeit wird die Taxonomie als Referenz für die Benennung von Incidents verwendet.

[1] SQL Slammer ist ein Computerwurm, welcher im Jahr 2003 erstmals detektiert wurde. Dabei nutzte er eine Schwachstelle in der Implementierung von Microsoft's SQL Server und Microsoft SQL Server Desktop Engine (MSDE) 2000 aus [50].

CLASSIFICATION	INCIDENT EXAMPLES
Malicious Code	Infected System
	C2 Server
	Malware Distribution
	Malware Configuration
Information Gathering	Scanning
	Sniffing
	Social Engineering

Tabelle 2.2: Auszug aus der Reference Security Incident Taxonomy von ENISA [25]

2.3 Information Security Incident Management

In der Literatur findet sich eine Vielzahl von Definitionen zum Begriff ISIM, wobei eine allgemeingültige Definition bisher nicht existiert. Daher muss bei der Verwendung des Begriffs darauf geachtet werden, in welchem Kontext dies geschieht, um Fehlinterpretationen zu vermeiden [46]. In der ISO/IEC 27035 wird ISIM wie folgt definiert: *"collaborative activites to handle information security incidents in a consistent and effective way"* [42]. Eine ähnliche Auffassung findet sich bei *National Institute of Standards and Technology* (NIST), wonach das ISIM die Aufgabe hat, alle Incidents zu überwachen und entsprechende Gegenmaßnahmen zu koordinieren. Des Weiteren wird die Bewertung der Incidents sowie dessen Priorisierung als besonders kritisch beim Erfolg des ISIM erachtet [54]. Das *Computer Emergency Response Team* (CERT)/*Coordination Center* (CC) definiert den Aufgabenbereich des ISIMs umfassender. Unter dem Begriff ISIMs, werden nach CERT/CC, neben der Bearbeitung von Incidents, auch zusätzliche Bereiche wie z. B. Vulnerability Handling und Artifacts Handling zusammengefasst [1]. Die Gründung des CERT/CC erfolgte wurde nach dem ersten identifizierten Wurm-Angriff, dem sogenannten Internet Worm. Es handelt sich hierbei um das erste CSIRT[2]. Der Good Practice Guide for Incident Management von ENISA folgt der Definition von CERT/CC [27].

[2]Ein CSIRT besteht aus Sicherheitsexperten, welche sich primär mit der Behandlung von Incidents befassen. Typischerweise bieten CSIRTs Unterstützung bei der Beseitigung von Incidents sowie bei der Wiederherstellung des Regelbetriebs, nachdem Incidents stattgefunden haben. Ein anderes Akronym für CSIRTs ist CERT [26]. In dieser Arbeit wird allerdings der Begriff CSIRT verwendet, da der Begriff CERT eine eingetragene Marke der Carnegie Mellon University ist. Darüber hinaus erscheint der Begriff CSIRT geeigneter, um den Fokus auf Incident Management zu betonen.

In der vorliegenden Arbeit wird der Begriff ISIM in ähnlicher Weise definiert wie in den Standards ISO/IEC und NIST, da diese die wichtigsten im Bereich ISIM sind [59]. Das Ziel des ISIMs besteht in der Schaffung adäquater Rahmenbedingungen innerhalb einer Organisation, um eine effiziente Koordination bei der Beseitigung von Incidents systematisch zu ermöglichen.

2.3.1 Einordnung im Information Security Management System

Das *Information Security Management System* (ISMS) einer Organisation vereint eine Vielzahl von Richtlinien, Leitlinien sowie den damit verbundenen Prozessen, wie beispielsweise Kontrollmechanismen, um Information Assets[3] zu schützen [41]. Dabei ist das ISMS nicht als technische Lösung zu betrachten, sondern stellt vielmehr den organisatorischen Rahmen für die Informationssicherheit dar [41]. Das Information Security Incident Management lässt sich innerhalb eines ISMS einordnen. In diesem Zusammenhang verweist die ISO/IEC 27000 auf die Bedeutung eines effektiven Information Security Incident Management Prozesses, als kritischen Faktor für ein erfolgreiches ISMS [41]; [46].

2.3.2 Vorteile von Information Security Incident Management

Die Tatsache, dass früher oder später eine Organisation Opfer eines Cyberangriffs wird, stellt die Notwendigkeit dar, warum sich Organisationen mit Incidents befassen müssen. Es lässt sich außerdem beobachten, dass Incidents zunehmend komplexer und zielgerichteter werden [27]. Aus diesem Grund ist ein ISIM von entscheidender Bedeutung. Der durch das ISIM geschaffene Rahmen ermöglicht eine detaillierte Auseinandersetzung mit Incidents sowie die Erstellung eines Handlungsablaufs, der im Falle einer Verletzung der Informationssicherheit eine schnelle und effektive Reaktion gewährleistet. Eine schnelle Reaktion ermöglicht eine zeitliche Minimierung der Ausfälle von Diensten und führt zu einer Verringerung der Menge an Informationen, die von einem Angreifer gesammelt werden können [16]; [46]. Des Weiteren leistet das ISIM einen wichtigen Beitrag zur langfristigen Verbesserung der Informationssicherheit innerhalb der Organisation, indem ähnliche Incidents, durch geeignete Gegenmaßnahmen effektiv verhindert werden [42].

[3] Der Begriff Asset bezeichnet einen Gegenstand, der für Personen von hohem Wert ist. Dabei kann es sich sowohl um materielle als auch um immaterielle Werte handeln, wie beispielsweise Informationen [52].

2.3.3 Abgrenzung von Incident Handling gegenüber Incident Response

Im Kontext des Information Security Incident Management werden die Begriffe Incident Handling und Incident Response häufig verwendet. In der SP 800-61 Rev. 2 werden die beiden Begriffe Incident Handling und Incident Response als bedeutungsgleich angesehen [16]; [46]. In der neuesten Version der SP 800-61 wird auf die Erwähnung der Bedeutungsgleichheit verzichtet, allerdings wird der Begriff des Incident Handlings weitestgehend gemieden [54]. Die ISO/IEC hingegen unterscheidet klar zwischen den beiden Begriffen. In der ISO/IEC 27035 wird das Incident Handling folgendermaßen definiert: *"actions of detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents"* [42].

Die Incident Response hingegen stellt einen Teilbereich vom Incident Handling dar und umfasst die Bereiche *responding to* und *dealing with*. In der ISO/IEC 27035 wird es wie folgt definiert: *"actions taken to mitigate or resolve an information security incident [...]"* [42]. Ebenso wie bei der ISO/IEC unterscheiden ENISA bzw. CERT/CC zwischen Incident Handling und Incident Response. In der Arbeit von ENISA wird Incident Handling in die Phasen Detection, Triage, Analysis und Incident Response unterteilt [27]. Incident Response wird damit ebenfalls als ein Unterprozess des Incident Handlings definiert. Die Incident Response befasst sich mit der Eindämmung von Incidents und Wiederherstellungsmaßnahmen [27]; [46]; [47]. Auch in dieser Arbeit wird unterschieden zwischen den beiden Begriffen und Incident Response als ein Unterprozess des Incident Handlings angesehen.

In der Abbildung 2.2 wird die Beziehung zwischen den Begriffen Information Security Management System, Information Security Incident Management, Incident Handling und Incident Response mit Hilfe eines Venn-Diagramms dargestellt.

2.3.4 Abgrenzung gegenüber Incident Management nach ITIL

Die Begriffe Event, Incident sowie Incident Management werden in unterschiedlichen Zusammenhängen verwendet, nicht nur im Kontext der Informationssicherheit. Auch in dem Standard ITIL finden sich die genannten Begriffe wieder. Es handelt sich hierbei um den am weitesten verbreiteten Standard für das *IT-Service-Management* (ITSM). Die Kernaufgabe des ITSM besteht in der Verwaltung und Bereitstellung von IT-Services sowie

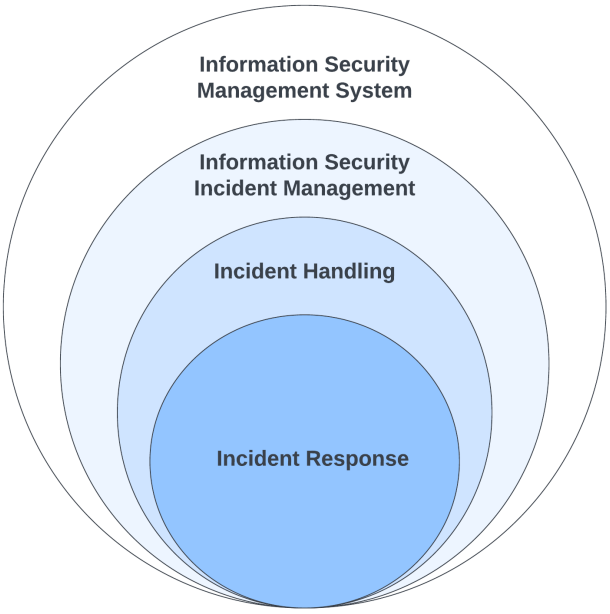

Abbildung 2.2: Einordnung der Begriffe Information Security Management System, Information Security Incident Management, Incident Handling und Incident Response, eigene Darstellung

der Analyse ihrer Einsatzmöglichkeiten zur Erfüllung der Unternehmens- und Kundenziele. Trotz der gleichen Verwendung der Begriffe ist der Kontext beim ISIM ein anderer als bei ITIL [3]. ITIL definiert einen Incident folgendermaßen: *"An unplanned interruption to a service or reduction in the quality of a service."* [3]. Der Begriff Incident nach ITIL umfasst dabei nicht nur die Informationssicherheit, sondern ist als allgemeiner zu verstehen. Als Beispiel für einen Incident führt ITIL den Ausfall eines Wireless Access Point, bedingt durch technisches Versagen, an. Der Ausfall führt dazu, dass das Unternehmen nicht mehr in der Lage ist, effizient zu arbeiten, da Mitarbeiter längere Strecken zurücklegen müssen, um in Bereiche mit WLAN-Empfang zu gelangen, in denen sie z. B. neue Aufträge erhalten können. Aus Sicht von ITIL liegt ein Incident vor, da die Unternehmensziele gefährdet sind, weil Aufträge ineffizienter abgearbeitet werden, was beispielsweise zu einer Verzögerung bei Lieferterminen führen kann. Aus der Perspektive der Informationssicherheit hingegen liegt kein Incident vor, da kein Asset des Unternehmens gefährdet ist [3].

Typischerweise erfolgt die Bearbeitung von Incidents, wie sie in den ITIL-Prozessen definiert ist, getrennt von Incidents, die die Informationssicherheit betreffen [3]. Dabei ist

eine präzise Trennung der Begriffe erforderlich, um eine Überschneidung und damit ggf. Unsicherheit zu vermeiden.

2.3.5 Abgrenzung gegenüber Vulnerability Management

Der Fokus des ISIM liegt auf der Untersuchung von Incidents, welche eine Verletzung der Schutzziele der Informationssicherheit darstellen [42]. Bei Schwachstellen, für die das Vulnerability Management zuständig ist, ist eine Verletzung der Schutzziele hingegen nicht automatisch der Fall. Die bloße Identifizierung einer Schwachstelle bedeutet nicht, dass diese auch tatsächlich von einem Angreifer ausgenutzt wurde oder werden kann [53]. Die Prüfung, ob die eigenen Systeme von einer Schwachstelle betroffen sind, können Organisationen z. B. mithilfe der Cyber-Sicherheitswarnungen des BSI vornehmen [7]. Falls eine Schwachstelle identifiziert wird, ist das Vulnerability Management dafür zuständig, diese durch Patches oder andere Maßnahmen zu schließen oder deren Ausnutzung zu verhindern. Sofern Anzeichen dafür vorliegen, dass die Schwachstelle bereits ausgenutzt wurde, erfolgt eine Meldung an die Verantwortlichen für das ISIM, damit eine Aufarbeitung des Incidents beginnen kann. [19]; [46].

2.4 Rahmenwerke für das Information Security Incident Management

Als geeignete Rahmenwerke wurden in einer vorherigen Arbeit die ISO/IEC 27035, die SP 800-61 von NIST und der Good Practice Guide for Incident Management von ENISA identifiziert. Alle drei Werke verfolgen das Ziel, eine generische Anleitung für die Etablierung eines ISIM zu sein. Des Weiteren handelt es sich hierbei um etablierte Rahmenwerke [46].

2.4.1 ISO/IEC 27035 - Information Technology — Information Security Incident Management

Die 1946 gegründete *International Organization for Standardization* hat sich zum Ziel gesetzt, Standards zu etablieren, die die Zusammenarbeit zwischen Menschen und Unternehmen auf der ganzen Welt ermöglichen. Die ISO kooperiert unter anderem mit der *International Electrotechnical Commission*, siehe ISO/IEC 27035 [39]. Die IEC wurde

1906 gegründet und ist spezialisiert auf Standards für elektrische und elektronische Produkte [38]. Die IEC ist wie die ISO eine internationale Nichtregierungsorganisation.

Die ISO/IEC 27035 verfolgt das Ziel, als generischer Standard für jede Organisation, unabhängig von ihrer Größe, die Implementierung eines ISIM zu ermöglichen. Er dient als Leitfaden zur Umsetzung der in der ISO/IEC 27001 bzw. ISO/IEC 27002 an ein ISIM gestellten Anforderungen [42]. Der Standard ISO/IEC 27035 ist in insgesamt vier Teile untergliedert. Der erste Teil des Standards präsentiert die Grundlagen sowie die Phasen des ISIM [42]. Das ISIM wird in fünf Phasen unterteilt:

- Plan and Prepare
- Detect and Report
- Assess and Decide
- Respond
- Learn Lessons

Im zweiten Teil des Standards erfolgt eine detaillierte Betrachtung der Phasen Plan and Prepare und Learn Lessons [43]. In der Phase Plan and Prepare wird zunächst erörtert, aus welchen Gründen und wofür eine Sicherheitsrichtlinie benötigt wird und wie sie strukturiert sein sollte. Des Weiteren wird dargelegt, welche Ressourcen erforderlich sind, um ein ISIM zu betreiben und wie die in dieser Phase entwickelten Security Incident Pläne getestet werden können [42]. Die Phase Learn Lessons dient der Evaluierung des Incident Handlings sowie der Beurteilung des zugrunde liegenden Prozesses [43]. Der dritte Teil beinhaltet Richtlinien für das Incident Handling. Darüber hinaus wird das Incident Handling feingranular gegliedert. Dies umfasst die Phasen, die im zweiten Teil nicht behandelt wurden. Die einzelnen Phasen sind der Abbildung 2.3 zu entnehmen [46]. Der vierte Teil richtet sich an CSIRTs, welche mehrere Organisationen bei der Bewältigung von Incidents betreuen [45].

In der Abbildung 2.3 werden die Zusammenhänge der ersten drei Teile des Standards ISO/IEC 27035 gezeigt.

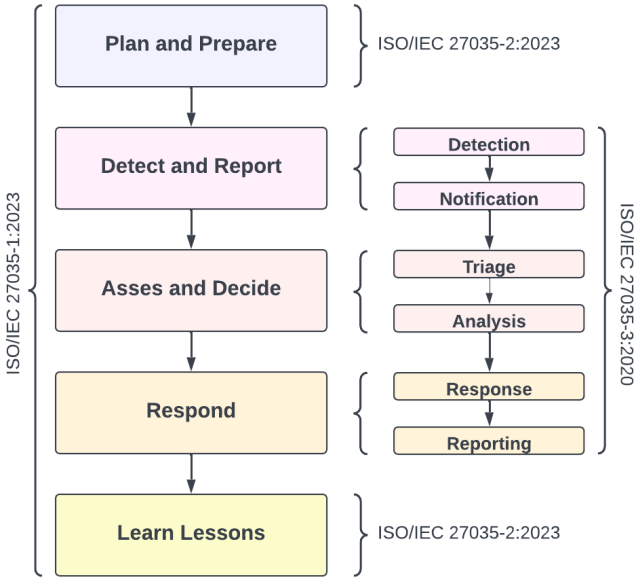

Abbildung 2.3: Zusammenhang der Standards ISO/IEC 27035-1:2023, ISO/IEC 27035-2:2023 und ISO/IEC 27035-3:2020, entnommen aus [46]

2.4.2 NIST SP 800-61 - Computer Security Incident Handling Guide

Das *National Institute of Standards and Technology* (NIST) wurde im Jahr 1901 gegründet und ist dem Handelsministerium der Vereinigten Staaten von Amerika unterstellt. Die Sicherung der Wettbewerbsfähigkeit der USA stellt dabei ein zentrales Ziel von NIST dar, welches durch die Erstellung bzw. Weiterentwicklung von Standards verfolgt wird [51]. Ein Standard ist dabei die *Special Publication* (SP) 800-61. Dieses Dokument wurde entwickelt, um in den Bundesbehörden der Vereinigten Staaten von Amerika zum Einsatz zu kommen. Es soll die Behörden bei der Erfüllung der Anforderungen an die Sicherheit von Informationssystemen unterstützen. Allerdings kann das Dokument auch von anderen Organisationen freiwillig verwendet werden [16]. Das NIST entwickelte die Richtlinie, um der gesetzlichen Verpflichtung nachzukommen, die sich aus dem *Federal Information Security Management Act* (FISMA) von 2002, Public Law 107-347 ergeben [46].

Zum Zeitpunkt dieser Arbeit (Juni 2024) liegt eine neue, dritte Version des Standards, als öffentlicher Erstentwurf, vor. Verglichen mit der zweiten Version aus dem Jahr 2012 hat sich am Lebenszyklus des ISIMs einiges verändert. Die Autoren begründen die notwendigen Änderungen damit, dass die Incidents häufiger auftreten und einen viel größeren Schaden sowie Umfang haben und damit das Incident Handling signifikant länger dauert.

Während die Autoren im Jahr 2012 von einer Dauer des Incident Handlings von wenigen Tagen ausgingen, gehen sie im Jahr 2024 von Wochen oder Monaten aus. Das Modell aus dem Jahr 2012 war entsprechend nicht auf ein kontinuierliches, paralleles Incident Handling ausgelegt, sondern auf die Behandlung eines einzelnen Incidents [54].

Das neue ISIM Modell von NIST basiert auf dem Cybersecurity Framework (CSF) 2.0, welches ebenfalls von NIST entworfen wurde [54]. Im neuen Modell gibt es sechs Kernkomponenten, deren Aufgaben im Folgenden kurz erläutert werden:

- **Govern**: Festlegung und Überwachung von Richtlinien für die Informationssicherheit
- **Identify**: Identifizierung von Risiken im Kontext der Informationssicherheit
- **Protect**: Festlegung von Schutzmaßnahmen
- **Detect**: Mögliche Angriffe identifizieren und analysieren
- **Respond**: Ergreifen von Maßnahmen, nach dem ein Incident festgestellt wurde
- **Recover**: Wiederherstellung des Regelbetriebs

In Abbildung 2.4 wird das Zusammenwirken der Kernkomponenten und damit der Lebenszyklus des ISIM aus der dritten Version veranschaulicht.

Die Aktivität *Improvement* wird durch grüne Pfeile hervorgehoben, damit soll symbolisiert werden, dass innerhalb jeder Aktivität eine Evaluierung nach möglichen Verbesserung erfolgen soll. Dies ist als Durchführung eines kontinuierlichen *Lessons learned* anzusehen und steht im Gegensatz zu der Durchführung der *Learn Lessons*, wie sie in der ISO/IEC 27035 beschrieben wird, die erst am Ende des Incident Handlings erfolgt.

Die Abbildung 2.5 präsentiert den Lebenszyklus in seiner zweiten Version. Bei der Betrachtung der Grafik fällt zunächst auf, dass zwei Zyklen erkennbar sind. Der erste Zyklus erstreckt sich über die Phasen *Containment, Eradication and Recovery* und *Detection and Analysis*. Er dient der Abbildung des Falls, dass bei der Beseitigung von Malware weitere Systeme betroffen sind, die eine tiefergehende Analyse notwendig machen. Der zweite Zyklus umfasst die Phase Post-Incident Activity und Preparation. Er verdeutlicht, dass nach einem erfolgreichen Incident Handling eine erneute Vorbereitung auf den nächsten Incident erforderlich ist [16]; [46].

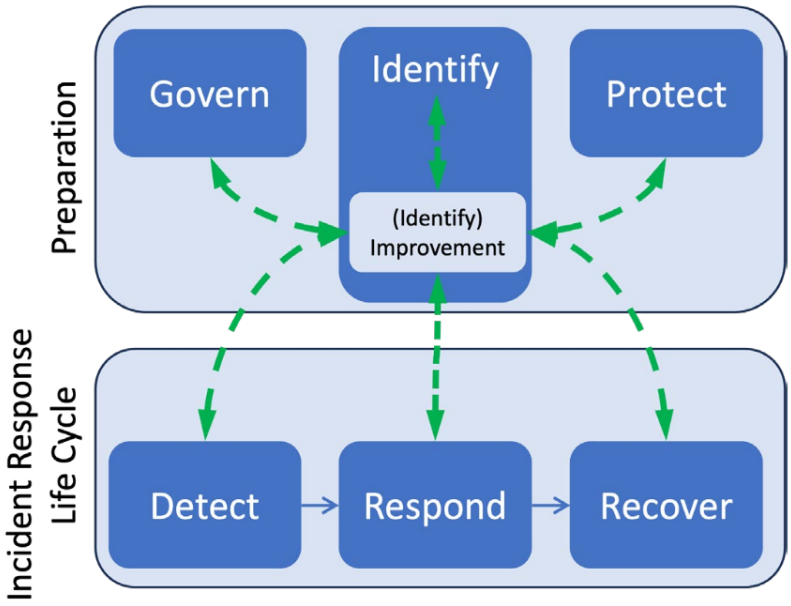

Abbildung 2.4: Lebenszyklus der SP 800-61 Rev. 3 beim Information Security Incident Management, entnommen aus [54]

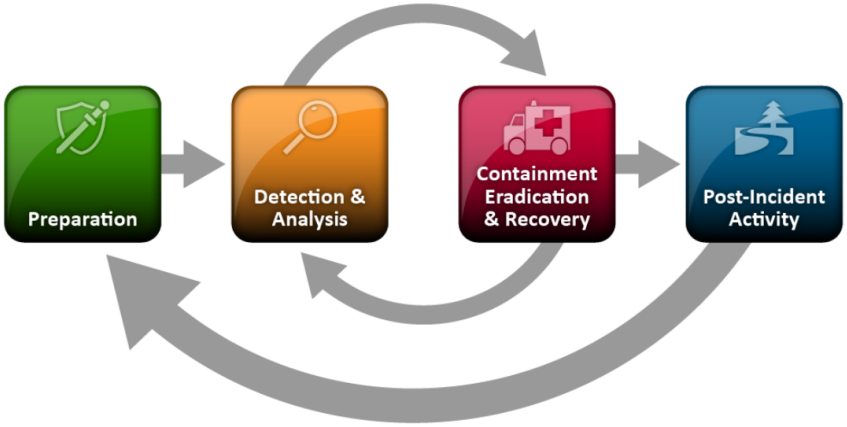

Abbildung 2.5: Lebenszyklus der SP 800-61 Rev. 2 beim Information Security Incident Management, entnommen aus [16]

2.4.3 ENISA - Good Practice Guide for Incident Management

Die im Jahr 2004 von der *Europäischen Union* (EU) gegründete *European Union Agency for Cybersecurity* (ENISA) hat das Ziel, die Cybersicherheit innerhalb der EU zu stärken. Zu diesem Zweck soll die Fragmentierung der europäischen Mitgliedsländer im Bereich

Cybersicherheit verhindert und stattdessen die Zusammenarbeit gefördert werden. Die Agentur wurde als unabhängige Einrichtung konzipiert, die als Kompetenzzentrum für Cybersicherheit dienen soll [32]. Im Rahmen dieser Verantwortung wurde im Jahr 2010 der Leitfaden Good Practice Guide for Incident Management veröffentlicht, dieser stellt gleichzeitig die aktuellste Version dar [27].

Der Good Practice Guide for Incident Management richtet sich in erster Linie an CSIRTs und präsentiert bewährte Praktiken und Richtlinien. Darüber hinaus geben die Autoren jedoch eine allgemeine Empfehlung an alle Gruppen, die sich mit Incidents auseinandersetzen wollen. Dabei liegt der Schwerpunkt des Dokuments auf dem Incident Handling [27]. Die Definition des Incident Handlings, welches von der ENISA verwendet wird, basiert auf der von CERT/CC [1]; [46]. Diese Definition umfasst vier Hauptkomponenten:

- Detection
- Triage
- Analysis
- Incident Response

In Abbildung 2.6 wird der Zusammenhang zwischen ISIM und Incident Handling gemäß der Auffassung von ENISA dargestellt. Die Phasen werden in dem Dokument von ENISA noch weiter aufgegliedert, wobei das dargestellte Grundmuster erhalten bleibt. Die Aufgliederung umfasst auch die Aktivitäten *Post Analysis* und *Improvement Proposals*, welche auch als *Lessons learned* aufgefasst werden können [27].

2.4.4 Auswahl eines geeigneten Rahmenwerkes für die HAW Hamburg

Im Rahmen einer vorherigen Arbeit des Autors wurden Anforderungen an ein Rahmenwerk als generische Vorlage für ein ISIM an der HAW Hamburg erarbeitet [46]. Die Anforderungen basierten zum einen auf dem IT-Grundschutz-Kompendium und zum anderen auf der ISO/IEC 27002. Das IT-Grundschutz-Kompendium wurde als Bewertungsgrundlage herangezogen, da im Rahmen-Sicherheitskonzept (RaSiKo) der Freien und Hansestadt Hamburg (FHH) die Anwendung des IT-Grundschutzes vom BSI vorgegeben wird [56]. Die ISO/IEC 27002 findet hingegen Anwendung, da die HAW Hamburg die Einführung eines ISMS auf Basis der ISO 27001 plant [46].

