Digital Business University
of Applied Sciences

Cyber- & IT-Security (M.Sc.)

Systemanalyse

Wintersemester 2024/25

Incident Response und Notfallmanagement: Analyse effektiver Strategien zur Reaktion auf Cyberangriffe

---

Studienarbeit

Eingereicht von:
Elias Häussler

Matrikelnummer:
200094

Dozent:
Ersel Dogan

12. März 2025

Inhaltsverzeichnis

Abkürzungsverzeichnis

BCM Business Continuity Management

BDA Big Data Analytics

DLP Data Loss Prevention

ECC Emergency Communications Center

HIRCT High-Impact Incident Response Coordination Team

IDS Intrusion Detection System

IP Internet Protocol

IRP Incident Response Plan

IRT Incident Response Team

KI Künstliche Intelligenz

ML Maschinelles Lernen

NIRT Network Incident Response Team

NIST National Institute of Standards and Technology

PDCA Plan-Do-Check-Act

PIR Post-Incident Report

SANS SysAdmin, Audit, Network, and Security

SIEM Security Information and Event Management

SOP Standard Operating Procedure

1 Einleitung

Im Jahr 2023 wurden in Deutschland über 130.000 Fälle von Cyberkriminalität polizeilich erfasst – mit einer vermutlich deutlich höheren Dunkelziffer (Statistisches Bundesamt, 2024b). Obwohl deutsche Unternehmen im selben Jahr bereits über 9 Milliarden Euro für IT-Sicherheit aufwendeten, belief sich der durch Cyberangriffe verursachte Gesamtschaden auf mehr als 200 Milliarden Euro (Statistisches Bundesamt, 2024a, 2024c). Diese Zahlen verdeutlichen, dass Cybersicherheit längst eine essenzielle Säule der Gesellschaft ist und von Unternehmen nicht mehr vernachlässigt werden darf.

Gleichzeitig werden Cyberangriffe immer ausgefeilter, schwerwiegender und komplexer. Sicherheitsvorfälle gehören in vielen Unternehmen bereits zum Alltag. Umso wichtiger ist es, effektive Strategien zur Bewältigung von Cyberbedrohungen zu entwickeln und konsequent umzusetzen.

1.1 Problemstellung

Ein essenzielles Feld der IT-Sicherheit ist das *Incident Management*, das sich mit der Bewältigung von Cyberbedrohungen befasst. Innerhalb dieses Bereichs spielt die *Incident Response* eine zentrale Rolle, da sie darauf abzielt, Bedrohungen frühzeitig zu erkennen und angemessen darauf zu reagieren.

Unternehmen investieren zunehmend in den Aufbau komplexer Prozesse, um potenzielle Sicherheitsvorfälle effizient zu bewältigen und geeignete Gegenmaßnahmen einzuleiten. Die steigende Komplexität von Cyberangriffen erschwert jedoch die Umsetzung einer wirksamen Incident-Response-Strategie. Diese Arbeit untersucht daher verschiedene Ansätze zur Etablierung effektiver Incident-Response-Prozesse in Unternehmen. Dabei stehen folgende Fragestellungen im Fokus:

- Welche Phasen umfasst ein etablierter Incident-Response-Prozess?
- Wie lassen sich diese Prozesse kontinuierlich weiterentwickeln und an aktuelle Bedrohungen anpassen?
- Welche Bedeutung hat Incident Response im Rahmen des Notfallmanagements?

1.2 Inhalte der Arbeit

Die Arbeit beginnt in Kapitel 2 mit einem grundlegenden Überblick über Incident Response und Notfallmanagement. In Kapitel 3 werden die einzelnen Phasen der Incident Response detailliert erläutert. Anschließend veranschaulicht Kapitel 4 die praktische Anwendbarkeit anhand zweier Fallstudien. Kapitel 5 behandelt zentrale Herausforderungen und bewährte Best Practices. Abschließend fasst Kapitel 6 die gewonnenen Erkenntnisse zusammen und gibt einen Ausblick auf zukünftige Entwicklungen im Bereich der Incident Response.

2 Grundlagen

2.1 Incident Response

Unter *Incident Response* versteht man die Eindämmung, Untersuchung, Beseitigung, Abschwächung und Reaktion auf eine Bedrohung im Kontext der Informationssicherheit (vgl. Maras et al., 2021, S. 198). Durch die Entwicklung geeigneter *Incident Response Plans (IRPs)* sollen Angriffe begrenzt und der entstandene Schaden minimiert werden. Der Fokus liegt dabei weniger auf der Eintrittswahrscheinlichkeit, sondern vielmehr auf dem konkreten Zeitpunkt eines Angriffs. Daher ist insbesondere die präventive Planung eines solchen Vorfalls von großer Bedeutung (Maras et al., 2021). Ziel einer Incident Response ist jedoch auch die Verhinderung weiterer Angriffe. Dabei stehen vor allem nicht vermeidbare Vorfälle wie etwa *Zero-Day-Exploits* im Vordergrund, da diese besonders großen Schaden nach sich ziehen können (Nayak & Rao, 2014).

