FOM Hochschule für Oekonomie & Management
Hochschulzentrum Nürnberg

IT-Infrastruktur

WS 2024 im Studiengang Wirtschaftsinformatik

über das Thema

Cybersecurity in der IT-Infrastruktur: Moderne Bedrohungen und Schutzmaßnahmen

von

Eray Yasar: 740108

Inhaltsverzeichnis

1 Einleitung

1.1 Hinführung zum Thema

Die zunehmende Digitalisierung und die stetig wachsende Vernetzung von IT-Systemen haben die Abhängigkeit sicherer IT-Infrastrukturen signifikant gesteigert. Besonders Unternehmen setzen vermehrt auf moderne Technologien wie Cloud Computing, das Internet der Dinge (IoT) und künstliche Intelligenz (KI), um ihre Geschäftsprozesse effizienter ausarbeiten zu können (vgl. Pohlmann 2022: 2, 52-53). Mit diesen technologischen Fortschritten geht jedoch eine Vielzahl an Sicherheitsrisiken einher.

Cyberangriffe wie Ransomware, Zero-Day-Exploits oder Supply-Chain-Attacken sind in den letzten Jahren stark angestiegen und stellen eine ernstzunehmende Gefahr für Unternehmen und öffentliche Institutionen dar (vgl. ebd.: 2-3). Besonders betroffen sind kritische Infrastrukturen wie der Finanzsektor oder das Gesundheitswesen. Diese bieten aufgrund ihrer sensiblen Daten und zentralen Bedeutung ein verlockendes Ziel für potenzielle Angreifer.

Angesichts dieser Bedrohungen zeigt sich, dass Cybersecurity nicht nur eine technische, sondern sich zusätzlich auch als eine strategische Herausforderung darstellt. Unternehmen sind gezwungen ihre Sicherheitsmaßnahmen kontinuierlich weiterzuentwickeln und anzupassen, um den immer komplexer werdenden Angriffstechniken effektiv begegnen zu können (vgl. Pufahl et al. 2024: 2).

1.2 Forschungsfragen

Diese Arbeit befasst sich mit den zentralen Herausforderungen und Schutzmaßnahmen der Cybersecurity in der IT-Infrastruktur. Folgende Forschungsfragen stehen im Fokus:

1. Welche aktuellen Bedrohungen gefährden die Sicherheit moderner IT-Infrastrukturen?
2. Wie können Unternehmen ihre Sicherheitsstrategien verbessern, um aktuellen Bedrohungen zu begegnen?
3. Welche Rolle spielen KI und Automatisierung bei der Abwehr von Cyberbedrohungen?
4. In welchem Maße beeinflussen menschliche Faktoren die Sicherheit moderner IT-Infrastrukturen?

Durch die Beantwortung dieser Fragen soll ein fundierter Überblick über aktuelle Cybersecurity-Entwicklungen sowie effektive Schutzmechanismen gegeben werden.

1.3 Relevanz der Arbeit

Die Relevanz dieser Arbeit ergibt sich aus der steigenden Anzahl und Komplexität von Cyberangriffen, die sowohl finanzielle als auch operationale Schäden verursachen. Besonders mittelständische Unternehmen und kritische Infrastrukturen stehen vor enormen Herausforderungen bei der Sicherung ihrer IT-Systeme (vgl. Pohlmann 2022: 636).

Neben wirtschaftlichen Risiken spielen auch gesetzliche Vorschriften wie die EU-Datenschutz-Grundverordnung (DSGVO) eine entscheidende Rolle. Unternehmen müssen ihre IT-Sicherheitsstrategien kontinuierlich anpassen, um den steigenden Anforderungen gerecht zu werden.

Diese Arbeit stellt einen wissenschaftlichen Überblick über moderne Cyberbedrohungen und Schutzmaßnahmen dar und gibt praxisnahe Empfehlungen zur Verbesserung der IT-Sicherheit.

1.4 Methodik

Um die in dieser Arbeit gestellten Forschungsfragen zu beantworten, wurde eine gründliche Literaturrecherche durchgeführt. Wissenschaftliche Quellen bilden die Grundlage, wobei SpringerLink als wichtigste Datenbank zur Suche relevanter Fachliteratur genutzt wurde. Die Arbeit kombiniert theoretische Ansätze mit praktischen Beispielen, um ein strukturiertes Gesamtbild über die Cybersecurity in IT-Infrastrukturen zu ermöglichen.

Die Analyse von KI-basierten Sicherheitsstrategien hat einen besonderen Schwerpunkt in dieser Arbeit. Ihr verstärkter Einsatz spielt eine ausschlaggebende Rolle bei der Erkennung und Abwehr von Cyberangriffen. Außerdem werden rechtliche Vorgaben und branchenspezifische Sicherheitsrichtlinien betrachtet, um die Herausforderungen in der Cybersecurity besser zu verstehen.

2 Grundlagen der Cybersecurity in der IT-Infrastruktur

2.1 Definition und Bedeutung von Cybersecurity

Cybersecurity, auch als Cybersicherheit bezeichnet, umfasst alle Maßnahmen zum Schutz von Informations- und Kommunikationstechnologien (IKT), sowie der darin verarbeiteten Daten. Es hat den Zweck, deren Vertraulichkeit, Integrität und Verfügbarkeit vor Bedrohungen zu schützen (vgl. Pohlmann 2022: 2-3).

Grund für diese Bedrohungen können Aspekte wie technische Störungen, menschliches Fehlverhalten oder gezielte Angriffe sein. Die stetig wachsende Digitalisierung und Vernetzung in beinahe allen Lebensbereichen resultieren in einer erhöhten Abhängigkeit von IT-Systemen. Dies führt dazu, dass sowohl Unternehmen als auch Privatpersonen anfälliger für Cyberangriffe werden, die in erheblichen wirtschaftlichen Schäden und Vertrauensverlusten resultieren können (vgl. ebd.: 7).

Die Bedeutung von Cybersecurity erstreckt sich über den Schutz sensibler Informationen hinaus. Sie stellt sicher, dass kritische Infrastrukturen wie Energieversorgung, Gesundheitswesen und Finanzsysteme vor Cyberangriffen geschützt sind. Zudem bildet sie die Grundlage für das Vertrauen in digitale Technologien und ist somit essenziell für die erfolgreiche digitale Transformation von Wirtschaft und Gesellschaft.