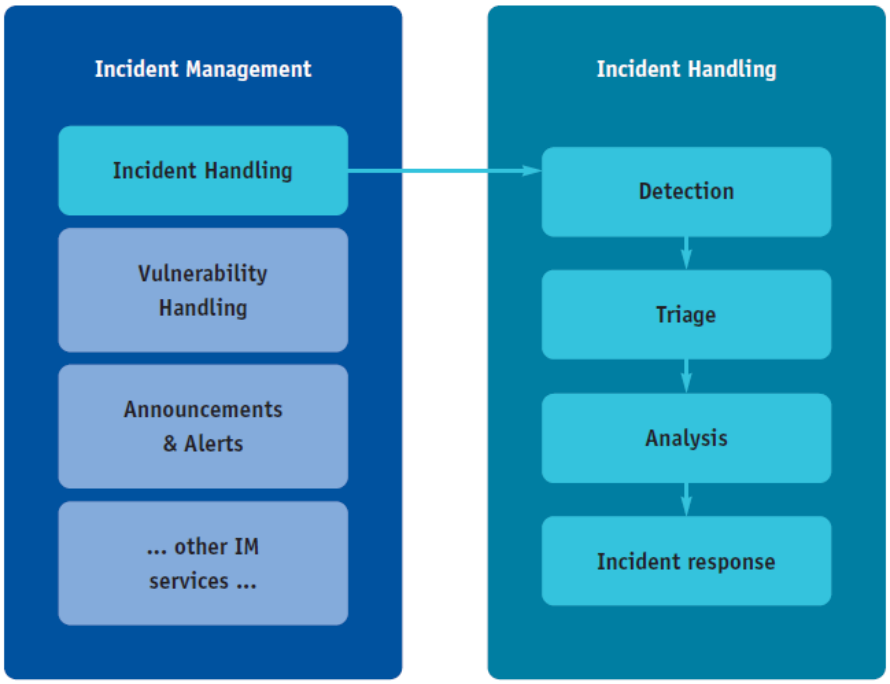

Abbildung 2.6: Zusammenhang zwischen ISIM und Incident Handling vom Good Practice Guide for Incident Management von ENISA, entnommen aus [27]

Im Rahmen der Untersuchung wurden insgesamt zwölf Anforderungen aus den beiden Dokumenten identifiziert, welche im Anhang dieser Arbeit aufgeführt sind, siehe Tabelle A.1, Tabelle A.2, Tabelle A.3. Diese dienen als Grundlage für die Entscheidung, welches der drei zuvor vorgestellten Rahmenwerke am geeignetsten eingeschätzt wurde, um als Vorlage für das ISIM an der HAW Hamburg verwendet zu werden. Die Zusammenfassung der Bewertung ist in Tabelle 2.3 dargestellt. Für die Bewertung wurde überprüft, ob das jeweilige Framework die in den Anforderungen aufgeführten Themen behandelt [46].

Bei der Bewertung wurde ersichtlich, dass die SP 800-61 Rev. 2 und die ISO/IEC 27035 alle zwölf Anforderungen erfüllten. Wohingegen der Good Practice Guide for Incident Management von ENISA nicht alle Anforderungen aus Kategorie Management erfüllen konnte. Der Schwerpunkt des Rahmenwerks von ENISA liegt auf CSIRTs. Im IT-Grundschutz-Kompendium und der ISO/IEC 27002 hingegen liegt der Schwerpunkt auf der gesamten Organisation. Dies führt zu einer anderen Perspektive. In einer Gegenüberstellung der drei Rahmenwerke wurde ersichtlich, dass der Good Practice Guide for Incident Management nur bedingt als Grundlage für ein ISIM an der HAW Hamburg geeignet ist [46].

	Good Practice Guide for Incident Management	SP 800-61 Rev. 2	ISO/IEC 27035
		Management	
Anf1	✗	✓	✓
Anf2	✗	✓	✓
Anf3	✓	✓	✓
Anf4	✓	✓	✓
Anf5	✗	✓	✓
		Aufgabenbereiche und Schulungen von Mitarbeitern	
Anf6	✓	✓	✓
Anf7	✓	✓	✓
Anf8	✓	✓	✓
		Information Security Incident Response	
Anf9	✓	✓	✓
Anf10	✓	✓	✓
Anf11	✓	✓	✓
Anf12	✓	✓	✓

Tabelle 2.3: Bewertung der Rahmenwerke für die Eignung zur Verwendung an der HAW Hamburg, entnommen aus [46]

In Bezug auf die genannten Anforderungen konnte festgestellt werden, dass sowohl die SP 800-61 Rev. 2 als auch die ISO/IEC 27035 für den Einsatz an der HAW Hamburg geeignet sind. Im Rahmen der vorherigen Arbeit wurde jedoch festgestellt, dass die ISO/IEC 27035 das geeignetste Rahmenwerk darstellt. Dies lässt sich zum einen darauf zurückführen, dass die SP 800-61 Rev. 2 im Vergleich zur ISO/IEC 27035 eine geringe Aktualität aufweist. Zum Zeitpunkt der Bewertung lag die dritte Version der SP 800-61 noch nicht vor, sodass lediglich die Version aus dem Jahr 2012 berücksichtigt werden konnte. Zudem stellt die ISO/IEC 27035 einen etablierten Standard mit hoher, globaler Anerkennung dar [59]; [46].

3 Meldepflichten und Meldepraktiken im Incident Handling Prozess

Im Rahmen der Modellierung des Incident Handling Prozesses stellen Meldepflichten einen wichtigen Teilaspekt dar. In diesem Zusammenhang wird der Fokus, auf externe Akteure gelegt, bei denen eine Benachrichtigung erforderlich ist. Neben der Gefahr, bei Nichteinhaltung empfindliche Strafen zahlen zu müssen, tragen Meldungen zudem zur Erstellung eines übergeordneten Lagebildes bei [46]. Außerdem wird eine erste Abschätzung abgegeben, wie sich die neuen Richtlinien und Verordnungen der Europäischen Union, wie NIS2 und DORA, auf die HAW Hamburg auswirken werden. Des Weiteren erfolgt eine Betrachtung freiwilliger Meldepraktiken, welche neben den gesetzlich vorgeschriebenen Meldepflichten durchgeführt werden sollten.

3.1 Meldepflichten für die HAW Hamburg

Bei der Durchführung des Incidents Handling stellt das Informieren der Meldestellen einen wichtigen Schritt dar. Im Rahmen einer vorherigen Arbeit wurden die Meldepflichten der HAW Hamburg herausgearbeitet [46]. Für die Modellierung des Incident Handling ist es empfehlenswert, zu dokumentieren, unter welchen Umständen und innerhalb welches Zeitraums eine externe Organisation benachrichtigt werden muss, auch um gesetzliche Verpflichtungen einzuhalten.

Im Rahmen der Untersuchung der Meldepflichten der HAW Hamburg wurde festgestellt, dass einige Meldepflichten in sämtlichen Bereichen der Hochschule bestehen, wobei sich andere Meldepflichten ausschließlich auf den Verwaltungsbereich beschränken. Die Einhaltung der *Datenschutz-Grundverordnung* (DSGVO) ist in jedem Bereich der HAW Hamburg erforderlich, da die HAW Hamburg bereichsübergreifend personenbezogene Daten erhebt und verarbeitet. Gemäß Art. 33 DSGVO ist die HAW Hamburg dazu verpflichtet, die Behörde für Wissenschaft, Forschung und Gleichstellung der Freien und

Hansestadt Hamburg innerhalb von 72 Stunden über Verletzungen des Schutzes personenbezogener Daten zu informieren [23]. Im Falle einer Verletzung des Schutzes personenbezogener Daten, welche ein hohes Risiko für die persönlichen Rechte und Freiheiten einer natürlichen Person birgt, ist die betroffene Person gemäß Art. 34 DSGVO unverzüglich darüber in Kenntnis zu setzen [24]; [46].

Im Bereich der Verwaltung bestehen weitere spezifische Meldepflichten. Im Hinblick auf die Verwaltung ist an der HAW Hamburg zwischen sogenannten BASIS (Büro-Arbeitsplatz Standard-Infrastruktur-Services) und Non-BASIS-Arbeitsplätzen zu unterscheiden. Die jeweiligen Zuständigkeiten und damit einhergehenden Meldepflichten variieren in Abhängigkeit vom betroffenen Arbeitsplatz. Für die Betreuung der BASIS-Arbeitsplätze ist Dataport als IT-Dienstleister der *Freien und Hansestadt Hamburg* (FHH) zuständig. Meldungen über Incidents sind grundsätzlich an den User Help Desk von Dataport zu richten. Das IT-Sicherheitsmanagement wird von Dataport übernommen, sofern dies erforderlich ist [56]; [46].

Im Falle einer Betroffenheit von Non-BASIS Arbeitsplätzen ist eine Ermittlung der Kritikalität des Sicherheitsvorfalls anhand einer Matrix der FHH erforderlich, welche auf der Grundlage der Kriterien Dringlichkeit und Auswirkung erstellt wurde, siehe Abbildung 3.1.

		Priorität / Kritikalität			
Dringlichkeit	Kritisch	Hoch	Hoch	Kritisch	Kritisch
	Hoch	Mittel	Hoch	Hoch	Kritisch
	Mittel	Niedrig	Mittel	Hoch	Hoch
	Niedrig	Niedrig	Niedrig	Mittel	Hoch
		Niedrig	Mittel	Hoch	Kritisch
		Auswirkung			

Abbildung 3.1: Matrix für die Klassifizierung von Sicherheitsvorfällen der FHH, entnommen aus [56]

Die Kritikalität sowie die Kriterien werden in vier Stufen bewertet von *Niedrig* bis *Hoch*. Das Kriterium Auswirkung dient der Bewertung der Anzahl betroffener Anwender, Kunden und Behörden sowie der Feststellung, ob die Geschäftstätigkeit noch aufrechterhalten

werden kann. Das Kriterium Dringlichkeit bewertet, ob Ersatzlösungen verfügbar sind und zu welchem Zeitpunkt Maßnahmen durchgeführt werden müssen. Die Kombination beider Kriterien ergibt die Kritikalitätsstufe. Bei hohen oder kritischen Kritikalitätsstufen ist die Leitungsebene und das Informationssicherheitsmanagement der FHH innerhalb eines Zeitraums von 12 Stunden bzw. unverzüglich zu informieren [56]. Des Weiteren besteht für die HAW Hamburg als Behörde der FHH gemäß § 1 Abs. 4 VwVfG die Möglichkeit, Vorfälle in der Verwaltung an das CERT Nord zu melden, um zusätzliche Unterstützung zu erhalten. Gemäß dem Rahmen-Sicherheitskonzept (RaSiKo) der FHH besteht jedoch keine Meldepflicht an das CERT Nord [56]; [46]. Für Non-BASIS-Arbeitsplätze trägt Dataport hingegen keine Verantwortung.

3.2 Neue regulatorische Meldepflichten unter NIS2 und DORA

Zur Gewährleistung eines einheitlichen Informationssicherheitsniveaus innerhalb der Europäischen Union wurden diverse Richtlinien und Verordnungen verabschiedet. Im Folgenden werden die Network and Information Security (NIS)2-Richtlinie sowie die Verordnung Digital Operational Resilience Act (DORA) betrachtet. Das Ziel dieses Abschnittes ist es zu überprüfen, inwiefern Meldepflichten und Meldepraktiken, die sich aus NIS2 und DORA ergeben, für den Incident Handling Prozess an der HAW Hamburg geeignet sind.

Im Rahmen von NIS2 und DORA ist zudem die Critical Entities Resilience Directive (CER) zu nennen. Die Richtlinie legt fest, welche Maßnahmen kritische Einrichtungen zur Steigerung ihrer Resilienz ergreifen müssen. Der Schutz der IT-Sicherheit von kritischen Einrichtungen wird bereits in der NIS2 und DORA behandelt. Die CER-Richtlinie verfolgt einen sogenannten All-Gefahrenansatz, der für diese Arbeit zu umfassend wäre, weshalb sie nicht näher betrachtet wird [14].

Wird die bisherige Entwicklung von Richtlinien und Verordnungen über Informationssicherheit und damit auch die Verschärfung der Meldepflichten in der EU betrachtet, wird deutlich, dass eine Zunahme der regulierten Unternehmen und Einrichtungen zu erwarten ist. Gemäß Schätzungen des Statistischen Bundesamts sind von den Meldepflichten, die in der NIS2 formuliert werden, rund 29.000 Unternehmen in Deutschland betroffen, was einem fünfmal so hohen Wert im Vergleich zur vorherigen Gesetzgebung entspricht

[12]. Demnach ist davon auszugehen, dass Hochschulen, wie die HAW Hamburg, in naher Zukunft eine größere Anzahl an Meldepflichten erfüllen müssen als in Abschnitt 3.1 beschrieben. Die HAW Hamburg zählt mit den 16.454 Studierenden, die im Sommersemester 2023 eingeschrieben waren, zu den größeren Hochschulen. Darüber hinaus sind an der HAW Hamburg 1.398 Personen angestellt und es gibt zusätzlich 457 Lehrbeauftragte (Stand: 01.06.2023) [34].

3.2.1 Network and Information Systems Directive 2 (NIS2)

Die NIS2-Richtlinie der EU muss zunächst in ein nationales Gesetz überführt werden, bevor sie in Deutschland Anwendung finden kann. Dies erfolgt mit dem NIS2-Umsetzungsgesetz (NIS2UmsuCG). Bis zum 17. Oktober 2024 hätte das NIS2UmsuCG erlassen werden müssen [13]. Allerdings geht das Bundesministerium des Innern und für Heimat davon aus, dass das Gesetz erst im ersten Quartal 2025 in Kraft treten wird [15].

Im NIS2UmsuCG wird differenziert zwischen Einrichtungen, die als wichtig oder als besonders wichtig gelten. Je nach Einstufung ergeben sich unterschiedliche Pflichten für die Einrichtungen. Eine Unterteilung erfolgt anhand von Sektoren [13]. Eine vollständige Aufführung der Sektoren ist in Abbildung 3.2 zu sehen.

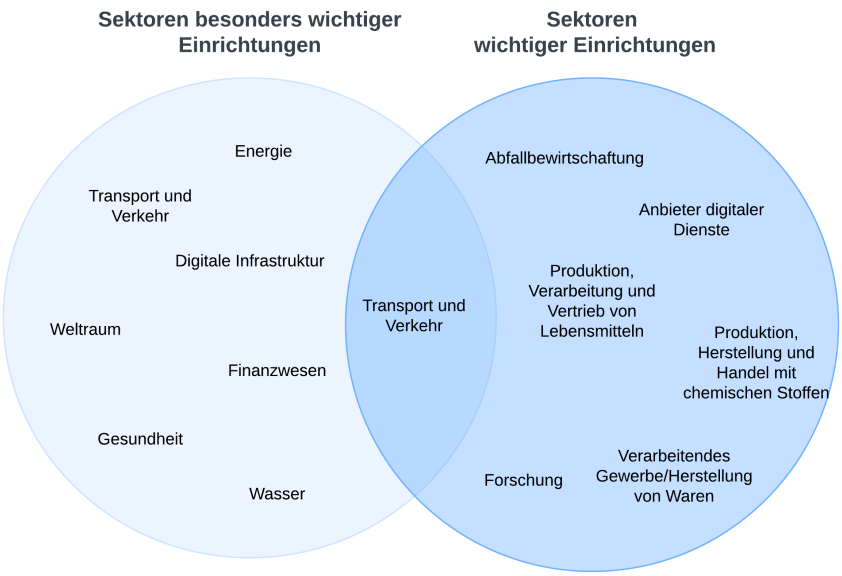

Abbildung 3.2: Sektoren für die Klassifikation von Einrichtungen nach dem NIS2UmsuCG, eigene Darstellung

Neben der Voraussetzung, dass die Einrichtungen in dem entsprechenden Sektor tätig sind, ist die Erreichung bestimmter Schwellenwerte erforderlich, um als wichtig oder als besonders wichtig nach dem NIS2UmsuCG gewertet zu werden. Einrichtungen, die als wichtig gelten, müssen z. B. mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen. Für Anbieter öffentlich zugänglicher Telekommunikationsdienste sowie Betreiber öffentlicher Telekommunikationsnetze gelten strengere Kriterien [13].

Einrichtungen, die als wichtig oder besonders wichtig eingestuft werden, unterliegen im Rahmen des NIS2UmsuCG einer umfassenden Reihe von Pflichten. Diese sind in § 30, § 31, § 32, § 33, § 34, § 35, § 36, § 37, § 38 und § 39 aufgeführt. Die Meldepflicht ist in § 32 NIS2UmsuCG geregelt und betrifft sowohl wichtige als auch besonders wichtige Einrichtungen. Gemeldet werden müssen erhebliche Sicherheitsvorfälle [13]. In der NIS2UmsuCG werden erhebliche Sicherheitsvorfälle folgendermaßen definiert:

> „[...] schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann [...]“[1]

Eine präzisere Begriffsbestimmung des Begriffs erheblicher Sicherheitsvorfall durch das Bundesministerium des Innern und für Heimat für die einzelnen Sektoren ist jedoch möglich. Ansonsten obliegt es den Einrichtungen zu beurteilen, ob nach der oben aufgeführten Definition ein erheblicher Sicherheitsvorfall vorliegt [13].

Im Falle der Identifizierung eines erheblichen Sicherheitsvorfalls in einer wichtigen oder besonders wichtigen Einrichtung ist eine Meldung innerhalb eines Zeitraums von 24 Stunden an eine vom BSI und vom *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* (BBK) eingerichtete Meldestelle abzugeben [13]. Innerhalb von 72 Stunden nach Kenntniserlangung des Vorfalls müssen die Informationen aus der ersten Meldung aktualisiert werden. Das BSI kann zudem eine Zwischenmeldung der betroffenen Einrichtung anfordern. Spätestens nach einem Monat muss eine Abschlussmeldung erfolgen. Sollte der erhebliche Sicherheitsvorfall bis dahin nicht abgeschlossen sein, erfolgt eine Fortschrittsmeldung und die Abschlussmeldung wird sobald wie möglich eingereicht [13].

Ein Sektor, der in der NIS2UmsuCG Erwähnung findet, ist der Bereich der Forschung. Der Sektor umfasst ausschließlich Forschungseinrichtungen, die Forschung für kommerzielle

[1] NIS2UmsuCG Referentenentwurf vom 22.07.2024 [13]

Zwecke betreiben. Einrichtungen, welche in diesem Sektor tätig sind und die festgelegten Schwellenwerte erreichen, werden als wichtige Einrichtungen eingeordnet. Gemäß des Referentenentwurfs gelten Bildungseinrichtungen nicht als Forschungseinrichtungen im Sinne der obenstehenden Definition [13]. Ob Forschungs- und Transferzentren der HAW Hamburg ebenfalls als Bildungseinrichtung und nicht als Forschungseinrichtung gemäß NIS2UmsuCG klassifiziert werden, bleibt abzuwarten und ist nicht Gegenstand dieser Arbeit.

Die Ableitung freiwilliger Meldepraktiken für die HAW Hamburg auf Basis des NIS2UmsuCG erscheint nicht zielführend, da die Definition von erheblichen Sicherheitsvorfällen zu allgemein gehalten ist und einer eigenen Bewertung durch die HAW Hamburg bedarf.

3.2.2 Digital Operational Resilience Act (DORA)

Im Gegensatz zur NIS2-Richtlinie stellt DORA eine Verordnung dar. Verordnungen müssen nicht erst in nationales Recht überführt werden, sondern sind in der Fassung gültig, wie sie von der EU beschlossen wurden [30]. Die Veröffentlichung der Verordnung erfolgte am 27. Dezember 2022 im Amtsblatt der Europäischen Union, sie ist am 17. Januar 2023 in Kraft getreten. Ab dem 17. Januar 2025 erfolgt die Anwendung [10].

Der Anwendungsbereich von DORA erstreckt sich auf nahezu alle beaufsichtigten Institute und Unternehmen des europäischen Finanzsektors [10]. Im NIS2UmsuCG existiert bereits der Sektor Finanzwesen. Um mögliche Kollisionen bei der Umsetzung zu vermeiden, hat DORA Anwendungsvorrang vor der NIS2-Richtlinie. Das bedeutet, dass Einrichtungen, die vom NIS2UmsuCG und DORA betroffen sind, lediglich die Vorgaben von DORA umsetzen müssen. Die Berücksichtigung des Finanzsektors im Rahmen der NIS2UmsuCG erfolgt vor dem Hintergrund, dass dieser Bestandteil eines sogenannten „Ökosystems“ sein soll, welches durch das NIS2UmsuCG etabliert wird. Ziel ist es, ein „sektorübergreifendes Lernen“ zu ermöglichen [31].

Im Gegensatz zum NIS2UmsuCG macht DORA konkrete Vorgaben, was die Bewertung von Incidents angeht. Für die Klassifizierung von Incidents werden sechs Kriterien genannt [31]:

- Anzahl und/oder Relevanz der betroffenen Kunden
- Dauer des Incidents

- Geografische Ausbreitung
- Verlust von Daten
- Kritikalität der betroffenen Dienste
- Wirtschaftliche Auswirkungen

Nach der DORA-Richtlinie müssen sogenannte Major Incidents an die zuständigen Behörde gemeldet werden. Basierend auf den oben genannten Kriterien werden feste Vorgaben gemacht, wann ein Major Incident vorliegt. Dies ist beispielsweise der Fall, wenn zwei oder mehr Schwellenwerte erreicht werden. Konkret bedeutet dies, dass z. B. 10 % der Kunden und 10 % der täglichen Transaktionen von einem Incident betroffen sein müssen, damit er als Major Incident eingestuft wird. Des Weiteren werden auch erneut auftretende Incidents, welche beim erstmaligen Auftreten nicht als Major Incident kategorisiert wurden, als Major Incident eingestuft, sofern spezifische Voraussetzungen erfüllt sind, wie beispielsweise das wiederholte Auftreten innerhalb eines Zeitraums von sechs Monaten [29].

In Deutschland ist die zuständige Meldebehörde die *Bundesanstalt für Finanzdienstleistungsaufsicht* (BAFIN), welche die Meldung an weitere Stellen weiterleitet. Dabei werden das BSI, die europäischen Finanzaufsichtsbehörden und ENISA in jedem Fall benachrichtigt. Weitere Institutionen werden benachrichtigt, sofern es relevant oder notwendig ist [11]. Der Aufbau der Meldung, welche von den Instituten und Unternehmen des europäischen Finanzsektors abgegeben werden muss, ist dabei vorgegeben [10]. Je nach der Art der Meldung variiert die Anzahl der verpflichtenden Felder. Analog zur NIS2-Richtlinie ist ebenfalls eine Erstmeldung, eine Zwischenmeldung sowie eine Abschlussmeldung abzugeben, siehe Artikel 19 Absatz 4 [31].

Während die NIS2-Richtlinie eine zu allgemeine Bewertung von erheblichen Sicherheitsvorfällen vornimmt, um sie auf die HAW Hamburg anwenden zu können, verhält es sich bei DORA umgekehrt. DORA ist eine speziell für den Finanzsektor konzipierte Verordnung. Während einige Kriterien, wie beispielsweise die Dauer des Vorfalls oder die Kritikalität der betroffenen Dienste, durchaus anwendbar sind, erweisen sich andere als ungeeignet, wie z. B. die geografische Ausbreitung. Die Schwellenwerte für Major Incidents sind ebenfalls für den Kontext einer Hochschule nicht geeignet. In diesem Zusammenhang wird darauf verzichtet, die Definition von Major Incidents, wie sie in DORA

vorgenommen wird, zu verwenden. Statt nur teilweise ein Bewertungsschema zu übernehmen, sollte ein Schema erarbeitet werden, welches den spezifischen Anforderungen der HAW Hamburg entspricht.

3.3 Freiwillige Meldepraktiken

Nachdem die bestehenden Meldepflichten für die HAW Hamburg identifiziert wurden, soll im Folgenden betrachtet werden, welche freiwilligen Meldepraktiken sinnvoll sind, auch wenn keine gesetzliche Pflicht dazu besteht.

Die HAW Hamburg ist Mitglied im Verein zur Förderung eines *Deutschen Forschungsnetzes e. V.* (DFN-Verein). Daher kann sie auch die Leistungen des DFN-CERTs in Anspruch nehmen. Das Leistungsspektrum des DFN-CERT umfasst unter anderem die Analyse und Beschaffung von Daten sowie die Bereitstellung von Hilfestellungen und Handlungsempfehlungen für das Incident Handling [22]. Darüber hinaus ist das DFN-CERT in der Lage, durch die Meldungen von Hochschulen bzw. Mitgliedern, Muster zwischen Incidents zu erkennen und seine Mitglieder vor Bedrohungen zu warnen. Dadurch können frühzeitig Gegenmaßnahmen ergriffen werden. Es empfiehlt sich daher, Vorfälle grundsätzlich an das DFN-CERT zu melden, sofern keine schwerwiegenden Gründe dagegen sprechen. Auf diese Weise können beide Seiten von den Erfahrungen des jeweils anderen profitieren [22]; [46].

Ein weitere Institution, an die die HAW Hamburg auf freiwillig melden sollte, ist das BSI. Die Meldungen werden verwendet, um ein und aussagekräftiges Lagebild für die Cybersicherheit in Deutschland zu erstellen und darauf basierend entsprechende Maßnahmen einzuleiten. Des weiteren kann die HAW Hamburg auch von der möglichen Unterstützung des BSIs profitieren [9]; [46].

4 Festlegung des Schweregrads für Information Security Incidents an der HAW Hamburg

Die Bestimmung des Schweregrads eines Incidents stellt einen wichtigen Bestandteil des Incident Handlings dar, da sie eine Reihenfolge der Bearbeitung vorgibt. Die Abarbeitung von Incidents sollte nicht nach dem First-In-First-Out-Prinzip erfolgen, da sich Incidents in ihren Auswirkungen auf eine Organisation erheblich unterscheiden können. Durch die Ermittlung des Schweregrads von Incidents soll sichergestellt werden, dass der Incident, mit der höchsten Priorität, auch vorrangig behandelt wird [16]. Die Notwendigkeit einer Priorisierung ergibt sich aus den begrenzten Ressourcen, über die die HAW Hamburg verfügt, um Incidents zu behandeln. Zudem wird durch die Bestimmung des Schweregrads festgelegt, welche Ressourcen zugewiesen werden, um den Incident zu behandeln.

4.1 Information Security Incident Schweregrad

Bei der Betrachtung der Sicherheitsleitlinien anderer Hochschulen wird ersichtlich, dass die Anzahl der Schweregrade, in die Incidents eingeordnet werden, in der Regel mindestens drei und maximal fünf beträgt [60]; [55]; [37]. Es existiert keine optimale Anzahl an möglichen Schweregraden. Die Anforderungen der Organisation, an der die Bewertung durchgeführt werden soll, sind dabei von Bedeutung um die Anzahl zu bestimmen. Für die HAW Hamburg werden vier Schweregrade eingeführt, siehe Tabelle 4.1.