2.1.1 Incident Response Plan (IRP)

Ein *Incident Response Plan (IRP)* enthält dokumentierte Richtlinien für den Umgang mit Sicherheitsvorfällen. Er hilft Unternehmen, sich auf Sicherheitsvorfälle vorzubereiten und Wiederherstellungsmaßnahmen festzulegen (Farok & Zolkipli, 2024). Dabei muss er neben den potenziellen Arten von Vorfällen, denen die Organisation ausgesetzt ist, auch beschreiben, was zu tun ist, wenn ein neuer und unerwarteter Vorfall auftritt. Außerdem enthält der IRP Angaben zur Konsultation externer Stellen bei Eintreten eines Sicherheitsvorfalls (vgl. Nayak & Rao, 2014, S. 89).

2.1.2 Incident-Response-Prozess

Aus einem IRP leiten sich konkrete Incident-Response-Prozesse ab. Bevorstehende, vermutete, laufende oder bereits abgeschlossene Angriffe bilden den Ausgangspunkt für verschiedene sicherheitsrelevante Maßnahmen, die im Rahmen dieser Prozesse durchgeführt werden. Die spezifische Gestaltung variiert je nach Organisation, da die Prozesse oft an individuelle Anforderungen angepasst werden. In der Regel sind diese Prozesse in verschiedene Phasen unterteilt, die schrittweise durchlaufen werden (siehe Kapitel 3) (Amoroso, 2011; Maras et al., 2021).

2.1.3 Lebenszyklus einer Incident Response

Die einzelnen Phasen eines Incident-Response-Prozesses bilden zeitgleich ihren Lebenszyklus ab. Es ist wichtig zu erwähnen, dass eine Incident Response nicht erst mit dem Eintreten eines Sicherheitsvorfalls beginnt. Schon lange bevor eine Bedrohung eintritt, beginnt der Lebenszyklus mit der Erstellung einer Incident-Response-Policy, Mitarbeiterschulungen und umfassenden Risikobewertungen (Nayak & Rao, 2014).

2.1.4 Incident Response Team (IRT)

Komplexität und Bandbreite möglicher Bedrohungen in der Informationssicherheit steigen stetig an und erfordern den Aufbau geeigneter *Incident Response Teams (IRTs)*, die maßgeblich zum Erfolg einer effektiven und effizienten Incident Response beitragen. Entsprechend wichtig ist die Auswahl der einzelnen Teammitglieder, damit ausreichend Wissen, Erfahrung und Fähigkeiten zur Erkennung, Eindämmung und Beseitigung von Sicherheitsvorfällen zur Verfügung stehen. Verschiedene Faktoren müssen beachtet werden, wenn es um die Auswahl einer geeigneten Teamstruktur geht, wobei grundsätzlich folgende Strukturen denkbar sind (nach Nayak und Rao, 2014):

- **Zentralisiertes IRT**: Aufbau eines IRT an einem einzelnen Standort. Sinnvoll bei kleineren Unternehmen, die geografisch nicht weit verteilt sind.
- **Dezentrale IRTs**: Aufbau verschiedener lokaler IRTs an mehreren Standorten. Nützlich für Unternehmen, die geografisch verteilt sind oder mehrere Unternehmen unter einem Dach haben.
- **Hybride IRTs**: Kombination beider Teamstrukturen. Ein zentrales Team mit weitreichender Expertise kann lokalen, oft weniger komplexen Teams bei entsprechenden Vorfällen zuarbeiten.

Teams können ausschließlich intern, vollständig ausgelagert oder durch eine Kombination interner und externer Experten besetzt sein. Die genaue Zusammenstellung hängt auch hier wieder von einigen Faktoren ab, wobei vor allem kleine mittelständische Unternehmen aufgrund des hohen Aufwands beim Aufbau eigener Expertise vorrangig auf externe Teamstrukturen setzen (Nayak & Rao, 2014).

2.2 Notfallmanagement & Business Continuity Management

„Das Notfallmanagement ist ein Managementprozess mit dem Ziel, gravierende Risiken für eine Institution, die das Überleben gefährden, frühzeitig zu erkennen und Maßnahmen dagegen zu etablieren“ (Bundesamt für Sicherheit in der Informationstechnik [BSI], 2008, S. 1). Es umfasst damit nicht nur Bereiche der IT-Sicherheit, sondern stellt etwa auch physische Risiken in den Fokus.

Im Gegensatz zur Incident Response zielt das Notfallmanagement darauf ab, „sicherzustellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz der Institution auch bei einem größeren Schadensereignis gesichert bleibt“ (BSI, 2008, S. 1). Der Schwerpunkt liegt somit insbesondere auf präventiven Maßnahmen, um einen möglichst unterbrechungsfreien Betrieb zu gewährleisten, während die Incident Response einen stärker reaktiven Ansatz verfolgt. Das Notfallmanagement wird daher auch als *Business Continuity Management (BCM)* bezeichnet (BSI, 2023).