Die weitergehende Implementierung digitaler Technologien erfordert daher robuste Sicherheitskonzepte, die sowohl vorbeugende als auch abwehrende Strategien umfassen. Nur eine regelmäßige Anpassung und Verbesserung dieser Schutzmechanismen gewährleistet die langfristige Widerstandsfähigkeit von IT-Systemen. Daher ist ihre kontinuierliche Weiterentwicklung essenziell.

2.2 Technologische Grundlagen moderner IT-Infrastrukturen

Moderne IT-Infrastrukturen sind essenziell für die digitale Transformation von Unternehmen und bestehen aus verschiedenen Komponenten, die zusammenarbeiten, um die Speicherung, Verarbeitung und den Austausch von Daten zu ermöglichen. Zu den zentralen Bestandteilen gehören Hardware, Software, Netzwerke und Rechenzentren.

Hardware umfasst physische Geräte wie Server, Speicherlösungen und Endgeräte. Server stellen dabei zentrale Recheneinheiten dar, die Dienste und Anwendungen bereitstellen, während Speichersysteme für die sichere und dauerhafte Aufbewahrung von Daten sorgen. Endgeräte wie Computer, Tablets und Smartphones ermöglichen den Zugriff auf diese Ressourcen und die Interaktion mit den bereitgestellten Diensten.

Software bildet die Schnittstelle zwischen Hardware und Anwendern. Sie umfasst Betriebssysteme, die die grundlegende Funktionalität der Hardware steuern, sowie Anwendungen, die spezifische Aufgaben erfüllen. Besonders Virtualisierungstechnologien spielen eine entscheidende Rolle, da sie die parallele Nutzung mehrerer virtueller Maschinen auf einer physischen Hardware ermöglichen und so die Ressourcennutzung optimieren (vgl. Sharma/Singh 2025)

Netzwerke verbinden die verschiedenen Hardwarekomponenten und ermöglichen den Datenaustausch. Sie bestehen aus physischen Verbindungen wie Kabeln und drahtlosen Verbindungen sowie aus Netzwerkgeräten wie Routern und Switches, die den Datenverkehr steuern. Eine stabile Netzwerkinfrastruktur ist entscheidend für die Leistung und Zuverlässigkeit von IT-Systemen. Besonders durch Cloud-Technologien und dezentrale Architekturen hat sich die Bedeutung flexibler Netzwerklösungen in den letzten Jahren verstärkt.

Rechenzentren sind spezialisierte Einrichtungen, die eine große Anzahl von Servern und Speichersystemen beherbergen. Sie bieten die notwendige Umgebung für den Betrieb dieser Hardware, einschließlich Klimatisierung, Stromversorgung und Sicherheitsmaßnahmen. Mit dem Aufkommen von Cloud-Computing werden zunehmend virtuelle Rechenzentren genutzt, die flexible und skalierbare Ressourcen über das Internet bereitstellen. Dies ermöglicht Unternehmen eine effizientere IT-Strategie, reduziert Kosten und erhöht die Anpassungsfähigkeit an sich verändernde Geschäftsanforderungen (vgl. ebd.).

Die Integration dieser Komponenten ermöglicht es Organisationen, ihre Geschäftsprozesse zu digitalisieren und effizienter zu gestalten. Gleichzeitig erfordert die Komplexität moderner IT-Infrastrukturen ein umfassendes Management und eine kontinuierliche Überwachung, um Sicherheit, Leistung und Verfügbarkeit sicherzustellen.

2.3 Relevante Standards und gesetzliche Vorgaben

Die Gewährleistung der Sicherheit in der IT-Infrastruktur erfordert die Einhaltung spezifischer Standards und gesetzlicher Vorgaben. Diese Richtlinien dienen dazu, einheitliche Sicherheitsniveaus zu etablieren und Risiken zu minimieren. Unternehmen und Organisationen sind verpflichtet, sich an diese Vorgaben zu halten, um ihre IT-Infrastrukturen gegen Bedrohungen abzusichern und rechtlichen Anforderungen zu entsprechen (vgl. Kipker/Pfeil 2016: 810-814).

IT-Sicherheitsgesetz (IT-SiG): Das IT-Sicherheitsgesetz wurde vom Deutschen Bundestag verabschiedet und richtet sich insbesondere an Betreiber Kritischer Infrastrukturen. Es enthält Vorgaben zur Verbesserung der IT-Sicherheit, um die Verfügbarkeit, Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten. Betreiber sind verpflichtet, angemessene organisatorische und technische Vorkehrungen zu treffen, um Störungen zu vermeiden (vgl. Kipker/Pfeil 2016: 810).

DIN-Standards: Das Deutsche Institut für Normung (DIN) entwickelt Standards, die auch in der öffentlichen Verwaltung und in Unternehmen Anwendung finden. Diese Normen unterstützen dabei, Prozesse zu standardisieren und die IT-Sicherheit zu erhöhen. Ein Beispiel ist die DIN ISO/IEC 27001, die Anforderungen an Informationssicherheits-Managementsysteme (ISMS) festlegt (vgl. Edwards 2024).

NIS2-Richtlinie: Die NIS2-Richtlinie der Europäischen Union zielt darauf ab, die Cybersicherheit Kritischer Infrastrukturen zu stärken. Sie legt Sicherheitsanforderungen für Betreiber wesentlicher Dienste fest und erweitert den Anwendungsbereich im Vergleich zur vorherigen NIS-Richtlinie. Zudem betont sie die Bedeutung von Risikomanagement und Meldepflichten bei Sicherheitsvorfällen (vgl. Vogel & Ziegler 2023: 13-15).

Die Einhaltung dieser Standards und gesetzlichen Vorgaben ist für Organisationen unerlässlich, um ein hohes Maß an IT-Sicherheit zu gewährleisten und gesetzlichen Verpflichtungen nachzukommen. Sie bieten einen Rahmen für die Implementierung effektiver Sicherheitsmaßnahmen und tragen dazu bei, das Vertrauen in digitale Infrastrukturen zu stärken.

