ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik & Security

fh st.pölten

Incident Handling als Königsklasse in der IT Security

Inhalte einer Incident Handling-Lehrveranstaltung und Konzipierung einer Cyberrange als Abschlussübung

Masterarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur

eingereicht von

Christoph Einsiedl, BSc

52003422

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer/in: FH-Prof. Dipl.-Ing. Dipl.-Ing. Christoph Lang-Muhr, BSc

Mitwirkung: -

Ehrenwörtliche Erklärung

Titel: Incident Handling als Königsklasse in der IT Security

Art der Arbeit: Masterarbeit

Autor: Christoph Einsiedl, BSc

Matrikelnummer: 52003422

Ich versichere, dass

- ich diese Arbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich das Thema dieser Arbeit bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Ich erkläre hiermit, dass

☐ ich ein Large Language Model (LLM) verwendet habe, um die Arbeit Korrektur zu lesen.

☒ ich ein Large Language Model (LLM) verwendet habe, um Teile des Inhalts der Arbeit zu erstellen. Ich versichere, dass ich jeden generierten Satz/Absatz mit der Originalquelle zitiert habe. Das genutzte LLM ist an entsprechenden Stellen durch eine Fußnote ausgewiesen.

☐ im Zuge dieser Arbeit kein Large Language Model (LLM) zum Einsatz gekommen ist.

Ort, Datum *Unterschrift*

Kurzfassung

Die Anforderungen an Incident Handler sind vielfältig und umfangreich. Diese Spezialist:innen werden immer dann gerufen, wenn ein Angriff auf IT- oder OT-Systeme bereits erfolgreich war und die Organisation möglicherweise gerade um ihr Fortbestehen und die Wiederherstellung des Betriebs kämpft. Diese Krisensituation der Unternehmen setzt auch die Fachleute unter enormen Druck, wobei neben der Kritikalität auch der Zeitfaktor belastend wirken kann. Um effizient zu helfen, müssen Incident Handler daher ein breites Set an Wissen (Knowledge) und Fähigkeiten (Skills) mitbringen. Zentral zu dem Berufsbild gehört dabei auch die hohe Flexibilität und Lernbereitschaft, da sich das IT-Security-Personal aufgrund der ständig verändernden Bedrohungslandschaft, immer neuen Bedrohungsakteuren und einer Vielzahl an Systemen in den Organisationen laufend weiterentwickeln muss.

Diese zahlreichen Fähigkeiten und Fertigkeiten gilt es für Studierende zu Beginn des Masterstudiengangs Information Security an der Fachhochschule St. Pölten noch zu erwerben. Um die Lehre einerseits auf einer inhaltlich wissenschaftlich fundierten Ebene und andererseits aus einer didaktisch angemessenen Perspektive planen zu können, befasst sich die vorliegende Arbeit mit den Anforderungen an Incident Handler und beschreibt davon ausgehend zu setzende Schritte in der Lehre dieser, um die Studierenden auf die Praxis im Bearbeiten von Security Incidents bestmöglich vorzubereiten.

Dazu wurden die Anforderungen an Incident Handler in der österreichischen Wirtschaft aus der Literatur und mittels Experteninterviews ermittelt und diese in Form von Task-, Knowledge-, und Skill-Statements festgehalten. Aus dem umfangreichen Katalog an Aufgaben, benötigtem Wissen und Fertigkeiten wurden dann Überlegungen zu den Inhalten einer Lehrveranstaltung zu den organisatorischen Facetten des Incident Handling an der Fachhochschule St. Pölten angestellt und als Lernziele festgehalten. Auf Basis dieser wurde wiederum eine Cyberrange konzipiert, die im Sinne des game-based Learning als abschließende Übung der Lehrveranstaltung die Vertiefung und praktische Anwendung Kerninhalte fokussiert.

Abstract

The requirements for incident handlers are diverse and extensive. These specialists are called whenever an attack on IT or OT systems has already been successful and the organization may be struggling to uphold its existence and restore operations. This crisis situation for companies also puts enormous pressure on the specialists, whereby the time factor can be a burden in addition to the criticality. In order to provide efficient assistance, incident handlers must therefore have a broad set of knowledge and skills. A high degree of flexibility and willingness to learn are also central to the profession, as IT security personnel must constantly evolve due to the ever-changing threat landscape, new threat actors and a large number of systems in the organizations.

Students still need to acquire these numerous skills and abilities at the beginning of the Master's degree program in Information Security at St. Pölten University of Applied Sciences. In order to be able to plan teaching on a scientifically founded level on the one hand and from a didactically appropriate perspective on the other, this thesis deals with the requirements for incident handlers and, based on this, describes the steps to be taken in teaching these skills in order to best prepare students for the practical handling of security incidents.

For this purpose, the requirements for incident handlers in the Austrian economy were determined from the relevant literature and interviews with experts and recorded in the form of task, knowledge and skill statements. From the extensive catalog of tasks, required knowledge and skills, considerations were then made regarding the content of a course on organizational aspects of incident handling at St. Pölten University of Applied Sciences and recorded as learning objectives. Based on these, a cyberrange was designed, which focuses on the consolidation and practical application of core content in the sense of game-based learning as the final exercise of the course.

Inhaltsverzeichnis

1. Einleitung

Security Handling ist ein fundamentaler Bereich der IT Sicherheit. Der Umgang mit Security Incidents beschäftigt heutzutage nicht mehr nur das Fachpersonal, sondern auch sämtliche Unternehmen, Behörden und deren Angestellte, da die Zahl der Sicherheitsvorfälle hoch ist und die Angriffsstrategien immer vielfältiger werden. Mandiant berichtet im M-Trends 2025 Report, dass Angreifer hauptsächlich opportunistisch vorgehen und jede Möglichkeit nutzen, um ihre Ziele zu erreichen. [1] Die früher oft gehörte Aussage kleiner und mittelständischer Unternehmen *Wer soll uns denn schon angreifen? Wir sind viel zu klein und unbedeutend.* ist längst widerlegt und entspricht nicht der Wahrheit.

Dabei haben 43% aller Organisationen, die 2024 kompromittiert wurden, diese Kompromittierung 2024 selbst erkannt. Weitere 43% wurden von einer externen Quelle, beispielsweise einer Behörde, darüber informiert. In den verbleibenden 14% der Fälle informierte der Bedrohungsakteur die betroffenen Organisationen selbst. Diese Art der Benachrichtigung ist selbstredend ausschließlich im Falle eines Ransomwareangriffes, beispielsweise über ein Erpresserschreiben nach der Verschlüsselung aller Daten, zu finden. [1]

Mehr als ein Fünftel aller als finanziell motiviert eingestuften Angriffe entfielen im Jahr 2024 auf Ransomwareangriffe. [1] ISACA schätzt, dass der alleine durch Ransomware verursachte Schaden bei 6 Billionen US-Dollar liegt. [2]

Die Problematik der immer komplexer und teurer werdenden Angriffe verstärkt sich durch den Fachkräftemangel im IT Security-Bereich. Das World Economic Forum meldet 2024, dass hierbei weltweit fast vier Millionen Fachkräfte im Cybersecuritybereich fehlen und führt an, dass auch bessere Bildungsmaßnahmen für diese notwendig seien, um auf derzeit vorherrschende Bedrohungen angemessen reagieren zu können. Bis 2030 könnten international sogar bis zu 85 Millionen Fachkräfte fehlen. Das WEF beschreibt auch die Gefahr von finanziellen Verlusten, wenn zu wenig Fachpersonal für das Security Incident Handling vorhanden ist. [3]

Dabei streicht das WEF insbesondere die Notwendigkeit von praktischen Assessments, beispielsweise in Form von Hackathons, hervor, durch die die Leistung von beispielsweise Incident Handlern oder Penetration Testern evaluiert und verbessert werden soll. [3]

Gleichzeitig existieren keine wissenschaftliche Arbeiten, die sich mit den Anforderungen an Incident Handler beschäftigen. NIST beschreibt eine Work Role Incident Response mit verschiedenen Task-, Knowledge-, und Skill-Statements [4]; es ist aber nicht transparent gemacht, wie diese entstanden sind. Um die dringend notwendige Qualifizierung der Fachkräfte jedoch evidenzbasiert voranzutreiben, strukturiert zu evaluieren und daraus Schlussfolgerungen abzuleiten, die die Lehre erneut verbessern und an die Erfordernisse der Praxis anpassen, ist eine wissenschaftliche Vorgangsweise bei der Erstellung von Lehrveranstaltungen unumgänglich.

Die vorliegende Arbeit nähert sich vor dem Hintergrund dieser Herausforderungen wissenschaftlich an das Thema der Planung einer Lehrveranstaltung mit organisatorischem Schwerpunkt im Incident Handling und der Implementierung einer Cyberrange als Abschlussübung dieser an und befasst sich dabei mit folgenden Fragestellungen:

- Welches Wissen und welche Skills im organisatorischen Bereich werden von einem Incident Handler in der österreichischen Wirtschaft von verschiedenen Incident Handling-Providern verlangt und in welchen Bereichen wird dieser eingesetzt?
- Welche Aspekte machen das notwendige theoretische organisatorische Wissen über Incident Handling aus und müssen daher im Rahmen einer Lehrveranstaltung gelehrt werden?
- Wie kann mittels einer Cyberrange als Abschlussübung das im Rahmen einer Lehrveranstaltung an der Fachhochschule St. Pölten erworbene Wissen gefestigt werden?

Mit der ersten dieser Forschungsfragen wird die Basis für die Arbeit und die Lehrveranstaltungskonzeption gelegt, da aus den erhobenen Anforderungen die Lernziele und die zu unterrichtenden Inhalte resultieren. Die erhobenen Anforderungen werden dabei in TKS-Statements formuliert, um die Ansprüche, die an Incident Handler seitens der Wirtschaft bestehen, transparent zu machen. Von der ersten Frage ausgehend werden im Zuge der Beantwortung der zweiten Fragestellung die Lernziele mittels Bloom'scher Lernzieltaxonomie definiert. Diese umfassen die Inhalte und Kompetenzen, die von den Studierenden erworben werden sollen und definieren dabei auch das Anforderungsniveau, auf dem diese beherrscht werden sollen. Auf dem Ergebnis der letzten Forschungsfrage sollen die Rahmenbedingungen für das Konzept und die Durchführung der Cyberrange beruhen, die als große Abschlussübung dienen soll. Bei dieser sollen die Studierenden in Gruppen als externe Incident Handler einen IT Sicherheitsvorfall analysieren, beheben und nachbereiten.

Um diese Fragestellungen zu beantworten werden im Folgenden zunächst die Grundlagen (siehe 2 Grundlagen) erarbeitet und verwandte Arbeiten präsentiert (siehe 3 Related Work), an die die Arbeit inhaltlich anschließt. In 4 Methodik wird die Vorgangsweise plausibilisiert, mit der die in 5 Ergebnisse präsentierten

Daten und Informationen erhalten wurden. Die Arbeit schließt mit einer Diskussion (siehe 6 Diskussion) und dem Fazit (siehe 7 Conclusio).

Die dabei erwarteten Ergebnisse sind einerseits ein Anforderungskatalog an Incident Handler in Form von TKS-Statements und andererseits Lernziele für eine Lehrveranstaltung zu diesem Thema im Masterstudiengang Information Security an der Fachhochschule St. Pölten. Auf diesen aufbauend soll eine Cyberrange als Abschlussübung dieser konzipiert werden, in der ein Sicherheitsvorfall in einem einfachen Enterprisenetzwerk simuliert wird. Diese Konzeption stellt dabei den Kern der Arbeit dar.

All diese Ergebnisse wären ohne die Beteiligung einiger Personen nicht möglich gewesen, weswegen diesen mein Dank für ihre Unterstützung gebührt. Zunächst gilt er meinen Interviewpartnern Philipp Mattes-Draxler, Andreas Plank, Utz Nisslmüller und Gideon Teubert für ihre wertvollen Beiträge, ihre Zeit und die Einblicke in ihre Tätigkeit. Ich danke auch dem Betreuer dieser Arbeit, Christoph Lang-Muhr, für seine hilfreichen Inputs und Verbesserungsvorschläge während des Schreib- und Forschungsprozesses. Weiters möchte ich mich bei meinen Eltern bedanken, die mein Studium durch ihre Unterstützung überhaupt erst ermöglicht haben. Einen besonderen Dank möchte ich aber Martina aussprechen. Sie hat nicht nur durch ihr Korrekturlesen, sondern auch durch zahlreiche Ideen, kritische Debatten und ihre moralische und emotionale Unterstützung den Erstellungsprozess dieser Arbeit begleitet und diese in der vorliegenden Form überhaupt erst möglich gemacht.

2. Grundlagen

Wie in der Einleitung (siehe 1 Einleitung) beschrieben, ist ein Ziel der Arbeit, eine Cyberrange zu konzipieren, an der die Bearbeitung eines Sicherheitsvorfalles geübt werden kann. Dafür ist es notwendig, in einem ersten Schritt zentrale Grundlagen zu beschreiben, auf denen die anschließenden Überlegungen basieren. Im Folgenden werden daher zunächst die Begriffe Security Incident und Incident Handling definiert und von verwandten Konzepten abgegrenzt. Daran anschließend wird das Konzept der Cyberrange und deren Ziele sowie der technische Aufbau in Grobform beschrieben, da diese als Abschlussübung einen wesentlichen Teil der im Zuge der Arbeit konzipierten Lehrveranstaltung darstellt. Darüber hinaus wird die NIST SP-800-181, besser bekannt als NICE Framework, skizziert, die mithilfe der darin enthaltenen TKS-Taxonomie die Anforderungen an einen Incident Handler modelliert. Des Weiteren werden einige der für die Tätigkeit im Bereich Incident Handling relevanten Standards und Normen wie ISO 27035, CIS Controls oder NIST SP 800-61 vorgestellt. Das Kapitel schließt mit der Darstellung der didaktischen Konzepte, auf Basis derer die Lehrveranstaltung konzipiert wurde.

2.1. Begrifflichkeiten und zentrale Konzepte

Im Bereich IT Security existiert eine Vielzahl von Begriffen und Abkürzungen, die im alltäglichen Sprachgebrauch oftmals nicht trennscharf voneinander abgegrenzt werden und daher nicht eindeutig auf die dahinterstehenden wissenschaftlichen Konzepte referieren. Deswegen sollen in einem ersten Schritt die zentralen Termini, die der Arbeit zugrunde liegen, definiert werden.

2.1.1. Begriffsabgrenzung Incident - Security Incident

ISO 27000:2023 versteht unter einem **Informationssicherheitsvorfall** oder einem Information Security Incident ein „einzelnes oder eine Reihe von ungewollten oder unerwarteten Informationssicherheitsereignissen [...], die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden oder die Informationssicherheit [...] zu bedrohen“ [5, S. 14]. Die Bedrohung der Informationssicherheit bedeutet dabei, dass

entweder die Vertraulichkeit, die Integrität oder die Verfügbarkeit von Informationen gefährdet sind. [5, S. 13].

Umgangssprachlich wird der Information Security Incident auch manchmal verkürzt als „**Incident**“ bezeichnet. In NIST SP800-61 findet sich eine solche Gleichstellung der Begrifflichkeiten: „A cybersecurity incident (or simply incident) is [...]“ [6, Kap. 1]. Auch im Internet finden sich Blogartikel namhafter Hersteller von Security-Lösungen, die beide Begriffe synonym verwenden [7]. Dies ist in der ISO-Normenreihe jedoch nicht vorgesehen. Andere Leitfäden wie ITIL verstehen unter einem Incident zudem eine ungeplante Unterbrechung eines Services oder eine Reduktion der Qualität des Services [8, S. 121]. Somit ist nicht jeder (ITIL-)Incident auch gleichzeitig ein Information Security Incident. Um in dieser Arbeit deutlich zwischen den beiden Begriffen zu unterscheiden, wird der Information Security Incident auch als solcher, beziehungsweise verkürzt als Security Incident, bezeichnet.

2.1.2. Begriffsabgrenzung Incident Handling - Incident Response - Security Incident Management

Incident Handling wird in ISO 27035-1:2023 als „actions of detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents*“ [9, Kap. 1.3.8] bezeichnet. Unter **Incident Response** sind laut der Norm aber „actions taken to mitigate or resolve an *information security incident* [...], including those taken to protect and restore the normal operational conditions of an information system and the information stored in it“ [9, Kap. 1.3.9] zu verstehen. Daraus lässt sich ableiten, dass Incident Response eigentlich nur ein kleiner Teil des gesamten Incident Handing ist, nämlich nur die Phase Response des im Standard angegebenen Prozesses. Die Phasen Plan and prepare, Detect and report, Assess and decide und Learn lessons sind offensichtlich nicht Bestandteil dieses Begriffes.

Diese Definition weicht jedoch stark vom alltäglichen Sprachgebrauch und anderen Definitionen ab, bei denen unter Incident Response oftmals eigentlich das gesamte Incident Handling gemeint ist. Auch die Webseiten einiger in Österreich tätiger Unternehmen, die laut Beschreibung ihres Services eindeutig Incident Handling gemäß ISO-Definition anbieten, sprechen in diesem Kontext von Incident Response [10], [11], [12]. NIST beschreibt im Computer Security Resource Center ebenso, dass Incident Response und Incident Handling synonym zu verstehen sind [13], [14]. In der vorliegenden Arbeit wird die Definition der ISO 27000 genutzt und so eine Unterscheidung zwischen Incident Handling und Incident Response geschaffen, auch wenn die für diese Arbeit verwendete Literatur diese Unterscheidung nicht immer vornimmt.

Unter **Security Incident Management**, zu deutsch Handhabung von Informationssicherheitsvorfällen, werden laut ISO 27000 die notwendigen Prozesse für die Aktivitäten des Incident Handlings verstanden [5,

Kap. 3.32]. Hier ist ebenso keine einheitliche Definition vorhanden. ISO 27035-1 beschreibt nämlich sehr viel allgemeiner „collaborative activities to handle information security incidents (3.1.5) in a consistent and effective way“ [9, Kap. 3.1.6]. Auch hier wird in der vorliegenden Arbeit aufgrund der Einheitlichkeit und der granulareren Unterscheidung die Definition der ISO 27000 genutzt.

2.1.3. Cyberrange

Eine Cyberrange wird von NIST als „safe environment (i.e., ‚sandbox‘) to deliver hands-on realistic training, scenarios, challenges, and excercises in an easy-to-access web-based environment“ [15] definiert.
Derartige Übungsumgebungen, in denen auch kritische Vorfälle ohne Einfluss auf Produktiv- oder Echtsysteme gefahrlos geübt werden können, existieren in der Luftfahrt stark vereinfacht bereits seit 1929. Der sogenannte Link-Trainer war ein einfaches, nachempfundenes Cockpit auf pneumatischen Balgen, die so Flugbewegungen simulieren konnten. Moderne Flugsimulatoren hingegen bilden Flugzeugcockpits penibel genau nach, bieten hochrealistische Grafiken und akkurate Physikmodelle, um kaum von einem echten Flug zu unterscheidende Erlebnisse zu bieten. [16]
Auch moderne Cyberranges bieten je nach Gestaltung und vorhandenen Ressourcen äußerst realistische Bedingungen für Blue oder Red Teams und eignen sich so zur Übung, bevor die Arbeit auf echten Systemen aufgenommen wird. Dabei können Netzwerke, Systeme, Tools oder Applikationen nachgestellt werden. NIST beschreibt in *The Cyber Range* weiters einige Use Cases und Zielgruppen für eine solche Cyberrange. Neben Bildungseinrichtungen, die ihren Lernenden Cybersecurity-Agenden allgemein näher bringen wollen, sind auch explizit das Training für „security operations, analysis and forensic specialists“ [17, S. 5] sowie „workforce training“ [17, S. 5] angegeben. [17, S. 5]
Cyberranges können aber nicht nur zu Bildungszwecken genutzt werden. Neben Wettbewerben und Zertifizierungen sind auch sogenannte *Test Cyberranges* für Forschung und Entwicklung übliche Einsatzbereiche. Mit Ausnahme von Entwicklungscyberranges sind an jeder Cyberrange neben Lernenden auch Instruktoren beteiligt. Die Instruktor:innen sind dabei neben der Überwachung der Lern- und Lösungsfortschritte insbesondere im Unterstützen der Lernenden gefragt, wenn diese auf Schwierigkeiten im Zuge des Bearbeitungsprozesses stoßen. [18, S. 4f.]
Zudem bieten Cyberranges operationelle Cybersecurityübungen, die so auch effektiv den wachsenden Fachkräftemangel im Cybersecuritybereich bekämpfen könnten. Yamin und Katt haben in ihrer Arbeit darüber hinaus den Erfahrungszugewinn der Teilnehmer:innen im Selbstevaluationsverfahren in einer technischen Übung gemessen, bei dem in einigen der erhobenen Kategorien ein Zuwachs von Fähigkeiten und Wissen nach bereits einer einzigen durchgeführten Übung beobachtet werden konnte. Bei einigen Items, die die

Einschätzung der eigenen Kompetenzen abbilden, haben sich die Teilnehmenden jedoch durchschnittlich schlechter beurteilt, weshalb davon ausgegangen werden kann, dass auch eine realistischere Selbsteinschätzung des eigenen Könnens einen positiven Nebeneffekt der Durchführung einer Cyberrange darstellt. [19, S. 20f.]

Die Einteilung von Cyberranges erfolgt in eine oder mehrere der drei folgenden Kategorien: **Simulation Cyberranges** nutzen vollständig virtualisierte Netzwerkumgebungen. Somit sind diese nicht nur gut skalierend und flexibel, sondern auch sehr kosteneffektiv. Virtuelle Maschinen werden beispielsweise, soweit möglich, mit einem identischen Image aufgesetzt, um den Erstellungsaufwand möglichst gering zu halten. **Overlay Cyberranges** hingegen nutzen physisches Netzwerkequipment und können so den Netzwerkverkehr realistischer darstellen, sind aber aufgrund ihrer Nicht-Virtualisierung weniger flexibel und aufgrund der Hardwarekosten meist auch teurer in der Umsetzung und im Betrieb. **Emulation Cyberranges** replizieren das wirklich existierende Netzwerk einer Organisation. Gerade deshalb sind sie meist wenig flexibel und teuer. Mischformen dieser drei Kategorien werden auch als **Hybrid Cyberrange** beschrieben. [17, S. 11f.], [18, S. 6]

Die Literatur zeigt aber nicht nur Vorteile von Cyberranges auf. Insbesondere der hohe Aufwand in der Vorbereitung, der bei Organisationen meist mit weiteren hohen Kosten verbunden ist, wird bei Katsantonis et al. beschrieben. Weiters wird auch der notwendige sogenannte Dry Run, also das Testen vor der tatsächlichen Nutzung, als nachteilig aufgeführt. Dieser muss von Expert:innen durchgeführt werden, um möglichst viele Fehler zu erkennen, und ist zeitaufwändig. In Lehrkontexten stellt außerdem die Beurteilung der Leistung der Lernenden ein Problem dar, da der Lösungsweg oftmals überhaupt nicht in die Beurteilung einfließt. [18, S. 8] Gerade dieser ist aber im Rahmen des analytischen Denkprozesses von Bedeutung. Je nach Lösungsweg können dabei unterschiedliche Ergebnisse erhalten werden.

Um den soeben beschriebenen Herausforderungen bei der Konzipierung von Cyberranges entgegenzuwirken, hat NIST in einem Versuch der Systematisierung ein sogenanntes Range Learning Management System definiert. Darin wird ein Basisset an Funktionen sowie der technische und organisatorische Aufbau einer Cyberrange beschrieben. Abbildung 2.1 liefert einen grafischen Überblick über die Systematik und zeigt neben den technischen Notwendigkeiten auch die Tasks in der Szenarioentwicklung auf.

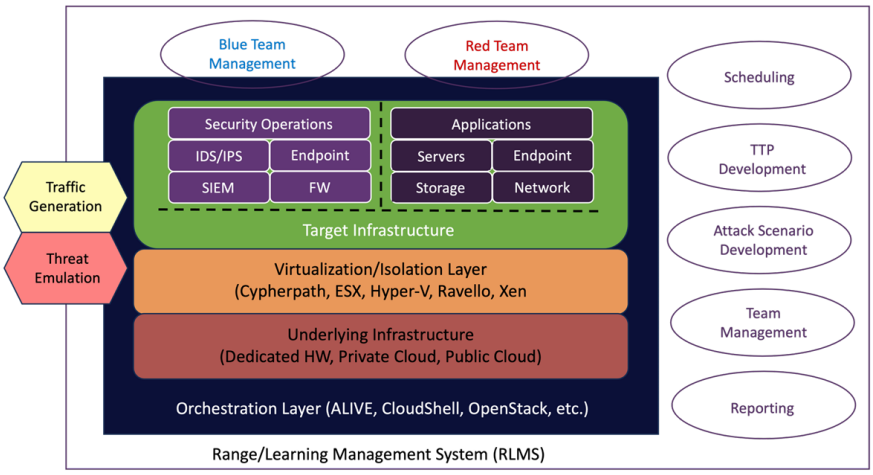

Abbildung 2.1.: Range Learning Management System [17, S. 6]

Der in der Grafik dargestellte **Orchestration Layer** dient als technische Basis für die Virtualisierung und Isolierung der Systeme. [17, S. 7] Er koordiniert alle untergeordneten und an späterer Stelle genauer beschriebenen Layer und verbindet sie zu einem Gesamtsystem. An der Fachhochschule St. Pölten wurden im Rahmen des Security Project I im Sommersemester 2024 mehrere Lösungen auf ihre Tauglichkeit evaluiert. Dabei wurde eine durch die Fachhochschule selbst betriebene OpenStack-Instanz als passende Lösung für das Projekt identifiziert. [20] Aufgrund der Parallelen in der Umsetzung wird daher auch für diese Arbeit das OpenStack-System der Fachhochschule verwendet.

Der Begriff **Underlying Infrastructure** bezeichnet die Infrastruktur, also Server, Netzwerkgeräte, Kabel und Speicherplatz, die für den Betrieb der Cyberrange notwendig ist. Neben der Nutzung physischer Hardware können hierfür auch Komponenten in die Cloud ausgelagert werden. [17, S. 7] In der Infrastruktur der Fachhochschule St. Pölten werden ausschließlich on-premise befindliche Ressourcen zum Betrieb genutzt. [20]

Der **Virtualization Layer** ist für die Virtualisierung und die Isolierung der einzelnen in der Übung befindlichen Systeme zuständig. [17, S. 7] Da die Infrastruktur der FH St. Pölten OpenStack als Orchestrierungslösung verwendet, werden OpenStack Nova als Hypervisor und OpenStack Zun als Plattform für die Erstellung von Containern genutzt. [20]

Als letzten Layer nennt NIST die **Target Infrastructure**. Diese ist nochmals in die in der Übung dargestellte Infrastruktur (beispielsweise Server, Endpoints, Netzwerk und Applikationen) und Security Operations (beispielsweise IDS/IPS, SIEM und Firewall) getrennt. [17, S. 7] Welche Systeme schlussendlich in der Abschlussübung zum Einsatz kommen, wird im Konzept unter 5.3 Konzeption der Cyberrange genauer erörtert.

Lifecycle

Katsantonis et al. beschreiben einen Cyberrange Lifecycle für die Entwicklung und Nutzung der Range, basierend auf dem PDCA-Cycle (Plan-Do-Check-Act) in den Phasen Analyse, Design, Configuration, Deployment, Dry Run und Execution. In der **Analysephase** sollen neben der Festlegung der Lernziele und -strategien auch die Lernenden selbst sowie deren Voraussetzungen und Background analysiert werden. In der zweiten Stufe, dem **Design**, soll die Cyberrange konzipiert werden. Dabei sollen die Erkenntnisse aus der Analyse Berücksichtigung finden. In dieser Phase werden neben dem Szenario und den im Spiel vorhandenen Maschinen und Computern, dem sogenannten *Cyberspace*, auch die sogenannten *Steps*, also die beabsichtigten Schritte, die der Lernende durchführen sollte, designt. Weiters sollen auch *Attribute* festgelegt werden, also beispielsweise der Name und eine Beschreibung der Cyberrange. Im dritten Schritt, der **Configuration**, wird der zuvor designte Cyberspace mittels Infrastructure as Code definiert und standardisiert konfiguriert. Anschließend wird im **Deployment**, dem vierten Schritt, die vorbereitete Cyberrange ausgerollt. Nach einem **Dry Run** als Schritt fünf folgt zuletzt die **Execution**, also die tatsächliche Durchführung der Cyberrange mit Teilnehmer:innen. [18]

2.1.4. NIST SP 800-181: NICE Framework

Mit der Special Publication 800-181, die aktuell in der Revision 1 aus November 2020 vorliegt, hat das National Institute of Standards and Technology ein „Workforce Framework“ [21, S. 11] geschaffen, mit dessen Hilfe Arbeit im Bereich Cybersecurity standardisiert beschrieben werden kann. [21, S. 11]

Dazu nutzt das Framework sogenannte Building Blocks in den drei Kategorien Tasks, Knowledge und Skills (kurz TKS). Ein Skill beschreibt eine Fähigkeit, wohingegen Knowledge notwendiges Wissen, um eine Aufgabe (einen Task) zu erfüllen, definiert. Building Blocks der Kategorie Tasks beschreiben dabei die Arbeit, die zu erledigen ist, während Knowledge und Skills gewissermaßen als Voraussetzungen für die korrekte Erfüllung eines Tasks bezeichnet werden können (siehe Abbildung 2.2). Die Komponenten Knowledge und Skills beschreiben daher, anders ausgedrückt, die Anforderungen an das IT-Personal, wobei zu berücksichtigen ist, dass Lernende diese Fähigkeiten und Fertigkeiten erst aufbauen müssen, um den Task erfolgreich erfüllen zu können. [21, S. 4] Obwohl das NICE Framework bereits einige Building Blocks für alle drei Kategorien bereitstellt, ist es auch vorgesehen, diese anzupassen oder, sofern es für die Organisation notwendig und zielführend ist, auch eigene Statements in einer oder allen Kategorien zu definieren. [21, S. 6]

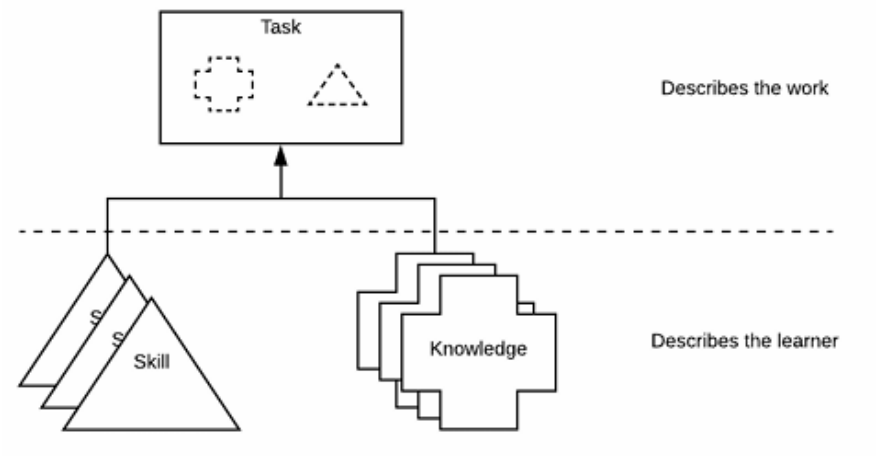

Abbildung 2.2.: Building Blocks [21, Fig. 1]

Jede der drei Kategorien kann durch sogenannte Statements beschrieben werden. In der Special Publication 181 wird auch für jeden Building Block festgelegt, wie dieser sprachlich möglichst verständlich zu formulieren ist. [21, S. 5]

Tasks

NIST versteht unter einem Task „an activity that is directed toward the achievement of organizatorial objectives“ [21, S. 4]. Ein standardisiertes Task-Statement muss einige Anforderungen erfüllen: Es muss einfach zu lesen und zu verstehen sein. Trotzdem ist es explizit gestattet, auch mehrere Schritte eines bestimmten Tasks in ein Statement aufzunehmen. Dies ist jedoch mit der gebotenen Vorsicht einzusetzen, da, um Einfachheit und Lesbarkeit nicht zu gefährden, das Aufnehmen mehrerer Aktivitäten in ein Task-Statement nicht gestattet ist. So ist beispielsweise „Identify, classify, or document organizatorial data elements in physical or digital form“ [22, S. 4] kein gültiges Task-Statement, da dieses mehrere Aktivitäten, nämlich das Identifizieren, Klassifizieren und Dokumentieren, in ein Statement zusammenfasst und so unnötig verkompliziert. [21, S. 4], [22, S. 4]

Weiters muss ein Task-Statement immer mit der Aktivität beginnen. Das bedeutet, dass das die Aktivität beschreibende Verb an erster Stelle im Task-Statement stehen sollte. Die Nutzung von Verben wie „sicherstellen“ sollte dabei vermieden werden, da dies Unklarheit über die Notwendigkeit, die Aufgabe tatsächlich auszuführen, hervorrufen könnte; es bleibt also unklar, ob die Ausführung der Aufgabe nur kontrolliert oder selbst durchgeführt werden soll. Gemäß des Standards müssen Task-Statements daher beispielhaft wie folgt aufgebaut sein: *Analysieren von Alarmen aus einem SIEM-System* oder *Isolieren von betroffenen Systemen*. Ein Negativbeispiel wäre *Sicherstellen, dass die Alarme aus einem SIEM-System analysiert werden*. [21, S.

4], [22, S. 3]

Task-Statements sollen möglichst universell einsetzbar und in verschiedenen Tätigkeitsfeldern nutzbar sein. Darum ist eines der Nicht-Ziele eines Task-Statements die Nennung des Task-Ziels, das mit diesem Task verfolgt werden soll, also der Angabe, warum der Task eigentlich durchgeführt wird. Der bereits vorher genannte Task *Analysieren von Alarmen aus einem SIEM-System* soll daher nicht auf *Analysieren von Alarmen aus einem SIEM-System, um mögliche Angriffe zu erkennen* erweitert werden, um die Task-Beschreibung beispielsweise auch im SOC-Engineering, also dem Entwickeln von Use Cases für SIEM-Systeme, nutzen zu können, da das korrekte Task-Statement mit angegebenem Ziel hier wohl *Analysieren von Alarmen aus einem SIEM-System, um die Funktionsweise von Use Cases beurteilen zu können* heißen müsste. [21, S. 4]

Knowledge

Knowledge ist „a retrievable set of concepts within memory [des Lernenden oder Arbeitenden, Anm. d. Verf.]“ [21, S. 5] und kann neben Konzepten im engeren Sinne auch Grundlagenwissen definieren. Knowledge steht dabei in einer n:n-Beziehung zu Tasks. Ein Knowledge-Statement kann also als Voraussetzung zur ordnungsgemäßen Erfüllung einer Aufgabe einem oder mehreren Tasks zugeordnet werden. Genauso kann ein Task ein oder mehrere Knowledge-Statements als Voraussetzung definieren.

Knowledge-Statements beginnen immer mit „Wissen über“ [22, S. 5, eigene Übersetzung], um sie klar als solche zu kennzeichnen, und dürfen, um die Lesbarkeit und Einfachheit zu wahren, pro Statement immer nur ein Konzept beschreiben.

NIST lässt hier die geforderte Genauigkeit der Definition offen. So führt es etwa sowohl das Knowledge-Statement „Knowledge of cyberspace threats and vulnerabilities“ [21, S. 5] als auch das Statement „Knowledge of vulnerability information dissemination sources (e.g., vendor alerts, government advisories, product literature errata, and sector bulletins.)“ [21, S. 5] als gültige Beispiele an. Darüber hinaus empfiehlt NIST das Wissen, beispielsweise mit der in 2.3.3 Bloom'sche Taxonomie beschriebenen Bloom'schen Taxonomie, einem Level zuzuordnen, um so die Tiefe beziehungsweise den vorausgesetzten Detailgrad des Wissens darzustellen. [21, S. 5]

Skills

Ein Skill ist „the capability to perform an observable action“ [21, S. 5] und kann, ähnlich wie Knowledge-Statements, unterschiedlich komplex ausgeführt sein. So ist sowohl das Skill-Statement „Skill in recognizing the alerts of an Intrusion Detection System“ [21, S. 5], als auch das Statement „Skill in generating a hypothesis as to how a threat actor circumvented the Intrusion Detection System“ [21, S. 5] gültig.

Skill-Statements müssen mit der Phrase „Fähigkeit, [*etwas zu tun*, Anm. d. Verf.]“ [22, S. 5, eigene Übersetzung] beginnen und ein Verb enthalten. Ein als falsch bezeichnetes Skill-Statement im TKS-Authoring Guide ist „Skill in test and evaluation reports“ [22, S. 6], da der eigentlich verlangte Skill unklar sei und verschiedene Skills gemeint sein könnten, beispielsweise das Erstellen oder das Korrekturlesen. Fehlt der Präfix „Fähigkeit, [*etwas zu tun*, Anm. d. Verf.]“ [22, S. 6, eigene Übersetzung], so könnte das Skill-Statement mit einem Task-Statement verwechselt werden. [22, S. 6]

Weiters müssen Skill-Statements, gemäß der vorangegangenen Definition eines Skills, eine beobachtbare Handlung enthalten. So ist beispielsweise „Skill in applying security controls“ [22, S. 6] ein gültiges Skill-Statement, während „Skill in structured analysis principles and methods“ [22, S. 7] eigentlich eher als Knowledge-Statement gelten würde. [22, S. 6f.]

Abermals ist ein Skill eine zwingende Voraussetzung zur erfolgreichen Erfüllung eines Tasks und steht ebenso, wie bei Knowledge in 2.1.4 Knowledge beschrieben, in einer n:n-Beziehung zu Tasks.

Competencies und Work Roles

Überdies hinaus existieren in der Special Publication noch Competencies und Work Roles, die auf den TKS-Statements basierend Anforderungsgruppen an einzelne Mitarbeiter:innen sowie das gesamte Team explizieren.

Kompetenzen (Competencies) beschreiben „a mechanism for organizations to assess learners“ [21, S. 7]. Diese Statements bestehen aus einem Namen und einer Beschreibung inklusive Assessment-Methode und dazugehörigen TKS-Statements. Der Einsatz dieser Kompetenz-Statements ist vielfältig und kann beispielsweise im Recruiting-Prozess dazu genutzt werden, die Bewerber:innen auf ihre Tauglichkeit für eine ausgeschriebene Stelle zu testen. Mehrere Kompetenzen könnten so eine Stellenbeschreibung ergeben. Der Fokus von Kompetenzen im Sinne des NICE Frameworks liegt also in der Ermittlung, ob bestimmte benötigte Skills und Knowledge bei einer Person vorhanden sind oder nicht. [21, S. 7f.]

Davon zu unterscheiden sind **Work Roles**. Diese sind „a way of describing a grouping of work for which someone [also eine Person oder Gruppe, Anm. d. Verf.] is responsible or accountable“ [21, S. 11]. Der Fokus liegt hauptsächlich auf den zu erledigenden Tasks, wobei Work Roles eine den Tasks übergeordnete Gruppe darstellen und die Rollen der Belegschaft beschreiben. Sie dürfen aber nicht mit Berufstiteln gleichgesetzt werden. So kann die Work Role Software Developer beispielsweise in den Jobtiteln Software Engineer oder Application Developer gültig sein. [21, S. 11f.]

Die SP 800-181 zeigt sich im Aufbau von Teams abermals flexibel und erwähnt, dass dieser sowohl mit der Definition von Work Roles als auch mit der Definition von Kompetenzen erfolgen kann. So wird beispiels-

weise erklärt, dass ein Cybersecurity Team unter anderem aus den Work Roles Security Controls Assessor, Cyber Defense Analyst und Cyber Defense Incident Responder bestehen kann. Alternativ kann ein Red Team unter anderem aus den Kompetenzen Engangement Planning, Pen Testing und Vulnerability Exploitation bestehen. [21, S. 12ff.]

2.2. Standards und Normen

Die Internationale Organisation für Normung (ISO) entwickelt durch die Zusammenarbeit unterschiedlichster Experten mit theoretischer und praktischer Expertise Standards, die den Anspruch haben, den besten Weg, um etwas zu tun, abzubilden. [23], [24] Dazu werden unterschiedliche Vorschläge und Good Practices als Draft gesammelt und konsolidiert. Darauf folgt eine Phase, in der die Änderungen kommentiert werden können. Abschließend folgt ein Abstimmungsprozess, bei dessen positivem Ausgang der Draft zu einem Standard wird. [25] Die Nutzung von Standards hat oftmals auch Compliancegründe. [26, S. 92] Die von manchen Gesetzen wie der NIS 2-Verordnung der Europäischen Union vorgeschriebene Nutzung des Standes der Technik kann durch Compliance mit diesen Standards meist erfüllt werden. [27, Art. 21], [26, S. 92]

Im Cybersecurity-Bereich kann die ISO 27000-Normenreihe für Informationssicherheits-Managementsysteme (ISMS) als de-facto Industriestandard angenommen werden. In über einem Dutzend Standards versucht die ISO so Ansätze zu vermitteln, um verschiedene Assets vor vielfältigen Cyberbedrohungen zu schützen. [28]

Incident Handling wird dabei in den vier Teilen der ISO 27035 näher beschrieben (siehe 2.2.1 ISO 27035). In der Einleitung des ersten Teils wird die Intention und Bedeutung des Standards als „guidance“ [9, S. V], also als Führung oder Hilfestellung für das Incident Handling, genannt. Der vorliegende Standard sei deswegen kein Leitfaden, sondern lediglich eine Referenz auf wichtige Prinzipien in Information Security Incidents. Der abgebildete Prozess solle auch dazu dienen, die passenden Methoden und Tools einzusetzen. [9, S. V] Darüber hinaus ist im Scope beschrieben, dass der genannte Prozess generisch und für Organisationen aller Größe gedacht sei und deshalb angepasst werden müsse. [9, Kap. 1] NIST Special Publication 800-61 beschreibt im Kapitel Purpose und Scope ebenfalls, dass die Publikation keinesfalls beschreiben könne, wie Incident Handling-Aktivitäten durchzuführen wären, da sich dies zu regelmäßig ändere. [6, Kap. 1.1] Beide Werke möchten also als Handlungsrahmen, von dem in begründeten Fällen abgewichen werden darf, verstanden werden.

2.2.1. ISO 27035

Die ISO 27035-Serie widmet sich dem Incident Handling und führt die in ISO 27002 genannten Controls zu diesem Thema weiter aus. Die Reihe besteht aktuell aus vier Teilen, die jeweils durch eine fortlaufende Zahl von eins bis vier am Ende der Normenbezeichnung gekennzeichnet werden. [9, S. V] Der erste Teil (ISO 27035-1:2023, „Principles and process“) bildet die Basis der gesamten 27035-Serie. Darin werden neben einem grundlegenden Incident Handling-Prozess auch Basiskonzepte erklärt. [9, Kap. 1] Der darauf aufbauende zweite Teil (ISO 27035-2:2023, „Guidelines to plan and prepare for incident response“) behandelt die erste und letzte Phase, also die Vorbereitung auf und die Nachbereitung beziehungsweise die Verbesserung („Lessons learned“) von Security Incidents. [29, Kap. 1] Daran anschließend beschäftigt sich der dritte Teil (ISO27035-3:2020, „Guidelines for ICT incident response operations“) mit den noch nicht in Teil 2 behandelten Phasen und Tätigkeiten, also „Detection and reporting“, „Assessment und decision“ und „Responses“. [30, Kap. 1] Der letzte Teil (ISO 27035-4:2024, „Coordination“) beschreibt die organisationsübergreifende Kommunikation und Koordination bei Security Incidents, die mehrere Organisationen betreffen. [31, Kap. 1]

2.2.2. NIST SP 800-61

Die Special Publication 800-61 („Incident Response Recommendations and Considerations for Cybersecurity Risk Management“) des National Institute of Standards and Technology beschreibt neben Hilfestellungen zum Themenbereich Incident Handling auch Cybersecurityrisikomanagement. [6, S. i]

Veraltetes Lifecyclemodell (R2)

In der Revision 3, veröffentlicht im April 2025, wurde der bisher bekannte, einfache Prozess (siehe Abbildung 2.3) mit den vier Prozessschritten Preparation - Detection & Analysis - Containment, Eradication & Recovery - Post-Incident-Activity – NIST nennt diesen Prozess Lifecycle – durch einen anderen, komplexeren Ablauf ersetzt. NIST begründet das mit der steigenden Anzahl von Sicherheitsvorfällen und immer höheren Schäden. Durch die erhöhte Komplexität der Vorfälle sei es beispielsweise auch notwendig, Verbesserungsvorschläge im Rahmen von Lessons Learned sofort nach Erkennen und nicht erst nach Abschluss des Security Incidents einzubringen und zu bearbeiten und somit kontinuierliche Verbesserung auch innerhalb eines aktiven Security Incidents zu erreichen. [6, Kap. 2.1]

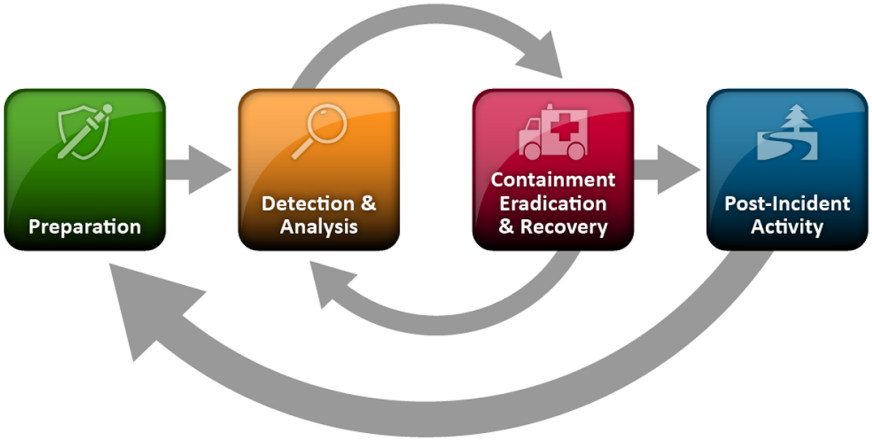

Abbildung 2.3.: Veraltetes Incident Response Lifecyclemodell nach NIST [6, S. 4]

NIST Cybersecurity Framework 2.0

Seit April 2025 basiert der NIST Incident Response Lifecycle auf den sogenannten Funktionen des NIST Cybersecurity Frameworks 2.0 (kurz CSF 2.0). Das Framework beschreibt in diesen Funktionen die positiven Auswirkungen verschiedener Cybersecuritymaßnahmen auf Organisationen. In der Funktion **Identify** werden dabei alle Controls zusammengefasst, um die derzeitigen Cybersecurityrisiken zu verstehen. Neben der Identifikation aller Assets ist hier beispielsweise auch die Identifikation von Verbesserungsmöglichkeiten verortet. In der Funktion **Protect** sollen anschließend die zuvor identifizierten Assets vor Risiken geschützt werden. Dazu zählen beispielsweise Maßnahmen im Bereich Awareness, Zugriffskontrolle oder Identity Management. Die Funktion **Detect** beschreibt Controls, die dazu führen, dass mögliche Angriffe und Kompromittierungen erkannt und analysiert werden und stellt eine wichtige Supportfunktion für das folgende Incident Handling dar. In der Funktion **Respond** werden darauf aufbauend die notwendigen Maßnahmen getroffen, um die Auswirkungen des Security Incidents zu analysieren, zu mitigieren und die entsprechenden Berichte zu verfassen sowie Kommunikationsmaßnahmen zu treffen. Abschließend werden in der Funktion **Recover** alle Assets, die durch den Sicherheitsvorfall beeinträchtigt waren, raschestmöglich wieder in den Normalbetrieb gebracht. Die Funktion **Govern** zieht sich dabei über alle anderen Phasen und stellt die notwendige ständige Governance und Steuerung dar. [32, S. 3f.]

Bei genauerer Betrachtung erkennt man, dass die im Cybersecurity-Framework modellierten Maßnahmen in den Phasen Govern, Identify und Protect „left of boom“, also vor dem Sicherheitsvorfall wirken sollen, während die Phasen Detect, Respond und Recover „right of boom“, also nach dem Sicherheitsvorfall ihre Wirkung entfalten. [32, S. 3f.], [6, S. 5]

Neues Lifecyclemodell (R3)

Im neuen Lifecyclemodell, das auf dem Cybersecurity Framework 2.0 basiert, lassen sich viele Parallelen zu eben diesem erkennen.

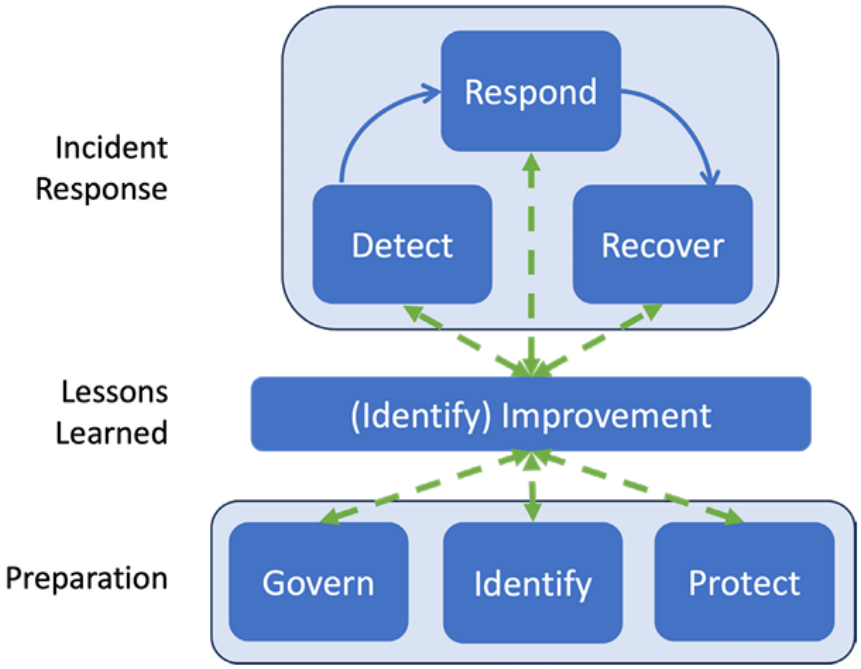

Abbildung 2.4.: Neuer NIST Incident Response Lifecycle auf Basis des CSF 2.0 [6, S. 13]

Die Basis des Modells bilden alle der Preparation zuzuordnenden Aktivitäten. NIST zeigt damit, dass in ihrem Modell die Phasen Govern, Identify und Protect nicht zu Incident Handling gehören, sondern Risikomanagementmaßnahmen darstellen, die wiederum Incident Handling unterstützen [6, S. 5f.] und Security Incidents proaktiv verhindern können. Der Bereich Incident Response, der in dieser Arbeit aufgrund der Definitionsunterschiede eigentlich Incident Handling beschreibt, besteht aus den drei Funktionen Detect, Respond und Recover. Das Zentrum des Prozesses bildet der Bereich Lessons Learned mit der Subfunktion Improvement, die wiederum der Funktion Identify zuzuordnen ist. Die wechselseitigen grünen Pfeile aus und zu jeder anderen Funktion sollen dabei andeuten, dass es kontinuierliche Verbesserung braucht und diese Lessons Learned, im Gegensatz zum Prozessmodell der ISO 27035, jederzeit und nicht nur am Ende eines Sicherheitsvorfalles gelernt werden müssen. [6, S. 5f.], [29, Kap. 12.1]

Das Herzstück der Special Publication ist eine Tabelle. Für jede der Phasen im neuen Lifecyclemodell beschreibt die SP anschließend mit einer für das Incident Handling fesetgelegten Priorität die einzelnen, in der jeweiligen Phase zu setzenden Aktivitäten aus dem NIST Cybersecurity Framework 2.0. Einzelne Maßnahmen werden zusätzlich noch mit einem Kommentar der Stufen Recommendation, also etwas, das

die Organisation tun sollte, Consideration, also etwas, das die Organisation zumindest überlegen sollte, und Note, also weitere Informationen zur jeweiligen Control, versehen. Hier zeigt sich wieder die nun auch im Lifecycle abgebildete starke Vernetzung der neuen Revision der Special Publication mit dem NIST CSF 2.0. [6, S. 11-35]

Neben dem Lifecycle beschreibt NIST SP 800-61 weiters verschiedene Rollen und Verantwortlichkeiten, bei denen neben Aufgaben der Leitung auch explizit das Hinzuziehen von externen Partnern oder einem hybriden Modell die Rede ist, um wirkungsvolles und situationsangepasstes Incident Handling zu ermöglichen. NIST nennt die damit verbundene Teilung der Verantwortlichkeiten auch, wie aus der Cloud bekannt, Shared Responsiblity Model. [6, S. 8], [33]

2.2.3. CIS Controls

Die CIS Controls, gewartet und herausgegeben vom Center for Internet Security (kurz CIS), stellen zwar keinen Standard und keine Norm im engeren Sinne dar, werden aber durch das CIS selbst als Teil der Security Best Practices, neben den CIS Benchmarks (für sichere Konfigurationsbaselines), beschrieben und sind „a prescriptive, prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and in alignment with all industry or government security requirements.“ [34, S. 2] Ein wesentlicher Vorteil der CIS-Controls ist ihre Anfängerfreundlichkeit. [34, S. 4] Eine einfache grafische Aufmachung und Sortierung nach großen Themenbereichen sollen so insbesondere Organisationen ohne oder mit wenig IT Security-Personal einen organisatorischen und technischen Grundschutz bieten.

Die CIS Controls bieten eine einfache Guideline aus 18 Kategorien, die Controls genannt werden. Als Beispiel dafür sei die erste Control „Inventory and Control of Enterprise Assets“ [34, S. 9] genannt. Jeder Control sind mehrere Safeguards zugewiesen. Ein Safeguard ist eine Maßnahme mit einem weiterführenden englischen Erklärungstext, beispielsweise „1.2 - Address Unauthorized Assets“ [34, S. 11], „Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.“ [34, S. 11] Jede Maßnahme ist zu Priorisierungszwecken einer Implementation Group von eins bis drei zugeordnet, wobei eins eine „Basic Cyber Hygiene“ [34, S. 5] beschreibt. Die anderen beiden Implementation Groups bauen dann mit erweiterten Maßnahmen darauf auf. [34, S. 5]

2.3. Hochschulbildung und Didaktik

Da der Aufbau von Fähigkeiten im Bereich des Incident Handlings zentral für Absolvent:innen eines Hochschullehrganges im Information Security-Sektor ist, sollen die wichtigsten Inhalte an der Fachhochschule St. Pölten gelehrt werden. Um die Lehrveranstaltung nach den aktuellen pädagogisch-didaktischen Anforderungen aufzubauen, werden im Folgenden die Grundlagen des (fach-)didaktischen Lehrens erläutert.

2.3.1. Didaktische Rekonstruktion

Die Entwicklung des Konzeptes für die Lehrveranstaltung basiert auf der von Kattmann et al. entwickelten und beschriebenen didaktischen Rekonstruktion, deren Ablauf schematisch in Abbildung 2.5 dargestellt ist. Diese geht davon aus, dass fachliche Inhalte unter der Berücksichtigung des Vorwissens und der Präkonzepte, also Vorstellungen, die wissenschaftlich nicht zureichend sind, der Lernenden so aufbereitet werden müssen, dass sie verstanden und gelernt werden können. [35, S. 3], [36, S. 405]

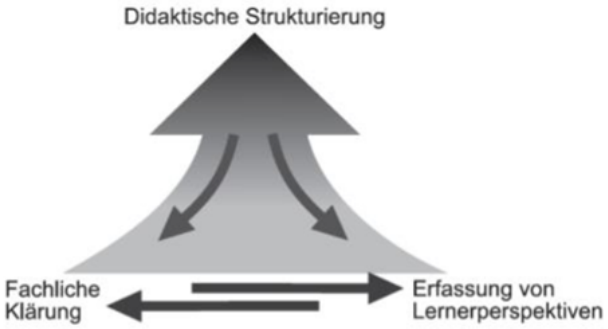

Abbildung 2.5.: Modell der didaktischen Rekonstruktion [37, S. 168]

In einem ersten Schritt wird daher im Zuge der fachlichen Klärung das wissenschaftliche Konzept erhoben. Zu diesem gehören alle in der Fachwissenschaft enthaltenen Erkenntnisse, Methoden, Theorien und Termini. Die dahinterstehenden Strukturen sollen in einem weiteren Schritt elementarisiert, also kleinteilig zerlegt und systematisiert, werden [35, S. 3-9], wodurch die zentralen Grundideen identifiziert werden. [38, S. 2ff.] Die Struktur des Fachhochschulunterrichts ergibt sich in weiterer Folge aus der Zusammenführung dieser wissenschaftlichen Struktur mit der Perspektive der Lernenden. [35, S. 4]
Aufgrund der Anforderung, den Unterricht der Lernendengruppe anzupassen, ist anschließend eine Einbettung der Inhalte „in umweltliche, gesellschaftliche und individuale Zusammenhänge“ [35, S. 3] notwendig, um die Bedeutsamkeit mit der Beschäftigung des Themas zu explizieren [35, S. 3] und so die motivationalen Ressourcen der Lernenden für die Auseinandersetzung mit den Lehrinhalten bereitzustellen. Darüber hinaus

müssen die Vorkenntnisse und Vorstellungen, Fähigkeiten sowie Interessen der Lernenden erhoben werden, wobei auch sprachliche und kognitive Voraussetzungen bedacht werden müssen. [39, S. 95f.] Zur Unterstützung können hierfür die Fragen der didaktischen Analyse nach Klafki herangezogen werden. [40, S. 5-34] Zudem müssen, folgt man konstruktivistischen Lerntheorien, den Lernenden Anknüpfungspunkte an bestehendes Wissen und vorhandene Kompetenzen geboten werden, um die neu zu erwerbenden Fähigkeiten und Fertigkeiten anschlussfähig zu machen, sodass die neuen Inhalte mit vorhandenen Wissensbeständen verknüpft werden können. [41, S. 80] Diese Verknüpfung kann wiederum nur dann vollzogen werden, wenn eine entsprechende Einbettung in die beschriebenen Zusammenhänge vorgenommen wurde. [36, S. 405]
Daraus ergibt sich, dass wissenschaftliche Konzepte um fachdidaktische Schwerpunktsetzungen angereichert werden müssen, wodurch sie komplexer werden als die ihnen zugrundeliegende Theorie. Gleichzeitig bedeutet dies für die Lehrenden, dass eine bloße Kürzung und Vereinfachung der wissenschaftlichen Konzepte und Praktiken nicht ausreichen, um die Inhalte zielführend unterrichten zu können. [35, S. 3f.] Es müssen stattdessen Lernwege von dem Vorwissen hin zu dem Aufbau neuer Kompetenzen geplant werden, wobei auch den Inhalten angemessene Methoden und Medien gewählt werden, die den Unterricht unterstützen. [38, S. 1] Im Zuge dieses Planungsprozesses werden auch die Unterrichtsziele festgelegt, die wiederum wechselseitig die Inhalte, Methoden und Medien bedingen. [39, S. 96f.]

2.3.2. Curriculare Vorgaben an der Fachhochschule St. Pölten

An der Fachhochschule St. Pölten befindet sich die Lehrveranstaltung *Incident Response* im Studiengang MIS Information Security im Modul *Incident Management and Security Analysis I* und wird im ersten Semester durchgeführt. [42]
Als Lernergebnisse, die mit den Lernzielen (siehe 2.3.3 Lernziele) gleichzusetzen sind, sind angegeben:

> Die Studierenden kennen den Incident Response Prozess und können aktiv an einem Incident Response Case technisch mitarbeiten. (L3)
>
> Die Studierenden können einen Incident Reponse [sic!] Case führen und unterschiedliche Teilnehmer und Stakeholder managen. (Timelines) (L3)
>
> Die Studierenden sind in der Lage ein kompromittiertes Einzelsystem auf wichtige Artefakte hin zu untersuchen (L4)
>
> Die Studierenden können in einem Enterprise Environment die Bewegung eines Angreifers nachvollziehen, eingrenzen und diesen am Ende der Investigation aus dem System entfernen (Remediation). (L5) [42]

Folgende Lehrinhalte, die zur Erreichung dieser Ziele führen sollen, werden in der LV-Beschreibung aufgelistet:

> In der Lehrveranstaltung wird den Studierenden anhand des Incident Repsonse [sic!] Prozesses (Preparation, Detection, Analysis, Remediation) das Handwerk der erfolgreichen Abhandlung eines Incident Response Verfahrens auf technischer und organisatorischer Ebene beigebracht.
>
> Dabei wird ein erstes Verständnis für die Themen Threat Landscape und Attacker Lifecycle vermittelt.
>
> Nach der Vermittlung der einzelnen Phasen innerhalb des Gesamtprozesses, lernen die Studierenden, wie von einem Einzelsystem wichtige Artefakte gewonnen werden können, wo diese zu finden sind und wie diese aus dem System extrahiert werden können.
>
> Nach der erfolgreichen Investigation eines Einzelsystems lernen die Studierenden die Analysemethoden, um die Bewegung eines Angreifers innerhalb eines Enterprise Networks nachvollziehen zu können.
>
> Neben der technischen Ausbildung erfahren die Studierenden wie diese einen Incident Response Case führen (Timelines) und unterschiedliche Stakeholder miteinander verbinden.
>
> Nach erfolgreicher Analyse bekommen die Studierenden einen Einblick in die Methodik einen Angreifer erfolgreich aus dem Netzwerk zu entfernen. (Remediation)
>
> Den Abschluss bildet die Herangehensweise, wie am Ende eines Incident Response Verfahrens überprüft werden kann, ob sich noch Spuren des Angreifers im System befinden (Threat Hunting) [42]

2.3.3. Lernziele

Die Didaktik unterscheidet die Begriffe Lehr- und Lernziele, wobei bei ersteren auf die Perspektive der Lehrenden und bei zweiteren auf die Perspektive der Lernenden fokussiert wird. Da nach konstruktivistischer Auffassung davon ausgegangen werden muss, dass nicht alles, was gelehrt wurde, von den Lernenden auch aufgenommen und gelernt wurde, ist eine Unterscheidung dieser Begriffe fundamental. [43, S. 3], [44, S. 162, 167f.] Für die vorliegende Arbeit wird im Sinne einer lernendenzentrierten Lehrveranstaltungsplanung der Blick auf die Perspektive der Studierenden gerichtet. Zudem kann im Rahmen der Hochschulbildung von stärker individuell gesteuerten Lernprozessen ausgegangen werden. Deswegen soll im Weiteren die Rede von Lernzielen sein, wobei für die angestrebte Lehrveranstaltungsplanung auch Lernziele formuliert werden sollen.

Dass es wichtig ist, Lernziele zu verschriftlichen, zeigt sich insbesondere in der Notwendigkeit, diese den Studierenden transparent zu machen, damit diese als Verantwortliche für ihren Lernprozess selbst die Lernziele verfolgen können. [45, S. 1] Zudem beeinflusst die Kommunikation von Lernzielen den Lernprozess positiv, da die Selbst- und Fremdeinschätzung anhand der angelegten Kriterien und Zielvorgaben erleichtert

werden. [43, S. 4] Darüber hinaus stellen Lernziele auf operationalisierte, messbare Art den Soll-Zustand nach dem Durchlaufen eines Lernprozesses dar und bilden so dessen Ziel ab. Sie geben an, welches Wissen und welche Kompetenzen die Lernenden am Ende des Lernprozesses erworben haben sollen und bieten so auch eine Verknüpfung zur Leistungsfeststellung. Da auch Vergleiche des angestrebten Ziels mit dem tatsächlichen Outcome des Unterrichts angestellt werden können, kann somit anhand der Lernziele auch die Wirksamkeit des Unterrichts gemessen [45, S. 4], [44, S. 162] und so Planlosigkeit und Ineffizienz vermieden werden. [46, S. 14]

Lernziele sind hierbei normativ und allen weiteren Entscheidungen übergeordnet, weswegen sie im Unterrichtsvorbereitungsprozess erstgelagert sein müssen. Dabei ist zu bedenken, dass die Inhalte, Methoden und Medien der Unterrichtssequenz zieladäquat zu wählen sind. [45, S. 1], [44, S. 162] Sturm beschreibt dafür auch den Zusammenhang mit den curricularen Vorgaben und der Leistungsfeststellung: „Bereits während der Veranstaltungsplanung sollte die Formulierung von Lernzielen im Einklang mit den im Modulhandbuch festgelegten Lernzielen erfolgen, damit eine gezielte Abstimmung der Lehr-Lern-Methoden und Prüfungen erfolgt.“ [43, S. 4]

Dabei lassen sich Lernziele nach der Hierarchie der Ziele, dem Fachbezug, dem Lernbereich und den Lehrzielstufen systematisieren. Ja nachdem, ob Lernziele für einen gesamten Studiengang, für ganze Module oder Lehrveranstaltungen oder einzelne Sequenzen formuliert wurden, spricht man von Richt-, Grob oder Feinzielen. [44, S. 163f.] Bezieht sich das Lernziel des Weiteren ausschließlich auf das Fach, wird von einem fachlichen Lernziel gesprochen. Von diesem unterschieden werden allgemeine Lernziele, die fachübergreifendes Wissen und Kompetenzen betreffen. Der Lernbereich findet im Lernziel dabei insofern Berücksichtigung, als dass kognitive, affektive und psychomotorische Lernziele je nach Inhalt beziehungsweise Lerngegenstand unterschieden werden können. [44, S. 165f.] Darüberhinausgehend benötigt es Lernzielstufen, um kompetenzorientiertes und vielseitiges Lernen zu ermöglichen. Sie geben an, auf welchem Niveau die geforderten Fähigkeiten und Fertigkeiten beherrscht werden müssen. Diese Ebenen bauen aufeinander auf, weswegen eine Systematisierung der Lernziele von einfach zu schwierig fundamental ist. [44, S. 166f.], [45, S. 5f.] Eine Taxonomie, die diese Ebenen differenziert, jene nach Bloom, wird aufgrund ihrer Relevanz am Department im Anschluss näher erläutert (siehe 2.3.3 Bloom’sche Taxonomie).