Die Motivation für vier Schweregrade liegt in der Differenzierbarkeit von Incidents ohne eine zu starke Fragmentierung zu begünstigen. Der Schweregrad *Minor Incident* ist der niedrigste Schweregrad und wird im Rahmen des Tagesgeschäfts behandelt. Bei dem Schweregrad *Incident* und *Major Incident* kann durch die Differenzierung feingranularer unterschieden werden, wie schwerwiegend der Incident ist, was auch bei einer Auswertung

Schweregrad	Beschreibung
Krise	Die *Krise* stellt den höchsten Schweregrad dar. Incidents, die in diesen Schweregrad eingestuft werden, sind eine extreme Bedrohung für die HAW Hamburg. Incidents dieses Schweregrads werden vom Krisenmanagement bearbeitet, obwohl es sich streng genommen um eine IT-Krise handelt. Jede IT-Krise stellt auch eine Krise für die Geschäftsprozesse an der HAW Hamburg dar.
Major Incident	Incidents mit diesem Schweregrad, stellen eine hohe Bedrohung für die HAW Hamburg dar und müssen innerhalb des Incident Handlings beseitigt werden. Sie sind priorisiert im Vergleich zu regulären Incidents zu behandeln.
Incident	Incidents mit diesem Schweregrad, stellen sie eine Bedrohung für die HAW Hamburg dar und müssen innerhalb des Incident Handlings beseitigt werden.
Minor Incident	Incidents in dieser Stufe stellen eine geringe Bedrohung für die HAW Hamburg dar und sind innerhalb der regulären Tätigkeit des Incident Analyst zu beseitigen.

Tabelle 4.1: Beschreibung der unterschiedlichen Schweregrade für Incidents an der HAW Hamburg

hilfreich sein kann. Die Unterscheidung zwischen *Incident* und *Major Incident* erweist sich anhand der qualitativen Bewertung der Schweregrade, siehe Tabelle 4.1, als schwierig. Um Klarheit zu schaffen, ist es erforderlich, eindeutigere Bewertungskriterien zu definieren. Der Schweregrad *Krise* ist hingegen als klare Abgrenzung zu den vorherigen Schweregraden zu sehen und wird erst dann erreicht, wenn die HAW Hamburg massiv in ihrer Funktion als Hochschule beeinträchtigt ist.

4.2 Bewertungskriterien

Um den Schweregrad eines Incidents zu bestimmen, können verschiedene Bewertungskriterien herangezogen werden. In Tabelle 4.2 werden die Bewertungskriterien aus der ISO/IEC 27035, der NIST SP 800-61 Rev. 2 und dem *National Cyber Incident Scoring*

System (NCISS) von der *Cybersecurity and Infrastructure Security Agency* (CISA)[1] aufgeführt. Hierbei werden lediglich Kriterien berücksichtigt, welche in mindestens zwei der zuvor genannten Standards Erwähnung finden.

Kriterium	ISO/IEC 27035	NIST SP 800-61 Rev. 2	NCISS
Ausmaß der Vorfallsart	✓		✓
Operativer Einfluss	✓	✓	✓
Wiederherstellungsaufwand		✓	✓
Art der betroffenen Informationen	✓	✓	✓

Tabelle 4.2: Kriterien die bei der Ermittlung von Schweregraden von Incidents herangezogen werden

Die Ermittlung des Schweregrads erfolgt unter Berücksichtigung der vier identifizierten Kriterien.

4.2.1 Ausmaß der Vorfallsart

In Abschnitt 2.2 wurde bereits darauf verwiesen, dass für die Klassifikation von Incidents die Taxonomie von ENISA verwendet wird. Um die Taxonomie als Kriterium bei der Bestimmung des Schweregrads von Incidents zu nutzen, ist eine Bewertung der einzelnen Kategorien der Taxonomie erforderlich. Die CIA-Triade[2] bildet die Grundlage für diese Bewertung. Im Rahmen der Bewertung der einzelnen Kategorien werden die möglichen Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit der HAW Hamburg analysiert. Insgesamt stehen zur Bewertung vier Stufen zur Verfügung. Die Einordnung in die Stufe 0 erfolgt, sofern kein Schutzziel betroffen ist. Bei Betroffenheit eines Schutzziels erfolgt die Einordnung in die Stufe 1 etc. Es besteht die Möglichkeit, dass eine Kategorie mehreren Stufen zugeordnet werden kann. In Tabelle 4.3 findet sich ein Beispiel für die Kategorie *Information Gathering*.

[1] Die Cybersecurity and Infrastructure Security Agency (CISA) ist eine Bundesbehörde der Vereinigten Staaten von Amerika. Sie ist für die Cybersicherheit auf Bundesebene und die Koordination für die Sicherheit und Widerstandsfähigkeit kritischer Infrastrukturen zuständig [18].

[2] Die CIA-Triade stellt ein grundlegendes Konzept in der Informationssicherheit dar, welches die folgenden Schutzziele umfasst: **C**onfidentiality (Vertraulichkeit), **I**ntegrity (Integrität) und **A**vailability (Verfügbarkeit)

Schutzziele	Betroffen	Begründung
Vertraulichkeit	✓	Beim Sammeln von Informationen **können** die Angreifer, durch z. B. Aufzeichnen des Netzwerkverkehrs, an vertrauliche Informationen gelangen.
Integrität		Das Sammeln von Informationen durch einen Angreifer hat keine Auswirkungen auf die Integrität von Daten.
Verfügbarkeit		Das Sammeln von Informationen durch einen Angreifer hat keine Auswirkungen auf die Verfügbarkeit von Daten oder Systemen.

Tabelle 4.3: Bestimmung der Einstufung der Kategorie *Information Gathering* als Incident

Die Einstufung für die Kategorie *Information Gathering* erfolgt in Stufe 0 und Stufe 1, da lediglich das Schutzziel Vertraulichkeit potenziell verletzt wird. Ein weiteres Beispiel ist in Tabelle 4.4 aufgeführt, hier wird die Kategorie *Intrusion* behandelt.

Schutzziele	Betroffen	Begründung
Vertraulichkeit	✓	Bei dem erfolgreichen Eindringen in Netzwerke oder Systeme, durch einen Angreifer, ist die Vertraulichkeit in jedem Fall verletzt.
Integrität	✓	Häufig manipulieren Angreifer Dateien, wenn sie erfolgreich in ein Netzwerk oder System eingedrungen sind, um sich bei einem Angriff einen Vorteil zu schaffen oder Schaden anzurichten. Eine Verletzung der Integrität kann bei einer Intrusion daher nicht ausgeschlossen werden.
Verfügbarkeit	✓	Ist der Angreifer erfolgreich in Netzwerke oder Systeme eingedrungen, **kann** er deren Verfügbarkeit, z. B. durch den Einsatz einer Ransomware einschränken.

Tabelle 4.4: Bestimmung der Einstufung der Kategorie *Intrusion* als Incident

Die Einstufung für die Kategorie *Intrusion* erfolgt in Stufe 2 und Stufe 3, da die Schutzziele Vertraulichkeit und Integrität in jedem Fall verletzt werden. Bei dem Schutzziel

Verfügbarkeit hingegen kann es zu einer Verletzung kommen. Eine Einordnung für alle Kategorien der Taxonomie findet sich in Tabelle 4.5.

Art des Incidents	Stufe 0	Stufe 1	Stufe 2	Stufe 3
Abusive Content	✓			
Malicious Code			✓	✓
Information Gathering	✓	✓		
Intrusion Attempts	✓	✓		
Intrusions			✓	✓
Availability	✓	✓		
Information Content Security			✓	✓
Fraud	✓	✓		
Vulnerable	✓	✓		
Other	✓	✓	✓	✓

Tabelle 4.5: Bewertungsschema für das Kriterium Ausmaß der Vorfallsart

4.2.2 Operativer Einfluss und Art der betroffenen Informationen

Die Kriterien *Operativer Einfluss* und *Art der betroffenen Informationen* werden im Rahmen der Schutzbedarfsanalyse berücksichtigt. Bei einer Schutzbedarfsanalyse wird für alle an der Informationsverarbeitung beteiligten Geschäftsprozesse, verarbeiteten Informationen und die eingesetzte Informationstechnik ein Wert festgelegt, der Auskunft darüber gibt, welcher Schutzbedarf notwendig ist. Für die Bewertung wird gemäß des BSI-Standards 200-2 auf die Schutzziele Vertraulichkeit, Integrität oder Verfügbarkeit zurückgegriffen. Bewertet wird der zu erwartende Schaden bei einer Verletzung einer oder mehrerer Schutzziele [6].

Die Schutzbedarfsanalyse für die HAW Hamburg wird in einer separaten Arbeit behandelt. Für die Ermittlung des Schweregrads von Incidents wird davon ausgegangen, dass es fünf Schutzbedarfskategorien gibt: kein, niedrig, mittel, hoch, sehr hoch. Zudem wird angenommen, dass bei der Schutzbedarfsanalyse für die HAW Hamburg zumindest die Kriterien *Operativer Einfluss* und *Art der betroffenen Informationen* berücksichtigt werden [35].

4.2.3 Wiederherstellungsaufwand

Das Kriterium *Wiederherstellungsaufwand* dient der Bewertung des voraussichtlich benötigten Zeitraums sowie der erforderlichen Ressourcen, um das Incident Response durchzuführen und somit den Regelbetrieb wiederherzustellen [16]. In Tabelle 4.6 werden die einzelnen Bewertungsstufen aufgezeigt.

Einordnung	Beschreibung
Stufe 0	Die Zeit bis zur Wiederherstellung ist mit den vorhandenen Ressourcen vorhersehbar.
Stufe 1	Die Zeit bis zur Wiederherstellung ist mit zusätzlichen Ressourcen vorhersehbar.
Stufe 2	Die Zeit bis zur Wiederherstellung ist unvorhersehbar; zusätzliche Ressourcen und Hilfe von außen werden benötigt.
Stufe 3	Eine Wiederherstellung ist nicht möglich (z. B. wenn sensible Daten exfiltriert und veröffentlicht wurden); Einleitung einer Untersuchung.

Tabelle 4.6: Bewertungsstufen des Kriteriums Wiederherstellungsaufwand, entnommen aus [16]

4.3 Berechnung des Schweregrads

Bei Ermittlung des Schweregrads existieren unterschiedliche Ansätze. Das Rahmensicherheitskonzept der Stadt Hamburg zum Beispiel basiert auf einer Matrix, welche die Grundlage für die Festlegung des Schweregrads bildet. Dabei werden die potenziellen Auswirkungen sowie die Dringlichkeit in vier Stufen bewertet [56]. Der NCISS von CISA hingegen berechnet den Schweregrad mittels eines gewichteten Mittelwerts. Der Vorteil dieser Methode liegt in der Möglichkeit, einzelnen Kriterien bei der Ermittlung des Schweregrads ein stärkeres Gewicht zu verleihen [21].

Für die HAW Hamburg bietet es sich ebenfalls an den Schweregrad mit Hilfe des gewichteten Mittelwerts zu ermitteln, da sich der Schutzbedarf aus mehreren Kriterien zusammensetzt. Bei der Berechnung kann dies entsprechend gewichtet werden. Aus diesem Grund wird der gewichtete Mittelwert als Berechnungsansatz zur Bestimmung des

Schweregrads gewählt. Im Vergleich zu den übrigen Kriterien erfolgt daher eine Gewichtung des Schutzbedarfs um den Faktor 2. Die Punkte, aus denen sich der gewichtete Mittelwert berechnet, definieren die Stufen für die Kriterien *Ausmaß der Vorfallsart* und *Wiederherstellungsaufwand*. Für die Stufe 0 sind demnach null Punkte zu berücksichtigen, für die Stufe 1 entsprechend ein Punkt usw.. Bei dem Schutzbedarf gehen die Punkte von null für den Schutzbedarf *kein* bis vier für den Schutzbedarf *sehr hoch*. Für die Berechnung des gewichteten Mittelwerts werden zunächst die einzelnen Kriterien normiert, siehe Gleichung 4.1.

$$\tilde{x} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{4.1}$$

Im Anschluss an die Normierung der einzelnen Kriterien wird der gewichtete Mittelwert auf einer Skala von 0 bis 100 berechnet und auf die nächsthöhere ganze Zahl gerundet. Siehe dafür Gleichung 4.2.

$$\bar{x}_{\text{gewichtet}} = \left\lceil \frac{\sum_{i=1}^{n} w_i \cdot (\tilde{x}_i \times 100)}{\sum_{i=1}^{n} w_i} \right\rceil \tag{4.2}$$

Hierbei sind:

- $\tilde{x}_i$ die normierten Werte der Variablen x,
- w_i die Gewichte,
- n die Anzahl der Werte.

Das Ergebnis $\bar{x}_{\text{gewichtet}}$ definiert den Schweregrad des Incidents. Der entsprechende Schweregrad kann anhand der Tabelle 4.7 abgelesen werden.

Schweregrad	Punktzahl
Krise	90 - 100
Major Incident	70 - 89
Incident	40 - 69
Minor Incident	0 - 39

Tabelle 4.7: Zuordnung der gewichteten Punktzahl zu den Schweregraden für Incidents

Im Folgenden soll die Ermittlung des Schweregrads anhand zweier exemplarischer Szenarien verdeutlicht werden.

Szenario 1: Die HAW Hamburg ist von einem umfassenden Ransomware-Angriff betroffen, wodurch Nutzer keinen Zugriff auf wichtige Systeme und Dateien haben. Zudem ist es den Systembetreibern nicht möglich, Nutzerrechte einzusehen oder zu ändern. Es besteht eine hohe Wahrscheinlichkeit, dass personenbezogene Daten kompromittiert wurden. Für die Berechnung des Schweregrads siehe Tabelle 4.8.

Kategorie	x	$\tilde{x}$	w
Ausmaß der Vorfallsart	3	1	1
Schutzbedarf	4	1	2
Wiederherstellungsaufwand	3	1	1

Tabelle 4.8: Bewertung des Schweregrads des in Szenario 1 beschriebenen Ereignisses

Die Berechnung ergibt einen Höchstwert von 100, wodurch der Incident aus dem Szenario 1 als *Krise* klassifiziert werden kann.

Szenario 2: Der Internetauftritt der HAW Hamburg ist nicht erreichbar, da der Webserver einem DDoS-Angriff ausgesetzt ist. Die Angreifer benutzen nur wenige IP-Adressen, um den Angriff durchzuführen. Um den Angriff zu unterbinden, ist eine Anpassung der Firewall-Regeln erforderlich. Für die Berechnung des Schweregrads siehe Tabelle 4.9.

Kategorie	x	$\tilde{x}$	w
Ausmaß der Vorfallsart	1	$0,3\overline{3}$	1
Schutzbedarf	0	0	2
Wiederherstellungsaufwand	0	0	1

Tabelle 4.9: Bewertung des Schweregrads des in Szenario 2 beschriebenen Ereignisses

Bei einer Berechnung des gewichteten Mittelwerts ergibt sich eine Punktzahl von 9, was die Einstufung als *Minor Incident* zur Folge hat.

5 Incident Handling an der HAW Hamburg

Zunächst werden die am Prozess beteiligten Rollen identifiziert. Anschließend erfolgt ein Vergleich der Rollen mit dem *Computer Security Incident Response Team (CSIRT) Services Roles and Competencies* von FIRST. In Unterabschnitt 2.4.4 wurde bereits die ISO/IEC 27035 als Rahmenwerk für das Incident Handling ausgewählt. In diesem Kapitel werden die einzelnen Phasen des Incident Handlings vorgestellt. Basierend auf Rollen und Phasen werden RASCI-Matrizen erstellt. Im Folgenden soll eruiert werden, an welchen Stellen und aus welchen Gründen bei der Modellierung des Prozesses von der ISO/IEC 27035 abgewichen wurde.

5.1 Rollen

Im Rahmen der Gestaltung des Incident Handling Prozesses ist eine eindeutige Zuteilung von Aufgaben zu Rollen von hoher Bedeutung, um potenzielle Kompetenzkonflikte zu verhindern. Bei der Benennung der Rollen ist zu berücksichtigen, dass das Incident Handling und damit die direkt beteiligten Rollen in eine bereits bestehende Abteilung, das Informationstechnik Service Center (ITSC), integriert werden. Dies hat zur Konsequenz, dass strategische Rollen wegfallen. Des Weiteren ist zu berücksichtigen, dass die HAW Hamburg über begrenzte finanzielle sowie personelle Ressourcen verfügt. Eine zu starke Fragmentierung der Rollen ist daher zu vermeiden.

Bei der Modellierung der Rollen wurde sich an der ISO/IEC 27035 orientiert, wobei einige Rollen zusammengefasst oder aufgrund der zuvor genannten Gegebenheiten nicht weiter berücksichtigt wurden. Die Identifikation der Rollen erfolgte im Rahmen von vorherigen Arbeiten [47]; [48]. Insgesamt wurden neun Rollen identifiziert, die im Folgenden kurz vorgestellt werden.

Nutzer: Nutzer sind von entscheidender Bedeutung für das Incident Handling. Sobald Nutzer Events im Kontext der Informationssicherheit feststellen, sollten sie eine entsprechende interne Meldung über festgelegte Meldewege abgeben. Dafür ist eine Sensibilisierung der Nutzer von zentraler Bedeutung [47]; [48]. Die Rolle der Nutzer lässt sich in weitere Unterrollen, wie beispielsweise Studierende oder Angestellte, aufgliedern. Im Rahmen des Prozesses sind sie jedoch, trotz unterschiedlicher Berechtigungen und Befugnisse, als gleichwertig zu betrachten, da sie im Rahmen des Incident Handling die gleiche Funktion erfüllen [47]; [48].

Systembetreiber: Ebenso wie Nutzer können Systembetreiber das Incident Handling initiieren, indem sie Events frühzeitig erkennen und melden. Darüber hinaus fungieren sie bei einer Analyse von Incidents als Point of Contact für zusätzliche Informationen über ihr System. Auch ihre Mitwirkung beim Incident Response ist von hoher Relevanz, da sie über entsprechende Rechte am System verfügen, um tiefgreifende Systemänderungen vorzunehmen [47]; [48].

Die HAW Hamburg ist im Hinblick auf die Systembetreiber fragmentiert, was auf die Aufteilung in Fakultäten und Departments, sowie anderen Einheiten zurückzuführen ist, die zum Teil ihre eigenen Systeme betreiben. Zentrale Dienste wie beispielsweise myHAW, HAW-Mailer und HAW-Cloud sowie die Verwaltung des IT-Betriebs mit dem Identity Management werden hingegen vom ITSC als zentralem Systembetreiber betrieben. Das ITSC ist dem Kanzler der HAW Hamburg unterstellt. Im Rahmen des Incident Handling ist eine Aufteilung der Rolle jedoch nicht erforderlich [47]; [48].

Monitoring Expert: Der Monitoring Expert fungiert als Point of Contact (PoC) für die Meldungen der Nutzer und Systembetreiber. Die Rolle ist im ITSC angesiedelt und hat die Aufgabe, die Systeme und den Netzwerkverkehr zu überwachen, um Events zu identifizieren und zu dokumentieren. Dazu wird in der Regel ein Security Information and Event Management (SIEM) eingesetzt [47]; [48].

Incident Analyst: Der Incident Analyst zeichnet sich durch eine hohe technische Expertise im Bereich der Analyse aus. Er unterstützt den Incident Coordinator bei der Einschätzung von Potential Incidents durch umfassende Systemanalysen. Zudem kann er im Rahmen der Incident Response unterstützend tätig werden [47]; [48].

Incident Responder: Der Incident Responder ist zuständig für die Koordinierung und Überwachung der Incident Response. In der Regel erfolgt durch den Incident Responder eine Zuweisung von Aufgaben an die Systembetreiber, da die Systembetreiber über die

notwendigen Rechte am betroffenen System oder Netzwerk verfügen. In vielen Fällen existieren mehrere Incident Responder, die sich in ihren Fachkenntnissen unterscheiden [47]; [48].

Incident Coordinator: Der Incident Coordinator nimmt eine leitende Rolle beim Incident Handling ein. Zu seinen Aufgaben gehört die Koordination der Incident Responder sowie die Funktion als Schnittstelle zwischen den internen Rollen, die an der Bewältigung von Incidents beteiligt sind, und dem CISO der HAW Hamburg. Darüber hinaus ist der Incident Coordinator für die Überprüfung und Klassifizierung von Potential Incidents im Rahmen der Triage verantwortlich. Es obliegt auch seiner Zuständigkeit das Incident Response für abgeschlossen zu erklären [47]; [48].

CISO: Der *Chief Information Security Officer* (CISO) trägt die Verantwortung für die Informationssicherheit an der HAW Hamburg. Zu seinen Zuständigkeiten zählen die Untersuchung von Incidents sowie die Erarbeitung verschiedener Sicherheitskonzepte. Der CISO wird in jedem Fall bei entscheidenden Momenten im Incident Handling, wie beispielsweise der Ausrufung einer *Krise*, konsultiert. Durch seine Expertise kann er den Incident Handling Prozess mitgestalten und seine Funktion überwachen. Der CISO berichtet dabei direkt dem Präsidium [47]; [48].

Management: Die Rolle des Managements umfasst alle organisatorischen Einheiten der HAW Hamburg. Dazu zählt zunächst das Präsidium als höchste Leitungsinstanz, darüber hinaus aber auch die vier Fakultäten, welche sich wiederum in Departments unterteilen [47]; [48].

Externe Akteure: Externe Akteure ist ebenfalls eine Rolle, welche sich aus mehreren eigenständigen Entitäten zusammensetzt. Beim Incident Handling sind sie in ihren Aufgaben und Funktionen jedoch als homogen zu betrachten und werden daher zusammengefasst. Die Rolle umfasst dabei unter anderem die Behörde für Wissenschaft, Forschung und Gleichstellung und Bezirke (BWFGB) der Freien und Hansestadt Hamburg. Die HAW Hamburg ist verpflichtet, Datenschutzverletzungen an die Behörde zu melden. Des Weiteren sind auch andere Organisationen zu berücksichtigen, denen gegenüber die HAW Hamburg freiwillig über Events oder Incidents berichtet, beispielsweise das BSI oder das DFN-CERT. Neben Organisationen fallen unter die Definition auch einzelne Entitäten wie z. B. externe Systembetreiber [47]; [48].

Ein Ziel der Arbeit ist es, ein Rollenkonzept zu erschaffen, das die begrenzten personellen Ressourcen der HAW Hamburg berücksichtigt. Aus diesem Grund wird darauf verzichtet,

den Incident Responder als permanente Rolle zu etablieren. Anstelle einer permanenten Ernennung soll der Incident Responder ad hoc ernannt werden, sobald ein Bedarf an dieser Rolle im Rahmen des Incident Handlings festgestellt wird. Da in der Praxis häufig mehrere Incident Responder in die Response eingebunden sind, werden sie in dieser Arbeit in einem Team, dem sogenannten Ad-hoc-Team, zusammengefasst. Die Größe des Teams kann dabei variieren, in Abhängigkeit vom Umfang des Incidents sowie den benötigten Fachkenntnissen der Incident Responder [47]; [48].

Die zeitliche Dauer der Existenz des Teams ist begrenzt. Sofern der Incident eingedämmt ist und lediglich noch die Beseitigung von Indicators of Compromise (IoC) sowie die Wiederherstellung des Normalbetriebs erforderlich sind, kann das Ad-hoc-Team aufgelöst werden oder sofern absehbar ist, dass die Maßnahmen eine bestimmte Anzahl an Tagen übersteigen werden. Dies entspricht auch den Anforderungen der HAW Hamburg, die personellen Ressourcen möglichst schnell wieder freizugeben [47]; [48].

Um die Rollen und deren Zuständigkeitsbereiche zu veranschaulichen, erfolgt in Abbildung 5.1 eine Darstellung in Form eines Venn-Diagramms.

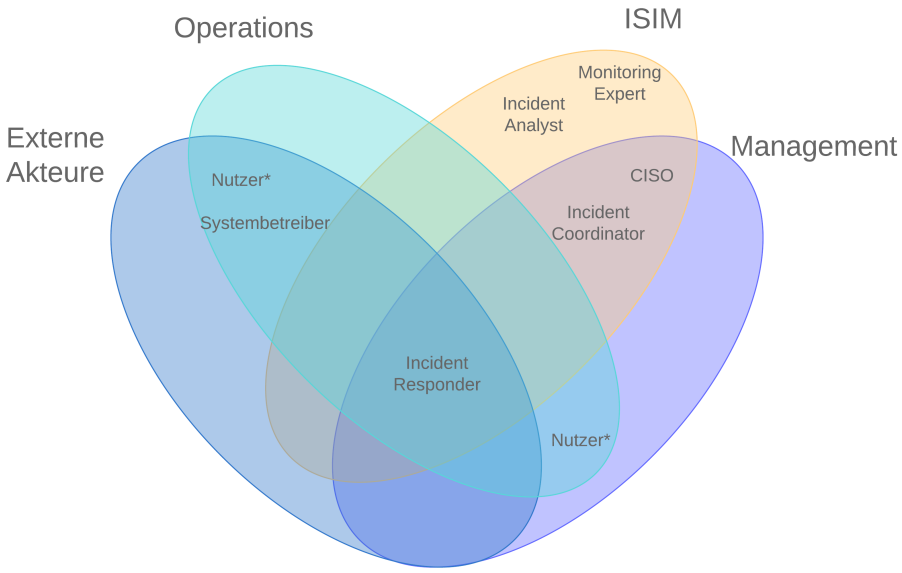

Abbildung 5.1: Rollenmodell des neuen Prozesses für Incident Handling an der HAW Hamburg, auf Basis von [48]

Die Zuständigkeitsbereiche werden dabei als Mengen dargestellt, welche *Externe Akteure*, *Operation*, *ISIM* sowie *Management* umfassen. Die Mengen *Externe Akteure* und *Management* umfassen sowohl Zuständigkeitsbereiche als auch Rollen im Incident Handling. Der Zuständigkeitsbereich *Operation* bezeichnet das operative Geschäft der HAW Hamburg. Der Zuständigkeitsbereich *ISIM* umfasst sämtliche Rollen, die maßgeblich am Incident Handling beteiligt sind. Die Rollen, welche beim Incident Handling nur informiert werden oder Events melden, sind davon losgelöst.

In Tabelle 5.1 werden die am ISIM beteiligten Rollen aufgeführt. Dabei wird zwischen permanent vorhandenen Rollen und ad hoc ernannten Rollen unterschieden.

Rolle	Typ (Permanent/Ad hoc)	Kriterium für Ernennung
Monitoring Expert	Permanent	
Incident Analyst	Permanent	
Incident Responder	Ad hoc	Vorliegen eines *Incidents*, *Major Incidents* oder *Krise*
Incident Coordinator	Permanent	
CISO	Permanent	

Tabelle 5.1: Unterscheidung von permanenten und ad hoc Rollen innerhalb des ISIMs

5.2 Vergleich der Rollen mit FIRST

FIRST wurde mit dem Ziel gegründet, die Kommunikation und den Austausch zwischen CSIRTs zu ermöglichen und zu verbessern. Zurzeit sind 759 Teams (Stand: 05.09.2024) Mitglied bei FIRST. Es gibt keine geografische Beschränkung. Im Rahmen von der Arbeit von FIRST werden zahlreiche Standards und Publikationen verfasst. Eine davon beschäftigt sich mit der Arbeit eines CSIRTs, das CSIRT Services Framework. In diesem Standard wird auch das Thema ISIM behandelt. FIRST richtet sich dabei mit dem Dokument nicht an spezifische CSIRTs, sondern will für alle CSIRTs gültig sein. Für die Kompatibilität wird der Standard *Computer Security Incident Response Team (CSIRT) Services Roles and Competencies* von FRIST mit der in dieser Arbeit entworfenen Lösung verglichen. Dabei werden die einzelnen Rollen miteinander verglichen und untersucht, wo

Unterschiede und Gemeinsamkeiten bestehen. Das Ziel ist es ein Mapping zwischen der Lösung dieser Arbeit und dem Standard von FIRST zu erstellen.