3 Moderne Bedrohungen für IT-Infrastrukturen

3.1 Neue und häufige Bedrohungsszenarien

Die zunehmende Digitalisierung und Vernetzung moderner IT-Infrastrukturen führen zu einer steigenden Anzahl an Cyberbedrohungen. Besonders gefährlich sind Ransomware-Angriffe sowie Supply-Chain-Angriffe, da sie erhebliche wirtschaftliche und operationelle Schäden verursachen können.

Ransomware ist eine Art Schadsoftware, die den Zugriff auf Systeme oder Daten sperrt, indem sie sie verschlüsselt. Anschließend werden Betroffene aufgefordert, Lösegeld zu bezahlen, um wieder Zugriff auf die Daten zu erhalten. In den letzten Jahren sind Ransomware-Angriffe immer raffinierter geworden. Angreifer nutzen oft Zero-Day-Schwachstellen, die noch nicht bekannt sind, Tricks des Social Engineerings oder Phishing, um in Netzwerke zu kommen. Ein weiteres großes Problem ist die Verbreitung von Ransomware-as-a-Service (RaaS), wo Cyberkriminelle fertige Angriffswerkzeuge an Dritte weitergeben, um am Gewinn beteiligt zu sein. Dies senkt die Einstiegshürden für Cyberkriminelle erheblich und erhöht das Risiko für Unternehmen weltweit (vgl. Rüdiger/Bayerl 2023: 513, 545-546).

Ein weiteres bedeutendes Bedrohungsszenario sind Supply-Chain-Angriffe. Hierbei kompromittieren Angreifer Drittanbieter, Dienstleister oder Softwarelieferanten, um Zugang zu den IT-Systemen der eigentlichen Zielorganisationen zu erlangen. Diese Art von Angriff nutzt das Vertrauen innerhalb der Lieferkette aus und ist oft schwer aufzuspüren. Ein besonders großes Problem tritt auf, wenn Angriffe auf Software-Updates oder Hardware-Teile durchgeführt werden, da man diese standardmäßig als sicher sieht und sie weit verbreitet sind. Unternehmen sind daher nicht nur gefordert, ihre eigenen IT-Sicherheitsmaßnahmen zu verstärken, sondern auch harte Sicherheitschecks bei ihren Lieferanten und Partnern durchführen (vgl. Pohlmann 2022: 46-47).

Die IT-Systeme werden immer komplexer, so dass Gefahren immer weiterwachsen. Unternehmen müssen daher immer ihre Sicherheitspläne auf den neuesten Stand halten, um sich gegen neue Angriffsarten zu verteidigen. Präventive Maßnahmen wie Zero-Trust-Architekturen, erweiterte Netzwerkanalysen und automatisierte Bedrohungserkennungssysteme gewinnen zunehmend an Bedeutung.

3.2 Komplexe Angriffstechniken und Schwachstellenanalyse

Moderne IT-Infrastrukturen sind zunehmend komplex und vernetzt, wodurch sich die Angriffsflächen für Cyberkriminelle erheblich erweitern. Eine der gefährlichsten Angriffstechniken ist der Zero-Day-Exploit, bei dem Sicherheitslücken in Software oder Hardware ausgenutzt werden, die noch nicht bekannt sind und für die keine Sicherheitsupdates existieren. Solche Exploits werden oft gezielt für Angriffe auf Unternehmen oder kritische Infrastrukturen genutzt, da sie von traditionellen Schutzmaßnahmen nicht erkannt werden (vgl. Parrend et al. 2018: 16).

Zero-Day-Exploits stellen eine besondere Herausforderung für herkömmliche Sicherheitslösungen dar. Signaturbasierte Antivirenprogramme und Firewalls können sie nicht identifizieren, da keine bekannten Muster vorliegen. Daher kommen zunehmend KI-gestützte Intrusion-Detection-Systeme (IDS) zum Einsatz, die durch maschinelles Lernen (ML) und Deep Learning (DL) Verhaltensanomalien analysieren und Bedrohungen frühzeitig erkennen (vgl. Salem et al. 2024: 15).

Neben Zero-Day-Exploits gewinnen auch Multi-Step-Angriffe an Bedeutung. Dabei nutzen Angreifer gestohlene Zugangsdaten oder manipulierte Systeme, um sich schrittweise im Netzwerk auszubreiten. Diese Angriffe sind schwer zu erkennen, da jeder einzelne Schritt unauffällig erscheint. Unternehmen setzen verstärkt auf KI-gestützte Analysen, um verschiedene zusammenhängende Angriffswege und verdächtige Muster aufzudecken (vgl. Parrend et al. 2018: 4).

Ein weiterer Bestandteil der Schwachstellenanalyse ist die präventive Sicherheitsbewertung. Unternehmen nutzen zum frühzeitigen Identifizieren potenzieller Angriffspunkte automatisierte Schwachstellenscanner und Threat-Intelligence-Plattformen. Penetrationstests und Red-Teaming-Simulationen helfen, Sicherheitslücken zu erkennen und gezielte Gegenmaßnahmen zu ergreifen (vgl. ebd.: 17).

3.3 Auswirkungen moderner Cyberangriffe auf Unternehmen

Cyberangriffe stellen eine zunehmende Bedrohung für Unternehmen dar und können weitreichende Konsequenzen haben. Neben den direkten finanziellen Schäden durch Betriebsunterbrechungen und Kosten für die Wiederherstellung von Systemen entstehen oft indirekte Verluste, beispielsweise durch Reputationsschäden oder rechtliche

Konsequenzen (vgl. Dreißigacker et al. 2024: 565-566). Insbesondere Ransomware-Angriffe führen häufig zu hohen Lösegeldzahlungen, während gleichzeitig Datenverluste drohen.

Ein weiteres Problem ist die steigende Prävalenz von Cyberkriminalität. Unternehmen in Deutschland berichten zunehmend über erfolgreiche Angriffe, wobei insbesondere kleine und mittelständische Betriebe (KMU) oftmals nicht über die ausreichenden Sicherheitsmaßnahmen verfügen. Die zunehmende Anzahl von Cyberangriffen auf Unternehmen macht deutlich, dass effektive Schutzmaßnahmen immer wichtiger werden (vgl. Dreißigacker et al. 2024: 604-605).