3 Phasen der Incident Response

Trotz der teilweise unterschiedlichen Ausprägungen von IRPs in verschiedenen Organisationen weisen die zugrunde liegenden Prozesse oft eine ähnliche Struktur auf. Zwei bekannte Incident-Response-Frameworks bieten eine Vielzahl an Elementen, die häufig Anwendung finden: der *Computer Security Incident Handling Guide* des *National Institute of Standards and Technology (NIST)* und das *Incident Handler's Handbook* des *SysAdmin, Audit, Network, and Security (SANS)*-Instituts (Maras et al., 2021).

Notfallmanagement-Prozess

Auch das Notfallmanagement enthält einen strukturierten Prozess zur Behandlung von Vorfällen. Typischerweise umfasst es die Phasen Initiierung, Konzeption, Umsetzung des Notfallvorsorgekonzepts, Notfallbewältigung, Tests & Übungen sowie die Aufrechterhaltung und kontinuierliche Verbesserung des Prozesses (BSI, 2008). Im modernen BCM wird dieser Prozess zunehmend in die vier Phasen des *Plan-Do-Check-Act (PDCA)-Zyklus* überführt, wodurch eine zyklische Optimierung gewährleistet wird. Diese Einteilung orientiert sich grundsätzlich an den etablierten Phasen des traditionellen Notfallmanagements (BSI, 2023).

3.1 Vorbereitung (*Preparation*)

In der *Preparation*- oder *Pre-Planning*-Phase geht es darum, sicherzustellen, dass alle notwendigen Prozesse, Teams und Kommunikationswege vorhanden sind, um im Falle eines Sicherheitsvorfalls effektiv zu reagieren. Dies umfasst neben der Erstellung einer Incident-Response-Policy und der Einrichtung eines Notfallteams auch die Entwicklung von Richtlinien, Verfahren und Ressourcen sowie die Durchführung von Schulungen und Übungen (Farok & Zolkipli, 2024; Maras et al., 2021).

3.1.1 Priorisierung

Ein wichtiger Bestandteil der Vorbereitungsphase ist die Priorisierung der zu schützenden Werte (*Assets*), wie zum Beispiel Infrastruktur, Software oder auch Wissen und geistiges Eigentum. Es muss außerdem festgelegt werden, in welcher Reihenfolge einzelne Systeme bei einem Sicherheitsvorfall wiederhergestellt werden. Darüber hinaus erfolgt eine Priorisierung potenzieller Sicherheitsvorfälle, nachdem diese identifiziert und klassifiziert wurden. Dies erfolgt durch die Kombination der beiden Hauptparameter Auswirkung (*Impact*) und Dringlichkeit (*Urgency*) (Maras et al., 2021).

3.1.2 Entwicklung von Standards, Rollen und Verantwortlichkeiten

Auf Basis der entwickelten Priorisierung wird ein *Standard Operating Procedure (SOP)* erstellt. Es enthält Richtlinien, Checklisten und Formulare für die Erfassung und den

Umgang mit Sicherheitsvorfällen. Dadurch wird eine einheitliche und effiziente Reaktion auf mögliche Bedrohungen sichergestellt (Maras et al., 2021).

Im nächsten Schritt werden IRTs definiert und festgelegt, welche Personen in welchen Situationen zuständig sind. Hierzu werden Verantwortlichkeiten definiert, beispielsweise in der Erkennung und Analyse von Bedrohungen, der Entscheidung über die anzuwendenden Gegenmaßnahmen, der Kommunikation mit internen und externen Stellen sowie der Dokumentation und Nachbereitung (Maras et al., 2021).

3.2 Erkennung (*Detection*) & Analyse (*Analysis*)

Security Information and Event Management (SIEM)-Systeme, *Intrusion Detection Systems (IDSs)* und *Data Loss Prevention (DLP)*-Software kommen in der ersten Phase zum Einsatz, um eine potenzielle Bedrohung zu identifizieren. Hierzu werden Logs, Warnmeldungen und verdächtige Aktivitäten analysiert. Gleichzeitig wird die Schwere des Vorfalls bewertet, um geeignete Maßnahmen zur Eindämmung, Behebung und Wiederherstellung abzuleiten. Ziel ist es, Schäden und Kosten so gering wie möglich zu halten (Farok & Zolkipli, 2024; Maras et al., 2021; Thompson, 2018).

3.3 Eindämmung (*Containment*)

Im nächsten Schritt geht es primär darum, die Auswirkungen des Vorfalls zu begrenzen und eine weitere Ausbreitung zu verhindern. Dies ist essenziell, um Schäden zu minimieren. Die dabei eingesetzten Maßnahmen können entweder auf eine kurzfristige oder eine langfristige Eindämmung abzielen (Maras et al., 2021).

Die kurzfristige Eindämmung dient der schnellen Isolation betroffener Systeme oder Konten, um eine unmittelbare Schadensbegrenzung zu ermöglichen. Sie erfordert eine schnelle Reaktion, um weitere Beeinträchtigungen zu verhindern. Im Gegensatz dazu liegt der Fokus der langfristigen Eindämmung auf der Stabilisierung der Systeme und der Vorbereitung auf die Wiederherstellung, wodurch sie einen eher strategischen Charakter erhält (Farok & Zolkipli, 2024; Maras et al., 2021).