Bei FIRST wird das ISIM auf insgesamt sechs Rollen aufgeteilt:

- Communication Liaison
- Incident Analyst
- Incident Responder
- Incident Triage Coordinator
- IT Administrator
- Malware/Forensic Analyst

Für die Vergleichbarkeit der beiden Rollenkonzepte, wird zunächst die jeweilige Rolle von FIRST vorgestellt und ihre Aufgaben. FIRST hat für jede Rolle einen Abschnitt in dem die allgemeinen Aufgaben der Rolle aufgeführt werden. Bei jeder Aufgabe wird überprüft, ob und zu welcher Rolle sie aus dem in dieser Arbeit entworfenen Rolle passt. Für eine bessere Differenzierung der beiden Rollenkonzepte, steht hinter jeder Rolle aus welcher Arbeit sie entnommen wurde.

Der *Communication Liaison* (FIRST) ist für die Kommunikation mit den Medien zuständig und dient als dessen Ansprechpartner. Darüber hinaus ist er für die Verwaltung der Kommunikation mit den Betroffenen von Incidents verantwortlich. Ebenso bietet er Beratung und Unterstützung für eine angemessene Kommunikation an. In Tabelle 5.2 sind seine Aufgaben den Rollen für den Prozess an der HAW Hamburg zugeordnet.

Die Aufgaben des *Communication Liaison* (FIRST) sind im Incident Handling der HAW Hamburg auf mehrere Rollen aufgeteilt. Das *Management* (HAW), konkret die Stabsstelle Presse und Kommunikation, übernimmt beispielsweise die Aufgabe der Kommunikation mit den Medien, eine klare Trennung und Zuordnung dieser Aufgabe ist jedoch schwierig, da sie zu generisch ist. Ebenso kommuniziert der Datenschutzbeauftragte oder *CISO* (HAW) mit den Betroffenen. Insofern sind die Aufgaben, die die Rolle abbildet, bedacht, aber aufgeteilt.

Der *Incident Analyst* (FIRST) ist dafür zuständig, mögliche Beziehungen zwischen Events und Incidents zu identifizieren, um ein effektiveres Incident Handling zu ermöglichen.

Aufgabe	Rolle (HAW)
1. Management der Kommunikation mit den Medien	Management
2. Verwaltung der Informationsverteilung an die Betroffenen	CISO
3. Kontaktstelle für die Kommunikation mit den Medien	Management
4. Unterstützung und Beratung des Krisenmanagement-teams bei der Krisenkommunikation	CISO
5. Beratung zu Kommunikationsstrategie, -prozessen und -verfahren	CISO

Tabelle 5.2: Zuordnung der Aufgaben des *Communication Liaison* (FRIST) zu den Rollen im Prozess für die HAW Hamburg

Darüber hinaus ist er für die Bewertung des potenziellen Schadens durch Incidents verantwortlich. Seine Aufgaben sind in Tabelle 5.3 aufgeführt.

Aufgabe	Rolle (HAW)
1. Analysieren von Events, Potential Incidents, Incidents	Monitoring Expert, Incident Analyst, Incident Coordinator
2. Bewertung der möglichen und tatsächlichen Auswirkungen und Schäden	Incident Analyst, Incident Coordinator
3. Analyse von Incidents zur Ermittlung von Ursachen und Auswirkungen	Incident Analyst, Incident Coordinator
4. Analysieren von mehren Incidents über einen längeren Zeitraum	Incident Analyst
5. Durchführung von initialen Analysen von Artefakten	Monitoring Expert
6. Suche von Schwachstellen, die den Incidents verursacht haben	Incident Analyst
7. Korrelation von Events und Incidents	Incident Coordinator

Tabelle 5.3: Zuordnung der Aufgaben des *Incident Analyst* (FIRST) zu den Rollen im Prozess für die HAW Hamburg

Im Gegensatz zu den in dieser Arbeit aufgeführten Rollen existiert eine Rolle wie der *Monitoring Expert* (HAW), der sich nur um die Begutachtung der Events kümmert, bei FIRST nicht. Daher werden einige Aufgaben der Rolle des *Incident Analyst* (FIRST) auf den *Monitoring Expert* (HAW) und den *Incident Analyst* (HAW) aufgeteilt. Darüber

hinaus übernimmt der *Incident Coordinator* (HAW) einige Aufgaben des *Incident Analyst* (FIRST), da dieser für die Durchführung der Triage und damit für die Korrelation von Potential Incidents zu Incidents zuständig ist.

Der *Incident Responder* (FRIST) ist bei bestätigten Incidents dafür zuständig, den Incident einzudämmen, um eine möglichst geringe Anzahl an betroffenen Personen bzw. Systemen sicherzustellen. Zudem obliegt ihm die Verantwortung, den Incident zu überwachen und alle relevanten Informationen über den Incident sowie dazugehörige Events zu sammeln. Eine detaillierte Aufstellung der Aufgaben ist in Tabelle 5.4 aufgeführt.

Aufgabe	Rolle (HAW)
1. Koordinierung der Sammlung und Analyse von Informationen über Incidents	Incident Responder
2. Erstellen von Recovery Plänen und Unterstützung bei Incident Response	Incident Responder
3. Koordination der Kommunikation, der Aktivitäten und der Informationsweitergabe	Incident Responder

Tabelle 5.4: Zuordnung der Aufgaben des *Incident Responder* (FIRST) zu den Rollen im Prozess für die HAW Hamburg

Ähnlich wie bei FIRST ist der *Incident Responder* (HAW) beim Incident Response dafür zuständig, die Koordination zu übernehmen. Daher lassen sich alle Aufgaben dem *Incident Responder* (HAW) zu ordnen.

Der *Incident Triage Coordinator* (FIRST) ist für die Analyse und Verifizierung von Events sowie die Bewertung von Incidents verantwortlich. Zudem steht er in engem Austausch mit anderen Stakeholdern, wie beispielsweise der IT-Abteilung oder Softwareanbietern. Die Aufgaben des *Incident Triage Coordinator* (FIRST) sind in Tabelle 5.5 dargestellt.

Die zuständige Rolle bei den Aufgaben 3 und 4 ist in Klammern gesetzt, da diese Aufgaben nicht explizit in dieser Arbeit erwähnt werden, jedoch die prinzipielle Zuständigkeit bei der jeweiligen Rolle liegt. Die Analyse von Events sowie die Bestimmung von Potential Incidents obliegen dem *Monitoring Expert* (HAW), im Gegensatz zur Vorgehensweise von FRIST. Das Ziel besteht in einer Reduzierung der Potential Incidents durch die Identifikation von False Positives, um den *Incident Coordinator* (HAW) zu entlasten.

Aufgabe	Rolle (HAW)
1. Analysieren von Events und überprüfen ob die Meldung valide ist	Monitoring Expert
2. Erkennen, analysieren und bestimmen von Potential Incidents	Monitoring Expert
3. Konfiguration von Tools zur Unterstützung der Triage	(Incident Coordinator)
4. Informieren über andere Incidents in anderen Organisationen, um bei ähnlichen Vorfällen bei der Triage besser vorbereitet zu sein	(Incident Coordinator)
5. Lesen und Verstehen von Vulnerability Reports, um eine Handlungsstrategie zu entwerfen	Incident Coordinator
6. Eskalation des Ergebnisses der Triage bei Bedarf	Incident Coordinator

Tabelle 5.5: Zuordnung der Aufgaben des *Incident Triage Coordinator* (FIRST) zu den Rollen im Prozess für die HAW Hamburg

Der *IT Administrator* (FIRST) nimmt bei FIRST eine besondere Rolle ein. Die Autoren gehen jedoch nicht davon aus, dass er Teil eines CSIRTs ist. Die Rolle wird jedoch für ein umfassenderes Verständnis aufgeführt. Der *IT Administrator* ist dafür verantwortlich, die Systeme nach einem Zwischenfall wieder in Betrieb zu nehmen. Die Aufgaben sind in Tabelle 5.6 beschrieben.

Aufgabe	Rolle (HAW)
1. Wiederherstellung von Benutzer-/Systemdaten aus Backup Dateien	Systembetreiber
2. Wiederherstellung von Konfigurationen aus Backup Dateien	Systembetreiber
3. Aktivieren deaktivierter Dienste und Wiederherstellung des Zugangs für Benutzer/Systeme/Netzwerke	Systembetreiber
4. Durchführen von funktionalen Tests, um die Kapazität und Fähigkeit der Systeme/Services/Netzwerke zu überprüfen	Systembetreiber

Tabelle 5.6: Zuordnung der Aufgaben des *IT Administrator* (FIRST) zu den Rollen im Prozess für die HAW Hamburg

Wie bei FIRST wird auch in dieser Arbeit die Rolle des *Systembetreibers* (HAW) eingeführt, der für die Durchführung von Änderungen und Wiederherstellungsmaßnahmen an seinen Systemen zuständig ist. Die Auffassung von FIRST und dem entwickelten Prozess für die HAW sind daher in diesem Punkt identisch.

Der *Malware/Forensic Analyst* (FIRST) ist dafür zuständig, Artefakte zu untersuchen, um ein breiteres Verständnis über den Incident und eine mögliche eingesetzte Malware zu erlangen. Die Aufgaben des *Malware/Forensic Analyst* (FIRST) sind in Tabelle 5.7 dargestellt.

Aufgabe	Rolle (HAW)
1. Durchführung der Analyse von Artefakten und forensischen Beweisen	Incident Analyst
2. Analyse der Malware um zu ermitteln, wie die Anwendung es geschafft hat die Detektion zu verhindern und den Host zu infiltrieren konnte	Incident Analyst
3. Suche von Schwachstellen, die den Incidents verursacht haben	Incident Analyst
4. Analyse und Korrelation von Incidents	Incident Analyst

Tabelle 5.7: Zuordnung der Aufgaben des *Malware/Forensic Analyst* (FIRST) zu den Rollen im Prozess für die HAW Hamburg

Die Rolle des *Malware/Forensic Analyst* (FIRST) wird vollständig vom *Incident Analyst* (HAW) übernommen. Aus der Perspektive der HAW ist eine Aufteilung der Rolle nicht erstrebenswert. Dies ist dadurch begründet, dass möglichst wenig Personalressourcen verwendet werden sollen, um dies zu erreichen wird auf eine geringere Fragmentierung der Rollen geachtet. Sollte der Bedarf an einem Experten für die Analyse von Malware entstehen, muss dieser extern bezogen werden.

In Abbildung 5.2 ist die Zuordnung der Rollen visuell dargestellt.

Neben den reinen Aufgaben führt das Dokument von FIRST auch aus, welche Kompetenzanforderungen an die jeweilige Rolle gestellt wird. Mit Hilfe der Zuordnung, kann aus dem Dokument abgelesen werden, welche Kompetenzen z. B. ein *Incident Responder* (HAW) generell als auch rollenspezifisch erfüllen sollte. Die Kompetenzen können als Grundlage für die Auswahl eines geeigneten Mitarbeiters dienen.

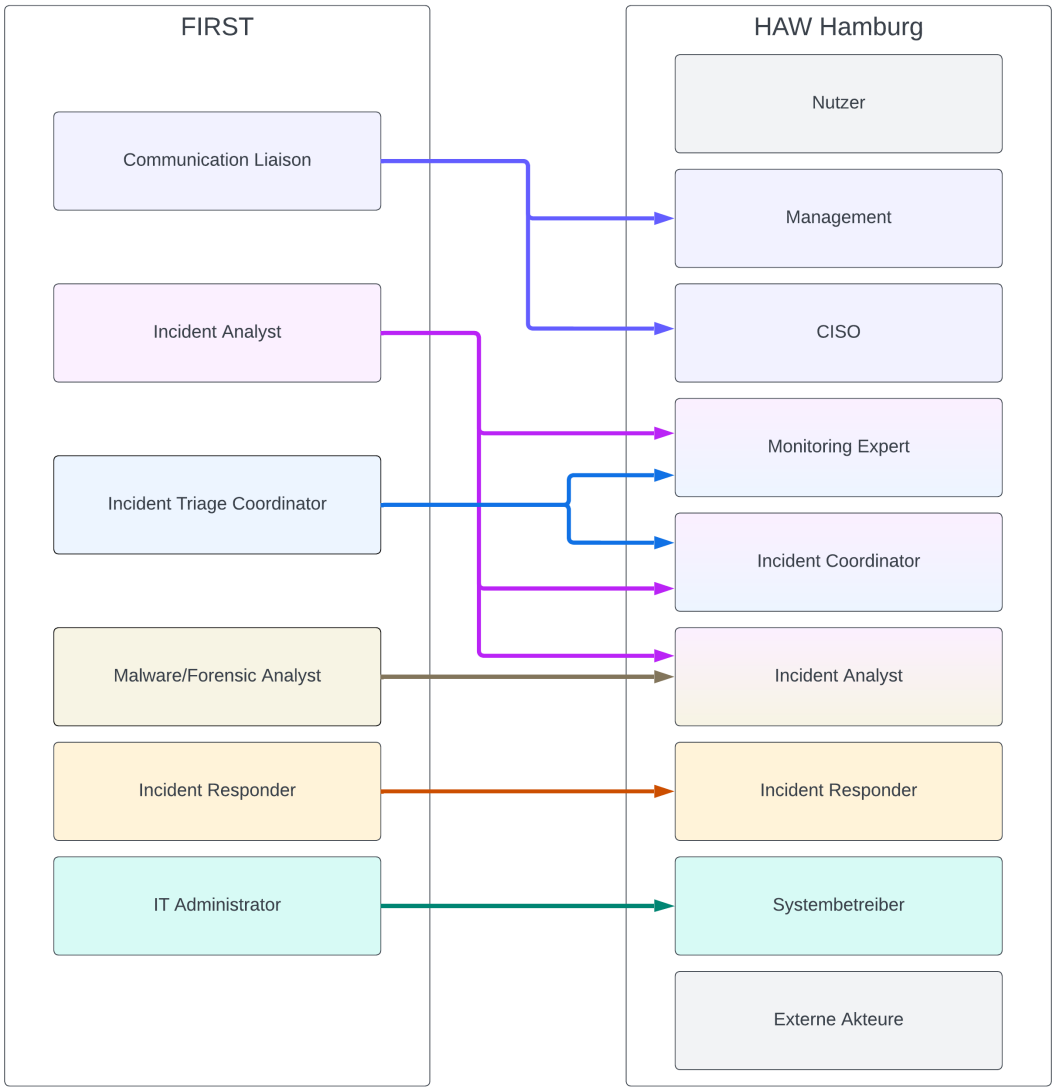

Abbildung 5.2: Zuordnung der Rollen von FIRST zu den Rollen für das Incident Handling an der HAW Hamburg, eigene Darstellung

5.3 Incident Handling Prozess

Der Incident Handling Prozess gliedert sich nach der ISO/IEC 27035 in vier Phasen:

- Detect and Report
- Assess and Decide
- Respond
- Learn Lessons

Die vier Phasen werden auch auf das Incident Handling an der HAW Hamburg übertragen. Für die Modellierung der Phasen wird die *Business Process Model and Notation* (BPMN) verwendet. Die Grundlagen der Prozessdiagramme wurden in vorangeangen Arbeiten erstellt [47]; [48]. Von essentieller Bedeutung für den Erfolg des Incident Handlings ist die lückenlose Dokumentation der gewonnenen Informationen. Aus diesem Grund wird bei der Modellierung darauf verzichtet, dies als zusätzliche Aktivität aufzuführen, sondern wird für jede Aktivität als inhärente Aufgabe und Verpflichtung gesehen.

5.3.1 Detect and Report

Initiiert wird das Incident Handling durch die Detektion eines Events im Kontext der Informationssicherheit, siehe Abbildung 5.3. Dies kann durch Personen, wie beispielsweise Nutzer oder Systembetreiber, automatisiert durch Intrusion Detection Systems (IDS) oder durch externe Akteure wie beispielsweise das DFN-CERT erfolgen. In Bezug auf die Events fungiert der Monitoring Expert als PoC. Die Erfassung der Events erfolgt mittels eines Event Reports, welcher an einer zentralen Stelle hinterlegt wird [47]; [48].

Anschließend erfolgt eine Plausibilitätsprüfung durch den Monitoring Expert, um festzustellen, ob es sich um einen Potential Incident handelt oder ob ein Fehlalarm vorliegt. Bei einer entsprechenden Unsicherheit bei der Prüfung oder bei der Einstufung als Potential Incident erfolgt eine Benachrichtigung des Incident Coordinators, sodass das Incident Handling in die nächste Phase *Assess and Decide* übergeht. Der Zusammenhang zwischen Event, Potential Incident und Incident wird in Abschnitt 2.1 behandelt [47]; [48].

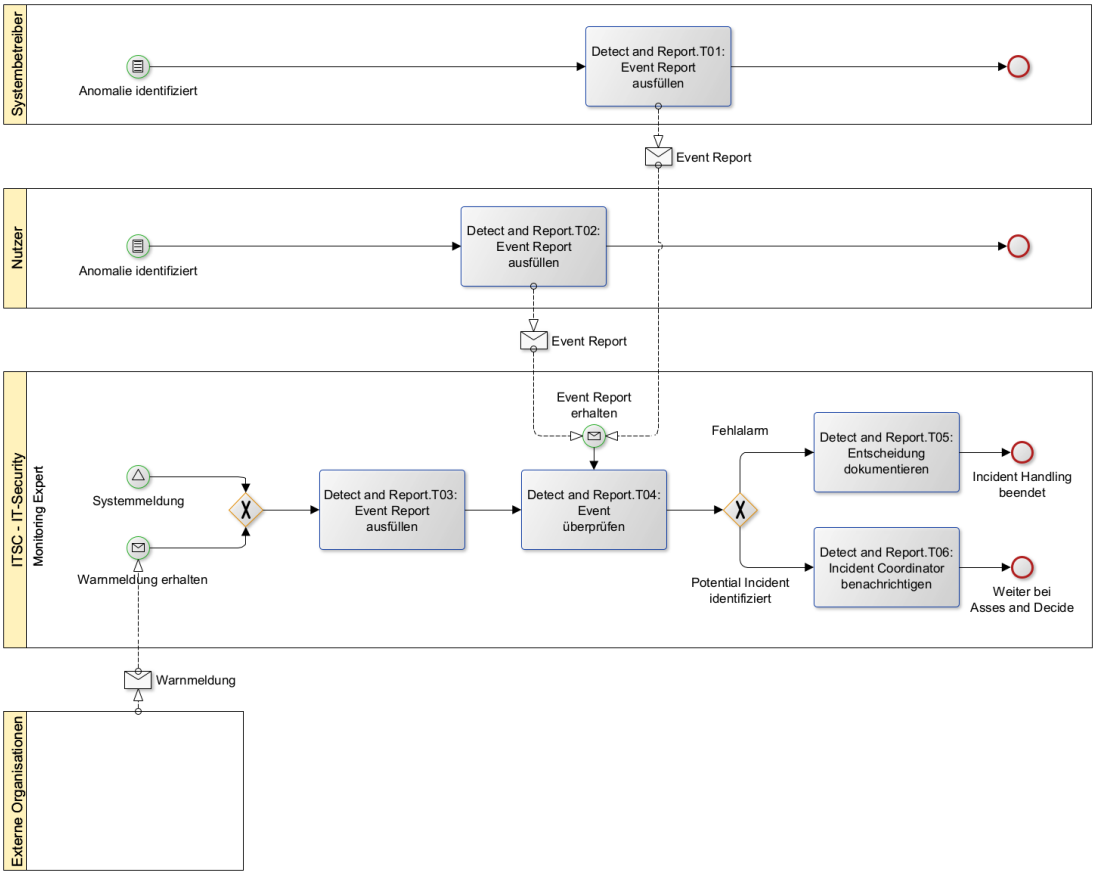

Abbildung 5.3: Prozessdiagramm für die Phase *Detect and Report*, auf Basis von [48]

5.3.2 Assess and Decide

In der Phase *Assess and Decide*, siehe Abbildung A.2 erfolgt durch den Incident Coordinator eine Durchführung der Triage. Die Triage ist in drei Schritte unterteilt, siehe Abbildung 5.5. Im ersten Schritt erfolgt eine Überprüfung, ob tatsächlich ein Incident vorliegt. Zu diesem Zweck wird eine initiale Analyse durchgeführt. Anschließend wird, sofern der Incident bestätigt wurde, der Incident mit anderen Incidents in Relation gesetzt, um festzustellen, ob ein Zusammenhang mit einem bereits bestehenden Incident besteht. Sofern diese Voraussetzung nicht gegeben ist, erfolgt im letzten Schritt die Festlegung des Schweregrads [47]; [48].

Falls ein Incident festgestellt wird erfolgt eine Überprüfung der Meldepflichten, siehe Abbildung 5.6, sowie, abhängig vom Schweregrad, eine Benachrichtigung des Managements

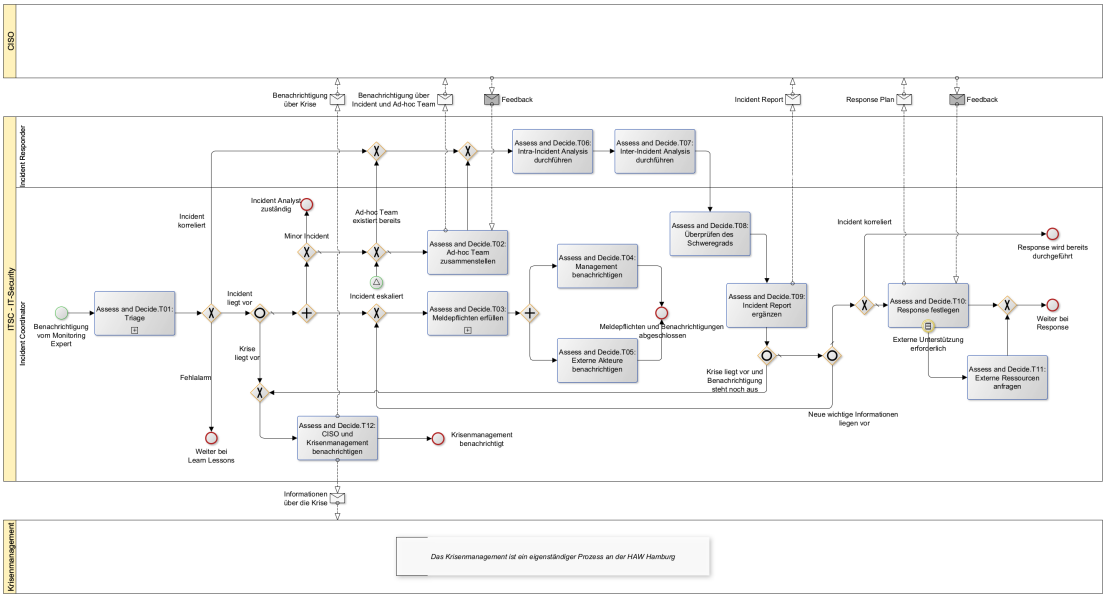

Abbildung 5.4: Prozessdiagramm für die Phase *Assess and Decide*, auf Basis von [48]

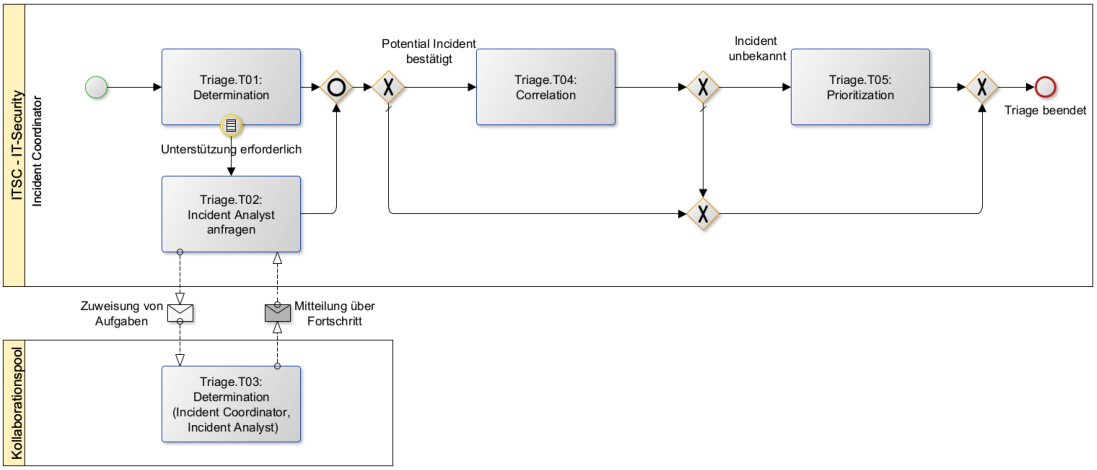

Abbildung 5.5: Prozessdiagramm für den Unterprozess *Triage* aus der Phase *Assess and Decide*, auf Basis von [48]

und gegebenenfalls externer Akteure. Bei der Benachrichtigung externer Akteure ist das Management zu informieren. Im Falle einer Einstufung des Incidents als Schweregrad *Incident* oder *Major Incident* erfolgt die Bildung eines Ad-hoc-Teams, dessen Ziel es ist, durch tiefgreifende Analysen ein umfassendes Bild über den Incident zu erlangen. Daraufhin legt der Incident Coordinator das Incident Response fest, wodurch diese Phase

abgeschlossen wird. Im Falle einer *Krise* ist das Krisenmanagement zuständig, welches als separater Prozess zu betrachten ist, sodass dies nicht Gegenstand der vorliegenden Arbeit ist. Das Vorliegen einer *Krise* beendet jedoch nicht das Incident Handling, es ändern sich lediglich die Verantwortlichkeiten. Statt dass der CISO übergeordnet das Incident Handling leitet, übernimmt der Krisenstab diese Funktion, wobei der CISO Teil vom Krisenstab sein kann [47]; [48].