Neben finanziellen und operativen Schäden können auch gesetzliche Konsequenzen drohen. Verstöße gegen Datenschutzrichtlinien, insbesondere die DSGVO, können hohe Strafen nach sich ziehen (vgl. Bundesrechtsanwaltskammer 2023). Unternehmen müssen daher nicht nur auf technische Sicherheitsmaßnahmen setzen, sondern auch präventive Strategien wie Security Awareness Trainings und Incident-Response-Pläne nutzen, um die Auswirkungen von Cyberangriffen zu minimieren.

4 Moderne Schutzmaßnahmen für IT-Infrastrukturen

4.1 Netzwerksicherheit und Endpoint-Security in modernen Umgebungen

Die Absicherung von IT-Infrastrukturen erfordert eine umfassende Sicherheitsstrategie, die sowohl Netzwerksicherheit als auch Endpoint-Security berücksichtigt. Während die Netzwerksicherheit primär auf den Schutz der unternehmenseigenen IT-Infrastruktur abzielt, konzentriert sich die Endpoint-Security auf den Schutz einzelner Geräte, die mit dem Netzwerk verbunden sind. In modernen Arbeitsumgebungen, die vermehrt Cloud-Technologien, mobile Geräte und Remote-Arbeit integrieren, sind klassische Sicherheitsansätze nicht mehr ausreichend.

Netzwerksicherheit verbindet Maßnahmen zur Abwehr von Cyberangriffen auf IT-Netzwerke und Datenkommunikation. Unternehmen setzen hierfür Firewalls, Intrusion Detection- und Prevention-Systeme (IDS/IPS) sowie Virtual Private Networks (VPNs) ein, um Zugriffsversuche von Unbefugten zu verhindern und sichere Verbindungen zu gewährleisten (vgl. Pufahl et al. 2024: 24). Insbesondere das Zero-Trust-Sicherheitsmodell, das jeglichen Zugriff auf IT-Ressourcen zunächst verwehrt und erst nach einer Identitätsüberprüfung freigibt, gewinnt zunehmend an Bedeutung. Zero Trust

reduziert das Risiko interner und externer Angriffe, indem es strenge Zugriffskontrollen und kontinuierliche Authentifizierungsprozesse implementiert (vgl. ebd.: 72-73).

Endpoint-Security bezieht sich auf Sicherheitslösungen, welche einzelne Endgeräte wie Laptops, Smartphones und IoT-Geräte vor Cyberangriffen schützen. Der traditionelle Ansatz, der sich stark auf signaturbasierte Antivirensoftware verließ, wird zunehmend durch verhaltensbasierte Bedrohungserkennung und KI-gestützte Analysen ergänzt. Endpoint Detection and Response (EDR)-Systeme ermöglichen die Echtzeitüberwachung von Endgeräten, erkennen verdächtige Aktivitäten und isolieren automatisch potenziell gefährdete Geräte (vgl. Pufahl et al. 2024: 24, 49). Unternehmen setzen zudem auf eine Multi-Faktor-Authentifizierung (MFA) und Verschlüsselungstechnologien, um die Sicherheit sensibler Daten zu garantieren.

Die Integration von Netzwerksicherheit und Endpoint-Security ist ausschlaggebend für die Cyberresilienz eines Unternehmens (vgl. BSI 2024). Besonders im Kontext von hybriden IT-Umgebungen und der stetig wachsenden Cloud-Nutzung ist eine flexible Sicherheitsstrategie notwendig. Moderne Sicherheitskonzepte setzen auf eine Zero-Trust-Architektur, die stetig Überprüfungen und Zugriffskontrollen für alle Nutzer und Geräte innerhalb eines Netzwerks verlangt (vgl. Pufahl et al. 2024: 28-29). Unternehmen müssen ihre IT-Sicherheitsstrategien regelmäßig erneuern, um mit immer komplexer werdenden Angriffstechniken Schritt zu halten und potenzielle Schwachstellen frühzeitig zu entdecken.

4.2 Automatisierung und KI-gestützte Technologien zur Bedrohungsabwehr

Die steigende Zahl an Cyberangriffen erfordert eine Weiterentwicklung der Cybersicherheitsstrategien. Traditionelle, signaturbasierte Schutzsysteme reichen nicht mehr aus, um dynamische Bedrohungen effektiv zu erkennen. Automatisierung und künstliche Intelligenz (KI) spielen daher eine zentrale Rolle in der Bedrohungsabwehr.

Automatisierte Sicherheitsprozesse ermöglichen eine schnellere Erkennung und Abwehr von Angriffen. Systeme wie Security Orchestration, Automation, and Response (SOAR) analysieren Bedrohungen in Echtzeit und leiten automatisch Gegenmaßnahmen ein. Dies reduziert Reaktionszeiten und entlastet IT-Sicherheitsteams erheblich (vgl. Pufahl et al. 2024: 25-26).

KI-gestützte Intrusion-Detection- und Intrusion-Prevention-Systeme (IDS/IPS) sind in der Lage, netzwerkbasierte Angriffe anhand von Verhaltensmustern frühzeitig zu erkennen (vgl. ebd.: 24, 50-51). Im Gegensatz zu signaturbasierten Methoden lernen sie kontinuierlich aus neuen Angriffsdaten und verbessern so ihre Erkennungsraten (vgl. Schmitt 2023: 2). Auch in der Malware-Erkennung setzen moderne Systeme auf KI-gestützte Analysen. Anstatt auf bekannte Signaturen angewiesen zu sein, erkennen sie Bedrohungen anhand von Anomalien im Verhalten von Anwendungen und bieten so Schutz vor polymorpher Malware und Zero-Day-Exploits.

Trotz dieser Vorteile bestehen Herausforderungen, Fehlalarme, hohe Rechenanforderungen und mögliche Manipulationen durch Angreifer. Ein rein KI-basierter Schutz ist daher nicht ausreichend. Vielmehr ist eine Kombination aus regelbasierter Sicherheit, maschinellem Lernen und menschlicher Überwachung notwendig, um eine robuste Sicherheitsstrategie zu gewährleisten.