Für die Formulierung von Lernzielen ist dabei zu beachten, dass Lernziele nur ein Verb, das wiederum einer Ebene der Lernzieltaxonomie nach Bloom zugeordnet werden kann und somit den Anforderungsgrad ausdrückt, enthalten. Die Lernziele sollen dabei, wie bereits angesprochen, messbar sein. Durch Beobachtung soll also bewertet werden können, inwiefern das angestrebte Lernziel erreicht wurde. Zu diesem Aspekt gehört auch eine Terminierung, um festzulegen, bis wann die Fähigkeiten und Fertigkeiten aufgebaut werden

sollen. [45, S. 7f.] Die hierfür zentralen Kriterien können unter anderem mit dem Akronym SMART abgebildet werden. Lernziele sollen demnach spezifisch, messbar, attraktiv, realistisch und terminiert formuliert werden. [46, S. 15-20]

Bloom'sche Taxonomie

„Die Lernzieltaxonomie nach Bloom [...] ermöglicht eine gute Orientierung zur Staffelung auf Aufgabenstellungen nach dem Schwierigkeitsgrad [...]" [47, S. 19] Auch an der Fachhochschule St. Pölten wird dieses Lernzieltaxonomiemodell genutzt und die geforderte Lernzielstufe für jedes Lernziel festgehalten (Kennzeichnung mit Lx, x = [1,6]). [42]
Die Bloom'sche Lernzieltaxonomie kennt im kognitiven Bereich sechs Stufen mit aufsteigender Komplexität:

Abbildung 2.6.: Bloom'sche Taxonomie: Darstellung in Pyramidenform [48, S. 1]

Wissen: Unter Wissen versteht man das Erinnern können an Begriffe und Terminologie, Kriterien, Fakten, konkreten Einzelheiten oder Abläufe. Mögliche Operatoren in der Aufgabenstellung für diese Lernzielstufe sind beispielsweise aufzählen, nennen oder wiedergeben. Eine in der Literatur beschriebene Schwierigkeit bei der Überprüfung dieser Stufe ist das gezielte Setzen von Hinweisen, Zeichen und Schlüsseln, um das geforderte Wissen zutage zu bringen. [47, S. 19], [48, S. 1]

Verstehen: Verstehen „stellt die niedrigste Ebene des Begreifens dar" [48, S. 3] und beinhaltet insbesondere das Erklären eines Sachverhaltes mit eigenen Worten. Mögliche Aufgaben beinhalten die Translation, also

die Übersetzung in eigene Worte, die Interpretation, bei der auch vom Material ausgehende weiterführende Gedanken enthalten sein dürfen oder die Extrapolation, also die Anwendung auf andere Datensätze oder Regelwerke. Es ist in dieser Stufe aber nicht notwendig, das Wissen „mit anderem Material in Bezug zu setzen oder seine umfassendste Bedeutung zu erkennen“ [48, S. 3f.]. Mögliche Operatoren dieser Ebene sind beschreiben, erklären oder interpretieren. [47, S. 19], [48, S. 1]

Anwendung: Unter der Anwendung versteht man den „Gebrauch von Abstraktionen in besonderen und konkreten Situationen“ [48, S. 4]. Das Erlernte muss also in einen anderen Zusammenhang gesetzt werden. Anwenden oder lösen sind mögliche Operatoren. [47, S. 19], [48, S. 4]

Analyse: Die Analyse zielt darauf ab, Kriterien zu ermitteln, Besonderes aufzuzeigen und Fehler festzustellen. Einzelne Aspekte werden systematisiert und zueinander in Beziehung gesetzt. Dadurch kann beispielsweise auch die Folgerichtigkeit einer Annahme überprüft werden. Als mögliche Operatoren kommen analysieren oder ableiten in Frage. [47, S. 19], [48, S. 4]

Synthese: Bei der Synthese werden einzelne Teile zu einem übergeordneten Konzept bzw. Gesamtbild zusammengefügt und so beispielsweise Pläne für eine Handung entworfen oder „Wege für die Überprüfung von Hypothesen“ [48, S. 5] vorgeschlagen. Entwickeln, verfassen oder konstruieren sind mögliche Operatoren für diese Stufe. [47, S. 19], [48, S. 5]

Evaluation: In der letzten Stufe wird das Abwägen von Alternativen oder die Beurteilung eines Sachverhaltes gefordert. Dabei können auch die Kriterien der Bewertung durch die Lernenden selbst festgelegt werden. Mögliche Operatoren sind bewerten, entscheiden oder beurteilen. [47, S. 19], [48, S. 5]

Zudem zeigt sich auch eine Verbindung zwischen der TKS-Taxonomie des NICE Frameworks (siehe 2.1.4 NIST SP 800-181: NICE Framework) und der Bloom’schen Lernzieltaxonomie, wenngleich diese nicht trennscharf, sondern aufgabenspezifisch betrachtet werden muss. Lernziele der ersten beiden Ebenen, Wissen und Verstehen, ordnen sich typischerweise in den Bereich Knowledge ein, da sie reproduktiv sind und keine beobachtbare Handlung implizieren. Die höheren Ebenen ordnen sich, je nach Anwendungsbereich, eher in Skills ein, da mit ihnen oftmals eine beobachtbare Handlung verbunden wird beziehungsweise verbunden werden kann, wenngleich sicherlich fast alle Lernziele auch eine unterschiedlich große Knowledge-Komponente beinhalten.

3. Related Work

Im Zuge der Literaturrecherche wurde über die grundlegenden Konzepte hinaus noch nach Werken, die sich mit Anforderungen an Incident Handler beschäftigen, gesucht. Dabei fiel auf, dass es keine wissenschaftliche Publikationen, die diese Anforderungen so detailliert wie diese Arbeit untersuchen, gibt. Die vorliegende Arbeit stützt sich daher neben den theoretischen Referenzwerken wie Standards und Normen und den fachdidaktischen Konzepten, die allgemein und für andere Schwerpunktsetzungen existieren, vorrangig auf die Curricula der Fachhochschule St. Pölten sowie die praktische Expertise der in den Interviews befragten Experten. Darüber hinaus sind dem Verfasser inoffiziell andere Lehrveranstaltungsplanungen anderer Bildungseinrichtungen im Bereich Incident Handling bekannt, deren Konzeption jedoch wissenschaftlich nicht fundiert ist, wodurch diese nur als praktische Beispiele für eine Implementierung von Cyberranges im Bereich Incident Handling im Studium gelten können. Für die vorliegende Arbeit können diese daher auch nicht als Grundlage herangezogen werden.
Dass game-based Learning jedoch eine beliebte Lehrmethode ist und als solche auch zielführend eingesetzt werden kann, arbeiten unterschiedliche didaktische Arbeiten heraus. Für den vorliegenden Kontext kann dabei insbesondere eine Arbeit von Haslinger und Lang-Muhr als Beispiel für den erfolgreichen Einsatz des game-based Learning, das durch die Implementierung einer Cyberrange in ähnlicher Form angestrebt wird, dienen.
Des Weiteren konnten im Rahmen der Literaturrecherche eine Sektion des NICE Frameworks und ein Abschnitt der ISO 27035 als relevante Referenzen für die Anforderungen an Incident Handler identifiziert werden. Diese können folglich als wichtige verwandte Arbeiten verstanden werden und werden daher im Folgenden näher abgebildet.

3.1. Anforderungen an Incident Handler im NICE Framework

Das NICE Framework, das bereits in 2.1.4 NIST SP 800-181: NICE Framework genauer erörtert wurde, bietet neben der Möglichkeit, eigene Statements zu formulieren auch vorbereitete sieben Work Role Categories mit insgesamt 52 verschiedenen untergeordneten Work Roles an. Diesen wiederum sind vorgefertigte Task-,

Knowledge-, und Skill-Statements zugewiesen. [49] Da die Publikationen der NIST fast ausschließlich für amerikanische Behördern und Unternehmen entwickelt wurden, erfolgt keine Einbeziehung europäischer oder gar österreichischer Umstände. Es ist daher davon auszugehen, dass das Framework als Basiskonzept auch in Europa Gültigkeit hat, jedoch Einzelheiten wie bereits ausgearbeitete Work Roles und deren Aufgaben differieren.

Die im NICE Framework vorgesehenen, für Security Incidents relevanten Work Roles sind dabei umfassend, wobei unter anderem Work Roles definiert werden, deren Rolleninhaber in einer Aufarbeitung eines Security Incidents durch ihr methodisches oder fachliches Know-How sowie ihre Kenntnisse über die betroffene Infrastruktur und das Aufrechterhalten des Regelbetriebes unterstützend mitwirken können. Die folgende Liste ist unvollständig und soll beispielhaft zeigen, wie viele verschiedene Fachgebiete für ein erfolgreiches Lösen eines Security Incidents notwendig sein können. Anzumerken ist, dass die Liste an Work Roles der NIST natürlich nicht abschließend zu verstehen ist.

- Kategorie Oversight and Governance (OG): Cybersecurity Legal Advice, Privacy Compliance [49]
- Kategorie Design and Development (DD): Cybersecurity Architecture, Enterprise Architecture [49]
- Kategorie Implementation and Operation (IO): Systems Administrator, Network Operations [49]
- Kategorie Protection and Defense (PD): Defensive Cybersecurity, Digital Forensics, Infrastructure Support, Insider Threat Analysis, Threat Analysis, Vulnerability Analysis [49]
- Kategorie Investigation (IN): Digital Evidence Analysis [49]
- Kategorie Cyberspace Intelligence (CI): All-Source-Analyst [49]

In der Kategorie Protection und Defense findet sich auch eine dedizierte Rolle namens Incident Response [49], die im Sinne der Arbeit von besonderem Interesse ist und daher im Folgenden näher beschrieben wird.

Work Role Incident Response

NIST beschreibt die Zuständigkeit der Work Role Incident Response (Kennzahl PD-WRL-003) als „[r]esponsible for investigating, analyzing, and responding to network cybersecurity incidents.“ [4]

Dabei werden die Aufgaben der Incident Handler in den Task-Statements näher spezifiziert. Diesen zufolge fallen beispielsweise die Tätigkeitsbereiche Vulnerability Management, Reporting und Kommunikation der Findings sowie die Mitigation potentieller Security Incidents in das Aufgabenfeld der Incident Handler. [4] Konkret finden sich dabei Task-Statements wie „T1316: Document cyber defense incidents from initial detection through final resolution“ [4] oder „T1299: Determine causes of network alerts“ [4]. Da die Tasks so breit gefasst sind, finden sich aber auch Task Statements wie „T1372: Advise law enforcement personnel as technical expert“ [4], die für einen Incident Handler in der österreichischen Wirtschaft nicht von Bedeutung sein dürften.

Darüber hinaus werden Knowledge-Statements aufgeführt. Diese behandeln unter anderem die Themenkomplexe Access Control oder Designprinzipien von Architekturen und Netzwerken. [4] Beispielhaft sind dafür Knowledge-Statements wie „K0898: Knowledge of cloud service models and frameworks“ [4], „K0833: Knowledge of cyberattack actor characteristics“ [4] oder „K0701: Knowledge of data backup and recovery policies and procedures“ [4].

Abschließend findet sich auch eine Liste mit Skill-Statements, die unter anderem die Bereiche Malware und Umgang mit digitalen Evidenzen beinhalten. [4] Als dafür relevante Skill-Statements seien exemplarisch „S0547: Skill in identifying malware“ [4], „S0572: Skill in detecting host- and network-based intrusions“ [4] und „S0483: Skill in identifying software communications vulnerabilities“ [4] aufgeführt.

3.2. Anforderungen an Incident Handler in ISO 27035-2

Im Unterkapitel 7.3.3 der ISO 27035-2:2023 werden verschiedene Skills für Mitarbeitende im Incident Response Team in vier Kategorien beschrieben. [29, Kap 7.3.3]

Als relevante *Personal Skills* werden „communication, problem solving, team interactions, time and project management“ [29, Kap 7.3.3] genannt.

Notwendige *Technical Skills* sind laut Norm „security principles, risks analysis, threat modelling, vulnerability analysis, log analysis“ [29, Kap 7.3.3].

Wichtige *Incident Response Skills* sieht die Norm in „ team policy/procedure [der Organisation, Anm. d. Verf.], communication, incident analysis, recording and tracking incident information“ [29, Kap 7.3.3].

Zuletzt werden als *Specialized Skills* noch „presentation, leadership, subject matter expertise“ [29, Kap 7.3.3] erwähnt.

Abschließend nennt die Norm verschiedene Bereiche, in denen die Mitarbeiter:innen des IRT, je nach Organisation, über Wissen verfügen sollten. Beispielsweise werden hier „[...] current network security issues, including attacks, threats, malware, and vulnerabilities“ [29, Kap 7.3.3] oder „system administration security practices such as patch management, secure configuration, backup, and disaster recovery“ [29, Kap 7.3.3] als für Incident Handler relevante Bereiche gelistet. Es finden sich darüber hinaus noch Anforderungen über Kenntnisse in grundlegenderen Themen der Datenübertragung wie verschiedene Netzwerk- und Applikationsprotokolle wie Ethernet, WiFi, TCP, UDP, DNS oder SMTP. [29, Kap 7.3.3]

3.3. Game-based Learning

In ihrer Arbeit *Business Continuity & Desaster Recovery als Planspiel umgesetzt* versuchen Haslinger und Lang-Muhr, Lehr- und Prüfungsmethoden im Hochschulbereich zu finden, die die individuellen Stärken der Studierenden fördern. [50] Damit wird der in 2.3.1 Didaktische Rekonstruktion beschriebenen Anforderung, den Unterricht an die Lernen anzupassen, Rechnung getragen. Konkret wurde hierzu eine prüfungsimmanente Lehrveranstaltung im Rahmen eines Planspieles erstellt, bei dem die Studierenden nach einer Naturkatastrophe auf der Erde in der Rolle verschiedener Unternehmen das gesamte Internet wieder aufbauen müssen, wobei jedes Unternehmen wirtschaftliche Interessen verfolgt, die zur Förderung der Leistungsbereitschaft auch auf die Beurteilung umgelegt werden. Diese Art des Planspieles wurde durch die Studierenden „vollumfänglich positiv“ [50] bewertet. [50] Somit wurde durch die Autoren nicht nur die Wichtigkeit von praktischen Übungen bestätigt, sondern auch belegt, dass sich Studierende dies explizit wünschen. Für die Konzeption der Lehrveranstaltung zu Incident Handling kann folglich angenommen werden, dass sowohl die Motivation, sich praktisch mit den Inhalten auseinanderzusetzen, vorhanden ist als auch Vorerfahrungen mit Lehrveranstaltungen mit überwiegend praktischem Charakter bestehen. Es kann daher gefolgert werden, dass ein praxisorientiertes Lehrveranstaltungskonzept positiv von den Studierenden aufgenommen wird.

Darüberhinausgehend streben Haslinger und Lang-Muhr auch eine Kompetenzorientierung an. Sie führen dabei die vier Kompetenzen Fachkompetenz, Methodenkompetenz, Sozialkompetenz und Selbstkompetenz nach dem Modell von Lehmann und Nieke an. Als Beispiele für Methodenkompetenzen werden der Wissenserwerb aus technischen Dokumentationen und Skills aus dem Projekt- und Konfliktmanagement genannt. Im Bereich der Sozialkompetenzen werden unter anderem Kritik- und Teamfähigkeit sowie Konflikt- und Kompromissfähigkeit aufgeführt. Beispiele für Selbstkompetenzen sind Selbstdisziplin, Stressmanagement und Flexibilität. [50] Aufgrund der ähnlichen Tätigkeiten und der allgemein gefassten Kompetenzbezeichnungen ist eine Übertragbarkeit auf diese Arbeit gegeben. Neben den technischen Fachkompetenzen sind dabei insbesondere die angegebenen Methoden-, Sozial-, und Selbstkompetenzen größtenteils auch auf Incident Handling umlegbar.

Mit der technischen Umsetzung und der Weiterentwicklung dieses Lehrveranstaltungskonzeptes befasste sich Machherndl in [51], der insbesondere die Automatisierung und zentrale Verwaltung des Planspiels über die Weiterentwicklung der vorhandenen Weboberfläche fokussiert. Da keine vorhandene Simulations- oder Emulationssoftware die Anforderungen erfüllen konnte, musste eine Eigenentwicklung auf Basis von Proxmox VE, über deren API über die zentrale Weboberfläche virtuelle Maschinen, Container oder virtuelle Netzwerke erstellt oder gelöscht werden können, etabliert werden. [51]

Die in der Arbeit von Machherndl angestellten Überlegungen für die technische Umsetzung können teilweise auch auf eine Cyberrange für Incident Handling umgelegt werden, wobei zu beachten ist, dass die volle Simulation eines vollständigen Enterprise-Netzwerkes zur Darstellung eines realistischen Incident Handling-Einsatzes deutlich mehr Ressourcen in Anspruch nimmt als der beschriebene Anwendungsfall in der BCDR-Lehrveranstaltung.

Einen spielerischen Zugang zur Lehrstoffvermittlung im Cybersecuritybereich zeigen auch Rajendran et al. mit dem game-based Learning (GBL) auf. Während sich die meisten GBL-Anwendungen in technischen Themen wiederfinden – bekannt sind insbesondere Hackathons oder Capture the Flag-Formate –, fand die Arbeit insbesondere in spielerischen Lernformen für prozessbezogene und nicht-technische Inhalte eine auffällige Lücke. [52, Kap. 2.3] Für generelles Incident Handling wurde ein einfaches Spiel mit vier Leveln beschrieben, bei dem die Spieler:innen mit verschiedenen Szenarien, beispielsweise unüblichem Netzwerkverkehr oder schädlichen Inhalten auf einem Computer, konfrontiert wird. Dadurch würden Unregelmäßigkeiten auch in Realität besser erkannt und Maßnahmen gesetzt werden können. [52, Kap. 3.5]

3.4. Einordnung und Anwendung des NICE Framework

Forscher:innen der JAMK University of Applied Sciences haben 2021 versucht, die Curricula von Studiengängen im Bereich Cybersecurity in den Vereinigten Staaten von Amerika sowie Europa auf das NICE Framework zu mappen. Dabei fiel auf, dass insbesondere die Anforderungskategorien *Operate and Maintain* sowie *Securely Provision* überdurchschnittlich erfüllt werden. Lücken zeigen sich in den Bereichen *Analyse*, *Collect and Operate*, *Investigate* und *Protect and Defend*. Dennoch wird beschrieben, dass die Curricula sich an den Bedürfnissen der Cybersecuritybranche orientieren. [53] In den Zielkategorien, die ursächlich mit Incident Handling verbunden sind, zeigen sich also sowohl in europäischen, als auch in US-amerikanischen Studiengängen Lücken.

Karagiannis et al. arbeiteten in ihrer Forschung daran, dieses Framework auch in Cyberranges in der Design- und Entwicklungsphase einzusetzen. Dabei wurden für eine Cyberrange Work Roles, die typischerweise in einem SOC anzutreffen sind – die Work Role Incident Response war keine davon –, analysiert und 16 Szenarien für diese entwickelt. Dabei wurde in zwei Schritten vorgegangen. Zunächst wurden Lernziele aus den Workforce Categories des NICE Framework ausgewählt. Anschließend folgte das Architektur- und Szenariendesign. [54] Damit sind die Vorgaben zur Erstellung, im Gegensatz zum in [18] vorgeschlagenen Cyber Range Design Framework, wesentlich rudimentärer, wenngleich dieses nicht vorschlägt, das NICE Framework zu nutzen. [18] In dieser Arbeit wurden daher die Hinweise zur Erstellung nur in geringem

Maße genutzt.

4. Methodik

Um die vorliegenden Fragestellungen zu beantworten, wurde zunächst das benötigte inhaltliche Fachwissen erhoben. Dazu wurden neben einer Literaturrecherche hauptsächlich Experteninterviews durchgeführt, um den Blickwinkel der Praxis in die Konzeption der Lehrveranstaltung miteinbeziehen zu können. Die Vorgehensweise wird in diesem Kapitel abgebildet und plausibilisiert.

4.1. Erhebung in der Praxis mittels Experteninterview

Um die Anforderungen ausgewählter österreichischer Unternehmen an ihre Mitarbeiter:innen im Bereich Incident Handling zu verstehen, wurden die Verantwortlichen für diese Dienstleistung befragt. Dazu wurde je ein Interview mit PwC Österreich GmbH Wirtschaftsprüfungsgesellschaft, ACP Group AG, der Magistratsabteilung 01 der Stadt Wien (Wien Digital - WienCERT) und der CANCOM Austria AG durchgeführt. Die Methode und das Erhebungssetting werden im Folgenden näher dargestellt.

4.1.1. Erhebungsinstrument Experteninterview

Zur Erhebung der Vorgangsweise bei Security Incidents und den daraus resultierenden Anforderungen an das Personal wurde mit Vertretern großer Firmen, die im Bereich des Incident Handling arbeiten, ein qualitatives, leitfadengestütztes Experteninterview durchgeführt.
Diese Form der Erhebung wurde gewählt, um den „Zugang zu Wissensbereichen [zu] eröffnen (Typus ‚systematisierendes Experteninterview')" [55, S. 671], die ausschließlich den Expert:innen bekannt sind, sich für die Konzeption der Lehrveranstaltung und der Cyberrange jedoch von Bedeutung erweisen. Dadurch soll der relevante Gegenstand beleuchtet und eine wissenschaftliche Behandlung überhaupt ermöglicht werden, was insbesondere bei Themen, zu denen keine oder wenig Literatur existiert, die übliche Vorgangsweise in der Forschungspraxis darstellt (siehe 3 Related Work). [56, S. 87]
Die Gestaltung der Interviewsituation ist dabei maßgeblich für den Erfolg des Interviews, da sie die Auskunftsbereitschaft beeinflusst. [57, S. 165] Zu bedenken ist dabei, dass die Interviewsituation durch eine

Asymmetrie in der Kommunikation geprägt ist, die durch die Rollenverteilungen im Interview entsteht. [57, S. 42ff.] Bei Experteninterviews verkehrt sich diese Hierarchie insofern, als dass Expert:innen als Fachleuten ein besonderer Status zugeschrieben wird. [57, S. 165] In diesem Fall ist jedoch von einer weniger asymmetrischen Kommunikation auszugehen, da auch der Interviewer eine Expertise in das Gespräch mitbringt.

Das Gelingen des Interviews ist dabei zudem davon abhängig, wie viel der:die Befragte erzählt. Im Zuge der Strukturierung des Interviews ist daher nach dem Grundsatz „so offen wie möglich [...] und so strukturiert wie nötig“ [55, S. 673] vorzugehen. Diese Anforderung, nach der Interviews zu gestalten sind, ist auch unter dem Prinzip der Offenheit bekannt. Helfferich beschreibt hierbei: „Der größte Fehler qualitativer Interviewdurchführung liegt darin, zu viel vorzugeben und abzufragen sowie in einer Haltung, bestätigt bekommen zu wollen, was man schon weiß.“ [55, S. 672] Eine Einschränkung der Offenheit muss jedoch durch die Beschränkung des für das Forschungsinteresse relevante Themengebiet vorgenommen werden. [55, S. 672] Auch hier ist demnach das Finden eines Mittelweges zentral.

Experteninterviews kommt hierbei eine besondere Stellung zu, da sie „mehr Strukturierung, eine vereinfachte Transkription und eine schneller die Komplexität reduzierende Auswertung“ [57, S. 156, S. 162] erlauben. Rein narrative Interviews werden bei Befragungen von Expert:innen nicht empfohlen, da offene Erzählaufforderungen Verwirrung stiften könnten, da Expert:innen eine knappe, zeitökonomische Befragung erwarten. [57, S. 162ff.] Stattdessen soll ein inhaltlich und sprachlich an das Fachgebiet der Expert:innen angepasster Leitfaden verwendet werden. Die Verwendung dessen bringt weitere Vorteile mit sich: Er grenzt das interessante Thema ab, berücksichtigt den Status der Interviewten als Expert:innen und positioniert den Interviewer als kompetent und in das Thema eingearbeitet. [57, S. 164], [55, S. 682]

Der soeben angesprochene „Leitfaden von Interviews stellt das zentrale Scharnier zwischen der Forschungsfrage und dem Erkenntnisgewinn dar. Er dient dazu, die Fragebereiche der Leitfrage aufzugliedern, relevante Themengebiete aufzugreifen und zu systematisieren.“ [56, S. 94] An den Interviewleitfaden, der grundsätzlich in Bezug auf den Grad der Ausformulierung und der Vorstrukturierung der enthaltenen Fragen relativ individuell gestaltet sein kann [57, S. 36], bestehen darüber hinaus noch weitere Anforderungen. Er darf nicht mit Fragen überladen sein, sodass genug Zeit bleibt, sich den einzelnen Frageitems zu widmen. Zudem soll die Gestaltung übersichtlich sein, sodass während des Gesprächs nicht der Fokus auf dem Leitfaden, sondern auf dem Gegenüber liegt. [57, S. 180] Reinders schlägt deswegen vor, eine ausformulierte Version zu haben und eine Variante mit Stichwörtern für das Interview selbst. [56, S. 94] Des Weiteren soll bereits dem Interviewleitfaden eine rote Linie inhärent sein, die sich durch das Gespräch zieht, wodurch keine Themensprünge erzwungen werden. Längere Fragen, die ausführlich beantwortet werden sollen, sollten dabei

eher zu Beginn des Gesprächs gestellt werden. Auch wenn ein Leitfaden erstellt wird, muss jedoch bei der Durchführung des Interviews immer berücksichtigt werden, dass auch über den Leitfaden hinausgehende Informationen aufgenommen und nicht abgeblockt werden sollen. [57, S. 180]

Diesen Ansprüchen versucht bereits der Interviewleitfaden gerecht zu werden. Im Zuge der Erstellung wurde gemischt induktiv und deduktiv vorgegangen [56, S. 94], wobei der SPSS-Prozess (Sammeln, Prüfen, Sortieren, Subsummieren) genutzt wurde. Dabei wurden in einem ersten Schritt die Fragen einerseits aus der Literatur und andererseits aus der persönlichen Erfahrung generiert. So wurde eine Sammlung an Fragen erstellt, die in einem weiteren Schritt auf ihre Eignung zur Beantwortung der Fragestellung der Arbeit sowie zur Erhebung in Experteninterviews geprüft wurden. Im Zuge dessen wurden vorrangig Items eliminiert, die durch die Literatur beantwortbar sind, sowie der Leitfaden um redundante oder weniger wichtige Fragen gekürzt. Anschließend wurden die Fragen sortiert, um dem Aufbau des Interviews gerecht zu werden, bevor übergeordnete und Anschlussfragen erstellt wurden. Im letzten Schritt wurde dabei auch die Formulierung der Fragen vorgenommen, sodass mehrere relevante Informationen mit einem Item erfragt werden konnten. [57, S. 182-185] Auch wenn die Unterordnung einzelner Frageitems unter offene Items, die Erzählaufforderungen beinhalten, für Experteninterviews nicht empfohlen wird [57, S. 179], wurde dies im vorliegenden Fall mehrfach so konzipiert, da insbesondere Vorgangsweisen zum Umgang mit Security Incidents erhoben werden sollten. Diese Frageitems benötigen ein Erzählen; da jedoch auch bestimmte Faktoren von Interesse waren, ergaben sich die Unterordnungen. Aus diesen Überlegungen ergab sich der nachfolgend beschriebene, aus vier Teilbereichen bestehende Interviewleitfaden.

Der erste Abschnitt zielt mit offenen Fragen darauf ab, das Unternehmen und das Produktportfolio im Bereich Incident Handling zu verstehen. Von Bedeutung ist dabei unter anderem auch, ob (nahezu) ausschließlich bereits bekannte Kunden, beispielsweise im Rahmen eines Retainer- oder SLA-Vertrages, betreut werden oder die Mitarbeiter:innen sich auch in kürzester Zeit auf für sie völlig unbekannte IT-Umgebungen und Geschäftsfelder einstellen können müssen. Die daraus gewonnenen Erkenntnisse sollen später in das Design der Rahmenbedingungen der Cyberrange einfließen.

Anschließend sollen die allgemeinen Anforderungen an Mitarbeiter:innen erhoben werden. In diesem Abschnitt wird bewusst noch keine Einschränkung im Bezug auf den Tätigkeitsbereich (beispielsweise technisch oder organisatorisch) gemacht, um ein holistisches Bild der Beschäftigung im Unternehmen zu erhalten. Stattdessen werden die offenen Fragen in diesem Bereich zu diesem Zweck möglichst allgemein gestellt. Besonders von Bedeutung sind dabei auch die Fragen zum Thema Spezialisierung, bei denen erhoben wird, ob Mitarbeiter:innen im Incident Handling eher auf eine Tätigkeit spezialisiert (beispielsweise Incident-Koordination) oder als „Allrounder“ in verschiedensten Bereichen tätig sind. Dies dient im späteren

Verlauf zur Konzipierung der Cyberrange als Basis für die Gruppengröße und die Anzahl, die Schwierigkeit beziehungsweise den Aufwand und Häufigkeit der während der Übung eingespielten Aufgaben.
Der dritte Teil des Interviews soll speziell die organisatorischen Anforderungen erheben. Dabei sind die Fragen bereits nach dem TKS-Prinzip gemäß NIST SP 800-181 R1 gegliedert. Zuerst werden die Aufgaben (Tasks) der Mitarbeiter:innen erhoben. Zusätzlich wird dabei auch das Setting zur Umsetzung dieser Aufgaben ermittelt, also die Anzahl der an diesem Task zusammenarbeitenden Personen und die üblichen zeitlichen Vorgaben zur Erledigung. Diese Erkenntnisse sollen abermals in die Konzipierung der Rahmenbedingungen der Übung, insbesondere der Ausgestaltung der Gruppengröße, einfließen.
Darauffolgend wird das notwendige Wissen (Knowledge) erhoben. Dabei soll festgestellt werden, inwieweit ein theoretischer Background in organisatorischen Themenfeldern überhaupt notwendig ist. An dieser Stelle wird auch bereits eine Verknüpfung zur Bloom'schen Lernzieltaxonomie hergestellt, mit der das geforderte Wissensniveau genauer beschrieben wird. [47, S. 19] Zusätzlich werden auch gebräuchliche Fachbegriffe und Schlagwörter erfragt, die für das Arbeiten im Bereich Incident Handling von Bedeutung sind. Mit dieser Frage sollen auch Konzepte und Systembezeichnungen gefunden werden, die bisher an der Fachhochschule St. Pölten nicht unterrichtet werden und gegebenfalls noch integriert werden müssen.
Der vierte und letzte Abschnitt befasst sich mit allgemeinen Anmerkungen zur Lehrveranstaltungsplanung und den Vorstellungen der Interviewten dazu. Hier sollen die Interviewpartner:innen die Möglichkeit erhalten, ihre Ideen und zentrale Inhalte für die Lehrveranstaltung zu nennen.
Der Interviewleitfaden ist im Annex A einzusehen.
Für die Durchführung der Interviews sei dabei noch angemerkt, dass neben den Frageformen auch nonverbale Steuerungsmaßnahmen das Erzählverhalten der Interviewten beeinflussen. [57, S. 117] Eine genauere Beschreibung der Interviewereffekte wäre hier zu umfangreich und kann unter anderem bei Jedinger und Michael in Baur und Blasius [58, S. 365-376] nachgelesen werden. Zentral für das Bewusstsein der Interviewer ist jedoch, dass das Antwortverhalten – bewusst und unbewusst – durch sie gesteuert und die Antworten verfälscht werden können. [57, S. 114f.] Um diesen Gefahren entgegenzuwirken wurde sich nicht nur mit der Thematik befasst, sondern auch die Offenheit der Fragen entsprechend konzipiert und die verbalen wie nonverbalen Signale während des Erzählens der Interviewten so gering wie möglich gehalten.

4.1.2. Erhebungssetting

Die Erstversion des Interviewleitfadens wurde anhand der Literatur auf offene Stellen untersucht und anschließend ausformuliert. Einem Pretest wurde der Interviewleitfaden aufgrund der fehlenden Machbarkeit nicht unterzogen, da dafür nicht ausreichend qualifizierte Interviewpartner:innen zur Verfügung gestanden

wären.

In weiterer Folge wurden die Interviews durchgeführt. Dafür wurden vier Vertreter:innen großer Unternehmen oder Behörden, die mit Incident Handling befasst sind, zu ihren Vorgangsweisen im Falle eines Security-Vorfalls befragt (siehe 4.1.3 Beschreibung der Stichprobe).

Die Interviews wurden in der Kalenderwoche 15 2025 durchgeführt. Um die zeitlichen Ressourcen der Teilnehmenden nicht überzustrapazieren, wurde im Interviewleitfaden auf die zentralen Punkte fokussiert. Die tatsächliche Dauer der Interviews erwies sich dann als länger als erwartet, da die Interviewpartner umfangreiche Beschreibungen lieferten und die Fragen ausführlich, teilweise über die Fragestellung hinausgehend, beantworteten. Daraus resultieren ein 40-minütiges Gespräch mit Philipp Mattes-Draxler (PwC), ein 56-minütiges Interview mit Andreas Plank (ACP), eine 53 Minuten dauernde Befragung von Utz Nisslmüller (MA01 der Stadt Wien) sowie eine 45-minütige Erhebung mit Gideon Teubert (CANCOM).

Zudem wurden die Interviews mit Andreas Plank, Utz Nisslmüller und Gideon Teubert aus Gründen der Zeiteffizienz online über Microsoft Teams durchgeführt. Die Befragung von Philipp Mattes-Draxler wurde im DC Tower Wien in Präsenz durchgeführt. Das Treffen fand dabei im Büro des Interviewten statt, wodurch eine ruhige, störungsfreie Atmosphäre gewährleistet wurde. Dass sich ein persönliches Gespräch ergeben hat, liegt daran, dass Philipp Mattes-Draxler dem Verfasser aufgrund eines Arbeitsverhältnisses persönlich näher bekannt ist. Der Interviewte ist bei PwC ein Vorgesetzter des Verfassers. Auch Andreas Plank ist dem Verfasser durch Lehrveranstaltungen als Lehrender an der Fachhochschule St. Pölten ebenso persönlich bekannt. Vor diesem Hintergrund sind insbesondere diese beiden Interviews in einem gut-kollegialen Kontext zu situieren, der den Austausch beeinflusst. Der Kontakt zu der Stadt Wien und deren Ansprechpartner für das Interview, Utz Nisslmüller, sowie zu CANCOM und Gideon Teubert wurden durch eine private Verbindung hergestellt.

Das persönlich geführte Interview wurde mittels OnePlus Recorder-App aufgezeichnet, die drei Online-Interviews wurden über die in Microsoft Teams vorgesehene Funktion aufgezeichnet, anschließend automatisiert transkribiert und manuell korrigiert. Hierfür wurde eine weite Transkription angelegt, da sprachliche Analysen sowie die Berücksichtigung von Versprechern und Pausen für den Kontext der vorliegenden Arbeit nicht relevant sind. Dementsprechend wurden im Zuge der Überarbeitung der Transkripte geringfügige Anpassungen an die Sprachnormen vorgenommen, wobei die Satzstruktur nicht verändert oder Wörter ausgetauscht wurden, um die Semantik nicht unabsichtlich zu verfälschen.

Die Transkripte wurden den jeweiligen Interviewpartnern zur Durchsicht geschickt, damit diese Schwärzungen vornehmen können, sollten sie Details, die nicht veröffentlicht werden dürfen, im Zuge des Interviews preisgegeben haben. Schwärzungen wurden dabei im Bereich des Kundenumfeldes von CANCOM und im

Bereich interner Abläufe und vorgehaltener Ressourcen durch das WienCERT vorgenommen. Da die durch die Interviewten gegebene Beschreibung deutlich detaillierter war als auf die mit der Frage abgezielten Informationen, enthalten die Schwärzungen dieser Angaben keine für die Arbeit wesentlichen Informationen. Die Kennzeichnung dieser Passagen erfolgte im Transkript durch den Passus „[Interviewabschnitt entfernt]“. Die Transkripte der Interviews sind im Annex B einzusehen.

4.1.3. Beschreibung der Stichprobe

Im Zuge der Erhebung konnten vier Interviewpartner aus unterschiedlichen Unternehmen zu ihrem Umgang mit Incident Handling befragt werden.

Das erste Interview wurde mit Philipp Mattes-Draxler, Partner bei PwC Österreich, durchgeführt. PwC ist ein Wirtschaftsprüfer, Steuerberater und Unternehmensberater und ist international als Netzwerk organisiert. In Österreich erbringt das Unternehmen im Team Cybersecurity & Privacy mit 50 Vollzeitäquivalenten verschiedenste Cybersecurity-Beratungsdienstleistungen, darunter auch Incident Handling für externe Kunden. Unabhängig von den beratenden Mitarbeiter:innen führt PwC auch mit einem eigenen Team Incident Handling für die interne globale Infrastruktur durch. Das Unternehmen betreut im Rahmen von Service Level Agreements (SLAs) unter dem Namen „Incident Response Retainer“ externe Kunden aus verschiedenen Branchen und verschiedenster Größe, wobei die meisten Kunden eher den Bereichen größere mittelständische Unternehmen und Enterprise zuzuordnen sind. Neben den reaktiven Dienstleistungen, die beispielsweise Krisenmanagement und koordinierende Tätigkeiten, IT-Forensik oder Schadsoftwareanalyse beinhalten, finden sich auch proaktive Angebote im Portfolio, von Beratung über Readiness-Assessments bis hin zu SOC-Beratung und -dienstleistungen. Incident Handler arbeiten bei PwC außerhalb aktiver Incidents auch in diesen Bereichen mit. (Interview B.1)

Daran anschließend wurde das zweite Interview mit Andreas Plank, Head of Security Services bei ACP, geführt. Neben Hybrid Cloud & Data Center, Modern Workplace und Digital Solutions bietet das Unternehmen im Bereich Network & Security auch Incident Handling aus dem SOC heraus an. Aber auch Kunden, die keine SOC-Variante der ACP nutzen, können ad hoc um Unterstützung bei Security Incidents ansuchen. Das dabei betreute Kundenumfeld bei ACP ist laut Andreas Plank im Gegensatz zu PwC heterogener, besteht aber ebenfalls aus KMU- und Enterprise-Umgebungen. 32 Mitarbeiter:innen betreuen diese Kunden dabei in drei Teams in der Analyse, im Consulting und im SOC-Engineering. Diese waren als seniorige Analysten bei ACP tätig und konnten sich im Laufe ihrer Karriere zu Incident Handlern weiterentwickeln. (Interview B.2)

Im dritten Interview wurde Utz Nisslmüller, ein Mitarbeiter im WienCERT in der Magistratsabteilung 01

der Stadt Wien, befragt. Diese deckt sowohl Blue- als auch Red-Team-Aufgaben für alle Magistratsabteilungen der Stadt Wien ab. Zusätzlich führt das CERT auch Security-Consulting für die IT-Verantwortlichen der anderen Magistrate durch. Alle auftretenden Security Incidents werden vom WienCERT selbst abgearbeitet. Extern werden nur beispielsweise Auditierungs- und Pentestingaufgaben vergeben, um eine Selbstüberprüfung zu verhindern. (Interview B.3)

Abschließend erfolgte im vierten Interview die Befragung von Gideon Teubert von CANCOM. CANCOM beschäftigt 5600 Mitarbeiter:innen im DACH-Bereich, ist aber auch international vertreten. In Österreich sind 60 Blueteamer tätig, das Kernteam im Bereich Incident Handling besteht dabei aus 15 Personen. Außerhalb von Security Incidents arbeiten diese Personen an Beratungsprojekten und Workshops sowie der Weiterentwicklung im Bereich *Digital Forensics and Incident Response*. Das Kundenumfeld besteht, ähnlich wie PwC, aus größeren KMU und Enterprises. Auch CANCOM bietet eine SLA für Incident Handling an. Die Besonderheit des Unternehmens in der Stichprobe besteht darin, dass auch zumindest ein SOC-Modul zur besseren Visibilität genutzt werden muss. (Interview B.4)

4.1.4. Auswertungsmethode: Inhaltsanalyse nach Mayring

Zur Auswertung der in den Experteninterviews erhaltenen Daten wurde eine *Qualitative Inhaltsanalyse* nach Philipp Mayring durchgeführt, um systematisches Vorgehen zu ermöglichen. [59, S. 49f.] Dafür wurde zunächst die Entstehungssituation analysiert (siehe 4.1.2 Erhebungssetting), bevor die Fragestellung an das Material herangetragen wurde, um die Analysetechnik auszuwählen. [59, S. 61] Als geeignet erwies sich die zusammenfassende Inhaltsanalyse, weswegen primär nach dieser vorgegangen wurde. Bei dieser Methode werden zunächst zusammengehörige Interviewabschnitte als Bedeutungseinheiten, sogenannte Makropropositionen, generiert, die dann mit den sogenannten Makrooperationen zusammengefasst werden. Zu diesen gehören unter anderem das Auslassen irrelevanter Inhalte sowie das Generalisieren detaillierter Abschnitte. [59, S. 44f.], [60, S. 164ff.], [61, S. 112-115] Dabei werden die Inhalte zunächst paraphrasiert und dann schrittweise reduziert. So sollen Kernaussagen herausgearbeitet und identische Inhalte eliminiert werden. In einem der Arbeit beiliegenden Dokument werden diese Aufarbeitungsschritte in den Stufen Paraphrase – Generalisation – Reduktion, wie sie auch bei Mayring vorgeschlagen werden [59], transparent gemacht.

Durch diese Prozessschritte wurden auch Abstraktionen vorgenommen, sodass die so generierten Aussagen den Anspruch haben, für den gesamten Datenkorpus zu gelten. Diese Abstraktionen hatten letztlich auch die Bildung induktiver Kategorien zufolge, die sich aus der Analyse des Materials ergeben haben. Nur auszugsweise gaben die im Interview gestellten Fragen bereits die Kategorie der Antwort vor, sodass in solchen Fällen abschnittsweise deduktiv Kategorien an das Material angelegt wurden. [62] Durch diese Vorgangs-

weise bedingt wurden die aus dem Material erhaltenen Kategorien wiederum an dem Ausgangsmaterial selbst auf ihre Anwendbarkeit, Abgeschlossenheit und Sinnhaftigkeit überprüft. Da alle Abschnitte Kategorien zugeordnet werden konnten, erfüllen diese die Anforderungen und konnten so weiterhin verwendet werden. [59, S. 61]

An die Überprüfung anschließend wurden die Ergebnisse zusammengestellt und abschließend mit den durch die Literatur gewonnenen Anforderungen zusammengeführt. Dies entspricht dem Arbeitsschritt der Kontextanalyse [59, S. 61, S. 89-92] und ist im Ergebnisteil der Arbeit explizit gemacht (siehe 5.1 Analyse der Anforderungen).

4.2. Erhebung mittels Literaturrecherche

Über die Erhebung mittels Experteninterviews hinaus wurde die in dem Kapitel 3 Related Work beschriebene Literatur auf Anforderungen an Incident Handler analysiert.

Im Rahmen der Literaturrecherche wurde die ISO-Normenreihe 27035 als besonders relevant für Incident Handling erachtet, da an der Fachhochschule St. Pölten auch in den anderen sicherheitsmanagementbezogenen Lehrveranstaltungen besonderer Wert auf die Nutzung von ISO-Standards gelegt wird. Viele der dahinterstehenden Konzepte und Abläufe sind in der Normenfamilie stringent und aufeinander bezogen, sodass durch die Verwendung dieser Standardreihe an das Vorwissen der Lernenden angeknüpft werden und dieses erweitert werden kann (siehe 2.3.1 Didaktische Rekonstruktion).

Da sowohl bei der Recherche auf Webseiten und in verwandten wissenschaftlichen Arbeiten als auch bei den Vorgesprächen zu den Interviews immer wieder NIST SP 800-61 genannt wurde, wurde auch diese Publikation im Rahmen der Arbeit berücksichtigt. Mit der Revision 3 wurde erst kürzlich eine neue Version veröffentlicht, die als Grundlage für die Arbeit herangezogen wurde, um dem aktuellen wissenschaftlichen Stand zu entsprechen. Dies impliziert aber, dass die darin vorgeschlagenen Änderungen im Prozess und den Controls in der Praxis vielfach noch nicht implementiert worden sein dürften. Zusätzlich verkomplizieren die Adaptionen den durch die Publikation skizzierten Prozess. NIST begründet die Änderungen damit, dass sich aktuelle Security Incidents mit dem veralteten Prozess nicht mehr abbilden lassen (siehe 2.2.2 Neues Lifecyclemodell (R3)), was zudem für die Anwendung der dritten Revision im Zuge der Arbeit spricht.

Darüber hinaus wurden die CIS Controls als Kontrast zu formalisierten und etablierten Standards berücksichtigt. In der Praxis werden die CIS Controls auch gerade wegen der Anfängerfreundlichkeit und Einfachheit genutzt; viele Controls sind auch ohne viel spezialisiertes Security-Personal einfach umzusetzen und zu betreiben. Daher sind sie für die Erforschung der Anforderungen an Incident Handling für Organisationen

mit geringem Reifegrad interessant.
In einem weiteren Schritt wurden aus diesen Werken alle Anforderungen und Konzepte extrahiert, analysiert sowie das dazu notwendige im Standard erklärte Hintergrundwissen tabellarisch aufgearbeitet. Dabei wurden die Inhalte reduziert, wodurch eine Kategorisierung möglich wurde. Die Zuordnungen sind als Anlage transparent gemacht.

4.3. Konsolidierung der Ergebnisse

Die aus den Interviews und der Literaturrecherche als Ergebnisse erhaltenen Tasks, Knowledge und Skills der Incident Handler wurden in einem anschließenden Schritt zusammengefasst, systematisiert und ausformuliert. Anschließend wurden daraus die bereits durch NIST in [4] beschriebenen Task-, Knowledge- und Skill-Statements auf ihre Gültigkeit für den Scope dieser Arbeit geprüft und gegebenenfalls übernommen.
Dazu wurden alle Statements nach ihrer Relevanz für den österreichischen Markt, für das Incident Handling und der organisatorischen Charakteristik geprüft. Nur, wenn alle drei Kategorien als relevant oder teilweise relevant eingestuft wurden, wurde das Statement aufgenommen. Synonym zu verstehende Anforderungen wurden dabei fusioniert. Für weitere Inhalte, die durch die NIST nicht, nicht in der notwendigen Tiefe oder zu spezifisch behandelt wurden, wurden eigene Statements formuliert.
Abschließend wurden aus den so erhaltenen Anforderungen die Lernziele abgeleitet (siehe 2.3.3 Lernziele).

4.4. Erstellung eines Konzeptes für eine Cyberrange als Abschlussübung

Das übergeordnete Ziel der Arbeit stellt die Konzipierung der Cyberrange als Abschlussübung einer Lehrveranstaltung zum Thema Incident Handling dar. Dabei wurde auf Basis der konsolidierten Ergebnisse das Konzept für die Cyberrange als Abschlussübung erstellt. Die Vorgehensweise beruhte auf dem von Katsantonis et al. vorgeschlagenen Lifecycle für die Erstellung von Cyberranges (siehe 2.1.3 Lifecycle):

4.4.1. Analyse

Der in *Cyber range design framework for cybersecurity education and training* beschriebene Prozess verlangt im ersten Schritt die Formulierung der Lernziele und der Lernstrategien. Um dies zu erfüllen, wurden in einem ersten Schritt die Anforderungen an Incident Handler mittels Literaturrecherche und Expertenin-

terviews erhoben. Davon ausgehend wurden in einem zweiten Schritt Lernziele und TKS-Statements abgeleitet.

Zusätzlich wurden auch die Voraussetzungen der Studierenden unter besonderer Berücksichtigung des vorhandenen Vorwissens analysiert. Von diesen Erkenntnissen ausgehend werden im Sinne der didaktischen Rekonstruktion (siehe 2.3.1 Didaktische Rekonstruktion) die Lernwege geplant, auf denen der Aufbau der Lehrveranstaltung beruht.

4.4.2. Design

In der Designphase werden neben den Attributen der Cyberrange, im vorliegenden Fall der Name und eine Beschreibung, auch das eigentlichen Szenario, der Cyberspace, also die beteiligten Computersysteme und das simulierte Unternehmensnetzwerk gestaltet. Dafür wurde in einem eigenen Bereich des Interviews explizit nach Ideen und Vorstellungen für eine Cyberrange als Abschlussübung gefragt. Insbesondere im Design des Unternehmensnetzwerkes und der vorhandenen Sicherheitssysteme sowie Logquellen ist der Input der Experten wichtig, um nicht nur eine realistische, sondern auch eine für Anfänger im Incident Handling lösbare Aufgabe zu stellen.

Eine weitere Herausforderung ist es, die Balance zwischen einer realistischen Übung, die die Studierenden möglichst gut praktisch auf einen realen Incident vorbereitet und einer guten Lernumgebung zu schaffen. Zu bemerken ist auch, dass der Fokus der Lehrveranstaltung auf dem organisatorischen Schwerpunkt liegen soll. Maßnahmen, um sicherzustellen, dass jeder Studierende auch organisatorische Tasks übernehmen muss, müssen daher konzipiert und implementiert werden. Zusätzlich sind auch die pädagogischen Elemente, also Hinweise und Hilfestellungen, Einspielungen mittels Injects und Zwischenaufgaben zu konzipieren. Im Zuge der Arbeit wurde dies auch exemplarisch umgesetzt.

Aus didaktischen Überlegungen wurde daher das Angreiferszenario nicht statisch, beispielsweise mittels Ansible-Playbooks, realisiert. Die Simulierung eines echten Angreifervorgehens ist so nicht nur schwierig abbildbar, sondern die genutzten Tactics, Techniques und Procedures der Angreifergruppierungen ändern sich auch regelmäßig, sodass die Gefahr besteht, dass vorbereitete Playbooks bereits im nächsten Run der Übung nicht mehr zeitgemäß oder realistisch sind. Aus diesem Grund wurde ein beispielhaftes Vorgehen skizziert, das von der Lehrveranstaltungsleitung jeweils vor der Durchführung der Übung pro Gruppe adaptiert werden soll. Dadurch besteht darüber hinaus die Möglichkeit, die Übungen auch an die Bedingungen der Lernendengruppe anzupassen. Zusätzlich lässt sich somit auch ein gruppen- bzw. jahrgangsübergreifendes Arbeiten verhindern.

4.4.3. Configuration

Anschließend wurden die virtuellen Maschinen der Cyberrange anhand des zuvor vorgestellten Konzepts mittels Infrastructure as Code erstellt. Dafür wurde Terraform genutzt. Die anschließende Konfiguration der Systeme, beispielsweise der Installation und Konfiguration von Active Directory Domain Services, wurden für ein Beispielszenario beschrieben.
Alle notwendigen Dateien, um die rudimentäre Struktur auf der derzeit an der Fachhochschule in Betrieb befindlichen OpenStack Bobcat-Instanz (2023.2) aufsetzen und betreiben zu können, wurden der Arbeit angehängt.

4.4.4. Deployment

In einem letzten Schritt wurden die in dieser Arbeit vorbereiteten Konfigurationen angewendet und ausgerollt, womit die Funktion der Virtualisierung und das automatisierte Deployment der virtuellen Maschinen auf Openstack auch praktisch überprüft werden kann. Ein Deployment der Detailkonfiguration, beispielsweise eine Active Directory Domain, ist nicht im Scope dieser Arbeit.

4.4.5. Dry Run und Execution

Im letzten Schritt erfolgte die Testung auf Funktionalität ohne Detailkonfiguration durch den Autor selbst. Es wurden keine, wie in der Literatur empfohlenen, strukturierten Tests mit Expert:innen auf dem Gebiet Incident Handling durchgeführt, da diese den Rahmen der Arbeit gesprengt hätten. Genau diese fehlende Testung stellt jedoch eine Limitierung der Arbeit dar (siehe 6.2 Limitationen).

5. Ergebnisse

Im folgenden Abschnitt werden die Ergebnisse der Literaturrecherche und der Interviews, die sich nach der soeben beschriebenen Auswertung ergeben haben, abgebildet und anschließend synthetisiert. Daran schließen weitere didaktische Überlegungen an, die mit den Anforderungen in der Konzipierung der Cyberrange zusammengeführt werden. So können sämtliche notwendige Aspekte – fachlich wie didaktisch – in der Cyberrange als Abschlussübung einer Lehrveranstaltung berücksichtigt werden.

5.1. Analyse der Anforderungen

Zunächst wurden die Anforderungen an Incident Handler aus der Literatur, den Interviews und dem Curriculum der Fachhochschule St. Pölten gesammelt und abgeglichen. Dabei sollte das Anforderungsprofil präzise und umfassend abgebildet werden, um dem Anspruch, die Studierenden bestmöglich auf ihre berufliche Tätigkeiten vorzubereiten, gerecht zu werden. Daher werden die in den einzelnen Quellen enthaltenen Anforderungen zunächst separat abgebildet und erst im Anschluss synthetisiert, um hierbei eine Priorisierung vornehmen zu können. Es muss dabei berücksichtigt werden, dass Standards und Normen den Best Practice-Fall abzubilden versuchen und daher vermutlich nicht alle Anforderungen auf die reale Situation der österreichischen Wirtschaft umzulegen sind.

5.1.1. In der Literatur beschriebene Anforderungen

Zu Beginn werden die in der Literatur aufgeführten Anforderungen an Incident Handler beschrieben. Die Abbildung dieser ist jedoch ob der starken Vernetzung des Security Incident Managements mit beinahe allen anderen Disziplinen der technischen und organisatorischen Informationssicherheit, nicht allumfassend, wobei allgemeine Anforderungen an andere Bereiche, beispielsweise Risk Management im Folgenden nur dargestellt werden, wenn sie einen starken direkten Einfluss auf das organisatorische Incident Handling haben. Das gilt auch für SP 800-61 (siehe 2.2.2 NIST SP 800-61), bei der mit der Dringlichkeit *Low* gekennzeichnete Anforderungen lediglich ein indirekter Einfluss auf Incident Handling angegeben wird. [6, S.

10] Dennoch wurde die Entscheidung getroffen, einzelne dieser Controls auch aufzunehmen, da sie entweder in anderen Werken ebenso oder ähnlich genannt wurden oder sie Entscheidungen im Incident Handling, besonders in der Rolle der externen Beratung, maßgeblich beeinflussen. Die identifizierten Anforderungen werden in einer der Arbeit beigelegten Tabelle nach Kategorien sortiert, ihrer Quelle zugeordnet und systematisiert.

Neben allgemeinen Kapiteln wurden alle Anforderungen auf die Phasen des Prozesses nach ISO 27035 (siehe 2.2.1 ISO 27035) gemappt. Somit ergeben sich teilweise andere Einordnungen, als sie in NIST und den Criticial Security Controls (siehe 2.2.3 CIS Controls) getroffen werden. Das folgende Unterkapitel ist in die Phasen des Prozessmodells nach ISO 27035 (Plan and Prepare, Detect and Report, Assess and decide, Respond, Learn lessons) geteilt. Zusätzlich finden sich Unterkapitel für die in der ISO 27035-Reihe als phasenübergreifende Aufgaben genannten Aufgaben Dokumentation und Reporting, Kommunikation und Koordination. Allgemeine Anforderungen des Prozesses, die notwendigen Rollen und Verantwortlichkeiten sowie Termini und eine Beschreibung des Wesens der Standards führen in das Kapitel ein.

Wesen der Standards

ISO beschreibt im Kapitel 4 der 23035-1 verschiedene Grundlagen zur Bearbeitung von IT-Sicherheitsvorfällen. Diese bilden das „Wesen“ der Standards und beschreiben beispielsweise die Vorteile und Ziele des strukturierten Security Incident Managements. [9, Kap. 4.2 bis 4.3] Die Grundlagen müssen den zukünftigen Incident Handlern näher gebracht werden, damit diese die Möglichkeiten der Standards kennen und sie gezielt einsetzen können.

Weiters werden auch die Merkmale und verschiedenen Arten von Security Incidents beschrieben. Neben der Unterscheidung zwischen absichtlich, unabsichtlich und durch Umwelteinflüsse verursachten Security Incidents wird auch eine Differenzierung zwischen technischen und nichttechnischen Sicherheitsvorfällen vorgenommen. Die Kenntnis der verschiedenen Charakteristiken ist insbesondere in der Vorbereitungsphase und für die Anwendbarkeit der ISO 27035 von besonderer Bedeutung und muss deshalb als Grundlagenwissen von den Incident Handlern beherrscht werden. [9, Kap. 4.1]

Termini

Wie bereits in Kapitel 2.1 Begrifflichkeiten und zentrale Konzepte der Arbeit herausgearbeitet wurde, sind einheitliche Termini die Basis für eine gelingende Kommunikation ohne Missverständnisse.

Auch CIS fordert die Etablierung einer *common language* innerhalb der Organisation oder eines Zusammenschlusses an solchen, also die Schaffung von Definitionen, die einheitlich nicht existieren beziehungs-

weise organisationsabhängig andere Bedeutungen haben können. So soll beispielsweise festgelegt werden, wann ein *security incident* auch als solcher bezeichnet werden soll und wann zutreffender von einer *security vulnerability* oder einer *abnormal activity* gesprochen werden soll. [34, Safeguard 17.9]
Darüber hinaus werden in ISO 27035 verschiedenste Termini eingeführt und definiert. Beispielsweise wird ein Unterschied zwischen Incident Reponse und Incident Handling definiert, der in anderen Werken wie NIST SP 800-61 nicht vorkommt (siehe 2.1.2 Begriffsabgrenzung Incident Handling - Incident Response - Security Incident Management).
Auch andere Differenzierungen, die zu allgemeinem Wissen in der IT-Sicherheitsbranche zählen, beispielsweise die Unterscheidung zwischen einem Security Incident und einem Security Event, werden getroffen. Diese werden aber in anderen Lehrveranstaltungen, die als Voraussetzung für diese gelten, gelehrt (siehe 5.2 Didaktische Überlegungen). [9, Kap. 3.1.4 bis 5, 4.1, 5.5]
Der Incident Handler muss daher wissen, dass Definitionen zwischen Organisationen nicht zwingend einheitlich gestaltet sein müssen und, damit es zu keinen Missverständnissen kommt, diese gegebenenfalls kritisch hinterfragen.
Weiters werden verschiedene Teams und Rollen mit unterschiedlichen Funktionen in ISO 27035 beschrieben und definiert. [9, Kap. 3.1.1 bis 3] Diese Rollenbeschreibungen muss der Incident Handler kennen, um ihre typischen Tätigkeitsfelder und Entscheidungskompetenzen zu kennen. Im folgenden Kapitel wird genauer auf diese eingegangen.

Personal, Rollen und Verantwortlichkeiten

Sowohl ISO, als auch NIST und CIS fordern die Zuweisung von Rollen und Verantwortlichkeiten für das Incident Handling. [34, Safeguard 17.5], [9, Kap. 4.5.3], [6, GV.RR-01 bis 02] Während NIST eher unspezifisch bleibt, welche Rollen genau durch welche Personen zu besetzen sind und nur beschreibt, dass diesen die notwendigen Rechte zur Erfüllung ihrer Aufgaben zuzusprechen sind und die Rollen zu dokumentieren sind [6, GV.RR-02], sprechen sowohl ISO 27035 als auch CIS Controls spezielle Tätigkeitsfelder an. [9, Kap. 4.5.3 e) bis i)], [34, Safeguard 17.5] Dabei fällt die unterschiedliche Zielgruppe der Werke auf. Während CIS-Controls fordert, dass Personal unter anderem der Bereiche Legal, Information Security, IT, Public Relations und Human Resources ihre Rollen im Incident Handling haben müssen [34, Safeguard 17.5], spricht ISO explizit von spezialisierten Teams, beispielsweise einem Change Management-, einem Vulnerability Management-, oder einem Awareness and training-Team. [9, Kap. 4.5.3 e) bis i)] Diese Teams sind aber vermutlich nur in großen Enterprises wirklich vorhanden und müssen in kleineren Unternehmensumfeldern auch oft in Personalunion erledigt werden. Ein Incident Handler in leitender Funktion, zum

Beispiel als Incident Koordinator, muss daher alle notwendigen Rollen und Verantwortlichkeiten kennen, deren Auslastung in verschiedenen Phasen des Security Incidents abschätzen und Aufgaben der richtigen Rolle zuweisen können.

ISO unterscheidet im Gegensatz zu den anderen beiden Werken eine Aufteilung in zwei Teams: ein Incident Management Team (IMT) und ein Incident Response Team (IRT). Während das IMT den Sicherheitsvorfall über den gesamten Lifecycle hinweg leitet, hat das IRT die Aufgabe, Root Causes des Security Incidents zu erkennen, die Evidenzen zu verwalten, zu analysieren und auf den Angriff zu reagieren. [9, Kap. 4.5.3 d)] [29, Kap. 7.3.2] Der Aufbau dieser Teams ist beispielhaft in der Norm angegeben, kann aber durch die Organisationen frei angepasst werden. [29, Kap. 7.2.2, Kap. 7.3.1]

CIS fordert die Benennung einer Person und zumindest eines Stellvertreters, die für Incident Handling verantwortlich sind. Dieses „Managementpersonal soll für die Koordination und Dokumentation von Incident Response und Recovery-Bemühungen“ [34, Safeguard 17.1] zur Verfügung stehen. [34, Safeguard 17.1] Es lassen sich dabei durchaus gewisse Parallelen zu den Anforderungen aus ISO 27035 ziehen, das für diese Aufgaben das oben beschriebene IMT definiert. [9, Kap. 4.5.3 a)], [29, Kap. 7.2.1] Zusätzlich beschreibt ISO auch die Rolle eines Incident Koordinators, der unter anderem das Ausrufen des Security Incidents sowie die folgende Aktivierung und Koordinierung des Incident Response Teams verantwortet. [9, Kap. 4.5.3 b)] Je nach vorhandener Struktur im Unternehmen muss der Incident Handler in der Lage sein, die typischen Aufgaben der Rollen zu verstehen und, sofern diese noch nicht etabliert sind, diese ad hoc während des Security Incidents zu implementieren.

Diese Anforderungen stellt auch NIST im Bereich der Governance. Diese sind zwar nicht direkt Teil von Incident Readiness, deren Vorhandensein ist aber die Grundlage für andere, weiterführende Maßnahmen. So wird beispielsweise in der Beschreibung des Themenkomplexes Governance - Roles and Responsibilities angemerkt, dass im Rahmen der definierten Cybersecurityrollen und Verantwortlichkeiten auch Incident Handling berücksichtigt werden muss. [6, GV.RR] Zusätzlich ist es notwendig, dass das Management der Organisation eine „risikobewusste, ethische und [sich] kontinuierlich verbessernde“ [6, GV.RR-01] Umgebung schafft. [6, GV.RR-01] Diese beiden Anforderungen müssen vor dem Auftreten eines Security Incidents erfüllt sein; ein grundlegendes Design von Verantwortlichkeiten gehört weder zum Aufgabenprofil eines Incident Handlers, noch kann es in der gebotenen Zeit konzipiert und implementiert werden. Der Incident Handler muss diesen Missstand aber erkennen und damit umgehen können, wenn diese Voraussetzungen nicht oder nur in einem geringen Reifegrad in der Organisation implementiert sind und in der Plan and prepare- oder der Learn lessons-Phase Verbesserungsvorschläge formulieren und begründen können.

Allgemeine prozessbezogene Anforderungen

Alle analysierten Werke stellen einen Prozess zur Vorbereitung, Behandlung und Nachbereitung eines Security Incidents auf. Dabei betonen aber sowohl ISO als auch NIST, lediglich eine Hilfestellung zur Bewältigung zu sein. Die passenden Methoden und Entscheidungen müssen daher situativ und organisationsabhängig getroffen werden (siehe 2.2 Standards und Normen). CIS beschreibt dies, vermutlich aufgrund der Vereinfachung für Organisationen mit geringem Sicherheitsgrad, nicht, sondern spricht davon, dass ein Prozess mit Rollen und Verantwortlichkeiten und einem Kommunikationsplan notwendig sei. [34, Safeguard 17.4] Diese Grundlagen sind für Incident Handler von zentraler Wichtigkeit, damit die Vorschläge nicht als Vorgaben interpretiert oder gar blind implementiert werden.

Auch die Verbindung des Prozesses und des Themas Incident Handling allgemein in andere Sicherheitsprozesse und Aktivitäten, beispielsweise das Business Continuity Management, muss einem Incident Handler bewusst sein, da bei der Planung von maximalen Wiederherstellungszeiten (RTO) auch die Response-Zeit inkludiert sein muss. [9, Kap. 5.2]

Darüber hinaus ist wichtig zu bedenken, dass einige Prozessaktivitäten, beispielsweise die Dokumentation oder die Koordination, phasenübergreifende Tätigkeiten sind. [9, Kap. 5.1] Dies muss durch den Incident Handler beachtet, durchgeführt und ständig überprüft werden.

Auch einige Zeitansätze, beispielsweise sofort nach Kenntniserlangen zu setzende Aktivitäten, sind beschrieben. Darunter fallen unter anderem die Kommunikation, aber auch die Eskalation und die Benachrichtigung von internen Ressourcen. [9, Kap. 5.2] Diese Zeitansätze sind insbesondere für die Priorisierung gewisser Aufgaben für den Incident Handler von besonderer Bedeutung.