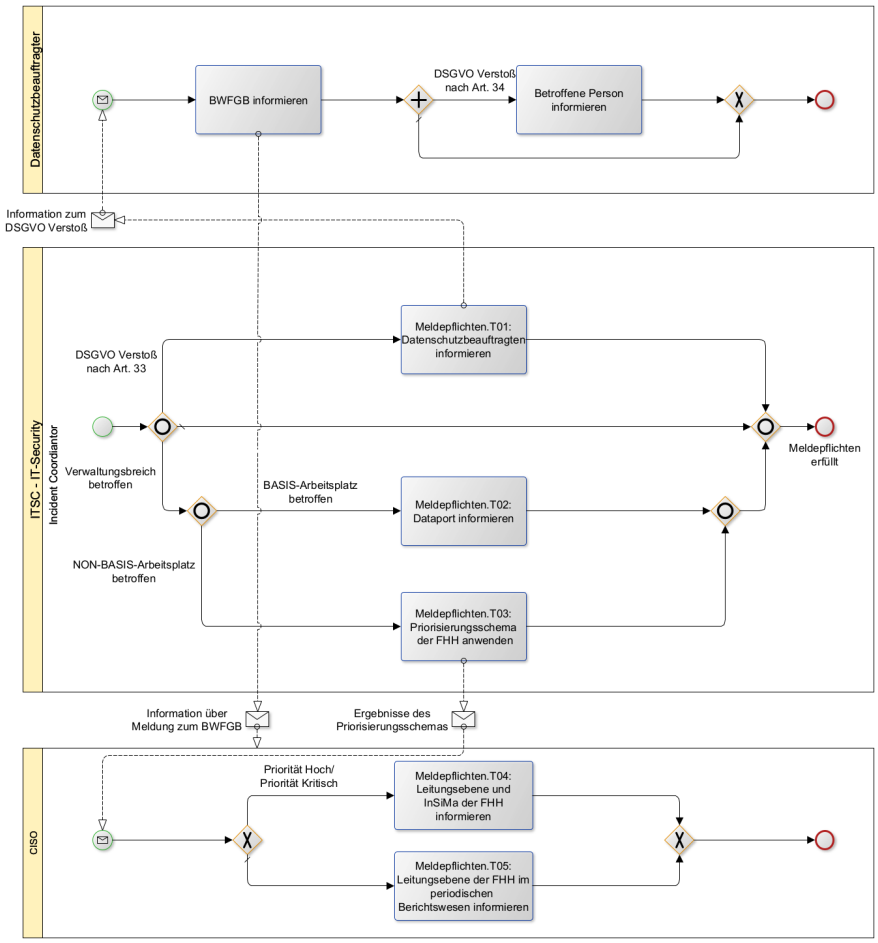

Abbildung 5.6: Prozessdiagramm für den Unterprozess *Meldepflichten* aus der Phase *Assess and Decide*, auf Basis von [48]

5.3.3 Respond

In der Phase *Respond*, siehe Abbildung 5.7, wird der Fokus auf die Eindämmung des Incidents, die Schließung des Angriffsvektors, die Beseitigung der Spuren des Angreifers

sowie die Wiederherstellung des Normalbetriebs gelegt. Die einzelnen Schritte in dieser Phase sind in hohem Maße von den Resultaten der vorangegangenen Analyse abhängig und bedürfen gegebenenfalls weiteren Untersuchungen. Die spezifischen Maßnahmen variieren in Abhängigkeit von der Art und dem Umfang des Incidents [47]; [48].

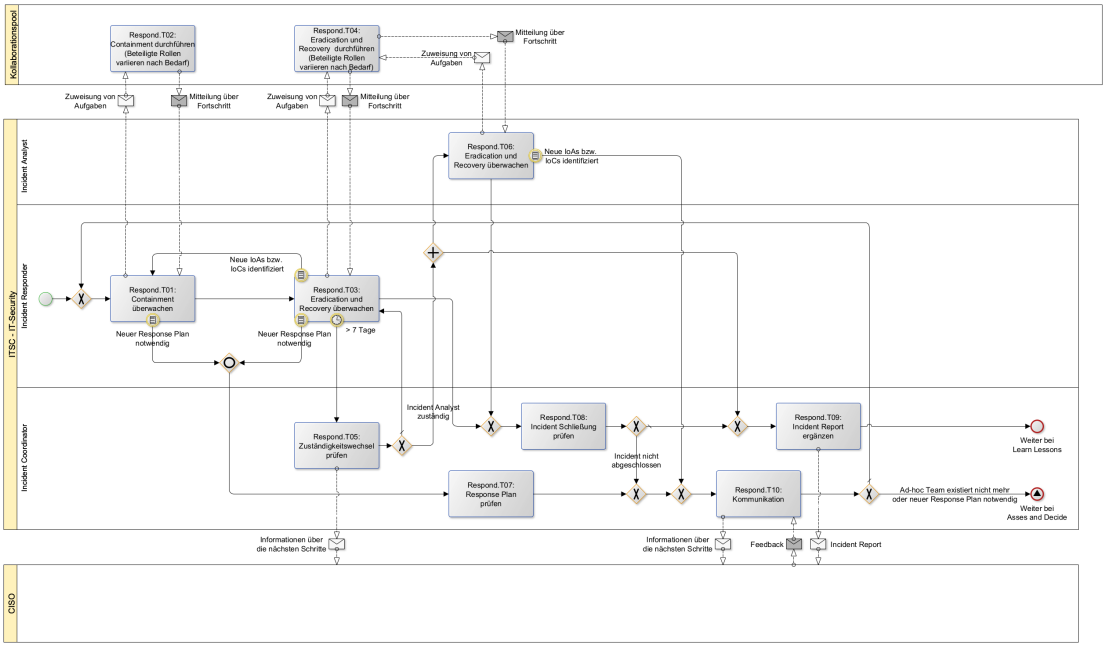

Abbildung 5.7: Prozessdiagramm für die Phase *Respond*, auf Basis von [48]

Das Prozessdiagramm bietet die Möglichkeit in die vorherige Phase *Assess and Decide* zu wechseln, sofern der Incident Response Plan als unzureichend erachtet wird. Ebenso kann ein Wechsel in die Phase *Learn Lessons* erfolgen, auch wenn das Incident Response noch nicht abgeschlossen ist. Dies ist der Fall, wenn der Incident unter Kontrolle gebracht wurde, jedoch noch nicht alle Spuren beseitigt wurden und der Regelbetrieb noch nicht vollständig wiederhergestellt wurde [47]; [48].

5.3.4 Learn Lessons

In der Phase *Learn Lessons*, siehe Abbildung 5.8, erfolgt eine Aufarbeitung des Incident Handlings. Die Phase sowie die einzelnen Aktivitäten sind komplett optional gestaltet. Es gibt Situationen, in denen auf die Durchführung des *Learn Lessons* verzichtet werden kann. Dies ist insbesondere der Fall, wenn die Ursachen des Incidents offensichtlich sind,

es sich um einen Einzelfall handelt und das Incident Handling zeitnah und effektiv erfolgt ist. Ansonsten umfasst diese Phase verschiedene Aktivitäten, wie beispielsweise die Durchführung einer Root-Cause-Analysis, die Evaluierung des Incident Handling Prozesses oder die Evaluierung des Ad-hoc-Teams. Das Ziel der Aktivitäten besteht darin, potenzielle Verbesserungsmaßnahmen zu identifizieren, um bei einer erneuten Durchführung des Incident Handlings besser vorbereitet zu sein. Die Leitung der Aktivitäten obliegt dem Incident Coordinator. Die Teilnahme an den Aktivitäten ist mit einer Vielzahl von Rollen verbunden, deren Beteiligung sich nach dem jeweiligen Bedarf richtet [47]; [48].

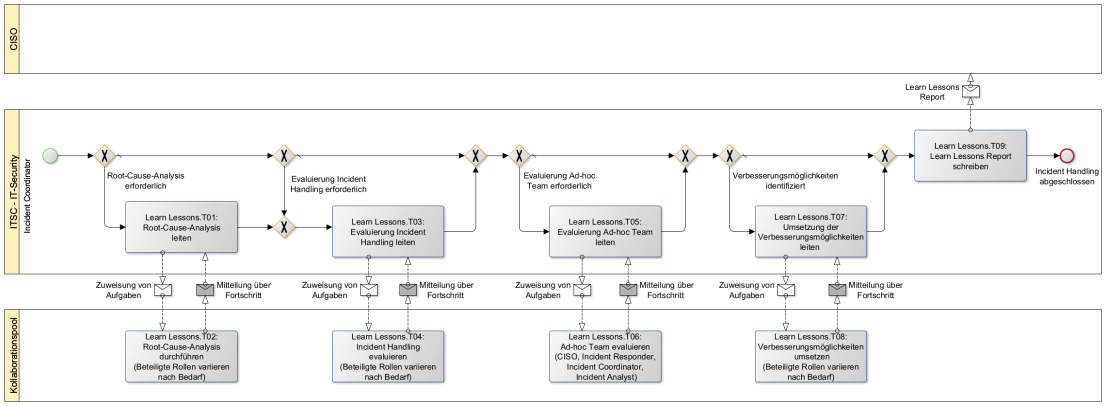

Abbildung 5.8: Prozessdiagramm für die Phase *Learn Lessons*, auf Basis von [48]

5.4 RASCI-Matrix

Für die Zuordnung der Aktivitäten zu den Rollen wird eine RASCI-Matrix verwendet. Dadurch sollen Kompetenzkonflikte vermieden werden, indem die Verantwortlichkeiten klar aufgeteilt werden. Bei der Anwendung der RASCI-Matrix werden die Aktivitäten in den Zeilen und die Rollen in den Spalten aufgeführt [49]. Mit den folgenden fünf Kategorien werden die Aktivitäten und die Rollen miteinander in Verbindung gesetzt, in Anlehnung an [49]:

- **Responsible**: Die Rolle ist für die Umsetzung der Aktivität zuständig
- **Accountable**: Die Rolle ist rechenschaftspflichtig bezüglich der Aktivität
- **Support**: Die Rolle leistet Unterstützung bei der Umsetzung der Aktivität

- **Consulted**: Die Rolle kann im Rahmen der Aktivität konsultiert werden
- **Informed**: Die Rolle muss über den Stand oder das Ergebnis der Aktivität informiert werden

Für die vier Phasen des Incident Handlings, sowie die zwei Unterprozesse wird jeweils eine RASCI-Matrix erstellt. Die RASCI-Matrizen stellen eine Erweiterung der BPMN-Diagramme dar. Während bei den BPMN-Diagrammen der Prozessablauf des Incident Handlings im Vordergrund stand und häufig nur ersichtlich war, welche Rolle verantwortlich (Responsible) für eine Aktivität war, gliedern die RASCI-Matrizen dies feiner mit den oben aufgeführten Kategorien auf.

In Abbildung 5.9 ist die RASCI-Matrix für die Phase *Detect and Report* dargestellt. In dieser Phase erfolgt eine Erfassung der Ereignisse sowie eine Evaluierung, ob ein Potenzial Incident vorliegt. Da davon auszugehen ist, dass es sich bei der Evaluierung um einen häufig vorkommenden Prozess handelt, sind nur wenige Rollen involviert. Der Einbezug mehrerer Rollen würde einen großen Overhead erzeugen.

	Nutzer	Systembetreiber	Monitoring Expert	Incident Analyst	Incident Responder	Incident Coordinator	CISO	Management	Externe Akteure
Detect and Report.T01: Event Report ausfüllen	R/A	-	S	-	-	-	-	-	-
Detect and Report.T02: Event Report ausfüllen	-	R/A	S	-	-	-	-	-	-
Detect and Report.T03: Event Report ausfüllen	-	-	R	-	-	-	A	-	-
Detect and Report.T04: Event überprüfen	C	C	R	-	-	-	A	-	-
Detect and Report.T05: Entscheidung dokumentieren	-	-	R/A	-	-	I	-	-	-
Detect and Report.T06: Incident Coordinator benachrichtigen	-	-	R/A	-	-	-	-	-	-

Abbildung 5.9: RASCI-Matrix für die Phase *Detect and Report*, eigene Darstellung

Der Monitoring Expert bildet in dieser Phase die wichtigste Rolle. Er unterstützt die Nutzer und Systembetreiber bei der Meldung von Events und übernimmt zudem die Überprüfung der Events sowie die Verantwortung für die daraus resultierenden Maßnahmen.

Die Abbildung 5.10 zeigt die RASCI-Matrix für die Phase *Assess and Decide*. In der Phase wird der Potential Incident bewertet, das Management und externe Akteure benachrichtigt und über das weitere Vorgehen entschieden. Erstmals in dem Incident Handling Prozess wird der CISO und das Management über einzelne Aktivitäten informiert.

Dabei gilt zu beachten, dass z. B. bei der Aktivität *Assess and Decide.T04: Management benachrichtigen* kein *Informed* bei der Rolle Management gesetzt wird. Dies ist dadurch begründet, dass das Management innerhalb der Aktivität selbst informiert wird und keine Benachrichtigung über den Stand der Aktivität erhält. Andernfalls würde das Management zweimal innerhalb einer Aktivität benachrichtigt werden.

	Nutzer	Systembetreiber	Monitoring Expert	Incident Analyst	Incident Responder	Incident Coordinator	CISO	Management	Externe Akteure
Assess and Decide.T01: Triage	C	C	-	S	-	R/A	I	-	-
Assess and Decide.T02: Ad-hoc Team zusammenstellen	-	-	-	-	-	R/A	I	-	-
Assess and Decide.T03: Meldepflichten erfüllen	-	-	-	S	-	R	R/A	I	-
Assess and Decide.T04: Management benachrichtigen	-	-	-	-	-	R	S/A	-	-
Assess and Decide.T05: Externe Akteure benachrichtigen	-	-	-	-	-	R	S/A	I	-
Assess and Decide.T06: Intra-Incident Analysis durchführen	C	C	-	S	R	A	-	-	-
Assess and Decide.T07: Inter-Incident Analysis durchführen	-	-	-	S	R	A	-	-	-
Assess and Decide.T08: Überprüfen des Schweregrads	-	-	-	C	C	R/A	-	-	-
Assess and Decide.T09: Incident Report ergänzen	-	-	-	-	-	R/A	I	-	-
Assess and Decide.T10: Response festlegen	-	C	-	S	S	R	C/A	-	-
Assess and Decide.T11: Externe Ressourcen anfragen	-	-	-	I	I	R/A	I	I	-
Assess and Decide.T12: CISO und Krisenmanagement benachrichtigen	C	C	-	C	C	R/A	-	-	-

Abbildung 5.10: RASCI-Matrix für die Phase *Assess and Decide*, eigene Darstellung

Die Rollen Nutzer und Systembetreiber werden in dieser Phase nur noch konsultiert, sofern zusätzliche Informationen über den Potential Incident bzw. Incident benötigt werden. Der Incident Coordinator hingegen nimmt eine wichtige Rolle in dieser Phase ein, er ist für die Umsetzung der meisten Aktivitäten in dieser Phase verantwortlich und führt sie auch selber durch.

Die RASCI-Matrix für den Unterprozess *Triage* ist in Abbildung 5.11 dargestellt. Bei der Triage ist der Incident Coordinator für die Durchführung aller Aktivitäten zuständig und verantwortlich.

In Abbildung 5.12 ist die RASCI-Matrix für den Unterprozess *Meldepflichten* dargestellt. In der Phase erfolgt die Durchführung der Aktivitäten durch den Incident Coordinator in Zusammenarbeit mit dem CISO. Die Kommunikation mit der FHH wird durch den

	Nutzer	Systembetreiber	Monitoring Expert	Incident Analyst	Incident Responder	Incident Coordinator	CISO	Management	Externe Akteure
Triage.T01: Determination	C	C	-	-	-	R/A	-	-	-
Triage.T02: Incident Analyst anfragen	-	-	-	-	-	R/A	-	-	-
Triage.T03: Determination (Incident Coordinator, Incident Analyst)	C	C	-	S	-	R/A	-	-	-
Triage.T04: Correlation	-	-	-	-	-	R/A	-	-	-
Triage.T05: Prioritization	-	-	-	-	-	R/A	I	-	-

Abbildung 5.11: RASCI-Matrix für den Unterprozess *Triage*, eigene Darstellung

CISO der HAW Hamburg wahrgenommen, da dies in dem RaSiKo der FHH entsprechend festgelegt ist. Das Management wird stets informiert, sofern Personen oder Institutionen außerhalb des ITSC benachrichtigt werden.

	Nutzer	Systembetreiber	Monitoring Expert	Incident Analyst	Incident Responder	Incident Coordinator	CISO	Management	Externe Akteure
Meldepflichten.T01: Datenschutzbeauftragten informieren	-	-	-	-	-	R	I/A	I	-
Meldepflichten.T02: Dataport informieren	-	-	-	-	-	R	I/A	I	-
Meldepflichten.T03: Priorisierungsschema der FHH anwenden	-	-	-	S	-	R	C/A	-	-
Meldepflichten.T04: Leitungsebene und InSiMa der FHH informieren	-	-	-	-	-	I	R	A	-
Meldepflichten.T05: Leitungsebene der FHH im periodischen Berichtswesen informieren	-	-	-	-	-	I	R	A	-

Abbildung 5.12: RASCI-Matrix für den Unterprozess *Meldepflichten*, eigene Darstellung

Die Abbildung 5.13 zeigt die RASCI-Matrix für die Phase *Respond*. In der Respond Phase sind die Systembetreiber verantwortlich für die Durchführung des Incident Response. Dabei können sie Unterstützung durch den Incident Analyst, den Incident Responder sowie durch externe Akteure, sofern erforderlich, erhalten. Der CISO wird über sämtliche Aktivitäten in Kenntnis gesetzt, um sich einen Überblick über den Stand des Incidents zu verschaffen und seine Funktion als Ansprechpartner in der Kommunikation mit der FHH zu erfüllen.

	Nutzer	Systembetreiber	Monitoring Expert	Incident Analyst	Incident Responder	Incident Coordinator	CISO	Management	Externe Akteure
Respond.T01: Containment überwachen	-	-	-	-	R	A	I	-	I
Respond.T02: Containment durchführen (Beteiligte Rollen variieren nach Bedarf)	C	R	-	R	S	A	I	-	S
Respond.T03: Eradication und Recovery überwachen	-	-	-	-	R	A	I	-	I
Respond.T04: Eradication und Recovery durchführen (Beteiligte Rollen variieren nach Bedarf)	C	R	-	R	S	A	I	-	S
Respond.T05: Zuständigkeitswechsel prüfen	-	-	-	-	-	R/A	I	-	
Respond.T06: Eradication und Recovery überwachen	-	-	-	R	-	A	I	-	I
Respond.T07: Response Plan prüfen	-	-	-	S	S	R/A	C	-	-
Respond.T08: Incident Schließung prüfen	-	C	-	C	C	R/A	C	-	C
Respond.T09: Incident Report ergänzen	-	C	-	C	C	R/A	C	I	C
Respond.T10: Kommunikation	-	-	-	-	-	R/A	-	-	-

Abbildung 5.13: RASCI-Matrix für die Phase *Respond*, eigene Darstellung

Der Incident Coordinator trägt in dieser Phase die Verantwortung für alle Aktivitäten. Bei der Überprüfung zur Schließung des Incidents kann er alle am Incident Response beteiligten Rollen konsultieren, um eine umfassende Einschätzung der Lage zu gewinnen.

Die RASCI-Matrix für die Phase *Learn Lessons* ist in Abbildung 5.14 dargestellt. Diese Phase ist durch eine kollaborative Arbeitsweise gekennzeichnet. Es ist jedoch zu beachten, dass nicht in jedem Fall alle aufgeführten Rollen an den einzelnen Aktivitäten beteiligt sein müssen. Die Darstellung dient lediglich der Einordnung der jeweiligen Rolle in eine der genannten Kategorien.

5.5 Abweichungen von der ISO/IEC 27035

Im Rahmen der Konzeption des Incident Handlings wurde ersichtlich, dass einzelne Vorschläge der ISO/IEC 27035 für den Einsatz an der HAW Hamburg nicht geeignet sind. Dies beginnt mit der Festlegung der notwendigen Rollen für das Incident Handling. Während die ISO/IEC 27035 neun direkt am Incident Management sowie zwei zusätzliche Rollen für das Incident Response beteiligte Rollen aufzählt, werden für den in dieser Arbeit entwickelten Prozess lediglich die internen Rollen Monitoring Expert, Incident Analyst,

	Nutzer	Systembetreiber	Monitoring Expert	Incident Analyst	Incident Responder	Incident Coordinator	CISO	Management	Externe Akteure
Learn Lessons.T01: Root-Cause-Analysis leiten	-	-	-	-	-	R/A	S	-	-
Learn Lessons.T02: Root-Cause-Analysis durchführen (Beteiligte Rollen variieren nach Bedarf)	C	S	S	S	S	R/A	S	S	S
Learn Lessons.T03: Evaluierung Incident Handling Plan leiten						R/A	S	-	-
Learn Lessons.T04: Incident Handling Plan evaluieren (Beteiligte Rollen variieren nach Bedarf)	C	C	C	S	S	R/A	S	C	C
Learn Lessons.T05: Evaluierung Ad-hoc Team leiten	-	-	-	-	-	R/A	S	-	-
Learn Lessons.T06: Ad-hoc Team evaluieren (CISO, Incident Responder, Incident Coordinator, Incident Analyst)	-	C	-	S	S	R/A	S	-	C
Learn Lessons.T07: Umsetzung der Verbesserungsmöglichkeiten leiten	-	-	-	-	-	R/A	S	-	-
Learn Lessons.T08: Verbesserungsmöglichkeiten umsetzen (Beteiligte Rollen variieren nach Bedarf)	R	R	R	R	-	R/A	I	I	I
Learn Lessons.T09: Learn Lessons Report schreiben	-	-	-	-	-	R/A	I	I	-

Abbildung 5.14: RASCI-Matrix für die Phase *Learn Lessons*, eigene Darstellung

Incident Responder sowie Incident Coordinator benötigt. Die Reduktion der Rollenanzahl lässt sich zum einen darauf zurückführen, dass das Incident Management in eine bereits bestehende Abteilung der HAW Hamburg integriert werden soll. Zum anderen werden die Rollen, so wie sie in der ISO/IEC 27035 aufgeführt sind, in der Mehrzahl der Fälle als zu feingranular betrachtet, sodass eine Zusammenfassung der Rollen erfolgte. Die Rolle des CISOs, der gemäß der Informationssicherheitsleitlinie der HAW Hamburg eine wesentliche Funktion im Incident Handling innehat, wird im Standard hingegen nicht berücksichtigt. In der ISO/IEC 27035 werden darüber hinaus weitere Rollen wie Nutzer oder Systembetreiber thematisiert, allerdings ohne sie in einer dedizierten Liste vollständig aufzuzählen.

Bei Betrachtung auf Prozessebene zeigen sich weitere Unterschiede. Ein wesentlicher Unterschied besteht darin, dass der in dieser Arbeit entwickelte Prozess mehrere Phasen und Aktivitäten iterativ durchlaufen kann. In der ISO/IEC 27035 ist eine solche Anpassungsfähigkeit nicht vorgesehen.

Eine entsprechende Iteration lässt sich im Wechsel zwischen den Phasen *Respond* und *Assess and Decide* finden. Der Wechsel dient unter anderem der Erstellung neuer Response Pläne. Ein neuer Response Plans kann beispielsweise erforderlich sein, wenn sich die Anzahl der von Malware betroffenen Hosts deutlich erhöht hat und daher eine erneute Analyse durchgeführt werden muss, um auf dieser Grundlage einen verbesserten Response Plan zu entwickeln. Eine Neubewertung des Incidents ist in diesem Zuge ebenfalls möglich. Ein weiterer Anlass für einen Wechsel kann darin bestehen, dass bei neu identifizierten IoAs[1] bzw. IoCs ein neues Ad-hoc-Team aufgestellt werden muss, weil das alte Team bereits aufgelöst wurde. Ein solcher Wechsel zwischen diesen beiden Phasen findet sich auch in der SP 800-61 R2 von NIST [16].

Des Weiteren besteht für den Incident Coordinator die Möglichkeit, nach Abschluss der Arbeit der Incident Responder zu beschließen, dass die Incident Response nicht erfolgreich war und eine Wiederholung der Incident Response anzuordnen. In der ISO/IEC 27035 ist ebenfalls festgelegt, dass der Incident Coordinator über die Schließung des Incidents entscheidet, jedoch werden keine Konsequenzen für den Fall einer nicht erfolgreichen Durchführung genannt.

Im Rahmen der Triage besteht ein weiterer Unterschied der beiden Prozesse in der Bedeutung des Ergebnisses aus der *Correlation* von Incidents. In der ISO/IEC 27035 dient diese Aktivität lediglich zur Evaluierung des Umfangs und der Schwere des aktuellen Incidents. Im Prozess für die HAW Hamburg werden hingegen, basierend auf dem Ergebnis der Aktivität, korrelierende Incidents zusammengefasst. Dies bietet den Vorteil einer effizienten Nutzung von Ressourcen, da eine wiederholte Ausführung von Aktivitäten vermieden wird.

Ein weiterer Unterschied besteht im Aufbau des Incident Response. Die in der ISO/IEC 27035 als eigenständig betrachteten Aktivitäten *Eradication* und *Recovery* werden im Prozess für die HAW Hamburg zusammengefasst. Die Zusammenfassung erfolgt in Anlehnung an die Empfehlungen des NIST in SP 800-61 R2, da eine eindeutige Abgrenzung der Aktivitäten *Eradication* und *Recovery* schwierig ist und eine parallele Durchführung häufig in der Praxis zu beobachten ist [16]. Des Weiteren besteht innerhalb der Incident Response die Möglichkeit, von der Aktivität *Eradication & Recovery* zur Aktivität

[1] In der populärwissenschaftlichen Literatur findet sich neben dem geläufigen Begriff Indicators of Compromise auch der Begriff Indicators of Attack [62]. Vereinzelt wird er auch in der wissenschaftlichen Literatur verwendet [4]. Der Begriff bezeichnet Indikatoren, die auf einen laufenden oder bestehenden Angriff hindeuten [62]. Im Rahmen dieser Arbeit wird auf eine Differenzierung der Begriffe IoA und IoC verzichtet. Stattdessen werden beide Varianten gemeinsam genannt [48].

Containment zu wechseln, sofern neue Indicators of Attacks (IoAs) bzw. Indicators of Compromise (IoCs) identifiziert wurden. Ein solches Szenario kann durch eine mangelhafte Durchführung der Aktivität *Containment* oder eine unvollständige Analyse des Incidents eintreten. Die ISO/IEC 27035 sieht hingegen keine wiederholte Durchführung der einzelnen Aktivitäten während des Incident Response vor [42].

Ein weiteres Unterscheidungsmerkmal ist die Auslegung der Phase *Learn Lessons*, welche in der ISO/IEC 27035 obligatorisch ist. Im Prozess für die HAW Hamburg hingegen ist sie vollständig optional gestaltet. Die Aktivitäten im Rahmen von *Learn Lessons* sind zeitintensiv und involvieren eine Vielzahl von Rollen. Dennoch kann es Situationen geben, in denen es nicht ratsam ist, jede Aktivität dieser Phase durchzuführen. Insbesondere bei Incidents, die ohne größere Anstrengungen bewältigt werden konnten, ist eine detaillierte Analyse nicht erforderlich. Die Option, auf bestimmte Aktivitäten zu verzichten, verleiht dem Incident Coordinator eine höhere Flexibilität sowie eine schnellere Freigabe personeller Ressourcen.