4.3 Organisatorische Maßnahmen und Best Practices für moderne Herausforderungen

Neben technischen Schutzmaßnahmen sind organisatorische Sicherheitsstrategien entscheidend, um Cyberangriffe abzuwehren und die Resilienz von Unternehmen zu stärken (vgl. Schmitt 2023). Ein zentraler Bestandteil ist die regelmäßige Sensibilisierung und Schulung der Mitarbeiter, da menschliches Fehlverhalten eine der größten Sicherheitsrisiken darstellt. Schulungen zu Phishing-Erkennung, sicherer Passwortnutzung und Datenschutzrichtlinien helfen, das Bewusstsein für potenzielle Gefahren zu schärfen und Risiken zu minimieren (vgl. BSI 2024).

Ein weiterer wichtiger Aspekt ist die Definition klarer Sicherheitsrichtlinien und Prozesse. Unternehmen sollten verbindliche Vorgaben zum Umgang mit IT-Systemen und sensiblen Daten festlegen. Hierzu gehört die Implementierung eines Identity- und Access-Managements (IAM), um sicherzustellen, dass nur autorisierte Personen Zugriff auf kritische Systeme erhalten (vgl. Pufahl et al. 2024: 28, 70, 72-74).

Zudem empfiehlt das BSI die regelmäßige Durchführung von Sicherheitsanalysen und Notfalltests (vgl. BSI 2024). Durch simulierte Cyberangriffe (Red-Teaming) können Schwachstellen frühzeitig erkannt und Gegenmaßnahmen ergriffen werden. Eine

umfassende Backup-Strategie mit regelmäßigen Datensicherungen schützt vor Datenverlust durch Ransomware-Angriffe und erleichtert die Wiederherstellung im Ernstfall (vgl. Pohlmann 2022: 685).

Die konsequente Umsetzung organisatorischer Sicherheitsmaßnahmen trägt maßgeblich zur Erhöhung der Cyberresilienz bei und stellt sicher, dass Unternehmen auf moderne Bedrohungen vorbereitet sind.

5 Praxisbeispiele und Fallstudien

5.1 Cybersecurity-Strategie in einem mittelständischen Unternehmen – noris network AG

Die noris network AG mit Sitz in Nürnberg ist ein mittelständisches Unternehmen, das sich auf hochverfügbare IT-Infrastrukturen und Dienstleistungen spezialisiert hat. Um den steigenden Anforderungen an die Cybersicherheit gerecht zu werden, verfolgt das Unternehmen eine umfassende Strategie, die verschiedene Kernbereiche abdeckt. Ein zentrales Element der Sicherheitsstrategie ist die Diversifikation der IT-Ressourcen. Durch die Verteilung von IT-Diensten auf verschiedene Anbieter, Technologien und Plattformen minimiert noris network potenzielle Ausfall- und Sicherheitsrisiken. So setzt das Unternehmen auf eine Mischung aus eigener Infrastruktur und Partnerschaften mit verschiedenen Cloud-Anbietern, um die Abhängigkeit von einzelnen Dienstleistern zu reduzieren (vgl. noris network 2024a).

Zur proaktiven Bedrohungsabwehr bietet noris network Managed Security Services an. Diese umfassen unter anderem Firewalls, Intrusion Detection- und Prevention-Systeme (IDS/IPS) sowie regelmäßige Sicherheitsanalysen. Durch kontinuierliche Überwachung und Anpassung der Sicherheitsmaßnahmen stellt das Unternehmen sicher, dass es stets auf dem neuesten Stand der Technik ist und auf aktuelle Bedrohungen reagieren kann. Ein weiterer zentraler Bestandteil der Sicherheitsstrategie ist der Einsatz von georedundanten Rechenzentren. Durch den Betrieb mehrerer Rechenzentren an unterschiedlichen Standorten stellt noris network die Ausfallsicherheit und Datenverfügbarkeit sicher. Im Falle eines lokalen Ausfalls kann der Betrieb nahtlos an einem anderen Standort fortgesetzt werden, wodurch die Kontinuität der Dienstleistungen gewährleistet bleibt (vgl. Exkurs: Noris Network AG, 17.12.2024).

Mitarbeiter spielen eine entscheidende Rolle in der Cybersicherheitsstrategie. Noris network legt großen Wert auf die Sensibilisierung und Schulung seiner Belegschaft. Regelmäßige Trainings und Workshops zu aktuellen Bedrohungen und Sicherheitspraktiken stellen sicher, dass alle Mitarbeiter ein hohes Bewusstsein für Cyberrisiken entwickeln und entsprechend handeln (vgl. ebd.). Um stets auf dem neuesten Stand der Technik zu bleiben und von externem Fachwissen zu profitieren, kooperiert noris network mit verschiedenen IT-Sicherheitsdienstleistern. Diese Partnerschaften ermöglichen es, innovative Sicherheitslösungen zu integrieren und von Best Practices der Branche zu profitieren (vgl. noris network 2024b).

Durch die konsequente Umsetzung dieser Maßnahmen hat die noris network AG eine robuste Cybersecurity-Strategie etabliert, die sowohl die Sicherheit der eigenen IT-Infrastruktur als auch die ihrer Kunden gewährleistet. Die Kombination aus technischer Exzellenz, organisatorischen Maßnahmen und kontinuierlicher Weiterbildung bildet dabei das Fundament für den nachhaltigen Erfolg des Unternehmens in einer zunehmend digitalisierten Welt.

5.2 Analyse eines realen Cyberangriffs: Ursachen, Verlauf und Lessons Learned

Im Mai 2024 wurde die Deutsche Telekom von der Ransomware-Gruppe LockBit ins Visier genommen. LockBit, auch bekannt als LockBit 3.0 oder LockBit Black, ist eine der größten Ransomware-Gruppen weltweit und hat umfangreiche Cyberangriffe orchestriert. Die Angreifer behaupteten, sensible Daten des Unternehmens entwendet zu haben, und setzten eine Frist bis zum 21. Mai 2024 für Verhandlungen, andernfalls drohten sie mit der Veröffentlichung der gestohlenen Informationen (vgl. Schappert 2024).