Prozess – Phase Plan and prepare

Das Center of Internet Security beschreibt in Kapitel 17 der Critical Security Controls eine Vielzahl an Prozessen und Strukturen, die als Grundvoraussetzung für funktionierendes Incident Handling benötigt werden. In Unternehmen, in denen Incident Handling bereits etabliert ist, kommt den Mitarbeiter:innen allenfalls die Verbesserung, oftmals im Rahmen von Lessons Learned nach einem Sicherheitsvorfall, zu. In Unternehmen, die ihre Incident Handling-Fähigkeiten aber gerade erst aufbauen, nicht zuletzt aktuell aufgrund der Vorgaben der NIS 2-Richtlinie der Europäischen Union, können diese Aufbaumaßnahmen notwendig sein. [27, Art. 21, Abs. 2, Z b]

Die notwendigen Aktivitäten in der Plan and prepare-Phase sind daher vielfältig und lassen sich meist in eine von fünf Gruppen einteilen. Sie dienen entweder der organisatorischen Vorbereitung im Bereich der

Prozesse oder des ISMS, der technischen Vorbereitung, dem Üben von Security Incidents, dem Verstehen der Organisation sowie deren Ziele und Wertschöpfungskette oder dem Identifizieren von Assets und Risiken. Die in diesen Gruppen enthaltenen Tasks und vorbereitende Tätigkeiten werden im Folgenden aufgelistet und näher beschrieben.

Organisatorische Anforderungen

1. In den CIS Controls 17.1 bis 17.3, die jeweils der Implementation Group 1 zuzuordnen sind und somit nach Dafürhalten des CIS Maßnahmen der „basic cyber hygiene“ [34, S. 5] darstellen, wird im Bereich der organisatorischen Vorbereitung neben der Vorhaltung von ausreichend Personal und der Zuweisung der Hauptverantwortlichkeit für das gesamte Incident Handling auch ein Prozess zur Meldung von Sicherheitsvorfällen für das eigene Personal gefordert. [34, Safeguard 17.1, 17.3] Auch ISO fordert in der Phase Plan and Prepare verschiedenste Prozesse, Policies und Konzepte, die für das Incident Handling von Bedeutung sind. [9, Kap. 5.1] Derartige Vorbereitungsmaßnahmen muss der Incident Handler einerseits kennen, um darauf aufbauend im Security Incident arbeiten zu können, andererseits muss er die vorliegenden Konzepte auch erstellen oder verbessern können, sollten diese nicht im notwendigen Reifegrad vorliegen.

2. Auch im Bereich der Kommunikation (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation) und des Informationsaustausches sind einige Vorbereitungen zu treffen. Insbesondere das Herstellen und Sammeln von Kontakten, beispielsweise interner Stellen wie Vertreter der IT, Legal HR oder PR [29, Kap. 8.2], aber auch von Behörden [29, Kap. 8.3] oder Cyberversicherungen, ist von Bedeutung. [34, Safeguard 17.2], [29, Kap. 8.1] Interne Kommunikation ist aber nicht nur innerhalb des CSIRT, sondern auch von allen Benutzer:innen der Organisation ausgehend notwendig – nämlich bei der Meldung eines Security Incidents. Diese Meldestelle (*Point of Contact*) soll Security Incidents zentral aufnehmen und diese anschließend an die zuständige Stelle weiterleiten (siehe 5.1.1 Prozess – Phase Detect and report). [9, Kap. 5.3], [30, Kap. 7.1] Somit muss der Incident Handler nicht nur kommunikativ sein, er muss auch alle für einen Informationssicherheitsvorfall wichtigen Kontaktstellen kennen, diese möglicherweise intern etablieren und mit internen und externen Partnern in Austausch bleiben.

Eine besondere Art von Informationsaustausch stellt das Erhalten und Teilen von Threat Intelligence dar. [6, ID.RA-02] Diese Informationen sind im Falle eines Security Incidents zur Ursachenforschung und Attribuierung des Angriffes von besonderer Wichtigkeit und sollten dem Incident Handler daher bekannt sein.

3. Zusätzlich sind Etablierungsmaßnahmen für Controls auch in den Safeguards 17.4 bis 17.6, die die Erstellung und Wartung eines Incident Handling Prozesses, das granularere Zuweisen von Rollen und Verantwortlichkeiten und das Definieren von Kommunikationswegen, jeweils für den Fall eines Sicherheitsvorfalles, fordern, vorhanden. All diese Maßnahmen sind der Implementation Group 2 durch die CIS zugeordnet und

stellen somit erweiterte Maßnahmen dar. Es kann aufgrund dieser Zuordnung auch davon ausgegangen werden, dass einige dieser Maßnahmen nicht oder nicht ausreichend gut in Unternehmen implementiert sind. [34, Safeguard 17.4 bis 17.6] Die Umsetzung oder Optimierung dieser Safeguards kann daher eine Aufgabe für eine:n Expert:in im Bereich Incident Handling sein.

4. ISO fordert insbesondere im Bereich des Informationssicherheitsmanagementsystems (ISMS) Anpassungen für das Incident Handling. [29, Kap. 5.2] Neben dem bereits beschriebenen Information Security Incident Management Plan werden hier auch Flow-Pläne für verschiedene Arten von Incidents gefordert [29, Kap. 6.1], womit die Vorbereitung von Playbooks gemeint ist. Es ist jedoch nicht sinnvoll, für jede Art von Attacke einen genauen Reaktionsplan zu konzipieren, da diese Arbeitsschritte zeit- und daher kostenaufwendig sind. Für typische und oft auftretende Security Incidents kann dies aber die Reaktionszeit reduzieren. [29, Kap. 6] Diese Pläne müssen vom Incident Handler in der Vorbereitungsphase geschrieben und an die Organisation und deren Voraussetzungen angepasst werden können.

5. Vor dem Design von Prozessen ist eine strukturierte Erhebung der Anforderungen und Rahmenbedingungen wichtig. Dazu zählen neben den vorhanden Skills im Incident Response Team (IRT) auch alle notwendigen Daten, die in einem nach einem Sicherheitsvorfall zu erstellenden Security Incident Report erwartet werden, oder Workarounds beim Ausfall businesskritischer Assets sowie Entscheidungswege. [29, Kap. 6.7] Diese Daten müssen vom Incident Handler berücksichtigt oder erfragt werden, bevor dieser Prozesse erstellt.

6. Um in der Phase Detect and report eine Klassifikation des Security Incidents durchführen zu können, ist es selbstredend davor notwendig, eine Klassifikationsskala zu definieren. Dies muss abhängig von der Organisation durch den Incident Handler in der Vorbereitungsphase durchgeführt werden.

7. Auch eine Sensibilisierung über die Wichtigkeit von strukturiertem Incident Handling sollte vorgenommen werden. [29, Kap. 10] Für den Incident Handler ist es somit wichtig zu wissen, welche Informationen für bestimmte Gruppen, beispielsweise Management, Endbenutzer oder IT, von Bedeutung sind und derartige Kampagnen rudimentär zu gestalten.

8. Incident Handling benötigt Informationen und Prozesse. Im Rahmen der Vorbereitung sind deshalb verschiedene Dokumente, Listen oder Systeme notwendig. Neben Kommunikationsprozessen und Anweisungen für das Krisenmanagement zählen insbesondere aktuelle Assetlisten [29, Kap. 9.1] oder der Zugang zu Systemen, die solche Informationen beinhalten, dazu. Der Incident Handler muss Bescheid wissen, welche Informationen zur Lösung eines Security Incidents benötigt werden und dafür sorgen, dass diese jederzeit in einer aktuellen Version vorliegen.

9. Eine Möglichkeit zur Erkennung von Incidents sind Meldungen von externen Personen (siehe 5.1.1 Pro-

zess – Phase Detect and report), sogenannte *Vulnerability Disclosures*. Diese müssen ebenfalls über einen Prozess standardisiert abgearbeitet werden. Die Bedeutung dieser Reports und die Berücksichtigung dieser Quelle ist für den Incident Handler von Relevanz.

10. Um eine Verbesserung auch außerhalb von Security Incidents und Übungen zu gewährleisten, sollte außerdem ein Incident Response Capability Monitoring vorgenommen werden, in welchem Sicherheitsvorfälle analysiert und so fehlende Capabilities, egal in welchem Bereich, erkannt werden. [29, Kap. 11.3] Dieser Vorgang setzt nicht nur ein breites Wissen über die eingesetzten Security Controls in der Organisation, sondern auch Wissen über die Branche und Zugang zu entsprechenden Bedrohungsinformationen voraus.

11. Für jede Phase listet ISO 27035-2 weitere Überlegungen auf, die in der Vorbereitung angestellt und dokumentiert werden sollten. Beispielhaft werden im Folgenden die Phasen und mögliche Überlegungen dargestellt:

- Plan and prepare: Prozeduren über das Dokumentieren von Sicherheitsvorfällen oder Eskalationsprozesse [29, Kap. 6.4 a)]
- Detect and report: Vorgehensweisen zur Sammlung weiterer Informationen zu einem Event [29, Kap. 6.4 b)]
- Assess and decide: Sammlung wichtiger Informationen zur Entscheidungsfindung [29, Kap. 6.4 c)], Scoring von Bedrohungen, Schwachstellen und Impact [6, ID.RA-05]
- Respond: Prozess der Informationssammlung durch den Incident Manager oder Klassifikationen [29, Kap. 6.4 d)]
- Learn lessons: Prozess zur strukturierten Aufarbeitung von Verbesserungen oder Integration ins Change Management [29, Kap. 6.4 e)]

All diese Fragestellungen und hilfreiche Dokumentationen müssen einem Incident Handler, sofern er auch in der Vorbereitung beratend tätig sein soll, bekannt sein.

Technische Anforderungen

Technisch sind für das Incident Handling insbesondere einige Supportfunktionen notwendig, die die spätere Analyse oder das Detektieren von Sicherheitsvorfällen, beispielsweise mit einem IDS/IPS, oder das Response Procedure, zum Beispiel mit einem EDR, unterstützen. [29, Kap. 9.2] Der Incident Handler muss diese Funktionen einerseits kennen, um ihren Nutzen im Security Incident ausspielen zu können, andererseits muss er aber auch in der Lage sein, die notwendigen Funktionen, sofern sie beim Auftreten des Sicherheitsvorfalles noch nicht implementiert sind, rasch auszurollen, um beispielsweise eine Visibilität aller Clients herzustellen.

Üben von Security Incidents

In den Safeguards 17.7 fordert CIS die regelmäßige, zumindest jährliche Durchführung von Incident Handling-Übungen für das Schlüsselpersonal. Darin soll neben der Nutzung von (alternativen) Kommunikationskanälen auch das Treffen von Entscheidungen beübt werden. [34, Safeguard 17.7] Dabei kann sowohl ausschließlich intern, als auch in Verbindung mit externen Partnern geübt werden. [29, Kap. 11.1] Leitende Mitarbeiter:innen im Bereich Incident Handling sind somit unter Umständen neben der Teilnahme an den Übungen auch mit der Organisation solcher Übungen, gegebenfalls unter Zuhilfenahme eines externen Partners, beauftragt.

Verstehen der Organisation, ihrer Ziele und der Wertschöpfungskette

Insbesondere, wenn Incident Handler als externe Dienstleister auftreten, müssen sie zunächst danach trachten, die Organisation, ihre Ziele, die Wertschöpfungskette und das ISMS zu verstehen. Zusätzlich sind auch die Erwartungen der Stakeholder und rechtliche oder vertragliche Verpflichtungen von besonderem Interesse. [6, GV.OC, GV.OC-01 bis 03] Insbesondere sind für die Lösung des Security Incidents auch für die Organisation kritische Ziele und Dienste zu identifizieren. Dies wird umso bedeutsamer, je mehr oder kritischere externe Stakeholder von diesen Services abhängen. [6, GV.OC-04 bis 05] Diese Informationen sind für den Incident Handler auch für alle folgenden Phasen von besonderer Bedeutung, da sie Prioritäten beträchtlich verschieben können.

Weitere wichtige Informationen, die einen Einfluss auf die folgenden Phasen haben können sind unter anderem Risikomanagementaktivitäten und -prozesse [6, GV.RM-03], auch im Hinblick auf den Risikoappetit und die -toleranz [6, GV.RM], insbesondere in der Supply Chain [6, GV.SC-05], vorhandene Rollen und Verantwortlichkeiten im Risikomanagement der Organisation [6, GV.SC-02] und Erwartungen an das Incident Handling. [6, ID.RA-07]

Identifizieren von Assets und Risiken

Ein gut aufgebautes und definiertes Risikomanagementsystem und eine Übersicht über alle Unternehmenssassets unterstützt Incident Handling auf mehreren Ebenen. Neben einer Übersicht an bekannten Risiken, für die unter Umständen bereits mitigierende Maßnahmen vorhanden oder geplant sind [6, S. ID], unterstützen standardisierte Risikoberechnungsmethoden die Priorisierung von Systemen zur Wiederherstellung. [6, GV.RM-06] Hardware-, Software-, Service- und Dateninventare geben Auskunft über genutzte Systeme, Programme und Informationen [6, ID.AM, ID.AM-01, ID.AM-07], eine Priorisierung dieser Assets gibt einen Hinweis auf die Wiederherstellungsreihenfolge. [6, GV.RM-06] Diese kurze, unvollständige Aufzählung der Risiko- und Assetmanagementmaßnahmen der NIST SP 800-61 zeigt deutlich die Verbindungen dieser beiden Disziplinen in das Incident Handling und die Abhängigkeit von Asset Management. Somit ist

ein Grundverständnis dieser Disziplinen für den Incident Handler von besonderer Wichtigkeit.
Viele der Controls in diesem Bereich sind technische Vorgaben, die oftmals eigentlich dem IT-Betrieb zuzuordnen sind. Diese wurden in der Arbeit nicht weiter beschrieben, um den Rahmen nicht zu sprengen. Möglicherweise muss ein externer Incident Handler diese aber auch ad hoc bei einem Sicherheitsvorfall implementieren, um eine Visibilität über die möglicherweise betroffene IT-Infrastruktur zu erlangen. Diese Inhalte werden aber bereits von anderen Lehrveranstaltungen auf der Fachhochschule St. Pölten behandelt (siehe 2.3.2 Curriculare Vorgaben an der Fachhochschule St. Pölten).
Die Bausteine der Funktion *Protect* wurden in dieser Arbeit vollständig ausgelassen. Diese Maßnahmen sollen Assets schützen und Security Incidents damit verhindern. Wenngleich die Planung und Ausrollung dieser Maßnahmen auch im Recovery-Bereich im Rahmen einer Architektenrolle auf einen Incident Handler zukommen können (Interview B.1), würden diese Controls den Rahmen der Arbeit sprengen, da ein Fokus auf organisatorische Aspekte gelegt wurde. Darüber hinaus werden diese Thematiken und deren korrekte Implementierung an der Fachhochschule St. Pölten in nahezu allen anderen technischen Lehrveranstaltungen behandelt. [63] Eine Wiederholung im Bereich Incident Handling scheint deshalb nicht notwendig.

Prozess – Phase Detect and report

ISO teilt Detect and report in zwei Subphasen, die Detektion, also das Erkennen, und das Reporting, also das Melden des vermuteten Security Incidents. [30, Kap. 5.2] Da diese Phase zum Großteil technisch geprägt ist, werden in dieser Arbeit nur jene technischen Controls angegeben, die zum Verstehen des Prozessschrittes von Nöten sind.
Zu den möglichen Quellen zur **Detektion** eines Security Incidents zählen neben technischen Mitteln wie IDS und IPS, Endpoint Security Lösungen oder SIEM-Systemen auch Personen, also interne oder externe Benutzer oder Kunden. Auch durch organisatorisch implementierte Quellen wie die IT-Abteilung, den Help Desk oder ein vorhandenes SOC können Events erkannt werden. [30, Kap. 7.2] Da jedes Security-System andere Schwerpunkte setzt und andere Daten sammelt, müssen die Informationen aus verschiedenen Quellen zusammengeführt und korreliert werden. [6, DE.AE-03] Das Wissen über diese Quellen ist für einen Incident Handler von besonderer Wichtigkeit, da er über diese möglicherweise noch weitere Informationen über ein Security Event erlangen kann. Diese Informationen müssen anschließend dem Incident Handling Team verfügbar gemacht werden, um diese tiefergehend zu analysieren.
Typische Aktivitäten der Phase umfassen das genaue Monitoring der Systeme, das Sammeln von Informationen über das verdächtige Security Event und die Sammlung von Situational Awareness. [9, Kap. 5.3] Das Monitoring soll neben Anomalien und Indicators of Compromise auch andere, möglicherweise feindliche

Security Events erkennen. Idealerweise werden die Events auch mit Threat Intelligence angereichert, um sie besser in Kontext setzen zu können. [6, DE.AE-03], [6, S. CM] Neben dem Monitoring von Systemen ist auch das Netzwerkmonitoring und das Monitoring der physischen Sicherheit, beispielsweise von Zutrittssystemen oder Verhaltensweisen von Bedeutung. [6, DE.CM-01 bis 03] All diese Daten müssen auch für die Aktivitäten externer Dienstleister sichergestellt werden. [6, DE.CM-06] Insbesondere das weiterführende Monitoring des alarmauslösenden Systems ist von besonderer Wichtigkeit. Daneben stellen Recherchen über ähnliche Events oder Cyber Threat Intelligence (CTI) Informationen einen Mehrwert dar. [30, Kap. 7.2] Der Incident Handler muss hierbei die beschriebenen Ziele und Möglichkeiten von Monitoring und den Vorteil von Kontextschaffung durch weitere Quellen, beispielsweise CTI, kennen, um sie im Security Incident nutzen zu können. Darüber hinaus ist das Wissen auch in der Konzeption von Monitoringsystemen in der Phase Plan and Prepare für den Incident Handler von Bedeutung.

Das Monitoring kann dem Incident Handler auch bei einer Einschätzung über das Schadensausmaß beziehungsweise in weiterer Folge einer Analyse des solchen helfen [6, DE.AE-04], weshalb dieser über die Möglichkeiten von SIEM- oder SOAR-Systemen Bescheid wissen muss.

ISO beschreibt darüberhinausgehend verschiedenste Möglichkeiten, Security Incidents proaktiv zu erkennen. Neben Honeypots und Sandboxes werden auch viele weitere Möglichkeiten wie IDS und IPS, Passive DNS Monitoring oder eine Firewall mit Netflow-Daten genannt. Zusätzlich können auch externe Threat Feeds mit Indicators of Compromise erworben und in vorhandene Sicherheitslösungen integriert werden. [30, Kap. 7.3.1] Diese Daten dienen auch dazu, die bereits vorhandenen Erkenntnisse in Kontext zu setzen (Situational Awareness) [30, Kap. 7.3.2] und sind für den Incident Handler auch nach einem bereits erkannten Security Incident von besonderer Bedeutung, da dadurch möglicherweise Ausbreitungsversuche des Angreifers (unter anderem durch Lateral Movement) erkannt werden können.

Dem gegenübergestellt werden reaktive Erkennungsmöglichkeiten beschrieben, die einen bereits vorgefallenen Security Incident erkennen sollen. Darunter fallen neben Reports von Benutzern [30, Kap. 7.3.4], [34, Safeguard 17.3] auch beispielsweise Alarme eines IDS. [30, Kap. 7.3.4] Incident Handler müssen die Quellen reaktiver Erkennung verstehen, um die richtigen Schlüsse für die folgende Analyse zu ziehen.

Das **Reporting**, also die Meldung, besteht aus drei Phasen: Der Incident Notification (Meldung von einem erkennenden System oder User zum Point of Contact), dem internen Reporting (vom CSIRT zu internen Stellen) und dem externen Reporting (vom CSIRT zu Behördern oder Partnern). [30, Kap. 8.1] Für die erste Phase sollten standardisierte Formulare genutzt werden, um die Informationen einheitlich aufzunehmen und keine wichtigen Details zu vergessen. Im Idealfall werden an dieser Stelle auch bereits Indicators of Compromise angegeben, um eine notwendige Investigation rascher beginnen zu können. [30, Kap. 8.1]

Die Erstellung oder Verbesserung eines solchen Formulars sowie die Arbeit damit in der Aufnahme von Meldungen ist eine Aufgabe eines Incident Handlers.
Die zentrale Einmeldestelle für Incidents wird in den ISO-Normen Point of Contact (PoC) genannt. Je nach Aufbau und Aufgaben dieses PoC muss dieser unterschiedliche Vorgaben erfüllen. Ist beispielsweise ein PoC weltweit zuständig, so weichen die Anforderungen an Verfügbarkeit und eine klare Rollendefinition klar von einem Modell ab, bei denen es mehrere PoCs mit unterschiedlichen Zuständigkeitsbereichen gibt. Gemein haben aber alle PoCs, dass die aufnehmende Person oder ein Vorgesetzter dessen nach der Meldung eine initiale Klassifizierung des Security Incidents vergeben. [30, Kap. 8.2.4, Kap 8.3] Dem Incident Handler müssen die Aufgaben und die verschiedenen Implementierungsmöglichkeiten von PoCs bekannt sein, um diese im Bedarfsfall rasch aufbauen beziehungsweise optimieren zu können.

Prozess – Phase Assess and decide

Die Phase Assess and decide ist abermals in zwei kleinere Subphasen unterteilt, die Triage und die Analyse. [30, Kap. 5.2]
Nach der Erkennung und Meldung eines verdächtigen Events in der vorherigen Phase Detect and report folgt die **Triage**. [6, RS.MA-02], [30, Kap. 9.1] „Triage ist der Prozess des Sortierens, Kategorisierens, Korrelierens und Priorisierens und der Zuweisung einlangender Events, Incident Reports, Vulnerability Reports und anderer Information Requests“ [30, Kap. 9.1] In dieser erfolgt typischerweise die Korrelation mit anderen Reports, einer Analyse des Business Impacts und eine Priorisierung anhand verschiedener Merkmale, beispielsweise ob Lebensgefahr besteht oder kritische Infrastruktur betroffen ist. Anschließend wird das priorisierte Event zur tiefergehenden Analyse mit Informationen angereichert an einen Analysten weitergeleitet. [30, Kap. 9.2] Neben den Begrifflichkeiten ist für einen Incident Handler von Bedeutung, welche Investigationsschritte in welcher Reihenfolge zu tätigen sind.
Nach dem ersten Assessment ist die wichtige Entscheidung *Security Incident or not?* zu treffen. [30, Kap. 5.4] NIST beschreibt, dass es definierte Kriterien geben muss, wann ein Security Incident als socher zu definieren und einzustufen ist. [6, DE.AE-08] Bei Treffen der Entscheidung *Kein Incident* wird für gewöhnlich keine weitere Investigation durchgeführt. Derartige Entscheidungen haben also eine weitreichende Tragweite, derer sich der Incident Handler in seiner Entscheidung bewusst sein muss.
Nach den ersten Assessments muss der Sicherheitsvorfall kategorisiert und priorisiert werden. Dazu wird diesem ein Incident-Typ (beispielsweise Data Breach oder Ransomware) vergeben. [34, Safeguard 17.8], [6, RS.MA-03] Je nach Dringlichkeitseinstufung folgt daraus eine Response Strategie, bei der zwischen den Reaktionsmöglichkeiten *Investigieren und Beobachten des Angreifers* und *rasche Wiederherstellung* abge-

wogen werden muss. [6, RS.MA-03] Im Idealfall erfolgt dies durch eine Risikoabschätzung mit festgelegten Faktoren. [6, RS.MA] Die Möglichkeiten und die Bedeutung von Kategorisierungen und Priorisierungen von Security Incidents müssen dem Incident Handler bekannt sein, da dieser sie nicht nur vornehmen, sondern auch mit den Folgen der Entscheidung arbeiten muss.

Die erste getroffene Priorisierung ist aber keineswegs unumstößlich. Je nach Fortschritt und Ergebnissen in der Analysephase kann der Security Incident auch jederzeit eskaliert oder hochgestuft werden. Dies hat meist zur Folge, dass mehr Zeit- oder Personalressourcen in die Lösung dieses Sicherheitsvorfalles fließen oder der Vorfall an höhere Managementebenen weitergeleitet wird. [6, RS.MA-04] Der Incident Handler muss sich darüber im Klaren sein, um so besonders relevante Sicherheitsvorfälle rechtzeitig hochzustufen.

In der nun folgenden **Analyse** werden Fragestellungen zum Security Incident beantwortet. Während ISO als Leitfragen W-Fragen (Was ist das Problem? Wer ist betroffen? Wie weit verbreitet ist das Problem? Welchen Impact hat das Problem?) beschreibt [30, Kap. 10.2], fokussiert NIST hauptsächlich auf den Root Cause des Security Incidents und schlägt vor, eine Zeitleiste von relevanten Events aufzustellen und die dahinterliegenden Schwachstellen, systematischen Fehler und Bedrohungsakteure zu ermitteln. [6, RS.AN, RS.AN-03]

Zunächst müssen dafür so rasch wie möglich die Auswirkungen auf die Organisation und die Reichweite festgestellt werden. Dies ist nicht nur von besonderer Bedeutung, sondern auch von besonderer Schwierigkeit, da kein betroffenes oder kompromittiertes System übersehen werden darf. NIST bezeichnet diese Aufgabe als „one of the most challenging aspects of incident response“ [6, RS.AN-08]. Dessen muss sich der Incident Handler bewusst sein und besonderes Augenmerk auf eine angemessen tiefe und vollständige Visibilität im Netzwerk legen.

In der Analyse werden die durch das kontinuierliche Monitoring erhobenen Events auf möglicherweise feindselige Aktivitäten untersucht. Aufgrund der Vielzahl an verschiedenen Security Incidents sind einige davon sehr einfach, andere nur mit tiefem technischen Verständnis zu erkennen. [6, DE.AE] Für die Analyse wird daher neben verschiedenen Tools wie SIEM- oder SOAR-Systemen abermals, wie bereits in 5.1.1 Prozess – Phase Detect and report beschrieben, Cyber Threat Intelligence genutzt. [6, DE.AE-02] Diese muss, neben anderen Informationsquellen wie Assetlisten und Vulnerability Disclosures, in die Analyse integriert werden, um alle Informationen zu kontextualisieren und somit besser einordnen zu können. [6, DE.AE-07] Der Nutzen von mit weiterem Wissen angereicherten Informationen muss dem Incident Handler bekannt sein, damit er diese Ergänzungen an den richtigen Stellen fordert.

ISO erklärt, dass auf verschiedenen Systemtypen, beispielsweise einem Desktopcomputer oder einem Server, unterschiedliche Artefakte relevant sind. So sind zum Beispiel auf einem Desktop neben einer Ana-

lyse der Registry auch Benutzer und Gruppen sowie mögliche Schadprogramme von Relevanz. Durch die Vielzahl an Analysemöglichkeiten ist aber auch diese in weitere Subschritte und Fachbereiche aufteilbar, beispielsweise die Systemanalyse, Netzwerkanalysen oder auch Malwareanalyse. [30, Kap. 10.1] Dem Incident Handler müssen somit nicht nur die auf einem System vorfindbaren Evidenzen, sondern auch deren Analyseaufwand und Wert in der Analyse bekannt sein, um die Analyseschritte richtig zu priorisieren und den Zeitaufwand realistisch abschätzen zu können.

Alle Analyseschritte und -handlungen müssen entweder handschriftlich, digital oder automatisiert dokumentiert werden und sind geheim zu halten, da diese vertrauliche Informationen über den aktuellen Wissensstand und mögliche Ursachen des Security Incidents enthalten. [6, RS.AN-06] Auch im Sinne eine späteren Nachvollziehbarkeit ist es wichtig, dass die Dokumentationen durch den Incident Handler vollständig und ordentlich geführt werden.

Selbiges gilt auch für gesammelte Daten und Evidenzen. Sollten diese, was mangels Ermittelbarkeit oder Greifbarkeit der Tätergruppierungen nur in seltenen Fällen vorkommt, vor Gericht Verwendung finden, so ist eine saubere Chain of Custody, also eine Beweismittelkette, mit der nachvollzogen werden kann, dass die Beweismittel nicht verändert wurden, wichtig. Die Bedeutsamkeit einer solchen lückenlosen Aufzeichnung ist somit direkt mit dem Aufwand und der Wahrscheinlichkeit einer strafrechtlichen Verfügung verknüpft. NIST merkt aber auch an, dass auch außerhalb des juristischen Bereiches die Evidenzen die Basis für wichtige Entscheidungen darstellen, weshalb durch den Incident Handler auf die Integrität dieser Beweise Wert gelegt werden muss. [6, RS.AN-07]

Prozess – Phase Respond

Der Bereich Respond gliedert sich in die beiden Subphasen Response und Reporting [30, Kap. 5.2], wobei erstere wiederum in die Bereiche Containment, Eradication und Recovery unterteilt wird. Die gesamte Phase zielt darauf ab, den Effekt des Angriffes oder den dadurch entstehenden Schaden zu stoppen oder zu verkleinern und die Systeme in einen Zustand zu versetzen, dass ein ähnlicher Security Incident, und somit auch ein weiteres Ausbreiten des Angreifers, nicht mehr möglich ist. [30, Kap. 11.1] Nach der Mitigation der Angreiferaktivität werden die Systeme wieder auf ein normales Betriebsniveau gebracht. [30, Kap. 11.1] NIST spricht in dieser Phase gar vom Herzstück des Incident Handling. [6, RS]

Im Rahmen eines dokumentierten Response Procedures, das eine Planung der nun durchzuführenden Phase darstellt (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting), werden alle notwendigen Informationen für die Respond-Phase schriftlich durch den Incident Koordinator festgehalten. Darin sind unter anderem alle geplanten Tätigkeiten in der Respond-Phase sowie die notwendigen

Ressourcen festzulegen. [9, Kap. 5.5] Für den Bereich Recovery müssen darin Wiederherstellungsmaßnahmen ausgewählt und priorisiert werden. [6, RC.RP-02] Essenzielle Services müssen zuerst wiederhergestellt werden. [6, RC.RP-04] Mit dem Schreiben dieses Procedures plant der Incident Handler somit die gesamte Phase. Dies stellt eine seiner Kernkompetenzen dar und muss daher beherrscht werden.

Die gesamte Respond-Phase ist jedoch durch Aufgaben wie *reconsider original assessment* und *evaluate proposed resolution* auch von einer ständigen Reevaluierung geprägt. [30, Kap. 5.5] Der ursprüngliche Response-Plan kann jederzeit durch neue Erkenntnisse oder unerwartete Angreiferaktivität verändert werden müssen. Dies muss dem Incident Handler in seiner Arbeit nicht nur bewusst sein; er muss auch aktiv auf Veränderungen der Lage reagieren und den Plan anpassen können.

Die Subphase **Response** zielt darauf ab, „to prevent expansion of an event and mitigate its effects“ [6, RS.MI].

Im Containment wird der Zugriff des Angreifers auf das kompromittierte System beendet und dieses abgeschottet. Erst dann kann es abschließend analysiert und wieder auf einen funktionsfähigen und nicht kompromittierten Zustand gebracht werden. [30, Kap. 11.2.1] Ein wesentliches Ziel des Containments ist das Verhindern von (weiterer) Datenexfiltration, dem Zerstören von Daten oder dem Weiterverbinden auf andere Systeme, beispielsweise durch Lateral Movement. [30, Kap. 11.2.2] Das Containment kann dabei auf verschiedenste Arten passieren. Von netzwerkbasierten Containments wie Routing Changes oder mittels Firewall Blocks kann die Verbindung des betroffenen Systems auch mittels einer Isolation, beispielsweise über das EDR, oder das Entfernen von Kabelverbindungen unterbrochen werden. Zusätzlich ist auch das Herunterfahren eine Möglichkeit zum Containen eines Systems. Vor dem Containment müssen jedoch, abhängig von der gewählten Continmentstrategie, alle flüchtigen Beweise gesichert werden. [30, Kap. 11.2.3 bis 4] An Stelle des manuellen Containments kann dies auch automatisiert durch verschiedene Securitylösungen vorgenommen werden. [6, RS.MI-01] Der Incident Handler muss verschiedene Containmentstrategien sowie deren Vor- und Nachteile kennen und das Containment planen und durchführen können.

Die an das Containment anschließende Eradication hat das Ziel, den Angreifer und seine Spuren aus dem System zu entfernen. Dazu zählen unter anderem die Entfernung von Malware, das Deaktivieren kompromittierter Accounts [30, Kap. 11.3.1], [6, RS.MI-02] oder die Beseitigung von Persistenzmechanismen und das Schließen von Eintrittsvektoren. [6, RS.MI-02] Zu möglichen Eradication-Strategien zählen unter anderem das Formatieren von Festplatten, Disk Wiping, Firmware Flashing oder die physische Zerstörung. [30, Kap. 11.3.2] Dabei kann es allerdings auch zu Daten- oder Datenträgerzerstörung oder zu Fehlern im Firmware Flashing kommen. [30, Kap. 11.3.3] Eine wirkungsvolle Eradication entfernt also nicht nur den Angreifer aus dem System, sondern bereitet auch den folgenden Wiederaufbau vor. Der Incident Handler

muss diesen Schritt also sowohl planen, als auch praktisch durchführen können.

Der letzte Bereich in der Subphase Response nennt sich Recovery. „Recovery ist die Wiederherstellung eines Dienstes, von Daten oder Systemen in ihren normalen, funktionalen Status.“ [30, Kap. 11.4.1] Entscheidend ist, dass die Recovery zum richtigen Zeitpunkt initiiert wird. Dazu sollten Kriterien festgelegt werden, die vor dem Beginn der Recovery erfüllt sein müssen. Neben diesen ist auch die operative Unterbrechung während der Recoverymaßnahmen zu beachten. [6, RS.MA-05] Daher ist eine frühzeitige Kommunikation und interne Absprache notwendig. [6, RC.CO] Während der gesamten Recovery ist ein dauernder Informationsaustausch mit internen und externen Stakeholdern notwendig. [6, RC.CO-03] Es gibt verschiedene Strategien zur Wiederherstellung: Neben dem Einspielen eines nicht kompromittierten Backups oder dem kompletten Neuaufbau von Systemen ist auch das Ändern von Benutzerkennungen und Passwörten eine Strategie. [30, Kap. 11.4.2], [6, RC] Bei hochentwickelten Bedrohungsakteuren und unklarem Vorgehen kann es sogar notwendig sein, die Hardware komplett auszutauschen. [6, RC] Neben unvollständigen Backups sind auch Zeit- oder Ressourcenmangel, Probleme im Bereich Patch-Management oder kompromittierte Recovery-Images [30, Kap. 11.4.3], zu diesen auch kompromittierte Backups zählen dürften, nennenswerte Risiken, die es durch sorgfältige Kontrolle zu minimieren gilt. [6, RC.RP-03] Der Incident Handler muss also nicht nur in der Lage sein, den richtigen Zeitpunkt für eine Wiederherstellung anzusetzen, er muss auch eine passende Strategie auswählen und ihre Risiken kennen.

Im Anschluss an die erfolgte Wiederherstellung müssen die wiederhergestellten Assets weiter sorgfältig auf Kompromittierungsindikatoren überprüft werden. Vor Inbetriebnahme müssen die Systeme nochmals auf eine korrekte und vollständig erfolgte Wiederherstellung überprüft werden. [6, RC.RP-05] Auch diese Überprüfung muss der Incident Handler durchführen können.

Sobald die Subphase Recovery beendet wird, folgt das **Reporting**. „In einem Bericht werden der Incident selbst, die durchgeführten Response- und Recoverytätigkeiten und die Lessons learned dokumentiert.“ [6, RC.RP-06]

Prozess – Phase Learn lessons

In der letzten Phase Learn lessons werden laut ISO verschiedene Verbesserungsmöglichkeiten nach der erfolgreichen Lösung des Security Incidents identifiziert. [9, Kap. 5.6] Anzumerken ist, dass NIST im neuen Lifecyclemodell betont, dass ein Lernen erst am Ende des Security Incidents zu spät sei, die Verbesserung müsse kontinuierlich über alle Phasen hinweg passieren (siehe 2.2.2 Neues Lifecyclemodell (R3)).

Die vorliegenden Werke fordern meist einen Verbesserungsprozess in drei Bereichen: dem Incident Handling selbst, in implementierten Security Controls und in Policies und Prozessen. [6, S. ID.IM–03][9, Kap.

12]

Ganz allgemein fordert CIS in den Critical Security Controls lediglich das Durchführen von Post-Incident Reviews, um Verbesserungsmöglichkeiten im Bereich Incident Handling aufzuzeigen und diese anschließend auch konsequent zu verfolgen. [34, Safeguard 17.8] ISO 27035-2 beschreibt im Rahmen der Prozessaktivität Learn lessons ebendieses Review der Aktvitäten nach einem Security Incident. [29, Kap. 12]

ISO fordert auch das Erheben von Kennzahlen und Metriken über Security Incidents, die nun in der abschließenden Phase ausgewertet werden. Dazu soll neben der „mean time between incidents“, also der durchschnittlichen Zeit zwischen zwei Sicherheitsvorfällen (höher ist besser), auch die „mean time between same type of incidents“, also die durchschnittliche Zeit zwischen der selben Art von Sicherheitsvorfällen (höher ist besser), und die „mean time to resolve same type of incidents“, also die Zeit von der Erkennung bis zur Behebung der selben Incidents (niedriger ist besser) erhoben werden. [29, Kap. 12.1]

Im Bereich der **Verbesserung von Incident Handling selbst** können gezielte Fragen helfen, den Security Incident Handling-Plan auf Verbesserungsmöglichkeiten zu untersuchen [29, Kap. 12.1], beispielsweise „Did the procedures outlined in the information security incident management plan work as intended?“ [29, Kap. 12.3] oder „Are there any procedures or methods that would have aided in the detection of the incident?“ [29, Kap. 12.3].

Auch die Leistung des Incident Handling Teams kann im Anschluss an die Lösung des Security Incidents durch Umfragen, in Gesprächen mit externen Partnern oder über festgelegte Qualitätskriterien kontrolliert werden. [29, Kap. 12.4]

Die **Verbesserung von implementierten Security Controls** beinhaltet hingegen beispielsweise die Überprüfung der eingesetzten Security Tools auf ihren Nutzen. Möglicherweise ist es notwendig, zukünftig auf andere, besser für den Anwendungsfall passende Sicherheitsprodukte zu setzen. [29, Kap. 12.5] Dies sollte für Produkte und Controls aller Funktionen des Cybersecurity Frameworks überprüft werden. [6, S. ID.IM]

Im Bereich der **Verbesserung von Policies und Prozessen** sollten, je nach Größe und Root Cause des Security Incidents, Vulnerability Management-Pläne und Business Continuity Pläne auf Verbesserungsmöglichkeiten hin untersucht werden. [6, S. ID.IM–04] Insbesondere muss aber das Risikomanagement im Hinblick auf den Security Incident überprüft und gegebenenfalls angepasst werden. [29, Kap. 12.6], [6, GV.OV-02]

Aber auch außerhalb von Security Incidents können Verbesserungen proaktiv durch Tests, Übungen, Audits oder Reviews von Policies und Prozessen identifiziert werden. [6, ID.IM-01 bis 02] Durch das regelmäßige Überprüfen von Trends und *areas of concern* können Verbesserungsmöglichkeiten für die Zukunft erkannt werden. [29, Kap. 12.2]

All diese Aspekte sind für die strukturierte Analyse und Aufarbeitung von Verbesserungsvorschlägen für

einen Incident Handler von Bedeutung und müssen von diesem beherrscht werden.

Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting

Dokumentation stellt eine Grundanforderung im Incident Handling dar. Um eine spätere Nachvollziehbarkeit zu garantieren, müssen so viele Informationen wie möglich systematisiert und dokumentiert werden. [9, Kap. 4.7.1-4.7.3] Diese Aufzeichnung stellt daher eine der Haupttätigkeiten eines Incident Handlers dar und muss von diesem beherrscht werden.

Ein Incident Report ist „the synthesis of all gathered information throughout the incident life cycle. It serves to analyse and evaluate the incident [...]“ [9, Kap. 4.7.4] und sollte darüber hinaus auch als Template vorliegen. [9, Kap. 4.7.4] Ein Incident Handler muss in der Lage sein, einen solchen Report zu verfassen. In Unternehmen, in denen ein systematisches Incident Handling gerade erst eingeführt wird, muss dieser auch an ein an die Organisation angepasstes Template erstellen können.

Zusätzlich ist auch eine besondere Form des Abschlussberichts bereits vor der Ausführung des *Response Procedure*, also der Durchführung verschiedener Schritte zum Containment, zur Eradication und zur Recovery, von Bedeutung. [9, Kap. 5.5] In diesem Bericht werden die nachfolgenden Aktivitäten auf Basis der Analyseergebnisse vorgeschlagen. Da die Tätigkeiten in der Respond-Phase eine Einschränkung in der Verfügbarkeit, beispielsweise durch Shutdowns von Systemen, verursachen können, ist eine Abstimmung mit dem Management [30, Kap. 11.2.3] und somit auch eine managementtaugliche Darstellung der geplanten Schritte unumgänglich. [9, Kap. 5.5]

Weiters stellt die Norm auch zwei Arten von Berichten vor, nämlich internes und externes Reporting. Für internes Reporting muss bereits vor einem Security Incident als Vorbereitungsschritt festgelegt werden, wer dieses wann und in welchem Umfang erhalten soll. [30, Kap. 12.2] Da externes Reporting oftmals auch öffentlichkeits- und medienwirksam sein könnte, sollte dieses nach Möglichkeit nicht durch das CSIRT selbst, sondern durch andere Rollen wie den Chief Information Security Officer oder Public Relations durchgeführt werden. [30, Kap. 12.3] Sicherlich kommt dem Incident Handler hier aber eine beratende Rolle zu, welche Informationen zu welchem Zeitpunkt veröffentlicht werden dürfen, sodass auch diese Aufgabe in den Kompetenzbereich eines Incident Handlers fallen kann.

Zusätzlich schlägt die Norm auch vor, abschließende Reports im Sinne der Transparenz beispielsweise an Sponsoren, aber auch an hohe Vertreter anderer Organisationen und Vendoren, die an der Behebung des Incidents mitarbeiten, zu versenden. [30, Kap. 12.5]

Auch an Threat Exchange Communities wie dem Austrian Trust Circle, der einen formellen Austausch von sicherheitsrelevanten Informationen begünstigen soll, kann das Senden eines Reports im Sinne eines

aktiven Informationsaustausches sinnvoll sein. [30, Kap. 12.4] Hierbei muss der Incident Handler typische Empfänger kennen und diese aktiv vorschlagen.

Prozessphasenübergreifende Tätigkeiten: Kommunikation

In ISO 27035 wird empfohlen, die internen sowie externen Kommunikationsprozesse so rasch wie möglich zu starten. [9, Kap. 5.1 d)] Hier muss der Incident Handler, sofern keine Spezialist:innen im Bereich Kommunikation in der Organisation vorhanden sind, in der Lage sein, die Aussendungen zu konzipieren und zu formulieren. Wenn diese Expert:innen vorhanden sind, muss der Incident Handler möglicherweise dennoch steuernd eingreifen, wenn er bemerkt, dass eine Kommunikation oder Nicht-Kommunikation die Analyse oder die Response-Maßnahmen gefährden könnte.

ISO nennt darüber hinaus einige Informationen und Best Practices, was im Falle eines Security Incidents dem Personal und betroffenen Partnern, die auf die Daten zugreifen müssen, kommuniziert werden soll. Unter anderem soll neben Verhaltensanweisungen an des Personal auch eine Kontaktstelle für weitere Fragen oder verdächtige Meldungen kommuniziert werden. Daneben stellt die Norm auch das Prinzip „no-fault“ vor; es soll also keine Schuldzuweisung erfolgen, um die zukünftige Motivation, beobachtete oder unter Umständen selbst verantwortete Sicherheitsvorfälle zu melden. [9, Kap. 4.6]

Der Incident Handler muss aber auch in der Lage sein, Kommunikationswege zu den relevanten internen und externen Stakeholdern [6, RS.CO-02], externen Vendoren, Mitarbeiter:innen und Behördern aufzubauen, offen zu halten und diese über den Sicherheitsvorfall informieren. Außerhalb eines Security Incidents muss diese Kontaktliste auch regelmäßig auf Aktualität überprüft werden [34, Safeguard 17.2], um eine Korrektheit der Kontaktdaten im Security Incident bestmöglich gewährleisten zu können. Die Erstellung eines Kommunikationskonzeptes [6, RS.CO-02], das gegebenenfalls erst zu Beginn des Security Incidents erstellt werden muss, sofern noch keines existiert, oder das Lesen und Einhalten eines solchen sind für einen Incident Handler von besonderer Bedeutung und Teil seiner Aufgaben.

NIST SP 800-61 erwähnt auch die Notwendigkeit der Meldung von Security Incidents an Behörden, sofern eine gesetzliche Verpflichtung dazu existiert. Darüber hinaus kann aber auch im Rahmen einer vertraglichen Verpflichtung eine Meldung an möglicherweise betroffene Partner wie Lieferanten oder Kunden von Nöten sein. Auch eine strafrechtliche Anzeige wird angeraten. [6, RS.CO-02] Der Incident Handler muss daher über die gesetzlichen Meldepflichten sowie die dafür notwendigen Daten und Informationen Bescheid wissen.

Besondere Kommunikationswege stellen jene innerhalb einer Community, wie beispielsweise jene des im Bereich 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting genannten Austrian

Trust Circle, dar. Neben der Nutzung von ad hoc-Kommunikationswegen über E-Mail oder Telefon, die oftmals stark von persönlichen Bekanntschaften innerhalb der Community abhängig sind, stellt ISO 27035-4 insbesondere (teil)automatisierte Kommunikationsmechanismen zum Teilen von Informationen in den Mittelpunkt, wenngleich auch beschrieben wird, dass Kommunikation niemals vollständig automatisiert werden kann und soll. [31, Kap. 6.2] Somit muss ein Incident Handler auch über eine gewisse Vernetzung verfügen und gegebenenfalls teilautomatisierte Kommunikation planen und implementieren.
Auch die interne Kommunikation über bekannte und etablierte Wege und Infrastrukturen kann während eines Incidents eine Herausforderung darstellen, da einzelne oder alle Kommunikationstools unter der Kontrolle der Angreifer stehen könnten und die den Security Incident betreffende Kommunikation so mitlesen könnten. [34, Safeguard 17.6] Somit ist der, eventuell rasche und ad hoc, Aufbau und Betrieb einer Kommunikationsinfrastruktur eine Aufgabe der Incident Handler.

Prozessphasenübergreifende Tätigkeiten: Koordination

Relevante Anforderungen zum Bereich Koordination stammen im Rahmen dieser Arbeit beinahe ausschließlich aus der ISO 27035-4, deren Schwerpunkt dieses Thema ist (siehe 2.2.1 ISO 27035). [31] NIST beschreibt in der SP 800-61 das Thema Koordination lediglich im Bereich Recovery genauer. [6, RS.CO]
Alle aus den anderen drei Teilen der ISO 27035 bekannten Phasen können auch koordiniert über mehrere Organisationen hinweg durchgeführt werden. Dies wird durch den Wortzusatz „Coordinated“ vor der Phasenbezeichnung gekennzeichnet. [31, Kap. 4.1] Dazu wird ein sogenanntes Coordination Team eingesetzt. Diese spezielle Form des Incident Response Teams (IRT) arbeitet hauptsächlich am organisationsübergreifenden Informationssharing und an der Koordination über die Organisationsgrenzen hinweg. [31, Kap. 4.2] Ein Incident Handler muss daher das Wesen, den Nutzen und die Funktion dieser Coordination Teams kennen, sofern diese in einer Organisation zum Einsatz kommen.
Das Coordination Team soll nach vier Prinzipien arbeiten: *Timeliness*, also einer raschen Weitergabe von Informationen, das Arbeiten nach festgelegten *Rollen und Verantwortlichkeiten* mit klaren Zuständigkeiten, einem *Common understanding*, also der Nutzung einheitlicher Taxonomie und Datenaustauschformate, und *Confidentiality*, also Vertraulichkeit mit klaren Regeln zur Weitergabe von Informationen über die Organisationsgrenzen hinweg. [31, Kap. 4.2] Diese Prinzipien muss ein Incident Handler insbesondere beim Aufbau und der Etablierung, aber auch beim Austausch von Informationen mit dem Coordination Team kennen.
In der ersten koordinierten Phase, dem Coordinated plan and prepare, wird das Framework für die Zusammenarbeit aufgebaut. Dazu müssen Kommunikationskanäle etabliert und gemeinsame Übungen geplant und durchgeführt werden. Zusätzlich soll jede Organisation einen Incident Koordinator als Point of Contact

benennen. Weiters müssen in verschiedenen Policies die Arbeitsweisen des Coordination Team festgelegt werden. Darunter fallen beispielsweise Definition von Purpose und Scope, aber auch Regeln zum Event Tracking und zum Information Sharing. Diese Notwendigkeiten müssen dem Incident Handler zum Aufbau eines solchen Teams bekannt sein. [31, Kap. 5.2]

In der anschließenden Coordinated Detect and report-Phase sollen alle Organisationen Threat Intelligence erstellen und diese teilen, damit diese von den anderen Mitgliedern analysiert und in Entscheidungen einbezogen werden kann. Das Teilen von Informationen soll so automatisiert wie möglich passieren, da die Informationen mit der Zeit an Wert verlieren und nicht mehr aktuell sein können. [31, Kap. 5.3] Um dies ermöglichen zu können, muss der Incident Handler Kenntnisse im Bereich Threat Intelligence und Umgang und Konfiguration von TIPs haben.

Coordinated Assessment and decision dient dazu, das Assessment von Sicherheitsvorfällen organisationsübergreifend durchzuführen. Dadurch ist eine leichtere Abschätzung der Notwendigkeit einer Koordination durch das Coordination Team möglich. Dies ist beispielsweise dann der Fall, wenn eine Organisation den Security Incident nicht alleine unter Kontrolle bringen kann oder mehrere ähnliche Incidents gleichzeitig auftreten. In diesen Prozessschritt sind insbesondere die Incident Koordinatoren intensiv einzubinden. [31, Kap. 5.4] Auch diese Vorgänge müssen dem Incident Handler bekannt sein, um eine effiziente Zusammenarbeit zu ermöglichen.

Während in den anderen Phasen eine Mitarbeit von nicht betroffenen Organisationen nicht ausgeschlossen und teilweise sogar gefordert ist, sollen an der Coordinated Respond-Phase nur Organisationen mitarbeiten, die auch tatsächlich von dem Security Incident betroffen sind. Die Organisationen arbeiten hier gemeinsam einen Response-Plan aus. Auch hier sind die Incident Koordinatoren wieder Schlüsselfiguren in der Abstimmung unter den Organisationen. [31, Kap. 5.5] Incident Handler müssen nicht nur den Sinn und das Wesen einer solchen koordinierten Response kennen, sie müssen auch, sofern sie die Rolle als Incident Koordinator innehaben, alle durchzuführenden Schritte der Reaktion gemeinsam mit den anderen Organisationen planen können.

Da die selben Angriffsmuster oftmals mehrere Organisationen betreffen, schlägt auch NIST vor, beispielsweise beobachtete TTPs zu teilen. Werden Erkennungsmöglichkeiten für Exploits geteilt, so steigt nicht nur die Situational Awareness für alle Organisationen, die über diese Information verfügen, sondern der Return of Investment der Angreifergruppierungen, die Exploits meist selbst käuflich erwerben müssen, sinkt gleichzeitig. [6, RS.CO-03]

In der letzten Phase, Coordinated learn lessons, identifiziert jede Organisation für sich oder gemeinsam Verbesserungspotenziale. Da sich die Tätigkeiten sehr jenen der Learn lessons-Phase (siehe 5.1.1 Prozess –

Phase Learn lessons) ähneln, folgt keine erneute Beschreibung der Aufgaben oder des notwendigen Wissens des Incident Handlers. Diese finden sich bereits in den Kommunikationsanforderungen.

5.1.2. Durch die Experteninterviews identifizierte Anforderungen

Des Weiteren wurden die Experten befragt, welche Anforderungen ihrer Auffassung nach an Incident Handler bestehen. Dabei wurden auch jene Anforderungen, die an Berufseinsteiger:innen bestehen, erhoben, um feststellen zu können, mit welchen Skills und welchem Knowledge die Fachhochschule ihre Absolvent:innen unbedingt ausstatten sollte, um ihnen einen guten Berufseinstieg zu ermöglichen.

Kundenumfeld und Dienstleistungen

Um die Anforderungen, die in den Unternehmen an Incident Handler bestehen, zu verstehen, ist es nötig, die Leistungen der Unternehmen im Bereich Incident Handling sowie deren Kundenumfeld besser zu kennen. Drei der vier befragten Unternehmen sind dabei Dienstleister (PwC, ACP und CANCOM) und bieten sowohl proaktive als auch reaktive Dienstleistungen im Bereich Incident Handling an.
PwC ist als Wirschaftsprüfer, Steuer- und Unternehmensberater international tätig. Etwa 50 Vollzeitstellen sind dabei österreichweit alleine im Bereich Cybersecurity-Beratung vergeben, wobei eine variierende Zahl dieser an Angestellten auch in Security Incidents mitarbeitet. Im Bereich der Cybersecurity-Beratung werden proaktiv Rediness Assessments, Übungen, SOC-Beratung, -Dienstleistungen und Implementierung von SOC angeboten. Reaktiv bietet PwC Incident Handling-Dienstleistungen, darunter die Unterstützung der Geschäftsführung, Krisenmanagement, koordinierende Tätigkeiten, Lagebilderstellung, technische Themen, IT-Forensik und Schadsoftwareanalyse sowie Retainer, also eine SLA, an. Werden die Mitarbeiter:innen gerade nicht zur Abarbeitung eines Security Incidents benötigt, so sind diese mit den Themen Threat Intelligence und Incident Handling Design befasst, worunter beispielsweise Beratungen zum Thema CSIRT- oder SOC-Design fallen. (Interview B.1)
Die ACP-Gruppe ist hingegen ein vorrangig im DACH-Raum tätiger IT Provider, der in den vier Geschäftsfeldern Hybrid Cloud und Data Center, Modern Workplace, Netzwerk und Security sowie Digital Solutions arbeitet. Im SOC arbeiten dabei 32 Mitarbeiter:innen in drei Tätigkeitsfeldern: Erstens, das Analyseteam, das die Analyse von Security Incidents übernimmt. Zweitens, das Consultingteam, das die Kundenbetreuung innehat und als Ansprechpartner fungiert. Dieses Team übernimmt auch Monatsmeetings, zeitunkritische Anfragen, betreut das Vulnerability Management und koordiniert alle das SOC betreffenden Aspekte mit dem Kunden. Drittens, das Engineeringteam, die sich um die betriebene Infrastruktur kümmern und Automatisierungen implementieren. Sobald kein Security Incident zu bearbeiten ist, sind die damit befassten

Mitarbeiter:innen als Analysten tätig. (Interview B.2)

Auch CANCOM ist IT-Unternehmer und vorwiegend im ICS-Bereich tätig. Die 5600 Mitarbeitenden sind dabei in der DACH-Region beschäftigt, wobei CANCOM auch über diese Region hinausgehend in kleineren Standorten agiert. Im Incident Response- und Digital Forensics-Team arbeiten dabei 60 Blueteamer, wobei das Kernteam der Incident Handler aus 15 Senior und Principal Analysten besteht. Ist die CANCOM gerade nicht mit der Aufarbeitung eines Security Incidents betraut, arbeiten die Analysten im SOC und die Incident Handler an der Weiterentwicklung des Digital Forensic und Incident Response (DFIR) sowie weiteren Projekten und Workshops. (Interview B.4)

Die MA01 nimmt unter den Befragten eine Sonderstellung ein, da es sich bei ihr um keinen Dienstleister im klassischen Sinne handelt. Sie übernimmt als Blue und Red Team sämtliche IT Security-bezogene Leistungen für die gesamte Stadt Wien und arbeitet hierbei - wie die anderen Unternehmen - sowohl proaktiv als auch reaktiv. Dabei kommt den proaktiven Tätigkeiten eine besonders große Bedeutung zu, wobei diese, wie zum Beispiel die Systemhärtung, zu niedrigen Zahlen an Security Incident-Vorfällen führen. Komme es jedoch zu einem solchen, wird dieser intern abgearbeitet. Darüber hinaus sind die MA01 und WienCERT als interne Security Consultants tätig, wobei viel projektbezogene Arbeit, beispielsweise bei der Implementierung neuer Systeme, geleistet wird. (Interview B.3)

Allgemeine Anforderungen an Berufseinsteiger:innen

Will man als Incident Handler bei PwC anfangen, ist eine laufende oder bereits abgeschlossene Security-Ausbildung auf Hochschulniveau erwünscht, da so das erwünschte Basiswissen durch die Curricula abgedeckt wird. Darunter fallen analytische und technische Skills, Projektmanagement sowie forensische Inhalte wie die Sicherung von Beweismitteln, die Schadsoftwareanalyse und der Netzwerk- und Serverbetrieb. Dies ermöglicht, Berufseinsteiger:innen im Incident Handling insbesondere im Bereich der Lagebilderstellung und der Dokumentation unterstützend einzusetzen. (Interview B.1)

Für die ACP-Gruppe ist ein Studium hingegen keine notwendige Voraussetzung für den Berufseinstieg, wobei hier Vorerfahrung im Bereich Softwareentwicklung als hochgradig interessant deklariert wird. Incident Handling aus der Analysetätigkeit im SOC heraus zu erarbeiten sei dabei sinnvoll, da verwandte Kenntnisse benötigt werden. (Interview B.2)

Auch für CANCOM ist ein Studienabschluss weniger relevant, da viel praktisches Wissen nötig sei, um Incident Handler zu werden. Ein Studium sei dafür zwar vorteilhaft, bedeutsamer sei jedoch das technische Assessment, das Bewerber:innen durchlaufen müssen. Darüber hinaus müssen die Incident Handler in der Lage sein, einen Perspektivwechsel zwischen der fachlichen Seite und der Sichtweise des Kunden zu

vollziehen, um so eine Einschätzung über die Machbarkeit der Maßnahmen treffen zu können. (Interview B.4)

Zudem definiert Utz Nisslmüller von WienCERT als benötigtes Einstiegswissen fundierte Windowskenntnisse sowie ein Grundverständnis für den Aufbau von Enterprise-Strukturen und deren Logquellen. Dabei müssen Logquellen, Logparsing und Alerts gekannt und verstanden werden. Konzepte und Systeme wie SIEM, EDR, XDR, PAM, VPN, DMZ, PKI und Loadbalancing, jeweils in Enterprise-Umgebungen, müssen den Incident Handlern ein Begriff sein und von diesen [als Analysewerkzeug sowie als Loquelle, Anm. d. Verf.] eingesetzt werden können. (Interview B.3)

Diese Relevanz des umfassenden, praktischen Wissens zeigt sich auch im Interview mit Philipp Mattes-Draxler, der betont, dass es insbesondere für junge Incident Handler wichtig ist, viel zu sehen, in allen Bereichen eingesetzt und von erfahrenen Kolleg:innen mitgenommen zu werden. Dadurch werde ein besseres Verständnis aufgebaut. Erst danach solle eine Spezialisierung erfolgen. (Interview B.1) Diese Ansicht teilt auch Gideon Teubert, wobei er ausführt, dass für Incident Handler Wissen verschiedener Fachgebiete relevant ist. (Interview B.4) Auch Andreas Plank erwähnt, dass ohne Erfahrung die meisten Tasks nicht umsetzbar seien, weshalb am Anfang ein Dabei sein im Vordergrund stehen sollte. (Interview B.2)

Um diese Skills und das benötigte Knowledge aufzubauen, führt auch CANCOM ihre Berufseinsteiger:innen an die Aufgaben im Incident Handling heran. Zunächst übernehmen junge Mitarbeiter:innen dabei rein technische Aufgaben, bevor sie mit organisatorischen Tätigkeiten betraut werden. Erst danach wird auch der Lead an sie übergeben, hinter dem wiederum Analysten stehen, die die Analyse tatsächlich durchführen. (Interview B.4)

Darüber hinaus sprechen alle Interviewpartner im Rahmen der persönlichen Anforderungen das Arbeiten unter Zeitdruck an. Über eine zunächst unübersichtliche Lage muss dabei rasch ein Überblick gewonnen werden, wobei Entspannung meist dann eintritt, wenn dieser Überblick geschaffen wurde. (Interview B.1) Im Zuge dessen werden Resilienz (Interview B.2, Interview B.3, Interview B.4) und das Bewahren von Ruhe unter Druck als Schlüsselskills genannt. Auch ein dementsprechendes, selbstbewusstes Auftreten gegenüber Kunden ist fundamental. (Interview B.2) Dabei spielen soziale Kompetenzen, Empathie (Interview B.4) und ausgeprägte Kommunikationsfähigkeiten eine wichtige Rolle, wobei letztere nicht nur in Bezug auf die Kommunikation mit Kunden, sondern auch in Bezug auf die interne Kommunikation essenziell sind. (Interview B.3)

Zu den erwünschten Personal Skills zählen des Weiteren Eigeninitiative und Verlässlichkeit, wofür auch eine gute Selbsteinschätzung notwendig ist. (Interview B.1) Dabei soll erkannt werden, was man selbst beherrscht und weiß und diese fachliche Expertise auch mit genügend Selbstvertrauen gegenüber den Kunden

vertreten. Gleichzeitig sind Lernfähigkeit (Interview B.3) und damit im Zusammenhang stehend Wissbegierde für Incident Handler fundamental, um sich rasch auf unbekannte Umgebungen und Systeme einstellen zu können. (Interview B.4) Zudem müssen Incident Handler zwar einerseits genau arbeiten (Interview B.1), andererseits aber auch effizient sein (Interview B.4), um rasch richtige und valide Ergebnisse liefern zu können.

Zusammenhänge verstehen und Entscheidungen treffen

Aus all den beschriebenen und den folgenden Anforderungen geht hervor, wie umfangreich die benötigten Skills und das vorausgesetzte Knowledge sind, das Incident Handler in ihren Beruf mitbringen oder allenfalls in diesem erlernen müssen. Philipp Mattes-Draxler formuliert dazu die große Aufgabe der Incident Handler wie folgt: „Incident Response ist Königsklasse. Incident Response repariert ja dann, wenn alles kaputt ist oder wenn einer aktiv da ist, der Dinge kaputt macht.“ (Interview B.1)

Im Zuge dessen ist es wichtig zu verstehen, dass Incident Handling nicht nur viel Wissen und Können voraussetzt, sondern auch in multiplen Abhängigkeitsbeziehungen steht. Deswegen ist das Kennen der Prozesse und die Anwendung derer fundamental für Incident Handler, um die gesamte Angriffskette nachvollziehen zu können. (Interview B.2) Dabei seien die grundlegenden, hinter verschiedenen Begriffen stehenden Konzepte relativ unveränderlich, sodass ein Verständnis dieser auf sämtliche Situationen und Begrifflichkeiten umgelegt werden könne und deswegen fundamental sei. (Interview B.1)

Incident Handling sei dabei als Teil des Notfallmanagements zu verstehen, wobei die Vorbereitung ebendieser Prozesse zentral sei. (Interview B.2) Dabei beziehen sich die interviewten Unternehmen auf unterschiedliche Prozesse und Vorgehensweisen. PwC arbeitet dabei mit der Cyber Kill Chain, dem MITRE Attack Framework und der ISO 27035, die in Grundzügen gekannt werden sollte. Grundlegend ist dabei das Verständnis der Zusammenhänge und der domänenspezifischen Wirkung, sowie der Funktionsweise von Sicherheitssystemen wie IDS, EDR oder SOAR. Aus letzterer sollen Indikatoren abgeleitet werden können, die wiederum auf Basis der bereits genannten Cyber Kill Chain und dem MITRE Attack Framework an der richtigen Stelle gesucht werden sollen. Die Zuordnung zu den Phasen und das Ziehen von Schlüssen sind darüberhinausgehend besonders relevant. (Interview B.1)

ACP nennt neben der bereits für PwC wichtigen Cyber Kill Chain und dem MITRE Attack Framework auch NIST als relevante Referenzwerke. Dabei stehe der analytische Denkprozess im Vordergrund. (Interview B.2)

Als Grundlage für das Vorgehen wird bei der MA01 die NIST SP 800-61 gewählt. Daher ist es für deren Mitarbeiter:innen wichtig, die vier Phasen dieses Prozesses benennen, beschreiben und anhand von Beispielen

erklären zu können. Dabei ist eine an die Situation angepasste Handhabung der Phasen wichtig, weswegen es zu wenig ist, wenn die Incident Handler die Phasen nur reproduzieren können (Interview B.3).
Während bei diesen Interviews nur implizit mitschwingt, dass insbesondere ein grundlegendes Verständnis des Prozesses wichtig ist, sodass eine adäquate Vorgehensweise im Incident ermöglicht wird, das Referenzwerk jedoch nur sekundär von Bedeutung ist, expliziert CANCOM genau diesen Umstand. Der Interviewpartner betont dabei die Wichtigkeit einer strukturierten Vorgangsweise, bei der die Phasen situationsangemessen durchgearbeitet werden sollen. (Interview B.4)
Im Zuge dessen ist auch das Arbeiten im Falle eines Security Incidents im Rahmen dieser Prozesse relevant. Bei der MA01 wird darüber hinaus in dem OODA-Loop eine strukturierte Vorgehensweise zu diesem Arbeitsprozess identifiziert. (Interview B.3) Auch Gideon Teubert streicht die Bedeutung des Treffens von Entscheidungen heraus, wobei Handlungen, Gegenmaßnahmen und No Gos zum richtigen Zeitpunkt kommuniziert werden müssen. Dabei ist zudem zu bedenken, welche Entscheidungen welche Folgen nach sich ziehen und was den Unternehmen daher empfohlen werden sollte, um den Security Incident bestmöglich zu bewältigen. Auch wäre sinnvoll, im Rahmen einer Lehrveranstaltung herauszuarbeiten, ab wann welche Systeme wiederhergestellt werden können. Es sei hierbei wichtig, dem Druck des gestressten Kunden standzuhalten und nicht zu früh einzuknicken, um eine erneute Kompromittierung zu vermeiden. (Interview B.4)
Utz Nisslmüller erklärt hierbei auch die Bedeutung des Treffens von Entscheidungen über notwendige Ressourcen, die zur Bewältigung des Security Incidents benötigt werden. (Interview B.3) Auch bei ACP stellt dies einen wichtigen Teil der ersten Schritte vor der Abarbeitung des Security Incidents dar. Andreas Plank führt dabei den Ablauf des Incident Handling bis zum Beginn der Bearbeitung des Security Incidents näher aus. Den ersten Schritt stellt hier das Scoping-Gespräch dar. Daran anschließend wird der Aufgabenbereich abgesteckt, wobei ACP entweder nur technische Aufgaben oder auch die Koordination und den Lead übernimmt. In Schritt drei werden die Ansprechpartner, Verantwortlichkeiten und Entscheidungsbefugnisse festgehalten. Darauf aufbauend werden die Umstände und die Priorität des Security Incidents geklärt. Abschließend plant ACP das benötigte Personal und Budget (Interview B.2), bevor die eigentliche Arbeit am Security Incident beginnt.