Die Gegenüberstellung der Prozesse zeigt, dass die ISO/IEC 27035 ein sequenziell ablaufendes Incident Handling vorsieht, das in einzelnen, aufeinander folgenden Phasen bzw. Aktivitäten durchgeführt wird. Demgegenüber ermöglicht der Prozess für die HAW Hamburg eine iterative Vorgehensweise, bei der mehrere Durchläufe der Phasen bzw. Aktivitäten möglich sind. In Abbildung 5.15 ist das Incident Handling nach der ISO/IEC 27035 grob dargestellt, die Abbildung 5.16 hingegen zeigt den in dieser Arbeit entworfenen Incident Handling Prozess für die HAW Hamburg. Bei beiden Abbildungen handelt es sich um eine Abstraktion des tatsächlichen Incident Handlings.

Der Vorteil eines iterativen Incident Handlings besteht darin, dass auf neue Informationen, wie beispielsweise das Eskalieren eines Incidents, reagiert und eine Neueinstufung des Incidents vorgenommen werden kann. Dies gewährleistet auch eine höhere Realitätsnähe. Des Weiteren ist die ISO/IEC 27035 in einer Weise verfasst, die es ermöglicht, die Inhalte an die spezifischen Bedürfnisse verschiedener Organisationen anzupassen. Daher werden lediglich Empfehlungen ausgesprochen, jedoch keine festen Vorgaben definiert. Infolgedessen ist der Prozess für die HAW Hamburg wesentlich konkreter, in dem beispielsweise festgelegt wird, dass nach einem Zeitraum von mehr als sieben Tagen, den das Ad-hoc-Team für die Aktivität *Eradication & Recovery* benötigt, die Verantwortung an die Incident Analysten abgegeben wird.

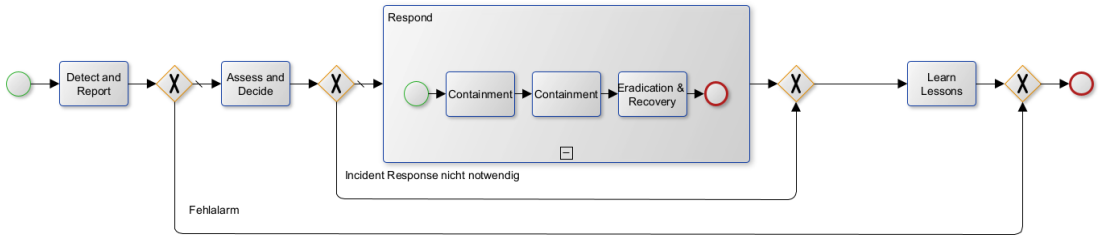

Abbildung 5.15: Grobe Darstellung des Incident Handlings nach der ISO/IEC 27035, eigene Darstellung

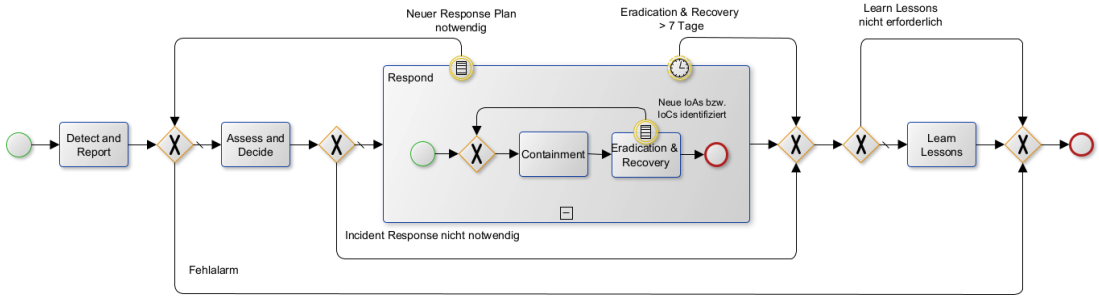

Abbildung 5.16: Grobe Darstellung des Incident Handling für die HAW Hamburg, eigene Darstellung

6 Evaluation des Incident Handlings

Die Evaluierung des Incident Handling Prozesses erfolgt anhand der simulierten Durchführung zweier typischer Szenarien. Diese Vorgehensweise dient der Identifikation von Verbesserungspotenzialen innerhalb des Prozesses. Ein solches Verfahren ist unter der Bezeichnung Tabletop Exercise bzw. TTX bekannt [20]. Um eine möglichst umfassende Evaluierung des Incident Handling Prozesses zu gewährleisten, werden zwei Szenarien ausgewählt, welche sich hinsichtlich des Angriffsmusters sowie der betroffenen Systeme voneinander unterscheiden. Somit kann eine detaillierte Überprüfung der verschiedenen Aktivitäten des Prozesses vorgenommen werden, was eine präzisere Identifizierung von Verbesserungspotenzialen ermöglicht.

Die Simulation der Szenarien erfolgt auf Basis der BPMN Diagramme, wobei die jeweiligen Aktivitäten referenziert werden. Das erste Szenario stellt eine Phishing Attacke dar, während das zweite Szenario DNS-Tunneling umfasst. Die dargestellten Szenarien sowie das vorgeschlagene Vorgehen basieren auf fiktiven, aber realitätsnahen, Annahmen.

6.1 Szenaro 1: Phishing Attacke

6.1.1 Beschreibung

Es wurden mehrere E-Mails an Mitarbeiter der HAW Hamburg versandt, in welchen diese dazu aufgefordert werden, ihren Cache im E-Mail-Postfach zu leeren. In der E-Mail ist ein Link angegeben, der auf eine gefälschte Webseite weiterleitet, auf der Unterstützung bei der Löschung des Caches angeboten wird. Auf dieser wird der Mitarbeiter aufgefordert, sich mit seinem Passwort für die Organisation zu authentifizieren. Der Angriff ist in seiner Konzeption an eine Phishing-Attacke angelehnt, die zuvor die Universität Hamburg betraf, siehe Abbildung 6.1

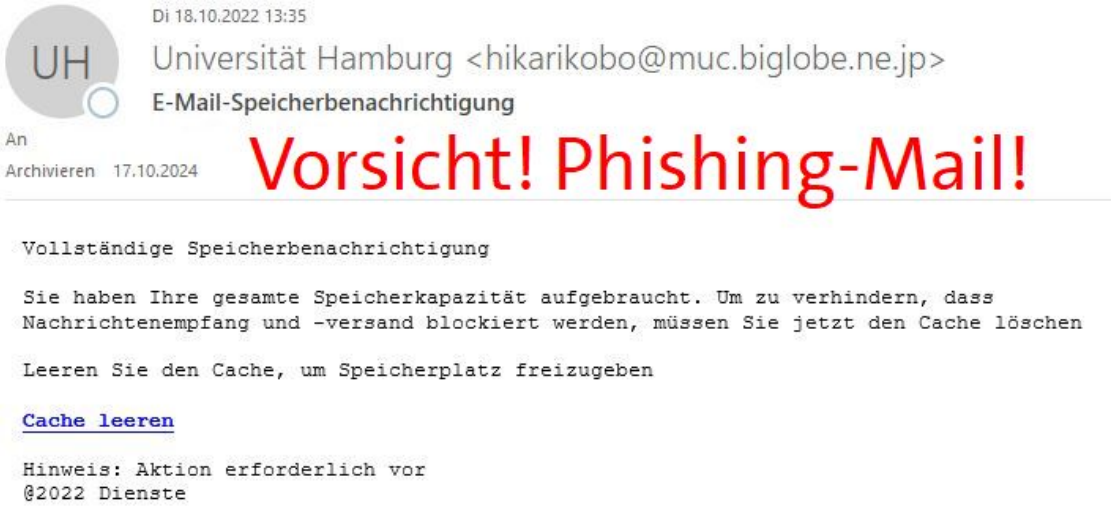

Abbildung 6.1: Phishing E-Mail an die Universität Hamburg, entnommen aus [61]

6.1.2 Detect and Report

Einige der Mitarbeiter, die die E-Mail erhalten haben, erachten diese als verdächtig. Der Absender zeigt die HAW Hamburg an, jedoch ist die E-Mail-Domain *muc.biglobe.ne.jp* verdächtig. Zudem weist die Nachricht an einigen Stellen eine ungewöhnliche Formulierung auf, wie beispielsweise *Vollständige Speicherbenachrichtigung*. Infolgedessen erstellen die Mitarbeiter ein Event Report *(Detect and Report.T01)* und übermitteln es dem Monitoring Experten über die zentrale Meldeadresse.

Der Monitoring Expert analysiert die Event Reports *(Detect and Report.T04)* und stellt fest, dass eine Vielzahl von Mitarbeitern betroffen ist, was auf einen umfangreichen Phishing-Angriff hindeutet. Der Monitoring Expert erklärt das Vorliegen eines Potential Incidents und informiert den Incident Coordinator *(Detect and Report.T06)*. Zudem können sich die Mitarbeiter im Einzelnen nicht daran erinnern, ob sie den Link in der E-Mail angeklickt und ihre Zugangsdaten eingegeben haben.

Verbesserungspotenzial: Obwohl der Monitoring Expert erkennt, dass ein Phishing Angriff stattfindet bzw. statt gefunden hat, wird diese Erkenntnis nicht genutzt, um Mitarbeiter darüber zu informieren und alle möglichen Betroffenen zu warnen. Es ist besonders wichtig frühzeitig, die Mitarbeiter zu informieren, da nicht jeder Mitarbeiter diese E-Mail als eine Phishing-Mail erkennt. Der Incident Handling Prozess sollte daher

um eine Aktivität ergänzt werden, die abbildet, dass der Monitoring Expert die Mitarbeiter schnell informieren und/oder erste Maßnahmen ergreifen kann. Auf diese Weise kann der Monitoring Expert auch reagieren, wenn registriert wird, dass verdächtig große Datenmengen über das Netzwerk an einen externen Host exportiert werden, in dem er die Netzwerkverbindung trennt.

Dabei ist jedoch zu beachten, dass der Monitoring Expert mit Bedacht vorgehen muss. Er sollte nur Maßnahmen ergreifen, wenn der akute und dringende Bedarf besteht Ad-hoc-Maßnahmen zu ergreifen. Ansonsten besteht die Gefahr, dass die Mitarbeiter falsch oder lückenhaft bzw. unvollständig informiert werden, weil eine tiefergehende Analyse noch nicht abgeschlossen wurde. Außerdem wird wichtiges Beweismaterial oder Daten zerstört, wenn z. B. Server frühzeitig heruntergefahren werden, um das Netzwerk zu schützen. Daher sollte der Handlungsrahmen des Monitoring Expert klar definiert sein.

6.1.3 Assess and Decide

Triage

Im Rahmen der Triage erfolgt eine Evaluierung der Schwere der Phishing Attacke durch den Incident Coordinator, wobei ergänzende Analysen durchgeführt werden, siehe *Triage.T01*. Die Analyse, welche durch den Incident Analyst unterstützt wird, siehe *Triage.T03*, ergibt, dass keine Kompromittierung der Netzwerke oder Systeme stattgefunden hat. Bei der Correlation *Triage.T02* werden alle Events bzw. Potential Incidents, die einen ähnlichen Ablauf besitzen, erfasst und einem Incident zugeordnet.

Es handelt sich hierbei um einen Vorfall, der als *fraud* klassifiziert wird. Da nicht auszuschließen ist, dass die Angreifer an die Passwörter der Mitarbeiter gelangt sind, ist die Vertraulichkeit verletzt. Die betroffenen Mitarbeiter sind Angestellte im Verwaltungsbereich, wodurch ihnen der Zugriff auf sensible Informationen möglich ist. Infolgedessen wurde die Auswirkung auf den Schutzbedarf mit *mittel*[1] bewertet. Der Wiederherstellungsaufwand wurde mit Stufe 0 bewertet, da derzeit kein oder sehr geringer Handlungsbedarf bei Systemen oder Netzwerken besteht. Es ist jedoch erforderlich, die betroffenen Mitarbeiter dazu aufzufordern, ihre Passwörter bis zu einem festgelegten Zeitpunkt zu ändern. Der Schweregrad wird gemäß der in Kapitel 4 vorgestellten Methode bestimmt. Die

[1] Es wird davon ausgegangen, dass der Schutzbedarf vorab festgelegt wurde bzw. eine Schutzbedarfsanalyse erfolgt ist.

Werte aus den einzelnen Kategorien sind in Tabelle 6.1 dargestellt. Bei der Berechnung des Schweregrads ergibt sich ein Punktwert von 34, was einen *Minor Incident* darstellt.

Kategorie	x	$\tilde{x}$	w
Ausmaß der Vorfallsart	1	$0,3\overline{3}$	1
Schutzbedarf	2	0,5	2
Wiederherstellungsaufwand	0	0	1

Tabelle 6.1: Bewertung des Schweregrads der Phishing Attacke

Verbesserungspotenzial: Bei der Durchführung der Triage bietet sich eine andere Reihenfolge der Aktivitäten an. Zunächst ist durch den Incident Coordinator zu überprüfen, ob der Incident korreliert. Im Falle einer Korrelation ist eine Einstufung des Potential Incidents nicht erforderlich, da bereits ein Incident vorliegt, dadurch kann er frühzeitig das Ad-hoc-Team informieren. Im Rahmen einer umfassenden Analyse des Ad-hoc-Teams kann Incident Coordinator über eine Neubewertung des bereits bestehenden Incidents entscheiden. Das beschriebene Vorgehen empfiehlt sich besonders bei Events bzw. Potential Incidents, die relativ eindeutig einem Incident zuzuordnen sind. In allen anderen Fällen ist eine Analyse durch den Incident Coordinator erforderlich, um eine Zuordnung zu ermöglichen bzw. auszuschließen.

Die Aktivität *Triage.T01: Determiniation* wird dann genutzt, um den Schweregrad des Incidents zu bestimmen. Die Zuordnung zu den einzelnen Kategorien führt zu einer Priorisierung, sodass die letzte Aktivität, *Triage.T05: Prioritization*, wie in den BPMN-Diagrammen dargestellt, nicht mehr erforderlich ist. Dies führt zu einer Reduktion der Anzahl notwendiger Aktivitäten während der Triage. Zudem werden keine Arbeitsschritte wiederholt und das Ad-hoc-Team bzw. die Incident Analysten werden zeitnah benachrichtigt, sobald ein Potential Incident mit einem Incident korreliert.

In dem aktuellen Prozess wird nicht ersichtlich, welche Maßnahmen zu ergreifen sind, wenn ein Potential Incident mit einem *Minor Incident* korreliert. Es besteht die Möglichkeit, dass der *Minor Incident* eskaliert, dies ist jedoch durch den Prozess nicht abgebildet.

Meldepflichten

Die von dem Phishing Angriff betroffenen Mitarbeiter sind im Verwaltungsbereich tätig. Dabei sind sowohl Basis- als auch Non-Basis-Arbeitsplätze betroffen. Da in jedem Fall eine Meldung an Dataport zu erfolgen hat, meldet der Incident Coordinator den Phishing Angriff, siehe *Meldepflichten.T02.*

Bei der Prüfung in welcher Form die FHH benachrichtigt werden soll, wird das Priorisierungsschema der FHH angewandt, siehe *Meldepflichten.T03.* Die Dringlichkeit sowie die Auswirkung sind als *niedrig* zu bewerten, weshalb der CISO den Incident im periodischen Berichtswesen der FHH mit aufnehmen wird.

Verbesserungspotenzial: *Keine*

Assess and Decide nach den Meldepflichten

Der Incident Coordinator informiert das Management *Assess and Decide.T04* über den Phishing Angriff und die bereits getroffenen Maßnahmen. Es besteht kein weiterer Handlungsbedarf.

Des Weiteren werden das DFN-CERT sowie das BSI über den Phishing Angriff in Kenntnis gesetzt *Assess and Decide.T05).* Auch hier handelt es sich um eine reine Informationsweitergabe.

Verbesserungspotenzial: *Keine*

Assess and Decide nach der Triage und den Meldepflichten

Da ein *Minor Incident* festgestellt wurde, ist der Incident Analyst für die Behebung des Incidents zuständig. Die Gründung eines Ad-hoc-Teams ist nicht erforderlich. Der Incident Analyst identifiziert zunächst alle Mitarbeiter, welche die E-Mail erhalten haben, und informiert sie. Zudem werden die E-Mail-Filter angepasst, sodass E-Mails mit der entsprechenden Domain gefiltert werden.

Verbesserungspotenzial: Im Rahmen des Incident Handling von *Minor Incidents* sollte ebenfalls die Möglichkeit bestehen, die Phase *Learn Lessons* optional durchzuführen. Die Evaluierung der Anzahl der Mitarbeiter, die auf die Phishing E-Mail hereingefallen

sind, sowie die Entscheidung über die Durchführung weiterer Maßnahmen, wie beispielsweise Awareness Trainings, kann in dieser Phase erfolgen. Auch wenn es sich lediglich um einen *Minor Incident* handelt, hat die HAW Hamburg einen hohes Interesse, solche Vorfälle zu vermeiden, um potenziellen Angreifern kein Einfallstor für umfassendere Angriffe zu bieten. Des Weiteren besteht die Möglichkeit, dass Tätigkeiten identifiziert werden, die sich für eine Automatisierung eignen. Durch die korrelierte Betrachtung von *Minor Incidents*, lassen sich repetitive Tätigkeiten schneller identifizieren.

6.2 Szenaro 2: Datenexfiltration

6.2.1 Beschreibung

Das SIEM meldet, dass ein Windows-PC eine hohe Anzahl an *Domain Name System* (DNS) Anfragen erzeugt, die vom lokalen DNS Server nicht beantwortet werden können. Der Alarm weist darauf hin, dass auf dem Windows-PC DNS Tunneling betrieben wird. Beim DNS Tunneling werden in die DNS Abfrage zusätzliche Informationen oder Befehle eingebettet und an einen zu einem Angreifer gehörenden DNS Server versendet. In Abbildung 6.2 wird der Ablauf von DNS Tunneling dargestellt.

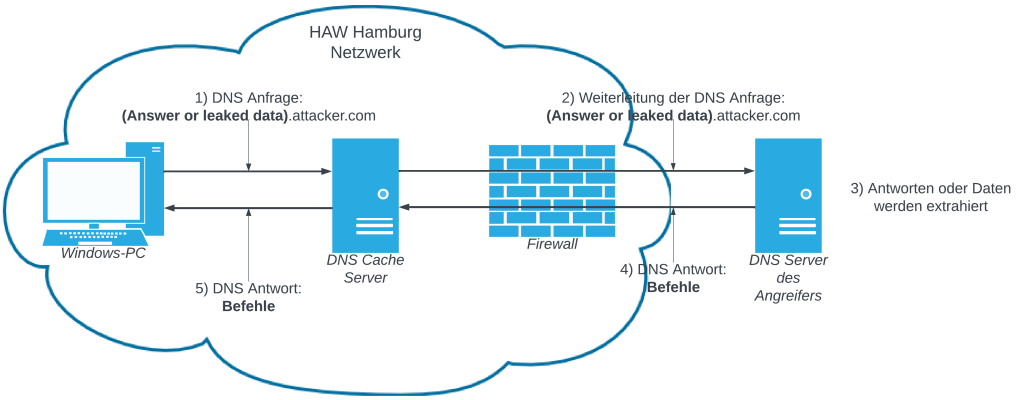

Abbildung 6.2: Vereinfachte Darstellung von DNS Tunneling, in Anlehnung an [40]

Zunächst überprüft der lokale DNS Server, ob eine Auflösung der Adresse aus dem Cache möglich ist. Da alternierende Domains verwendet werden, ist er dazu jedoch nicht in der Lage, sodass die Anfrage an den DNS Server des Angreifers weitergeleitet wird [40]. DNS stellt ein essenzielles Protokoll in einem Computernetzwerk dar, dessen Funktionalität in

der Regel nicht eingeschränkt wird. Daher erfreut es sich bei Angreifern großer Beliebtheit [40]. Im Rahmen des Szenarios wird davon ausgegangen, dass DNS unverschlüsselt verwendet wird.

In diesem Szenario werden Verbesserungspotenziale nicht erneut aufgeführt, sofern diese bereits im ersten Szenario Erwähnung gefunden haben.

6.2.2 Detect and Report

Der Monitoring Expert analysiert die DNS Anfragen vom Windows-PC, dabei fällt ihm auf, dass die Subdomains in den Anfragen in der Länge stark variieren, siehe *Detect and Report.T03*. Dieses Muster entspricht DNS Tunneling (*Detect and Report.T04*), aus diesem Grund wird der Systembetreiber identifiziert [40]. Der Windows-PC wird im Bereich Forschung und Lehre betrieben. Bei der Kommunikation mit dem Systembetreiber stellt sich heraus, dass dieser keine Kenntnisse über die verdächtigen DNS Anfragen hat und diese auch nicht im Rahmen eines Experiments erzeugt werden. Infolgedessen klassifiziert der Monitoring Expert dieses Event als Potential Incident und informiert den Incident Coordinator, siehe *Detect and Report.T06*.

Verbesserungspotenzial: *Keine weiteren oder neuen*

6.2.3 Assess and Decide

Triage

Bei der Art des Incidents handelt es sich um *Intrusion*, da Angreifer auf das System gelangt sind und einen DNS Tunnel zu einem sich in ihrer Hand befinden DNS Server betreiben können. Das Schutzziel Vertraulichkeit ist in jedem Fall verletzt, da eine Veränderung der Daten und des Systems nicht ausgeschlossen werden kann, ist auch die Integrität betroffen. Auf dem Windows-PC werden Forschungsergebnisse gespeichert. Die Forschungsergebnisse werden im Rahmen von Bachelor- und Masterarbeiten erhoben und dienen nicht der Patentanmeldung oder ähnlichen Zwecken. Es werden keine personenbezogenen Daten verarbeitet. Allerdings ist nicht auszuschließen, dass weitere

Systeme betroffen sind. Daher wird der Schutzbedarf mit *mittel*[2] angegeben. Der Wiederherstellungsaufwand wird mit Stufe 1 angegeben, für die Bearbeitung werden zusätzliche Ressourcen benötigt, um eine Wiederherstellung zu ermöglichen. Damit ergibt sich eine Punktzahl von 50 und damit eine Einstufung als *Incident*.

Bei der Identifikation nach ähnlichen Incidents wird festgestellt, dass keine ähnlichen Incidents vorliegen (*Triage.T02*).

Wie bereits bei Szenario 1 wird ebenfalls die Schwere des Angriffs, mit der in Kapitel 4 vorgestellten Methode, in Tabelle 6.2 bestimmt, siehe *Triage.T01*.

Kategorie	x	$\tilde{x}$	w
Ausmaß der Vorfallsart	2	$0,6\overline{6}$	1
Schutzbedarf	2	0,5	2
Wiederherstellungsaufwand	1	$0,3\overline{3}$	1

Tabelle 6.2: Bewertung des Schweregrads des DNS Tunnelings

Verbesserungspotenzial: *Keine weiteren oder neuen*

Meldepflichten

Es ist nur der Bereich Forschung und Lehre betroffen, aus diesem Grund erfolgt keine Meldung an Dataport oder die FHH. Da auch keine personenbezogenen Daten betroffen sind, erfolgt keine Meldung an den Datenschutzbeauftragten.

Verbesserungspotenzial: *Keine*

Assess and Decide nach den Meldepflichten

Der Incident Coordinator informiert das Management *Assess and Decide.T04* über das DNS Tunneling und die bereits getroffenen Maßnahmen. Es besteht kein weiterer Handlungsbedarf.

[2] Es wird davon ausgegangen, dass der Schutzbedarf vorab festgelegt wurde bzw. eine Schutzbedarfsanalyse erfolgt ist.

Allerdings erfolgt eine Weitergabe der Informationen an das DFN-CERT sowie das BSI im Hinblick auf den Angriff *Assess and Decide.T05)*. Es handelt sich hierbei um eine reine Informationsweitergabe.

Verbesserungspotenzial: *Keine*

Assess and Decide nach der Triage und den Meldepflichten

Im Rahmen des Incident Handlings gründet der Incident Coordinator ein Ad-hoc-Team, damit dieses die unverzüglich Arbeit aufnehmen kann (*Assess and Decide.T02*). Das Team setzt sich aus Personen mit Netzwerk- und Forensik-Wissen zusammen.

Bei der Durchführung der Intra-Incident Analyse *(Assess and Decide.T06)* identifizieren die Incident Responder eine auffällige Word-Datei, welche kurz vor Beginn des DNS-Tunnelings heruntergeladen wurde. Es wird der Hash Wert der Datei ermittelt. Eine Suche des Hash Wertes bei VirusTotal, einer Plattform, die die Ergebnisse von Analysen von Artefakten von mehreren Sicherheitsanalyse-Anbietern kumuliert, zeigt, dass die Datei im Zusammenhang mit der Schadsoftware DNSMessenger steht [63]. Durch die Aktivierung von Makros in der Word-Datei wird ein Powershellskript heruntergeladen, welches die Verbindung zu dem externen DNS Server ermöglicht [17]. Zudem wurde das Windows-Betriebssystem auf dem Windows-PC länger nicht aktualisiert, sodass die Antivirus-Software keine aktuellen Signaturen aufwies, um die Schadsoftware zu erkennen.

Die Analyse der Daten auf dem Windows-PC zeigt zudem, dass Bewerbungen von Studierenden als studentische Hilfskräfte auf dem PC gespeichert wurden. Da nicht auszuschließen ist, dass diese Daten von den Angreifern eingesehen wurden, wird der Incident Coordinator nach der Analyse darüber in Kenntnis gesetzt. Weiterhin werden keine weiteren betroffenen Systeme identifiziert. Die Inter-Incident Analyse ergibt hingegen keine Ergebnisse (*Assess and Decide.T07*).

Basierend auf den neuen Informationen entschließt sich der Incident Coordinator den Schweregrad nicht zu ändern *(Assess and Decide.T08.* Der Incident Coordinator passt den Incident Report an *(Assess and Decide.T09).* Da jetzt personenbezogene Daten betroffen sind, muss die Aktivität Meldepflichten erneut durchlaufen werden. Der Incident Coordinator benachrichtigt den Datenschutzbeauftragten und übergibt ihm eine Liste

von allen Personen, deren Bewerbungsunterlagen gespeichert wurden und den weiteren Nutzern des Windows-PCs.