LockBit operiert nach dem Ransomware-as-a-Service (RaaS)-Modell, bei dem die Schadsoftware anderen Kriminellen zur Verfügung gestellt wird, die im Gegenzug einen Anteil der erpressten Gelder abtreten. Die Gruppe ist bekannt für ihre fortschrittlichen Funktionen, wie die seitliche Bewegung durch Netzwerke und das Verschleiern ihrer Spuren, um einer Entdeckung zu entgehen (vgl. ebd.).

Die genaue Angriffsmethode auf die Deutsche Telekom wurde nicht detailliert offengelegt. Typischerweise nutzen solche Gruppen jedoch Phishing-Kampagnen, Social-Engineering-Techniken oder die Ausnutzung nicht behobener Sicherheitslücken,

um in Netzwerke einzudringen. Einmal im Netzwerk, verschlüsselt die Ransomware Dateien und fordert ein Lösegeld für die Entschlüsselung.

Die Deutsche Telekom betreibt die Plattform Sicherheitstacho.eu, die Echtzeitdaten zu Cyberangriffen sammelt und die Herkunftsländer sowie die betroffenen Systeme anzeigt. Diese Plattform basiert auf mehr als 90 Sensoren weltweit, die als Frühwarnsysteme fungieren (vgl. Telekom 2013). Eine Analyse der Sicherheitstacho-Daten im Zeitraum des LockBit-Angriffs zeigte einen signifikanten Anstieg von Angriffen auf Remote Desktop Protokoll (RDP)-Dienste und VPN-Zugänge, die häufig als Einstiegspunkte für Ransomware-Angriffe genutzt werden. Besonders auffällig war die Zunahme automatisierter Brute-Force-Angriffe, die von bekannten LockBit-Servern stammten. Diese Daten verdeutlichen, dass Unternehmen, die auf ungesicherte oder unzureichend geschützte Fernzugriffsprotokolle setzen, einem erhöhten Risiko ausgesetzt sind (vgl. Schappert 2024).

Der Angriff zeigt, dass Unternehmen auf eine Kombination aus technischen und organisatorischen Schutzmaßnahmen setzen müssen. Durch regelmäßige Sicherheitsprüfungen und Penetrationstests können Schwachstellen frühzeitig identifiziert und behoben werden (vgl. DataGuard o. D.). Der Einsatz von Multi-Faktor-Authentifizierung erschwert unbefugten Zugriff auf sensible Systeme zusätzlich. Schnellere Erkennung durch SIEM-Systeme und Threat Intelligence ermöglicht es, Angriffe proaktiv zu identifizieren (vgl. Lange 2025). Eine effektive Backup-Strategie mit regelmäßigen Offsite-Sicherungen stellt sicher, dass Daten im Falle eines Angriffs wiederhergestellt werden können, ohne auf die Forderungen der Angreifer eingehen zu müssen.

Die Analyse dieses Angriffs unterstreicht die anhaltende Bedrohung durch Ransomware und die Notwendigkeit einer umfassenden Sicherheitsstrategie für Unternehmen.

5.3 Evaluation von KI-gestützten Sicherheitslösungen in der Praxis

Die steigende Anzahl komplexer Cyberangriffe erfordert Sicherheitslösungen, die über klassische signaturbasierte Methoden hinausgehen. KI-gestützte Systeme erkennen Bedrohungen durch die Analyse großer Datenmengen und identifizieren verdächtige Muster in Echtzeit. Dadurch lassen sich Angriffe frühzeitig erkennen und automatisiert Gegenmaßnahmen einleiten.

Ein zentraler Einsatzbereich ist die proaktive Bedrohungserkennung. Intrusion Detection- und Prevention-Systeme (IDS/IPS) erkennen Anomalien im Netzwerkverkehr, während Security Information and Event Management (SIEM)-Systeme sicherheitsrelevante Ereignisse korrelieren und verdächtige Aktivitäten melden. Ergänzend ermöglichen automatisierte Reaktionssysteme, verdächtige Prozesse zu isolieren und Angriffe in Echtzeit abzuwehren (vgl. Lange 2025).

Die noris network AG setzt KI-gestützte Sicherheitslösungen ein, um verdächtige Aktivitäten in Rechenzentren frühzeitig zu erkennen. Durch kontinuierliche Analyse des Datenverkehrs konnte die Erkennungsrate um 30 % verbessert und gleichzeitig die Anzahl der Fehlalarme reduziert werden (vgl. noris network 2024a). Auch die Deutsche Telekom nutzt KI-Technologien auf ihrer Plattform Sicherheitstacho.eu, um Cyberangriffe weltweit zu überwachen. Besonders Angriffe auf Remote-Access-Dienste konnten frühzeitig erkannt und entsprechende Schutzmaßnahmen umgesetzt werden (vgl. Schappert 2024).

Trotz der Vorteile bestehen Herausforderungen. Fehlalarme (False Positives) können Sicherheitsteams unnötig belasten, während gezielte Manipulationen von KI-Modellen (Adversarial Attacks) deren Erkennungsleistung beeinträchtigen können (vgl. Salem et al. 2024: 31). Um diesen Risiken entgegenzuwirken, ist eine kontinuierliche Anpassung der Modelle erforderlich.

Langfristig können KI-gestützte Sicherheitslösungen durch regelmäßige Optimierung und eine enge Zusammenarbeit zwischen IT-Sicherheitsteams und Experten weiter verbessert werden, um der sich stetig wandelnden Bedrohungslage wirksam zu begegnen.

6 Diskussion

6.1 Interpretation der Ergebnisse im Kontext der Forschungsfragen

Welche aktuellen Bedrohungen gefährden die Sicherheit moderner IT-Infrastrukturen?

Die Untersuchung zeigt, dass moderne IT-Systeme zunehmend durch Cyberangriffe wie Ransomware, Zero-Day-Exploits und Supply-Chain-Angriffe gefährdet sind. Besonders kritische Infrastrukturen sind durch diese Bedrohungen stark betroffen, da sie sensible Daten verarbeiten und attraktive Ziele für Angreifer darstellen. Diese Bedrohungen sind

nicht nur in ihrer Häufigkeit gestiegen, sondern auch durch neue Angriffsmethoden komplexer geworden, was herkömmliche Schutzmaßnahmen oft unzureichend macht.