Aufgaben in der Preparation

Die Wichtigkeit der Preparation-Phase wurde insbesondere von Andreas Plank, Gideon Teubert und Utz Nisslmüller herausgearbeitet. (Interview B.2, Interview B.3, Interview B.4) Doch auch bei PwC wird der Phase Bedeutung zugemessen, wobei Philipp Mattes-Draxler insbesondere auf die Wichtigkeit von Play-

books als proaktive Maßnahme Bezug nimmt. (Interview B.1) Andreas Plank hingegen beschreibt für diese Phase die Relevanz der Abhaltung von vorbereitenden Workshops. (Interview B.2)

Dokumentation und Reporting

Insbesondere bei den Dienstleistern spielt die Dokumentation und das Reporting eine zentrale Rolle. Bei PwC müssen die Incident Handler dabei Lagebilder erstellen, eine Dokumentation im *Incident Response Tracker* vornehmen und auch für den Kunden Aufwandsbeschreibungen und das Tracking des Aufwands aktuell halten. (Interview B.1) Die Aufzeichnung der Arbeitszeiten ist auch bei der ACP ein wichtiger organisatorischer Task der Mitarbeiter:innen. (Interview B.2) Im Gegensatz zu PwC wird bei der CANCOM die Erstellung von Lagebildern primär aufgrund des Zeitmangels und mangelnder Relevanz nicht immer verfolgt. Werden solche jedoch erstellt, ist eine grafische Aufbereitung wichtig. (Interview B.4)
Zudem wird das Verfassen des Reports als essenziell herausgearbeitet, wobei auch festgehalten wird, bei Reports handle es sich um eine eigene Textsorte. (Interview B.1) Daraus kann gefolgert werden, dass das Schreiben von Reports erlernt werden muss.
An den Report bestehen dabei zahlreiche Anforderungen. In ihm sollen technische Analysen zusammengeführt werden (Interview B.1), wobei dennoch auf Verständlichkeit Wert gelegt werden muss, damit der Bericht managementtauglich ist. (Interview B.2) Diese Einfachheit darf jedoch nicht auf Kosten der fachlichen Korrektheit gehen. (Interview B.1, Interview B.2) Gideon Teubert beschreibt dabei, dass sich der Report aus mehreren Teilen zusammensetze, die jeweils zielgruppenorientiert zu verfassen seien. (Interview B.4) Dennoch darf die nötige Stringenz nicht verloren gehen. Zudem ist auch die Sprachnormativität zu beachten. (Interview B.1)

Kommunikation

Funktionierende Kommunikation ist vital zur Abarbeitung eines Security Incidents. Utz Nisslmüller bezeichnet Kommunikationsfreude dabei als einen zentralen Personal Skill von Incident Handlern. (Interview B.3)
Je nach Unternehmensstruktur haben die Incident Handler dabei unterschiedlich viel Kundenkontakt, wodurch die Kommunikation um weitere Facetten erweitert wird. Bei PwC und CANCOM haben diese Mitarbeiter:innen hoch frequent direkten Kontakt mit Kunden (Interview B.1, Interview B.4), wohingegen bei ACP vorrangig der:die Service Delivery Manager die Kundenkommunikation übernimmt. Die Rollenverteilung ergibt sich dabei aber insbesondere aus der Größe des Security Incidents. (Interview B.2) Utz Nisslmüller streicht für solche Situationen heraus, dass in der Kommunikation bedacht werden muss, dass man

mit Menschen spricht, die sich gerade in einer Stresssituation befinden und sich zudem oftmals nicht mit Security-Themen auskennen. (Interview B.3) Andreas Plank erwähnt in diesem Zusammenhang wie schon beim Reporting, dass die sowohl mündlich als auch schriftlich ablaufende Kommunikation mit dem Management trotz der mangelnden Fachkenntnis für dieses verständlich sein muss, sodass Entscheidungen getroffen werden können. (Interview B.2)
Um diese gute Kommunikation gewährleisten zu können, sei es wichtig, klare Ansprechpartner:innen zu benennen. (Interview B.1)

Koordination

Bei PwC gehört zu den organisatorischen Aufgaben von Incident Handlern in größeren Security Incidents auch die interne Koordination der Streams durch einen Incident Koordinator, wobei jedes dieser Teams unterschiedliche Aufgaben übernimmt. Dabei werden beispielhaft das Analyseteam, das IT-Team, das Team für Legal, Compliance und Öffentlichkeit, das Team für Härtung, sowie das Team zur Implementierung eines SOC aufgeführt. (Interview B.1)
Bei CANCOM fallen die koordinierenden Tätigkeiten dem Incident Lead, der ähnliche Aufgaben zum gerade beschriebenen Koordinator übernimmt, zu. Dieser muss den Überblick bewahren, die Informationen strukturieren und den Incident Handlern ihre Tasks zuweisen, die diese Schritt für Schritt abarbeiten. (Interview B.4)

5.1.3. Aktuelle curriculare Anforderungen der Fachhochschule St. Pölten

Als Lernergebnisse fordert das Curriculum der Fachhochschule St. Pölten derzeit, dass „ [d]ie Studierenden [...] den Incident Response Prozess [kennen] [...]“ [42]. Aufgrund der Vielzahl an Prozessmodellen ist diese Vorgabe jedoch zu ungenau, da es nicht eine, sondern unzählige Vorgehensweisen gibt. In den Lehrinhalten wird der Prozess noch weiter spezifiziert: „ [...] anhand des Incident Reponse [sic!] Prozesses (Preparation, Detection, Analysis, Remediation) [...]“ [42] Dieser geforderte Prozess existiert jedoch in der öffentlich auffindbaren Literatur nicht. Die einzelnen Prozessschritte haben aber eine auffallende Ähnlichkeit zum aus heutiger Sicht veralteten Lifecyclemodell der R2 der NIST SP 800-61, bei dem die Phasen aber Preparation – Detection & Analysis – Containment, Eradication & Recovery – Post-Incident Activity heißen müssten.
Andere Anforderungen sind derzeit technisch geprägt, was dem vorgesehenen Ziel der Trennung der Lehrveranstaltung in einen organisatorischen und einen technischen Teil widersprechen würde. Somit ist insbesondere das Lernergebnis „Die Studierenden sind in der Lage ein kompromittiertes Einzelsystem auf wichtige Artefakte hin zu untersuchen (L4)“ [42] nicht mehr haltbar.

Die Ziele „Die Studierenden können einen Incident Reponse [sic!] Case führen und unterschiedliche Teilnehmer und Stakeholder managen. (Timelines) (L3)“ [42] und „Die Studierenden können in einem Enterprise Environment die Bewegung eines Angreifers nachvollziehen, eingrenzen und diesen am Ende der Investigation aus dem System entfernen (Remediation). (L5)“ [42] können in einer umformulierten und abgeschwächten Art auch in Zukunft genutzt werden.

Alle Interviewpartner haben angegeben, dass sich diese Fähigkeiten ohne praktische Erfahrung in einer Vielzahl an realen Security Incidents nur durch Fachhochschulunterricht alleine nicht erreichen lassen. (Interviews B.1, B.2, B.3, B.4) Es ist somit generell in Frage zu stellen, ob derartige Ziele in diesem Umfeld realistisch erreichbar sind. Realistisch umsetzbar wäre somit im Bereich der Führung von Security Incidents vermutlich das Ziel, dass die Studierenden nach der Lehrveranstaltung in einfachen organisatorischen Aufgaben wie der grafischen Lagebilderstellung oder der Dokumentation von Aufwänden oder Analyseergebnissen unterstützen können.

5.1.4. TKS-Statements

Wie in der Methodik aufgezeigt (siehe 4.3 Konsolidierung der Ergebnisse) wurden auf das Thema der Lehrveranstaltung zutreffende vorgefertigte TKS-Statements der NIST aus der Work Role *Incident Response* (siehe 2.1.4 Competencies und Work Roles) übernommen und eigene Statements aufgrund der erhobenen Anforderungen formuliert. Die Basis dafür bildet das in 2.1.4 NIST SP 800-181: NICE Framework beschriebene NICE Framework der NIST.

Dabei hat sich insbesondere gezeigt, dass nicht alle Anforderungen der auf den amerikanischen Raum abgestimmten vorgefertigten TKS-Statements der NIST auch auf Österreich übertragbar sind. Beispielsweise fand sich weder in den internationalen Standards noch in den Interviews ein Hinweis auf den Task „T1372: Advise law enforcement personnel as technical expert“ [4]

Task-Statements

1. Klassifizieren von IT Security Incidents (siehe 5.1.1 Wesen der Standards)
2. „T1252: Determine the scope, urgency, and impact of cyber defense incidents“ [4]
3. Etablieren einer Aufbauorganisation für das Incident Handling (siehe 5.1.1 Personal, Rollen und Verantwortlichkeiten)
4. Anpassen der Aufbauorganisation für das Incident Handling (siehe 5.1.1 Personal, Rollen und Verantwortlichkeiten)

5. Anpassen eines Incident Handling Prozessmodelles auf die Anforderungen der Organisation (siehe 5.1.1 Allgemeine prozessbezogene Anforderungen)
6. „T0510: Coordinate incident response functions“ [4] (siehe 5.1.1 Allgemeine prozessbezogene Anforderungen)
7. Identifizieren von Anforderungen der Organisation im Incident Handling, beispielsweise aufgrund von Vorgaben im Risikomanagement, im ISMS oder in der Prozesslandschaft (siehe 5.1.1 Allgemeine prozessbezogene Anforderungen und 5.1.1 Prozess – Phase Plan and prepare)
8. Etablieren von Prozessen und Abläufen im Bereich Incident Handling (siehe 5.1.1 Prozess – Phase Plan and prepare)
9. Etablieren von Kontakten zu wichtigen Stakeholdern im Security Incident Management (siehe 5.1.1 Prozess – Phase Plan and prepare)
10. Interpretieren und Verknüpfen von Bedrohungsinformationen (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Assess and decide)
11. „T1407: Correlate threat assessment data“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Assess and decide)
12. Erstellen von Bedrohungsinformationen (siehe 5.1.1 Prozess – Phase Plan and prepare)
13. Erstellen von Playbooks (Flow-Plänen) für IT-Sicherheitsvorfälle (siehe 5.1.1 Prozess – Phase Plan and prepare)
14. Konzipieren von Awareness-Kampagnen für unterschiedliche Zielgruppen im Bereich Security Incident Management (siehe 5.1.1 Prozess – Phase Plan and prepare)
15. Konzipieren eines Incident Response Capability Monitorings (siehe 5.1.1 Prozess – Phase Plan and prepare)
16. Dokumentieren von Prozessen und Abläufen für den Security Incident (siehe 5.1.1 Prozess – Phase Plan and prepare)
17. Ausrollen von technischen Maßnahmen zur Detektion oder Analyse von Sicherheitsvorfällen (siehe 5.1.1 Prozess – Phase Plan and prepare)
18. Konzipieren von Security Incident Handling-Übungen (siehe 5.1.1 Prozess – Phase Plan and prepare)
19. Teilnehmen an Security Incident Handling-Übungen (siehe 5.1.1 Prozess – Phase Plan and prepare)
20. Identifizieren von Risiken (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Assess and decide)
21. „T1085: Identify potential threats to network resources“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)

22. „T1020: Determine the operational and safety impacts of cybersecurity lapses“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
23. „T1118: Identify vulnerabilities“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
24. Identifizieren von Assets (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Assess and decide)
25. Interpretieren von Detektionen, die auf einen Sicherheitsvorfall hindeuten könnten (siehe 5.1.1 Prozess – Phase Detect and report)
26. Entgegennehmen von Meldungen, die auf einen Sicherheitsvorfall hindeuten könnten (siehe 5.1.1 Prozess – Phase Detect and report)
27. Etablieren eines Point of Contact (siehe 5.1.1 Prozess – Phase Detect and report)
28. „T1250: Perform cyber defense incident triage“ [4] (siehe 5.1.1 Prozess – Phase Detect and report)
29. „T1489: Correlate incident data“ [4] (siehe 5.1.1 Prozess – Phase Detect and report)
30. „T1299: Determine causes of network alerts“ [4] (siehe 5.1.1 Prozess – Phase Detect and report)
31. Ableiten von Kompromittierungsindikatoren auf Basis der Erkenntnisse aus Sicherheitssystemen (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
32. Ziehen von Schlüssen auf Basis der vorliegenden Fakten (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
33. Treffen von Entscheidungen (siehe 5.1.1 Prozess – Phase Assess and decide)
34. Vorbereiten von Grundlagen für Entscheidungen (siehe 5.1.1 Prozess – Phase Assess and decide)
35. „T1582: Maintain currency of cyber defense threat conditions“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
36. Kommunizieren von Empfehlungen oder Nicht-Empfehlungen (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
37. Erstellen von Lagedarstellungen bzw. Lagebildern (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
38. Durchführen von Erstgesprächen bzw. Scoping-Gesprächen bei IT-Sicherheitsvorfällen (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
39. Planen von Ressourcen (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
40. Durchführen von Preparation-Workshops (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen und 5.1.2 Aufgaben in der Preparation)
41. Kategorisieren von Sicherheitsvorfällen (siehe 5.1.1 Prozess – Phase Assess and decide)
42. Priorisieren von Sicherheitsvorfällen (siehe 5.1.1 Prozess – Phase Assess and decide)

43. Herstellen der Visibilität im Netzwerk (siehe 5.1.1 Prozess – Phase Assess and decide)
44. Finden der Ursache des Sicherheitsvorfalles (siehe 5.1.1 Prozess – Phase Assess and decide)
45. Erstellen eines Reponse Procedure-Plans (siehe 5.1.1 Prozess – Phase Respond)
46. „T1119: Recommend vulnerability remediation strategies“ [4] (siehe 5.1.1 Prozess – Phase Respond)
47. „T1260: Perform real-time cyber defense incident handling“ [4] (siehe 5.1.1 Prozess – Phase Respond)
48. „T1257: Recommend mitigation and remediation strategies for enterprise systems“ [4] (siehe 5.1.1 Prozess – Phase Respond)
49. Auswählen geeigneter Containment-Maßnahmen (siehe 5.1.1 Prozess – Phase Respond)
50. Durchführen von Containment-Maßnahmen (siehe 5.1.1 Prozess – Phase Respond)
51. „T1371: Mitigate potential cyber defense incidents“ [4] (siehe 5.1.1 Prozess – Phase Respond)
52. Auswählen geeigneter Eradication-Maßnahmen (siehe 5.1.1 Prozess – Phase Respond)
53. Durchführen von Eradication-Maßnahmen (siehe 5.1.1 Prozess – Phase Respond)
54. „T1251: Recommend incident remediation strategies“ [4] (siehe 5.1.1 Prozess – Phase Respond)
55. Durchführen von Recovery-Maßnahmen (siehe 5.1.1 Prozess – Phase Respond)
56. „T1109: Resolve cyber defense incidents“ [4] (siehe 5.1.1 Prozess – Phase Respond)
57. Analysieren von Verbesserungsmöglichkeiten (siehe 5.1.1 Prozess – Phase Learn lessons)
58. „T1485: Prepare after action reviews (AARs)“ [4] (siehe 5.1.1 Prozess – Phase Learn lessons)
59. Implementieren von Verbesserungsmöglichkeiten (siehe 5.1.1 Prozess – Phase Learn lessons)
60. Dokumentieren von Informationen (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
61. Dokumentieren von Analyseschritten (siehe 5.1.1 Prozess – Phase Assess and decide)
62. „T1316: Document cyber defense incidents from initial detection through final resolution“ [4] (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
63. „T0164: Perform cyber defense trend analysis and reporting“ [4] (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
64. „T1315: Track cyber defense incidents from initial detection through final resolution“ [4] (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
65. Synthetisieren aller Informationen zu einem Security Incident Report (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
66. „T1332: Produce incident findings reports“ [4] (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)

67. „T1617: Prepare cyber defense reports“ [4] (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
68. Erstellen eines Kommunikationskonzeptes (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
69. Kommunizieren mit internen und externen Stakeholdern sowie Behörden (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
70. „T1333: Communicate incident findings to appropriate constituencies“ [4] (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
71. Koordinieren der am Security Incident mitarbeitenden Personen und Organisationen (siehe 5.1.2 Koordination)
72. „T1110: Coordinate technical support to enterprise-wide cybersecurity defense technicians“ [4] (siehe 5.1.2 Koordination)

Philipp Mattes-Draxler betont, dass auch Architektenaufgaben in der Recovery-Phase zu den Aufgaben eines Incident Handlers zählen können. (Interview B.1) Diese sind nicht primär Ziel dieser Lehrveranstaltung, sind aber der Vollständigkeit halber trotzdem in den Task- und Knowledge-Statements separat aufgeführt:

73. „T0262: Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness)“

Knowledge-Statements

1. Wissen über die Vorteile des strukturierten Incident Managements (siehe 5.1.1 Wesen der Standards)
2. Wissen über die Ziele des strukturierten Incident Managements (siehe 5.1.1 Wesen der Standards)
3. Wissen über Arten von Security Incidents (deren Merkmale und Kategorisierungsmöglichkeiten) (siehe 5.1.1 Wesen der Standards)
4. Wissen über verschiedene Definitionen (z.B. „IT Security Incident“, „Incident Response“, „Incident Handling“ oder „Krise“) (siehe 5.1.1 Termini)
5. Wissen über die verschiedenen Rollen, Aufbauorganisationen und Verantwortlichkeiten im Security Incident (siehe 5.1.1 Personal, Rollen und Verantwortlichkeiten)
6. Wissen über die Zuordnung von Aufgaben zu Rollen im Security Incident (siehe 5.1.1 Personal, Rollen und Verantwortlichkeiten)
7. Wissen über die Aufgaben eines Incident Koordinators (siehe 5.1.1 Personal, Rollen und Verantwortlichkeiten)
8. Wissen über die verschiedenen Prozessmodelle des Incident Handlings (siehe 5.1.1 Allgemeine pro-

zessbezogene Anforderungen)

9. Wissen über die Intention der Prozessmodelle (siehe 5.1.1 Allgemeine prozessbezogene Anforderungen)
10. Wissen über die Verbindungen des Incident Handling Prozesses in andere Prozesse (z.B. Business Continuity Management) (siehe 5.1.1 Allgemeine prozessbezogene Anforderungen)
11. Wissen über die priorisiert in einem Security Incident durchzuführenden Aufgaben (siehe 5.1.1 Allgemeine prozessbezogene Anforderungen)
12. Wissen über die Voraussetzungen und notwendigen Strukturen für Security Incident Handling (siehe 5.1.1 Prozess – Phase Plan and prepare)
13. Wissen über die notwendigen Policies, Prozesse und Konzepte für einen Security Incident (siehe 5.1.1 Prozess – Phase Plan and prepare)
14. „K0677: Knowledge of cybersecurity policies and procedures“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare)
15. „K0679: Knowledge of privacy policies and procedures“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare)
16. Wissen über die Bedeutung von internen und externen Kommunikationskanälen zu Stakeholdern (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
17. Wissen über die Aufbaumöglichkeiten und Aufgaben eines Point of Contact (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Detect and report)
18. Wissen über den Nutzen von Threat Intelligence (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Detect and report)
19. „K0682: Knowledge of cybersecurity threats“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Detect and report)
20. „K0684: Knowledge of cybersecurity threat characteristics“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Detect and report)
21. „K0751: Knowledge of system threats“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Detect and report)
22. „K0752: Knowledge of system vulnerabilities“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Detect and report)
23. „K0683: Knowledge of cybersecurity vulnerabilities“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Detect and report)

24. „K0833: Knowledge of cyberattack actor characteristics“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Detect and report)
25. Wissen über Reaktionsmöglichkeiten als Handlungsoptionen auf Sicherheitsvorfälle (siehe 5.1.1 Prozess – Phase Plan and prepare)
26. Wissen über die benötigten Informationen und Informationsquellen in einem Security Incident (siehe 5.1.1 Prozess – Phase Plan and prepare)
27. Wissen über die Bedeutung von *Vulnerability Disclosures* (siehe 5.1.1 Prozess – Phase Plan and prepare)
28. Wissen über die Wichtigkeit kontinuierlicher Verbesserung (siehe 5.1.1 Prozess – Phase Plan and prepare)
29. Wissen über die Bedeutung von Incident Response Capability Monitoring (siehe 5.1.1 Prozess – Phase Plan and prepare)
30. Wissen über technische Systeme im Incident Handling zur Detektion und Response (beispielsweise IDS/IPS oder EDR) (siehe 5.1.1 Prozess – Phase Plan and prepare)
31. Wissen über die Bedeutung von Visibilität von Systemen im Security Incident (siehe 5.1.1 Prozess – Phase Plan and prepare)
32. Wissen über die Charakteristiken und Vorteile von Incident Handling-Übungen (siehe 5.1.1 Prozess – Phase Plan and prepare)
33. Wissen über die Bedeutung von Wertschöpfungsketten und Organisationszielen (siehe 5.1.1 Prozess – Phase Plan and prepare)
34. „K0675: Knowledge of risk management processes“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare)
35. Wissen über die Verbindungen des Risikomanagementprozesses ins Incident Handling (siehe 5.1.1 Prozess – Phase Plan and prepare)
36. „K1079: Knowledge of web application security risks“ [4] (siehe 5.1.1 Prozess – Phase Plan and prepare)
37. Wissen über die Quellen zur Detektion von Security Incidents (siehe 5.1.1 Prozess – Phase Detect and report)
38. „K0732: Knowledge of intrusion detection tools and techniques“ [4] (siehe 5.1.1 Prozess – Phase Detect and report)
39. Wissen über die Reportingprozesse von Security Incidents (siehe 5.1.1 Prozess – Phase Detect and report)

40. Wissen über den Zweck der Triage von Systemen und Events (siehe 5.1.1 Prozess – Phase Assess and decide)
41. Wissen über die Folgen und Auswirkungen der Entscheidung *Incident or not?* (siehe 5.1.1 Prozess – Phase Assess and decide)
42. Wissen über Werkzeuge strukturierter Entscheidungsfindung (z.B. OODA-Loop) (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
43. Wissen über die Folgen der Eskalation oder der Hochstufung von Security Incidents (siehe 5.1.1 Prozess – Phase Assess and decide)
44. Wissen über verschiedene Herangehensweisen in der Analyse von Security Incidents (z.B. mittels W-Fragen (ISO 27035) oder Root Cause Analyse (NIST SP 800-61)) (siehe 5.1.1 Prozess – Phase Assess and decide)
45. Wissen über die auf kompromittierten Systemen auffindbaren Evidenzen und der dahinterstehenden Analysetätigkeit (siehe 5.1.1 Prozess – Phase Assess and decide)
46. „K0969: Knowledge of cyber-attack tools and techniques“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
47. „K0783: Knowledge of network attack characteristics“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
48. „K0832: Knowledge of cyberattack characteristics“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
49. Wissen über die Bedeutung der Tätigkeiten im Bereich Respond (Response (Containment, Eradication, Recovery), Reporting) (siehe 5.1.1 Prozess – Phase Respond)
50. „K0726: Knowledge of incident handling tools and techniques“ [4] (siehe 5.1.1 Prozess – Phase Respond)
51. Wissen über die notwendigen Inhalte in einem Response Procedure (siehe 5.1.1 Prozess – Phase Respond)
52. Wissen über verschiedene Recoverystrategien und ihre Vor- und Nachteile (siehe 5.1.1 Prozess – Phase Respond)
53. „K0701: Knowledge of data backup and recovery policies and procedures“ [4] (siehe 5.1.1 Prozess – Phase Respond)
54. „K0709: Knowledge of business continuity and disaster recovery (BCDR) policies and procedures“ [4] (siehe 5.1.1 Prozess – Phase Respond)
55. Wissen über den Aufbau und die Inhalte eines stakeholderübergreifenden Incident Reports (siehe 5.1.1

Prozess – Phase Respond)

56. Wissen über die Bedeutung von Lessons learned und kontinuierlicher Verbesserung (siehe 5.1.1 Prozess – Phase Learn lessons)
57. Wissen über die Bereiche der Verbesserung (Incident Handling selbst, Security Controls oder Policies und Prozesse)
58. Wissen über die Nutzungsmöglichkeiten eines Security Incident Reports für die betroffene Organisation (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
59. Wissen über die Unterschiede von internem und externem Reporting (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
60. Wissen über typische Empfänger eines Security Incident Reports (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
61. Wissen über Best Practices im Bereich der Incident-Kommunikation (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
62. „K0676: Knowledge of cybersecurity laws and regulations“ [4] (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
63. „K0678: Knowledge of privacy laws and regulations“ [4] (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
64. Wissen über die Grundprinzipien der Arbeit des Coordination Teams (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Koordination)
65. Wissen über die Voraussetzungen zur Zusammenarbeit (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Koordination)
66. Wissen über die Besonderheiten der koordinierten Phasen (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Koordination)
67. „K0778: Knowledge of enterprise information technology (IT) architecture principles and practices“ [4] (siehe 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)
68. „K0710: Knowledge of enterprise cybersecurity architecture principles and practices“ [4] (siehe 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)
69. „K0870: Knowledge of enterprise architecture (EA) reference models and frameworks“ [4] (siehe 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)
70. „K0871: Knowledge of enterprise architecture (EA) principles and practices“ [4] (siehe 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)
71. Wissen im Bereich Notfallmanagement (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen

treffen)

72. Wissen im Bereich MITRE Attack Framework (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
73. Wissen im Bereich Cyber Kill Chain (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
74. „K0844: Knowledge of cyber attack stages“ [4] (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
75. Wissen im Bereich der Phasen eines Incident Handling Standards (beispielsweise ISO 27035 oder NIST SP 800-61) (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
76. „K0724: Knowledge of incident response principles and practices“ [4] (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
77. „K0845: Knowledge of cyber intrusion activity phases“ [4] (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)

Auch im Bereich Knowledge finden sich vorgefertigte Knowledge-Statements der NIST, die sich auf Security Architecture beziehen (Interview B.1):

78. „K0680: Knowledge of cybersecurity principles and practices“ [4]
79. „K0689: Knowledge of network infrastructure principles and practices“ [4]
80. „K0681: Knowledge of privacy principles and practices“ [4]
81. „K0685: Knowledge of access control principles and practices“ [4]
82. „K1014: Knowledge of network security principles and practices“ [4]
83. „K0837: Knowledge of hardening tools and techniques“ [4]
84. „K0791: Knowledge of defense-in-depth principles and practices“ [4]
85. „K0829: Knowledge of account creation policies and procedures“ [4]
86. „K0830: Knowledge of password policies and procedures“ [4]
87. „K0934: Knowledge of data classification policies and procedures“ [4]
88. „K0898: Knowledge of cloud service models and frameworks“ [4]

Skill-Statements

Insbesondere bei den in der Work Role *Incident Response* beschriebenen Skill-Statements wurden beschreibungsgemäß organisatorische und technische Skills aufgeführt [4]. Diese werden aber zum Großteil durch andere Lehrveranstaltungen an der Fachhochschule St. Pölten abgedeckt [63] und werden deshalb an dieser Stelle nicht weiter ausgeführt.

1. Fähigkeit, anhand einer Definition zwischen Security Event und Security Incident zu unterscheiden (siehe 5.1.1 Termini)
2. Fähigkeit, die Auslastung verschiedener Rollen in den Phasen des Security Incidents einzuschätzen (siehe 5.1.1 Personal, Rollen und Verantwortlichkeiten)
3. Fähigkeit, eine Incident Handling-Struktur mit Rollen und Verantwortlichkeiten ad hoc aufzubauen, sofern sie noch nicht vorhanden ist (siehe 5.1.1 Personal, Rollen und Verantwortlichkeiten)
4. Fähigkeit, ein Incident Handling Prozessmodell an die Organisation angepasst anzuwenden (siehe 5.1.1 Allgemeine prozessbezogene Anforderungen)
5. Fähigkeit, Aufgaben zu evaluieren und zu priorisieren (siehe 5.1.1 Allgemeine prozessbezogene Anforderungen)
6. Fähigkeit, Prozesse zu entwerfen und zu implementieren (siehe 5.1.1 Prozess – Phase Plan and prepare)
7. Fähigkeit, Prozesse zu verbessern (siehe 5.1.1 Prozess – Phase Plan and prepare)
8. Fähigkeit, Policies zu entwerfen und zu implementieren (siehe 5.1.1 Prozess – Phase Plan and prepare)
9. Fähigkeit, Policies zu verbessern (siehe 5.1.1 Prozess – Phase Plan and prepare)
10. Fähigkeit, Konzepte zu erstellen und umzusetzen (siehe 5.1.1 Prozess – Phase Plan and prepare)
11. Fähigkeit, Konzepte zu verbessern (siehe 5.1.1 Prozess – Phase Plan and prepare)
12. Fähigkeit, interne und externe Kommunikationskanäle aufzubauen und offen zu halten (siehe 5.1.1 Prozess – Phase Plan and prepare)
13. Fähigkeit, einen Point of Contact zu konzipieren und zu implementieren (siehe 5.1.1 Prozess – Phase Plan and prepare und 5.1.1 Prozess – Phase Detect and report)
14. Fähigkeit, einen Flow-Plan für verschiedene Arten von Security Incidents zu erstellen (Playbooks) (siehe 5.1.1 Prozess – Phase Plan and prepare)
15. Fähigkeit, die Visibilität von Systemen und im Netzwerk zu evaluieren (siehe 5.1.1 Prozess – Phase Plan and prepare)
16. Fähigkeit, die Visibilität von Systemen und im Netzwerk zu erhöhen (siehe 5.1.1 Prozess – Phase Plan and prepare)
17. Fähigkeit, Incident Handling-Übungen zu konzipieren (siehe 5.1.1 Prozess – Phase Plan and prepare)
18. Fähigkeit, Incident Handling-Übungen durchzuführen (siehe 5.1.1 Prozess – Phase Plan and prepare)
19. Fähigkeit, kritische Dienste und Ziele einer Organisation zu identifizieren (siehe 5.1.1 Prozess – Phase Plan and prepare)
20. Fähigkeit, sicherheitsrelevante Events über verschiedene Quellen hinweg zu identifizieren (siehe 5.1.1

Prozess – Phase Detect and report)

21. Fähigkeit, sicherheitsrelevante Events über verschiedene Quellen hinweg zu korrelieren (siehe 5.1.1 Prozess – Phase Detect and report)
22. Fähigkeit, Threat Intelligence Recherchen durchzuführen (siehe 5.1.1 Prozess – Phase Detect and report)
23. Fähigkeit, eine Triage von Systemen durchzuführen (siehe 5.1.1 Prozess – Phase Assess and decide)
24. Fähigkeit, eine Triage von Security Events durchzuführen (siehe 5.1.1 Prozess – Phase Assess and decide)
25. Fähigkeit, Evidenzen zu systematisieren (siehe 5.1.1 Prozess – Phase Assess and decide)
26. „S0589: Skill in preserving digital evidence integrity“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
27. „S0607: Skill in collecting digital evidence“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
28. „S0608: Skill in processing digital evidence“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
29. „S0609: Skill in transporting digital evidence“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
30. Fähigkeit, aufgrund von gesammelter Evidenzen Entscheidungen zu treffen (siehe 5.1.1 Prozess – Phase Assess and decide und 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
31. Fähigkeit, einen Sicherheitsvorfall zu klassifizieren (siehe 5.1.1 Prozess – Phase Assess and decide)
32. Fähigkeit, einen Sicherheitsvorfall zu priorisieren (siehe 5.1.1 Prozess – Phase Assess and decide)
33. Fähigkeit, einen Incident strukturiert methodisch (z.B. mit W-Fragen oder Root Cause Analyse) zu analysieren (siehe 5.1.1 Prozess – Phase Assess and decide)
34. „S0544: Skill in recognizing vulnerabilities“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
35. „S0080: Skill in performing damage assessments“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
36. Fähigkeit, alle kompromittierten Systeme zu identifizieren (siehe 5.1.1 Prozess – Phase Assess and decide)
37. „S0547: Skill in identifying malware“ [4] (siehe 5.1.1 Prozess – Phase Assess and decide)
38. Fähigkeit, Analyseschritte zu dokumentieren (siehe 5.1.1 Prozess – Phase Assess and decide und 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
39. „S0550: Skill in reporting malware“ [4] (siehe 5.1.1 Prozess – Phase Detect and report)
40. Fähigkeit, die Response-Phase mittels Response Procedure zu planen (siehe 5.1.1 Prozess – Phase Respond)
41. Fähigkeit, ein vollständiges Containment gemäß Response Procedure durchzuführen (siehe 5.1.1 Prozess – Phase Respond)

42. „S0549: Skill in containing malware“ [4] (siehe 5.1.1 Prozess – Phase Respond)
43. Fähigkeit, eine Eradication gemäß Response Procedure durchzuführen (siehe 5.1.1 Prozess – Phase Respond)
44. Fähigkeit, eine geeignete Recoverystrategie zu wählen (siehe 5.1.1 Prozess – Phase Respond)
45. „S0805: Skill in designing incident responses“ [4] (siehe 5.1.1 Prozess – Phase Respond)
46. Fähigkeit, eine Recovery gemäß Response Procedure durchzuführen (siehe 5.1.1 Prozess – Phase Respond)
47. „S0806: Skill in performing incident responses“ [4] (siehe 5.1.1 Prozess – Phase Respond)
48. Fähigkeit, einen Incident Report sowohl für technisches als auch für nichttechnisches Publikum zu gestalten (siehe 5.1.1 Prozess – Phase Respond und 5.1.2 Dokumentation und Reporting)
49. Fähigkeit, ein Post-Incident-Review durchzuführen (siehe 5.1.1 Prozess – Phase Learn lessons)
50. Fähigkeit, Metriken zum Incident Handling zu erheben (siehe 5.1.1 Prozess – Phase Learn lessons)
51. Fähigkeit, eine strukturierte Analyse der Verbesserungsmöglichkeiten durchzuführen (siehe 5.1.1 Prozess – Phase Learn lessons)
52. „S0509: Skill in evaluating security products“ [4] (siehe 5.1.1 Prozess – Phase Learn lessons)
53. Fähigkeit, eine strukturierte Analyse der Verbesserungsmöglichkeiten aufzuarbeiten und damit deren Implementierung zu planen (siehe 5.1.1 Prozess – Phase Learn lessons)
54. Fähigkeit, die Ereignisse in einem Security Incident nachvollziehbar zu dokumentieren (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Dokumentation und Reporting)
55. Fähigkeit, komplexe Sachverhalte grafisch aufzubereiten (siehe 5.1.2 Dokumentation und Reporting und 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)
56. Fähigkeit, komplexe Sachverhalte mündlich managementtauglich zu erklären (siehe 5.1.2 Kommunikation)
57. Fähigkeit, Kommunikationsprozesse zu gestalten und im Bedarfsfall steuernd einzugreifen (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
58. Fähigkeit, eine Kommunikationsstruktur außerhalb potenziell kompromittierter Systeme aufzubauen (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
59. Fähigkeit, Incident Handling in allen Phasen koordiniert durchzuführen (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Koordination)
60. „S0821: Skill in collaborating with internal and external stakeholders“ [4] (siehe 5.1.1 Prozessphasenübergreifende Tätigkeiten: Kommunikation)
61. Fähigkeit, Vorbereitungsworkshops für Incident Handling durchzuführen (siehe 5.1.2 Kundenumfeld

und Dienstleistungen und 5.1.2 Aufgaben in der Preparation)

62. Fähigkeit, unter Zeitdruck zu arbeiten (siehe 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)
63. Fähigkeit, selbstbewusst aufzutreten (siehe 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)
64. Fähigkeit, Prozesse einer Organisation schnell zu verstehen (siehe 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)
65. Fähigkeit, einen Security Incident anhand von Modellen (beispielsweise Cyber Kill Chain oder MITRE Attack Framework) zu beschreiben (siehe 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)
66. Fähigkeit, notwendige personelle Ressourcen in einem Security Incident einzuschätzen (siehe 5.1.2 Zusammenhänge verstehen und Entscheidungen treffen)
67. „S0572: Skill in detecting host- and network-based intrusions“ [4] (siehe 5.1.2 Allgemeine Anforderungen an Berufseinsteiger:innen)

5.2. Didaktische Überlegungen

Ausgehend von einem Vollzeitstudium findet die Lehrveranstaltung *Incident Response* derzeit gemeinsam mit den Lehrveranstaltungen CDC Fundamentals, Data Science for Security, Identity and Access Management, OT Fundamentals and Security und Privacy and Law im ersten Semester des Information Security-Studiums statt. [63] Bei der Analyse der Anforderungen fielen die Abhängigkeiten von *Threat Modeling and Intelligence*, das allerdings erst im zweiten Semester verortet ist, auf. Die Abhängigkeiten von *Incident Response* zu *Threat Modeling and Intelligence* dürften hingegen geringer ausfallen, weshalb ein Tausch der beiden Lehrveranstaltungen anzuraten ist.

Damit untrennbar verbunden ist das Vorwissen, das die Studierenden in die Lehrveranstaltung mitbringen müssen (siehe 2.3.1 Didaktische Rekonstruktion). Aufgrund der aktuellen Position im Curriculum können nur die Inhalte und erworbenen Fähigkeiten des Bachelorstudiums vorausgesetzt werden. Wie bereits ausgeführt wurde, wäre es sinnvoll, auch Threat Modeling and Intelligence als Grundlagenwissen heranziehen zu können (siehe 5.2.1 Perspektive der Studierenden).

Zur Konzeption der Lehrveranstaltung zum aktuellen Zeitpunkt kann festgehalten werden, dass diese, wie alle anderen Lehrveranstaltungen im Curriculum des Studienganges Master Information Security mit Ausnahme des Diplomandenseminars und der Diplomarbeit [63], mit 5 ECTS, also einem Gesamtaufwand von etwa 125 Stunden, veranschlagt ist. [42]

Dabei ist derzeit eine geblockte Lehrveranstaltung in diesem Ausmaß an der Fachhochschule St. Pölten im Regelfall in drei Wochen mit jeweils drei Lehrveranstaltungstagen in der Woche im Lehrveranstaltungsplan

vorgesehen. Geht man von einer Dauer der Vorlesungs- und Übungsphase von zwei der drei Wochen und einem durchschnittlichen Aufwand von 8 Stunden pro Tag, inklusive Vor- und Nachbereitung der Studierenden, aus, bleiben 3 ECTS, also in etwa 75 Stunden pro Person, für die Bearbeitung und die Nachbereitung, die Dokumentation und das Reporting der Cyberrange. Dieser Aufwand scheint für ein Szenario gemäß Grobkonzept für die genannten Aufgaben realistisch. Dazu wurden jeweils 25 Stunden für die Vorbereitung, die tatsächliche Durchführung an drei aufeinanderfolgenden Tagen ohne vorgegebene Pausen und für die Nachbereitung, die auch das Verfassen des Reports beinhaltet, veranschlagt.
Darüber hinaus wurde die Sozialform für die Durchführung der Übung als Gruppenaufgabe festgelegt. Laut Informationsseite der Fachhochschule St. Pölten werden pro Jahr 36 Plätze im berufsbegleitenden und 10 Plätze im Vollzeitstudium angeboten [63], weshalb die Größe der Gesamtgruppe auch in diesem Bereich einzuordnen ist. Im Rahmen der praktischen Abschlussübungen ist dies von Bedeutung, da die Gruppe in mehrere Kleingruppen, deren Größe je nach Szenarioumfang und -schwierigkeit gestaltet werden muss, aufgeteilt werden muss. Da eine geringfügige Anpassung der Szenarien pro Gruppe angedacht ist, erhöht das den Vorbereitungsaufwand, je nach Anzahl der Gruppen, erheblich.

5.2.1. Perspektive der Studierenden

Da die Lehrveranstaltung für die Fachhochschule St. Pölten erstellt wird, wird die Annahme getroffen, dass der Wissensstand der Studierenden dem Bachelorabschluss in IT-Security an der FH St. Pölten entspricht. Alternativ kann die Aufnahme in den Studiengang zwar beispielsweise auch mit einem „[a]bgeschlossene[n] gleichwertige[n] Studium an einer anerkannten [...] postsekundären Bildungseinrichtung“ [64] erfolgen, „wobei mindestens 12 ECTS im Bereich IT-Security und/oder Sicherheitsmanagement abgedeckt sein müssen“ [64], jedoch wird davon ausgegangen, dass aufgrund der Zugangsvoraussetzungen auch Abschlüsse anderer Universitäten oder Fachhochschulen gleichwertig sind und damit einhergehend auch das Vorwissen annähernd äquivalent ist.
Unter der Annahme, mit 18 Jahren die standardisierte Reifeprüfung abzulegen, gegebenenfalls danach einen Präsenz- oder Zivildienst in der Dauer von sechs bis neun Monaten ableisten zu müssen, daran anschließend ein Bachelorstudium an einer Fachhochschule zu beginnen und direkt nach Abschluss desselben das Masterstudium Information Security zu absolvieren, sind die Studierenden in etwa zwischen 21 und 30 Jahren alt, wobei dies für berufsbegleitend Studierende nicht unbedingt gelten muss. Aufgrund dessen und der freien Studienwahl kann davon ausgegangen werden, dass die kognitiven und motivationalen Ressourcen zur Bearbeitung des Themas durch die Studierenden ohne gröbere Steuerungsmaßnahmen durch die Lehrveranstaltungsleitung bereitgestellt werden können. Auch ermöglicht die Volljährigkeit aller Studierenden das

oben beschriebene Setting (siehe 5.2 Didaktische Überlegungen).

Da als Unterrichtssprache, wie in den anderen Lehrveranstaltungen, Deutsch angegeben ist [63], ist zudem nicht davon auszugehen, dass sprachliche Barrieren bestehen. Da sämtliche Fachbegriffe, sofern diese nicht in 5.1.1 Termini aufgeführt und daher im Rahmen der vorangehenden Lehrveranstaltung zu unterrichten sind, als bekannt angenommen werden können, ist auch auf der fachsprachlichen Ebene nicht von Verständnisschwierigkeiten auszugehen.

Eine größere Herausforderung könnten hingegen die anzutreffenden Präkonzepte darstellen, die aufgrund der unterschiedlichen Vorerfahrung zwischen berufsbegleitend und Vollzeit Studierenden schwierig abzuschätzen und sicherlich nicht abschließend aufzuzählen sind. Insbesondere berufserfahrene Personen haben möglicherweise einen oder mehrere Sicherheitsvorfälle in der Praxis miterlebt oder sogar bei der Lösung dieser unterstützt. Dies bedeutet aber nicht, dass das Incident Handling im damaligen Fall strukturiert abgelaufen sein muss. Deshalb kann es bereits zu einem induktiven Schluss gekommen sein, wie das Lösen von Sicherheitsvorfällen zu geschehen hat. Instinktiv könnte auch der erste Reflex nach Erkennen eines Security Events sein, sofort mit dem Containment zu beginnen, was, sollte ein vollständiges Containment nicht erfolgreich sein, da wesentliche Teile des Angriffes durch die voreilige Aktion übersehen wurden, zu weiterem und größerem Schaden führen könnte. Im Zuge der Vermittlung ist daher ein besonderer Wert darauf zu legen, diese Konzepte zu erheben, sie zu thematisieren und eine strukturierte, wissenschaftliche Vorgangsweise bei Security Incidents zu erarbeiten. Dabei sollen die vorhandenen Erfahrungen wertgeschätzt, jedoch auch die Nachteile einer unstrukturierten Vorgangsweise erörtert und die Vorteile einer einem strukturierten Prozess folgenden Abarbeitung von Security Incidents erfahrbar gemacht werden. Dadurch soll eine Hinwendung zu der wissenschaftlich fundierten Abwicklung bewirkt werden.

5.2.2. Lernziele

Aus der Analyse der TKS-Statements in Kapitel 5.1.4 gehen zahlreiche Tasks, Knowledge und Skills hervor, die für Incident Handler relevant sind. Eine Lehrveranstaltung mit dem vorgegebenen Stundenmaß kann dabei unmöglich all diese Bereiche abdecken, ohne Qualitätsverlust in den gelehrten Kompetenzen zu erleiden. Da eine rein oberflächliche Thematisierung vermieden und stattdessen auf ein tiefgreifendes Verständnis und die Anwendung des Gelernten gesetzt werden soll, wurden für die Lernziele die zentralen Tasks, Knowledge und Skills herausgegriffen. Als Kriterium für die Ermittlung dieser TKS wurde die Nennung dieses Statements als wichtige organisatorische Anforderung an Incident Handler durch einen Interviewpartner festgelegt. Auch Lernziele, die als Voraussetzung für eine genannte Anforderung fungieren, wurden mitaufgenommen. Ebenso Voraussetzung war dabei, dass diese nicht durch andere Lehrveranstaltungen abgedeckt

sind und nach Absolvierung einer Incident Handling-Lehrveranstaltung von den Studierenden unbedingt beherrscht werden müssen. Ebenso fand die These, nicht alle notwendigen Fähigkeiten seien im Rahmen einer universitären Ausbildung erlernbar, Eingang in die Auswahl der Lernziele, da über die Erreichbarkeit der Lernziele in diesem Kontext reflektiert wurde.

Daraus ergaben sich die folgenden Lernziele (siehe 2.3.3 Lernziele), die den in 2.3.3 Bloom'sche Taxonomie erklärten Ebenen zugeordnet wurden:

1. Die Studierenden kennen die Voraussetzungen und notwendigen Strukturen für ein effektives Incident Handling (Knowledge 12) (L2). Sie können die Intention und die Phasen verschiedener Incident Handling-Prozessmodelle sowie der zugehörigen Publikationen (z.B. ISO 27035, NIST SP 800-61) beschreiben und eines der Prozessmodelle an eine Organisation angepasst anwenden (Knowledge 9, 75, Skill 4) (L3).
2. Die Studierenden können verschiedene Arten von IT Security Incidents nennen und diese klassifizieren und priorisieren (Task 1, 41, 42, Knowledge 3, Skills 1, 31, 32) (L5).
3. Die Studierenden können Anforderungen der Organisation an das Incident Handling, beispielsweise aus dem Risikomanagement, dem ISMS, der Prozesslandschaft oder den Wertschöpfungsketten und Organisationszielen identifizieren und die Ergebnisse der Identifikation beurteilen (Task 7, Knowledge 33, Skill 64) (L5). Sie können kritische Dienste ermitteln (Skill 19) (L3) und auf Basis dessen Aufgaben evaluieren und priorisieren (Skill 5) (L5).
4. Die Studierenden kennen eine mögliche Aufbauorganisation für das Incident Handling (L1) und können diese sowohl geplant als auch ad hoc während eines Incidents etablieren und anpassen (Tasks 3, 4, Skill 3) (L6). Sie können die darin enthaltenen Rollen und Verantwortlichkeiten, insbesondere die Rolle des Incident Koordinators, erklären (Knowledge 5, 7) (L2).
5. Die Studierenden können die Inhalte von Erst- bzw. Scopinggesprächen bei IT-Sicherheitsvorfällen benennen (Task 38) (L1). Sie können mit internen und externen Stakeholdern sowie Behörden kommunizieren (Task 69) und die Best Practices in der Incident-Kommunikation anwenden (Knowledge 61) (L3).
6. Die Studierenden können den Wirkbereich, die Dringlichkeit und die Auswirkungen eines Informationssicherheitsvorfalles untersuchen (Task 2, Skill 35) (L5). Sie können während eines Sicherheitsvorfalles damit verbundene Risiken identifizieren (Task 20, Skill 23), Sicherheitslücken bewerten (Task 22), passende Bedrohungsinformationen interpretieren und verknüpfen (Task 10) und alle kompromittierten Systeme im Netzwerk identifizieren (Skill 36) (L5).
7. Die Studierenden können Assets identifizieren (Task 24) und die Erhöhung der Visibilität in kleineren

und mittleren Netzwerken planen und durchführen (Task 43) (L6). Sie kennen Systeme zur Detektion und Response (Knowledge 30) (L1), können deren Detektionen interpretieren und Gründe für diese identifizieren (Task 25, 30) (L5). Sie können die Ursache eines Sicherheitsvorfalles mittels Auswertung von W-Fragen oder Root Cause Analysis-Tätigkeiten schlussfolgern (Task 44, Knowledge 44, Skill 33) (L4).

8. Die Studierenden können den Zweck und den Vorgang der Triage von Systemen und Security Events erklären (Knowledge 40) (L1) und diese durchführen (Task 28, Skill 23, 24) (L3). Sie können Erkenntnisse aus verschiedenen Systemen über verschiedene Quellen hinweg identifizieren, korrelieren (Task 29, Skill 20, 21) und daraus Kompromittierungsindikatoren ableiten (Task 31) (L6).
9. Die Studierenden können Reaktionsmöglichkeiten auf typische Sicherheitsvorfälle (Knowledge 25) nennen (L1), bewerten (L5) und Containment-, Eradication- und Recoverymaßnahmen in einem Response Procedure Plan vorbereiten (Task 45, 46, 48, 49, 52, 54, Skill 40, 44) und durchführen (Task 50, 53, 55, Skill 41, 43) (L3).
10. Die Studierenden können auf Basis von vorliegenden Fakten im Security Incident Schlüsse ziehen (Task 32) (L4), Entscheidungen treffen (Task 33) (L5) oder die Grundlage dafür vorbereiten und Informationen aufbereiten (Task 34) (L4). Dabei können sie Werkzeuge zur strukturierten Entscheidungsfindung anwenden (Knowledge 42) (L3). Sie können die Folgen einer Entscheidung (z.B. *Incident or not*) analysieren (Knowledge 41) (L4) und Empfehlungen oder Nicht-Empfehlungen entwerfen und managementtauglich kommunizieren (L6).
11. Die Studierenden können Lagedarstellungen bzw. Lagebilder zielgruppengerecht erstellen (Task 37) (L6), grafisch aufarbeiten (Skill 55) und mündlich managementtauglich erklären (Skill 56) (L2). Dazu können sie Informationen und die durchgeführten Analyseschritte dokumentieren (Tasks 60, 61) (L1) und einen stakeholderübergreifenden Incident Report gestalten (Knowledge 55, Skill 48) (L6). Sie können in diesem einen Security Incident anhand von Modellen (z.B. Cyber Kill Chain oder MITRE Attack Framework) beschreiben (Skill 65, 77) (L1).
12. Die Studierenden können Playbooks (Flow-Pläne) für verschiedene IT-Sicherheitsvorfälle erstellen und anwenden (Task 13, Skill 14) (L6).
13. Die Studierenden können verschiedene Funktionen und Aufgaben in einfachen Security Incidents koordinieren, evaluieren und priorisieren (Task 6, Skill 5) (L6).

5.3. Konzeption der Cyberrange

Auf Basis der vorangegangenen Ergebnisse wurde eine Cyberrange (siehe 2.1.3 Cyberrange) als Abschlussübung für die Lehrveranstaltung zum Thema Incident Handling konzipiert, bei der das erworbene Wissen und die erlernten Fähigkeiten praktisch angewendet und vertieft werden sollen. Für die Konzeption wurde der Lifecycle von Katsantonis et al. (siehe 2.1.3 Lifecycle) genutzt.

5.3.1. Analyse

In der Cyberrange sollen die Lernziele aufgegriffen werden, sodass die damit verbundenen Inhalte vertieft und praktisch ausprobiert werden können. Zusätzlich soll der abschließende Incident Report auch einen Teilaspekt in der Beurteilung darstellen (siehe 5.2.2 Lernziele).

Neben den Lernzielen haben sich in den Interviews mit den Experten weitere Anforderungen an die Cyberrange gezeigt. Wichtig ist dabei, die Studierenden an einem realitätsnahen Beispiel üben zu lassen. (Interview B.2, Interview B.3) Dies bedeute Irrwege (Interview B.2), viele Findings, von denen die wichtigen erst durch die Studierenden identifiziert werden müssen, um diese dann im Anschluss bearbeiten zu können (Interview B.4), sowie das Verwenden und die Analyse unterschiedlicher Systeme. (Interview B.3) Darüber hinaus sollten nicht alle Informationen von Beginn an zugänglich sein. Ebenso realistisch sei es, dass Kunden falsche oder veraltete Informationen geben, worunter beispielsweise fallen könnte, dass betroffene Systeme eigentlich abgeschaltet sein sollten. (Interview B.2) Zudem sei wichtig, die Gegenmaßnahmen zu den richtigen Zeitpunkten zu setzen. Dafür wäre wünschenswert, dass sich der Angreifer im Verlauf der Cyberrange weiterbewegt. (Interview B.4)

Vorbereitend ist zudem die Erstellung von Playbooks von Interesse, mit denen dann der Security Incident bearbeitet werden soll. Anschließend sei eine Reflexion anzustellen, inwiefern das Playbook zu der vorgefundenen Situation gepasst habe und wo Lücken aufgefallen seien. (Interview B.3)

Aus organisatorischer Perspektive ist des Weiteren interessant, dass die Interviewten einen Fokus auf das abschließende Reporting legen. Schon während der Bearbeitung des Sicherheitsvorfalles solle die Erstellung von kurzen Lagebildern gefordert werden, wobei auch die Abgabe von Zwischenberichten möglich wäre. Der Abschlussbericht sei jedoch besonders wichtig. (Interview B.4) Dieser müsse dabei alle Teile inklusive einer nachvollziehbaren Timeline enthalten und managementtauglich verfasst sein. (Interview B.2) Um diese Nachvollziehbarkeit der zentralen Erkenntnisse auch zu einem späteren Zeitpunkt gewährleisten zu können, sei es besonders wichtig, das Schreiben des Abschlussberichts angeleitet im Rahmen der Lehrveranstaltung aufzubauen. (Interview B.3)

5.3.2. Design

Für den Namen wurde ChatGPT befragt[1]. Daraus wurde der Namensvorschlag *Incident Zero* als Wortspiel dafür, dass es für die meisten der Studierenden der erste Security Incident sein wird, gewählt.
In der Designphase wurde ein besonderer Wert darauf gelegt, dass die Cyberrange die im Vorlesungsteil enthaltenen Inhalte in der Praxis schult, schärft und als Grundlage für eine Beurteilung auch überprüft.

Szenariendesign

Die Studierenden nehmen im Szenario die Rolle eines externen Incident Handling-Dienstleisters ein. Diese wurde gewählt, damit, im Gegensatz zu Inhouse-Personal, kein Vorwissen über die Geschäftsprozesse, das Risikomanagement oder die IT-Landschaft vorhanden ist und dies erst im Rahmen eines Scoping-Gespräches erhoben werden muss.
Aus diesem Grund erhalten die Studierenden vor Beginn der Abschlussübung ausreichend Vorbereitungszeit, um teamintern Abläufe, Prozesse und Rollenverteilungen festzulegen und Knowledge Bases, technische Hilfsmittel und Dokumentationsplattformen selbstständig aufzubauen.
Nach der internen Vorbereitungsphase werden die Studierenden durch einen Kunden kontaktiert, der diese um Unterstützungsdienstleistungen in einem aktuellen Security Incident ersucht. Anschließend erhalten die Studierenden über eine VPN-Lösung Zugriff auf die mutmaßlich kompromittierte Infrastruktur des Unternehmens.
Das genaue Szenario, also die Beschreibung, welche Art von Security Incident simuliert wird, ist bewusst nicht festgelegt. Diese Strategie bietet mehrere Vorteile. Erstens kann die Lehrveranstaltungsleitung so bei jeder Durchführung flexibel auf derzeit aktuelle und realistische Angriffsmuster eingehen, wodurch die Realitätsnähe der Übung gewahrt bleibt und verhindert werden kann, dass veraltete, in Realität nicht mehr angewendete Angriffsszenarien beübt werden. Zweitens können so die Szenarien pro übender Kleingruppe leicht angepasst werden. Denkbar wären beispielsweise jeweils unterschiedliche initiale Eintrittsvektoren, Persistenzmechanismen oder Zielsysteme der fiktiven Angreifergruppierung. Somit ist ein nicht vorgesehenes gruppenübergreifendes Arbeiten und Austauschen von Informationen deutlich erschwert. Zusätzlich besteht somit die Möglichkeit der Binnendifferenzierung in heterogenen Lernendengruppen. Sollten starke Leistungsunterschiede und Differenzen im Vorwissen in der Gruppe bestehen, ist so die Möglichkeit, unterschiedlich schwierig zu lösende Szenarien an die Gruppen auszuspielen, gegeben. Dadurch kann die Cyberrange dem didaktischen Anspruch, allen Lernenden ein Weiterlernen zu ermöglichen, gerecht werden. Diese

[1] ChatGPT, GPT-4o mini. Prompt: Generiere Namen für den Namen einer Cyberrange der Fachhochschule St. Pölten als Abschluss des Faches Incident Handling. Sei kreativ und nenne 10 Namen.

Unterschiede im Schwierigkeitsniveau müssen im Zuge des Beurteilungsprozesses berücksichtigt werden, wobei hier anhand von Kriterien und den Lernziele prozessorientiert die Leistung der Studierenden berücksichtigt werden muss. Fehler in der Bearbeitung schwierigerer Szenarien müssen dementsprechend mit den über die Mindestanforderungen hinausgehenden Anforderungen aufgrund der höheren Komplexität des Szenarios aufgewogen werden, um zu einer fairen Beurteilung zu gelangen.

Aus diesem Grund ist darüber hinaus auch die praktische Umsetzung des Angriffes nicht statisch, beispielsweise mithilfe von vorgefertigten Playbooks, die die Angriffe automatisiert abarbeiten können, ausgeführt, da diese eine realistische Darstellung von Angreiferaktivität zumeist nicht leisten können. (Interview B.2)

Netzwerkdesign - Cyberspace

Die betroffene Infrastruktur soll einfache Enterprisenetzwerke möglichst realistisch emulieren. (Interview B.3) Dazu sind einige Sicherheitssysteme, beispielsweise ein SIEM oder EDR, in einem geringen Reifegrad, also ohne spezifische Konfiguration und nicht alle Assets abdeckend, implementiert.

Die Studierenden erhalten die Informationen zum Aufbau des Netzwerkes grundsätzlich durch eine verantwortliche Stelle beim Kunden, die durch die Lehrveranstaltungsleitung dargestellt wird. Dabei können durch diese aber auch veraltete oder unvollständige Informationen über die Systeme kommuniziert werden. (Interview B.2) So sollen die Studierenden auch angehalten werden, fehlende Informationen über eigene Investigationen, beispielsweise Asset Discovery, zu finden.

Auf Basis dieser Anforderungen wurde das folgende Basisnetzwerk für ein fiktives, großes Autohaus (BigCarCompany) designt:

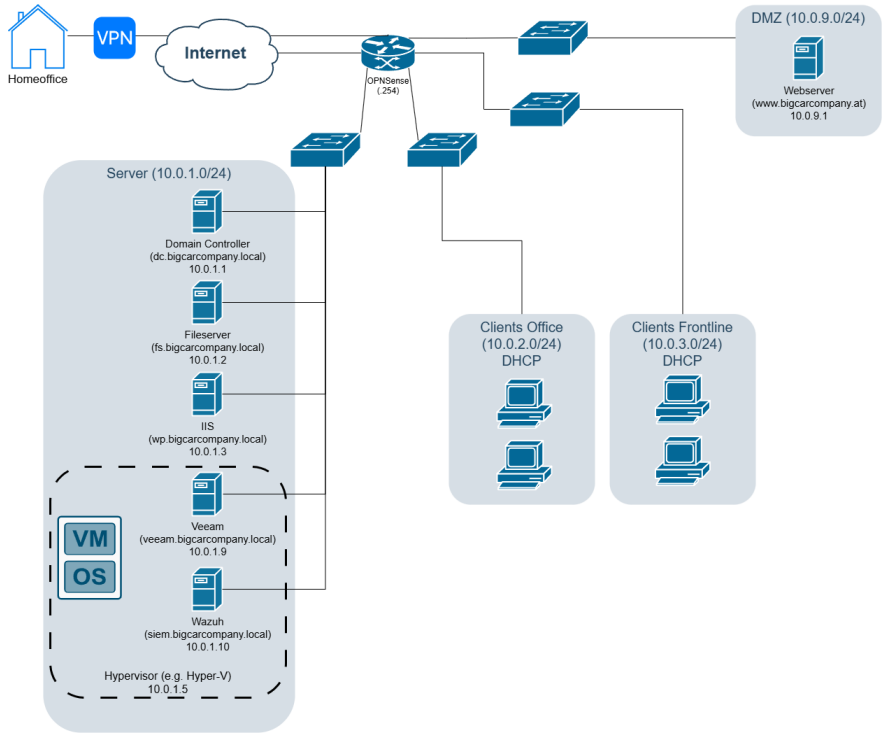

Abbildung 5.1.: Beispielhaftes, vereinfachtes Enterprisenetzwerk für die Cyberrange

Das Netzwerk besteht aus vier segmentierten Netzen: Einem Server-Netz, zwei Client-Netzen und einer DMZ.

Im Server-Netz finden sich neben der Basisinfrastruktur für eine Active Directory-Domäne (Domain Controller und File Server) auch ein interner Webserver mit einem Intranet, über den neben der Verteilung interner Informationen und Warnungen während des Security Incidents auch, beispielsweise über Schwachstellen in der verwendeten Blog-Software, ein Lateral Movement durch den Angreifer dargestellt werden könnte. Virtualisiert, beispielsweise mit Hyper-V, sind anschließend noch die Backup-Software Veeam Community Edition[2], die insbesondere bei veränderten oder zerstörten Daten im Szenario eine bedeutende Rolle spielen wird, und Wazuh[3] als Open Source XDR- und SIEM-Lösung im Einsatz.

In den beiden Client-Netzen sind eine beliebige Anzahl an Client-Computern vorhanden. Diese Anzahl ist variabel und stark vom gewählten Szenario und der gewünschen Schwierigkeit abhängig. Je mehr Systeme vorhanden sind, desto mehr Events finden sich im SIEM und desto mehr Events sind zu triagieren und zu bearbeiten. Die beiden Netze wurden auch wieder aufgrund der hohen Anzahl an möglichen Szenarien, von Insidern aus dem Office-Bereich bis hin zu unberechtigten Zugriffen vor Ort auf Frontline-Computer, deren

[2]Siehe https://www.veeam.com/de/products/free/backup-recovery.html.
[3]Siehe https://wazuh.com/.

Bildschirm nicht gesperrt wurde, auf diese Art und Weise implementiert.
Durch die Unterteilung des gesamten Netzwerkes in verschiedene Netzwerksegmente können, je nach Szenario, auch unterschiedlich restriktive Firewallregeln implementiert werden, von einer offenen Struktur mit oder ohne Logging kann auch nur eine stark eingeschränkte Kommunikation zwischen den Segmenten realisiert werden.
Über die DMZ können auch Angriffe auf öffentlich im Internet verfügbare Webserver simuliert werden, die anschließend auf die interne Infrastruktur übergreifen können.
Die Beschreibung des Cyberspace ist bewusst generisch gehalten, um der Lehrveranstaltungsleitung den notwendigen Spielraum für die Gestaltung der Szenarien zu lassen. Eine beispielhafte Konfiguration, die auch als Basis oder Inspiration für andere Szenarien genutzt werden kann, findet sich dennoch in 5.3.2 Beispielszenario.

Anforderungen und Injects während des Szenarios

Während der Übung erhalten die Studierenden durch sogenannte Injects, also Einspielungen durch die Übungsleitung, immer wieder weiterführende Lageinformationen und Aufgaben, die sie zu erfüllen haben. Um einen Fokus auf die organisatorischen Aspekte des Incident Handlings legen zu können, muss die Übungsleitung als Simulation des Kunden regelmäßige Rückfragen in verschiedenen Rollen (beispielsweise als Mitglied der Geschäftsführung, IT-Leitung oder Öffentlichkeitsarbeitsverantwortliche:r) stellen und Lagebriefings mit Lagebildern oder Update-Calls bei Situationsänderungen einfordern. Zusätzlich besteht die Möglichkeit, je nach Szenario, auch Meldungen an Behörden durchführen und die darauffolgenden Rückfragen beantworten zu lassen.
Wird die Übung vor Ort, also nicht remote, durchgeführt, so können alle Injects auch persönlich eingespielt werden.
Im Rahmen der Lehrveranstaltung soll die Cyberrange die Studierenden zwar fordern, aber nicht überfordern, um diesen den Spaß an der Disziplin Incident Handling nicht zu nehmen. Die Übungsleitung darf und soll den Gruppen also, je nach gezeigter Leistung und (Über)forderungslevel, auch unterschiedliche Ausprägungen der folgenden Injects einspielen. Insbesondere bieten sich der gewählte Zeitansatz, also die Zeit, bis zu der das Inject fertig bearbeitet sein muss, und die geforderte Ausführlichkeit des Ergebnisses als Steuerungsmechanismen an.
Möglicherweise wird also eine Gruppe, die im Szenario bereits weit fortgeschritten ist, ein zehnminütiges Lagebriefing innerhalb einer Stunde vorbereiten müssen, während eine andere Gruppe für die gleiche Aufgabe mehrere Stunden Zeit bekommt.