Zu den Maßnahmen der kurzfristigen Eindämmung zählt beispielsweise die Trennung betroffener Systeme vom Netzwerk oder die Sperrung kompromittierter Konten und Dienste. Eine langfristige Eindämmung kann unter anderem durch das Blockieren schädlichen Datenverkehrs erfolgen (Maras et al., 2021).

3.4 Beseitigung (*Eradication*)

Nach der Eindämmung folgt die Beseitigung der Bedrohung, wobei der Schwerpunkt auf der Entfernung der Ursache des Sicherheitsvorfalls liegt. Dies umfasst unter anderem die Identifikation und Löschung von Malware oder schädlichen Skripten. Falls der

Angriff durch Sicherheitslücken ermöglicht wurde, müssen diese im Rahmen der *Eradication* geschlossen werden. Abschließend werden alle betroffenen Systeme auf Spuren des Angriffs überprüft, um sicherzustellen, dass keine akute Bedrohung mehr besteht (Maras et al., 2021).

3.5 Wiederherstellung (*Recovery*)

In der Wiederherstellungsphase werden betroffene Systeme wieder in Betrieb genommen. Falls erforderlich, kommen Redundanzmechanismen wie Backups zum Einsatz. Zudem erfolgt eine abschließende Prüfung, um sicherzustellen, dass der Vorfall vollständig behoben ist und die Systeme ordnungsgemäß funktionieren. Vor der Rückkehr in den produktiven Betrieb werden Tests durchgeführt, um die Stabilität der Systeme zu gewährleisten (Maras et al., 2021).

Bereits in dieser Phase findet eine erste Analyse der getroffenen Maßnahmen statt. Diese dient der kontinuierlichen Verbesserung und erfordert die Einbindung aller relevanten Stakeholder sowie betroffener Personen und Interessengruppen (Maras et al., 2021).

3.6 Präventive Maßnahmen (*Lessons Learned*)

Diese Phase dient der systematischen Auswertung des Vorfalls, um präventive Maßnahmen abzuleiten und zukünftige Sicherheitsvorfälle zu verhindern oder zumindest unwahrscheinlicher zu machen. Dazu wird der Vorfall detailliert analysiert, indem Abläufe rekonstruiert, Ursachen erforscht und die getroffenen Maßnahmen bewertet werden (Farok & Zolkipli, 2024; Maras et al., 2021). Mögliche Fragestellungen, die dabei untersucht werden, sind (nach Maras et al., 2021):

- Wann und wie trat der Vorfall auf?
- Wie effektiv hat das IRT reagiert?
- Wurden Prozesse und Vorgaben eingehalten?
- Welche Maßnahmen waren erfolgreich, welche nicht?
- Welche Änderungen sind erforderlich, um ähnliche Vorfälle in Zukunft zu verhindern?

Auf Basis der gewonnenen Erkenntnisse werden Strategien zur Verbesserung des Incident-Response-Prozesses und zur Stärkung der Sicherheitsmaßnahmen entwickelt. Eine umfassende Dokumentation des Vorfalls ermöglicht es, bestehende Richtlinien und Verfahren zu optimieren sowie technische und organisatorische Schutzmaßnahmen anzupassen. Dazu gehören unter anderem gezielte Schulungen und Awareness-Maßnahmen für Mitarbeitende (Farok & Zolkipli, 2024; Maras et al., 2021).

4 Incident Response in der Praxis

Nachfolgend werden zwei Fallstudien vorgestellt, um den praktischen Nutzen und die Anwendung realer Incident-Response-Prozesse zu verdeutlichen.

4.1 Fallstudie: Finanzunternehmen

Ein global agierendes Finanzunternehmen mit über 20.000 Mitarbeitenden und Millionen Kund*innen hat umfangreiche IRPs implementiert, um die Sicherheit der Daten zu gewährleisten und regulatorischen Anforderungen nachzukommen. Das *Network Incident Response Team (NIRT)* als Teil des *Information Security Departments* ist für Netzwerksicherheit, proaktive Tests und die Behebung von Sicherheitsvorfällen zuständig; ein *High-Impact Incident Response Coordination Team (HIRCT)* koordiniert schwerwiegende Vorfälle und erstellt *Post-Incident Reports (PIRs)* (Ahmad et al., 2012).

4.1.1 Incident-Response-Prozess

Low-Impact-Vorfälle werden direkt vom NIRT bearbeitet, wobei der Fokus auf einer schnellen Problemlösung liegt, während eine umfassende Ursachenanalyse in den Hintergrund tritt. In diesem Kontext werden hauptsächlich technische Details dokumentiert, während strategische Erkenntnisse eine untergeordnete Rolle spielen. Kritische Vorfälle hingegen fallen in den Zuständigkeitsbereich des HIRCT, das den Vorfall umfassend koordiniert und gezielt nach den Ursachen sucht. Dabei erfolgt eine enge Zusammenarbeit sowohl auf technischer Ebene – beispielsweise mit dem NIRT – als auch mit dem Management, um eine klare Kommunikation sicherzustellen. Anschließend wird der Vorfall systematisch analysiert, um Ursachen zu identifizieren und gezielte Maßnahmen zur Vermeidung künftiger Vorfälle abzuleiten (Ahmad et al., 2012).