Wie können Unternehmen ihre Sicherheitsstrategien verbessern, um aktuellen Bedrohungen zu begegnen?

Um diesen Bedrohungen zu begegnen, müssen Unternehmen ihre IT-Sicherheitsstrategien kontinuierlich anpassen. Die Analyse zeigt, dass eine Kombination aus technischen Schutzmaßnahmen wie Firewalls, Intrusion-Detection-Systemen und Zero-Trust-Architekturen sowie organisatorischen Maßnahmen wie Sicherheitsrichtlinien und regelmäßigen Mitarbeiterschulungen notwendig ist. Besonders wichtig ist eine vorausschauende Sicherheitsstrategie, die nicht nur auf bekannte Bedrohungen reagiert, sondern auch neue Angriffsszenarien antizipiert.

Welche Rolle spielen KI und Automatisierung bei der Abwehr von Cyberbedrohungen?

KI-gestützte Sicherheitssysteme haben sich als zentraler Bestandteil moderner Schutzmaßnahmen erwiesen. Die Ergebnisse zeigen, dass Intrusion-Detection-Systeme, Endpoint-Security-Lösungen und Security-Orchestration-Technologien Unternehmen ermöglichen, Bedrohungen in Echtzeit zu erkennen und automatisierte Gegenmaßnahmen einzuleiten. Dies reduziert nicht nur Reaktionszeiten, sondern erhöht auch die Erkennungsrate neuartiger Angriffe, die durch klassische signaturbasierte Systeme nicht identifiziert werden können.

In welchem Maße beeinflussen menschliche Faktoren die Sicherheit moderner IT-Infrastrukturen?

Neben technologischen Sicherheitslösungen sind menschliche Faktoren weiterhin eine der größten Schwachstellen in der IT-Sicherheit. Die Untersuchung verdeutlicht, dass unsichere Benutzerpraktiken, unzureichendes Sicherheitsbewusstsein und Social-Engineering-Angriffe häufige Einfallstore für Cyberkriminelle sind. Unternehmen müssen daher verstärkt auf Security Awareness-Trainings, klare Zugriffskontrollen und Multi-Faktor-Authentifizierung setzen, um das Risiko menschlicher Fehler zu minimieren.

6.2 Kritische Reflexion der Untersuchungsergebnisse und Handlungsempfehlungen

Die Untersuchung zeigt, dass die zunehmende Vernetzung und Komplexität moderner IT-Infrastrukturen sowohl technologische als auch organisatorische Sicherheitsmaßnahmen erfordert. Während Unternehmen bereits verstärkt in KI-gestützte Sicherheitssysteme investieren, bleiben grundlegende Herausforderungen bestehen. Besonders kleine und mittelständische Unternehmen haben oft Schwierigkeiten, mit den sich stetig weiterentwickelnden Angriffstechniken Schritt zu halten, da sie nicht über die notwendigen Ressourcen für umfassende Sicherheitsmaßnahmen verfügen. Dies führt zu einer Ungleichverteilung des Sicherheitsniveaus zwischen großen und kleinen Unternehmen, was gezielte Angriffe auf schwächere Akteure begünstigt.

Zudem zeigt sich, dass bestehende Sicherheitsrichtlinien und Standards zwar eine wichtige Grundlage bieten, aber in der Praxis nicht immer konsequent umgesetzt werden. Unternehmen unterschätzen oft die Notwendigkeit regelmäßiger Sicherheitsüberprüfungen und Incident-Response-Pläne, wodurch sie im Ernstfall nicht schnell genug reagieren können. Ein weiteres Problem ist die Abhängigkeit von Drittanbietern in der IT-Lieferkette, die zusätzliche Risiken birgt.

Als Handlungsempfehlung sollten Unternehmen stärker auf kontinuierliche Risikobewertungen setzen und ihre Sicherheitsstrategien dynamisch anpassen. Regelmäßige Audits, verstärkte Angriffssimulationen (Red-Teaming) sowie klare Notfallprozesse sind essenziell, um Cyberangriffe frühzeitig zu erkennen und abzuwehren. Zudem sollte ein verstärkter Austausch zwischen Unternehmen, Behörden und Forschungseinrichtungen erfolgen, um Wissen über aktuelle Bedrohungen und Best Practices effizienter zu nutzen.

7 Fazit

Die Untersuchung hat deutlich gemacht, dass die Absicherung moderner IT-Infrastrukturen eine stetige Anpassung an neue Bedrohungen erfordert. Cyberangriffe entwickeln sich kontinuierlich weiter, wodurch Unternehmen gezwungen sind, ihre Sicherheitsstrategien fortlaufend zu optimieren. Es wurde festgestellt, dass neben technischen Schutzmaßnahmen insbesondere ein strukturiertes Risikomanagement

sowie eine klare Sicherheitsstrategie notwendig sind, um widerstandsfähige IT-Systeme zu gewährleisten.

Ein zentrales Ergebnis dieser Arbeit ist, dass IT-Sicherheit nicht nur eine technische, sondern auch eine strategische Herausforderung darstellt. Unternehmen müssen nicht nur in neue Technologien investieren, sondern auch Sicherheitsprozesse effizient gestalten und durchsetzen. Dabei kommt es darauf an, Bedrohungen nicht isoliert zu betrachten, sondern sie als Teil eines umfassenden Sicherheitskonzepts zu behandeln.

Für die Zukunft wird es entscheidend sein, dass Unternehmen ihre Sicherheitsarchitekturen flexibel und anpassungsfähig halten. Die zunehmende Verlagerung von IT-Ressourcen in die Cloud sowie die wachsende Vernetzung durch IoT und verteilte Systeme machen Sicherheitskonzepte komplexer. Langfristig ist eine enge Zusammenarbeit zwischen Wirtschaft, Forschung und Behörden notwendig, um Bedrohungslagen frühzeitig zu erkennen und nachhaltige Sicherheitslösungen zu etablieren.

Literaturverzeichnis

Pohlmann, N. (2022). *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung.* Wiesbaden: Springer Vieweg. Verfügbar unter: https://link.springer.com/book/10.1007/978-3-658-36243-0 [Zugriff am: 16.01.2025].