Beispielszenario

In dem folgenden Beispielszenario wird ein fiktiver Ransomware-Vorfall, wie er auch tatsächlich in einem österreichischen mittelständischen Unternehmen stattgefunden haben könnte, in einem Autohaus simuliert. Gerade diese Vorfälle fordern von Incident Handlern ein rasches und überlegtes Handeln, sodass der meist vollständig zum Stillstand gekommene Betrieb möglichst rasch wieder aufgenommen werden kann.
Die Aufgabe der Studierenden, die als externe Incident Handler auftreten, ist es nicht nur, die Systeme rasch wiederherzustellen, um somit den Betrieb wieder aufnehmen zu können, sondern auch die Ursache für den Sicherheitsvorfall zu finden, Handlungen und Unterlassungen zu empfehlen und die Entscheidungsgrundlage für die Geschäftsführung des Unternehmens vorzubereiten.
Details zum Szenario und der Szenarioführung finden sich im Bereich der geplanten Injects.

Konfiguration der Infrastruktur

Um das Beispielszenario praktisch umzusetzen, müssen folgende Konfigurationen auf der Infrastruktur getätigt werden:

OPNsense

- Zuweisung der virtuellen Interfaces zu den Subnetzen, anschließend Festlegen der IP-Adressen der Interfaces (jeweils 10.0.x.254)
- Herstellen der Routing-Fähigkeit zwischen den Subnetzen, Firewallregeln für freie Kommunikation zwischen den Subnetzen (internes allow any - any)
- Konfigurieren eines beliebigen VPN-Servers auf der OPNSense mit Zugriff auf alle Subnetze
- Einrichten eines VPN-Benutzers *hans.wurst*, der auf alle Subnetze zugreifen darf
- Port-Forwarding für den Webserver in der DMZ einrichten, sodass dieser aus dem „Internet“ erreichbar ist

Domain Controller

- Setzen des Computernamens auf *DC*
- Installation der DNS-Rolle, Erstellen der laut Netzwerkdiagramm notwendigen Forward- und Reverse Lookup-Zonen, Konfiguration für automatische Updates der Zonen
- Installation der Active Directory Domain Services-Rolle, Erstellen eines neuen Forests und der Domäne *bigcarcompany.local* mit dem Netbios-Namen *BIGCARCOMPANY* und dem Domain- und Forestlevel auf Windows Server 2012, ansonsten Standardeinstellungen verwenden; anschließend muss der Computer neu gestartet werden.
- Erstellen einer OU-Struktur für Benutzer, Gruppen und Computer; in der Computer-OU sollen wiederum drei Unter-OUs (*Domain Controller, Clients, Server*), in der Benutzer OU die Unter-OUs *Ge-*

schäftsführung, IT, Verkauf und KFZ-Service existieren.

- Erstellen von etwa 20 bis 30 fiktiven Benutzern in der Domäne, davon zumindest der oben genannte Benutzer *hans.wurst* sowie zumindest zwei weitere Accounts mit Domänenadministratorenprivilegien; die Benutzer müssen auf die OUs sinnvoll aufgeteilt werden.

File Server

- Setzen des Computernamens auf *FS*
- Durchführen eines Domain Joins, Verschieben des Servers in die Server-Sub-OU
- Installation der Fileserver-Rolle
- Anlegen von drei Netzlaufwerken für Geschäftsführungsdaten, Verkaufsdaten und KFZ-Servicedaten; Setzen von Full Control-Berechtigungen für alle Authentifizierten Nutzer auf allen Ordnern
- Platzieren von Bogusfiles auf den drei Fileshares; die Inhalte der Dateien sind für die Übung irrelevant

IIS

- Setzen des Computernamens auf *WP*
- Durchführen eines Domain Joins, Verschieben des Servers in die Server-Sub-OU
- Installation der IIS-Rolle
- Zusätzlich ist noch das Erstellen von Websiteinhalten möglich; für diese Übung ist das aber nicht notwendig und kann daher unterbleiben.

Hypervisor

- Setzen des Computernamens auf *HV*
- Setzen des DNS-Records
- Installation der Hyper-V-Rolle
- Erstellen von zwei virtuellen Maschinen, jeweils eine für Veeam und Wazuh
- Konfiguration der Veeam-VM: Setzen des Computernamens auf Veeam, Setzen des DNS-Records, Installation von Veeam Backup & Replication Community Edition, Durchführung der Grundkonfiguration von Veeam
- Konfiguration der Wazuh-VM: Setzen des Computernamens auf SIEM, Setzen des DNS-Records, Installation von Wazuh mit dem Installation Assistant[4]

Zentrale Konfiguration mit Gruppenrichtlinien

Folgende Einstellungen sollen anschließend zentral mit Gruppenrichtlinien konfiguriert werden:

- Gruppenrichtlinien aus dem Microsoft Security Compliance Toolkits, jeweils für Member Server,

[4] Siehe https://documentation.wazuh.com/current/installation-guide/wazuh-server/installation-assistant.html#wazuh-server-cluster-installation.

Domain Controller und Clients herunterladen und an die korrekte Stelle importieren.

- Verbinden der am Fileserver angebundenen Netzlaufwerke, jeweils auf die passende Unter-OU (Geschäftsführungsdate Netzlaufwerk soll beispielsweise nur für Benutzer in der Geschäftsführung gemappt werden)
- Softwareverteilung des Veeam Backup Agents an alle Server
- Softwareverteilung des Wazuh-Agents und Start des Wazuh-Service

Zentrale Konfiguration der Clients

Die Clients werden grundsätzlich zentral über Gruppenrichtlinien konfiguriert, weshalb im Folgenden lediglich zwei zentrale Vorbereitungsarbeiten beschrieben sind.

- Durchführen eines Domain Joins, Verschieben der Computer in die Client-Sub-OU
- Neustarten der Systeme

Im Anschluss müssen alle Event Logs auf allen Systemen, Clients wie Servern, gelöscht werden, damit keine Rückstände des Deployments mehr zu finden sind. Diese könnten im Rahmen der Untersuchung des Falles ansonsten zur Verwirrung führen, da nicht klar ist, ob es sich um Deploymentartefakte oder um absichtlich platzierte Hinweise handelt.

Injects

Für das Beispielszenario wurden folgende Injects als Richtlinien festgelegt. Wie bereits beschrieben kann es aufgrund der Niveauunterschiede innerhalb eines Studienganges notwendig sein, ad hoc weitere Injects situationsangepasst einzuspielen oder vorgegebene Injects bewusst nicht einzuspielen. Im Folgenden werden auch die zentralen TKS-Statements zu den Beispielinjects angegeben.

Scoping-Gespräch: Das Scoping-Gespräch bildet den Beginn des Szenarios für die Studierenden. In einem Gespräch mit dem Geschäftsführer erklärt dieser, dass die Gruppe ihm zur Abwehr von Hacker-Angriffen empfohlen worden sei und erzählt beunruhigt, dass alle Systeme nicht verfügbar seien und die Daten komplett verschlüsselt wären. Die Studierenden müssen den Lead in diesem Gespräch übernehmen und alle wichtigen Informationen für das nun folgende Incident Handling erhalten (Tasks 38 und 69, Knowledge 61).

Gewährung des Zugriffes: Durch einen Mitarbeiter in der IT wird der VPN-Zugang an die Gruppe übergeben, mit dem sie auf die Infrastruktur zugreifen können. Der IT-Mitarbeiter wirkt dabei überfordert und gibt auf Nachfrage zu, erst seit wenigen Wochen im Betrieb zu sein, nachdem die alte IT-Mannschaft geschlossen gekündigt hatte. Der Mitarbeiter ist dennoch hilfsbereit und drückt den Studierenden auch ein offensichtlich veraltetes Netzwerkdiagramm in die Hand, dass er von seinen Vorgängern bekommen habe (Tasks 24 und 43).

Anfrage aus dem Autohaus: Ein Autoverkäufer meldet sich beim IT-Mitarbeiter, der das Anliegen an die

Incident Handler weiterleitet: Er komme nirgendwo mehr hin, nichts gehe. Was soll er tun? Die Studierenden müssen, spätestens bei diesem Inject, klare Verhaltensweisen an die Mitarbeiter:innen kommunizieren (lassen) (Task 69, Knowledge 61).

Anfrage der Geschäftsführung (Datenschutz): Der Geschäftsführer fragt, ob er seine vorbereitete Datenschutzmeldung schon an die DSB schicken kann oder ob das Team sich die Meldung noch einmal ansehen möchte (Task 69, Knowledge 62).

Anfrage der Geschäftsführung (Zahlen oder nicht): Der Geschäftsführer fragt, ob es nicht einfacher wäre, den Ransom-Betrag zu zahlen. Er habe eine E-Mail vom Erpresser erhalten, das scheine ihm eigentlich die günstigere Variante zu sein (Task 32 bis 34, Knowledge 25, 41 und 42).

Anfrage der Geschäftsführung (Datenschutzmeldung an die Kunden): Der Geschäftsführer möchte die Kunden, egal ob er das nun müsse oder nicht, über den Angriff und die Betroffenheit ihrer personenbezogenen Daten informieren (Task 69, Knowledge 61).

Anfrage der Geschäftsführung (Lagemeldung): Der Geschäftsführer möchte eine detaillierte Lagemeldung erhalten. Dieses Inject kann regelmäßig und mit unterschiedlich langer Vorlaufzeit durch die Übungsleitung eingespielt werden (Task 37 und 60 bis 61, Skill 55 und 56).

Anfrage der Versicherung (Vertragsdienstleister): Die Cyberversicherung teilt mit, dass mit einem Vertragspartner der Versicherung zusammengearbeitet werden müsse. Dieser werde sich innerhalb der nächsten drei Tage melden und mit der Aufarbeitung des Security Incidents beginnen. Der Geschäftsführer ist außer sich (Task 32 bis 34, Skill 56, Knowledge 41 und 42).

Anfrage der Versicherung (Bericht): Die Cyberversicherung meldet, dass ein genauer und detaillierter Bericht (sowohl der Arbeiten, als auch der aufgewendeten Zeiten) notwendig sei, damit die Kosten übernommen werden könnten (Task 37, 60 und 61, Knowledge 55, Skill 55, 56, 65 und 77).

Eine detailliertere Planung, beispielsweise inklusive der Einspielzeitpunkte, ist bewusst nicht getroffen, um der Übungsleitung eine gewisse Flexibilität zu ermöglichen und auf die Fortschritte und das Vorwissen der Studierenden eingehen zu können.

Durchführung/Simulation des Angriffes

Im Folgenden wird, angelehnt an das MITRE Attack Framework, ein beispielhaftes Szenario beschrieben, das im oben angeführten Beispielnetzwerk ausgeführt werden kann.

Reconnaissance: Über eine Fake CAPTCHA-Attack[5], bei der der IT-Mitarbeiter *hans.wurst* in seinem administrativen Account über Social Engineering dazu gebracht wurde, ein schädliches Kommando in der Befehlszeile auszuführen, wurden über den RedLine-Infostealer Anmeldedaten sowie grundlegende Daten

[5] Siehe https://social.bund.de/@bsi/114092216088487773.

über das Unternehmen (beispielsweise die IP-Adresse) erbeutet (Gather Victim Identity Information: Credentials - T1589.001, Gather Victim Network Information: IP Addresses - T1590.005).

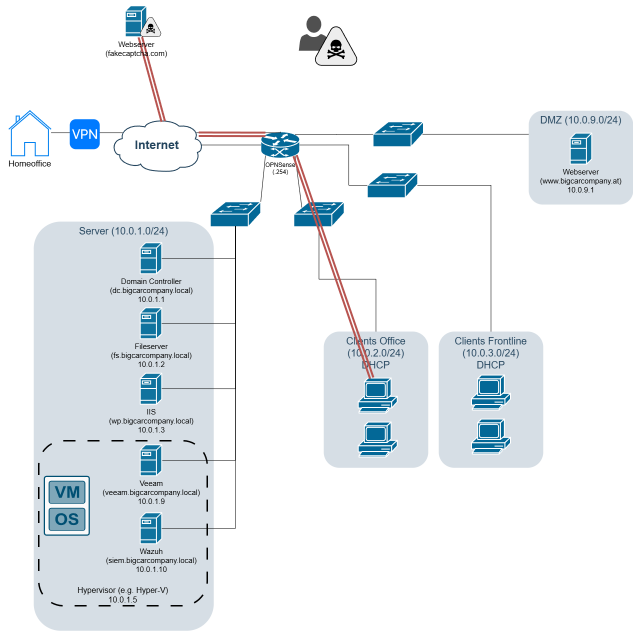

Abbildung 5.2.: Social Engineering Angriff auf den IT-Mitarbeiter

Resource Development: Der Bedrohungsakteur erhält die Daten, untersucht diese und bereitet daraufhin über einen beliebigen Ransomware-as-a-service-Anbieter eine Ransomware für den Angriff auf die Organisationen vor (Obtain Capabilities: Malware - T1588.001).

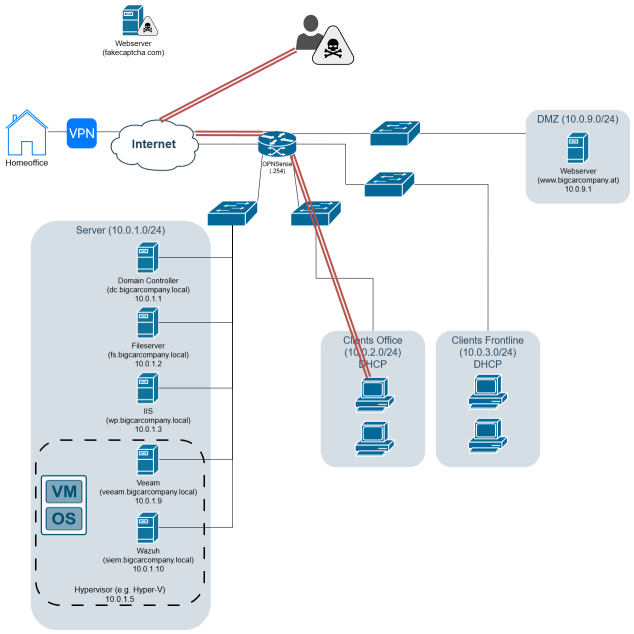

Abbildung 5.3.: Die über den Infostealer entwendeten Daten werden an den Bedrohungsakteur gesendet.

Initial Access: Der Bedrohungsakteur versucht nun über die erbeuteten Benutzerdaten einen Login auf dem VPN-Server der Organisation. Dieser gelingt; somit befindet sich der Akteur nun hinter der Firewall im internen Netz (External Remote Services - T1133).

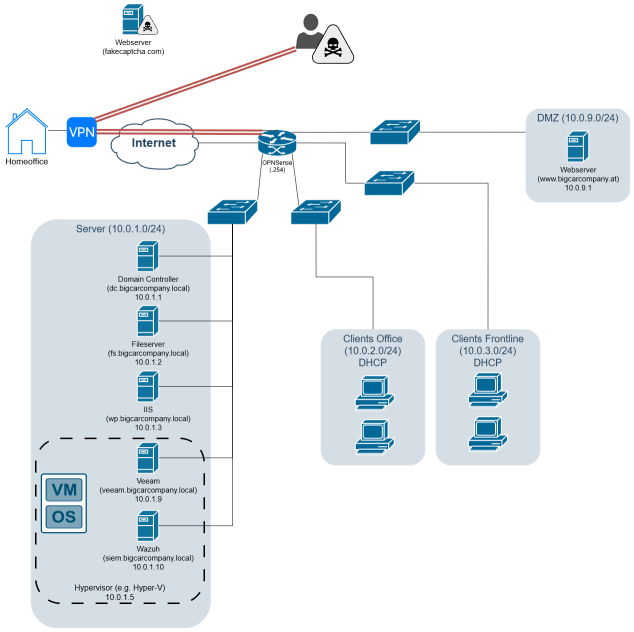

Abbildung 5.4.: Über die erhaltenen Login-Daten kann sich der Bedrohungsakteur am VPN-Server anmelden und somit Zugriff auf das Netzwerk erhalten.

Lateral Movement: Der Angreifer scannt das Netzwerk und findet den Domain Controller. Über Remote Desktop-Sitzungen meldet sich der Angreifer am Domänencontroller mit dem erbeuteten Benutzer an, der über Domänenadministratorberechtigungen verfügt (Remote Services: Remote Desktop Protocol - T1021.001).

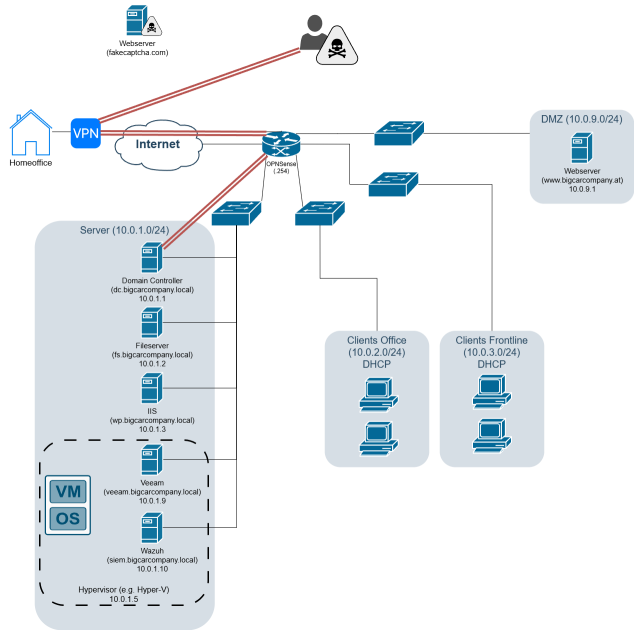

Abbildung 5.5.: Der Bedrohungsakteur bewegt sich nun auf den Domänencontroller weiter.

Persistence und Privilege Escalation: Der Angreifer legt zusätzlich noch einen Account in der Domäne an (Create Account: Domain Account - T1136.002) und berechtigt diesen über Active Directory-Gruppen, über das VPN-Gateway auf das Netzwerk zuzugreifen (Account Manipulation: Additional Local or Domain Groups - T1098.007).

Defense Evasion: Anschließend versucht der Angreifer, auf einzelnen Systemen die Windows Event Logs zu löschen, um die Nachvollziehbarkeit zu erschweren (Indicator Removal: Clear Windows Event Logs - T1070.001).

Collection: Dabei versucht der Angreifer, Daten von Netzlaufwerken (Data from Network Shared Drive - T1039) oder vom lokalen System (Data from Local System - T1005) zusammenzusammeln und somit für die Exfiltration vorzubereiten.

Exfiltration: Über ein Code Repository auf Github exfiltriert der Angreifer anschließend die Daten (Exfiltration Over Web Service: Exfiltration to Code Repository - T1567.001).

Execution: Über einen Scheduled Task, der mittels Gruppenrichtlinie an die gesamte Domäne ausgerollt wird, ist es dem Angreifer mit seinem neu erstellten Account möglich, seine Ransomware auszuführen (Scheduled Task - T1053.005).

Mögliche Lösung des Beispielszenarios

Der Lösungsweg für ein derartiges Szenario kann nie abschließend vorgegeben werden, da er von vielen Faktoren, beispielsweise dem Zeitpunkt des Entdeckens einiger Artefakte im Szenario, abhängt. Im Folgenden soll daher nur eine mögliche Lösung beschrieben werden. Wichtig ist dennoch, dass die Studierenden sich eines strukturierten Incident Handling-Modells bedienen und dieses an die Organisation und die Situation angepasst anwenden (LZ 1).

Bereits im Vorfeld wird im Rahmen der Lehrveranstaltung ein Playbook, unter anderem zu diesem Thema, erarbeitet, das die Studierenden nun, soweit möglich, auch einsetzen sollen (LZ 12).

Zu Beginn wird das Scoping-Gespräch durchgeführt, das von den Studierenden aktiv geführt werden soll (LZ 4). Darin sollen insbesondere die Wertschöpfungskette und die Prozesslandschaft des Unternehmens erfragt und verstanden sowie kritische Dienste identifiziert werden, um im Rahmen des Incident Handlings die richtigen Prioritäten zu setzen und für die Wiederherstellung dieser Dienste und Daten relevante Aufgaben zu priorisieren (LZ 2). Im Scoping-Gespräch sollen auch die Aufgaben zwischen ihnen als externem Dienstleister und der Inhouse-IT-Abteilung des Autohauses sowie der Geschäftsführung abgeklärt werden. Auf Basis dieser Informationen muss eine passende Aufbauorganisation etabliert und dokumentiert werden. Die Rolle des Incident Koordinators soll jeweils ein:e Studierende:r innehaben (LZ 3). Aufgrund des vollständigen Betriebsstillstandes kann bereits an dieser Stelle von einer hohen Priorität und, aufgrund der Beschreibung, von einem Ransomwarevorfall ausgegangen werden (LZ 5).

Da bereits zu Beginn des Incident Handling-Einsatzes eine Verschlüsselung stattgefunden hat, können direkt nach dem Scoping-Gespräch betroffene Netzwerksegmente oder das gesamte Netzwerk containt werden, da der Impact hier bereits eingetreten ist und dem Angreifer mit dem Beginn der Verschlüsselung bewusst ist, dass der Angriff bemerkt wurde (LZ 9).

Nach der Gewährung des Zugriffes kann die Gruppe bereits mit der Analyse des Sicherheitsvorfalles beginnen. Aus dem Gespräch mit dem Mitarbeiter ist bekannt, dass über das Netzwerk kein Know-How mehr vorhanden ist. Die Studierenden sollten außerdem bemerken, dass der vorhandene Netzwerkplan veraltet ist. Daher sollte zunächst mit einer Discovery von Systemen begonnen und überprüft werden, ob, beispielsweise mittels des bereits vorhandenen SIEM-Systems, überhaupt eine vollständige Visibilität im Netzwerk gegeben ist, um so alle kompromittierten Systeme ermitteln zu können (LZ 6 und 7). Sie müssen in weiterer Folge Systeme triagieren, analysieren und somit die Auswirkungen des Sicherheitsvorfalles nachvollziehen (LZ 6).

Möglichst rasch sollte auch eine interne Information an die Mitarbeiter:innen erfolgen. Hierbei sollen Best Practices der Kommunikation in Information Security Incidents eingehalten werden (LZ 4).

Da zur Durchführung echte Malware, beispielsweise der RedLine Stealer, genutzt wurde, ist es auch möglich, Bedrohungsinformationen aus dem Internet dafür zu nutzen, Kompormittierungsindikatoren abzuleiten, nach diesen zu hunten und somit alle kompromittierten Systeme im Netzwerk zu entdecken (LZ 6).

In der Analyse soll anschließend die Ursache des Sicherheitsvorfalles gefunden werden (LZ 7): Im Rahmen der Analyse des Active Directory sollte dann erkannt werden, dass eine neue Gruppenrichtlinie angelegt und über diese ein Scheduled Task zur Verschlüsselung auf alle Domänencomputer verteilt wurde. Dadurch ist auch erkannbar, von welchem Benutzer dieser Scheduled Task angelegt wurde. Da dieser Benutzer unbekannt ist und erst kurz vor der Verschlüsselung erstellt wurde, ist davon auszugehen, dass dieser durch den Angreifer kontrolliert wird. Bei einer genaueren Analyse, beispielsweise über das SIEM, kann dann der ursprünglich betroffene Benutzeraccount erkannt und, bei genauerer Prüfung der Aktivitäten dieses Benutzers, auch schlussgefolgert werden, dass es zu der Ausführung einer Stealer Malware gekommen sein muss. Somit kann angenommen werden, dass der Benutzeraccount als initaler Eintrittsvektor dadurch kompromittiert worden sein könnte. Diese Erkenntnisse können als Kompromittierungsindikatoren über mehrere Systeme hinweg korreliert werden (LZ 8).

Zusätzlich sind durch die „laute“ Vorgehensweise des Bedrohungsakteurs auch mehrere Alarme im SIEM zu erkennen, die von den Studierenden gefunden und analysiert werden sollten, um so weitere Rückschlüsse auf das Vorgehen des Angreifers ziehen zu können (LZ 8). Darüber hinaus sollten die Studierenden ihre erkannten Artefakte aus der Analyse dokumentieren (LZ 11) und aufgrund der vorliegenden Fakten Entscheidungsgrundlagen für die Geschäftsführung des Kunden vorbereiten, Informationen für diese mangementtauglich aufbereiten und Empfehlungen formulieren (LZ 10). Dabei soll auch sichtbar sein, dass die getroffenen Entscheidungen sturkturiert und nicht „aus dem Bauch heraus“ getroffen werden, beispielsweise indem die verschiedenen Handlungsmöglichkeiten und deren Folgen dargelegt werden können (LZ 10).

Weiters sollte über den vom Ransomware Affiliate bereitgestellten Weg Kontakt mit diesem aufgenommen werden, um weitere Informationen über die erbeuteten Daten zu erhalten. Ein Informationsaustausch muss außerdem mit der Datenschutzbehörde aufgenommen werden, da persönliche Daten betroffen sind (LZ 4).

Anschließend sollte ein Eradication-Event im Rahmen eines Response Procedure geplant, mit dem Kunden besprochen und durchgeführt werden, um die Malware und die Persistenzen koordiniert von den Systemen zu entfernen (LZ 9). Da die Backups nicht durch die Ransomware betroffen sind, ist eine mögliche Recovery-Taktik, die Backups nach Prüfung auf Unversehrtheit auf die Systeme zurückzurollen. Dabei müssen die Studierenden aber darauf achten, möglicherweise notwendige Daten und Dokumente aus den neueren, bereits kompromittierten Backups zu sichten und gegebenenfalls ebenfalls zurückzurollen.

Während allen Phasen des Security Incidents ist es notwendig, der Geschäftsführung Lageinformationen,

insbesondere in grafischer Form, zukommen zu lassen und Sachverhalte einfach zu erklären (LZ 11).

Im Rahmen der anschließenden Learn Lessons-Phase sollen auch aktiv Verbesserungsvorschläge gebracht werden, wie dieser Sicherheitsvorfall verhindert hätte werden können. Unter anderem sind im Beispielszenario folgende Fehlkonfigurationen zu erkennen:

- Es gibt keine Firewallregeln zwischen den Netzwerksegmenten, wodurch diese beinahe keinen Nutzen mehr hat. Dies wurde durch den Angreifer für Lateral Movement genutzt.
- Das SIEM-System Wazuh ist nur mit Standardeinstellungen deployt. Es ist keine Konfigurationsanpassung erfolgt.
- Der VPN-Zugriff ist nicht sicher konfiguriert, beispielsweise ist über VPN ein Zugriff auf kritische Systeme im Netzwerk möglich.
- Die Shares sind nicht mit den korrekten NTFS-Rechten abgesichert, es ist lediglich über Gruppenrichtlinien der korrekten Benutzergruppe zugewiesen. Dennoch kann, bei Kenntnis des UNC-Pfades, jeder Domänenbenutzer auf die Dateien zugreifen.
- Es fehlt an organisatorischen Vorbereitungen für das Incident Handling.
- Die Cyberversicherung hat eigene Incident Handling-Vertragspartner, die eine zu lange Reaktionszeit angegeben hat.

Zu diesen sind von den Studierenden Maßnahmen zu formulieren.

Abschließend müssen die Studierenden noch einen Incident Report ausarbeiten. Dieser ist, nicht zuletzt aufgrund des Injects der Versicherung, sowohl für technisches, als auch für nichttechnisches Publikum zu gestalten. Für das technische Publikum ist insbesondere eine Darstellung beispielsweise in Form einer Cyber Kill Chain anzufertigen (LZ 11).

Über den gesamten Security Incident hinweg sollte jeweils ein:e Studierende:r im Wechsel als Incident Koordinator auftreten und somit die Aufgaben an das Incident Handling Team sowie die Kundenkommunikation koordinieren (LZ 13).

An die Arbeit angehängt finden sich Flow-Diagramme mit möglichen Ablaufdiagrammen, erwarteten Aktionen und Reaktionen. Ein Auszug davon ist in Abbildung 5.6 dargestellt.

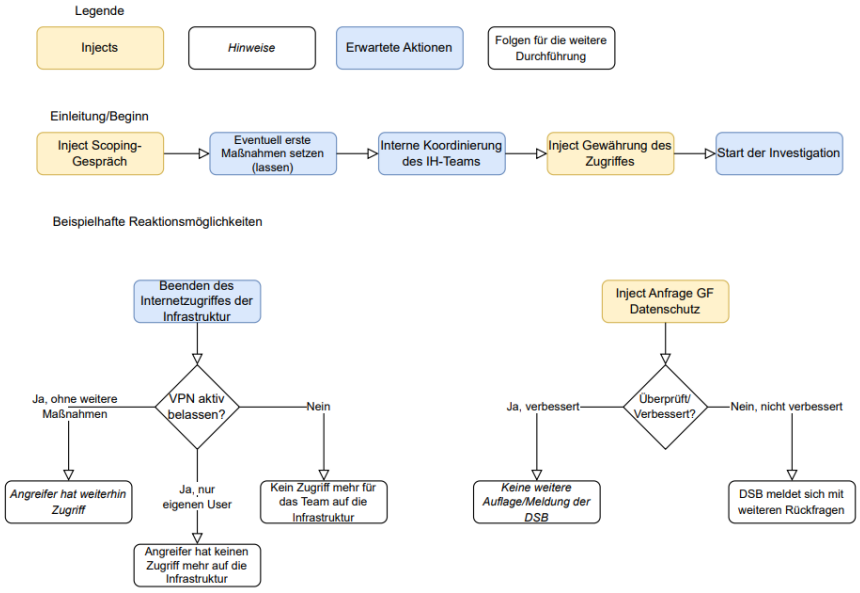

Abbildung 5.6.: Auszug aus den Flowdiagrammen für das Beispielszenario

5.3.3. Praktische Umsetzung: Configuration

Bereits im Security Project konnte gezeigt werden, dass, neben kostenpflichtigen Cloud-Angeboten verschiedener Anbieter, aktuell nur Openstack zur Virtualisierung derart großer Umgebungen im Stande ist und die notwendige Flexibilität, insbesondere auch für das Betreiben mehrerer Umgebungen für parallel arbeitende Gruppen bieten kann [20]. Zusätzlich ist auch die Freiheit von Lizenzkosten der gesamten Software sowie die Verwaltung über eine einzige zentrale Management Plane ein bedeutender Vorteil von OpenStack (siehe 2.1.3 Cyberrange).

Zur Realisierung der Infrastruktur mittels Infrastructure as Code (IaC) fiel die Wahl aus mehreren Gründen auf Terraform. Neben einer großen und starken Community, die auch die Weiterentwicklung der Software und der Provider vorantreibt, ist insbesondere auch die Multicloudfähigkeit von besonderer Bedeutung. Diese ermöglicht, Infrastruktur auf verschiedensten Cloud-Plattformen zu automatisieren. [65] Ein möglicher späterer Wechsel auf Technologien oder sogar Public Cloud-Anbieter fällt somit wesentlich leichter.

Konfiguration der virtuellen Maschinen mit Terraform

Die Erstellung der virtuellen Maschinen sowie der virtuellen Netzwerke wurde mittels Terraform v1.11.4 durchgeführt. Openstack ist mit der Nutzung des entsprechenden Providers voll unterstützt. Somit können beinahe alle Einstellungen, die manuell im Webinterface eingegeben werden können, auch über Infrastructure as Code provisioniert werden.

Für die Durchführung wurde, wie in vielen Unternehmensumgebungen üblich, der Fokus auf die Windows-Betriebssystemfamilie (Windows 10, 11 und Windows Server 2022) gelegt.

Für das Windows Server Betriebssystem wurde nach einem Download der ISO-Datei von der Herstellerwebseite zusätzlich noch das Windows Assessment and Deployment Toolkit (ADK) genutzt, um mittels Antwortdateien eine automatische Installation und Konfiguration ohne Eingreifen des Benutzers zu ermöglichen. Zusätzlich wurde darin sowohl das lokale Administrator-Passwort, als auch ein neuer Benutzer namens *Ansible* mit einem Standardpasswort angelegt, um darüber alle notwendigen Konfigurationen für angepasste Szenarien im Nachgang durchführen zu können. Die autounattend.xml-Datei wurden anschließend in das Stammverzeichnis der ISO-Datei integriert und lokal in VMWare Workstation Pro (17.6.3) geladen. Mit dem auf der Herstellerwebseite angebotenen Script[6] wurde anschließend die notwendigen Konfigurationen für WinRM und die Firewallregeln gesetzt sowie die benötigten VirtIO-Treiber für OpenStack installiert[7]. Zuletzt wurde noch mit der zuvor erstellten Antwortdatei als Argument das System mit dem Windows-Tool zur Systemvorbereitung (Sysprep) generalisiert. Anschließend wurde die von VMWare Workstation erstellte .vmdk-Disk mit dem Linux-Systemzeilentool qemu-image in das QCOW2-Format, ein für OpenStack verwendbares Festplattenformat, umgewandelt und auf OpenStack hochgeladen.

Dieser Vorgang wurde für das Windows 10 und das Windows 11 Image entsprechend wiederholt, wobei hierfür eine angepasste Antwortdatei mit dem Windows ADK zu erstellen war.

Auch der Upload der Images zu OpenStack erfolgt mittels *openstack_images_image_v2*-Ressource. Das garantiert, dass auch bei einem allfälligen Wechsel der OpenStack-Instanz die Images einfach erneut gepusht werden können, wodurch das Deployment deutlich beschleunigt wird.

Es wurden alle im Kapitel 5.3.2 Netzwerkdesign - Cyberspace angegebenen Maschinen inklusive der notwendigen Netzwerkverbindungen über Terraform erstellt. Zu Demonstrationszwecken wurde jeweils ein Client jeweils im Frontline- und im Backofficebereich ausgerollt.

Die dafür notwendigen Konfigurationsdateien wurden der Arbeit angehängt.

Systemkonfiguration der virtuellen Maschinen mit Ansible

Zur weiterführenden Konfiguration der virtuellen Maschinen fiel die Wahl, wie im Security Project [20], ebenfalls auf Ansible. Dadurch ist es möglich, die Konfigurationen in verschiedenen Rollen zu strukturieren und diese anschließend in sogenannten Playbooks den Maschinen zuzuweisen. Neben einer einfachen Vorbereitung der zu konfigurierenden virtuellen Maschinen mittels eines Scripts von der Herstellerwebseite

[6] Siehe https://docs.ansible.com/ansible/latest/os_guide/windows_winrm.html#winrm-setup.

[7] Siehe https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/archive-virtio/?C=M;O=D.

ist kein weiteres Deployment von Agents notwendig. Auch bei einer kurzfristigen Änderung an der Infrastruktur kann rasch mit einer einfachen Anpassung des Inventoryfiles oder eines Playbooks eine identische Konfiguration auch auf andere Maschinen übertragen werden.
Die weitere, genauere Konfiguration der einzelnen virtuellen Computer über Ansible ist nicht mehr im Scope dieser Arbeit. Die für das Beispielszenario vorzunehmenden Konfigurationen finden sich unter 5.3.2 Beispielszenario.

5.3.4. Praktische Umsetzung: Deployment

Im Bereich des Deployments wurde das Ausrollen der virtuellen Maschinen mittels Standardimage ohne zusätzliche szenariospezifische Konfiguration vorgenommen.
Dazu wurden zuerst die lokal vorbereiteten QCOW2-Images auf den OpenStack-Server gepusht, sodass diese dort zur Erstellung von virtuellen Maschinen bereitliegen (siehe Abbildung 5.7).

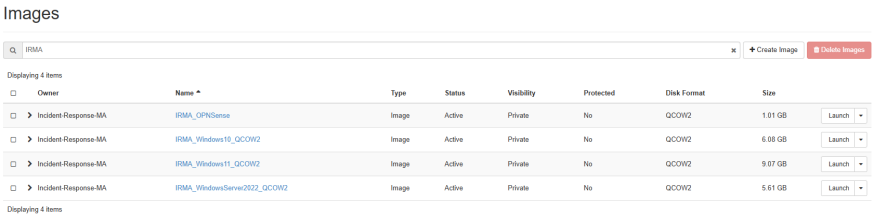

Abbildung 5.7.: Liste der hochgeladenen Images auf OpenStack

Anschließend können alle vorbereiteten Netzwerke (siehe Abbildung 5.8) und Maschinen über Terraform deployt werden.

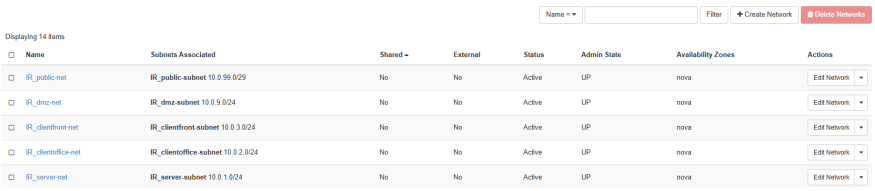

Abbildung 5.8.: Netzwerke in OpenStack

In Abbildung 5.9 ist zu erkennen, dass die Clients wie beabsichtigt über DHCP IP-Adressen erhalten und eine Floating IP-Adresse aus dem FH-Netz dem OPNSense-Router zugewiesen wurde, die nun sowohl zur Vorbereitung der Cyberrange als auch durch die Studierenden zum Fernzugriff auf die Infrastruktur genutzt werden kann.

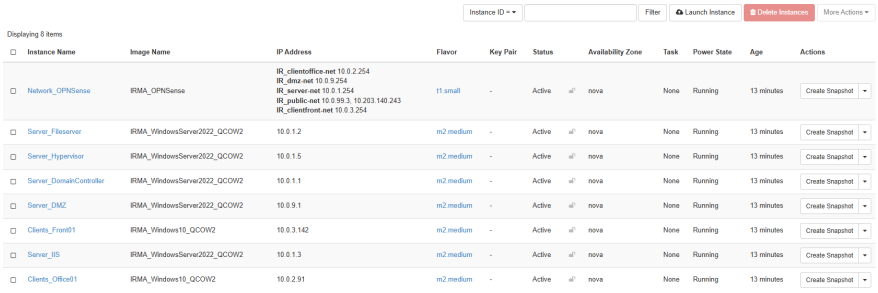

Abbildung 5.9.: Instanzen in OpenStack

Abschließend wird zu Testzwecken noch auf einen Windows Server und einen Windows 10-Client über die OpenStack Console zugegriffen. Beide Systeme sind darüber erreichbar und ohne Fehler gestartet:

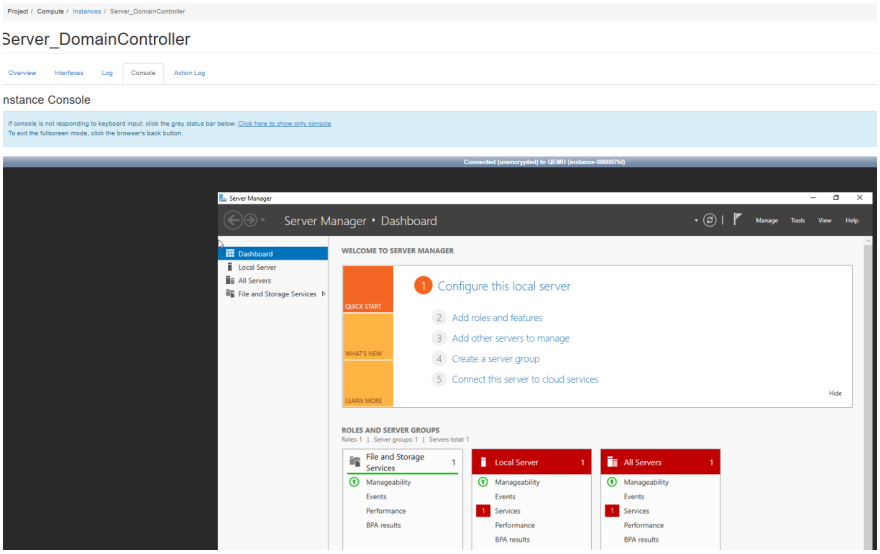

Abbildung 5.10.: Test der Verbindung zu einem Windows Server

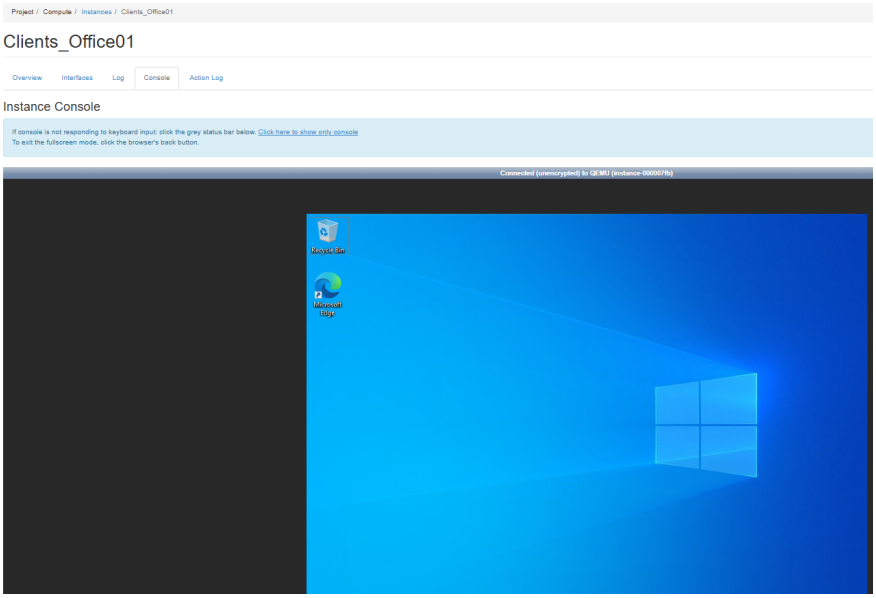

Abbildung 5.11.: Test der Verbindung zu einem Windows Client

Nun ist die Infrastruktur vorbereitet, um die Detailkonfigurationen der einzelnen Systeme über Ansible zu erhalten. Anschließend kann der simulierte Angriff durchgeführt werden.

6. Diskussion

Im Folgenden sollen der Erstellungsprozess sowie die auf die Forschungsfragen erhaltenen Antworten diskutiert werden.

Für den Prozess des Verfassens ist dabei zu bedenken, dass der geplante zeitliche Rahmen aufgrund des Umfanges des Themas deutlich gesprengt worden ist; es haben sich immer weitere Themenfelder ergeben, die nicht unbearbeitet gelassen werden konnten. Eine weitere, noch tiefer gehende Ausarbeitung der Themen sowie die praktische Konfiguration und ein wissenschaftlich begleiteter Dry Run der Cyberrange mit Expert:innen im Bereich Incident Handling würde sicherlich noch weitere Verbesserungsmöglichkeiten im Design und in der Umsetzung der Cyberrange aufzeigen. Weiters wäre auch eine weitere wissenschaftliche Begleitung der Lehrveranstaltung wünschenswert, um die Machbarkeit und den Erfüllungsgrad der Lehrziele zu erheben. Zusätzliche zeitliche und personelle Ressourcen in diesem Bereich wären daher wertvoll. Die daraus resultierenden Einschränkungen sind auch in den Limitationen (siehe 6.2 Limitationen) aufgezeigt.

Gleichzeitig hat sich durch die ausufernde inhaltliche Auseinandersetzung nach Rücksprache mit dem Betreuer auch eine Kürzung des praktischen Anteils der Arbeit ergeben. Ursprünglich wäre erhofft worden, die Cyberrange bereits noch detailreicher umzusetzen. Mit dem vorhandenen Zeitkontingent war dies jedoch nicht realisierbar.

Eine weitere Schwierigkeit in der Ausarbeitung zeigte sich in der Inkonsistenz verschiedener Quellen, insbesondere in den Definitionen (siehe 2.1.2 Begriffsabgrenzung Incident Handling - Incident Response - Security Incident Management). Warum es selbst bei der Definition von *Incident Response* derartige Auslegungsunterschiede gibt, konnte im Rahmen dieser Arbeit nicht abschließend geklärt werden. Bei allen Unterschieden konnte aber auch festgestellt werden, dass die Grundaussagen der untersuchten Incident Handling-Modelle beinahe identisch sind, unabhängig davon, in wie viele Phasen mit verschiedenen Namen diese durch die herausgebenden Organisationen geteilt wurden.

Diesen Herausforderungen steht jedoch insbesondere die umfassende Abbildung der Anforderungen an Incident Handler gegenüber, auf Basis derer eine wissenschaftlich fundierte Lehrveranstaltungskonzeption erfolgen und die Cyberrange als Abschlussübung implementiert werden kann, sodass die Arbeit einen ent-

scheidenden Beitrag zum Verständnis des Berufsbild der Incident Handler leisten kann. Dabei ist insbesondere die gelungene Verknüpfung zwischen Theorie und Praxisnähe als besonders fundamental herauszustreichen.

6.1. Beantwortung der Forschungsfragen

In der Arbeit galt es herauszufinden, welches Wissen und welche Skills Incident Handler in der österreichischen Wirtschaft benötigen und in welchen Bereichen diese durch die Unternehmen eingesetzt werden. Weiterführend sollte erhoben werden, welches theoretische Wissen für die Fachkräfte unabdingbar ist und deshalb in einer Lehrveranstaltung zu diesem Thema behandelt werden muss. Zuletzt sollte eine Cyberrange konzipiert werden, die zur Festigung des erworbenen Wissens im Rahmen einer Abschlussübung in einer Lehrveranstaltung an der Fachhochschule St. Pölten eingesetzt werden kann.

Zur Beantwortung der ersten Forschungsfrage wurde im Rahmen einer Literaturrecherche nach bereits verschriftlichen Anforderungen an Incident Handler gesucht. Die Recherche ergab lediglich die Work Role Incident Handling im NIST NICE Framework, die sämtliche Anforderungen in Form von Task-, Knowledge- und Skill-Statements beschreibt. Diese Struktur wurde für die Beschreibung der Anforderungen übernommen, wobei die bereits vorhandenen Kriterien um die in den vier Experteninterviews zutage geförderten Anforderungen der österreichischen Wirtschaft ergänzt und spezifiziert wurden. Zur Systematisierung wurden die Anforderungen aus ISO 27035, NIST SP 800-61 und CIS Controls erhoben und auf das Prozessmodell der ISO 27035 gemappt.

In der Erhebung des notwendigen Wissens, der Aufgaben und der Skills im organisatorischen Bereich für einen Incident Handler, der in der österreichischen Wirtschaft tätig sein möchte, konnten mit der Formulierung von 72 Task-, 77 Knowledge- und 67 Skill-Statements die umfangreichen Anforderungen an Incident Handler in der österreichischen Wirtschaft sichtbar gemacht werden. Das notwendige Wissen reicht dabei von grundlegenden Kenntnissen über das Wesen von strukturiertem Security Incident Management, Prozessen, Aufgaben und Aufbauorganisationen im Incident- und Krisenfall, Risikomanagement, Kommunikation bis hin zu Wissen im Bereich Threat Intelligence, Backup und Recovery und IT-Betrieb. Die durch die Standards und die Wirtschaft genannten praktischen Skills decken sich dabei zu einem Großteil mit dem Wissen, was den Rückschluss zulässt, dass nicht nur ein theoretisches, sondern auch praktisches Know-How im Bereich Incident Handling unabdingbar ist. Bei der Erhebung der Tasks und Aufgabengebiete eines Incident Handlers wurde festgestellt, dass Incident Handler üblicherweise als Allrounder tätig sind und sowohl technische als auch organisatorische Tasks übernehmen. Eine Spezialisierung in die organisatorische Richtung

ist bei allen befragten Organisationen, wenn überhaupt, erst nach umfangreicher Berufserfahrung möglich. Somit ist es nicht realistisch, direkt nach der positiven Absolvierung der Incident Handling Lehrveranstaltung in diesem Bereich beruflich eigenmächtig tätig zu werden. Trotzdem ist bei einer von vier befragten Organisationen ist ein derzeit laufendes oder abgeschlossenes Hochschulstudium im Bereich Informatik oder IT-Security notwendig, da eben dieses die notwendigen Vorkenntnisse vermittle.

Von den zuvor erwähnten TKS-Statements ausgehend wurden zentrale Anforderungen aus allen Bereichen des Incident Handlings herausgegriffen, verwandte Themen zusammengeführt und somit 13 Lernziele, die die Studierenden am Ende der Lehrveranstaltung beherrschen sollen, erstellt. Lernziele, die bereits in anderen Lehrveranstaltungen behandelt werden, wurden jedoch nicht in die Lernziele für diese Veranstaltung aufgenommen. Entsprechende TKS-Statements wurden aber in Kapitel 5.1.4 belassen. In Vereinheitlichung mit den Lernzielen anderer Lehrveranstaltungen an der Fachhochschule St. Pölten wurden diese in der Bloom'schen Lernzieltaxonomie ausgearbeitet und jeweils einer Lernzielebene zugewiesen. Dabei wurde besondere Acht darauf gelegt, aus jedem Bereich, von Standards und Prozessen über Kommunikation bis hin zu Triage von Systemen und Response, die wichtigsten Fähigkeiten abzudecken. Zusätzlich ist auch aufgrund der Vielzahl an Abhängigkeiten der Lehrveranstaltung *Incident Response* von *Threat Modeling und Intelligence* ein Tausch der beiden Lehrveranstaltungen anzustreben, um das Vorwissen bestmöglich auch im Bereich Incident Handling einsetzen zu können. Mit diesen Erkenntnissen konnte die zweite Forschungsfrage beantwortet werden.

Aus diesen Lernzielen wurde anschließend eine Cyberrange als Abschlussübung zur Festigung des erworbenen Wissens erstellt und so die letzte Forschungsfrage bearbeitet. Die Vorbereitung auf die Durchführung der Cyberrange, beispielsweise das Schreiben von Playbooks, erfolgt dabei teilweise in der Input-Phase der Lehrveranstaltung selbst, zum Teil ist diese jedoch von den Studierenden selbstständig durchzuführen. Für die Durchführung der Cyberrange sind drei Lehrveranstaltungstage veranschlagt. Die Konzeption wurde nach dem Lifecycle von Katsantonis et al. in den Phasen Analyse, Design, Configuration, Deployment, Dry Run und Execution durchgeführt, wobei die Arbeit sich insbesondere auf die ersten beiden Teile des Lifecycles konzentriert. Die Analyse-Phase beinhaltet dabei neben weiteren Inputs zur Durchführung derartiger Übungen aus den Interviews die Erkenntnisse aus den formulierten Lernzielen und TKS-Statements sowie der didaktischen Rekonstruktion. Im Bereich des Szenariendesigns fiel die Wahl auf die Durchführung als externer Incident Handling-Dienstleister, um das Fehlen von Informationen über die Prozesse und die Wertschöpfungsketten der betroffenen Organisation darzustellen. Wenngleich in dieser Arbeit ein Beispielszenario ausgearbeitet wird, ist das genaue Szenario bewusst nicht für die Lehrveranstaltung vorgeschrieben. Das ermöglicht dem Lehrbeauftragten nicht nur eine einfache Anpassung an derzeit realistische Bedrohungssze-

narien, sondern lässt diesen auch das Niveau der Übung an die Gruppe anpassen. Von besonderer Bedeutung ist auch, dass die Simulation des Angriffes nicht statisch, beispielsweise mittels Playbooks, implementiert werden soll, da dies die Angriffe nicht nur unflexibel, sondern vor allem auch unrealistisch macht. Im Bereich des Netzwerkdesigns wurde ein fiktiver Autohändler namens BigCarCompany genutzt, der von seiner IT-Umgebung für seine Kernprozesse abhängig ist. Neben mehreren Clientnetzen wurde auch ein Servernetz und eine DMZ konstruiert und in Terraform auf OpenStack realisiert. Dies ermöglicht die Simulation einer Vielzahl von Angriffsszenarien. Zusätzlich wurden auch Beispielinjects, unter anderem für das Scoping-Gespräch, Anfragen der Mitarbeiter:innen und Datenschutzfragen konstruiert, die von der Übungsleitung flexibel eingespielt werden können. Für das Beispielszenario wurde auch eine mögliche Musterlösung und einfache, rudimentäre Flow-Diagramme, wie sich bestimmte Entscheidungen auf die weitere Durchführung der Übung auswirken, erstellt.

6.2. Limitationen

Die im Folgenden beschriebenen Limitationen ergeben sich, wie bereits angesprochen, aus dem eingeschränkten Umfang und dem Scope der Arbeit.

In der Erhebung der Anforderungen wurden dabei lediglich Experten größerer österreichischer Unternehmen befragt. Somit ist nicht erhoben worden, ob eine Umlegbarkeit der ermittelten Anforderungen an Incident Handler auf kleinere Unternehmen oder Organisationen aus dem europäischen oder gar internationalen Ausland gegeben ist. Die Betrachtung ausländischer Organisationen war jedoch nicht im Scope der Arbeit.

Weiters wurde, wie in 5.2 Didaktische Überlegungen beschreiben, das Vorwissen einer Person mit Bachelorabschluss an der Fachhochschule St. Pölten als Basis für die Konzepterstellung herangezogen, da auch die konzipierte Lehrveranstaltung an der Fachhochschule St. Pölten stattfinden soll. Aufgrund des vorausgesetzten Hintergrundwissens ist somit ein Einsatz an Hochschulen mit anderen Voraussetzungen nicht ohne Weiteres möglich.

Darüber hinaus ist der Masterstudiengang Cybersecurity and Resilience nicht Zielgruppe dieser Lehrveranstaltung. Zum einen ist im Curriculum derzeit nur eine Lehrveranstaltung mit 4 ECTS für den Bereich Digital Forensics und Incident Handling vorgesehen, zum anderen sind die Zugangsvoraussetzungen im Gegensatz zum Masterstudium Information Security aufgrund der fehlenden 12 ECTS im Bereich IT-Security niedriger gesteckt. [66] Aufgrund dessen wird für diesen Studiengang anderes Vorwissen vorausgesetzt, was sich wiederum direkt auf die Ziele der Lehrveranstaltung auswirkt.

Im Bereich der Entwicklung der Cyberrange ist für eine praktische Umsetzung noch die Detailkonfiguration

der Maschinen mit Ansible ausständig. Erst nach der Konfiguration und der Simulation eines Angriffes, beispielsweise aus dem Beispielszenario, kann die Cyberrange praktisch im Rahmen der Lehrveranstaltung durchgeführt werden. Die im Lifecycle von Katsantonis et al. noch vorgesehenen Phasen Dry Run, also einem Test mit Expert:innen und Execution, also der tatsächlichen Durchführung in der Lehrveranstaltung, wurden im Rahmen dieser Arbeit nicht durchgeführt (siehe 4.4.5 Dry Run und Execution).

6.3. Weiterführende Arbeiten

Aus diesen Limitationen lassen sich jedoch auch an diese Arbeit anschließende, zu bearbeitende Themen identifizieren.

Da diese Arbeit die erste ihrer Art ist, die versucht, die Anforderungen an Incident Handler wissenschaftlich fundiert und strukturiert zu erheben, hat sie sicherlich den Grundstein für viele weitere Forschungsarbeiten im Bereich der Anforderungserhebungen und der auf deren Basis aufgebauten Lehrveranstaltungen gelegt.

Für die Durchführung der Lehrveranstaltung müssen in einem nächsten Schritt noch auf Basis der Anforderungen in Form der TKS-Statements und der Lehrziele Medien wie Präsentationen, Unterlagen, Zwischenübungen und Ähnliches gestaltet werden.

Aufgrund der noch ausständigen vollständigen Konfiguration der Cyberrange ist in einem nächsten Schritt nach den Beschreibungen in der Arbeit das Beispielszenario technisch zu implementieren. Anschließend ist es noch ratsam, einen Dry Run vor der tatsächlichen Verwendung der Umgebung im Rahmen einer Lehrveranstaltung durchzuführen.

7. Conclusio

Abschließend lässt sich festhalten, dass Incident Handling aufgrund der umfassenden Aufgaben des Personals, für die nicht nur ebenso umfangreiches Wissen und Fähigkeiten notwendig sind, sondern die auch in druck- und stressreichen Arbeitsumfeldern bewältigt werden müssen, wahrlich als Königsklasse in der IT Security gelten kann.

Incident Handler müssen dabei beispielsweise IT Security Incidents klassifizieren und priorisieren, die betroffene Organisation verstehen und Reaktionsmaßnahmen auf verschiedene Sicherheitsvorfälle planen und durchführen können. Darüber hinaus müssen sie ein breites Wissen, unter anderem in den Bereichen strukturiertes Incident Management und Prozesse, Vulnerability Management, Risikomanagement sowie Backup und Data Recovery mitbringen. Zudem müssen sie Lernbereitschaft, Resilienz und Kommunikationsbereitschaft in den Beruf einbringen.

Auch wenn es nicht realistisch scheint, Berufseinsteiger:innen selbst nach Absolvierung einer Lehrveranstaltung mit Schwerpunkt Incident Handling selbstständig IT Sicherheitsvorfälle bearbeiten zu lassen und sie in der Praxis zu Beginn viele Erfahrungen durch erfahrene Incident Handler angeleitet sammeln müssen, konnte dennoch die Wichtigkeit des Erwerbs von Grundlagen im Rahmen eines Fachhochschulstudiums aufgezeigt werden. Dazu zählen unter anderem das Verstehen der Prozessmodelle verschiedener Standards, das Kennen und Etablieren möglicher Aufbauorganisationen und die Triage und Analyse von Systemen. Diese wurden in den Lernzielen verschriftlicht.

Bei der Formulierung dieser Lernziele wurde neben der Relevanz für die Praxis und der inhaltlichen Passung zu den Inhalten der Lehrveranstaltung darauf geachtet, unterschiedliche Anforderungsniveaus zu konzipieren, um Abstufungen im Grad der Erreichung messbar machen zu können. Dies ist insbesondere vor dem Kontext der Beurteilung im Rahmen der Lehrveranstaltung relevant. Dabei wurden die Lernzielebenen der Bloom'schen Taxonomie, die am Department standardmäßig verwendet wird, zur Systematisierung der Schwierigkeitsstufen herangezogen.

Auf Basis dieser mit der Lehrveranstaltung zu erreichenden Ziele wurde eine Cyberrange konzipiert. Diese dient einerseits als Mittel zur Festigung und Anwendung des erworbenen Wissens und kann andererseits

Aufschluss über die Erreichung der Lernziele geben. Darüber hinaus bietet sie einen motivierenden, spielbasierten und vor allem praxisorientierten Ansatz der Auseinandersetzung mit wichtigen Lerninhalten und bringt deswegen einen besonderen Mehrwert in die Lehrveranstaltung ein.
Die Studierenden werden hierbei als Incident Handler in ein realitätsnahes Szenario entlassen, in dem sie als externe Dienstleister ein Unternehmen, das einen Security Incident bemerkt hat, bei der Aufarbeitung desselben unterstützen müssen. In diesem Beispielszenario wurde ein Ransomwarevorfall in einem Autohaus simuliert, das sich bisher noch nicht mit dem Thema Security Incident Managment befasst hat, daher auch kein kompetentes IT-Personal vorhält und völlig unvorbereitet ist. Bei der Bearbeitung des Security Incidents liegt der Fokus auf den organisatorischen Tätigkeiten. Die Studierenden sollen dabei unter anderem ein Scoping-Gespräch durchführen, managementtaugliche Reports und Lagebilder liefern und Anfragen von Behörden kompetent beantworten.
Diese Vorgangsweise soll wiederum gewährleisten, dass die von der österreichischen Wirtschaft gestellten Anforderungen an Berufseinsteiger:innen von den Absolvent:innen des Masterstudienganges Information Security an der Fachhochschule St. Pölten bestmöglich erfüllt werden können. Somit sind die Studierenden nach dem Besuch der Lehrveranstaltung mit dem Schwerpunkt Incident Handling darauf vorbereitet, erfahrene Incident Handler in der Praxis zu unterstützen und Teilaufgaben wie Dokumentationstasks oder Mithilfe in der Lagebilderstellung selbst zu übernehmen.

Abbildungsverzeichnis

Literatur

[1] Mandiant, „M-Trends 2025: Data, Insights, and Recommendations From the Frontlines“, Google Cloud, Techn. Ber., Apr. 2025. besucht am 23. Mai 2025. Adresse: https://services.google.com/fh/files/misc/m-trends-2025-en.pdf.

[2] Cheng, Joseph. „The Human Consequences of Ransomware Attacks“, besucht am 23. Mai 2025. Adresse: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/the-human-consequences-of-ransomware-attacks.

[3] World Economic Forum, „Strategic Cybersecurity Talent Framework“, Techn. Ber., Apr. 2024. besucht am 23. Mai 2025. Adresse: https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.

[4] National Institute of Standards and Technology. „Incident Response“, besucht am 18. Apr. 2025. Adresse: https://niccs.cisa.gov/workforce-development/nice-framework/work-role/incident-response.

[5] *Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2018)*, Mai 2020.

[6] Alex Nelson, Sanjay Rekhi, Murugiah Souppaya und Karen Scarfone, „Incident response recommendations and considerations for cybersecurity risk management: A csf 2.0 community profile“, National Institute of Standards und Technology, Special Publication 800-61 Revision 3, Apr. 2025. DOI: 10.6028/NIST.SP.800-61r3. Adresse: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

[7] Laiba Siddiqui. „Incident-Management: Ein umfassender Leitfaden“, besucht am 15. März 2025. Adresse: https://www.splunk.com/de_de/blog/learn/incident-management.html.

[8] AXELOS, *ITIL Foundation, ITIL 4 Edition*, 2022. besucht am 15. März 2025. Adresse: https://www.mizekhedmat.com/wp-content/uploads/2022/07/ITILFoundation-ITIL4Edition.pdf.

[9] *ISO/IEC 27035-1:2023: Information technology – Information security incident management – Part 1: Principles and process*, Feb. 2023.

[10] PricewaterhouseCoopers Austria GmbH. „Cyber Incident Response Retainer“, besucht am 15. März 2025. Adresse: https://www.pwc.at/de/dienstleistungen/wirtschaftspruefung/cybersecurity/cyber-incident-response-retainer.html.

[11] IKARUS Security Software GmbH. „IKARUS 24/7 Incident Response“, besucht am 15. März 2025. Adresse: https://www.ikarussecurity.com/managed-it-ot-security-solutions/ikarus-24-7-incident-response/.

[12] Sophos Ltd. „Incident Response Services“, besucht am 15. März 2025. Adresse: https://www.sophos.com/de-de/products/managed-detection-and-response/incident-response-services.

[13] National Institute of Standards and Technology. „Incident Response“, besucht am 15. März 2025. Adresse: https://csrc.nist.gov/glossary/term/incident_response.

[14] National Institute of Standards and Technology. „Incident Handling“, besucht am 15. März 2025. Adresse: https://csrc.nist.gov/glossary/term/incident_handling.

[15] National Institute of Standards and Technology. „Cyber Range“, besucht am 22. März 2025. Adresse: https://csrc.nist.gov/glossary/term/cyber_range.

[16] AXIS Flight Simulation. „The Evolution of Flight Simulation“, besucht am 22. März 2025. Adresse: https://www.axis-simulation.com/2024/01/30/the-evolution-of-flight-simulation/.

[17] National Institute of Standards and Technology, *The Cyber Range: A Guide*, Sep. 2023. besucht am 22. März 2025. Adresse: https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf.

[18] M. N. Katsantonis, A. Manikas, I. Mavridis und D. Gritzalis, „Cyber range design framework for cyber security education and training“, *International Journal of Information Security*, Jg. 22, Nr. 4, S. 1005–1027, 2023. DOI: 10.1007/s10207-023-00680-4. Adresse: https://link.springer.com/article/10.1007/s10207-023-00680-4.

[19] Muhammad Yamin und Basel Katt, „Modeling and executing cyber security exercise scenarios in cyber ranges“, *Computers & Security*, Jg. 116, S. 102 635, 2022. DOI: 10.1016/j.cose.2022.102635. Adresse: https://www.sciencedirect.com/science/article/pii/S0167404822000347.

[20] Benjamin Baureder, Christoph Dorner, Christoph Einsiedl, Samuel-Markus Haim, Lukas Mozgovicz, Niels Pfau und Manuel Werka, *Security Project I: Cyber Range*, Fachhochschule St. Pölten, 2024.

[21] Rodney Petersen, Danielle Santos, Matthew C. Smith, Karen A. Wetzel und Greg Witte, „Workforce Framework for Cybersecurity (NICE Framework)“, National Institute of Standards und Technology, Special Publication 800-181 Revision 1, Nov. 2020. DOI: 10.6028/NIST.SP.800-181r1. Adresse: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

[22] *Task Knowledge Skill (TKS) Statements Authoring Guide for Workforce Frameworks*, Apr. 2021. Adresse: https://www.nist.gov/system/files/documents/2021/07/30/TKS_Authoring_Guide13apr2021-508Compliant.pdf.