4.1.2 *Lessons Learned*

Das NIRT verfolgt bei der Bearbeitung von Low-Impact-Vorfällen einen *Single-Loop Learning*-Ansatz, bei dem primär die direkte Beseitigung der Ursache im Vordergrund steht. Dies führt jedoch dazu, dass systemische Probleme oder strukturelle Mängel nur unzureichend untersucht werden, was die Entwicklung präventiver Maßnahmen im Rahmen der *Lessons Learned* erschwert. Im Gegensatz dazu setzt das HIRCT auf ein *Double-Loop Learning*-Modell, das Prozesse kritisch hinterfragt und strukturelle Anpassungen anstrebt. Obwohl das Team den Mehrwert detaillierter Ursachenanalysen erkannt hat, fehlt allerdings eine institutionalisierte Umsetzung. Zwar sind die erstellten PIRs äußerst ausführlich, doch mangelt es an einer geregelten Verbreitung der Berichte. Zudem erschwert die Silostruktur des Unternehmens eine effiziente Weitergabe von Erkenntnissen, wodurch wertvolle Informationen nicht optimal genutzt werden können (Ahmad et al., 2012).

4.2 Fallstudie: Emergency Communications Center (ECC)

Im Jahr 2019 wurde ein *Emergency Communications Center (ECC)* Ziel eines Malware-Angriffs, der sich auf mehrere Rechner ausbreitete und insgesamt etwa acht Stunden andauerte.

4.2.1 Incident-Response-Prozess

Ein Mitarbeiter meldete zunächst ungewöhnliches Verhalten auf seinem Rechner, das später auch auf einem zweiten Gerät festgestellt wurde. Daraufhin begann umgehend die Eindämmung des Vorfalls: Die betroffenen Rechner wurden vom Netzwerk getrennt, die Festplatten ausgebaut und mit Antivirensoftware überprüft. Dabei stellte sich heraus, dass ein Wurm Netzwerkdaten extrahierte und sie an eine ausländische *Internet Protocol (IP)*-Adresse übermittelte (Cybersecurity and Infrastructure Security Agency [CISA], 2021).

Im Zuge der Wiederherstellung mussten alle betroffenen Computer vollständig gelöscht und neu aufgebaut werden. Zwar führte das ECC tägliche Backups aller Rechner durch, doch diese umfassten nur Festplattendaten – nicht jedoch Betriebssysteme. Daher mussten externe Anbieter die Systeme neu installieren, was den Wiederherstellungsprozess auf etwa einen Monat verlängerte (CISA, 2021).

4.2.2 *Lessons Learned*

Der Vorfall führte im Rahmen der *Lessons Learned* zur Identifikation verschiedener Präventionsmaßnahmen (nach CISA, 2021):

- **Regelmäßige Backups**: Neben Nutzerdaten müssen auch Betriebssysteme gesichert werden, um eine schnelle Wiederherstellung zu ermöglichen.
- **Schulungen**: Mitarbeiterschulungen sind essenziell, um sicheres Verhalten im Internet zu fördern und das Risiko von Malware-Infektionen zu minimieren.
- **Netzwerksegmentierung**: Die Aufteilung des Netzwerks in Subnetze kann die Ausbreitung von Malware erheblich einschränken.
- **Notfallpläne**: Unternehmen sollten Notfallpläne für Cyberangriffe entwickeln und regelmäßig aktualisieren.
- **Zusammenarbeit mit Versicherungen**: Eine enge Abstimmung mit Cyber-Versicherern kann helfen, die finanziellen Folgen eines Angriffs zu bewältigen.

5 Herausforderungen & Best Practices

Jeder noch so durchdachte und sorgfältig ausgearbeitete Prozess bietet Potenzial für Verbesserungen. Nachfolgend werden einige Aspekte benannt, die bei der Entwicklung und Durchführung einer erfolgreichen Incident Response herausfordernd, aber im Rahmen einiger Best Practices auch erfolgversprechend sein können.

5.1 Balance zwischen Geschwindigkeit & Genauigkeit

Bei der Entwicklung eines IRP muss eine ausgewogene Balance zwischen schneller Wiederherstellung und umfassender Analyse gefunden werden. Dies führt zu einem strategischen Dilemma: Ein Fokus auf die rasche Wiederherstellung der Systeme ermöglicht eine schnelle Wiederaufnahme des Geschäftsbetriebs und minimiert finanzielle sowie reputative Einbußen. Allerdings kann dies eine tiefgehende (forensische) Analyse einschränken, wodurch wertvolle Spuren verloren gehen und die Möglichkeit zur Erarbeitung präventiver Maßnahmen verringert wird. Eine umfassende Analyse hingegen bietet den Vorteil, Täter zu identifizieren und zukünftige Angriffe zu verhindern. Sie kann jedoch den gesamten Wiederherstellungsprozess erheblich verzögern und dadurch potenziell größeren Schaden verursachen (Maras et al., 2021).