Der Incident Coordinator legt die Response fest, siehe *Assess and Decide.T10*. Als erste Maßnahme soll der Windows-PC vom Netzwerk getrennt werden. In einem zweiten Schritt werden die Host-Based Firewall Regeln angepasst, um die Kommunikation mit dem bösartigen DNS Server zu verhindern. Darüber hinaus ist es erforderlich, alle Prozesse, die zum Angriff gehören, zu stoppen und das Word-Datei zu vernichten, um die Artefakte des Angreifers zu beseitigen. Anschließend soll das System aktualisiert und neugestartet werden und die Netzwerkverbindung, sowie die Prozesse des Systems überwacht werden. Dadurch kann gewährleistet werden, dass alle Spuren vollständig beseitigt wurden.

Verbesserungspotenzial: Die Analyse des Incidents, sowie das Entwickeln der Response Pläne sind Aktivitäten, die in der Realität sehr umfassend und komplex sein können. Aus diesem Grund kann es sinnvoll sein, die Aktivitäten detaillierter herauszuarbeiten und einen Rahmenplan für die Analyse von Netzwerken und Servern zu entwickeln, sowie verschiedene Playbooks die für die verschiedenen Arten von Incidents entwickelt werden, um den Incident Coordinator einen roten Faden an die Hand zu geben.

6.2.4 Respond

Nachdem der Respond-Plan durch den Incident Coordinator festgelegt und durch den CISO bestätigt wurde, übernehmen die Incident Responder das Management des Incidents. Sie kommunizieren mit den Systembetreibern erste Maßnahmen, um den Incident einzudämmen (*Respond.T01*). Dabei orientieren sie sich an dem Response Plan, das bedeutet, dass die Systembetreiber den Windows-PC vom Netzwerk nehmen und die Firewall-Regeln anpassen.

Nachdem die Systembetreiber diese Maßnahmen erfolgreich durchgeführt haben, beginnt die Beseitigung der Artefakte und Wiederherstellung des Normalbetriebs (*Respond.T03*). Im Rahmen der Kommunikation zwischen Incident Respondern und Systembetreibern werden die zu beachtenden IoCs sowie die zu entfernenden Dateien und zu stoppenden Prozesse definiert. Im Anschluss an einen vollständigen Systemscan sowie eine Aktualisierung der Software erfolgt eine Wiederanbindung des Windows-PCs an das Netzwerk. Da die Dauer der Maßnahmen weniger als sieben Tage beträgt, findet kein Zuständigkeitswechsel von Incident Respondern zu Incident Analysten statt. Der Incident Coordinator

überprüft die Schließung des Incidents (*Respond.T08*), stimmt diesem zu und ergänzt den Incident Report *(Respond.T09)*.

Verbesserungspotenzial: Diese Phase ist, wie die Analyse und die Entwicklung des Response Plans, in ihrem Ablauf sehr spezifisch und abhängig vom Umfang des Incidents. Bei dem vorliegenden spezifischen Incident wurden keine Verbesserungspotenziale identifiziert.

6.2.5 Learn Lessons

Durch die intensive Analyse in der Phase *Assess and Decide* ist aus Sicht des Incident Coordinators keine Root-Cause-Analysis notwendig *(Learn Lessons.T01)*. Es ist aus dem Incident Report ersichtlich, dass eine mit Schadsoftware versehene Word-Datei auf einem Windows-PC mit veralteten Virensignaturen geöffnet wurde. Dabei wurden Makros aktiviert, die auf die Powershell zugreifen konnten. Über DNS wurden Befehle empfangen und Daten versendet. Die Schadsoftware heißt DNSMessenger.

Eine Evaluierung des Incident Handlings ist aus Sicht des Incident Coordinators ebenfalls nicht erforderlich, da die Behandlung des Incidents schnell und ohne Komplikationen vonstattenging *(Learn Lessons.T03)*. Ebenso ist die Evaluierung des Ad-hoc-Teams aus den gleichen Gründen nicht notwendig *(Learn Lessons.T05)*.

Da keine Aktivität in der Phase Learn Lessons durchgeführt wurde, ergeben sich aus dieser Phase auch keine Verbesserungsvorschläge die umgesetzt werden könnten, siehe *Learn Lessons.T07*. Der Incident Coordinator muss im Learn Lessons Report darlegen, warum er sich gegen die Durchführung der einzelnen Aktivitäten für das Learn Lessons entschieden hat *(Learn Lessons.T09)*.

Verbesserungspotenzial: Bei der Phase Learn Lessons liegt der Fokus stark auf dem organisatorischen Ablauf. Vernachlässigt werden hingegen die technischen Maßnahmen die ergriffen werden könnten, um z. B. den vorgestellten Incident zu verhindern. Die möglichen technischen Maßnahmen könnten umfassen, dass die Makros von Windows standardmäßig deaktiviert sind. Weiterhin kann es sinnvoll sein PCs den Zugang zum Internet zu verweigern, wenn sie nicht über eine aktuelle Virensignatur verfügen. Eine solche Lösung kann mit Hilfe eines Network Access Control (NAC) implementiert werden.

7 Fazit

7.1 Zusammenfassung und Bewertung der Ergebnisse

Das Ziel der Arbeit war es einen generischen Incident Handling Prozess zu entwerfen, der sowohl dem aktuellen Stand der Technik, als auch den spezifischen Anforderungen der HAW Hamburg entspricht. Dies entstand im Rahmen des Projekts InSights, das zum Ziel hat ein umfassendes Information Security Management System an der HAW Hamburg zu etablieren, in dem sich der Incident Handling Prozess einordnet. Zu Beginn der Arbeit erfolgte zunächst die Definition und Abgrenzung wesentlicher Begriffe im Kontext des Information Security Incident Managements. Des Weiteren erfolgte eine Abgrenzung des ISIMs von ähnlichen Konzepten, wie beispielsweise dem Incident Management nach ITIL oder dem Vulnerability Management. Im Anschluss erfolgte eine Vorstellung der wesentlichen Rahmenwerke für das ISIM. In einer vorherigen Arbeit wurde die ISO/IEC 27035 als Grundlage für die Umsetzung des Incident Handlings an der HAW Hamburg ausgewählt, da der Standard den definierten Anforderungen der HAW Hamburg entspricht und eine globale Akzeptanz aufweist.

Für eine vollständige Modellierung des Incident Handling Prozesses wurden zunächst die externen Meldepflichten betrachtet, die die HAW Hamburg rechtlich zu erfüllen hat. Dabei wurde festgestellt, dass sich für den Bereich Verwaltung spezifische Meldepflichten ergeben. Darüber hinaus existieren Meldepflichten, welche sowohl in der Verwaltung als auch im Bereich Forschung und Lehre eingehalten werden müssen, wie z. B. Meldungen nach Verletzungen des Schutzes personenbezogener Daten. Außerdem wurde eine erste Abschätzung zu den Auswirkungen von NIS2 und DORA abgegeben, sowie eine Betrachtung, welche freiwilligen Meldepraktiken sich für die HAW Hamburg anbieten.

Ein weiterer wichtiger Schritt bei der Modellierung des Incident Handlings war es, ein Verfahren zur Bestimmung des Schweregrads von Incidents festzulegen. Dafür wurden

Kriterien basierend auf der ISO/IEC 27035, der NIST SP 800-61 Rev. 2 und dem National Cyber Incident Scoring System (NCISS) von CISA untersucht und ermittelt. Sie umfassen den Ausmaß der Vorfallsart, den Schutzbedarf und den Wiederherstellungsaufwand. Das Kriterium Ausmaß der Vorfallsart betrachtet die Auswirkung des Incidents auf die Schutzziele. Der Schutzbedarf basiert auf der sogenannten Schutzbedarfsanalyse, die in einer anderen Arbeit durchgeführt wurde. Der Wiederherstellungsaufwand bewertet, wie lange es dauert, bis der Regelbetrieb wiederhergestellt wurde. Die Kriterien ermöglichen die Berechnung eines Punktwerts, welcher eine Zuordnung zu vier Schwergeraden erlaubt. In dieser Arbeit wurden dafür die folgenden Schweregrade eingeführt: *Minor Incident*, *Incident*, *Major Incident* und *Krise*. Die Schweregrade ermöglichen eine Priorisierung von Incidents und eine sinnvolle Ressourcenzuweisung.

Für den Incident Handling Prozess wurden insgesamt neun Rollen festgelegt. Bei der Festlegung der Rollen lag der Fokus auf einer geringen Fragmentierung, daher wurden Entitäten mit identischen Funktionen im Rahmen des Incident Handlings in einer Rolle zusammengefasst. Die Rollen leiten sich teilweise aus der ISO/IEC 27035 ab, wurden jedoch spezifisch an die Anforderungen an die HAW Hamburg angepasst, wie z. B. den begrenzten personellen Ressourcen. Mit Hilfe des Standards *Computer Security Incident Response Team (CSIRT) Services Roles and Competencies* von FIRST wurden die Rollenprofile mit dem Stand der Technik verglichen. Ziel war die Erstellung eines Mapping, welches eine sinnvolle Anwendung des Standards mit Blick auf die Anforderungen der HAW Hamburg gewährleistet. Der Standard ermöglicht die Identifikation der für die Erfüllung der Rolle benötigten Kompetenzen.

Nach der Festlegung der Rollen erfolgte die Modellierung des Incident Handling Prozesses. Der Prozess ist in insgesamt vier Phasen unterteilt: Detect and Report, Assess and Decide, Respond und Learn Lessons. Die Modellierung erfolgte mit Hilfe von BPMN-Diagrammen. Die einzelnen Aktivitäten der Phasen wurden mit Hilfe einer RASCI-Matrix den Rollen zugewiesen, um die Verantwortlichkeiten klar zu benennen und Kompetenz- und Rollenkonflikte im Vorfeld auszuschließen. Im Anschluss wurde dargelegt, an welchen Punkten sich in dieser Arbeit von dem Rahmen der ISO/IEC 27035 gelöst wurde. Es konnte festgestellt werden, dass der Hauptgrund für die Abweichungen darin besteht, dass die ISO/IEC 27035 sequenziell bei der Bearbeitung von Incidents vorgeht, wohingegen in dem Prozess für die HAW Hamburg iterativ und insgesamt flexibler vorgegangen wird. Ein weiterer wesentlicher Unterschied zwischen den beiden Prozessen besteht darin, dass der Prozess für die HAW Hamburg die Zusammenfassung von Incidents, die korrelieren, ermöglicht. Dies führt zu einer erheblichen Reduzierung des Ressourcenaufwands für die

Bearbeitung von Incidents, da eine wiederholte Ausführung von Aktivitäten vermieden wird. In der ISO/IEC 27035 ist dies hingegen nicht vorgesehen.

Für die Evaluation des Incident Handling Prozesses wurde eine Tabletop Exercise durchgeführt. Dabei wurden zwei fiktive Szenarien untersucht. Hierbei handelte es sich zum einen um eine umfangreiche Phishing Attacke und zum anderen um eine Datenexfiltration mit Hilfe von DNS Tunneling. In beiden Szenarien wurde der Incident Handling Prozess durchlaufen und ausgewertet. Die Szenarien wurden bewusst so gewählt, dass sie sich in ihrer Schwere und Auswirkung voneinander unterscheiden und damit einen besseren Einblick in die generelle Anwendbarkeit des Prozesses geben. Die Phishing Attacke wurde als *Minor Incident* bewertet, weshalb ein anderes Vorgehen im Prozess definiert ist, als bei dem Szenario der Datenexfiltration, welches als *Incident* bewertet wurde. Dabei konnte gezeigt werden, dass der Prozess eine effektive und flexible Methode zur systematischen Bewältigung von Incidents darstellt. Zuvor wurde an der HAW Hamburg keine einheitliche Vorgehensweise bei der Bearbeitung von Incidents angewandt, sodass der Ablauf beim Incident Handling von den jeweiligen handelnden Mitarbeitern abhängig war. Der in dieser Arbeit erstellte Prozess schafft daher auch Handlungssicherheit für die Mitarbeiter bei der Bearbeitung von Incidents, da er eine klare Handlungs- und Bewertungsstruktur vorgibt. Der Prozess stellt somit eine signifikante Verbesserung der Informationssicherheit an der HAW Hamburg dar.

7.2 Ausblick

Die Konzeption eines Incident Handling Prozesses stellt ein wichtigen Schritt dar, um an der HAW Hamburg ein umfassendes ISMS einzuführen. Hier ist es auch in Bezug auf das manuelle Reporting von Incidents, auf das ein ISMS angewiesen ist, besonders wichtig, ein Bewusstsein für Informationssicherheit bei den Angestellten und Studierenden an der HAW Hamburg zu schaffen. Dies muss z. B. über Security Awareness Maßnahmen und einer offen Kommunikation erreicht werden. Es muss beachtet werden, dass die Konzeption erst der Anfang ist. Um die Effektivität und Effizienz des Incident Handlings für die HAW Hamburg zu gewährleisten, ist eine regelmäßige Evaluierung des Prozesses unerlässlich. Dazu bietet sich die Durchführung von Tabletop Exercises an, wie in dieser Arbeit vorgestellt. Dabei sollte auf einen offenen Austausch sowie ein kritisches Hinterfragen des Prozesses geachtet werden. Für eine realistischere Erprobung können zudem

Penetrationstests oder Red Teaming durchgeführt werden. Darüber hinaus ist eine kontinuierliche Aktualisierung des Prozesses erforderlich, wenn sich z. B. neue Meldepflichten ergeben, müssen diese so schnell wie möglich mit in den Prozess aufgenommen werden. Im Rahmen der Evaluierung wurden bereits sieben Verbesserungspotenziale identifiziert, die in Tabelle 7.1 dargestellt sind.

In dieser Arbeit wurde der Incident Handling Prozess konzeptionell erarbeitet. Seine Etablierung an der HAW Hamburg steht jedoch noch aus. In einer weiterführenden Arbeit sollte daher überprüft werden, welche technischen Anwendungen sich für eine erfolgreiche Umsetzung eignen. Für die Detektion von Events und die Bearbeitung von Incidents sollte ein Log-Management eingesetzt werden, um eine umfassende Datenbasis zu schaffen. Des Weiteren bietet sich darauf aufbauend die Etablierung eines SIEMs an, für eine möglichst effiziente Auswertung der Logs. Aufgrund der knappen Personalressourcen der HAW Hamburg sollte dabei ein Fokus auf einen hohen Automatisierungsgrad gelegt werden.

Bei der Einstellung von geeignetem Personal oder für Schulungen für Mitarbeiter für das Incident Handling, kann auf das in dieser Arbeit erstellte Mapping zwischen den Rollen und dem *Computer Security Incident Response Team (CSIRT) Services Roles and Competencies* zurückgegriffen werden, um Kompetenzprofile zu erstellen.

Diese Arbeit bildet den Grundstein für ein strukturiertes Incident Handling und damit für eine verbesserte Informationssicherheit an der HAW Hamburg. Viele weitere Schritte und Arbeiten sind jedoch notwendig, um ein effektives und effizientes Information Security Incident Management vollständig an der HAW Hamburg zu implementieren.

	Phase	Beschreibung
1.	Detect and Report	Der Monitoring Expert sollte die Erlaubnis haben, bei einer akuten Notwendigkeit zu handeln, ohne dass auf das Ergebnis der Triage gewartet werden muss.
2.	Assess and Decide - Triage	Es sollte überprüft werden, ob die Reihenfolge der Aktivitäten in der Triage angepasst werden sollen. Dabei sollte zunächst überprüft werden, ob der Incident korreliert, um weiteren Aufwand zu vermeiden.
3.	Assess and Decide - Triage	Die Notwendigkeit der Durchführung der Aktivität *Triage.T05: Prioritization* ist zu überprüfen, weil in der Aktivität *Triage.T01: Determiniation* bereits ein Wert festgelegt wird, der zur Priorisierung genutzt werden kann.
4.	Assess and Decide - Triage	In dem aktuellen Prozess besteht nicht die Möglichkeit, dass ein *Minor Incident* durch Korrelation mit einem Potential Incident eskaliert obwohl diese Möglichkeit grundsätzlich gegeben ist.
5.	Assess and Decide - Hauptphase	Wird ein Incident als *Minor Incident* kategorisiert endet das Incident Handling, ohne die Möglichkeit die Phase *Learn Lessons* durchzuführen. In einigen Situationen kann dies jedoch als sinnvoll erachtet werden.
6.	Assess and Decide - Hauptphase	Es sollte überprüft werden, ob Playbooks zu den jeweiligen Arten von Incidents entwickelt werden, um sich besser auf potenzielle Incidents vorbereiten zu können.
7.	Learn Lessons	In der Phase *Learn Lessons* sollten neben den organisatorischen Maßnahmen auch technische Maßnahmen überprüft werden, um die Informationssicherheit der HAW Hamburg zu gewährleisten.

Tabelle 7.1: Identifizierte Verbesserungspotenziale basierend auf der Evaluation des Incident Handlings

Literaturverzeichnis

[1] Alberts, Christopher J. ; Dorofee, Audrey J. ; Killcrece, Georgia ; Ruefle, Robin ; Zajicek, Mark T.: Defining Incident Management Processes for CSIRTs: A Work in Progress, 2004

[2] Andreas Heil: *EduSec - Sicherheitsvorfälle an deutschsprachigen Hochschulen.* – https://aheil.de/edusec/, letzter Zugriff am 27.11.2024

[3] AXELOS: *ITIL Foundation, ITIL 4 Edition.* Axelos, 2019 (ITIL 4 Foundation Series). – ISBN 9780113316168

[4] Bhardwaj, Akashdeep: *Cybersecurity Incident Response Against Advanced Persistent Threats (APTs).* S. 189–209. In: Bhardwaj, Akashdeep (Hrsg.) ; Sapra, Varun (Hrsg.): *Security Incidents & Response Against Cyber Attacks*, Springer International Publishing, 2021. – URL https://doi.org/10.1007/978-3-030-69174-5_9. – ISBN 978-3-030-69174-5

[5] Bishop, Matt ; Bailey, David: A Critical Analysis of Vulnerability Taxonomies, URL https://api.semanticscholar.org/CorpusID:14422571, 1996

[6] Bundesamt für Sicherheit in der Informationstechnik: *BSI-Standard 200-2.* – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2, letzter Zugriff am 17.04.2024

[7] Bundesamt für Sicherheit in der Informationstechnik: *Cyber-Sicherheitswarnungen.* – https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Cyber-Sicherheitswarnungen/cyber-sicherheitswarnungen_node.html, letzter Zugriff am 04.06.2024

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Die Lage der IT-Sicherheit in Deutschland 2024*. – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html?nn=129410, letzter Zugriff am 27.11.2024

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Vorfälle/Meldungen*. – https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/Meldungen-Vorfaelle/meldungen-vorfaelle_node.html, letzter Zugriff am 29.08.2024

[10] Bundesanstalt für Finanzdienstleistungsaufsicht: *DORA - Digital Operational Resilience Act*. – https://www.bafin.de/DE/Aufsicht/DORA/DORA_node.html, letzter Zugriff am 28.08.2024

[11] Bundesanstalt für Finanzdienstleistungsaufsicht: *Transparenz dank Meldepflicht*. – https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_0618_DORA.html?nn=19669324, letzter Zugriff am 21.11.2024

[12] Bundesministerium des Innern und für Heimat (BMI): *EU-Richtlinien zum Schutz Kritischer Infrastrukturen*. – https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2023/01/eu-richtlinien-kritis.html, letzter Zugriff am 27.08.2024

[13] Bundesministerium des Innern und für Heimat (BMI): *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz*. – https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf.pdf?__blob=publicationFile&v=1, letzter Zugriff am 27.08.2024

[14] Bundesministerium des Innern und für Heimat (BMI): *Umsetzung der Richtlinie (EU) 2022/2557*. – https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/KRITIS-DachG-2.pdf;jsessionid=758AC0EE1942A1461C33F425CC4A871A.live861?__blob=publicationFile&v=5, letzter Zugriff am 30.08.2024

[15] BVMW e.V.: *Innenministerium rechnet nicht mit fristgerechter Einführung von NIS-2*. – https://www.bvmw.de/de/internet-und-digitalisierung/n

ews/innenministerium-rechnet-nicht-mit-fristgerechter-einfuehrung-von-nis-2, letzter Zugriff am 21.11.2024

[16] Cichonski, Paul ; Millar, Thomas ; Grance, Timothy ; Scarfone, Karen: *NIST SP 800-61 Rev. 2*. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2012-08-06 2012

[17] Cisco Talos: *Covert Channels and Poor Decisions: The Tale of DNSMessenger*. – https://blog.talosintelligence.com/dnsmessenger/, letzter Zugriff am 15.10.2024

[18] Cybersecurity and Infrastructure Security Agency (CISA): *About CISA*. – https://www.cisa.gov/about, letzter Zugriff am 17.07.2024

[19] Cybersecurity and Infrastructure Security Agency (CISA): *Cybersecurity Incident & Vulnerability Response Playbooks*. – https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf, letzter Zugriff am 04.06.2024

[20] Cybersecurity and Infrastructure Security Agency (CISA): *Cybersecurity Tabletop Exercise Tips*. – https://www.cisa.gov/sites/default/files/publications/Cybersecurity-Tabletop-Exercise-Tips_508c.pdf, letzter Zugriff am 04.10.2024

[21] Cybersecurity and Infrastructure Security Agency (CISA): *National Cyber Incident Scoring System (NCISS)*. – https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss, letzter Zugriff am 12.07.2024

[22] DFN-CERT: *Meldungen des DFN-CERT*. – https://www.dfn-cert.de/informationen/meldungen-des-dfn-cert/, letzter Zugriff am 29.08.2024

[23] DSGVO: *Art. 33*. – https://dejure.org/gesetze/DSGVO/33.html, letzter Zugriff am 21.07.2024

[24] DSGVO: *Art. 34*. – https://dejure.org/gesetze/DSGVO/34.html, letzter Zugriff am 21.07.2024

[25] ENISA - EU Agency for Cybersecurity: *Reference Security Incident Taxonomy Working Group*. https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force. 2024

[26] European Union Agency for Cybersecurity (ENISA): *EINRICHTUNG EINES CSIRT SCHRITT FÜR SCHRITT.* – https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-german/@@download/fullReport, letzter Zugriff am 23.12.2022

[27] European Union Agency for Cybersecurity (ENISA): *Good Practice Guide for Incident Management.* – https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management, letzter Zugriff am 04.06.2024

[28] European Union Agency for Cybersecurity (ENISA): *Reference Incident Classification Taxonomy.* – https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy, letzter Zugriff am 25.06.2024

[29] Europäische Kommission: *RTS Regulation (EU) 2022/2554.* – https://www.bafin.de/SharedDocs/Downloads/DE/Anlage/dl_JC_2023_83_-Final_Report_on_draft_RTS_on_classification_of_major_incidents_and_significant_cyber_threats.pdf?__blob=publicationFile&v=4, letzter Zugriff am 27.08.2024

[30] Europäische Union: *Arten von Rechtsvorschriften.* – https://european-union.europa.eu/institutions-law-budget/law/types-legislation_de, letzter Zugriff am 28.08.2024

[31] Europäische Union: *Regulation (EU) 2022/2554.* – https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554, letzter Zugriff am 27.08.2024

[32] Europäisches Parlament: *VERORDNUNG (EU) 2019/881.* – https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881, letzter Zugriff am 17.06.2024

[33] FH Münster: *Hackerangriff: FH Münster zieht Bilanz und teilt zentrale Erkenntnisse.* – https://www.fh-muenster.de/eti/aktuell/news/pressemitteilungen.php?pmid=9215, letzter Zugriff am 27.11.2024

[34] HAW Hamburg: *Über ung.* – https://www.haw-hamburg.de/hochschule/ueber-uns/, letzter Zugriff am 08.09.2024

[35] Herrmann, Marvin: Grundprojekt: Einordnung der Schutzbedarfsanalyse in die Informationssicherheit, 2024

[36] Howard, John D.: *An analysis of security incidents on the Internet 1989-1995.* USA, Dissertation, 1998. – UMI Order No. GAX98-02539

[37] Imam Abdulrahman Bin Faisal University: *Information Ssecurity Incident Management Policy.* – https://www.iau.edu.sa/sites/default/files/resources/information_security_incident_management_policy.pdf, letzter Zugriff am 12.07.2024

[38] International Electrotechnical Commission IEC: *Frequently asked questions.* – https://www.iec.ch/faq, letzter Zugriff am 12.06.2024

[39] International Organization for Standardization (ISO): *About ISO.* – https://www.iso.org/about, letzter Zugriff am 12.06.2024

[40] Ishikura, Naotake ; Kondo, Daishi ; Vassiliades, Vassilis ; Iordanov, Iordan ; Tode, Hideki: DNS Tunneling Detection by Cache-Property-Aware Features. In: *IEEE Transactions on Network and Service Management* 18 (2021), Nr. 2, S. 1203–1217

[41] ISO/IEC: *27000:2018*

[42] ISO/IEC: *27035-1:2023*

[43] ISO/IEC: *27035-2:2023*

[44] ISO/IEC: *27035-3:2020*

[45] ISO/IEC: *27035-4:2024*

[46] Kowoll, Lars: Forschungswerkstatt 1: Identifizierung eines Information Security Incident Management Frameworks für die HAW Hamburg, 2023

[47] Kowoll, Lars: Grundprojekt: Incident Handling für die HAW Hamburg, 2024

[48] Kowoll, Lars: Hauptprojekt: Verbesserte Incident Handling Prozesse für die HAW Hamburg, 2024

[49] Leyendecker, Bert: *Teammanagement und Moderation.* S. 15–48. In: Leyendecker, Bert (Hrsg.) ; Pötters, Patrick (Hrsg.): *Werkzeuge für das Projekt- und*

Prozessmanagement: Klassische und moderne Instrumente für den Management-Alltag. Wiesbaden : Springer Fachmedien Wiesbaden, 2022. – URL https://doi.org/10.1007/978-3-658-34724-6_3. – ISBN 978-3-658-34724-6

[50] Moore, David ; Paxson, Vern ; Savage, Stefan ; Shannon, Colleen ; Staniford, S. ; Weaver, Nicholas: Inside the Slammer worm. In: *Security & Privacy, IEEE* 1 (2003), 08, S. 33 – 39

[51] National Institute of Standards and Technology (NIST): *About NIST*. – https://www.nist.gov/about-nist, letzter Zugriff am 17.06.2024

[52] National Institute of Standards and Technology (NIST): *Asset*. – https://csrc.nist.gov/glossary/term/asset, letzter Zugriff am 04.06.2024

[53] National Institute of Standards and Technology (NIST): *Vulnerability*. – https://csrc.nist.gov/glossary/term/vulnerability, letzter Zugriff am 04.06.2024

[54] Nelson, Alexander ; Rekhi, Sanjay ; Souppaya, Murugiah ; Scarfone, Karen: *NIST SP 800-61 Rev. 3 (Initial Public Draft)*. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2024-04-03 2024

[55] New York University: *Cyber Incident Response*. – https://www.nyu.edu/life/information-technology/safe-computing/protect-nyu/cyber-incident-response.html, letzter Zugriff am 12.07.2024