[23] International Organization for Standardization. „Standards“, besucht am 11. Apr. 2025. Adresse: https://www.iso.org/standards.html.

[24] International Organization for Standardization. „Who Develops Standards?“, besucht am 11. Apr. 2025. Adresse: https://www.iso.org/who-develops-standards.html.

[25] International Organization for Standardization. „Developing Standards“, besucht am 11. Apr. 2025. Adresse: https://www.iso.org/developing-standards.html.

[26] Georg Disterer, „Iso/iec 27000, 27001 and 27002 for information security management“, *Journal of Information Security*, Jg. 4, Nr. 2, S. 92–100, Apr. 2013. DOI: 10.4236/jis.2013.42011. besucht am 4. Apr. 2025. Adresse: https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf.

[27] Europäisches Parlament und Rat der Europäischen Union, *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)*, 14. Dez. 2022. besucht am 4. Apr. 2025. Adresse: https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=de.

[28] International Organization for Standardization. „ISO/IEC 27000 family“, besucht am 11. Apr. 2025. Adresse: https://www.iso.org/standard/iso-iec-27000-family.

[29] *ISO/IEC 27035-2:2023: Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*, Feb. 2023.

[30] *ISO/IEC 27035-3:2020: Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations*, Sep. 2020.

[31] *ISO/IEC 27035-4:2024: Information technology – Information security incident management –Part 4: Coordination*, Dez. 2024.

[32] Cherilyn Pascoe, Stephen Quinn und Karen Scarfone, „The nist cybersecurity framework (csf) 2.0“, National Institute of Standards und Technology, Cybersecurity White Paper CSWP 29, Feb. 2024. DOI: 10.6028/NIST.CSWP.29. Adresse: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[33] Microsoft. „Incident Response Services“, besucht am 15. Apr. 2025. Adresse: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility.

[34] *CIS Controls v8, Center for Internet Security Controls Version 8*, Mai 2021.

[35] U. Kattmann, R. Duit, H. Gropengießer und M. Komorek, „Das Modell der Didaktischen Rekonstruktion - Ein Rahmen für naturwissenschaftliche Forschung und Entwicklung“, *Zeitschrift für Didaktik der Naturwissenschaften*, Nr. 3, S. 3–18, 1997.

[36] Sibylle Reinfried, Christian Mathis und Ulrich Kattmann, „Das Modell der Didaktischen Rekonstruktion. Eine innovative Methode zur fachdidaktischen Erforschung und Entwicklung von Unterricht“, de, *BzL - Beiträge zur Lehrerinnen- und Lehrerbildung*, Jg. 27, Nr. 3, S. 404–414, Dez. 2009, ISSN: 2296-9632. DOI: 10.36950/bzl.27.3.2009.9826. besucht am 12. Apr. 2024. Adresse: https://bop.unibe.ch/BzL/article/view/9826.

[37] U. Kattmann, „Lernen mit anthropomorphen Vorstellungen? Ergebnisse von Untersuchungen zur Didaktischen Rekonstruktion in der Biologie“, *Zeitschrift für Didaktik der Naturwissenschaften*, Jg. 3, Nr. 3, S. 165–174, 2005, Number: 3.

[38] Reinders Duit, „Didaktische Rekonstruktion“, de, *Piko-Brief*, Jg. 3, 2010.

[39] Ulrich Kattmann, „Didaktische Rekonstruktion - eine praktische Theorie“, ger, in *Theorien in der biologiedidaktischen Forschung: Ein Handbuch für Lehramtsstudenten und Doktoranden*, Ser. Springer-Lehrbuch, Dirk Krüger und Helmut Vogt, Hrsg., Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, S. 93–104, ISBN: 978-3-540-68166-3. DOI: 10.1007/978-3-540-68166-3.

[40] Wolfgang Klafki, „Didaktische Analyse als Kern der Unterrichtsvorbereitung“, in *Auswahl, Didaktische Analyse*, H. Roth und A. Blumental, Hrsg., Hannover: Schroedel, 1969, S. 5–34.

[41] Claudia Nerdel, *Grundlagen der Naturwissenschaftsdidaktik: Kompetenzorientiert und aufgabenbasiert für Schule und Hochschule* (Lehrbuch), de, 1. Auflage. Berlin [Heidelberg]: Springer Spektrum, 2017, ISBN: 978-3-662-53158-7. DOI: 10.1007/978-3-662-53158-7.

[42] *LV Beschreibung Incident Response*, 2025.

[43] Nanina Marika Sturm, *Handreichung der Prüfungswerkstatt - Lernzielformulierung*, 2018. besucht am 16. Apr. 2025. Adresse: https://www.zq.uni-mainz.de/files/2018/08/4_Lernziele-formulieren.pdf.

[44] Victor Tiberius, *Hochschuldidaktik der Zukunftsforschung*. VS Verlag für Sozialwissenschaften, 2011, ISBN: 9783531928692. DOI: 10.1007/978-3-531-92869-2. Adresse: http://dx.doi.org/10.1007/978-3-531-92869-2.

[45] Stefanie Wagner, *Lehr- und Lernziele formulieren*, Handreichung, Hochschule Neubrandenburg, Okt. 2021. besucht am 22. März 2025. Adresse: https://www.hs-nb.de/storages/hs-neubrandenburg/Hochschule/Digitalisierung/DigitalLehrenUndLernen/LehrLernziele.pdf.

[46] Patrick Haag und Stefan Luppold, *Zielgruppenorientierte Veranstaltungskonzeption: Messen, Kongresse und Events auf Zielgruppen ausrichten*. Springer Fachmedien Wiesbaden, 2020, ISBN: 9783658318888. DOI: 10.1007/978-3-658-31888-8. Adresse: http://dx.doi.org/10.1007/978-3-658-31888-8.

[47] Österreichisches Zentrum für Begabtenförderung und Begabungsforschung, *Methodenskript*, 2017. besucht am 22. März 2025. Adresse: https://www.oezbf.at/wp-content/uploads/2017/03/Methodenskript_Neuauflage_WEB.pdf.

[48] Universität Innsbruck, *Taxonomie von Lernzielen im kognitiven Bereich*, 2015. besucht am 12. Apr. 2025. Adresse: https://www.uibk.ac.at/bologna/curriculums-entwicklung/dokumente/taxonomie.pdf.

[49] National Institute of Standards and Technology. „NICE Workforce Framework for Cybersecurity (NICE Framework)“, besucht am 15. Apr. 2025. Adresse: https://niccs.cisa.gov/workforce-development/nice-framework.

[50] Daniel Haslinger und Christoph Lang-Muhr, „Business Continuity & Desaster Recovery als Planspiel umgesetzt“, in *Tagungsband zum 5. Tag der Lehre an der FH St. Pölten am 20.10.2016*, Okt. 2016, S. 117–125. DOI: 10.13140/RG.2.2.28345.98403. Adresse: https://www.researchgate.net/publication/309293506_Business_Continuity_Desaster_Recovery_als_Planspiel_umgesetzt.

[51] Stefan Machherndl, „Business Continuity & Desaster Recovery - das Planspiel in Containern“, Master's thesis, University of Applied Sciences St. Pölten, St. Pölten, Okt. 2021.

[52] Dixon Prem Daniel Rajendran und Rangaraja P. Sundarraj, „Designing Game-based Learning Artefacts for Cybersecurity Processes Using Action Design Research: Nascent Design Theory Implications“, *Business & Information Systems Engineering*, Feb. 2024, ISSN: 1867-0202. DOI: 10.1007/s12599-024-00852-z. Adresse: http://dx.doi.org/10.1007/s12599-024-00852-z.

[53] Karo Saharinen, Jaakko Backlund und Jarmo Nevala, „Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework“, in *Proceedings of the 12th International Conference on Education Technology and Computers*, Ser. ICETC '20, London, United Kingdom: Association for Computing Machinery, 2021, S. 172–176, ISBN: 9781450388276. DOI: 10.1145/3436756.3437041. Adresse: https://doi.org/10.1145/3436756.3437041.

[54] Stylianos Karagiannis, Emmanouil Magkos, Eleftherios Karavaras, Antonios Karnavas, Maria Nefeli Nikiforos und Christoforos Ntantogian, „Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams“, *Journal of Network and Systems Management*, Jg. 32, Nr. 2, Apr. 2024, ISSN: 1573-7705. DOI: 10.1007/s10922-024-09816-w. Adresse: http://dx.doi.org/10.1007/s10922-024-09816-w.

[55] Cornelia Helfferich, „Leitfaden- und Experteninterviews“, in *Handbuch Methoden der empirischen Sozialforschung*, Nina Baur und Jörg Blasius, Hrsg. Wiesbaden: Springer Fachmedien Wiesbaden, 2019, S. 669–686, ISBN: 978-3-658-21308-4. DOI: 10.1007/978-3-658-21308-4_44. Adresse: https://doi.org/10.1007/978-3-658-21308-4_44.

[56] Heinz Reinders, „Interview“, in *Empirische Bildungsforschung: Strukturen und Methoden*, Heinz Reinders, Hartmut Ditton, Cornelia Gräsel und Burkhard Gniewosz, Hrsg. Wiesbaden: VS Verlag für Sozialwissenschaften, 2011, S. 85–97, ISBN: 978-3-531-93015-2. DOI: 10.1007/978-3-531-93015-2_7. Adresse: https://doi.org/10.1007/978-3-531-93015-2_7.

[57] Cornelia Helfferich, *Die Qualität qualitativer Daten*. VS Verlag für Sozialwissenschaften, 2011, ISBN: 9783531920764. DOI: 10.1007/978-3-531-92076-4. Adresse: http://dx.doi.org/10.1007/978-3-531-92076-4.

[58] Alexander Jedinger und Tobias Michael, „Interviewereffekte“, in *Handbuch Methoden der empirischen Sozialforschung*, Nina Baur und Jörg Blasius, Hrsg. Wiesbaden: Springer Fachmedien Wiesbaden, 2019, S. 365–376, ISBN: 978-3-658-21308-4. DOI: 10.1007/978-3-658-21308-4_44. Adresse: https://doi.org/10.1007/978-3-658-21308-4_44.

[59] Philipp Mayring, *Qualitative Inhaltsanalyse : Grundlagen und Techniken*, 13., überarbeitete Auflage. Weinheim/Basel: Beltz, 2022, ISBN: 9783407258991.

[60] Philipp Mayring, „Qualitative Inhaltsanalyse“, in *Texte verstehen: Konzepte, Methoden, Werkzeuge*, Andreas Boehm, Andreas Mengel und Thomas Muhr, Hrsg., Konstanz: UVK Universitätsverlag Konstanz, 1994, S. 159–175. Adresse: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-14565.

[61] Michaela Gläser-Zikuda, *Qualitative Auswertungsverfahren*, Heinz Reinders, Hartmut Ditton, Cornelia Gräsel und Burkhard Gniewosz, Hrsg. Wiesbaden: VS Verlag für Sozialwissenschaften, 2011, S. 109–120, ISBN: 978-3-531-93015-2. DOI: 10.1007/978-3-531-93015-2_7. Adresse: https://doi.org/10.1007/978-3-531-93015-2_7.

[62] Philipp Mayring, „Qualitative Inhaltsanalyse“, *Forum Qualitative Sozialforschung*, Jg. 1, Nr. 2, Art. 20, Juni 2000. Adresse: http://nbn-resolving.de/urn:nbn:de:0114-fqs0002204.

[63] Fachhochschule St. Pölten. „Information Security Studium“, besucht am 22. Apr. 2025. Adresse: https://www.fhstp.ac.at/de/studium/informatik-security/information-security.

[64] Fachhochschule St. Pölten. „Bewerbungsinfo Information Security“, besucht am 22. Apr. 2025. Adresse: https://www.fhstp.ac.at/de/studium/bewerbungsinfo#/stage-two/step/0.

[65] Hashicorp. „Terraform“, besucht am 22. Mai 2025. Adresse: `https://developer.hashicorp.com/terraform`.

[66] Fachhochschule St. Pölten. „Studieninhalte Cyber Security and Resilience“, besucht am 22. Apr. 2025. Adresse: `https://www.fhstp.ac.at/de/studium/informatik-security/cyber-security-and-resilience/studieninhalte`.

A. Interviewleitfaden

A.1. Begrüßung

- Bedanken für die Zeit des Interviewpartners
- Einholen der Einverständnis für Transkription und Nennung, Abstimmung über die Form der Nennung
- Kurze Erklärung bzw. Einführung in den Background der Arbeit

A.2. Organisation und Umfeld verstehen

In diesem Bereich soll zunächst das Umfeld und die Organisation verstanden werden, um die späteren Antworten adäquat in Kontext bringen zu können.

- In welchen Geschäftsfeldern ist die Organisation tätig? Wie viele Mitarbeiter:innen gibt es? Wie viele Mitarbeiter:innen gibt es im Bereich IT, IT-Security und Incident Response?
- Wenn es spezialisierte Mitarbeiter:innen im Bereich Incident Response gibt, was machen diese außerhalb von Sicherheitsvorfällen?
- Sofern die Organisation als Dienstleister für andere Unternehmen Incident Response-Leistungen anbietet: Wie sieht das Kundenumfeld aus? Gibt es hauptsächlich kleine und mittelständische Unternehmen oder sind große Unternehmen und Enterprise-Umgebungen der Fokus?
- Sofern die Organisation als Dienstleister für andere Unternehmen Incident Response-Leistungen anbietet: Welche Produkte oder Dienstleistungen gibt es im Incident Response-Umfeld? Gibt es einen Retainer-Vertrag bzw. SLAs oder nur Ad-Hoc-Support bei Incidents? Wird ein SOC betrieben?

A.3. (Allgemeine) Anforderungen an Mitarbeiter:innen verstehen

Anschließend sollen allgemeine Anforderungen an die Mitarbeiter:innen im Bereich Incident Response verstanden werden. Dabei gibt es keine Einschränkung im Themenbereich. Das heißt, dass hier auch Anforderungen technischer bzw. forensischer Natur angegeben werden können und sollen.

- Stellen Sie sich vor, ein Mitarbeiter gibt im Bewerbungsprozess an, Incident Response an der Fachhochschule gelehrt bekommen zu haben. Was erhoffen bzw. wünschen Sie sich von diesem Mitarbeiter? Was erwarten Sie sich bzw. welche Fähigkeiten wären essenziell?
- Wenn Sie eine freie Stelle in diesem Bereich ausschreiben, welche Anforderungen werden als Voraussetzung für Incident Responder genannt?
- Sind die Mitarbeiter:innen im Bereich Incident Response „Allrounder“, also müssen sowohl organisatorische Themen (z.B. Incident Koordination, Lagebild, Krisenmanagement, ...) als auch technische Themen (z.B. Loganalyse oder Recovery) betreuen oder werden diese Bereiche getrennt?

  Gibt es Personen, die nur Incident Response machen? Gibt es externe Kräfte, die beispielsweise Spitzen abdecken?

  Fängt man zum Beispiel mit einem technischen Schwerpunkt an und „arbeitet sich dann Richtung Incident Koordination bzw. Management hoch“?
- Gibt es Zertifizierungen und Ausbildungen, die für Sie von besonderem Interesse sind?

A.4. TKS-Anforderungen an Mitarbeiter:innen im organisatorischen Bereich verstehen

In diesem Interviewabschnitt sollen ausschließlich die organisatorischen Anforderungen an die Mitarbeiter:innen im Format TKS (Tasks, Knowledge und Skills) besprochen werden.

Tasks

- Welche Aufgaben im Incident Response übernehmen die Mitarbeiter:innen?
- In welchem Setting werden die Aufgaben erfüllt? Wie groß sind die Teams, die an einer Aufgabe gleichzeitig arbeiten? Welcher Zeitraum steht dafür üblicherweise zur Verfügung? Wie schnell müssen die Tasks umgesetzt sein?
- Welche Tasks muss ein Junior Incident Responder erfüllen können? Was wäre darüber hinaus wünschenswert?

Knowledge

- Über welchen theoretischen Background müssen die Mitarbeiter:innen verfügen und wie detailliert?

  Beispiel: Phasen des Incident Response gemäß ISO 27035 oder NIST SP800-61:

  L1: Phasen auflisten können,

  L2: Phasen beschreiben können,

  L3: Phasen anwenden und planen können,

L4: Phasen vergleichen und differenzieren können,

L5: Phasen bewerten/kritisieren/einschätzen können,

L6: Phasen entwerfen/konstruieren können.

- Mit welchen Schlagwörtern und Begriffen müssen die Mitarbeiter:innen umgehen können?
- Welches Knowledge muss ein Junior Incident Responder mitbringen? Was wäre darüber hinaus wünschenswert?

Skills

- Welche Social Skills müssen die Mitarbeiter:innen mitbringen?
- Inwieweit haben die Incident Responder direkten Kundenkontakt?

A.5. Lehrveranstaltungsplanung

Der letzte Abschnitt des Interviews dient insbesondere dazu, unabhängig von den anderen Fragen noch Ideen für die Lehrveranstaltungsplanung oder die praktische Übungsphase einbringen zu können.

- Was sind Ihrer Ansicht nach die zentralen Punkte, die in den Vorlesungen transportiert werden müssen (z.B. Vorbereitungs- und Lessons Learned Phase? Playbooks?)
- Was sind Ihrer Ansicht nach die zentralen Punkte, die bei der Konzipierung der praktischen Übungsphase/Cyberrange beachtet werden müssen?

  Umgang mit der Zeit: Anhalten oder mehrtägige zusammenhängende Übung

  Unerwartete Kundentermine? Regelmäßige Lagebildupdates?

  Berichterstattung (Zwischenberichte und Abschlussbericht, formell oder informell)

B. Transkription der Interviews

B.1. Interview am 07.04.2025 mit Mag. (FH) Philipp Mattes-Draxler, MSc (Partner Cybersecurity & Privacy, PwC Österreich)

CE: Was macht PwC, wie viele Mitarbeiter gibt es, wie viele in der IT, in der IT Security und im Incident Response Bereich?

PMD: Schwierige Frage, PwC allgemein ist ja Wirtschaftsprüfer, Steuerberater und Unternehmensberater; grundsätzlich ein Firmennetzwerk, das heißt, ein internationales Netzwerk mit insgesamt 370 000 Mitarbeitern, von denen eine mir nicht bekannte Anzahl in der IT Security ist, also was intern an Security Tätigkeiten gemacht wird, ist für mich ein gutes Stück intransparent. Ich bin ja im Bereich Unternehmensberatung tätig, und in Österreich haben wir Team von 50 Vollzeitäquivalenten in der Beratung für Cybersecurity Themen, davon eine fließende Anzahl an Mitarbeitern, die auch in Security Incidents mitarbeiten und EMEA-weit sind die Zahlen stark unterschiedlich. Da kann ich auch nicht genau sagen, wie viele davon wirklich für Incident Response und Beratung insgesamt tätig sind. Aber die Größenordnung ist wahrscheinlich zwischen 1200 und 1400 Mitarbeitern alleine in der Cybersecurityberatung.

CE: PwC bietet in diesem Bereich also nur Dienstleistungen für für externe Kunden an. PwC macht also inhouse keine Incident Response?

PMD: Nein, machen wir schon auch. Also PwC macht für sich selbst Incident Response insofern, als dass wir eine eigene IT Organisation haben, die für sich selber Incident Response machen. Das ist das sogenannte Network Information Security Team, das global aufgestellt ist und mit den lokalen IT-Mitarbeitern dann jeweils die Security Events und Incidents bearbeitet. Die beratenden Kollegen, so wie ich, bieten das hauptsächlich extern an. Wir machen aber auch intern Krisenübungen und die Tabletop Exercises für unser Management und unsere IT.

CE: Wenn man sich da das Kundenumfeld grob ansieht, sind das hauptsächlich wirklich größere Enterprises oder da finden sich da bei PwC auch kleine und mittelständische Unternehmen?

PMD: Gemischtes Publikum wahrscheinlich, was die Unternehmensgrößen betrifft. Aber wir sind eher im

größeren Unternehmensumfeld, also KMU, eher höhere Tendenzen, also größere Tendenz und Großunternehmen tätig, also börsennotierte Unternehmen, große familiengeführte Unternehmen, so etwas in die Richtung.

CE: Welche Produkte und welche Dienstleistungen gibt es im Incident Response Umfeld? Gibt es da nur ad hoc Support oder gibt es da auch SLAs, die die angeboten werden und wird zum Beispiel auch sowas wie ein SOC oder Ähnliches betrieben?

PMD: Ja, also wir haben sowohl auf der proaktiven, als auch in der reaktiven Domäne Serviceleistungen. Proaktiv beraten wir, wir führen Readiness Assessments durch, wir machen Übungen, bieten auch SOC-Beratungsleistungen an beziehungsweise bei der Implementierung von SOCs, also Security Operations Centern unterstützen wir in der Konzeption und auch im Onboarding von Dienstleistungen beziehungsweise im laufenden Betrieb im Management von den Dienstleistern. Wir erbringen aber auch selber Security Operation Center Dienstleistungen bei Kunden. Und im reaktiven Bereich bieten wir insbesondere SLAs in Form eines Incident Response Retainers an, wo wir eine interne Bereitschaft haben und diese interne Bereitschaft aus unterschiedlichen Mitarbeitern besteht und im Fall des Falles, wenn Kunden anrufen, Unterstützung brauchen, bilden wir dann ad hoc Incident Response Teams, die dann in unterschiedlichen Ausprägungen den Kunden situativ unterstützen. Und das wär dann die reaktive Dienstleistung eigentlich. Und die reaktive Dienstleistung geht von der Unterstützung der Geschäftsführung, Krisenmanagement, koordinierende Tätigkeiten, Erstellen von Lagebild bis hin zu sehr technischen Themen. Wir unterstützen unsere Kunden auch in IT Forensik und Digital Forensik-Themen bis hin zu Schadsoftwareanalysen, die nicht von uns hier vor Ort durchgeführt werden, sondern die unsere Kollegen vom Global Threat Intelligence Center dann für uns übernehmen.

CE: Das heißt, diese spezialisierten Mitarbeiter und Mitarbeiterinnen im Bereich Incident Response und machen nicht nur Incident Response, sondern die machen nebenbei auch noch was anderes, wenn gerade kein Incident ist. Was sind da typische Aufgaben für Leute, die in diesem Bereich spezialisiert sind?

PMD: Naja, wir sind normale Securityberater und haben unterschiedliche Themenbereiche, vornehmlich im Bereich Cyber Defence Management Consulting würde ich sagen. Wir arbeiten viel mit Threat Intelligence, um auch für Unternehmen ihre situativen Bedrohungen greifbarer zu machen und haben da unterschiedliche Produkte und Möglichkeiten, die wir unterstützen. Wir unterstützen in Incident Response Design Themen wie beispielsweise das Designen von Prozessen von CSIRT oder SOC-Organisationen. Es kann aber auch sein, dass unsere Mitarbeiter bei ganz anderen Projekten mitarbeiten, wenn keine Incident Response Einsätze da sind. Es ist aber nicht so, dass unsere Mitarbeiter hauptamtlich nur Incident Response-Einsätze machen und dann sozusagen Lücken füllen durch andere Themen, sondern ich würde das eher als Gesamtkonzert

an unterschiedlichen Tätigkeitsbereichen im Consulting bezeichnen. Und der Incident Response-Einsatz ist halt eine Form von Consultingeinsatz in dem Sinne.

CE: Im nächsten Abschnitt soll es um allgemeine Anforderungen gehen. Das heißt jetzt wirklich der Kreativität freien Lauf lassen, nicht irgendwie auf Organisatorisches oder Ähnliches einschränken lassen, auch wenn die Arbeit hauptsächlich darum geht. Angenommen, du bekommst eine Bewerbung von einem Mitarbeiter und da steht drinnen „Ich hab an der Fachhochschule Sankt Pölten Instant Responses gelernt." Was erhoffst du dir und wünscht du dir, dass dieser Mitarbeiter jetzt kann und vielleicht auf der anderen Seite was erwartest du dir, also das ist jetzt so das Minimum was der wirklich können muss, um nicht enttäuscht zu sein.

PMD: Und der Mitarbeiter ist Berufseinsteiger oder schon berufserfahren?

CE: Berufseinsteiger.

PMD: Also von einem Berufseinsteiger erwarte ich mir eher Schulwissen, das heißt analytische Fähigkeiten, wahrscheinlich eher technische Fähigkeiten, ein gewisses Basisset an Projektmanagement oder Arbeitstechniken, aber wenig ausgeprägt. Und bei den technischen Fähigkeiten wird es halt darauf ankommen, wo seine Spezialisierungen sind, eher im forensischen Sinne: Beweismittel sichern wird er wahrscheinlich können, zumindest wird er dazu einem Kurs gemacht haben. Schadsoftwareanalyse wird er können, und dann wird er rudimentäre Basiserfahrungen haben was Netzwerkbetrieb beziehungsweise Serverbetrieb betrifft, weil da für gewöhnlich auch ein, zwei Vorlesungen im Repertoire der Fachhochschule sind.

CE: Und irgendetwas Incident Response-Spezifisches vielleicht, wo du sagst, das wäre gut?

PMD: Ja, Incident Response ist schwierig zu greifen in dem Bereich, ja, weil das ja letztlich dann analytische Fähigkeiten sind.

CE: Wenn jetzt eine Stelle ausgeschrieben wird in diesem Bereich und der später auch im Incident Response mitarbeiten soll, was stehen da für Voraussetzungen, auch vielleicht in irgendwelchen Jobausschreibungen, drinnen oder was wünscht du dir, das da drinnen steht?

PMD: Also, wenn es wieder um Berufseinsteiger geht: Von den fachlichen Fähigkeiten, also man muss ja immer die fachlichen und die personellen Fähigkeiten unterscheiden, und dann gibt es motivatorische Themen auch noch wahrscheinlich, von den fachlichen Fähigkeiten erwarte ich mir ein Security Studium oder zumindest eine im Moment laufende Ausbildung im Security Bereich, also auf FH- oder Uniniveau. Das wär die Voraussetzung und über die Curricula von diesen Ausbildungen erwarte ich mir dann eben die Inhalte, die wir gerade vorher gehabt haben, dass die entsprechend abgedeckt sind, um ein gewisses strukturiertes Basisverständnis voraussetzen zu können, was jetzt die Technik betrifft. An persönlichen Fähigkeiten oder persönlicher Einstellung würd ich mir Eigeninitiative erwarten, Verlässlichkeit und auch die Fähig-

keit, seine eigenen Fähigkeiten tatsächlich abschätzen zu können, was bei Berufseinsteigern wahrscheinlich schwieriger ist als bei erfahreneren Kollegen.

CE: Wenn wir jetzt gleich beim Themenbereich Incident Response bleiben, muss dieser Mitarbeiter im Bereich Incident Response ein Allrounder sein, also sowohl organisatorische Fähigkeiten – Lagebild malen, Krisenmanagement, Koordination machen – haben oder nur technisch arbeiten? Sind die beiden Bereiche voneinander getrennt oder macht der eine Mitarbeiter einmal das und am nächsten Tag oder im nächsten Incident vielleicht das andere?

PMD: Also Spezialisierung ist immer gut. Die Frage ist, wann beginnt Spezialisierung? Ich glaube, dass ein gewisses „Generalistentum“, das jetzt vielleicht unter Anführungszeichen zu setzen, wichtig ist, um das Verständnis zu haben, was wie funktioniert. Das heißt, gerade junge Mitarbeiter würde ich schon mehrfach einsetzen, heute da, morgen dort oder bei dem Incident so und beim nächsten wieder anders, einfach nur, damit sie verschiedene Rollen und verschiedene Tätigkeiten besser verstehen und greifen können. Ab einem gewissen Niveau, und das wäre wahrscheinlich so noch 2 Jahren, so Senior Associate-Level bei uns, würde ich schon danach trachten, dass man die Mitarbeiter dann spezialisiert durch einschlägige Kurse und dann eben entweder eher Richtung Krisenmanagement ausbildet oder eher Richtung IT-Forensik oder in Richtung Schadsoftware-Analyse oder, oder, oder.

CE: Bleiben wir gleich bei diesen Zertifizierungen, Ausbildungen - wie auch immer – Fortbildungen. Was wären da für dich so wichtige Schlagworte, die du gerne in einem Lebenslauf oder sonst irgendwo sehen möchtest?

PMD: Ich glaube, dass die SANS-Kurse der Klassiker sind, wenn es jetzt in die Technik geht. Wenn es eher in Richtung Krisenmanagement oder allgemein Incident Handling geht, ist wahrscheinlich TRANSITS ein gutes Schlagwort, also da gibt's die TRANSITS 1 und 2, aber es gibt auch andere namhafte Anbieter und ich glaub, das wird dann situativ drauf ankommen. Wir bei PwC bieten auch mit der Cyber Academy entsprechende technische Schulungsmöglichkeiten, die über Pluralsight, also einen E-Learning-Anbieter abgebildet wird, wo einfach verschiedene Kurse dann aufeinander aufbauend insgesamt zu einem runden Bild führen sollen. Natürlich kann man auch vendorenspezifische Ausbildungen wie Firewall-Zertifizierungen oder Splunk, einem namhaften Anbieter von SIEMs oder Microsoftzertifizierungen da ins Treffen führen. Ich glaube, dass das gar nicht so relevant ist, welcher Anbieter das ist, sondern eher, dass die Tätigkeit, die dahintersteckt, letztlich einmal erlernt worden ist und die man dann in der Lage ist, auch auf andere Themenbereiche umsetzen zu können.

CE: Ich hab gerade schon ein bisschen diese Tasks, Knowledge und Skills angekündigt, dass die jetzt kommen werden. Jetzt soll es wirklich ausschließlich um organisatorische Anforderungen gehen, das heißt die

technischen Geschichten, Analysefähigkeiten und Ähnliches versuchen wir jetzt bitte ein bisschen auszuklammern, auch wenn es vielleicht nicht ganz einfach ist. Wenn wir jetzt im Bereich der Tasks bleiben, im organisatorischen Bereich, welche Aufgaben müssen da die Instant Responder:innen bei PwC übernehmen? Oder eigentlich das gesamte CSIRT übernehmen?

PMD: Da gibt es unterschiedliche Themen. Das eine ist einmal Lagebilderstellung, das heißt, das Zusammenführen von den jeweiligen Erkenntnisständen aus den unterschiedlichen Streams, das ist sicher ein organisatorischer Task. Ein anderer organisatorischer Task wäre es, die Streams zu führen. Das heißt wirklich zu koordinieren, die Analyse zu koordinieren, IT Recovery zu koordinieren und andere Themengebiete zu koordinieren. Das heißt, da gibt es Taskmanagement als klassischen Task, den man da ausfüllen muss und über das Zusammenführen der unterschiedlichen Erkenntnisstände in einem Lagebild gilt es dann eben das Lagebild zu führen, das ist auch ein organisatorischer Task. Auch ein organisatorischer Task wäre es wahrscheinlich, was kundenseitig zu erbringen ist, was wir dann noch als Spezifikum haben, dass wir im Hintergrund eine genaue Aufgabenbeschreibung und ein Aufwandstracking vollziehen und nachvollziehbar zu machen, sodass der Kunde weiß, wofür er eigentlich bezahlen muss und wir auf der anderen Seite wissen, dass der gesamte Incident Response-Einsatz betriebswirtschaftlich auch Sinn macht. Aus den technischen Streams heraus ist eine organisatorische Notwendigkeit, dass wir die Analyseergebnisse auch entsprechend dokumentieren. Dazu haben wir den Incident Response Tracker, in dem Indikatoren, Sichtungen, Events, etc. plausibel zusammengeführt werden, um dann letztlich die Hypothesen, die wir aufstellen, auch beweisen zu können und für einen Report nachvollziehbar machen zu können. Jetzt kann man drüber streiten, ist das technisch oder ist es organisatorisch? Aber das Reporterstellen ist für uns auch obligatorisch, wenn es um Incident Response geht.

CE: Was gibt es da zum Beispiel dann für Aufgaben im Reporting im Nachhinein?

PMD: Naja, einerseits die technischen Analysen zusammenzuführen. Andererseits einen roten Faden sicherzustellen, sodass sich ein natürlicher Lesefluss ergibt und dann eine Qualitätssicherung sowohl in fachlicher, inhaltlicher Sicht, dass da zum Beispiel die IP Adressen richtig sind, die da referenziert werden, dass die Evidenzen richtig referenziert sind, aber auch natürlich Orthographie und Semantik.

CE: Bleiben wir jetzt gleich bei diesen Aufgaben. Bei den nächsten paar Fragen geht es ein bisschen um das Setting, das heißt, wie werden die Tasks erfüllt? Werden die in Teams erfüllt, werden die alleine erfüllt hat? Welcher Zeitraum steht dafür zur Verfügung? Das ist natürlich ein bisschen spezifisch je nachdem, was ich mache. Das ist, ist schon klar, aber wie kann man das im Großen und Ganzen beschreiben?

PMD: Also da muss man unterscheiden in größere und kleinere Incidents. Kleinere Incidents werden in kleineren Teams erfüllt von ein bis wahrscheinlich 3 Mitarbeitern, wo einerseits die Tuchfühlung mit dem

Kunden, also das Kontakthalten mit dem Kunden, das Beraten vom Kunden, sicher im Vordergrund steht und dann im Hintergrund Analysen getätigt werden oder Sachverhalte vom Kunden plausibilisiert werden in einem kleineren Umfang, sodass sich da nicht die Notwendigkeit einer größeren Koordination ergibt. Wir haben zum Beispiel Kunden, die uns immer wieder dazu ziehen, wenn bei ihnen größere Incidents sind, sodass wir einfach die Tätigkeiten vom Kunden plausibilisieren und qualitätssichern, einfach in den Krisenmeetings dabei sind, um Hinweise zu geben oder auch insofern qualitätssichernd wirken, dass wir den Kunden darauf hinweisen, wenn er aus unserer Sicht auf Arbeitsschritte vergisst. Wir sind aber in keiner koordinierenden oder führenden Rolle, sondern eben lediglich in der Qualitätssicherung. Das sind wahrscheinlich die Incidents, die wir als Incident im kleineren Maßstab oder Umfang bezeichnen. Größere Incidents sind dann jene Incidents, wo sich der Kunde darauf verlässt, dass wir einen oder mehrere Teilstreams wirklich selber leiten. Das heißt, wir verfolgen für uns hier eine gewisse Teameinteilung, ein Analyseteam oder einen Analysestream, wo wir Logfileanalysen machen, Threat Intelligence Analysen machen, die Erkenntnisse aus der Schadsoftwareanalyse wieder zusammenführen und Hypothesen zum Angreifer aufstellen, die wir dann eben falsifizieren oder verifizieren. Dann gibt es einen IT-Stream für gewöhnlich, in dem die IT des Kunden entweder durch uns angeleitet oder qualitativ unterstützt wird. Das ist dann ganz besonders wichtig fürs Recovery. Für gewöhnlich haben wir dann noch einen Stream, der sich eher um Legal, Compliance und Öffentlichkeitsarbeit kümmert, also so ein bisschen das Krisenmanagement unter Anführungszeichen. Dann haben wir gewöhnlich noch einen Stream, der sich dann mit der Härtung auseinandersetzt. Das könnte auch beim Analyse- oder beim IT-Stream dabei sein, es kann aber auch ein eigener Stream sein, der dann ein SOC implementiert, der ad hoc Detektionsmaßnahmen etabliert, der ad hoc Securitymaßnahmen etabliert. Das ist meistens eine Architektenrolle, die da wahrgenommen wird und dann ganz wesentlich für uns ist das entscheidende Element der Koordination, dass der Incident Handler, meist unterstützt von jemandem, der das Lagebild zeichnet, wirklich den Kunden an der Hand nimmt, die einzelnen Streams und die Tätigkeiten in den Streams entsprechend koordiniert und mit den Geschäftsführern oder mit den Verantwortlichen vom Kunden entsprechend abstimmt.

CE: Wie schaut das Arbeiten aus? Ist das so, wie man es sich vorstellt, dass man sehr viel Stress hat, dass sehr viel in sehr kurzer Zeit fertig werden muss oder ist es eher ein „die Sachen gehen sich schon irgendwie aus“?

PMD: Also die Sachen gehen sich immer irgendwie aus, wenn man irgendwie als Qualitätsmaßstab nimmt. Aber natürlich ist es so, dass man zu Beginn eher zeitlich angespannt arbeitet, oft in kurzer Zeit sehr viele Ergebnisse bringen muss, vor allem Unklarheiten erkennen muss, weil ja die Lage oft zu Beginn sehr unklar ist, daher sehr viele Dinge parallel passieren müssen, um Klarheit und Orientierung zu bringen; nicht nur

für uns und unsere Mitarbeiter, sondern auch für den Kunden. Und ich glaube schon, dass die ersten zwei Wochen insbesondere zeitlich sehr angespannt sind und sich sobald sich dann die Lage etwas aufklärt, die Maßnahmen klarer sind, ein konkreter Fahrplan da ist, wie man weiter vorgehen möchte, die Analysen zu einem Gutteil abgeschlossen sind, so dass das Containment dann beginnen kann, dass sich dann auch die Zeitachse etwas entspannt.

CE: Du hast jetzt gerade vorher schon ein paar Tasks genannt, was wären davon jetzt so diese typischen, ich sag mal Junior International Responder Tasks, also der kommt gerade, vielleicht einem Praktikum oder frisch von der FH, hat das gelernt, was sind so typische Tasks, wo du sagst das ist jetzt genau deins im organisatorischen Bereich.

PMD: Im organisatorischen Bereich wäre es wahrscheinlich das Mitarbeiten in der Lagebilderstellung im Nachsteuern von Tasks zum Dokumentieren. Das sind wahrscheinlich schon eher so die organisatorischen Beginner-Tasks.

CE: Dann sind wir mit den Tasks schon durch und kommen schon zum Knowledge. Da gleich als Einstiegsfrage: Über welchen theoretischen Background im Incident Response müssen die Mitarbeiter:innen verfügen und wie detailliert muss dieses Backgroundwissen sein? Also als Beispiel die Phasen des Instant Response nach ISO 27035 zum Beispiel. Muss der die Phasen auflisten können, muss er sie beschreiben können, anwenden und planen, vergleichen und differenzieren, bewerten, kritisieren, entwerfen oder...?

PMD: Ich glaub, wichtig ist, dass man ein grundsätzliches Verständnis darüber hat, wie Informationssicherheit generell zusammenhängt, wie einzelne Maßnahmen zusammenhängen, auf welche Domäne sie wirken, also auf Netzwerk, Applikation, Mitarbeiter etc. Das ist einmal das eine, das Grundwissen. Das andere wäre technisches Grundwissen im Sinne von wie Security Controls funktionieren. Wie funktioniert eine Firewall? Was ist ein IDS, was ist der Unterschied zwischen einem network-based IDS und einem host-based IDS? Was ist ein EDR? Was ist SOAR? Also, diese ganzen Schlagwörter richtig einordnen zu können, um letztlich dann auch ableiten zu können, was ich denn wo erkennen kann. Organisatorisch sicher Grundwissen ist die Cyber Kill Chain als Konzept, aber auch das MITRE Attack Framework als Konzept, um dann letztlich eben die Indikatoren an der richtigen Stelle zu suchen, den richtigen Phasen zuordnen zu können und die richtigen Ableitungen machen zu können.

CE: Ein paar Begriffe und Schlagworte hast du ja jetzt auch gerade schon gesagt, gerade in der IT Welt dreht sich ja irrsinnig schnell. Das heißt, es ist schon auch eine Grundvoraussetzung, dass man mit solchen Abkürzungen auch umgehen kann und auch weiß, was dahinter steckt.

PMD: Also die IT Welt dreht sich, glaube ich, gar nicht so dramatisch schnell. Das Konzept Firewall ist sehr alt. Und ob das Ding jetzt EDR heißt oder host-based intrusion detection oder prevention System ist

jetzt wahrscheinlich auch semantisch seit den 2000er Jahren oder Mitte 90er Jahren ähnlich geblieben. Also ich glaub, diese Basiskonzepte sind tatsächlich wichtig fürs Verständnis. Dass ich mit neuen Technologien und neuen Ansätzen, Data Lake in der Cloud und so weiter einfach eine andere Dynamik ergibt, ist das andere, aber das Basisthema, ein System macht eine Aktion oder ein User macht auf einem System eine Aktion, das wird geloggt und dieses Log dann auswerten zu können, das ist vom Prinzip her immer noch gültig und das sollte vom Prinzip her verstanden sein. Und jetzt haben wir die Kill Chain und so weiter gehabt, das wäre sozusagen das, was wir jetzt ursächlich, glaube ich, im Incident Response, suchen im analytischen Bereich, klarerweise wenn es dann in die nächsten Phasen geht, in Containment, Erdadication und Recovery sind dann eher architektonische Fähigkeiten gefragt. Das hat ja dann weniger mit Incident Response im Sinne von Feuerlöschen zu tun, sondern sind dann eher planerische Designmaßnahmen und auch da ist es gut natürlich, wenn man die mitbringt. Die ist aber wahrscheinlich wenig für Juniors geeignet, weil da ein bisschen Erfahrung dann auch notwendig ist.

CE: Vom Backgroundwissen her, es gibt ja, schon ganz kurz angeschnitten, verschiedenste Standards, die versuchen, Incident Response zu beschreiben und darzustellen. Was würdest du dazu sagen? Was sind da so Werke, die man kennen sollte und inwieweit sollte man die kennen oder brauche ich das als Junior eigentlich gar nicht, weil ich im Endeffekt irgendwo hingeführt werde und sich dann mehr oder weniger ergibt, was man Aufgaben dabei sind?

PMD: Naja, wie gesagt, ich erwarte mir, dass jemand mit einer Fachhochschulwissen zu mindestens kommt. Da ist eine gewisse Form von theoretischem Hintergrundwissen schon, glaub ich, auch voraussetzbar. Also an Konzepten, wie schon gesagt die Kill Chain, MITRE Attack Framework. Die ISO 27035 ist eher sicher gut zu wissen oder zu kennen, ob man da jetzt jeden 27. Unterpunkt von links rezitieren kann, weiß ich nicht, ob das notwendig ist. Aber was als Grundsatzpapier sicher recht sinnvoll ist, wenn man es kennt und auch verstanden hat, ist das 11 Strategies of a world-class Cybersecurity Operations Center vom MITRE-Institute, natürlich hat auch das SANS-Institut entsprechende Konzepte, also auch SANS, hat ja einen Incident-Handling-Cycle. Also ich glaub, es ist jetzt gar nicht so entscheidend, welches Konzept man da kennt oder ob man nach dem NIST Framework vorgeht, das ist wahrscheinlich relativ egal. Ich glaub, es ist wichtig, dass man systematisch sich in der Materie einfach zurechtfinden kann.

CE: Und damit sind wir schon beim letzten Punkt in diesem TKS-Bereich, nämlich bei den Skills und da möchte ich gleich mit den Social Skills anfangen, die wir gerade schon einmal angeschnitten haben ein bisschen, was sind so diese persönlichen Voraussetzungen, die du besonders im Bereich Internet Response für wichtig erachtest.

PMD: Eigeninitiative und Verlässlichkeit. Und Genauigkeit.

CE: Inwieweit haben die Incident Responder, egal welches Level, egal welche Seniorität Kundenkontakt bei euch? Ist das eher so, einer spricht mit dem Kunden und alle anderen sitzen im Hintergrund, arbeiten dieser einen Person zu und haben keinen Kundenkontakt oder ist das schon so, dass es da verschiedene Kommunikationswege auch immer wieder Richtung Kunde gibt?

PMD: Das kommt tatsächlich voll drauf an. Es gibt Situationen, wo der Kunde mit vielen unserer Analysten in Kontakt kommt, es gibt Situationen, wo der Kunde genau einen Ansprechpartner hat, und der sozusagen unserer Mitarbeiter im Hintergrund steuert. Das ist wirklich situativ abhängig. Rein tendenziell ist es so, dass wir versuchen, dem Kunden klare Ansprechpartner zu bieten, damit er auch weiß, zu welchem Thema er mit welchem Mitarbeiter reden kann oder soll. Übersetzt auf die Streams, die wir vorher gehabt haben heißt das, dass ich davon ausgehe, dass zu mindestens die Streamleads und der Incident Handler mit dem Kunden in stetigem Austausch sind. Dass innerhalb des Streams dann Mitarbeiter mit den Kunden sich austauschen, ist aber sicher je nach Situation natürlich auch eine faktische Notwendigkeit.

CE: Vielen Dank, dann sind wir mit dem TKS-Bereich schon fertig und hüpfen zum letzten Bereich, nämlich der Lehrveranstaltungsplanung, die insbesondere bei dir sehr interessant ist, weil du ja auch am Technikum Incident Response unterrichtest. Der Bereich dient jetzt auch dazu, unabhängig von den anderen Fragestellungen, die wir gerade schon schon diskutiert haben, auch Ideen, Ansätze und Ähnliches einzubringen, die man einfach in einer Lehrveranstaltung zu dem Thema gut benutzen und durchbringen kann. Und da wäre die erste Frage, was sind vielleicht so zentrale Themen und und Konzepte, die man in so einer Vorlesung transportieren kann oder in Wahrheit transportieren muss? Ein Beispiel, an der Fachhochschule St. Pölten werden beispielsweise derzeit auch Playbooks im Fach Incident Response unterrichtet. Ist das da sinnvoll und welche Themen fallen dir vielleicht sonst noch ein, wo man sagt, das gehört da eigentlich voll dazu?

PMD: Das ist ein bisschen eine philosophische Frage, wahrscheinlich, je nachdem, wie man sich die Welt baut. Frei nach Pipi Langstrumpf, ich bau mir die Welt, wie sie mir gefällt. Wenn ich an der Rallye Paris–Dakar teilnehme, dann bin ich in erster Linie entweder Auto- oder Motorradfahrer, der aber in der Wüste fahren muss, dort wo halt wenig Leute sind, die einem helfen. Wenn ich wenig Leute habe, die mir helfen, dann brauche ich ein Basisverständnis von Mechanik, ich muss im schlimmsten Fall vielleicht sogar mein Getriebe mit ein, zwei Kollegen ausbauen können und wieder einbauen können. Ich weiß nicht, was es da alles gibt, es geht auf jeden Fall wahrscheinlich mehr als nur Reifen wechseln vom Skillset her. Bei Internet Response ist ein bisschen ähnlich. Also ich hab an der FH St. Pölten oder am Technikum Wien oder Hagenberg unterschiedlichste Lehrveranstaltungen, die mich alle in Incident Response unterstützen werden, je nachdem, wie gut ich da bin. Ich werd IT forensisches Basiswissen brauchen, ich werd verstehen müssen, wie sich Schadsoftware persistiert, wie das funktioniert, dass man sich andere Rechte erarbeitet, im Sinne

von Angreifervorgehenswissen, muss aber dazu auch kein Pentester sein. Wenn ich Pentester-Fähigkeiten hab, ist es wahrscheinlich besser, um die Courses of Action aus Angreifersicht beurteilen zu können. Aber was meine ich jetzt insgesamt? Ich glaub Incident Response ist so ein Alles und Nichts, wo ich ganz viele verschiedene Fähigkeiten gemeinsam zur Anwendung bringe, weil ich, eben letztens wie bei der Rallye Paris–Dakar einfach Auto fahre, ohne dass ich jetzt im Detail wissen muss wie ein Getriebe funktioniert, aber wenn ich alleine bin und es wechseln muss, dann sollte ich verstehen, wie es geht, weil sonst werde ich nicht weiterfahren können. Ob jetzt Playbooks im Sinne von Incident Response Plänen in einem Fach Incident Response gelehrt werden oder wie man solche erstellt ja, wenn man es als proaktives Thema sieht. Wenn man jetzt rein eine technische Incident Analyse haben möchte, ist es vielleicht nicht unbedingt notwendig. Das ist schwierig zu beantworten, aber wenn man jetzt sich methodisch-didaktisch sich an der ISO 27035 orientiert, dann ist es sicher richtig, wenn man solche Inhalte da drinnen hat.

CE: Das heißt, wenn ich jetzt richtig verstanden habe, ist auch insbesondere diese Verknüpfung von den anderen Fähigkeiten, die man aus anderen Lehrveranstaltungen hat, vielleicht auch gar nicht so uninteressant, weil ja bei Incident Response sehr viele verschiedene Fähigkeiten zusammenkommen.

PMD: Ja, Incident Response ist Königsklasse. Incident Response repariert ja dann, wenn alles kaputt ist oder wenn einer aktiv da ist, der Dinge kaputt macht. Und unter dem Gesichtspunkt brauche ich bei Incident Response sowohl Wissen über die Geschäftsprozesse, das geht jetzt in Richtung Business Continuity wahrscheinlich, aber auch eben sehr stark koordinierende Fähigkeiten. Ich brauch aber auch technische Expertise, um die richtigen Schritte ableiten zu können, richtige analytische Maßnahmen zu setzen, richtige Folgemaßnahmen zu setzen. Deswegen ist das schwierig zu fassen, aber ich glaub, dass die ISO 27035, so haben wirs an der FH Technikum auch gemacht, ein guter Leitfaden ist, um sich da zu orientieren. Aber wenn wir jetzt Playbooks machen, heißt das ja auch, dass man Prozesse wahrscheinlich verbessert. Und wenn man in Prozessen denkt, braucht man Fähigkeiten aus dem Prozessmanagement heraus. Es gibt dann andere Frameworks wie COBIT, das sich sehr stark mit IT Prozessen auseinandersetzt oder der Gestaltung von IT Prozessen auseinandersetzt. Es gibt das ITIL-Framework, das sich sehr stark mit IT Service Management auseinandersetzt. Das ist dann schwierig, dass man irgendwo eine klare Grenze setzt wahrscheinlich.

CE: Und die allerletzte Frage ist, wie bereits besprochen, es soll ja eine praktische Abschlussübung geben, in der auch mal ein Incident praktisch ausprobiert werden kann. Was sind da für dich zentrale Punkte, um auch wirklich Take Aways möglich zu machen? Zum Beispiel, Umgang mit der Zeit. Soll man die Zeit zwischendrin anhalten oder, wenn man eine Woche Übungszeit hat, dann läuft die einfach eine Woche durch und die Studierenden können mehr oder weniger machen, wie sie wollen? Soll man zwischendrin zum Beispiel unerwartete Lagebild Updates anfordern, „in einer Stunde möchte der Vorstand ein Lagebild-

Update haben“?

PMD: Ich glaub, das kommt auf die Rahmenbedingungen und auf die Zielsetzung an, die man verfolgt. Wenn man realistische Übungen machen möchte, um ein Szenario auch technisch zu beüben, dann wird das die Zeit brauchen, die es braucht. Da kann man dann auch gerne eine Woche durchüben. Die Frage ist, ob sich das organisatorisch abbilden lässt. Also die großen Cyberübungen von Bundesheer, NATO etc, die spielen dann tatsächlich zwei Wochen durch, also Locked Shields zum Beispiel ist da so ein Übungsformat, das genau dem entspricht. Da passieren dann technische Dinge, es passieren Updates, es passieren Lageupdates, man muss als Organisation darauf reagieren. Wenn man weniger Zeit hat oder auch der Übungsinhalt jetzt ein anderer ist, dass man eben spezielle Fähigkeiten oder Lagerbilderstellung oder nur Entscheidungsfindungsprozesse übt, dann geht das wahrscheinlich auch in deutlich reduzierter Zeit.

CE: Aber macht es Sinn, auch ein bisschen die Studierenden unter Zeitdruck zu setzen, mit mit gewissen Aufgaben?

PMD: Die Sinnfrage kann nur dann beantwortet werden, wenn man den Zweck kennt. Wenn der Zweck die Anlernstufe ist, dann nein, wenn der Zweck das Enablen der Anwenderstufe ist, dann ja. Also Zeitdruck würde ich nur dann hineinbringen, wenn bereits ein höheres Niveau da ist, ansonsten macht es keinen Sinn, weil man da aus der Anlernstufe nicht rauskommt, sondern in die Überforderung hineinkommt. Überforderung heißt, dass man in eine Negativstrudel hineinkommt und keinen Spaß an der Disziplin haben wird.

CE: Du hast vorher auch schon gesagt die Berichterstattung ist ein sehr, sehr wichtiges Thema. Das heißt würdest du, und inwieweit würdest du zum Beispiel eine Berichterstattung auch in so einer Übung im Nachhinein einfordern?

PMD: Also das Schreiben von technischen Berichten würde ich tatsächlich als Disziplin in einem Fachhochschulstudiengang sehr stark fordern. Jetzt wird mir jeder, der an einer Fachhochschule lehrt oder für die Gestaltung von Fachhochschulstudiengängen verantwortlich ist, sagen, naja, das Schreiben von wissenschaftlichen Arbeiten, Bachelorarbeiten, Masterarbeiten ist inhärent Bestandteil von solchen Studiengängen und trotzdem ist es so, dass das Schreiben von technischen Analysepapieren, glaube ich, eine eigene Disziplin ist, die es wert ist, auch entsprechend gelehrt zu werden. Also ganz wenige Leute können das, glaube ich, wirklich gut.

CE: Dann vielen Dank für deine Zeit!

B.2. Interview am 08.04.2025 mit Dipl.-Ing. Andreas Plank, BSc (Head of Security Services, ACP Gruppe)

CE: Die ACP-Gruppe ist ja ein ganz bekanntes Unternehmen im Cyber Security Kontext, in welchen Geschäftsfeldern seid ihr grundsätzlich tätig?

AP: Die ACP ist grundsätzlich primär in Österreich und Deutschland tätig. Wir haben, ich glaube, ein bisschen über 2500 Mitarbeiter und sind in Österreich auf jeden Fall einer der größten IT Provider und haben im Prinzip vier Geschäftsfelder, in denen wir aufgestellt sind. Das ist einerseits Hybrid Cloud und Data Center, das heißt sowohl on premise gibt es bei uns in Österreich, in Wien ein Data Center und in Deutschland in Kolbermoor. Aber natürlich auch in der Cloud haben wir verschiedenste Leistungen beziehungsweise etablieren gerade Cloud Center of Excellence, wo wir dann Kunden unterstützen, ihren Cloudbedarf zu befriedigen. Das zweite Geschäftsfeld ist Modern Workplace, das ist so eines, wo wir eigentlich so am größten sind. Also alles rund um den Arbeitsplatz, von einerseits im Betrieb des Arbeitsplatzes, aber auch aufsetzen, ausliefern, im Büro des Auftraggebers aufstellen, verkabeln also alles Mögliche von Repair Services, hin zu vollen Managed Services. Das dritte Geschäftsfeld ist dann Netzwerk und Security. Da fällt dann auch mein Bereich rein, also wir haben im Netzwerkbereich natürlich ganz normal Network Operation Center in der ACP und haben natürlich auch Leistungen in dem Bereich. Und im zweiten Part Security, wo es im Prinzip heute ja um das Thema geht, haben wir auch verschiedene Lösungen. Ich bin zuständig in der ACP Ost für das SOC und andere Leistungen und im SOC prinzipiell ist bei uns neben dem klassischen Security Operations für unsere Kunden auch Incident Response angesiedelt. Wir bringen Incident Response grundsätzlich aus dem SOC-Team heraus. Wir haben da keinen eigenen Bereich gegründet, sondern haben gesagt, unsere Senior Analysten, die dazu Interesse und Lust haben, bilden wir zu Incent Respondern aus und die machen dann sozusagen einerseits für unsere Managed Incent Response Kunden die Fälle beziehungsweise, wenn irgendwelche anderen Kunden anfragen, dann machen wir das nach best effort ebenso. Das heißt, wir haben sehr viele Einsätze, vor allem bei Nicht-SOC-Kunden. Sehr, sehr selten SOC-Kunden, die meisten Kunden sind welche, die zwar irgendwie von der ACP betreut werden oder schon mal eine Hardware gekauft haben oder Software, die aber oft gar nicht in einem Managed Service sind. Das heißt, da kommen wir dann zu Infrastrukturen, die wir auch nicht kennen, also wir kennen beide Welten, sage ich mal. Das letzte Geschäftsfeld ist Digital Solutions, wo es im Prinzip unterschiedliche Themenbereiche gibt. Das dreht sich grundsätzlich um Digitalisierung, Stichwort Automatisierung, Prozessautomatisierung, KI, Datenanalyse und solche Sachen, wo es im Prinzip einfach wirklich um eher Daten geht und wie können wir bei unseren Kunden Automatisierung umsetzen oder aus Daten Mehrwerte generieren.

CE: Wie viele Mitarbeiter habt ihr da im Bereich SOC dann eigentlich? Wie du ja schon gesagt hast, es gibt ja keinen eigenen Bereich für nur Incident Response.

AP: Also im SOC sind wir derzeit 32 Mitarbeiter, wenn ich mich selbst mitzähle, die im Wesentlichen in drei Bereiche aufgegliedert ist. Wir haben einerseits unser Analystenteam, die für die tägliche Analyse von Security Incidents bei unseren Kunden zuständig ist. Wir haben das Consultingteam, die im Endeffekt die Kundenbetreuung übernehmen. Das heißt, das sind Ansprechpartner, die dem Kunden namentlich bekannt sind, die Monatsmeetings machen, die zeitunkritische Anfragen lösen, die das Vulnerability Management betreuen und im Prinzip alle Aspekte rund ums SOC-Service mit dem Kunden koordinieren. Und der dritte Bereich ist dann Engineering. Wir haben natürlich sehr viel Infrastruktur, die wir betreiben müssen, das wird alles auch aus dem SOC heraus erbracht. Das heißt, wir haben hier nicht den Ansatz, dass wir sagen, unsere Infrastruktur wird von anderen Serviceeinheiten betreut, sondern das machen wir quasi aus dem SOC heraus. Da gibt es auch viel Automatisierungsbedarf, das heißt wir verwenden verschiedene Technologien, um unsere Workflows zu automatisieren, damit das halt dann auch in so einer Breite überhaupt möglich ist. Das heißt, wir skalieren jetzt rein von der Kundenanzahl stark über Automatisierung – also jetzt nicht in der Analyse mit Stand heute, sondern eher im Betrieb dieser ganzen Infrastrukturen im aktuell und gleich halten, also wie werden Use Cases über alle Kunden ausgerollt, wie wird sichergestellt, dass die funktionieren und solche Themen, die halt einfach im Betrieb auch wichtig sind und Prozesse erfordern. Diese ganze Analyse funktioniert so, dass wir im Prinzip in einem Analyseteam, das auf Basis einer zentralen Alert-Queue Incidents und Alarme von unterschiedlichsten Kunden analysiert, die dann aber auch die Möglichkeit haben, in kleineren Analysteams zusammen gewisse Themen zu untersuchen. Das heißt, es ist nicht so, dass wir sagen der Herr Müller ist jetzt dafür, den Kunden 123 zuständig und kein anderer schaut sich den an, sondern es wird relativ viel übergreifend gearbeitet und ausgetauscht. Da haben wir einfach die Erfahrung gemacht, dass das sinnvoll ist, weil du weniger Betriebsblindheit entwickelst, wenn du ständig andere Kunden analysierst. Was dafür wichtig ist, ist eine gute Dokumentation, das heißt ohne Dokumentation funktioniert das Ganze nicht. Da setzen wir dann auch „Schichtnotizen“, so nennen wir das, ein. Das heißt, wenn es Vorkommnisse gibt zu Kunden, dann wird es dokumentiert, jeder hat Zugriff auf diese Dokumentation und wenn von Früh- zu Spätschicht gewechselt wird, können die nachschauen: Was ist bei dem Kunden gerade los? Was ist da passiert? und können sich dann relativ schnell wieder auf die neue Situation einstellen. Ich mach vielleicht gleich die Überleitung zum Incident Response, dass da vielleicht auch ein bisschen klar ist, wie das bei uns dann organisiert ist. Wie gesagt, unsere Inident Responder, wenn gerade kein Fall zu bearbeiten ist, sind im Prinzip auch Analysten, in den meisten Fällen Senior Analysten, die schon ziemlich gutes Analyse-Know-How haben und die dann mit Ausbildungen, also vor allem technischer Natur, in

Richtung Incident Response ausgebildet werden. Das heißt, Forensikkenntnisse sind da im Endeffekt wichtig. Meiner Meinung nach ist es ein schmaler Grat, weil auch Analysten einen Großteil dieser Kenntnisse haben müssen. Jetzt nicht unbedingt: Wie kann ich ein Artefakt von einem Betriebssystem heraussuchen, aber sehr wohl: Wie funktionieren die Angriffe? Welche Dinge passieren, wo kann ich quasi Use Cases und Alarme entwickeln? Was sind Nachweise, dass ein Angriff auf dem System war? Das brauch ich eigentlich in beiden Welten, deswegen funktioniert es auch sehr gut, dass du Analysten zu Incident Respondern ausbildest. Was da dazu kommt, du hast es eh auch schon vorher gesagt, sind Prozesse. Wir haben die Erfahrung gemacht, dass es sehr wichtig ist, nach einem gewissen Framework vorzugehen. Das heißt, bei uns beginnt im Endeffekt alles einmal immer mit einem Scoping, also im Normalfall schreit der Kunde „Hey, ich hab da ein Problem, ich glaub ich bin gehackt worden, bitte helft‘s mir“. Dann benötigt man vorher einmal ein Scoping, das heißt in dem Scoping muss ich wissen: Worum geht’s überhaupt? Wir nennen das Ganze „das erste Interview“ und im Prinzip gibt es da einen Fragenkatalog. Wichtig für uns ist einfach einerseits einmal: Gibt es schon eine Klarheit über Kosten? Da reden wir jetzt wieder aus Dienstleistersicht. Für uns ist natürlich wichtig, bevor wir da Stunden um Stunden investieren, zahlt der Kunde überhaupt, gibt es eine Kostenfreigabe? Gibt es eine Cyber Versicherung? Wir haben schon oft den Fall gehabt, dass Kunden mit uns einen Incident Response Fall angefangen haben, abzuwickeln. Dann hat sie herausgestellt, er hat eine Versicherung, der Versicherer hat gesagt ja, war nur mit einem von mir, das heißt, wir sind dann wieder heimgegangen. Und dann geht es im Prinzip eh schon in diese Rollenverteilung rein. Incident Response kann aus unserer Sicht relativ unterschiedlich ausschauen. Manchmal gibt es wirklich rein eine technische Analyse, wo ein Kunde sagt „Hey, bitte beantwortet mir jetzt hier diese technische Frage. Ich will wissen, ist das wirklich ein Phishing gewesen” oder irgendwelche anderen technischen Fragen oder benötigt er auch Koordination dazu. Also ein Incident Management in dem Fall, das ist im Prinzip genau das, wo man dann in so eine Koordinatorfunktion reingeht. Da geht es dann darum, dass du auch, wie ein Projektmanager in Wirklichkeit ein Projekt leitet, einen Incident leiten musst, indem du sagst, so schauen die Timelines aus, um diese Uhrzeiten gibt es einen Termin zum Status Update, wo wir die weiteren Schritte besprechen und so weiter. Was natürlich auch sein kann ist, dass man andere Stellen beim Kunden koordinieren muss, wie zum Beispiel Unterstützung bei der Pressearbeit oder einen Juristen. Für uns ist auch wichtig, mit wem wir überhaupt sprechen, also wer ist unser Gegenüber? Ist das der Geschäftsführer? Ist das IT Leiter? Ist das ein Mitarbeiter? Ist das ein User? Und ist überhaupt klar, wer für was zuständig ist? Da kommen wir oft in Situationen rein, wo es keine Vorbereitung gegeben hat. Da muss für uns klar sein, ist dem Kunden überhaupt selber klar, wer darf überhaupt welche Dinge beschließen oder entscheiden? Gibt es irgendwelche Kontaktinformationen und so weiter und sofort. Und dann geht es im Prinzip schom bisschen ins technische rein,

dass man sagt: Wer hat den Incident erkannt, wann ist aufgefallen, wie ist erkannt worden, also was sind die Umstände zu diesem ganzen Incident? Was ist betroffen? Und was müssen wir uns eigentlich alles ansehen? Das ist im ersten Schritt immer wichtig zu wissen, wie groß wird das Ganze und wieviel Zeitressourcen, wieviel Personalressourcen brauch ich, um diesen Incident überhaupt bewältigen zu können? Und natürlich, wie zeitkritisch ist das Ganze? Wenn sich das jetzt voll arg anhört, aber der Kunde sagt na, ich hab keinen Stress, weil ich hab eh die Internetleitung gekappt und alles geht auf dem zweiten Standort weiter, dann muss man vielleicht jetzt nicht die Nacht durcharbeiten, sondern kann's vielleicht am nächsten Tag machen, ja.

CE: Vielleicht bleiben wir gleich genau bei dem Thema Kunden, nur um es ungefähr zu verstehen: Habt ihr hauptsächlich eher kleinere mittelständische Unternehmen oder hauptsächlich Enterprises?