Best Practice: Unterschiedliche Prozesse durch Klassifikation des Vorfalls

Fallstudie 1 (siehe Abschnitt 4.1) verdeutlicht, wie dieser anspruchsvolle Designansatz erfolgreich umgesetzt werden kann. Durch die Klassifikation in Low-Impact- und High-Impact-Vorfälle sowie die daraus resultierenden differenzierten Incident-Response-Prozesse wird sichergestellt, dass weniger kritische Vorfälle den Geschäftsbetrieb minimal beeinträchtigen, während bei schwerwiegenden Vorfällen der Fokus auf einer umfassenden Analyse und Prävention liegt.

5.2 Frühzeitige Erkennung von Vorfällen

Um das Ausmaß einer potenziellen Bedrohung so gering wie möglich zu halten, ist eine frühzeitige Erkennung von Sicherheitsvorfällen entscheidend. Die zentrale Herausforderung besteht darin, eine Bedrohung als solche zu identifizieren. Gelingt dies nicht oder kommt es in der frühen Phase des Vorfalls zu Verzögerungen oder Fehlern, kann dies die Effektivität der Reaktion erheblich beeinträchtigen (Thompson, 2018).

Best Practice: Dokumentierte Prozesse zur Erstbewertung eines Vorfalls

Dokumentierte Prozesse (*Playbooks*) zur Erstbewertung von Vorfällen tragen dazu bei, den kritischen Zeitpunkt der Erkennung erheblich zu verkürzen. Sie ermöglichen eine schnelle und koordinierte Untersuchung, unabhängig vom zunächst un-

bekannten Schweregrad der Bedrohung. Zudem helfen sie dabei, Alarmmeldungen korrekt einzuordnen und notwendige Eskalationen ohne Verzögerung einzuleiten. Durch definierte Abläufe wird darüber hinaus vermieden, dass Warnungen ignoriert oder falsch gehandhabt werden (Thompson, 2018).

5.3 Klare Rollenverteilung & Zuständigkeiten

Beim Auftreten eines Sicherheitsvorfalls ist es essenziell, dass jedes Mitglied eines IRT eine klar definierte Rolle mit spezifischen Aufgaben hat. Unabhängig von der Teamstruktur kann das Fehlen eindeutiger Zuständigkeiten schnell zu unkoordinierten und ineffektiven Reaktionen führen, die möglicherweise nicht mit dem IRP übereinstimmen (Thompson, 2018).

Best Practice: Regelmäßige Evaluation von Rollen & Zuständigkeiten

Durch regelmäßige Übungen und Diskussionen sollte das Rollenverständnis kontinuierlich geschärft werden. Es ist entscheidend, die Notwendigkeit der Einhaltung festgelegter Maßnahmen zu verdeutlichen und nach einem Vorfall in Form von Nachbesprechungen eine erneute Bewertung der Rollen und Zuständigkeiten vorzunehmen (Thompson, 2018).

5.4 Gemeinsames Verständnis auf allen Geschäftsebenen

Die Effektivität der Incident Response hängt maßgeblich davon ab, dass auf allen Geschäftsebenen ein gemeinsames Verständnis für die Bedeutung und Priorität eines funktionierenden IRP besteht. Wird Incident Response von der Führungsebene lediglich als Kostenfaktor oder notwendiges Übel betrachtet, kann selbst ein sorgfältig ausgearbeiteter Plan nur schwer erfolgreich umgesetzt werden (Thompson, 2018).

Best Practice: Jährliche Tests & Bereitstellung notwendiger Ressourcen

Die oberste Führungsebene muss Incident Response als integralen Bestandteil der Unternehmensstrategie anerkennen und mit den notwendigen Ressourcen sowie dem erforderlichen Engagement unterstützen. Jährliche Tests und Abhilfemaßnahmen dienen nicht nur der Reaktionsvorbereitung, sondern sind auch von Aufsichtsbehörden und Wirtschaftsprüfern anerkannte Maßnahmen zur Implementierung eines umfassenden Sicherheitskonzepts auf allen Geschäftsebenen. Dies fördert zudem die Akzeptanz innerhalb der gesamten Organisation (Thompson, 2018).

6 Zusammenfassung

6.1 Ergebnisse

Trotz aller Herausforderungen ist die Incident Response ein unverzichtbares und wirksames Mittel im Kampf gegen Cyberangriffe. Mithilfe durchdachter Prozesse und umfassender Konzepte können Unternehmen den Schaden zunehmend komplexer Attacken erheblich reduzieren.