[56] Rahmen-Sicherheitskonzept der Freien und Hansestadt Hamburg: *RaSiKo Version 1.1*. – http://daten.transparenz.hamburg.de/Dataport.HmbTG.ZS.Webservice.GetRessource100/GetRessource100.svc/4c792633-a668-4d5c-88eb-97494252b187/Akte_FB1a.803.73-50.pdf, letzter Zugriff am 19.07.2024

[57] Simmons, Chris ; Ellis, Charles ; Shiva, S. ; Dasgupta, Dipankar ; Wu, Chase: AVOIDIT: A Cyber Attack Taxonomy. (2009), 01

[58] Staatskanzlei des Landes Nordrhein-Westfalen: *Hochschulen starten gemeinsames Security Operation Center*. – https://www.land.nrw/pressemitteilung/fuer-mehr-cybersicherheit-hochschulen-starten-gemeinsames-security-operation, letzter Zugriff am 27.11.2024

[59] Tøndel, Inger A. ; Bartnes, Maria ; Jaatun, Martin: Information security incident management: Current practice as reported in the literature. In: *Computers & Security* (2014), 09

[60] University of Cincinnati: *Information Security Incident Response Procedure.* – https://www.uc.edu/content/dam/uc/infosec/docs/general/Information_Security_Incident_Response_Procedure.pdf, letzter Zugriff am 12.07.2024

[61] Universität Hamburg: *IT-Sicherheitshinweis: Warnung vor Phishing-Mail mit Betreff: E-Mail-Speicherbenachrichtigung.* – https://www.slm.uni-hamburg.de/service/it/aktuelles/2022/2022-10-18-phishing-e-mail-speicherbenachrichtigung.html, letzter Zugriff am 02.10.2024

[62] UpGuard: *What are Indicators of Attack (IOAs)? How they Differ from IOCs.* – https://www.upguard.com/blog/what-are-indicators-of-attack, letzter Zugriff am 15.08.2024

[63] VirusTotal: *DNSMessenger.* – https://www.virustotal.com/gui/file/340795d1f2c2bdab1f2382188a7b5c838e0a79d3f059d2db9eb274b0205f6981/details, letzter Zugriff am 15.10.2024

A Anhang

ID	Beschreibung	Herkunft	
		ISO/IEC 27002	**IT-Grundschutz-Kompendium**
	Management		
Anf1	Organisatorisch sollten Sicherheitsleitlinien zu Themen des ISIM erstellt werden, in denen Zweck und Ziel sowie Anforderungen und Vorgaben der Richtlinie festgehalten werden. Folgende Themen sollten Berücksichtigung finden: Detektion von sicherheitsrelevanten Ereignissen, Behandlung von IS Incidents und Planung und Vorbereitung für IS Incident Response	• 16.1.1	• DER.1.A1 • DER.2.1.A2 • DER.2.1.A7
Anf2	Es sollte eine Sicherheitsleitlinie erstellt werden, die sich mit der Beweissicherung befasst. Die Themen Identifizierung, Sammlung, Beschaffung und Aufbewahrung von Informationen, die als Beweismittel dienen können, sollten behandelt werden.	• 16.1.7	
Anf3	Organisatorisch sollte vorab ein Team für die Behandlung von IS Incidents ernannt werden. Innerhalb des Teams muss Klarheit über die Aufgaben und Anforderung an die einzelnen Teammitglieder herrschen. Weiterhin sollte eine Einbindung in das Sicherheits- und Notfallmanagement erfolgen, sowie eine Festlegung der Schnittstellen innerhalb der Organisation bei der Behandlung von IS Incidents.	• 16.1.1	• DER.2.1.A3 • DER.2.1.A8 • DER.2.1.A12 • DER.2.1.A13

ID	Beschreibung	Herkunft	
		ISO/IEC 27002	**IT-Grundschutz-Kompendium**
	Management		
Anf4	Der Begriff Sicherheitsvorfall sollte definiert und Klassifikationen für eben diese erstellt werden. Basierend auf den ausgearbeiteten, einheitlichen Klassifikationen sollte entschieden werden, ob ein IS Event als IS Incident zu bewerten ist. Weiterhin soll eine Priorisierung der IS Incidents erfolgen.	• 16.1.1 • 16.1.4	• DER.2.1.A1 • DER.2.1.A11 • DER.2.1.A19
Anf5	Für Information Security Events sollte eine Festlegung von Meldewegen erfolgen, sowie die Benennung eines Point of Contact. Weiterhin sollte eine Kommunikations- und Kontaktstrategie erstellt werden, in der geregelt wird an wen gemeldet werden darf bzw. muss. Außerdem sollte eine Eskalationsstrategie verfasst werden in der festgelegt wird an wen und wann im Falle eines IS Incident eskaliert werden soll.	• 16.1.1 • 16.1.2	• DER.1.A3 • DER.2.1.A9 • DER.2.1.A14

Tabelle A.1: Anforderungen aus der Kategorie *Management* für die Bewertung der ISIM-Frameworks, entnommen aus [46]

ID	Beschreibung	Herkunft	
		ISO/IEC 27002	IT-Grundschutz-Kompendium
Aufgabenbereiche und Schulungen von Mitarbeitern			
Anf6	Damit Mitarbeiter die im Bereich es ISIM tätig sind über die notwendigen Qualifikationen verfügen, sollten regelmäßige Schulungen durchgeführt werden.		• DER.1.A7 • DER.2.1.A15
Anf7	Die Aufgabenbereiche der Mitarbeiter, innerhalb des ISIM, sollten u. a. die Überwachung der Integrität und Funktionsweise der Systeme und Benutzerberechtigungen, sowie die Protokollierungsdaten zu analysieren und auszuwerten umfassen.		• DER.1.A6 • DER.1.A13 • DER.1.A18
Anf8	Es sollte eine Sensibilisierung der Mitarbeiter erfolgen, welche Maßnahmen sie bei IS Events durchzuführen haben.	• 16.1.1 • 16.1.2	• DER.1.A4

Tabelle A.2: Anforderungen aus der Kategorie *Aufgabenbereiche und Schulungen von Mitarbeitern* für die Bewertung der ISIM-Frameworks, entnommen aus [46]

ID	Beschreibung	Herkunft	
		ISO/IEC 27002	**IT-Grundschutz-Kompendium**
Information Security Incident Response			
Anf9	Bei der Behebung eines IS Incidents sollten die folgenden Maßnahmen vom Prozess abgedeckt werden: Sammeln von Beweismaterial, Durchführung forensischer Analyse (wenn nötig), Eskalieren des Prozess (wenn nötig), Dokumentieren aller durchgeführten Maßnahmen bei der Behebung des Sicherheitsvorfall, Kommunikation auf einer need-to-know Basis mit internen und externen Organisationen bzw. Personen, Behandeln von Schwachstellen die den Sicherheitsvorfall ausgelöst bzw. begünstigt haben, nach erfolgreicher Behandlung den Incident formal schließen und dokumentieren	• 16.1.5	• DER.2.1.A4 • DER.2.1.A5 • DER.2.1.A16
Anf10	Bei der Behandlung eines IS Incidents sollte zunächst das Problem eingegrenzt und die Ursache gefunden werden. An dieser Stelle sollte darüber entschieden werden, ob die Priorisierung auf dem Eindämmen des Schadens oder der Aufklärung des IS Incidents liegt. Danach müssen Maßnahmen identifiziert werden, um das Problem zu bekämpfen. Erst nach erreichen eines normalen Security Levels kann mit der Wiederherstellung des Normalbetriebs begonnen werden.	• 16.1.5	• DER.2.1.A5 • DER.2.1.A6 • DER.2.1.A10

ID	Beschreibung	Herkunft	
		ISO/IEC 27002	**IT-Grundschutz-Kompendium**
Information Security Incident Response			
Anf11	Ein Lessons Learned sollte nach der erfolgreichen Beseitigung eines IS Incidents durchgeführt werden. Das Ziel ist es die Wahrscheinlichkeit und den Einfluss zukünftiger IS Incidents zu verringern. Weiterhin soll das Lessons Learned dazu dienen, den entwickelten Prozess für die Behandlung von IS Incidents kritisch zu bewerten und basierend auf den gesammelten Erkenntnissen weiterzuentwickeln.	• 16.1.6	• DER.2.1.A17 • DER.2.1.A18
Anf12	Mit Hilfe von Übungen sollte das ISIM in regelmäßigen Abständen auf die Effizienz überprüft werden. Weiterhin sollten bei einem IS Incident wichtige Messwerte dokumentiert werden, die die Effizienz des Managements quantifizieren und eine Vergleichbarkeit ermöglichen.	• 16.1.6	• DER.2.1.A22

Tabelle A.3: Anforderungen aus der Kategorie *Information Security Incident Response* für die Bewertung der ISIM-Frameworks, entnommen aus [46]

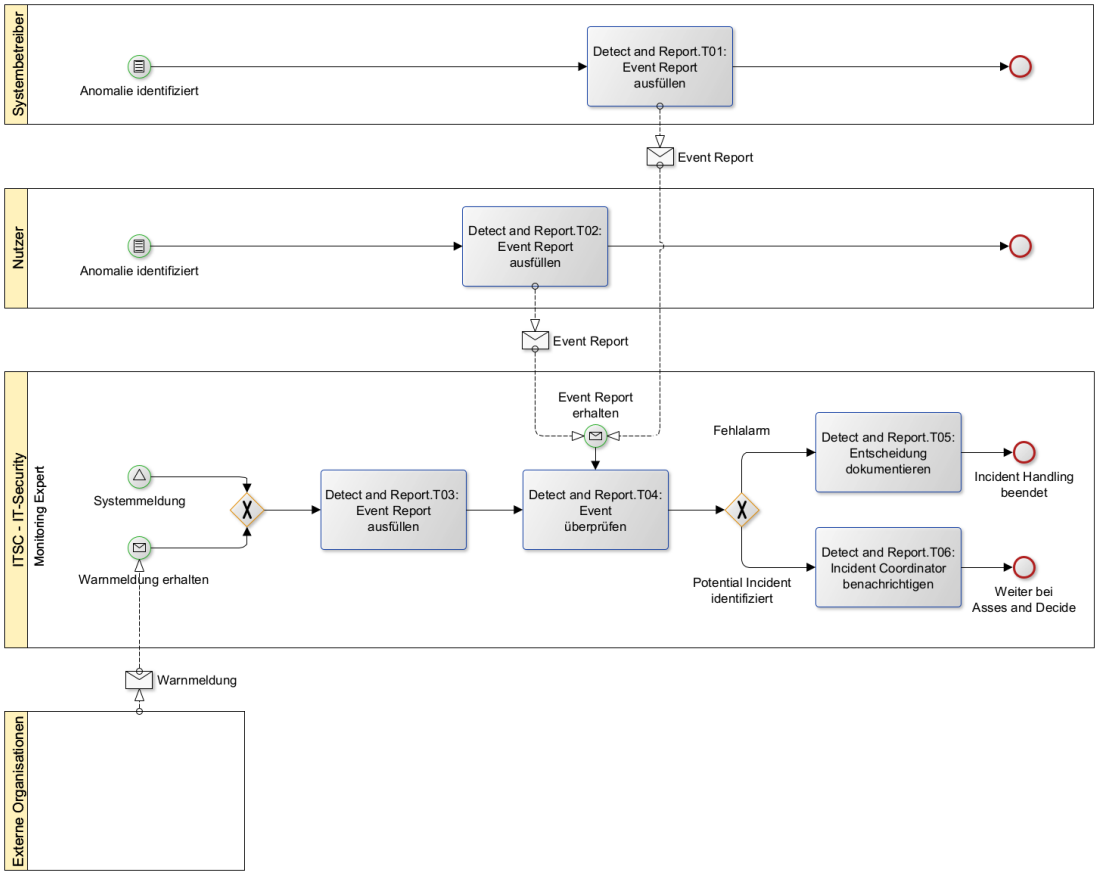

Abbildung A.1: Prozessdiagramm für die Phase *Detect and Report*, auf Basis von [48]

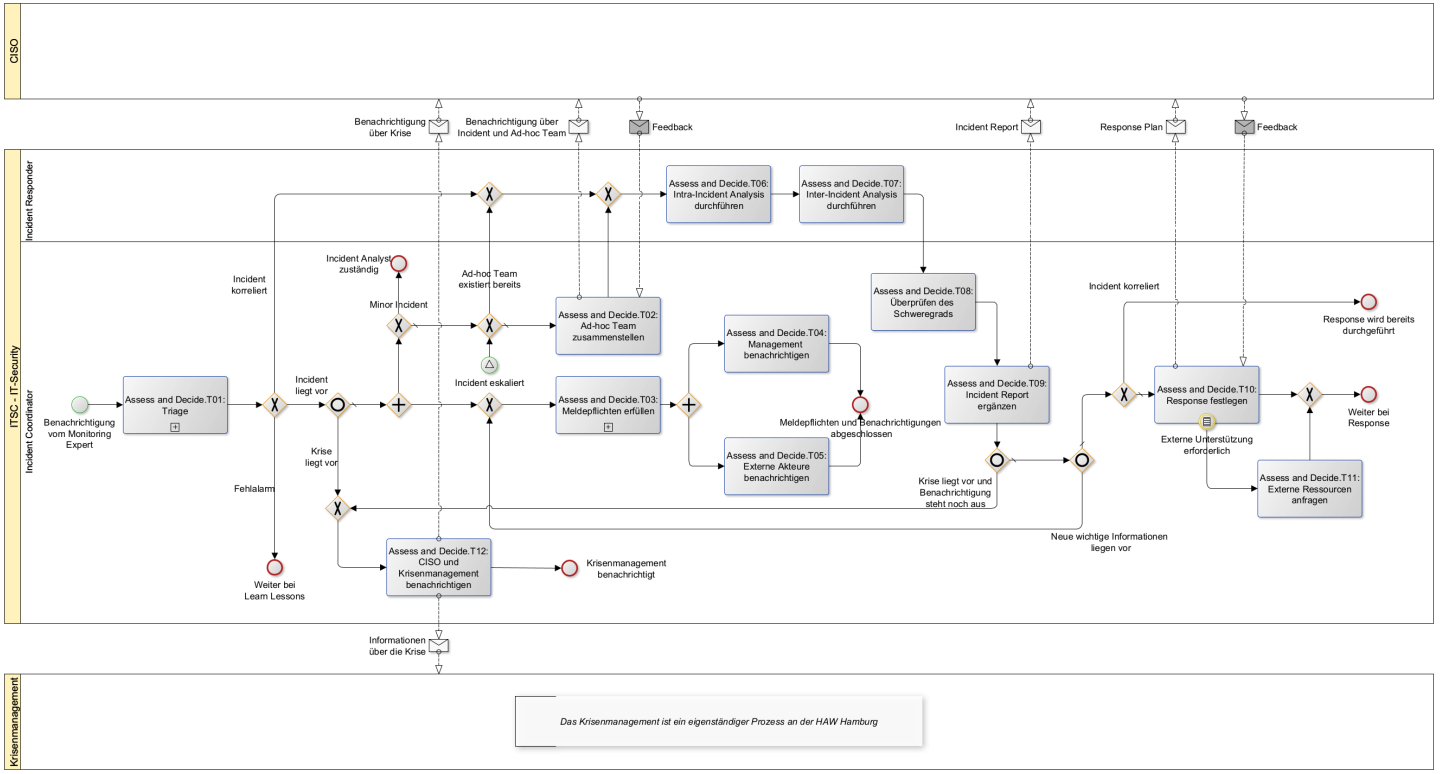

Abbildung A.2: Prozessdiagramm für die Phase *Assess and Decide*, auf Basis von [48]

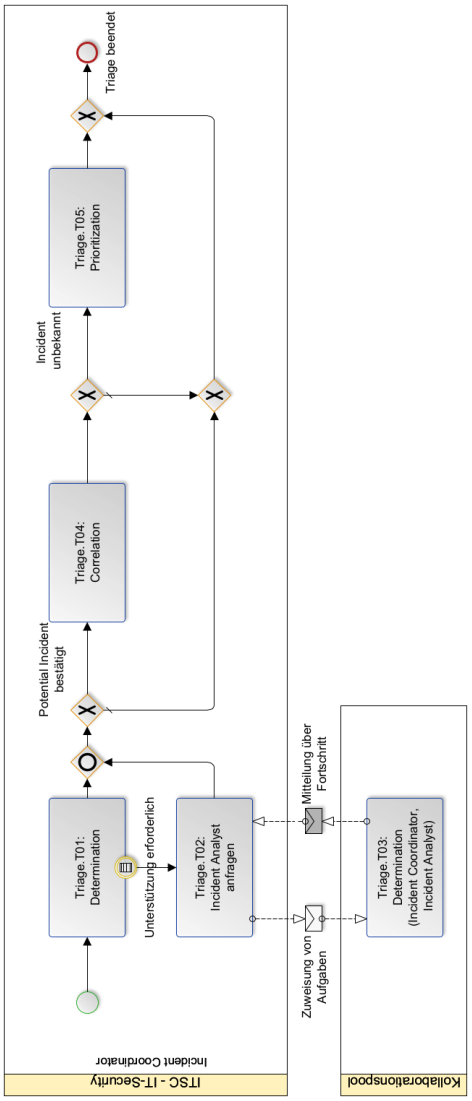

Abbildung A.3: Prozessdiagramm für den Unterprozess *Triage* aus der Phase *Assess and Decide*, auf Basis von [48]

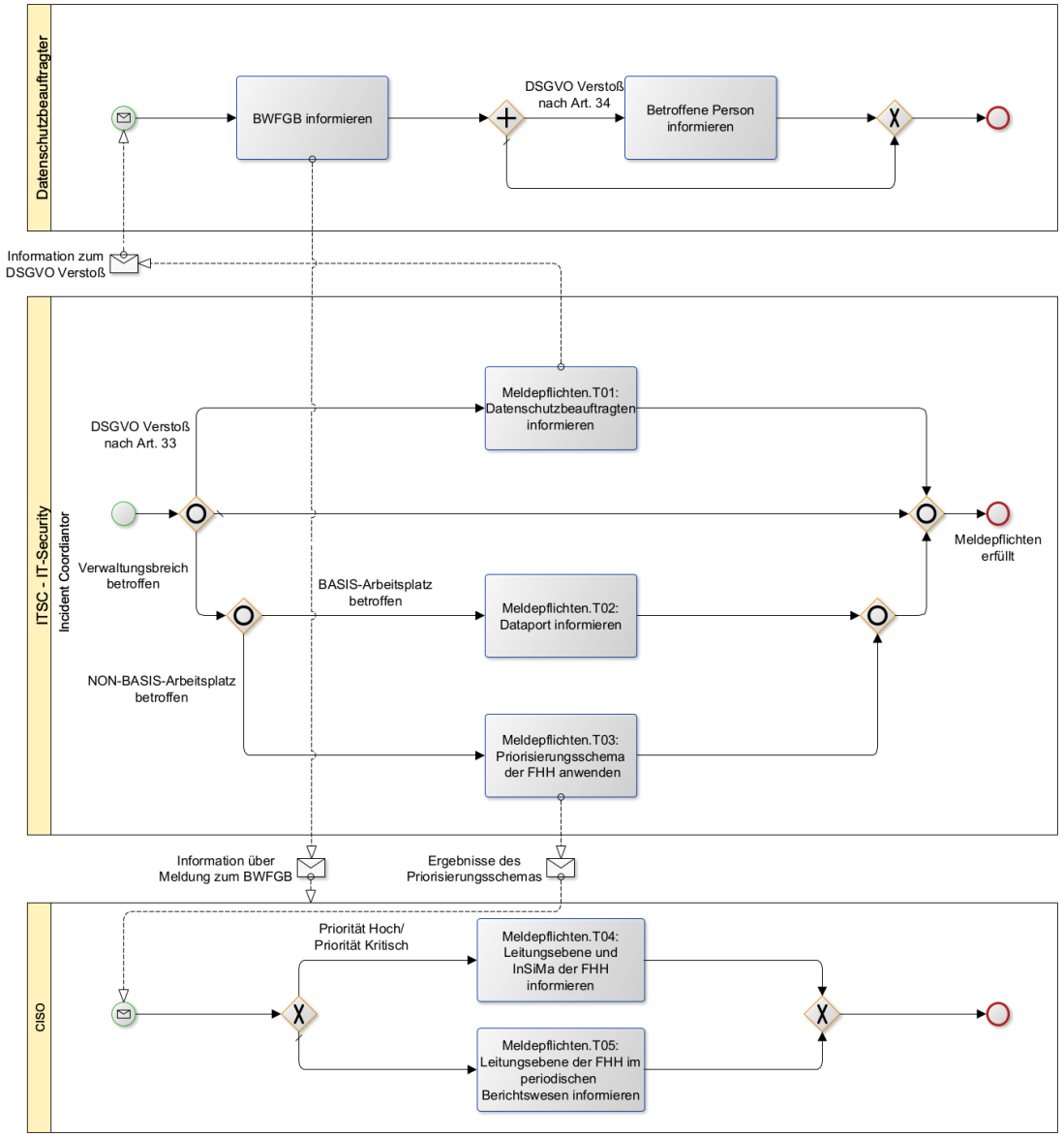

Abbildung A.4: Prozessdiagramm für den Unterprozess *Meldepflichten* aus der Phase *Assess and Decide*, auf Basis von [48]

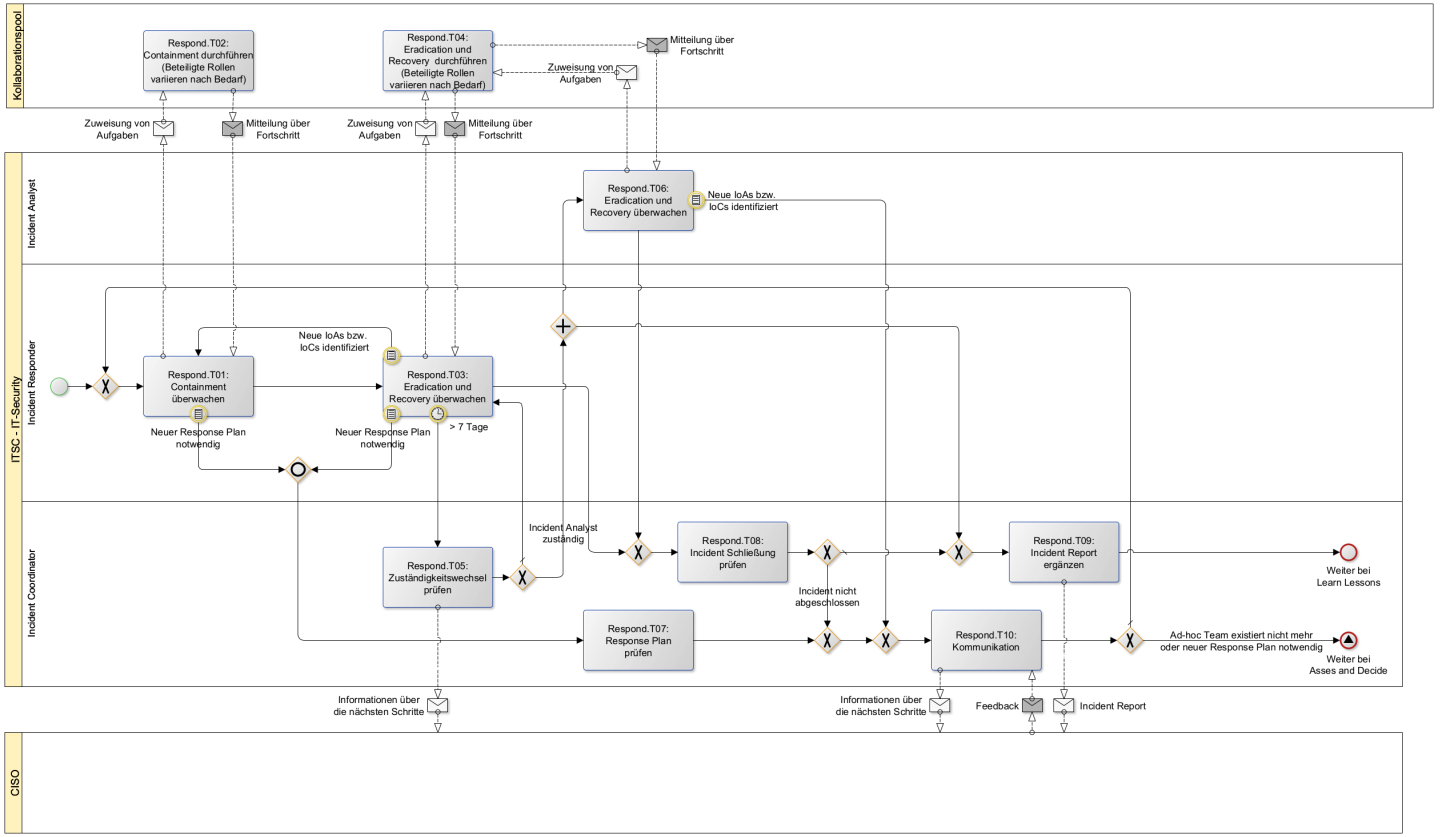

Abbildung A.5: Prozessdiagramm für die Phase *Respond*, auf Basis von [48]

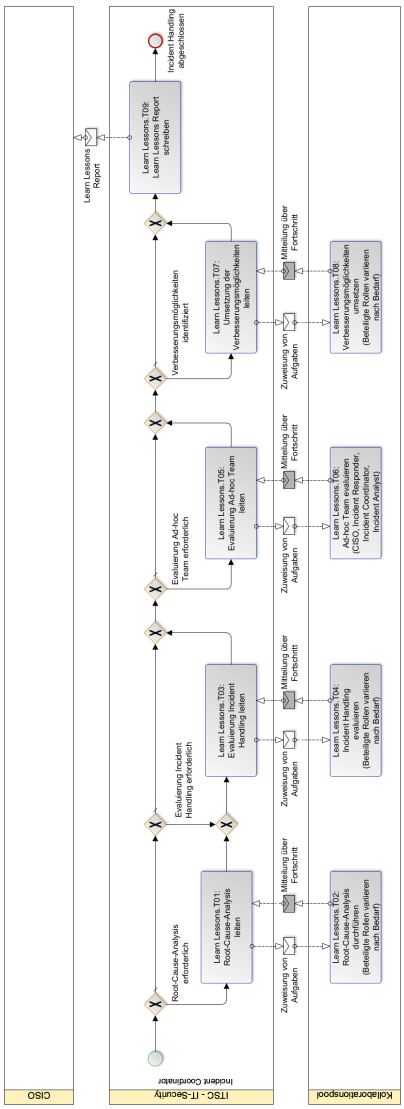

Abbildung A.6: Prozessdiagramm für die Phase *Learn Lessons*, auf Basis von [48]

Erklärung zur selbständigen Bearbeitung

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

Ort	Datum	Unterschrift im Original