AP: Da ist die ACP sehr breit aufgestellt. Wir haben vom KMU-Segment bis zum Enterprise-Segment alle Kunden da drinnen und auch bei Incident Response haben wir von bisher von großen Banken bis hin zu einem kleinen Autohändler, also das ist sehr unterschiedlich und dementsprechend gibt es auch unterschiedliche Voraussetzungen, die du beim Kunden vorfindest. Bei einem Kunden, den wir noch nie gesehen haben, was aus unserer Sicht eigentlich die bessere Variante ist, ist es einfacher, wenn sich jemand auf so einen Fall vorbereitet. Wir haben ja schon von Prozessen gesprochen, was wir machen mit Kunden, wo wir sagen „Hey, Incident Response – schon mal drüber nachgedacht?" und sie sagen „Ja, das wollen wir machen", dann machen wir einfach Incident Response Preparation Workshops und das ist im Prinzip auch aus unserer Sicht ein wichtiger Prozess, dass man sagt, der Incident Response startet am besten bei der Preparation und da gehen wir mit dem Kunden, meistens in so zwei Tagesworkshops, wirklich von Themen wie: Gibt es überhaupt definierte Zuständigkeiten, wer darf solche Dinge dann entscheiden, bis hin aber auch zu technischen Vorbereitungen, wo wir sagen zum Beispiel bist du in der Lage, Technologie innerhalb von ein paar Stunden auszurollen? Hast du Softwareverteilung? Können wir Agents ausbringen? Wie schnell schafft man das? Schafft man das flächendeckend? Gibt es Blind Spots und so weiter und so fort. Also wirklich die technischen Voraussetzungen klären, technische Vorbereitungen treffen wie irgendwelche Notfall-VLANs vorbereiten und so weiter und so fort, da gibt es unterschiedlichste Sachen, aber natürlich auch und das ist meistens das schwierigere, die organisatorischen Vorbereitungen. Das greift ein bisschen auch immer ins in so eine Art von Notfallmanagement rein. Also ich habe ganz oft auch das Thema, dass wir aus einem Notfallmanagement heraus oft dann ins Incident Response reinkippen und umgekehrt auch. Wenn ich Incident Response beim Kunden in der Vorbereitung habe und das ein größerer Kunde ist, dann wird es sich meistens auch ins Notfallmanagement eingliedern. Also das ist aus meiner Sicht auch wichtig, dass man, dass man das einfach mitberücksichtigt, dass das nicht für sich alleine steht, sondern dass die Unternehmen

einfach prozessual gut aufgestellt sein sollten, um dann solche Incidents, wenn sie eintreten, auch behandeln zu können und dass jeder weiß, was er jetzt tut. Das Schlimmste und das ist leider meistens der häufigste Fall ist, wenn die Kunden das nicht gemacht haben und dann hektisch anrufen und wollen, dass du ihnen hilfst. Das würde ich mal sagen, wäre auf jeden Fall wichtig, dass man quasi behandelt, wie bereite ich ein Unternehmen auf Incident Response vor? Also diese Preparation-Phase, da einen Schwerpunkt drauf zu geben und sagen wie bereite ich mich darauf vor, was sind wichtige Dinge? Das würde schon als wichtig empfinden.

CE: Dann gehen wir mal kurz in den nächsten Bereich. In diesem zweiten Bereich wollen wir jetzt die allgemeinen Anforderungen an den Mitarbeiter verstehen, das heißt Bereich Incident Response ohne Einschränkung des Tätigkeitsbereichs. Das heißt nicht nur prozessual, das kann auch jetzt wirklich sehr technisch und sehr, sehr forensisch werden. Das heißt, wir überlegen uns jetzt einfach mal, ein Bewerber gibt an, Incident Response, das habe ich an der Fachhochschule gelernt. Was erhoffst du dir und was ist so ein bisschen so dieses bare minimum, wo du sagst, naja, das sollte der schon können.

AP: Also das bare minimum wär für mich, dass er grundsätzlich, eine Killchain versteht, dass er MITRE Attack versteht, du hast das vorher selber schon angesprochen und ich glaub das ist etwas, was oft gar nicht vermittelt wird, weil wir so sehr im technischen drinnen sind. Dieser analytische Denkprozess. Also dass wenn ich jetzt da ein Signal hab irgendwo wo ich sag, keine Ahnung, du hast vorher das Beispiel genannt „ich hab diese Malware entdeckt“, dass ich mir überleg OK, was heißt es jetzt? Wo bin ich, in welcher Phase? Was könnte davor gewesen sein, was könnte danach gewesen sein und von diesem Pivot Point mir dann weiter überlege „Was muss ich mir jetzt nur anschauen? Welche Dinge sollten wir noch prüfen? Was könnte da der Angreifer gemacht haben?“ Dann sehe ich auf dem Storage wieder die Malware, das heißt, wie du vorher gesagt hast, da muss man eigentlich überlegen „Wie sind die da hinkommen? Wie waren die Wege und welche Data Sources machen Sinn, sich anzuschauen, wenn ich diese These, die da aufstehe, wie der Angriff funktionieren hätte können, dann verifizieren will?“ Dieser analytische Prozess, der ist für mich wichtig und darauf aufbauend natürlich, je besser die die Leute schon ausgebildet sind in Technologie, also wie kann ich das jetzt untersuchen? Was gibt es da für Artefakte wie collecte ich die, wie schau ich mir das an, wie funktioniert das in scale über vielleicht tausende Endpunkte? Weil das ist ein Unterschied, ob ich jetzt mit einem Tool einen Client triagier oder ob ich das über Tausende mache. Dann ist das natürlich super, aber mir ist eigentlich viel wichtiger, dass das Mindset oder dieses analytische Denken zu vermitteln. Das ist, auch wenn ich jetzt wieder von Incident Response auf die Analysten hüpfe, das ist ja das, was wir bei der Ausbildung der Leute eigentlich forcieren. Nicht nur dieses „Was gebe ich da jetzt ein in der Search, damit ich das rauskriege?“, sondern „Wie kann dieser Angriff funktioniert haben?

Was ist das für eine Art Angriff? Wie schaut diese Art von Angriff im Normalfall aus oder wie könnte sie ausschauen und was glaube ich, ist davor und danach passiert?" Also das ist für mich essentiell. Zweiter Punkt, den ich sehr wichtig finde und der oft vernachlässigt wird, ist diese Information dann transportieren zu können. Da geht es mir um managementtaugliche Berichterstellung, die aber technisch auch präzise ist. Wir haben die Erfahrung gemacht, dass die Berichte, die wir erstellt haben, zu technisch waren, sodass die, die die konsumiert haben, nicht verstanden haben, weil im Incident Response kommunizierst du selten mit ITlern, sondern oft mit Entscheidern. Und wenn dann drinnen steht, irgendwas auf einer Seite beschrieben mit irgendwelchen technischen Details, dann verstehen sie das überhaupt nicht mehr. Das heißt, ich finde, managementtaugliches Bericht-Schreiben - wie strukturiert man den Bericht? Wie kann ich Informationen so aufbereiten, dass sie auch verständlich sind und trotzdem technisch präzise sind. Das sind die Themen, die sind die Hauptthemen, die ich sehe. Analytisches Denken und das Ganze auch niederschreiben und zu Papier bringen. Was ich auch wichtig finde ist, dass man einen Fokus darauflegt, beizubringen, wie so ein Kundenscopeinggespräch funktionieren kann. Also Kommunikation in so einem Krisenfall ist, glaube ich, auch ein guter Skill, also wenn wir von Soft Skills jetzt reden. Weil da kann recht viel schief gehen. Also was ich auch gelernt hab, ist, es gibt teilweise technisch sehr, sehr gute Leute, die aber das vom Auftreten her nicht perfekt vielleicht transportieren können, ja, die vielleicht ein bisschen unsicher wirken und du musst meiner Meinung nach auch im Incident Response klarkommen damit, dass du bis zu einem gewissen Grad nicht alle Informationen hast. Das heißt, du hast immer ein nicht vollständiges Bild, das du interpretieren musst und das aber mit einer Confidence danach zu transportieren, so dass ein Entscheider nicht verunsichert ist und glaubt der hat keine Ahnung. Das ist auch ein Skill, der wichtig ist.

CE: Du hast doch gerade schon gesagt, irgendwer muss es ja kommunizieren, irgendwer muss vielleicht daran ein Lagebild malen, sind da eure Internet Responder unter Anführungszeichen „Allrounder", also machen, die sowohl technische Analyse als auch Lagebild oder gibt es da wirklich Leute, die jetzt spezialisiert mehr in der koordinativen Rolle sind und die anderen, die mehr fokussiert in der in der technischen Analyserolle sind?

AP: Also Lagebild per se haben wir eigentlich selten, sondern wir arbeiten eigentlich meistens mit Berichten, also so quasi wirklich: Es gibt eine Situation, es gibt, wir nennen es investigative Fragestellungen. Das heißt, wir formulieren für den Kunden wirklich Fragestellungen, wo wir sagen, ist das das, was du von uns wissen willst? Wenn wir jetzt über einen Bericht für Incident Response sprechen, also wie ist der Angreifer reingekommen? Was haben wir gemacht? Das machen die Incident Responder selbst. Da, glaube ich, geht es wirklich nur, wenn du wirklich groß bist, dass du das trennst, also wenn Mandiant einen Fall macht, werden sie sowas sicher tun, oder große Beraterunternehmen werden da wahrscheinlich auch eine

gewisse Trennung haben, also Qualitätssicherung haben wir auch, dass da nochmal wer drüber liest, aber wirklich diese funktionelle Trennung in der Incident Responder, der Berichtschreiber, der Qualitätssicherer, der Malwareanalyst, das haben wir nicht, dafür sind wir zu klein. Wir haben wirklich eher die Allrounder, die das alles machen müssen. Was ich vergessen habe vorher, neben dem Tathergang analysieren, was da natürlich wichtig ist, Maßnahmen zu empfehlen, die tatsächlich mit dem Incident etwas zu tun haben, das ist auch ein wichtiger Skill. Wir haben schon oft erlebt, auch von anderen Firmen, die teilweise auch wir als Sub beauftragt haben, in der Vergangenheit, dass Berichte geschrieben werden, wo Maßnahmen drinnen stehen, die mit dem Incident genau gar nichts zu tun haben. So generelle Maßnahmen, die kopieren sie einfach immer weiter und das kommt extrem schlecht an und hilft dem Kunden auch nichts, wenn er jetzt einen Phishing-Vorfall hat und ich empfehle Netzwerksegmentierung – hat mit meinem Incident jetzt nichts zu tun. Ist zwar nette generelle Empfehlung, aber hat in meiner Welt in einem Incident Response Bericht nichts verloren, sondern wir konzentrieren uns wirklich darauf, und auch das wieder gemappt auf MITRE, deswegen bin ich da auch so ein Fan davon, die Angriffsvektoren, die wir erkennen, zu denen formulieren wir Maßnahmenempfehlungen, wo wir sagen, mit diesen Maßnahmenempfehlungen hätte man diesen Angriff verhindern können und nicht, ja wäre gut, wenn die Sekretärin keinen Adminuser hätte, obwohl die gar nicht involviert war.

CE: Das heißt, ihr habt aber schon jemanden, der bei dem Incident overall koordiniert und auch die, die Kundenschnittstelle und Ähnliches sind, aber das ist halt immer jemand, oder gibt es das überhaupt nicht, dass einer im Lead ist?

AP: Na ja, das schon, also es ist immer einer im Lead und es kommt drauf an, wie groß das Ganze ist, ob dann mehr Leute mitarbeiten oder ob das jemand alleine macht. Und bei ganz großen Sachen ist es auch so, dass wir dann teilweise zusätzliche Funktionen dazunehmen, die normalerweise jetzt nicht dabei sein, also zum Beispiel, wenn wir jetzt da einen großen Managed Service Kunden haben und da gibt es einen Vorfall, dann würden wir zum Beispiel den SDM als den Kunden-Koordinator natürlich dazu nehmen.

CE: Der SDM ist der Service Delivery Manager?

AP: Service Delivery Manager genau, der würde dann zum Beispiel dieses ganze Beziehungsmanagement machen, diese Updates übernehmen, das Sprachrohr zum Kunden sein, während dann im Hintergrund der Incident Responder arbeitet und natürlich die Dinge aufbereitet. Also das ist ziemlich anlassbezogen, also ich bin der Meinung, so wie fast überall im Leben, es muss nur so komplex wie nötig sein und so wenig komplex wie möglich. Das heißt, je weniger Leute notwendig sind, desto besser, aber wenn es notwendig sind, dann sollten wir es schon dazunehmen.

CE: Du hast doch gerade schon was von Ausbildungen gesagt, die ihr euren Mitarbeitern in dem Bereich

dann zukommen lässt. Gibt es da Zertifizierungen oder sonstige irgendwelche externen Ausbildungen? Abgesehen von euren internen Weiterbildungen, wo du sagst, die sind sinnvoll, die verfolgen irgendein sinnvolles Ziel oder wo du sagst, der Anbieter ist besonders gut, weil ist es eigentlich egal, welchen Anbieter ich nehme, Hauptsache ich habe das System und die Denkweise verstanden.

AP: Ich kenn natürlich jetzt nicht alle Anbieter, die es gibt. Wir haben für Incident Response natürlich SANS, wie viele. Also vor allem der FOR-508 für Windows Forensik ist quasi Industriestandard. Es gibt sicher andere, die das ähnlich gut transportieren. Ich weiß es aber ehrlich gesagt nicht. Aber ich könnte mir schon vorstellen, wenn man sich so die Vorlesungen zum Beispiel auf der FH derzeit anschaut, sind viele Inhalte da natürlich übernommen worden aus diesen SANS-Geschichten, von dem her, das passt schon. Was immer mehr wird und wo wir vor ein, zwei Jahren angefangen haben auch Zertifizierungen und Kurse zu machen, ist Cloud Forensic, also Azure und AWS. Das seh ich gerade in Österreich, im deutschsprachigen Raum Azure und AWS beide relativ wichtig, fast jeder Kunde ist mittlerweile in der Microsoft Cloud in irgendeiner Form mit Office 365 und du hast gefühlt über 50% Fälle, wo du in der Cloud deine Daten besorgen musst. Also da haben wir Invictus Incident Response. Das ist ein Instruktor bei der SANS, der hat eine eigene Firma gemacht, der bietet da so Cloud Incident Response-Kurse an, die sind recht gut und auch ein bisschen günstiger als von SANS, daher nehmen wir die. Und grundsätzlich so die „Grundausbildung“ ist bei uns Offensive Security der SOC200. Das ist natürlich immer ein bisschen überlappend; was tut ein Security Analyst, was tut ein Incident Responder? Von dem her bringt das auch immer viel. Das sind so die drei Hauptsachen, die wir immer extern machen.

CE: Das heißt aber für dich ist jetzt für einen Incident Responder ein Hochschulstudium kein Muss oder würdest du sagen, das bildet so grundlagenmäßig aus, dass er das schon haben sollte?

AP: Nein, ist kein Muss. Also ich hab ehrlicherweise niemanden, der es nicht hat, aber es wär für mich jetzt kein Muss, dass ich sag, ich stell nur jemanden ein, der eine Hochschule besucht hat. Ich glaube, es gibt durchaus Leute, die über andere Wege in die Security reinkommen, also wir haben auch hier ein bisschen einen anderen Weg gewählt wie andere Marktbegleiter. Wir bilden auch Leute aus, die kein IT-Security-Studium haben im SOC. Wir haben jetzt mittlerweile schon einige, die über einen anderen Weg reingekommen sind. Ich bin der Meinung oder wir merken auch, dass auch immer mehr Softwareentwicklungs-Know-How notwendig ist in einem SOC, vor allem, wenn ich so Richtung Use Case Design und so weiter und so fort denke. Das heißt, eine Person, die schon einige Zeit in der IT ist, vielleicht auch schon viel mit Softwareentwicklung gemacht hat oder die grundlegend viel Know-How hat, wie Operating Systems, Netzwerk und so weiter und sofort funktionieren, ein sehr breites im besten Fall, den kann man schon dazu ausbilden. Ich glaub nicht, dass es ein Muss ist, dass man vorher auf einer Hochschule war, aber es ist halt viel leichter.

Gerade, wenn jemand im Studium ein bisschen gepentestet hat, ein bisschen Analyseerfahrung gekriegt hat, vielleicht eine Incident Response Vorlesung genossen hat, dann ist natürlich viel, viel leichter. Da kann man sofort zum Beispiel den SANS-Kurs drauf packen und die Person ist relativ schnell ready, dass er beim Kunden Incident Response macht. Wenn ich jemanden habe, der in der IT Quereinsteiger ist, dann braucht es wahrscheinlich schon so 2, 3, 4 Jahre, bis der so weit ist, dass er das machen kann.

CE: Dann sind wir schon im vorletzten Block, jetzt soll es wirklich ausschließlich um organisatorische Anforderungen gehen. Jetzt sind wir im NICE Framework, also in den Tasks, dem Knowledge und den Skills. Wir fangen einfach einmal mit den Tasks an und ich stelle die Frage jetzt absichtlich sehr offen, welche Aufgaben also welche Tasks übernehmen die Mitarbeiter im organisatorischen Bereich im Incident Response?

AP: Was ist der organisatorische Bereich?

CE: Der organisatorische Bereich ist für mich in dem Fall jetzt alles, was nicht aktive Analyse und Forensik ist. Also nicht Log-Auswertung, ein System forensisch anschauen, Images ziehen oder sowas.

AP: Also im Incident Response Bereich sag ich einmal sind primär die organisatorischen Aufgaben, dass sie sicherstellen, dass ihre Zeiten aufgezeichnet sind, also das es ein Billing gibt dahinter. In diesem Bereich ist es wichtig, dass man ein Zeitmanagement hat und seine Stunden, die man aufwendet, da irgendwann zur Verrechnung bringt. Das heißt, bei uns ist es wirklich die Verantwortung vom Incent Responder, dass er alle Zeiten, die er verwendet hat, gebucht hat, dass er sein Ticketing dann schließt und dass das dann auch bei uns weitergeleitet wird zur Verrechnung. Die wissen, mit was für einem Stundensatz und was für einem Stundenartikel das verrechnet werden muss. Auch auf die Kommunikation mit dem Vertrieb, bei uns passiert es oft, das Kunden reinkommen, die keine SOC-Kunden sind, die brauchen Hilfe. Meistens ist es der Vertriebler, der uns dann kontaktiert. Und die Incident Responder müssen da mit dem Vertriebler kommunizieren und sagen du, dies ist die Leistung, so schaut es aus, so und so viel schätzen wir. Das heißt, Stundenabschätzung, Aufwandsabschätzungen abgeben, einschätzen können, wieviel Zeit werde ich brauchen, damit ich einen Fall so wie er mir da beschrieben worden, ist abwickeln kann? Und der zweite Punkt, der wichtig ist, ist einfach so ein bisschen diese Koordination also, dass ich selbstständig in der Lage bin, wenn ich einen Kunden habe und bei dem Incident Response mache, dass ich mit ihm eine Timeline ausmache. Dass ich sag, wir starten jetzt einmal und wir machen alle zwei Tage oder jeden Tag oder wann auch immer um die Uhrzeit einen Update Call. Muss diese Information aufbereiten, muss sie transportieren und muss einfach diese koordinative Tätigkeit mit dem Kunden selbständig wahrnehmen.

CE: Das heißt, diese Aufgaben, die wir jetzt gerade gerade besprochen haben, in welchem Setting finden die statt? Das heißt, wie groß sind die Teams, die gleichzeitig an der gleichen Aufgabe arbeiten? Wieviel Zeit

habe ich dafür? Habe ich da Zeitdruck? Das ist natürlich von Fall zu Fall unterschiedlich, aber wie schnell muss das umgesetzt sein?

AP: Ich würd sagen, Zeitdruck gibt es natürlich im Incident Response-Bereich. Es muss relativ rasch gehen von der Anfrage bis zur Zusage, dass man das jetzt tun kann oder dass wir den Fall jetzt wahrnehmen oder wenn wir ihn nicht wahrnehmen, sagen, wann wir es wahrnehmen können beziehungsweise sagen, wir würden es nicht machen, aber wir haben einen Partner, der es macht. Da haben wir wirklich einen Zeitdruck und bei der Abwicklung natürlich kommt es darauf an, aber in den meisten Fällen hat man natürlich auch einen gewissen Zeitdruck, weil der Kunde will natürlich nicht länger offline sein, oder die manchmal stehen Produktionen. Das darf natürlich nicht unnötig lange dauern. Das heißt, du hast immer einen Zeitdruck dabei. Also du musst aus meiner Sicht schon Resilienz haben, dass du in einer stressigen Situation unter Druck ruhig bleibst, diese Ruhe dem Kunden vermittelst und hier sozusagen der Stein in der Brandung bist, der hilft, seinen Notfall top zu bewältigen.

CE: Und von der Teamgröße her, macht ihr das alleine oder arbeitet man auch auch zu mehrt?

AP: Zumindest meistens alleine. Ich sag einmal 80% alleine und in den anderen Fällen entweder zu zweit oder zu dritt. Es ist immer schwierig zu sagen, also die eigene Arbeit alleine und natürlich brauchst du für den Incident Response-Fall immer Leute, die dir zuarbeiten. Irgendein Kollege, der irgendwas konfigurieren muss oder beim Kunden jemand, der etwas konfigurieren muss, weil du das brauchst. Also Zuarbeiter hast du immer, aber du erbringst deine Leistung meistens alleine selbstverantwortlich.

CE: Wenn wir jetzt uns wieder vorstellen, es kommt jemand, der relativ frisch im Incident Response Bereich ist. Was sind da Aufgaben, die du dem auch ohne viel Berufserfahrung in dem Bereich geben kannst? Was ist wieder das bare minimum, welche Aufgaben muss der erfüllen können und was wäre wieder darüber hinausgehend wünschenswert?

AP: Also ich glaub ehrlich gesagt, dass du jemandem, der nur keine Erfahrung hat wenig geben kannst, das der selbständig umsetzt. Ich glaube, es ist, wenn dann ein dabei sein und nach ein bisschen dabei sein, wenn das technische Know-How da ist, kann man natürlich sagen, weiß ich nicht, ich habe jetzt 20 Maschinen triagiert und die gehören jetzt angeschaut, dass du sagst, mach da zwei davon und erzähl mir, was du gefunden hast. Aber da braucht man halt auch schon diese technische Erfahrung. Wenn die technische Erfahrung da ist, dann kann man sicher Zuarbeiten und machen, also Analyse an den Kollegen weitergeben. Wenn die Erfahrung noch nicht da ist, dann würde ich sagen ist es eher ein Dabeisein und Mitlernen. Und eher ein Aufwand für den, der ihn dabei hat, ohne dass er da großartige Unterstützung ist.

CE: Im Bereich Knowledge, in dem wir jetzt schon ein bisschen angekommen sind, lautet die erste Frage: Über welchen theoretischen Background müssen die Mitarbeiter verfügen? Und wie detailliert natürlich?

Als Beispiel nehm ich jetzt einfach mal diese Incident Response Phasen nach ISO 27035 oder NIST SP 800-61. Ist das was, wo du sagst, na ja, da muss man vielleicht Phasen auflisten können, oder die muss man beschreiben, erklären können, anwenden, planen, vergleichen, differenzieren, bewerten, entwerfen? Wo würdest du ungefähr dieses Backgroundwisssen verorten?

AP: Also die NIST ist schon gut. Also ich würd jetzt vor keinem erwarten, dass er mir das jetzt aus dem Gedächtnis aufsagt oder beschreibt, wie das funktioniert. Ich bin der Meinung, solche Standards sind da, damit man sie anwendet, indem man sie liest, versteht und anwendet, nicht, dass man sie auswendig kann. Ich bin eher der Meinung, diese Dinge zu verstehen und in die praktische Tat umzusetzen ist das, was wichtig ist. Ich glaub, eben die NIST ist gut, das gepaart mit Killchain bzw. MITRE-Framework, das wären so die theoretischen Grundlagen, die ich wichtig fände.

CE: Gibt gibt es irgendwelche Schlagwörter, Begriffe, bei denen du sagst, die sollte man unbedingt schon einmal schon einmal gehört haben, oder irgendwas Spezifisches, wo du sagst, das Konzept solltest du zumindest schon einmal gehört haben?

AP: Na ja, ich mach es mir jetzt einfach. In Wirklichkeit alle gängigen Techniken und Taktiken aus der MITRE, das ist für mich das Um und Auf, also das muss jeder kennen, verstehen, inhalieren. Wenn ich jemanden um zwei in der Früh aufwecke, muss er wissen, wo in der Registry suchst du danach, dann muss er wissen, was sind die Orte. Also jetzt vielleicht nicht alle ja, aber zumindest die gängigsten. Das ist wichtig, das musst du wissen, weil wenn du in der Analyse bist, dann die ganze Zeit irgendwo nachzuschauen, das funktioniert nicht, also das den theoretischen Background brauchst du auf jeden Fall.

CE: Womit wir bei den Skills angekommen wären. Du hast vorher schon Resilienz ein bisschen gesagt, weil es ein bisschen stressig ist. Welche anderen Social Skills wären dir wichtig In dem Bereich Incident Response?

AP: Managementtaugliche Kommunikation, Resilienz und so ein bisschen diese Gesprächsführung. Die managementtaugliche Kommunikation hab ich sehr gemeint im Bericht, also in Schrift, aber auch wie führe ich so ein Meeting in einer Krisensituation. Also ich stell mir vor, die Produktion steht, jede Minute kostet 100000€ und ich hocke jetzt mit dem Geschäftsführer im Meeting und erklär ihm, dass wir noch drei Tage lang warten müssen, bis das wieder online geht. Also solche Gespräche zu führen, das mal zu üben und zu versuchen sich in solche Lagen zu versetzen - ich glaub schon, dass das was bringt.

CE: Perfekt, vielen Dank, da sind wir jetzt schon in der letzten Phase angekommen. Unabhängig von dem, was wir bisher gesagt haben, was sind deiner Meinung nach so zentrale Punkte, die wir später dann in der Vorlesung transportieren müssen? Von Vorbereitungen, die du gerade schon gesagt hast, vielleicht sind so Sachen wie Playbooks ein Thema oder ist das überhaupt nicht wichtig?

AP: Ich glaub schon wichtig wäre, auf jeden Fall so Setup einmal zu machen, also wie kann ich on scale mir technisch diese Informationen holen, keine Ahnung. Eine Velo aufbauen und einmal probieren das über die Cloud zu deployen auf 10 Maschinen oder was auch immer. Und dann quasi ja wirklich Artefakte sich zu holen oder auch Angriffe zu simulieren, zu schauen in welcher Phase würde ich jetzt was sehen? Solche Dinge glaube ich, wären auf jeden Fall gescheit in einer Übung. Beziehungsweise, was meiner Meinung nach auch immer ein bisschen ignoriert wird, ist das Zusammenspiel, also zum Beispiel bei einer Mandiant, wenn die Incident Response machen, dann gibt es natürlich unterschiedlichste Rollen, die haben einen Koordinator, die haben Analysen, die haben ein eigenes Malware-Analyse-Team und da ist es ganz klar, wenn ich im Incident Response vorher irgendwo Malware finde, dann wird die natürlich weitergeben. Das wird analysiert, blablabla. Das ist natürlich in Österreich ein bisschen schwieriger. Du hast diese ganzen Leute nicht, meistens ist das nicht so aufgestellt. Aber wirklich jetzt einmal so einen Angriff durchzuspielen in einer Übung, um zu sagen, ich simuliere das jetzt und ich habe von dem Scoping-Gespräch bis zur Analyse bis zur Malware, die ich vielleicht irgendwo find, dass ich die Malware vielleicht da dann irgendwann zumindest bis zu einem gewissen Grad untersuche und dann irgendwo auch die Exfiltration nachvollziehen kann, ja, weil, weiß ich nicht, in dem Binary steht das Passwort zum FTP-Server drin, solche Sachen, also so eine schöne Angriffskette einfach wirklich einmal zu simulieren. Und die Studenten reinzuschmeißen und zu sagen „Wir haben gesehen auf dem Storage, da ist das Backup gelöscht worden und weiß auch nicht, also Ransomware - was ist da passiert? Und sie müssen wirklich die gesamte Angriffskette nachvollziehen und diesen analytischen Prozess anwenden. Das wäre das wäre sicher eine geile Geschichte ja, weil du vorher auch von Cyberrange geredet hast.

CE: Das wäre nämlich schon der zweite Punkt. Was wären zentrale Punkte, die wir jetzt nicht in der Theorie vorher in den Vorlesungen und im Ausprobieren, sondern wirklich in so einer zusammenhängenden Übung beachten sollen, bei der bei der Konzeption? Wie gesagt, Stichworte Zeit, vielleicht auf einmal ein unerwarteter Kundentermin, regelmäßige Lagebildupdates, Berichterstattung, Zwischenbericht oder Abschlussbericht schreiben?

AP: Ja, also mir wär wichtig, dass es realitätsnahes Beispiel ist. Das ist sehr schwierig, also du hast das selbst gesehen, bei unserer Übung. So einen Angriff zu simulieren, wie er in der echten Welt ist, ist gar nicht so einfach. Also ich glaube, das wäre sehr wichtig. Was ich auf jeden Fall nicht machen würde, ist irgendeine Form von fertiges Caldera-Playbook oder sowas ausführen. Das ist ausgelutscht, da hat eh schon jeder die Lösung und irgendwelche Artefakte drin und man kann eh nachlesen, wie der Angriff funktioniert, sondern wirklich irgendwas Realitätsnahes zu simulieren. Wirklich das Verhalten zu kopieren, wie Angriff wirklich ausschauen könnte. Das wäre sehr sinnvoll. Und wie gesagt, es gepaart mit jemandem, der auch einen

Kunden spielt und ich würd‘s wirklich so aufsetzen, ned irgendwie von Montag bis Freitag und das rennt die ganze Zeit, sondern wirklich auch simulieren, dass ich teilweise warten muss, was ja oft die Schwierigkeit ist, ja, du kommst zu so einem Fall hin, du hast mal das Scoping gemacht und sagst „Wir müssen uns diese 10 Maschinen anschauen“, da hast du den Agent, roll den aus und dann hast du vielleicht an dem einen Tag einmal 3, 4, 5, die letzten fehlen noch, du fängst mal an zu analysieren, verrennst dich vielleicht irgendwo und musst es wieder verwerfen, dann am nächsten Tag kommen die nächsten 3, 4 Maschinen dazu, also wirklich eine realitätsnahe Simulation, wo du nicht von Anfang an alle Informationen zur Verfügung hast. Ich glaub, dass das durchaus sehr lehrreich wäre, dass du gewisse Sachen erst nachher siehst oder später siehst oder dir keiner sagt. Ein Kunde, der dir dann Blödsinn erzählt, solche Sachen. Also vor allem der Kunde, der Blödsinn erzählt, finde ich, wäre auf jeden Fall eine wichtige Lektion, die man gleich mitgeben könnte, so quasi so, verlass dich nie auf das, was da der Kunde erzählt. Vertraue, aber kontrolliere, sagen wir es einmal so.

CE: Also ein ganz einfaches Beispiel, du kriegst ein Infrastrukturdiagramm, das aber leider jetzt schon zwei Jahre alt ist und wo sich leider keiner mehr drum gekümmert hat?

AP: Genau, wo vielleicht auch das Datum oben steht und dann können sie das vielleicht eh schon sehen, dass es vielleicht schon 5 Jahre alt ist. Oder der Phishing Link, auf den man zwar draufgeklickt hat, aber wo die Sekretärin sagt, sie hat ihr Passwort nicht eingegeben, solche Sachen. Ein Beispiel: Wir haben bei einem Kunden den Patient Zero gefunden, bei dem der Kunde der Meinung war, den gibt es gar nicht. Also es war irgendeine Admin Test Maschine für Admin Test, die schon seit 3 Jahren nicht mehr aufgedreht sein sollte, die aber gelaufen ist, wo natürlich dann kein Agent ausgebracht worden ist, weil natürlich hat ja keiner mehr gewusst, dass der existiert. Also solche Sachen, incomplete Information in so einer Übung, das ist sicher sehr, sehr viel Aufwand, aber ich glaube, das war auf jeden Fall eine coole Geschichte und sie würden sich voll aufregen darüber natürlich, aber das ist die Realität.

CE: Berichterstattung weil du das vorher auch angesprochen hast, dass das ein Skill wäre, den du dir wünschen würdest, inwieweit wär das wichtig?

AP: Ja, absolut ja. Ich glaub, man sollte es auf jeden Fall vorher einmal schon auch zeigen, wie macht man das gescheit? Und dann, nach der Übung, natürlich das Ganze in einem Bericht zusammenzufassen, wo sie managementtaugliche Aufbereitung haben, einen technischen Teil, IOCs, Timeline, also alle diese Sachen, die auch dazu gehören. Auf jeden Fall! Würde ich auf jeden Fall machen. Gerade, was ich glaube, was auch gut ist als Inhalt, wenn man sagt, wie baue ich eine Incident Response Timeline auf und wie kann ich diese Timeline dann auch in meinem Bericht nachvollziehbar machen? Weil gewisse Dinge werd ich weglassen müssen, ich kann nicht jedes Detail reinnehmen, aber wichtige Dinge schon.

CE: Sehr gut, dann sind wir jetzt am am Ende meiner meiner Frageliste angekommen, vielen Dank!

B.3. Interview am 08.04.2025 mit Utz Nisslmueller, MSc (Mitarbeiter WienCERT, Magistratsabteilung 01, Stadt Wien)

CE: Vielen, vielen Dank nochmal, ich starte gleich einmal mit der ersten Frage du bist ja im WienCERT tätig. Wie kann man sich das grob vorstellen? Was macht ihr, was sind eure Aufgaben?

UN: Wir sind eigentlich die zentrale Anlaufstelle für generell Security bei der Stadt Wien. Da hilft es vielleicht ein bisschen, die Struktur zu verstehen, wie die Stadt Wien aufgebaut ist. Wir setzen uns zusammen aus den ganzen Magistratsabteilungen, also MA01 das sind wir, Wien digital, und wir sind der IT-Dienstleister für alle anderen Magistratsabteilungen von 02 bis 70. Für alle anderen Entitäten der Stadt Wien, also die Schulen, die Kindergärten - ist eine eigene MA - auch ganz, ganz groß bei uns sind alle Krankenhäuser, also das AKH und auch die ganzen anderen Kliniken in Wien, fallen quasi unter unsere Obhut aus Security Sicht. Wir sind sowohl das Blue Team als auch das Red Team. Ich bin jetzt auf der Blue Team-Seite, also ich bin für Angriffserkennung und Behandlung zuständig bei WienCERT. Die anderen Kollegen machen ein bisschen was von allem, also die unterstützen die AD-Admins beim Härten. Externe Applikationspentests machen sie nicht, das macht ein Externer, aber wenn sie Zeit haben, dann hunten sie zum Beispiel im Netzwerk, schauen „Ah okay. Diese interne Applikation hat Schwachstellen“, gehen ihnen nach, schreiben Reports und unterstützen einfach generell alle IT-Abteilungen, die hier so an der Stadt Wien werkeln in Security Fragen. Das mal generell. Wir haben natürlich auch ein SIEM, das aus Logquellen gefüttert wird, wo Alerts hineinkommen, und die arbeiten wir auch ab anhand von Playbooks und dann, wenn es über das Playbook hinaus geht von der Komplexität her, auch individuell. Bei uns ist das so geregelt, wir sind ein eher kleineres Team, [Interviewabschnitt entfernt]. Genau das ist so grob unser Doing würde ich mal sagen.

CE: Das heißt auch außerhalb von Sicherheitsvorfällen seid ihr dann natürlich tätig mit diesem Team und macht halt dann einfach schon proaktiv was, bevor es reaktiv was zu tun gibt.

UN: Genau, ja.

CE: OK, das heißt, ihr seid wirklich Dienstleister für alles, was die Stadt Wien quasi hat, und ihr habt aber sonst keine außenstehenden Entitäten, die irgendwie betreut, also ihr macht das wirklich nur für alle Subentitäten, sag ich mal, der Stadt Wien selber.

UN: Jawoll.

CE: Und seid ihr da auch projektmäßig irgendwie drinnen, also wenn jetzt irgendwer was umsetzen möchte und da gern euer Security Know-How haben will, auch in auch in der Richtung?

UN: Ja absolut, also wir sind quasi auch die internen Security Consultants sozusagen. Ein Beispiel, das ich

dir nennen kann, ist Ausrollung von Privileged Access Management, was wir letztes Jahr abgeschlossen haben. Wenn es da Fragen dazu gibt, weil das hat natürlich viele unserer Workflows durcheinander gebracht und wir haben noch ein wöchentliches Jour Fix zu diesem Privileged Access Management, wo auch einer ein Kollege immer vom WienCERT dabeisitzt für Securityfragen und Einschätzungen. Also im Operativen sind wir auch manchmal mit eingebunden, je nachdem, wo es Sinn macht und wo nicht, zum Beispiel – ganz grobes Thema jetzt – Firewallfreischaltungen: Wir haben hier einen Automatismus, wenn gewisse Ports angefordert werden, die securityrelevant sind, dann müssen wir hier immer ein Auge drauf werfen und vorher sagen ja/nein, bevor das die Kollegen vom Netzwerk dann tatsächlich implementieren auf der Firewall. Und auch so Sachen, die eigentlich bei den Proxy-Leuten liegen, so Proxyfreischaltungen, MIME-type-Filterausnahmen, solche Sachen, schauen wir auch immer drüber. Also wir sind da schon relativ stark ins operative Doing auch eingebunden.

CE: [Interviewabschnitt entfernt] oder habt ihr dann auch noch weitere Kräfte, auf die ihr zurückgreifen könnt, wenn jetzt mal, sag ich, wirklich wie man auf Englisch so schön sagt: Shit hits the fan?

UN: Wenn shit hits the fan, machen wir es selber. Wir haben Externe, aber die machen bei uns nur die Pentests, weil pentesten, du weißt, pentesten und auditen muss immer ein Externer, also sich selbst prüfen ist halt immer so eine schöne Sache, die man nicht darf, ne? Und wir haben auch [Interviewabschnitt entfernt] externe Mitarbeiter, die uns bei den lästigen operativen Sachen unterstützen, dass wir quasi wirklich mehr die Sicht auf die essenziellen Dinge haben, aber wenn shit hits the fan, dann sind wir Hands on Deck, intern. [Interviewabschnitt entfernt]

CE: Verstehe, das klingt ja schon mal sehr spannend und herausfordernd eigentlich, für die Riesen-IT, die ihr da habt.

UN: Aber wir haben Gott sei Dank also, seitdem ich da bin – ich bin seit Anfang Oktober da. Vielleicht bisschen Hintergrund zu mir: Ich war davor ein paar Jahre in England, ich habe im Security Consulting gearbeitet, war im Bereich Purple Teaming vermehrt unterwegs und seitdem ich da bin, gab es eigentlich ein paar kleinere Incidents, die wir aber alle relativ schnell und relativ gut unter Kontrolle bekommen haben. Eben auch, und das attribuiere ich eigentlich auch an die auf die langjährige Vorarbeit meiner Kollegen, die hier wirklich den Admins, den Server- und Applikationsadmins im Nacken sitzen, dass sie ihre Sachen gescheit härten.

CE: Gut, vielen, vielen, lieben Dank. Damit sind wir jetzt auch schon mit unserem Organisation und Umfeld Verstehen fertig. Ich glaube, ich habe jetzt schon einen ganz, ganz guten Überblick. Dann kommen wir jetzt gleich zum nächsten Part: Anforderungen, wirklich diese allgemeinen Anforderungen, an eure Mitarbeiter im CERT Verstehen. Da darfst du jetzt wirklich alles nennen, von forensisch bis organisatorisch darf da jetzt

wirklich alles, alles dabei sein. Jetzt überlegen wir uns einfach mal und stellen uns vor, wir haben jemanden, der kommt von der Fachhochschule und sagt: Incident Response, das habe ich gelernt. Was erhofft ihr euch von dem, was der jetzt kann? Und vielleicht auf der anderen Seite, was erwartet ihr euch, also was muss der jetzt wirklich können? Was ist da jetzt wirklich das bare Minimum, dass man nicht enttäuscht ist von dem?

UN: Ich würde es einmal auf mehrere Schienen aufgliedern, also wirklich was IT Security angeht, würde ich mir wünschen, dass diese Person in Windows echt gut ist. Ist halt die Frage, was kann man von einem Studenten erwarten? Ich schließ dann immer so ein bisschen auf mich, wie ich nach der Uni dabei war. Das war nicht so gut, muss ich gestehen. Ist die Frage, willst du jetzt eine Wunschliste von mir oder was ich mir realistisch erwarten würde?

CE: Gerne, wir können das ja gerne so machen, was erwartest du dir realistisch? Und auch gerne danach, was wünscht du dir, also was wäre wirklich cool, wenn der könnte?

UN: Realistisch hätte ich sehr gerne ein solides Grundverständnis, was IT angeht. Ich hätte gern, dass die Person einen Kurs Betriebssysteme gehabt hat, dass die Personen einen Kurs gehabt hat zu Netzwerk, wie funktioniert ein Netzwerk auf einer technischen Basis. Was ich finde, dass auf der Uni extrem fehlt – und ich weiß jetzt nicht, ob das so relevant ist für Incident Response, aber generell in IT, dass die Leute auch einen Kurs haben, wo Enterprise IT bisschen beschrieben wird, weil du kommst halt von der Uni und du weißt halt: Da gibt es das ISO/OSI-Modell und die Packets fließen so und so, syn-syn/ack-ack, bla bla, aber Leute haben überhaupt keine Ahnung, was ein Reverse Proxy ist und wie der funktioniert. Was ist ein Load Balancer und wie funktioniert der? Das war bei mir genauso, nachdem. Ich bin mit diesem System in Kontakt gekommen und war so: Okay und wie funktioniert das also? Es wäre cool, wenn die Leute wissen: Wie ist eigentlich der Flow? Also diese User Stories, wenn du jetzt quasi denkst, von außen nach innen auf den Servern. Wie funktioniert dieser Flow von A nach B wirklich und welche Systeme sind da dazwischengeschaltet und was ist so normal in einer Enterprise Architektur. Das würde ich mir auf einer grundlegenden Ebene wünschen. Dann, Studiengang Incident Response, ich würde gern von der Person fordern, dass sie circa so die Logquellen in einem Enterprise Umfeld so runter rattern kann, quasi also Windows Logs. Wo finde ich die Windows Logs, auf was für einer Ebene spielen sich die ab? Sind das eigentlich Applikationslogs, oder Unterschied auch: Windows Event Logs – Sysmon, vielleicht auch ein Third Party Agent, Linux Logs natürlich auch, was da überhaupt geloggt wird oder dass die Logging-Umgebung zwischen Linux und Windows ist ja doch relativ distinkt. Da ist halt immer das Lizenzproblem, wenn man damit nicht herumspielen kann, aber dass die Leute auch ein bisschen eine Ahnung haben von Network Logs: Wo kann ich meine Network Logs überhaupt erheben? Also Firewalls, Proxys, VPN- Gateways und so weiter. Das muss nicht im Detail da sein, aber zumindest mal ein Verständnis und zumindest mal im Hinterkopf haben für

Problemlösungsansätze. Das wäre es auf der technischen Schiene. Organisatorisch – gut, das ist halt auch wieder ein Klassiker –, aber Kommunikation, finde ich, ist auch ein bisschen vernachlässigt in der Security. Vor allem auch als Incident Responder bist du dann ja oft, wenn halt ein Incident passiert ist, bist du mit Leuten konfrontiert, die sich entweder nicht mit Security auskennen, die ein bisschen Angst haben vor dir und generell überfordert sind mit der Situation, und das muss man halt auch sanft, aber dennoch bestimmt und gut handeln können. Da ist dann die Frage: Kann man das direkt nach der Uni oder lernt man das mit Lebenserfahrung? Aber ich finde, wenn die Person einen Kurs hätte, quasi wie kommuniziere ich in einer Art und Weise, die dem Gegenüber quasi das Gefühl gibt, dass er oder sie mir vertrauen kann und da ein bisschen einfach die Friktion rauszunehmen, das wäre, finde ich, auch sehr hilfreich. Und vor allem natürlich auch intern die Kommunikation mit dem Team, weil als Incident Responder agierst du ja nicht selber. Wenn du wirklich dezidiert Incident Responder bist, dann kriegst du den Ping vom Blue Team und musst dann mit den internen Teams, auch also mit den Server Admins und so, auf einer technischeren Ebene sprechen. Dass du da dann einfach einen guten, wie soll ich sagen, Kommunikationschannel hast, dass du einfach immer Rückmeldungen gibst und da auch verlässlich bist, was das angeht.

CE: Also gerade diese Kommunikation, du bist jetzt mein drittes von vier Interviews in dem Bereich, das haben alle genannt und haben alle gesagt, dass das viel zu kurz kommt auf der Uni. Das wird sicher Berücksichtigung finden, das weiß ich eigentlich, glaub ich, jetzt schon.

UN: Ja, jetzt generell Kommunikation, oder?

CE: Also insbesondere immer so stakeholder-spezifische Kommunikation, auch von einem Incident Response Anbieter, mit dem ich gesprochen hab, der gesagt, er hat schon ganz tolle Techniker gehabt, aber wenn der dann doch mal irgendeinem Firmenchef erklären muss, dem hunderttausend Euro pro Minute durch die Lappen gehen: Wir müssen das Ding schon noch drei Tage abgedreht lassen, dann muss man das halt irgendwie rüberbringen.

UN: Ich überleg nur grad, wieder spezifisch Incident Responder. Vor allem, ich glaub, das ist auch relevant für Incident Responder, ist, dass man auch – das kann man schwer einen Lehrgang packen, aber ich sag dir jetzt wieder, was ich mir generell persönlich und charakterlich wünschen würde von der Person – dass du eine Awareness hast, was Rabbit Holes sind und dass du dich jetzt nicht fünf Stunden wo verrennst und währenddessen alles andere vergisst, nur weil du quasi diesem Trail of Bits quasi im Logmanagementsystem folgst, sondern dass du immer re-evaluierst: Ist das, was ich gerade mache, am Zielführendsten, dass ich den Incident am besten und am schnellsten abarbeite? Dann machst du wieder zehn/20 Minuten, dann: Bin ich immer noch auf der richtigen Spur? Das ist, glaube ich, was, auch vielen Leuten fehlt, vor allem denen, die wirklich tief technisch drin sind im Verständnis. Das wäre auch ganz, ganz, ganz wichtig, finde ich von

meiner Seite.

CE: Bestes Beispiel: Nämlich genau bei dieser Übung, die wir schon gemacht haben in Forensik, da haben dann Leute angefangen, eine Ransomware, die wir extra entwickelt haben, reverse zu engineeren. Die war auch dafür gemacht und am Ende des Tages haben uns die Lösungswege präsentiert, wo wir alle dagesessen sind und uns gedacht haben so: Okay, es wäre auch viel einfacher gegangen. Wie du sagst, ich glaube, das fehlt wirklich einfach und was wir da auch gemerkt haben, ist dass...

UN: Ich weiß nicht, ob du es kennst, dieser OODA-Loop, die da oft quasi erwähnt wird. Also wenn man einfach solche Frameworks einfach mal kurz erwähnt, so hey, das gibt so das ist eigentlich nicht nur blödsinniger theoretischer Schwachsinn, sondern das vielleicht auch anhand eines Incidents, eines hypothetischen, durchgehe, so okay OODA: Ich observe hier das, ich orientiere mich, ich decide, was ich mache, ich acte und dann mache ich wieder diesen Loop durch und durch bis ich zum Ende komme. Das wäre vielleicht ganz praktisch.

CE: Was wir auch bemerkt haben bei der Übung, war, dass ganz viel dieses Grundsatzverständnis fehlt. Als Beispiel: Ich finde auf einem Client eine Malware, und ich finde nachher auf einem Fileserver die gleiche Malware und was uns da einfach aufgefallen ist und was auch einfach so ein bisschen der Anstoß für mich war, warum ich das jetzt als Arbeit mache: Es fehlt einfach die Denkweise: Ok, ich habe da und da die gleiche Malware und es kommt aber nicht der Rückschluss, wie ist die jetzt von A nach B gekommen? Diese Denkweise quasi fehlt, glaube ich, einfach ein bisschen aktuell bei unseren.

UN: Ja, es ist für mich schwierig, weil ich bin halt immer am Scheideweg. Liegt das daran, dass der Studiengang nicht genug vorbereitet oder liegt das daran, dass die Leute alle noch so jung sind? Weißt du, das kann ja auch sein, dass das erst mit der Erfahrung kommt. Das kann ich dir nicht beurteilen.

CE: Danke schön, dann hüpfen wir jetzt einfach zur nächsten Frage. Wenn ihr das Ganze als Stelle ausschreibt, im Bereich Incident Response, im Bereich WienCERT, was steht da in euren Stellenausschreibungen drin? Was sind da so, die Fähigkeiten, die ihr, sag ich mal, verlangt und was wünscht ihr euch vielleicht auch gerne an Personal Skills oder Soft Skills dazu?

UN: [Interviewabschnitt entfernt] Wenn ich jetzt aber aufschreiben müsste für einen Incident Responder in meinem Team, dann würde ich sehr ähnlich verfahren, so wie ich dir vorher gesagt habe, also Kenntnisse von Logquellen und Formaten und wie diese quasi in Tooling eingespeist werden, also Logparsing, generell Logformate, also JSON, CEF und so weiter. Wie diese in Toolings eingespeist werden und wie Alerts quasi generiert werden, überhaupt. Du hast da auch eine Pipepline, die du im Überblick behalten musst und wo kommen meine Alerts überhaupt her? Also so ein Verständnis. Dann würde ich mir wünschen, gut, das nehme ich aber an bei einem Incident Response Posten, dass die Leute zumindest nach NIST SP 800-61

die vier Phasen kennen. Man muss jetzt nicht eine A4-Seite zu jeder Phase sagen können, aber er muss mir nur grob sagen, was wird in welcher Phase wie abgehandelt? Und vielleicht ein Beispiel auch immer geben. Das wär ganz cool. Und sonst noch technisch, einfach die 0815 Sachen reinschreiben, also IT-Verständnis, vielleicht IT-Erfahrung, bei uns – wir sind relativ stark Windows geprägt sowieso wie viele Unternehmen – vielleicht Erfahrung was Windows Loganalysis angeht. Genau und organisatorisch, beziehungsweise auf einer Metaebene auch das, was ich vorher angesprochen habe, also kommunikationsfreudig. Aber das sind eigentlich Sachen, die man eher dann im Interview herausfindet, also reinschreiben würde ich wirklich nur so Basics, Incident Response-Sachen und ich bin eher ein Freund, dass man die Beschreibung grob hält und dann im Interview wirklich mit den Leuten redet.

CE: Wenn wir uns jetzt einen Incident Response Fall vorstellen, ist das bei euch im Team getrennt nach technischen und organisatorisch? Das heißt, sind die einen spezialisiert darauf, das Ganze technisch forensisch zu analysieren und die anderen für Krisenmanagement, Incident Koordination, Lagebild malen und so Geschichten oder seid ihr eigentlich Allrounder und jeder macht halt das, was er gerade dazukommt?

UN: Wir sind Allrounder. Also die technische Analyse, so wie ich vorher erwähnt habe, wir haben den CERT-Kollegen, der halt am jeweiligen Tag die Tickets abarbeitet. [Interviewabschnitt entfernt] die Person, die jeweils an dem Tag zuständig ist, die macht wirklich die technische Analyse und trifft dann auch die technische Decision: Hey, Leute, da ist ein Incident, wo wir alle hin müssen, hey Leute da ist ein Incident, den ich alleine arbeiten kann oder hey Leute, es ist ein false Positive. Das ist dieser Person dann selber überlassen. [Interviewabschnitt entfernt] Und die Kommunikation nach außen. Wir haben einen Teamleiter und der Teamleiter übernimmt dann von uns die Kommunikation nach außen und erfragt von uns Updates, sollte er hier Updates benötigen.

CE: Perfekt danke, du hast gerade schon die NIST erwähnt. Für die gibt es ja keine Zertifizierung, aber sonst kann man sich ja eigentlich wirklich in ziemlich jeden Blödsinn zertifizieren lassen im IT-Bereich. Gibt es da irgendwelche Zertifizierungen, Ausbildungen oder Ähnliches, wo du sagst, die sind sinnvoll? Sowohl einerseits inhaltlich sinnvoll als auch das lest ihr gerne bei Bewerbern oder wie auch immer.

UN: Also ich kenn die Kurse von Hack the Box. Ich weiß jetzt nicht, ob die einen expliziten Incident Response Path haben. Ich weiß, sie haben einen Defensive Analyst Path, kann aber nicht beurteilen, inwiefern sich der überschneidet. Ja natürlich, wenn ich es mir aussuchen könnte, dann hätte der Kandidat zwei bis drei SANS-Zertifizierungen, aber mir ist auch genauso bewusst, dass, wenn du von der FH kommst, das dazahlst nicht und du bist auch deppert, wenn du das selber zahlst, weil das zahlt ja entweder die Firma oder was auch immer. Ja, ich würd's eigentlich schon auf Ausbildung würde ich vielleicht darauf Wert legen, ob die Person so ein Freizeit Lab hat quasi. Beispiel: Ich hatte früher oder habe auch immer noch, aber ich

pfleg es nicht mehr so gut wie früher, einen Docker Container, der zu Hause bei mir am Server, wo Elastic drauf gelaufen ist mit der Security Solution und ich habe von all meinen Devices zu Hause einfach meine Logs forwarded in das Ganze und dadurch Use Cases laufen gehabt. Also wenn die Person sowas hat, ein bisschen was noch darüber erzählen kann, dann wäre das für mich ein Indikator, so hey, entweder du hast Spaß dran, du hast dir dazu Gedanken gemacht oder du machst das quasi, um bei Potential Employers einen guten Eindruck zu machen, was auch für mich ein guter Indikator ist, dass du den Job wirklich möchtest.

CE: Gut, Danke schön, dann sind wir jetzt schon im nächsten Abschnitt angekommen. Wir werden die Arbeit ein bisschen nach dem NIST-Nice Framework bauen und das kennt ja 3 Kategorien ganz grob, nämlich Tasks, Knowledge und Skills. Das heißt, da geht es drum, welche Aufgaben haben meine Mitarbeiter, meine Mitarbeiterinnen, welches Knowledge, also welches Hintergrundwissen, welchen theoretischen Background brauchen Sie dafür und zu guter Letzt welche Skills müssen sie dafür mitbringen? Also da geht es vor allem auch um Social Skills, aber natürlich auch darum, was sollen die so können? Und dann fangen wir gleich einmal mit den Tasks an. Es soll jetzt wirklich eher weniger ums technische, sondern mehr ums organisatorische Drumherum gehen, weil das ja dann auch das Vorlesungsthema sein wird und daher die erste Frage: Welche Aufgaben übernehmen Incident Responder, die ihr ja so nicht habt? Aber wenn sie gerade im Incident arbeiten, sage ich mal, welche organisatorischen Aufgaben werden da übernommen? Auf allen Ebenen.

UN: Organisatorisch, also mal jetzt technisch ganz weglassen, wäre so die Kommunikation mit den betroffenen Parteien. Wie gesagt, wenn es auf einem Windows Server passiert, dann schauen wir, wer ist verantwortlich für diesen Windows Server und dann die Kommunikation erstmal in diese Richtung. Dann die Kommunikation mit den surrounding Kollegen, also mit den Teamleitern von den jeweiligen Gruppen, falls notwendig. Und was ich vorher auch schon erwähnt hab, die Kommunikation nach intern, also, wenn diese Person jetzt zum Beispiel gerade CVT ist, also der CERTler vom Tag und diesen Incident hat, dann erwarte ich mir, dass die Person sich zuerst über überlegt, OK welche von diesen drei Kategorien passt, also fast positive Incident, schaff ich allein oder Incident, schaff ich nicht allein und dann auch wirklich einfach rückmeldet und hier verlässlich ist einfach. Ansonsten organisatorisch: Dokumentation natürlich, auch ein ganz großer Punkt. Das muss jetzt nicht irgendeiner strukturierten Weise erfolgen, aber einfach in einem OneNote mitschreiben und vielleicht auch mit Timestamps, so hey, hier ist mir das aufgefallen und dann einfach dokumentiert, wie die Interaktion abläuft; einfach damit man, falls dieser Incident sich länger zieht und man am Nachmittag wegmuss oder den Incident dann übergibt an die Kollegen, die noch da sind oder die länger Zeit haben, dass die hier einfach den Trail of Evidence und of Actions einfach haben. Das war das zur Kommunikation. Genau und halt auch klassisch wieder Kommunikation einfach, falls man sieht, dass

man Meetings hat an dem Tag, dass man die halt verschiebt oder absagt, sagt, so hey Leute, ich kann heute nicht kommen, dass man einfach seinen, wie soll ich sagen, seinen Wirksamkeitsbereich generell in seinen Tasks im Auge hat und hier auch den jeweiligen Personen Rückmeldung gibt.

CE: Bezüglich Lagedarstellung macht ihr da irgendwas oder ich habe es nämlich auch schon gehört: Wir malen eigentlich kein Lagebild, dann habe ich von dem anderen auch schon gehört: Lagebild ist das größte und das wichtigste und unsere unser Augensternchen quasi. Wie wird das bei euch gehandhabt?

UN: Wir persönlich verfassen kein Lagebild. Wir beziehen Lagebilder von den anderen CERTs in Österreich, [Interviewabschnitt entfernt] Wir sind auch Teil der kritischen Infrastruktur in Österreich und in Wien, also wir bekommen, wenn nötig, auch die Informationen [Interviewabschnitt entfernt], die uns betreffen. Von dem her sehen wir hier nicht wirklich den Need, [Interviewabschnitt entfernt], dass wir unsere Kräfte besser wo einsetzen können.

CE: Lagebild jetzt eher gemeint im Sinne von Lagebild von diesem einen Incident, dass ich mir grafisch aufmale: Ich hab das System betroffen, das macht eine Connection dahin, das System, das System, das System; dass ich das mal ein bisschen grafisch aufmale, macht ihr sowas?

UN: Nein, das hätte ich unter allgemeine Dokumentation eigentlich.

CE: Das heißt das, das macht sie schon, aber jetzt nicht in irgendeinem mega arg ausgereiften, wunderschönen, grafisch dargestellten, sondern einfach, ihr schreibt euch die wichtigsten Facts auf und damit ist es dokumentiert.

UN: Ja.

CE: OK, das heißt, wir haben gerade schon gesagt...

UN: Du entschuldige, falls ich was sage oder deine Frage falsch verstehe, kannst du mich gerne früher unterbrechen, also damit ich keine Zeit da verschwende.

CE: Ja ja, nein, nein, nein, ich nehm das gerne alles auf. Ich hab das vorher auch schon mal bei einem anderen Interview gehabt, da waren wir eigentlich noch bei wieviel Mitarbeiter habt ihr und auf einmal erklärt er, wie sie einen Incident abarbeiten. Das war so interessant, das wollt ich dann gar nicht unterbrechen deswegen. Du hast gerade schon gesagt, ihr schaut, dass ihr eher kleinere Teams baut. In welchem Setting werden diese Aufgaben erfüllt? Das heißt, wir haben gerade schon gesagt, entweder alleine oder in kleinen Teams, aber arbeiten dann auch wirklich halt zwei, drei Leute zusammen an einer Aufgabe oder arbeitet jeder an seiner Teilaufgabe, sag ich mal, meldet das dann irgendwohin zurück und von dem geht es dann geht es dann weiter oder kann ich auch irgendwo zusammenarbeiten oder muss ich irgendwo an einer Aufgabe zusammenarbeiten?

UN: Na ja, zusammenarbeiten teils, teils. Es ist es entsteht bei uns immer relativ dynamisch, also ich hatte

vor ja paar Monaten einen Incident, [Interviewabschnitt entfernt] Das gliedert sich in der Gruppe auf und das entsteht einfach aus der Situation heraus. Ich weiß gar nicht, ob das so viel Sinn macht, hier arg abzugrenzen. Wenn es Sachen gibt, die man alleine machen kann, also, wenn einer sagt: Hey Leute, ich übernehme die Kommunikation jetzt mit den jeweiligen Personen, die hier betroffen sind, dann gerne, aber prinzipiell haben wir eben als zentralen Knotenpunkt quasi unseren Chat und von dort aus branchen die Leute entweder gemeinsam zu einem Task aus oder machen halt was alleine und melden dann wieder in den Chat zurück.

CE: Gut, das heißt, das haben wir alles erledigt. Ja, im Incident ist natürlich immer ein bisschen Zeitstress, das ist schon klar. Wie schnell müssen denn? Und auch das ist natürlich incidentabhängig, das ist mir schon klar, aber wie schnell müssen gewisse Dinge einfach erledigt werden? Geht es da wirklich drum, bis 19:00 Uhr brauche ich ein Ergebnis, weil da rede ich mit irgendwem, bis dahin müssen wir irgendwas sagen können? Oder ist das bei euch eher vielleicht auch aufgrund von einer anderen Struktur, weil ihr ja keine klassische Dienstleister-Kunden-Struktur habt, so wie man sie sich vorstellt, da kann man natürlich dann eher sagen, wir brauchen noch eine Stunde, als wenn ich dann externer Dienstleister bin und dann Vorstandsmeeting hab.

UN: Na, das ist bei uns Gott sei Dank nicht so kritisch, vor allem auch, weil wir kein Incident Response Dienstleister sind. Wir haben ein System, das gegliedert ist nach Severity, [Interviewabschnitt entfernt], je nachdem werden bei uns andere Workflows getriggert und sind auch gewisse Zeitrahmen einzuhalten, aber es ist jetzt nicht, zum Beispiel, dass bei einem Notfall innerhalb von einer Stunde genauer gesagt werden muss, was das Problem ist. Wenn wir nicht wissen, was das Problem ist, dann ist das okay, aber wir müssen innerhalb dieser einen Stunde sagen: Leute, es ist in Untersuchung. Wir vermuten es aktuell hier, hier, hier oder hier, aber wir können es auch nicht sagen. [Interviewabschnitt entfernt], dass wir hier wirklich keine Deadline haben, wo wir es wissen müssen.

CE: Wenn du dir jetzt wieder den Junior Incident Response oder den Junior CERTler vorstellst: Was wären so Tasks, wo du sagst, das muss der können, und ist zum Beispiel wer, der jetzt bei euch aufgenommen wird, der vielleicht noch frisch von der FH oder eher an der Untergrenze von der notwendigen Berufserfahrung bei euch ist, ist der dann auch sofort CERTler vom Tag oder macht das dann irgendwer anderer und er erst nach einer gewissen Zeit? Also welche Tasks muss der da vielleicht schon erfüllen, auch mit relativ wenig Erfahrung?

UN: Also am Anfang ist es nicht so. Da wird diese Person gar nicht im Rad eingesetzt. So in den ersten drei Monaten. Also wir geben den Leuten wirklich auch viel Einarbeitungszeit. In den ersten drei Monaten geht es mal drum: Wie schaut überhaupt unsere Hierarchie aus? Was sind unsere Abteilungen? Was macht der Betrieb, was machen die Services, machen die Developer? Dass man so ein bisschen ein Gespür dafür kriegt

und nach der Einarbeitungszeit kommen dann quasi die Reverse Shadow, also die Shadowphase kommt zuerst, wo man einfach mit dem jeweiligen CVT quasi zusammensitzt und die Tickets abarbeitet und schaut wie macht diese Person das? Wir leiten die Person dann auch immer quasi an mehrere Stellen also nicht, dass sie sich nur von einer Person abschaut, sondern dass sie wirklich mit drei, vier CVTs das macht und schaut okay, wie machen die anderen das? Und sich dann da rauspicken kann, was sein oder ihr bester Workflow ist. Dann kommt mal die Reverse Shadow Phase, da drehen wir das Ganze um, und zwar die Person arbeitet da erstmal eigenständig Tickets ab, aber der CERTler sitzt daneben und schaut halt zu und sagt, ob was nicht passt, und dann wird diese Person ins eigenständige Arbeiten entlassen und das auch das habe ich in meiner alten Firma auch gehabt also immer dieses zuerst Anschauen, dann Shadow, dann Reverse Shadow und danach ok, allein. Und war es natürlich auch wichtig, dass das im Prozess established ist. Ich mein natürlich, wenn das eine fünf Mann-Bude ist, wo einmal alle 10 Jahre ein Neuer kommt, dann braucht man das jetzt nicht niedergeschrieben haben, aber ich finde, es ist wichtig, dass hier das Ding niedergeschrieben ist und festgehalten ist, was die Methode ist.

CE: Danke schön. Da sind wir jetzt schon beim Knowledge angekommen. Du hast das vorher eh schon ganz kurz angeschnitten. Meine Frage dazu wäre, über welchen theoretischen Background müssen die Mitarbeiter, Mitarbeiterinnen bei euch im CERT verfügen und vor allem wie detailliert müssen sie das können? Das heißt, wenn wir jetzt einmal bei den Phasen sind, gemäß - hier beliebigen Standard einsetzen – ISO 27035, NIST SP 800-61: Phasen auflisten, beschreiben, anwenden und planen oder vielleicht doch auch wirklich entwerfen, konstruieren können, kritisieren, einschätzen, was würdest du da grundsätzlich sagen? Was brauche ich an Hintergrundwissen und wie detailliert brauche ich das?

UN: Meinst du spezifisch jetzt auf organisatorisches Wissen auf diese Standards bezogen?

CE: Nicht unbedingt auf Standards bezogen, aber auf generell organisatorisches Wissen. Was muss ich wissen? So wie du das eh gerade schon auch zu dem einen Standard zum Beispiel angeschnitten hast und wie genau muss ich das wissen?

UN: Ich kann das jetzt nur für mich sagen, ich glaub, das hängt sehr stark von der jeweiligen Person ab, die du interviewst. [Interviewabschnitt entfernt] Also kann ich nur für NIST SP 800-61 sprechen. Ein Knowledge von den Phasen, wie gesagt, was in der Phase jeweils ansteht, was zu tun ist. Ich finde auf einer niederen Schwelle, würde ich sagen, dass ein Knowledge dieser Phasen reicht. Wie ich es anfangs schon erwähnt habe, die Person sollte kurz wissen, was in der jeweiligen Phase zu tun ist und dass die Phasen, das ist vielleicht auch wichtig, nicht immer ganz linear sind, weil es kann ja sein, dass ich während meiner Remediation auf ein neues Artefakt stoße, was mich wieder zurückschmeißt in die Detect und Analyse Phase, also hier bisschen eine geistige Flexibilität beizubehalten und nicht quasi stumpf auswendig zu lernen. Ein

Verständnis dafür, dass es wirklich im Unternehmensumfeld zwischen akademischem Umfeld und Unternehmensumfeld, ein bisschen Unterschiede, mehr Graubereiche, gibt und wie man am besten mit diesen Graubereichen umgeht.