6.1.1 Der Lebenszyklus einer Incident Response

Cyberangriffe sind komplex und werden in Zukunft noch weitaus größere Ausmaße annehmen. Eine effektive Abwehrstrategie ist daher unverzichtbar, um Unternehmen finanziell und reputativ vor erheblichem Schaden zu bewahren. Die Incident Response setzt genau dort an: Mit ihren einzelnen Phasen beschreibt sie den gesamten Zyklus der Reaktion auf eine Bedrohung – von der Vorbereitung über die Beseitigung und Wiederherstellung bis hin zur Entwicklung präventiver Maßnahmen. Unternehmen mit gut aufgestellten Incident Response Teams (IRTs) und effektiven Incident Response Plans (IRPs) sollten in der Lage sein, Bedrohungen zu bewältigen, geeignete Maßnahmen einzuleiten und sich für zukünftige Vorfälle besser zu wappnen.

Incident Response, Notfallmanagement und das modernere Business Continuity Management (BCM) haben eine gemeinsame Grundlage: strukturierte Prozesse und wiederkehrende Elemente, die in konkrete Notfallpläne und Strategien überführt werden können. Diese Prozesse sind häufig an spezifische Anwendungsfälle eines Unternehmens angepasst. Frameworks wie der *Computer Security Incident Handling Guide* des NIST bieten jedoch wiederverwendbare Strukturen, die insbesondere bei der Integration neuer Teammitglieder von Vorteil sind.

6.1.2 *Lessons Learned* als fundamentale Präventionsstrategie

Die abschließende Phase eines Incident-Response-Prozesses ist essenziell, da hier eine bewältigte Bedrohung noch einmal umfassend analysiert wird. Im Rahmen der *Lessons Learned* wird dokumentiert, inwieweit bestehende Prozesse verbessert werden können, um auf zukünftige Bedrohungen besser vorbereitet zu sein. Prävention steht hierbei im Mittelpunkt: Die gewonnenen Erkenntnisse ermöglichen eine fundierte Bewertung, welche Aspekte ergänzt und welche Strategien optimiert werden müssen. Beide in Kapitel 4 dargestellten Fallstudien verdeutlichen die zentrale Rolle dieser Reflexion für die Weiterentwicklung von Cyberstrategien.

6.1.3 Incident Response im Kontext der Business Continuity

Unternehmen haben ein fundamentales Interesse an der Aufrechterhaltung ihrer Geschäftstätigkeit. Jeder Ausfall – auch unabhängig von Cyberbedrohungen – kann zu erheblichen finanziellen und reputativen Schäden führen. Daher ist ein effektives BCM für Unternehmen unerlässlich. Da Notfallmanagement und BCM nicht primär auf die Abwehr von Cyberangriffen ausgerichtet sind, können sie durch Incident Response sinnvoll ergänzt werden. Der Aufbau von IRTs und IRPs verdeutlicht die Bedeutung der Cyberabwehr im Kontext der Business Continuity und stärkt die Notfallstrategie eines Unternehmens erheblich.

6.2 Ausblick

Künstliche Intelligenz (KI) und *Maschinelles Lernen (ML)* bieten auch im Bereich der Incident Response und des BCM wirksame Mittel zur Abwehr von Cyberangriffen und zur Aufrechterhaltung des Geschäftsbetriebs. KI-gestützte Systeme verbessern die Angriffserkennung und reduzieren die Anzahl von False-Positive-Meldungen. Ali et al. (2025) zeigen in ihrer Studie, dass ML-Modelle die bisher überwiegend manuell durchgeführten Analysen durch einen automatisierten Prozess mit einer Treffergenauigkeit von 99,6 % erheblich verbessern können. Durch diese automatisierte, KI-gestützte Angriffserkennung, die sich in bestehende Sicherheitslösungen integrieren lässt, können Incident-Response-Mechanismen optimiert, Entscheidungsprozesse beschleunigt und False Positives weiter minimiert werden.

Zusätzlich unterstreichen Naseer et al. (2023) in ihrer Feldstudie die Relevanz von *Big Data Analytics (BDA)* für die Incident Response. Sie heben hervor, dass die Nutzung großer Datenmengen die Agilität erhöht und eine schnellere Reaktion auf Sicherheitsvorfälle ermöglicht. Die Autor*innen schlagen zudem vor, fortgeschrittene Analyseansätze wie *Advanced Analytics* und *Pervasive Analytics* in die Incident Response zu integrieren, um eine proaktive Reaktion zu fördern und Lernprozesse innerhalb von IRTs zu verbessern.

Incident Response, Notfallmanagement und BCM werden auch in Zukunft eine zentrale Rolle bei der Bewältigung von Cyberbedrohungen spielen. Zunehmend komplexere Angriffsmethoden erfordern die kontinuierliche Weiterentwicklung und Optimierung bestehender Prozesse. Unternehmen sollten daher aktuelle Trends stets im Blick behalten und ihre Strategien fortlaufend anpassen, um auch künftigen Bedrohungen effektiv begegnen zu können.

Literaturverzeichnis

Ahmad, A., Hadgkiss, J., & Ruighaver, A. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security*, *31*(5), 643–652.

Ali, G., Shah, S., & ElAffendi, M. (2025). Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection. *Results in engineering*, *25*.

Amoroso, E. G. (2011). 11 - Response. In E. G. Amoroso (Hrsg.), *Cyber Attacks* (S. 193–206). Butterworth-Heinemann.

Bundesamt für Sicherheit in der Informationstechnik. (2008). *Notfallmanagement* (Techn. Ber. Nr. BSI-Standard 100-4) (Version 1.0). Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2023). *Business Continuity Management* (Techn. Ber. Nr. BSI-Standard 200-4). Bonn. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf

Cybersecurity and Infrastructure Security Agency. (2021). Malware Attacks: Lessons Learned from an Emergency Communications Center [Online; abgerufen am 10. März 2025]. https://www.cisa.gov/sites/default/files/publications/22_0414_cyber_incident_case_studies_malware_final_508c.pdf

Farok, N. A. Z., & Zolkipli, M. F. (2024). Incident response planning and procedures. *Borneo International Journal eISSN 2636-9826*, *7*(2), 69–76.

Maras, M.-H., Maras, M.-H., & Shapiro, L. R. (2021). Cybersecurity: Incident Response. In *Encyclopedia of Security and Emergency Management* (S. 197–203). Springer International Publishing.

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. *Computers & security*, *135*.

Nayak, U., & Rao, U. H. (2014). *The InfoSec Handbook*. Apress.

Statistisches Bundesamt. (2024a). Ausgaben für IT-Sicherheit in Deutschland in den Jahren 2017 bis 2023 und Prognose bis 2024 [Online; abgerufen am 11. März 2025]. https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/

Statistisches Bundesamt. (2024b). Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland von 2007 bis 2023 [Online; abgerufen am 11. März 2025]. https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/

Statistisches Bundesamt. (2024c). Schadenssumme durch Cyberattacken in Milliarden Euro in den Jahren 2023 und 2024 [Online; abgerufen am 11. März 2025]. https://de.statista.com/statistik/daten/studie/1546525/umfrage/schaeden-durch-cyberattacken-nach-jahren/

Thompson, E. C. (2018). *Cybersecurity Incident Response*. Apress.

Eigenständigkeitserklärung

Ich trage die Verantwortung für die Qualität des Textes sowie die Auswahl aller Inhalte und habe sichergestellt, dass Informationen und Argumente mit geeigneten wissenschaftlichen Quellen belegt bzw. gestützt werden. Die aus fremden Quellen direkt oder indirekt übernommenen Texte, Gedankengänge, Konzepte, Grafiken usw. in meinen Ausführungen habe ich als solche eindeutig gekennzeichnet und mit vollständigen Verweisen auf die jeweilige Quelle versehen. Alle weiteren Inhalte dieser Arbeit (Textteile, Abbildungen, Tabellen etc.) ohne entsprechende Verweise stammen im urheberrechtlichen Sinn von mir.

Hiermit erkläre ich, dass ich die vorliegende Studienarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle sinngemäß und wörtlich übernommenen Textstellen aus fremden Quellen wurden kenntlich gemacht.

Die vorliegende Arbeit wurde bisher weder im In- noch im Ausland in gleicher oder ähnlicher Form einer anderen Prüfungsbehörde vorgelegt.

Erklärung zu (gen)KI-Tools

Verwendung von (gen)KI-Tools

Ich versichere, dass ich mich (gen)KI-Tools lediglich als Hilfsmittel bedient habe und in der vorliegenden Arbeit mein gestalterischer Einfluss überwiegt. Ich verantworte die Übernahme jeglicher von mir verwendeter Textpassagen vollumfänglich selbst. In der Übersicht verwendeter (gen)KI-Tools habe ich sämtliche eingesetzte (gen)KI-Tools, deren Einsatzform sowie die jeweils betroffenen Teile der Arbeit einzeln aufgeführt. Ich versichere, dass ich keine (gen)KI-Tools verwendet habe, deren Nutzung der Prüfer bzw. die Prüferin explizit schriftlich ausgeschlossen hat.

Hinweis: Sofern die zuständigen Prüfenden bis zum Zeitpunkt der Ausgabe der Aufgabenstellung konkrete (gen)KI-Tools ausdrücklich als nicht anzeige-/kennzeichnungspflichtig benannt haben, müssen diese nicht aufgeführt werden.

Ich erkläre weiterhin, dass ich mich aktiv über die Leistungsfähigkeit und Beschränkungen der unten genannten (gen)KI-Tools informiert habe und überprüft habe, dass die mithilfe der genannten (gen)KI-Tools generierten und von mir übernommenen Inhalte faktisch richtig sind.

Übersicht verwendeter (gen)KI-Tools

Die (gen)KI-Tools habe ich, wie im Folgenden dargestellt, eingesetzt.

(gen)KI-Tool	**Einsatzform**	**Betroffene Teile der Arbeit**
ChatGPT	Generierung von ersten Ideen für eine geeignete Gliederung	Gesamte Arbeit
	Generierung von Zusammenfassungen verschiedener Literaturwerke	Gesamte Arbeit

Münster, 12. März 2025

Elias Häußler