CE: Ich hab die Standards ja eh schon ein bisschen aufgearbeitet, das steht auch in jedem vorne und das hab ich zum Beispiel damals in der FH nicht gelernt. Ich bin jetzt im Bereich Internet Response auch beruflich unterwegs, deswegen weiß ich das. Aber es werden Standards immer so ein bisschen rübergebracht, als: so steht das da und genau so machen wir das. Vor allem in der ISO 27035 zum Beispiel, aber auch in der NIST, steht drinnen, da: ist keine Schritt-für-Schritt-Anleitung mehr oder weniger, sondern das ist was, woran du dich anhalten kannst, um das zu strukturieren und ich glaube, das ist einfach ein wichtiger Punkt, den man auch mitgeben muss, wie du das schon gesagt hast. Mit welchen Schlagwörtern und Begriffen muss man vielleicht umgehen können? Ich finde, es hat sich doch in der IT-Welt, oder es ändert sich immer wieder Einiges oder Vieles ändert sich eigentlich nicht, sondern wird nur neu genannt. Was sind da für dich so ein paar Beispiele, wo muss ich zumindest grob wissen, was ist das, oder da muss ich irgendwelche Konzepte grob verstanden haben?

UN: Kannst du mir ein Beispiel geben, da könnte man jetzt zwei Stunden über Abkürzungen reden.

CE: Ich weiß, ich weiß, du kannst zwei Stunden über Abkürzungen reden, aber jetzt zum Beispiel: SIEM ist, finde ich, so ein gutes Beispiel. Ich muss wissen, meines Erachtens nach zumindest, vielleicht was ist es, ob ich jetzt genau weiß, wofür die Abkürzung steht, wahrscheinlich nicht, aber ich muss wissen, was macht das System und wofür kann ich es verwenden? Also was sind da so Sachen, wo ich sag: Wenn ich jetzt zumKunden gehe, gut, ist bei euch jetzt nicht so, aber ich geh jetzt zum Kunden und der erklärt mir ja, wir haben da ein SIEM, dann sollte ich wissen, was das ist, und ungefähr wissen, was ist das für ein System, was kann ich damit machen? Das wäre der Hintergrundgedanke hinter der Frage.

UN: Gut, ja, SIEM, ganz klar, EDR, XDR – Die Leute sollten wissen, was das ist. PAM – auch ein ganz großes Thema. Es ist wirklich schwierig, da generell das zu sagen. Die Leute, finde ich, sollten wissen: VPN: Was sind überhaupt die Technologien dahinter? Was ist ein VPN-Gateway? Was sind die unterschiedlichen Strukturen, wie das aufgebaut sein kann? DMZ sollten die Leute wissen, was das ist circa, wieso die Abstufung von Trust Levels von intern nach außen immer abnimmt, und das es hier mehrere Zonen gibt. Aber das haben wir vorher angesprochen, dass die Leute quasi zumindest mal in Berührung damit kommen, wie schauen Enterprise Umfelder überhaupt IT-technisch aus, weil das ist, wie gesagt, das hast du jetzt sicher auch bemerkt, dass das Tag und Nacht ist zu dem, was man auf der Uni hat.

CE: Da muss ich jetzt schon ganz kurz für die FH St. Pölten eine Lanze brechen, das machen sie tatsächlich sehr, sehr gut und sehr, sehr praxisnah. Gerade diese Sachen, die du die du vorher gesagt hast, die waren bei

uns eigentlich fast alle im Bachelor sogar schon drinnen. Sie schauen, finde ich, da wirklich drauf, dass man solche Sachen auch praktisch übernehmen kann.

UN: Okay, super. Dann aus dem IT-Betrieb halt Load Balancing, ganz klar: Was ist Load Balancing? Ja, weißt eh, der klassische Blödsinn, Unterschied Hashing – Encryption, Unterschied Authentication – Authorization, aber da könnte man zwei Stunden drüber reden.

CE: Perfekt, dann haben wir hier schon ein paar gute Begriffe, die man noch einmal kurz einbringen kann.

UN: Ja, vielleicht auch ganz, ganz nützlich: Generell was ist PKI, wie funktioniert das?

CE: Ja, das ist sicher auch cool und wichtig. Perfekt, danke, dann sind wir jetzt schon bei den Skills angelangt. Die Social Skills haben wir ja schon ganz kurz besprochen. Kommunizieren muss er können, fällt dir da noch etwas in die Richtung ein, sowas muss ich jetzt persönlich mitbringen?

UN: Ich muss eine Stressresistenz mitbringen, weil es kann auch sein, dass ich quasi der Fels in der Brandung bin, aber auf mich prasselt ordentlich was von vielen Seiten möglicherweise auch gleichzeitig ein. Also ich muss hier auch unter Stress immer in der Lage sein, diesen OODA-Loop zu verfolgen. Was ist jetzt überhaupt für mich auf Information hineingekommen und das sich nicht quasi Reverse Social Engineeren zu lassen, dass man jetzt, weil man Stress vor einer Person, von einem Kunden kriegt, dass man hier quasi priorisiert, sondern dass wir das natürlich priorisieren anhand vom Incident, was der Incident erfordert. Das ist natürlich, würde ich sagen, fast das Wichtigste an einem, der viele Incidents wirklich abarbeiten muss. Es gibt auch Incident Responder, die machen ein Jahr lang nichts. Gott sei Dank. Genau Stressresistenz, Kommunikation und vielleicht doch ein gewisses Vertrauen in die eigenen Fähigkeiten. Weil es ist ja auch oft, dass man von der anderen Seite bekommt, so hä, das kann nicht sein auf unserem Server, der ist super gehärtet und dass man sich da dann quasi die Lage anschauen sollte und wenn man sagt, okay, ich komme trotzdem zu dem Schluss, dass du einen Blödsinn gebaut hast, dass man hier nicht quasi einstecken sollte aufgrund von Unsicherheit statt aufgrund von der Datenlage, das wäre auch ganz wichtig. Man ist dann immer der Junge und man ist dann der Neuere, der von der FH kommt, man sollte hier auch ein bisschen, wenn man hier quasi die Lage auf seiner Seite sieht, hier auch standfest bleiben können und sollen. Und generell in der Security lernfreudig sein und ich hab gesagt, wie gesagt standfest sein in eigenen Punkten, aber, wenn man was nicht weiß, aufsaugen und acknowledgen, dass man es nicht wusste.

CE: Super, danke schön, dann sind wir jetzt schon in der letzten Phase in der letzten Phase meiner Frage angelangt. Das ist jetzt ein bisschen deine oder so ein bisschen unsere Brain Dump Phase, da geht es jetzt nämlich zum Beispiel einfach um alles, was wir jetzt noch nicht angesprochen haben. Wenn du jetzt entscheiden könntest, wie baust du eine Lehrveranstaltung Incident Response auf, was wäre für dich drinnen? Ein Beispiel, weil ich das schon vorher gehört hab, ist zum Beispiel insbesondere auch auf Vorbereitung

und auf Lessons Learned eingehen als Vorbereitung auf den Job bei einem Dienstleister. Zum Beispiel zu erklären: Was sind Playbooks? Vielleicht sowas auch mal selber aufzumalen. Auch da jetzt gerne einfach alle deine Ideen, alles, was dir in den Kopf kommt.

UN: Weil du Cyberrange angesprochen hast, ich fänd, bei der Cyberrange ist wärs ganz wichtig – ich mein, ich weiß nicht, vielleicht habt ihr die ja aktuell so aufgebaut...

CE: Cyberrange kommt gleich kommt gleich nächste Frage, wenn du möchtest? Also das wäre jetzt wirklich einmal: Was sollen wir in den in den Vorlesungen und in vielleicht auch kurzen praktischen Zwischenübungen transportieren?

UN: Nicht, dass mir nichts einfällt, ich versuche, gerade meine Gedanken zuordnen. Ich glaub, wir haben eh schon sehr viel besprochen und du hast ja auch gemeint, dass die FH St. Pölten da sehr auf die Enterprise Architektur von IT-Netzwerken Wert legt. Ja, vielleicht fällt mir noch was ein, aber ich würde eher in Bezug auf die Cyberrange sagen, dass es wichtig ist, dass man hier einen Incident durchspielt, wo man den Incident wirklich von A bis Z verfolgen kann. Also man kann auch verfolgen über das, je nachdem, was der was der IoC oder was der Incident ist, das sieht man dann wirklich von außen die Spur durch das Netzwerk zum Asset oder zum Target dann ziehen kann, bzw. dann auch, wenn man es nicht schafft, dass man hier dann am Ende der Lehrveranstaltung zumindest weiß und auch versteht, was der Compromise Path war, entlang des Netzwerkes. Hier auch möglichst viele, wo sinnvoll natürlich, unterschiedliche Systeme, also VPN, Firewall, Linux und Windows. Ich glaub mit den 4 Hauptthemen, vielleicht darüber über Proxy zurück, je nachdem wie tief ihr geht in der Investigation, also C2-Server oder was auch immer, dass man hier einfach mal die Hauptbestandteile eines Firmennetzwerks abdeckt, was Loganalysis angeht.

CE: Auch da noch was sollen wir da vielleicht bei der Konzeption oder bei der Durchführung sonst noch beachten? Ich schmeiß jetzt vielleicht ein paar ein paar Stichworte hin: Umgang mit der Zeit: Sollen wir die Zeit, sag ich mal, am Ende des Tages anhalten oder, wenn es möglich ist, wirklich sagen, das läuft jetzt knallhart eine Woche durch und wenn ihr wollt, könnt ihr auch am ersten Tag direkt bis um 23:50 Uhr dann sitzen oder sollen wir wirklich sagen, wir begrenzen die Zeit nur zu den Vorlesungsübungszeiten?

UN: Ihr könnt es ja vielleicht zweiteilen. Also ich will da jetzt nicht wirklich ins Konzept reinpfuschen oder sonst irgendwas aufzwingen, aber ich find es eigentlich cool und vielleicht auch für dich als Feedback, wenn ihr am Anfang einen Incident habt, den die Leute frei abarbeiten können, in Gruppen und vielleicht anhand dessen auch ein paar Playbooks erstellen oder einfach kollaborativ daran arbeiten und dass sie dann einen zweiten Incident haben, um quasi die Bewertung und Beurteilung für die Lehrveranstaltung anzunehmen, wo ihr dann wirklich eine harte Deadlines setzt. Das wäre vielleicht ganz, ganz praktisch, dass man das schon einmal durchgespielt hat im eigenen Pace und in diesem eigenen Pace auch lernen kann, wie geht sowas

überhaupt, weil wenn man sofort ins kalte Wasser geschmissen wird, ohne das vorher gemacht zu haben, ist das vielleicht ein bisschen asozial, aber dass man hier quasi schon einmal in Ruhe das gemacht hat, vielleicht auch als Gruppenarbeit oder so und dann den Incident quasi mit ein bisschen härteren Bedingungen hat.

CE: Wie siehst du das in Bezug auf Berichterstattung zum Beispiel: Sollen immer wieder irgendwelche Zwischenberichte abgegeben werden müssen oder vielleicht auch irgendein formeller Abschlussbericht am Ende?

UN: Formeller Abschlussbericht am Ende finde ich sehr sinnvoll, weil wenn du aus dem Management Level drauf schaust, für was stellst du einen Incident Responder ein? Du stellst ein Responder ein, A damit er es behebt und B, damit er mit den Leuten kommuniziert und quasi die Information dann am Ende bereitstellt und dokumentiert, also dass du dann am Ende ein Dokument da hast von diesem Incident, dass du dann herzeigen kannst deinen anderen Stakeholdern. Also ich finde Berichte schreiben extrem wichtig. Hier wäre vielleicht ganz praktisch, die Leute vielleicht wieder am Anfang ein bisschen an der Hand zu führen, so hey, wir schlagen vor das so und so zu machen. Es gibt natürlich in der Welt – Jeder hat andere Templates oder was auch immer, dass man hier vielleicht mal ein Template für alle mal irgendwie bereitstellt, dass sie da hier vielleicht mal, wie ich schon vorher angesprochen habe, diesen introductory Incident vielleicht abspielen können und dann am Ende müsst ihr quasi einen Incident reporten und ihr könnt euch das Template dann aussuchen, falls ihr dann was anderes haben wollt und dass ihr dann hier vielleicht einfach die Beurteilungskriterien, vielleicht gebt ihr rein als Anforderung, wir brauchen diese und diese Überschriften und alles drunter könnt ihr euch frei aussuchen, aber dass die Leute auch mal in dieses Reporten reinkommen. Ja gut, ich bin Consultant, ich bin halt immer ein Verfechter des Reportens im Herzen.

CE: Ich versteh es, ich auch.

UN: Weil ich liebe das halt, wenn du halt ein Dokument hast, wo am Anfang deine Executive Summe drinsteht, was jeder C Level versteht und du dann halt reingehst und du quasi ein Dokument hast, mit dem du überall hingehen kannst mit den jeweiligen Sections und das finde ich ist auch extrem wichtig. Weil in zwei, drei Jahren, nachdem der Incident war und du vielleicht irgendwo weg bist, dann hat man aus der zurückblickenden Perspektive, dir umsonst 60-70 000€ im Jahr gezahlt; Lohnnebenkosten 100 000€ im Jahr und das am Ende wenigstens das Dokument überlebt, wie haben wir diesen Incident abgehandelt? Was war der Grund? Wie können wir daraus lernen? Das ist schon extrem wichtig für mich.

CE: Vielleicht jetzt noch mal genau auf diese Vorbereitungs- und Vorlesungsphase zurück, wie du auch gerade gesagt hast, das heißt, wenn ich dich richtig verstanden habe, sollten wir vielleicht auch dieses Reporting ein bisschen behandeln? Wie schaut das aus? Was sagst du zu mehr Vorbereitungen und Richtung Lessons Learned-Geschichten und eben Playbooks machen, Playbooks gestalten. Ist das sinnvoll deines

Erachtens nach?

UN: Absolut, weil, ich glaub, dir brauch ich das ja nicht erzählen, das ist ja das, wovon du dann lebst. Während dem Incident von deiner Preparation, das ist absolut wichtig, ja, seh ich auch so. Und das ist halt die Frage, wie man das am besten einbauen will. Will man quasi den Leuten sagen, vielleicht bei diesem ersten Incident, eins von diesen drei Themen wird sein und schreibt mal Playbooks zu diesen drei Themen in dem Netzwerk, wo sie gerade mal im Netzwerk umschauen können, damit sie überhaupt mal die technischen Indikatoren für dieses Playbook aufstellen können und dann sucht ihr euch einen Incident aus, den ihr Durchlaufen lasst durch die Range und dass die dann anhand des Playbooks, den Incident abarbeiten können. Ihr könnt es vielleicht auch in die Bewertung einfließen lassen. Es wäre vielleicht auch ganz spannend, so hey, wie gut hat das Playbook dann eigentlich gepasst zu den Incidents und wie gut ist dann der Report geworden daraus, also ja vielleicht auch was zu überlegen.

CE: Sehr gut, da waren jetzt einige coole Ideen dabei, die ich tatsächlich auch noch nicht so hatte, auch noch von keinem gehört, hab vielen, vielen Dank.

UN: Und vielleicht doch bei den Playbooks so einfach einen kurzen Exkurs machen, dass die halt auf Git gehostet werden, damit halt jeder über seine Pull Request Verbesserungsvorschläge machen kann. Vielleicht, wenn ihr das in Gruppenarbeit auslegt, könnt ihr das auch einbauen. Ich bin halt, aber da kommt wieder vielleicht mein Bias raus, weil ich bin extrem großer Git-Fan, [Interviewabschnitt entfernt]. Bei mir liegen alle Incident Response Playbooks auf Git herum und jeder, der eine Verbesserung hat oder einen Incident abarbeitet nachdem, und sieht, okay, ich brauche noch zusätzliche Steps, dass der dann einfach mittels Pull request quasi die Verbesserung einbaut und ich das dann approve.

CE: Wie hast du die gebaut auf Git, dass man die standardisiert auch bearbeiten kann oder ist es einfach: Dokument hoch und Dokumente durch den Pull request einfach ersetzt mit einem anderen Dokument?

UN: Ja, also bei uns haben die eine gewisse Struktur. Ganz grob ist das so, dass du oben mal quasi die Kategorisierung hast, was ist das überhaupt für ein Playbook? Dann hast du Kategorisierung nach MITRE Attack. Dieses Playbook ist für XYZ und dann hast du unten ein Flowdiagramm und zu jedem Knoten und Punkt in diesem Flowdiagramm hast du dann unten in Details quasi die technischen Details, was man hier untersuchen muss. Das ist eine Vektordatei, diese Grafik, die einfach gelinkt ist im Markdown, das heißt du kannst sowohl die Vektordatei einfach anpassen und das Markdown kannst du auch editieren und mit dem Pull request hast du dann quasi nochmal das 4-Augen-Prinzip, was drüber geht, so ja, dieser Change war OK und das kommt in production.

CE: Super spannend, perfekt. Dann wären wir am Ende meiner Liste angekommen vielen, vielen, vielen, lieben Dank für deine Zeit.

UN: Danke dir, ich hoffe, es war für dich als reinen Incident Responder nützlich, auch wenn ich nicht der pure Incident Responder bin, sondern also nur Teil meiner Tätigkeit ist.

CE: Es war extrem viel Spannendes dabei, vielen, vielen Dank.

B.4. Interview am 17.04.2025 mit Gideon Teubert, MSc (Incident Response Lead, CANCOM Austria AG)

CE: Gut, dann starte ich gleich mit dem ersten Fragenblock. Wie schon angekündigt, es geht einmal drum, dass wir verstehen, was macht die CANCOM eigentlich? In welchen Geschäftsfeldern seid ihr tätig und wie viele wie viele Mitarbeiter habt ihr? Und wie viele vor allem im Bereich IT Security und vielleicht auch Incident Response?

GT: Vieles. Wir sind IT-Unternehmer, ICS vorwiegend aber von-bis. Bis vor kurzem waren wir noch Legacy quasi die Kapsch oder die K-Businesscom, das ist auch ein 2 Jahre her. Wir sind auch sehr stark im IT Security Bereich vertreten, aber die Cancom macht von-bis, in der IT so ziemlich alles, würde ich mal grob pauschalisieren. Wir sind eine SE, sprich wir sind in der DACH-Region tätig und darüber hinaus. In der DACH- Region mit um die 5600 Mitarbeiter. In Österreich sind wir um die 1 600, jetzt nicht alle in der Security, auf jeden Fall in der IT oder vorwiegend in der IT und sind aber auch in Slowenien, Rumänien, etc. vertreten und auch in Übersee vertreten, aber halt kleinere Standorte. Die Hauptstandorte sind Österreich, Schweiz und Deutschland.

CE: Und wie viele sind in deinem Bereich? Wenn ich das richtig verstanden hab, verantwortest du ja das CDC.

GT: Nein, unser Head of CDC verantwortet das CDC. Ich verantworte das Incident Response und Digital Forensic Team, das ist ein Teil des CDCs. Wir sind um die 60 Blueteamer, quasi Analysten.

CE: OK, das heißt diese 60 Leute, die grundsätzlich im SOC tätig sind, sind dann auch fallweise, sofern halt was anfällt, im Incident Response tätig?

GT: Nachdem es gemischt ist, also es gibt viele Unternehmen, die haben nur die Bindung an den Incident Response Retainer und SOC, die haben das sehr klar getrennt. Bei uns ist es so, dass wir um die 15 Responder haben. Das sind eher die, ich sag mal, Senior und Principal Analysten, aber wie er jederzeit auf Analysten zugreifen können, weil die Tätigkeit sich sehr, sehr ähnelt. Das ist ein bisschen Open End, bis zu 60, aber die Vorwiegenden sind es um die 15.

CE: OK und außerhalb von Incidents sind die auch ganz normal als SOC-Analysten tätig oder irgendwie als Team Leads tätig oder was machen die außerhalb von Incidents, in Friedenszeiten quasi?

GT: In Friedenszeiten machen die Analysten SOC. Und die 15 Leute sind in der Weiterentwicklung von DFIR, also Digital Forensic und Incident Response tätig, aber auch in Side-Projekten, die das SOC vorantreiben oder die Kunden unterstützen oder auch Workshops machen, die Incident Readiness zum Beispiel tätigen, aber langweilig wird uns nicht. So wie auch aus dem SOC Incidents rauskommen können, da gibt es

keine klare Trennung, das sind halt schwerwiegender Fälle, wo schnell gehandelt werden muss, wo Incident Response eingeleitet werden muss. Also es ist ein bisschen verworren, wenn du das SOC und Incident Response zeitlich gleichzeitig anbietest. Was aber absolut Sinn macht, Improvements vorwiegend, wenn mal wirklich below effort da ist oder low load da sein sollte.

CE: Danke. Wie sieht so ganz grob euer Kundenumfeld aus? Nur, dass man sich ungefähr was vorstellen kann. Sind das hauptsächlich KMU? Sind das sehr große Enterprise Umgebungen oder ganz gemischtes Publikum?

GT: Es ist gemischt. Weniger KMU, mehr Enterprise, [Interviewabschnitt entfernt]. Wir haben auch kleinere Kunden dabei, aber da reden wir, also unser kleinster Kunde hat, glaube ich, 100 Mitarbeiter, das ist einer der wenigen, aber wir gehen bis über hunderttausend rauf. Auch die Branchen sind sehr gemischt, wirklich von-bis, [Interviewabschnitt entfernt], alles Mögliche.

CE: Wir haben jetzt gerade schon gehört, SOC bietet ihr an und die Incident Responses hast du gesagt, bietet ihr nicht, oder zumindest nicht nur, einen Retainer an. Bietet ihr trotzdem entsprechende SLA Retainer-Verträge, wie auch immer, oder ist das nur so ein ad hoc-Support, ausgenommen natürlich für SOC-Kunden?

GT: Wir bieten das auch explizit an, mittlerweile auch nur in Kombination mit zumindest einem SOC-Modul, um die Visibilität schon zu haben bei einem Incident. Wir haben SLA-Zeiten. Das sind zwei Stunden. Unsere maximale Reaktionszeit 24/7, egal wann, sind zwei Stunden, aber das kommt meistens nicht mal über ein paar Minuten. Wir sind mit mehreren Bereitschaften aktiv.

CE: OK, perfekt, danke schön. Dann sind wir schon mit dem ersten Teil fertig und hüpfen schon in den zweiten Teil, wo es um Anforderungen an Mitarbeiter geht. Und die erste Frage ist: Jetzt stell dir vor, es kommt ein Mitarbeiter zu dir, der sagt: Incident Response habe ich an der Fachhochschule gelernt. Was erhoffst du dir von dem, also was ist so der der Best Case, wo du sagst das ist schon echt cool, wenn er das kann? Und was ist, auf der anderen Seite vielleicht, so ein bisschen das bare minimum, wo du sagst, OK also das muss er jetzt schon unbedingt können, wenn er das so gelernt hat auf der FH?

GT: Ja, vielleicht ein bisschen an zur Historie, wie man Incident Responder bei uns wird. Natürlich kann man sich bewerben. Als SOC-Analyst musst du schon quasi IT Know-How haben, und zwar gar nicht wenig, damit du die ganzen Angriffe auf den verschiedensten Systemen einfach kombinieren kannst und auch connecting the dots quasi übst. Das heißt, du musst schon eine Menge IT-Erfahrungen mitbringen, damit du überhaupt mal Analyse tätigen kannst, die toolunterstützt ist, proaktiv oder halt während die Incidents passieren. Incident Response ist sehr, sehr reaktiv, sprich, du hast oft keine Visibilität, kein Tooling. Du musst wirklich auf die windows-forensischen Artefakte zugreifen, auf verschiedenste Betriebssysteme, auf verschiedene Systeme, wie ESXi. Du brauchst ein sehr, sehr großes IT-Know-How als Grundlage, das al-

leine reicht noch nicht. Du brauchst das Angreifer-Know-How, dass du weißt, wie die Angreifer vorgehen und du brauchst den forensischen Teil, wie du Analysen durchführst, das heißt also kurz und knapp: Ohne Erfahrung ist es kaum möglich, ein Incident Responder zu sein, auch wenn man sich theoretisch das beibringt. Diese Vorerfahrung von der IT und von Analyse und von Angreifern wird sehr schwer innerhalb von einem Studium zum Beispiel zu lernen sein. Die Grundzüge absolut, das heißt, wir schauen weniger, ob diese Person einen Abschluss hat zum Beispiel, auch wenn die meisten den haben. Oder ist die schon seit zehn Jahren Pentester, sondern mehr technisch wirklich: Kennt sie Angriffe? Kann sie die richtigen Schlüsse ziehen und kann sie auch die richtigen Gegenmaßnahmen ziehen? Sehr praktisches technisches Assessment, das wir durchführen.

CE: Das heißt, eigentlich ist es auch zum Beispiel bei euch jetzt nicht Voraussetzung, dass man unbedingt ein Fachhochschulstudium absolviert haben muss, so habe ich das auch schon gehört. So mit: Ja, das erwarten wir uns eigentlich schon, sondern man kann quasi auch bei euch über andere Wege auch in diesen Bereich kommen.

GT: Korrekt. Es ist ein nicer Benefit, aber im Grunde kommt es nur drauf an, kann ich richtig reagieren auf die Angriffe und das kann ich mit oder auch ohne Abschluss. Mit Abschluss sagt man zumindest OK, da ist, ich sag mal, mehr connecting the dots, da habe ich mehr Bereiche schon gesehen, was sehr beneficial ist, aber das alleine wird auch noch nicht reichen. Das kann ich natürlich auch ohne Abschluss mir selber beibringen oder halt eine Vorerfahrung aneignen.

CE: Das heißt, was wären da jetzt so Fähigkeiten, die ihr in diesem Assessment grob sehen wollt? Wir haben gerade schon gesagt, quasi dieses vernetzte Denken, dieses connecting the dot, wie du es gerade genannt hast. Was wären noch so Fähigkeiten, die euch da wichtig wären, dass eure sie Bewerber:innen mitbringen?

GT: Wenn wir mal noch nicht die Soft Skills erwähnen, die Hard Skills sind sehr technisch: Kann ich End Point Analysen-Forensik wirklich durchführen? Hab ich da Erfahrung? Kann ich Angreifer tracken durch Domänen, also Enterprise Umgebungen? Da gibt es verschiedenste Techniken dafür und wenn man es gemacht hat, weiß man diese. Dann kann ich auch abfragen, welche Techniken nutzen Angriff am häufigsten? Erklär diese wie zum Beispiel Persistenzen und dann natürlich auch wie kann ich die detektieren, wenn ich ein System bekommen würde, quasi das, was wirklich die Person im Job machen würde. Sehr technisch.

CE: Sehr gut, danke. Das heißt, eure Mitarbeiter im Bereich Incident Response, sind die eher Allrounder oder sind organisatorische und technische Themen natürlich bei größeren Incidents, jetzt nicht bei irgendwelchen kleinen Sachen, aber trennt ihr das bewusst auf, dass quasi einer koordiniert, Lagebild malt, wie auch immer, und der andere Loganalyse, Recovery, wie auch immer, betreibt.

GT: Ja und nein, kommt natürlich auch auf die Incident-Größe drauf an, aber ich sag es mal ein bisschen

ordinär: Unsere Responders sind eierlegende Wollmilchsauen. Sie müssen sozial sein, organisatorisch stark, weil wir nicht nur die Analyse tätigen. Wir gehen nicht nur einfach zum Kunden und okay, wir haben jetzt Analyse gemacht, und das war es. Auch wenn das der Hauptfokus ist. Das ist halt unser größter Teil der Arbeit, weil der Kunde kann es nicht delivern. Aber wir sind auch sehr beratend tätig, und auch in, ich sag mal, nicht direkt in der Leitung von dem Kunden, von dem Incident, nicht als Krisenmanager dort, wo wir die Führung übernehmen, aber schon sehr stark in einer sehr, sehr starken beratenden Tätigkeit, wo halt die Leitung ein wenig auch auf uns übergeht, wo wir auch C-Levels suiten, quasi eine Empfehlung geben müssen, Gegenmaßnahmen, Impactabschätzungen und das kann ich als alleiniger, wenn ich jetzt mich nur auf die Forensik konzentrieren würde, nicht tätigen, da kenne ich den Businessimpact nicht. Da sind wir halt sehr beratend dabei und natürlich auch in kürzester Zeit müssen Entscheidungen getroffen werden, die auch hart sind, ob es dem Kunden gefällt oder nicht. Wir müssen sie trotzdem empfehlen. Das ist alles in einer Konstellation, die oft in einem sehr stressigen Environment und Panikreaktion beim Kunden ist. Das heißt, man braucht sehr viel Feingefühl, also man braucht das IT-Know-How darunter, dass man die ganzen Schritte vom Angreifer sieht, man braucht das technisches Know-How, also das ist sehr technisch. Das kommt auf die Visibilität drauf an, aber man braucht auch ein sehr gutes Gespür vom sozialen, organisatorischen und damit auch Rahmenbedingungen wie z.B. NIS, KRITIS, Einmeldefristen, also Randwissen. Wir sind alle keine DSGVO-Experten zum Beispiel, aber Eckdaten. Das heißt, man muss ein bisschen ein Allrounder sein auf verschiedenen Gebieten, aber mit einem sehr, sehr starken Fokus auf Spezialisierung bezüglich Analyse.

CE: Und das heißt, man fängt dann eher bei euch mit dem technischen Schwerpunkt an und arbeitet sich dann auch in Richtung Incident Responder, mehr so diese koordinativen Rollen hoch. Kann man das so sagen?

GT: Genau, man könnte sagen, wenn wir da beim Kunden sind, haben wir zumindest einen, der im Lead ist, der ist, ich würd mal sagen, in größeren Incidents mindestens zu 50% der Zeit beim Führen von Kunden oder Beraten vom Kunden und wir haben dann, kommt drauf an, wie groß der Incident ist, Responder dahinter, die die technischen Analysen durchführen und die dann angeleitet werden vom Lead. Der Lead ist quasi der Multitasker, der viele Bereiche abdecken muss, aber nicht Heavy Lifting machen muss von der Analyse und das sind die meistens sehr Erfahrenen. Das sind bei uns die Senior und Principle Responder, die haben einfach schon auch die Ruhe, um halt eben diese Panik rauszunehmen und die Analysten, die die Fachexperten sind, können sich dann auch auf die Analyse konzentrieren und haben den Druck dann ein bisschen weggenommen. Die Kombo funktioniert ziemlich gut.

CE: Sehr gut. Gibt es irgendwelche Zertifizierungen und Ausbildungen, wo du sagst die siehst du sehr

gerne?

GT: Das Problem bei den Zertifizierungen ist, die sind sehr, sehr teuer, also, wenn wir jetzt hier aus dem Studium kommen, die wird sich keiner selbst zahlen. Vorwiegend sind's SANS-Zertifizierungen zum Beispiel 508, 500, das ist quasi, also auf Deutsch übersetzt, ist es der Windows Forensiker und der Advanced Incident Responder. Andere SANS-Zertifizierungen sind auch sehr willkommen. Das ist, ich weiß nicht, ob du es kennst, eine sehr komprimierte high intensity Schulung und extremst technisch in 5 Tagen und man hat Quantico-Ausbilder, NSA-Ausbilder, also ziemlich cool. Kostet halt ein Vermögen, sieht man aber sehr gerne, wird von Firmen auch sehr gern quasi übernommen, wenn man mal drinnen ist. Wenn das nicht der Fall ist, eben gerade für Studienabgänger, wenn wir schon sehen, sie machen CTF, sie machen Blue Teams, sie machen bei solchen Events mit, dann zeigt uns das schon mal, sie wollen. Nicht jeder kann es sich leisten, das ist absolut verständlich, aber uns geht es im Endeffekt darum, hat er genug Wissen, oder sie, und falls nicht, gibt es auch den Weg, dass man bei uns im SOC zum Beispiel anfängt als Analyst, da ist man unterstützt durch die Tools sehr stark und kommt damit quasi, so sind die meisten Responder von uns Responder geworden quasi. Nachdem sie sehr stark Analyst geworden sind, sind sie dann zum Incident Responder geworden.

CE: Gut, danke schön, dann sind wir jetzt schon bei diesem Bereich mit den TKS-Anforderungen, die ich schon ganz kurz angekündigt hab vorhin. Da soll es jetzt wirklich ausschließlich um diesen organisatorischen Bereich gehen, den du ja auch schon ganz kurz angeschnitten hast, der ja auch der Hauptfokus der Lehrveranstaltung sein wird und da fangen wir gleich mit den Tasks an. Ganz breite Frage dazu: Welche Aufgaben im organisatorischen Bereich übernehmen die Incident Responder da eigentlich?

GT: Ja, also vom technischen ist relativ klar, ist auch nicht der Schwerpunkt von dem Call. Die nützen eine beratende Funktionalität von-bis im Security Bereich während Incidents. Das ist vorwiegend, sag ich mal, Gegenmaßnahmen zu bestimmten Zeitpunkten zu empfehlen, aber auch quasi Handlungsempfehlungen auszusprechen oder eben auch die klare Empfehlung zu geben, diese zu unterlassen. Ein perfektes Beispiel dafür ist, Kunden wollen am liebsten alles resetten, dann sind sie ja clean, aber man weiß auch noch nicht, wann der Angreifer drinnen ist. Auf was resette ichs? Wie weit ist er gekommen? Auch solche Handlungsempfehlungen auszusprechen, beratend auch beim C-Level, sprich Beispiel Ransomware, C-Level sieht gern Zahlen. Die Zahl ist, ich habe ja einen Erpresser, ich sag jetzt mal, ein Bitcoin und auf der anderen Seite ist mein Unternehmen verschlüsselt, dann zahle ich es einfach. Das ist wesentlich billiger, als dass ich jetzt nicht weiterarbeiten kann. Ist halt ein Trugschluss, auch über sowas klären wir sie auf, während den Incident-Fällen. Kann schon sein, dass sie decrypted werden dadurch, aber der Angreifer ist immer noch drinnen. Solche Empfehlungen geben wir ab. Auch dass wir, nachdem wir ein MSSP sind in der CANCOM,

haben wir sehr viele Ressourcen im Hintergrund, Firewall-Experten, Netzwerk-Experten, die sind nicht im CDC, aber die sind halt in der CANCOM. Das heißt, wir können auch auf diese zurückgreifen und diese auch heranziehen. Angenommen, die Firewall ist verschlüsselt und wir müssen sie neu aufsetzen: Kein Problem, wir holen jemanden ran. Auch das ist eine Aufgabe des Incident Response Leads, ein wenig Struktur reinbringen. Es gibt Kunden, die sind sehr gut vorbereitet im Notfallmanagement, die haben ihre Streams, Krisenstab schon aufgesetzt. Es gibt Kunden, die haben gar nichts und sind kopfüber oder kopflos, das heißt wir bringen Struktur rein mit Streams. Wir machen einen Management Stream, wir machen einen technischen Stream. Wir halten die auseinander, dass jeder gut arbeiten kann. Wir versuchen, es klein zu halten. Ein paar Empfehlungen dahin gehend, in dem Fall halt sehr kurzgehalten, weil Zeit ist das A und O dort, und sie machen auch Incident Readiness Assessments. Das heißt, das ist Operations, da ist mehr Zeit, da fahren wir auch zu den Kunden und bereiten sie quasi auf potenzielle Incidents vor, was sie tun sollen, beraten Sie in der Gegend.

CE: Wenn wir uns jetzt das Aufgabensetting anschauen, ist das eher so, auch dann natürlich wieder sehr Incident-abhängig, aber wenn wir es jetzt mal auf eine einzelne Aufgabe herunterbrechen, brauche ich für diese einzelne Aufgabe mehrere Leute, die da gleichzeitig dran arbeiten oder arbeite ich eigentlich alleine immer an vielen Teilaufgaben? Also inwieweit muss ich wirklich im Team an einer Sache arbeiten? Und inwieweit hat eigentlich jeder sein Bröckerl, um das er sich halt kümmert?

GT: Also von den Respondern selber, das ist ziemlich klar, das gibt der Incident Lead vor, zum Beispiel: Hey, analysier mir das System auf das und das. Die haben quasi Brocken nach Brocken nach Brocken. Der Incident Lead hat keine Brocken, das ist Open End. Wenn der Kunde Consulting braucht in 'Was tue ich jetzt?'-Gegenmaßnahmen ist er für die Gegenmaßnahmen zuständig. Er implementiert sie nicht, er berät mit Impactabschätzungen. Er gibt auch vor, was die Analysten analysieren sollen, analysiert auch ein bisschen mit, also er ist Multitasking. Da gibt es im Securitybereich oder in der Analysetätigkeit und in der Führung von den Kunden, Incident Handling kaum ein Stopp. Das kann eben von-bis sein, damit ist er auch bisschen, ich sag mal, crippled, nachdem er im Dauermultitasking ist und die Analysten halt damit sehr schnell sind, weil sie nicht multitasken müssen, auch wenn es ein sehr high paced-Environment ist.

CE: Wenn du dir jetzt jemanden vorstellst, der vielleicht gerade relativ frisch im Incident Response-Bereich ist, wir haben gerade schon gesagt, ohne Erfahrung geht Incident Response nicht, aber wenn man jetzt sagt, der ist jetzt eher neu, was wären da so typische Aufgaben für den?

GT: Das Gute ist, es gibt auch kleine Incidents, sagen wir mal, ein System ist infiziert, das kann natürlich große Ausmaße annehmen, aber da setzt man die Maßnahmen zuerst und dann kann man es in Ruhe analysieren. Ist nicht so kritisch, das heißt wir also, wir haben einerseits Trainings und Academies, wo wir die

Incident Responder nach und nach dorthin bringen. Die haben schon meistens eine Grunderfahrung, die gar nicht schlecht ist, nachdem sie Analysten waren. Die gehen durch diese Trainings. Dort lernen sie, wie sie Basic Windows analysieren, Basic Linux analysieren, machen dann die ersten Fälle unter Supervision von den Seniors oder Principals, also den Erfahrenen quasi, und werden dann langsam herangeführt an größere Fälle oder Nischenfälle wie Kubernetes, sowas in die Richtung. Und so werden sie aufgebaut, bis sie halt ihren ersten größeren Incident haben, da halt quasi auch noch überwacht und geholfen und so führen wir die Leute ran, ohne dass wir ein Risiko eingehen, dass wir Fehler machen.

CE: Vielleicht auch wollen wir jetzt noch kurz bei den organisatorischen Tasks bleiben? Ich habe jetzt schon fast so ein bisschen zwei Welten kennengelernt, im Rahmen meiner anderen Interviews zur Lagebilddarstellung. Da ist zum Teil die Lagebilddarstellung insbesondere grafisch und so sehr wichtig und auf der anderen Seite habe ich aber auch schon gehört, nein, ist uns gar nicht so wichtig. Wir dokumentieren das kurz in einem OneNote und damit ist es fertig. Wie haltet ihr das generell mit der Lagedokumentation? Ist das auch was, was ihr schön grafisch aufbereitet, vielleicht auch eben für den Kunden?

GT: Ja, beides, also wir liefern am Ende natürlich immer ein Report, der super nice ausschaut. Auch grafisch schön vereinfacht für das Management, das man das schön sieht, weil technisch wird man es wahrscheinlich als Laie einfach nicht verstehen und das ist auch voll in Ordnung. Der Report hat einen Managementteil, hat einen technischen Teil, wo alles drinsteht. Auch für Behörden, Versicherungen, etc. Während des Incidents ist ja Zeitmangel, das heißt, da kommt es drauf an: Wir dokumentieren das in unserem Dokumentationstool für uns selber, der Kunde kriegt quasi nur kurz und knackig, meistens sogar nur beim Telefon quasi Fortschritte. Man sitzt sowieso schon alle zwei Stunden mindestens zusammen, bei größeren Incidents eher mehr. Da gibt es so viele Themen, da ist ein exaktes Lagebild nicht wichtig, sondern die Kerninformationen. Es gibt aber auch Themen, wo wir quasi ein Lagebild anfertigen mussten, um wirklich alle an einem Tisch zu holen: So schaut es jetzt aus – und das bereitet man natürlich schöner auf, auch grafisch; vor allem grafisch ist es viel leichter und man kann dann bestätigen, der Angreifer ist so weit drinnen, grafisch also auch für Laien halbwegs verständlich, aber das ist eher die Seltenheit, weil bei den meisten Incidents einfach der Zeitdruck da ist, sowas einfach nicht zu fertigen.

CE: Vielen, vielen Dank wir sind schon im nächsten Thema. Die Tasks haben wir hinter uns gelassen, wir kommen zum Knowledge. Da geht es jetzt wieder im organisatorischen Setting darum, über welchen theoretischen Background müssen die Mitarbeiterinnen und Mitarbeiter da verfügen und wie detailliert? Wenn ich gleich ein Beispiel geben darf, diese Incident Response Phasen gemäß ISO 27035 oder NIST SP800-61, je nachdem, was man auch gerne verwendet, reicht das, wenn man die Phasen da einfach auflisten kann oder soll man sie beschreiben können, soll man sie anwenden, planen können, vergleichen, differenzieren, um da

so ein bisschen diese Lernzielebenen reinzubringen?

GT: Wir sind das sehr, ich sag mal, auf der technischen Seite. Uns geht es gar nicht um irgendwelche Standards, ich mein, Standards sind schön, aber Standards veralten auch, ob er jetzt den ISO 27035 oder den 800-61er, ist relativ egal, weil wir prüfen ihn ab, ob er richtig vorgehen würde. Und die Phasen sind sich einfach extremst ähnlich, macht auch Sinn. Es ist daraus gewachsen. Die einen nennen es halt Containment, die anderen nehmen das Containment raus, nennen es halt gleich Eradication, die anderen machen es Analyse, die anderen nennen es Identification, ist egal, sobald sie erklären können inhaltlich, was sie machen würden. Es gibt gute Frameworks dafür, aber wir pinnen keinen drauf, ob er jetzt das eine Framework kennt oder nicht. Wichtig ist, dass er das Doing dann machen kann und auch kennt.

CE: Das heißt quasi, es ist nicht wichtig, dass man jetzt den Standard X kennt, aber es ist wichtig, dass man den Ton oder die generelle Vorgehensweise, die ja bei allen Standards und Normen und Handreichungen relativ ähnlich sind, dass man die einfach kennt und quasi da strukturiert vorgehen kann.

GT: Genau. Vielleicht ist das für Incident Response, für Forensik also wirklich Chain of Custody Forenstik, gerichtsverwertbare Forensik, da geht es halt nicht, da müssen halt die Standards sitzen, da müssen die Vorgangsweisen sitzen, da kann ich es quasi nicht einfach nur erzählen und wird schon passen. Da darf ich halt keinen Fehler machen und ich muss es auch in der richtigen Reihenfolge machen. Bei Incident Response auch, weil es ist da wesentlich weniger kritisch, wenn es inhaltlich stimmt. Das Containment, sollte ich natürlich nicht vorziehen, aber es passiert auch, dass quasi wir empfehlen: Hey, jetzt containen wir, bevor wir analysieren, das wäre eine Seltenheit. Da verschwimmen die Phasen plötzlich, Analyse plötzlich hinten, Containment vorne. Es kommt sehr, sehr auf den Fall darauf an. Das kann ich halt bei Forensik nicht bringen. Bei Incident Response kann ich es machen, deswegen ist es nicht so kritisch.

CE: Die Frage ist jetzt auch wieder relativ offen gestellt, die jetzt kommt. Ich grenze sie vielleicht gleich noch ein bisschen ein. Mit welchen Schlagwörtern und Begriffen, also was sind so diese Dinger, wo man sagt, das muss einfach sitzen, oder diese Konzepte, die müssen einfach sitzen, wenn jemand im Bereich Incident Response mitarbeiten will? Womit muss er da umgehen können?

GT: Sehr generelle Frage.

CE: Ich weiß, dass es eine absichtlich sehr, sehr generelle Frage ist. Das kann aber jetzt sein, von zum Beispiel wissen, was ein SIEM ist und das System dahinter verstehen oder wie auch immer. Was sind so Konzepte, die man vielleicht auch immer wieder sieht und die man einfach verstanden haben muss, um da sinnvoll arbeiten zu können?

GT: Dann fokussiere ich mich auf den technischen Teil. Damit man quasi, ich sage mal, das bare minimum eben hat, gibt es zwei Sachen bei uns: Das eine ist, man muss unbedingt einen Endpoint gescheit analysieren

können. Forensisch, auch ohne Tooling. Uns ist das Tooling relativ egal, der nächste Kunde hat ein anderes Tooling und der Faktor, den richtig interpretieren können, dass ich ausschließen kann, dass er infiziert ist, oder es beweisen kann. Das ist das eine vorwiegend. Ich kann mich auch nur auf ein Betriebssystem fokussieren wie Windows, weil es einfach am meisten vorkommt bei den Unternehmen. Das zweite ist, dass ich Lateral Movement erkennen kann und auch ausschließen kann, wo ich es erkennen kann. Das kann ich jetzt, wenn der Kunde ein SIEM hat, am SIEM machen, aber die Daten sind dieselben. Uns geht es nicht um das SIEM, aber ich muss wissen, wie ich das feststellen kann. Wie kann ich einen Angreifer durch die Domäne quasi verfolgen oder überhaupt beweisen, dass er sich bewegt hat, weil wenn ich das nicht kann, dann mach ich einen Fehler, dann schließe ich den Incident, obwohl der Angriff dann noch auf einem anderen System ist, weil ich den Endpoint nicht gescheit analysieren kann, kann ich es erst nicht beweisen. So mit diesen zwei Sachen bin ich schon sehr, sehr weit dabei, da ist noch nix mit Gegenmaßnahmen oder mit Preparation. Das ist wirklich, dass ich die Analyse hinbekomme, ohne den Angreifer, nachdem wir Gegenmaßnahmen angesetzt haben, im Unternehmen zu lassen, weil es fällt mit der Analyse im Endeffekt.

CE: Da sind wir jetzt schon beim Bereich Skills angelangt. Da hast vorher auch gerade schon diese Social Skills ein bisschen angesprochen. Wie muss ein Incident Responder beschaffen sein? Aus welchem Holz muss der geschnitzt sein?

GT: Ich glaub, es gibt so zwei, drei Key Traits, die sich bei dem Responder durchgesetzt haben. Das eine ist Resilienz. Das ist, glaube ich, ziemlich klar. Es ist ein sehr stressiger Job, der Incident kann unerwartet kommen und dann hat man halt sehr stressige Arbeitstage. Und auch stressige Kunden, eine stressige Umgebung. Das ist Incident Response im Endeffekt. Da muss ich sehr stressresistent sein. Andererseits muss ich sehr, sehr effizient sein. Ich darf also, was unsere Responder nicht sind, ohne etwas schlecht zu reden, sie sind jetzt keine extremen Perfektionisten, weil du hast keine Zeit. Der Angreifer ist schnell, der verbreitet sich weiterhin. Habe ich jetzt jemanden, der den einen Host bis zu 110% durch analysieren möchte, um wirklich jedes Artefakt zu finden, auch wenn noch so unwichtig, macht das mehr Schaden als jemand, der sagt: Okay, ich habe jetzt vielleicht 80% gefunden. Das System ist absolut infiziert, das quarantänisieren wir, macht das gleiche und ich geh zum nächsten System, schau, wo der da oben ist, dämm den dort ein. Das heißt, man muss sehr, sehr effizient da sein und man muss auch sehr effizient diese Informationen verarbeiten können. Das bringt mich auch zum letzten Punkt: Jeder der Responder ist, ist extremst eager to learn, also wissbegierig. Die sind extremst wissbegierig, damit man dieses Connecting the dots hat oder bekommt, muss man in verschiedensten Bereichen wissbegierig sein, nicht nur auf einer Spezialität. Damit ich aber auch schnell lernen lerne, muss ich mir immer wieder neue Dinge anschauen. Gerade im Incident Response kommt das System X daher, das haben wir noch nie gesehen, weil es gibt einfach so viele Systeme, Betriebssysteme,

Produkte da draußen. Der Incident Responder muss es aber trotzdem können. Dann kommt die Firewall FortiGate, haben wir noch nie gesehen zum Beispiel. Also haben wir schon gesehen, aber nur als Beispiel. Ich muss wissen, ohne das Produkt selber zu kennen, wie kann ich die Daten rausziehen, die ich brauche und bestätigen, ist die gefallen oder nicht? Und das kann ich nicht, wenn ich ein langsamer Lerner bin oder alles perfektionistisch machen möchte. Ich muss mir schnell Sachen aneignen können und diese kombinieren. In dem Fall wäre es: Ok, ich habe andere Firewalls gesehen, dort war es so und so, wahrscheinlich gibt es das auf dem auch, schaut ein bisschen anders aus und ich krieg die Logs und bin viel schneller. Also das sind glaub ich drei Haupttraits. Natürlich sozial muss man sein.

CE: Apropos sozial: Für den Incident Lead natürlich vollkommen klar, aber inwieweit hat das ganze restliche Incident Management oder Incident Response Team wirklich Kundenkontakt? Inwieweit müssen die vielleicht auch einmal, auch wenn sie jetzt nicht gerade im Lead sind, Dinge an den Kunden kommunizieren oder Dinge rückfragen oder was auch immer notwendig ist?

GT: Ist gar nicht so wenig, also ist auf jeden Fall nicht so viel, wie der Incident Lead. Die Incident Responder können auch auf die technischen Ressorts von Kunden direkt zugehen, das ist absolut in Ordnung, aber es ist eher auf der technischen Ebene zwischen uns und den technischen Ressorts auf der Kundenebene. Das ist meistens sehr kurzgehalten und sehr nerdig, einfach kurz, knapp antworten, könntet ihr das blockieren, kein Problem. Aber sie sind genauso dran, wenn kleine Infektionen stattfinden. Kleine Incidents machen sie auch schon selbständig, können sie auch selbstständig. Da müssen sie genauso mit dem Kunden kommunizieren und Report präsentieren und auch Gegenmaßnahmen empfehlen. Aber es ist in einer weniger stressreichen Umgebung, der Druck ist nicht so stark da und es ein bisschen weniger Multitasking. Da bezieht man sich auf eins anstatt auf 100 000 Systeme. Also passiert genauso, muss man genauso sein, nur die Resilienz kommt nicht so zum Vorschein in dem Fall.

CE: Gut, danke schön. Wir sind schon bei der letzten Sektion quasi angekommen. Es geht jetzt um die Lehrveranstaltungsplanung. Du darfst dir jetzt alles von uns wünschen, was du quasi gerne hättest, das vielleicht deine zukünftigen Incident Responder und Responderinnen alles mitbringen und da vielleicht gleich die erste Frage: Was sind zentrale Punkte, die wir in den Vorlesungen, also vielleicht noch in dieser vorherigen theoretischen Inputphase, unbedingt transportieren und mitgeben sollen?

GT: Da hätte ich jetzt gerne die technischen Vorlesungen, da würden mir viele, viele Dinge einfallen. Dann bleiben wir mal vielleicht beim Stakeholder-Management. Ich weiß nicht, wie man es rüberbringen wollen würde, aber ich habe die Erfahrung gemacht und ich habe sie auch selber so gelebt zu Beginn meiner Karriere, dass ich in einer Bubble gelebt habe, in meiner technischen Bubble. Ich habe jetzt Sicht auf die Security und empfehle den Kunden: mach MFA, das ist natürlich die Gegenmaßnahme, super toll. Aber

das ist meine Bubble und die Realität sieht halt so aus, dass MFA halt eben nicht so einfach ist, weil ich hab 10000 verschiedene Mitarbeiter, ich hab das C-Level, das dagegen ist und ich hab sehr viel Gegenwind als Kunde, dass ich ein bisschen auch... Die Empfehlung muss ich abgeben, aber auch natürlich die Kundensicht einnehmen kann. Man kann es auch Empathie nennen, aber dass ich ein bisschen auch den Businessfokus reinbekomme, weil eine Gegenmaßnahme des useless, wenn der Kunde sie nicht annimmt. Das heißt, ich kann damit schon ein bisschen einschätzen, die Entscheidung obliegt immer noch dem Kunden, aber ich kann damit immer schon ein bisschen einschätzen, okay, das ist eine Gegenmaßnahme, die ist gut, und die wird auch angenommen, wahrscheinlich, anstatt dass ich Gegenmaßnahmen setze, wie: Macht einfach alles neu, dein ganzes Unternehmen. Ist richtig, securitytechnisch, ich bin clean danach, aber das kann ich halt nicht bringen. Ist ein krasses Beispiel, aber das wäre ein Punkt, bisschen in die Businesssicht reinzukommen. Ein anderer Punkt wäre, welche Leute muss ich denn eigentlich reinnehmen. Viele nennen es auch im Notfallhandbuch, sind sie verankert oder im Krisenmanagement. Welche Kunden möchte ich reinnehmen, welche Personen oder Rollen möchte ich unbedingt nicht reinnehmen? Wie groß möchte ich diesen Kreis halten? Sowas sollte besprochen werden. Wenn ich 20 Leute hab, wird es kein Weiterkommen geben. Was sind Themen, die wichtig sind, die zeitkritisch sind, was nicht? Eine DSGVO-Meldung hat ein paar Stunden Zeit, da ist eher wichtig, Gegenmaßnahmen zu setzen. Für die DSGVO-Rolle ist natürlich das das Wichtigste, aber das muss man auch ein bisschen abschätzen können. Ransomware würde ich auf jeden Fall reinnehmen, Ransomware ist sowieso das A und O, liest man in den Nachrichten. Aber was bedeutet das eigentlich, wenn zahle oder nicht zahle, dass das den Leuten bewusst ist, dass das eigentlich den Angreifer nicht rausbringt aus dem Unternehmen. Und dass das halt auch dem Management vermittelt werden kann. Auch das Management, das die finanzielle Entscheidung trifft, ist nicht so weit, das muss man auch vermitteln können, was bedeutet das eigentlich? Ich glaub, das sind die drei wichtigsten Punkte.

CE: Ich hab noch, ich hab noch zwei, drei Schlagworte da stehen. Zum einen, vielleicht diese Vorbereitungsphase, was da wichtig ist, weil du ja auch vorher von von Readiness-Workshops und so gesprochen hast und vielleicht auch das Thema, das wird zumindest aktuell unterrichtet, Playbooks. Inwieweit wäre das wichtig?

GT: Ja stimmt, hätte ich jetzt beim technischen eingeordnet, aber ja, ist absolut organisatorisch. Wir haben verschiedenste Playbooks, gar nicht wenig, ich kann nur aus Erfahrung reden oder sprechen: Es bietet eine schöne Grundlage, aber die Realität ist immer extrem abweichend. Das heißt, Playbooks sollten auf jeden Fall vorbereitet sein und mit den Kunden abgestimmt in der Preparation. Wir machen es auch gemeinsam mit dem Kunden, sagen wir, ein Ransomware-Playbook. Das nimmt nur extremst riesige Maßstäbe an, da sind wir bei Business Continuity, da sind wir bei Incident Response, da sind wir bei Wiederherstellung und,

und, und. Und auch Krisenhandbüchern. Das ist ein Riesenteil, ist auch quasi ein Incident Response Plan, der das enthält. Aber auch jeder Incident, der vermieden werden kann, ist der beste Incident. Und wenn ich das nicht kann, sollte eine Visibilität da sein, davor. Das besprechen wir bei solchen Readiness-Workshops genauso, was für Visibilität brauchen wir als Minimum vor dem Incident, auch wenn er dann nicht verhindert werden konnte, kann es sein, zumindest haben wir ein zentrales Logging mit diesen Daten. Was wir nämlich immer wieder sehen ist, Kunde hat gar kein Logging, Angriff ist eine Woche her, die Logs gehen drei Tage zurück. Viel Glück, den Angreifer die ganze Kette durchzufinden, kann auch passieren, dass es gar nicht geht und was mache ich dann als Kunde? Wir können den Angreifer einfach nicht zu 100% bereinigen, also für solche Dinge, Preparation, sagt man eigentlich, ist das Wichtigste. Andere sagen Lessons Learned ist das wichtigste. Ich würd sagen, das Doing ist natürlich, wenn das Doing da ist, das Wichtigste, aber es sind alle Phasen wichtig.

CE: Genau diese Lessons learned wär nämlich das andere gewesen, weil, was man ja auch immer wieder sieht oder auch liest, ist dass gerade dieses Davor und Danach immer so ein bisschen vernachlässigt wird. Während es brennt, sind immer alle natürlich gut dabei und danach haben wir das auch ganz schnell wieder vergessen.

GT: Wenn ich mich zwischen Preparation und Lessons learned entscheiden müsste, wäre es die Preparation, weil wir bringen zum Beispiel auch Lessons Lernen von anderen Kunden, also natürlich anonymisiert, in diese Preparation rein. Ist keine hundertprozentige Lessons Learned für diesen Kunden, aber lässt mich schon mal sehen, OK, das sind die Haupteinfallstore, das sind die Hauptfehler, technisch sowie organisatorisch. Wie es dann wirklich ausschaut, lernt man dann eh wieder am eigenen Leib und braucht auch ein Lessons learned, aber Preparation ist Key, das macht das Um und Auf bei einem Incident.

CE: Gut, dann sind wir mit der Vorbereitung fertig und wir kommen jetzt in die zweite Phase der Lehrveranstaltung, nämlich die praktische Abschlussübung. Da ist aktuell geplant, dass wir eine Cyberrange bauen, mit einem nicht allzu komplexen Szenario. Das heißt, das Szenario sollte gut lösbar sein und der Fokus sollte tatsächlich darauf sein, dass man Stakeholder-Management macht, Lagebild malt, aber auch einfache Analysen, Containment und Recovery macht. Was wären da für dich so zentrale Punkte, die wir da bei der Planung oder auch bei der Durchführung von so einer Übung beachten müssen?

GT: Im organisatorischen Teil?

CE: Ja, aber gerne auch, wie wir gewisse technische Themen einbringen können oder sollen, was da besonders wichtig wäre für dich?

GT: Ich glaub, was wir noch gar nicht geredet haben, ist, es ist grenzwertig technisch, grenzwertig organisatorisch, vielleicht können wir in dieser Cyberrange einbauen, einerseits Ransomware, dazu komme ich

gleich, sondern auch der Kunde ist mega gestresst, möchte quasi wiederherstellen, weil es geht nichts mehr, seine Produktion, aber die Analyse ist quasi am Beginnen erst und man weiß nicht, seit wann er drinnen ist, wie weit er ist und dass man den Studenten auch mitgibt, wenn ich jetzt den Kunden dort einknicke, muss ich das alles noch mal machen, weil er ist ganz sicher wieder infiziert. Ich wiederherstelle nicht vor die Ransomware zum Beispiel, sondern bevor der Angreifer drinnen war. Das kann Wochen davor sein, das weiß man halt noch nicht. Den Punkt würde ich irgendwie hervorheben, wenn es möglich ist. Auch dass, wie auch immer man das bei der Cyberrange abbilden möchte, weil es halt sehr organisatorisch ist, diesen Druck nachzubilden, von, ich nenne es jetzt mal wieder ein C-Level: Hey, wir haben jetzt hier Millionenverluste am Tag und wir stehen jetzt seit einem Tag, seit zwei Tagen. Die Analyse dauert mindestens 3 Tage. Wie gehen die Studenten damit um? Dass sie eben nicht einknicken. Vielleicht kann man noch ein bisschen was einbauen, dass viel mehr zu finden ist auf einem System zum Beispiel, aber man sich auf die Hauptthemen fokussieren sollte. Wie schlimm ist es, was ist grob passiert und ist infiziert oder ist er dort reingekommen? Dass man vielleicht auch misst, wie schnell sind die Leute? Wie tief gehen Sie rein? Wäre halt ein Fehler eigentlich. Und Gegenmaßnahmen zu den richtigen Zeiten setzen. Könnte man in der Cyberrange tatsächlich abbilden, wenn ihr einen aktiven Angreifer habt, der sich halt weiterbewegt. Wann würde ich Gegenmaßnahmen setzen? Was wahrscheinlich ein Fehler sein könnte, ist, ich habe eine Domäne, die blockiere ich jetzt einfach, anstatt dass ich mal grundsätzlich scope und dann Entscheidungen treffe, sonst mach ich es quasi mit einem blinden Auge. Und dass sie, währenddem sie Zeitdruck haben, eben auch ein Lagebild machen, da werden wir wahrscheinlich in den Perfektionismus reinrennen, die ist sehr perfekt machen wollen. Wir haben auch solche Planspiele gemacht, wo es für jede falsche Entscheidung länger dauert zur Wiederherstellung. Damit haben wir Kohle verloren, das heißt, da läuft ein Timer, der halt zum Beispiel hochzählt und Geldverluste macht, wie es halt in der Realität ist. Dass man bei jedem falschen Abbiegen, bei jedem zu tief Reinschauen, natürlich diesen Zähler hochzählt, aber wenn man es zu schlampig macht, genauso diesen Zähler hochzählt, weil, das ist halt noch ein größerer Schaden, dass man diesen Druck nachmacht. Wie auch immer das machbar ist, das wären so meine Ideen.

CE: Was hältst du zum Beispiel auch von der Notwendigkeit einer Berichterstattung? Auch da wieder ein kleines Stichwort: Zum Beispiel Zwischenberichte, Abschlussbericht, formell, informell, wie auch immer.

GT: Ja, ein Abschlussbericht ganz sicher und dann wahrscheinlich sollte irgendwas benotet werden. Da sieht man dann auch, wie tief sie reingegangen sind, was sie alles gefunden haben, wieviel Zeit sie gebraucht haben, dann wahrscheinlich, ob alles gefunden worden ist, also das auf jeden Fall. Bei uns verbraucht der Abschlussbericht teilweise die Hälfte der Zeit, weil es einfach sehr viel nachzuarbeiten ist und der Fokus auf der Vollständigkeit liegt, wo er vorher nicht gelegen ist. Zwischenberichte, wenn es möglich ist. Ich weiß

nicht, es ist halt sehr organisatorisch, eine Cyberrange nachzuspielen. Lagebilder, die kurz und knackig sind, wo halt, ich sag mal, fünf Key-Fakten drinnen sein müssen: Wo stehe ich? Wie schlimm ist es? Was das Scope? Weiß ich schon irgendwas, wie der Angreifer hier reingekommen ist? Was sind die Gegenmaßnahmen zu setzen? Und ungefähr, wie lang könnte es noch dauern als Abschätzung? Das wird sich sicher ändern, aber dass das kurz und knapp beantwortet ist, von mir aus. Also natürlich auch mit Bild, wenn möglich, aber Zeit wird da wahrscheinlich eher weniger sein.

CE: Apropos Zeit, wie siehst du das? Auch schon Unterschiedliches gehört. Sollen wir quasi, wenn wir natürlich organisatorisch von der FH her die Zeit bekommen, die Übung einfach wirklich Montag in der Früh beginnen und dann läuft die einfach knallhart bis Freitag, 23:59 Uhr, durch. Oder ist das vielleicht sinnvoll, dass man das ein bisschen am Anfang entspannter angeht und sagt: Ah, wir machen das? Bis jeweils um 17:00 Uhr und dann machen wir Pause bis morgen. Oder sollen wir ihnen schon noch die Möglichkeit geben, so wie es halt in Realität ist, sich auch 24/7 dransetzen zu können?

GT: Ich bin mir ziemlich sicher, zumindest hätte ich das so gemacht, dass einige halt wahrscheinlich durchhackeln würden, was natürlich ein Fehler wäre, weil das machen auch wir im Incident Responding nicht. Das sind sehr lange Arbeitstage, aber du brennst nach zwei, drei Tagen einfach aus im high Stresslevel und du kommst nicht mehr weiter. Ich weiß nicht, ob man das dann wirklich fördert damit oder halt abbilden kann, keine Ahnung, wo die Leute sagen, sie haben halt nur bis 17:00 Uhr gearbeitet und analysiert und machen es in der Nacht weiter, das ist halt schwer messbar. Und von Montag bis Freitag würde ich es nicht machen. Arbeitstechnisch wäre schon mal schwierig. Ich weiß nicht, wie es bei Studenten ist, könnte auch sehr schwierig werden. Ich würde tatsächlich an einem sehr langen Tag alles durchspielen. Dafür halt einen kleineren Incident, dafür ist halt der Druck auch massiv da. Und halt ein wenig schwächer bewerten, weil niemand wird alles finden, wenn es richtig aufgebaut ist. Niemand wird die hundertprozentig richtigen Entscheidungen treffen. Das ist manchmal so. Mit dem Lagebild treffe ich die Entscheidung und es muss nicht die richtige sein, dass man es ein bisschen nachspielt, aber dass sie den Stress spüren, nur halt jetzt nicht eine Woche lang durcharbeiten, das glaube ich, da werden einige sich hinsetzen in der Nacht und wesentlich weiterkommen und andere werden halt irgendwann nicht weitermachen. Ist nicht das Feeling vom Incident, wir arbeiten auch in Schichten. Damit wir eben frisch sind und ich glaub, da hat man keine Kontrolle drüber, wenn man quasi sagt: Hey, Montag bis Freitag, viel Glück. Und sie könnten sich natürlich auch austauschen, was es auch schwieriger macht. In einer high Stresssituation an einem Tag wird es wahrscheinlich schwierig sein, sich richtig auszutauschen, wenn ich das eine Woche mache, dann wird wahrscheinlich jeder alles finden, zumindest aus meiner Studienzeit.

CE: Ich verstehe, ich kann ein bisschen relaten. Dann vielen, vielen, vielen herzlichen Dank für deine Zeit.

GT: Bitte gerne.