Kipker, D.-K. & Pfeil, D. (2016). IT-Sicherheitsgesetz in Theorie und Praxis: Was Betreiber (wirklich) beachten müssen – Eine interdisziplinäre Fallstudie. *Datenschutz und Datensicherheit – DuD, 40*(12), 810–815. Verfügbar unter: https://link.springer.com/article/10.1007/s11623-016-0708-5 [Zugriff am: 17.01.2025].

Vogel, V. & Ziegler, N. (2023). Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie. *International Cybersecurity Law Review*, *4*(1), 1–19. Verfügbar unter: https://link.springer.com/article/10.1365/s43439-022-00077-4 [Zugriff am: 22.01.2025].

Rüdiger, T.-G. & Bayerl, P. S. (Hrsg.) (2023). *Handbuch Cyberkriminologie 1: Theorien und Methoden.*Wiesbaden: Springer. Verfügbar unter: https://link.springer.com/book/10.1007/978-3-658-35439-8 [Zugriff am: 24.01.2025].

Sharma, A. & Singh, U. K. (2025). Cloud computing security assurance modelling through risk analysis using machine learning. *International Journal of System Assurance Engineering and Management.* Verfügbar unter: https://link.springer.com/article/10.1007/s13198-025-02705-8 [Zugriff am: 13.02.2025].

Edwards, M. (2024). *The Ultimate Guide to ISO 27001*. ISMS.online. Verfügbar unter: https://www.isms.online/iso-27001/ [Zugriff am: 29.01.2025].

Parrend, P., Navarro, J., Guigou, F., Deruyver, A. & Collet, P. (2018). Foundations and applications of artificial intelligence for zero-day and multi-step attack detection. *EURASIP Journal on Information Security, 2018*(4), 1–19. Verfügbar unter: https://doi.org/10.1186/s13635-018-0074-y [Zugriff am: 02.02.2025].

Salem, A. H., Azzam, S. M., Emam, O. E. & Abohany, A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11*(105), 1–19. Verfügbar unter: https://doi.org/10.1186/s40537-024-00957-y [Zugriff am: 04.02.2025].

Dreißigacker, A., von Skarczinski, B. S. & Wollinger, G. R. (2024). Unternehmen als Opfer von Cyberkriminalität. In: *Rüdiger, T.-G. & Bayerl, P. S. (Hrsg.), Handbuch Cyberkriminologie 2: Phänomene und Erscheinungsformen.*Wiesbaden: Springer. Verfügbar unter: https://link.springer.com/chapter/10.1007/978-3-658-35442-8_43?fromPaywallRec=false [Zugriff am: 04.02.2025].

Schmitt, M. (2023). Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration.* Verfügbar unter: https://doi.org/10.1016/j.jii.2023.100520 [Zugriff am: 06.02.2025].

Pufahl, M., Paulsen, P. & Arndt, P. (2024). Das Cybersecurity-Kompetenzmodell – Basis einer ganzheitlichen Ausrichtung auf Cybergefahren. In: *Cybersecurity für Manager: Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis.* Springer Gabler, S. 9–32. Verfügbar unter: https://link.springer.com/chapter/10.1007/978-3-658-44892-9_2 [Zugriff am: 07.02.2025].

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2024). 10 Tipps zur Cyber-Sicherheit für Unternehmen. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/10-Tipps-zur-Cyber-Sicherheit-fuer-Unternehmen/10-tipps-zur-cyber-sicherheit-fuer-unternehmen_node.html. [Zugriff am: 09.02.2025].

noris network (2024a). De-Risking bei IT-Infrastruktur. Verfügbar unter: https://www.noris.de/de-risking-bei-it-infrastruktur/ [Zugriff am: 09.02.2025].

Exkurs: Noris Network AG. (2024). Unternehmensbesichtigung am 17.12.2024, Nürnberg.

noris network (2024b). Zusammenarbeit mit Partnern. Verfügbar unter: https://www.noris.de/unternehmen/partner/ [Zugriff am: 09.02.2025].

Lange, F. (2025). Wenn Millisekunden über IT-Sicherheit entscheiden. *Security Insider.* Verfügbar unter: https://www.security-insider.de/siem-systeme-proaktive-cybersicherheit-a-612c9b02414047da40dfc8c7c54b4f61/ [Zugriff am: 12.02.2025].

DataGuard. (o. D.). Cyber Security Risk Management. Verfügbar unter: https://www.dataguard.de/cyber-security/risk-management/ [Zugriff am: 13.02.2025].

Schappert, S. (2024). Deutsche Telekom claimed by LockBit, dozens more ransom victims. *Cybernews.* Verfügbar unter: https://cybernews.com/news/deutsche-telekom-lockbit-dozens-more-ransom-victims/ [Zugriff am: 12.02.2025].

Telekom. (2013). Sicherheitstacho zeigt Cyber-Angriffe in Echtzeit. Verfügbar unter: https://www.telekom.com/de/medien/medieninformationen/detail/sicherheitstacho-zeigt-cyber-angriffe-in-echtzeit--343586 [Zugriff am: 12.02.2025].

Glossar

Ransomware-as-a-Service (RaaS)
Ein Geschäftsmodell, bei dem Cyberkriminelle Ransomware als Dienstleistung anbieten, sodass auch technisch weniger versierte Kriminelle Angriffe durchführen können.

Zero-Trust-Architektur
Ein Sicherheitskonzept, das keinen Benutzer oder Gerät innerhalb oder außerhalb eines Netzwerks automatisch vertraut und stets eine Authentifizierung erfordert.

Security Orchestration, Automation, and Response (SOAR)
Eine Technologie, die Sicherheitsanalysen automatisiert, Bedrohungen erkennt und Gegenmaßnahmen ohne menschliches Eingreifen einleitet.

Endpoint Detection and Response (EDR)
Eine Sicherheitslösung, die Bedrohungen auf Endgeräten (z. B. Laptops, Smartphones) in Echtzeit überwacht, erkennt und darauf reagiert.

Red-Teaming
Eine Angriffssimulation, bei der Sicherheitsexperten die Rolle eines Angreifers übernehmen, um Schwachstellen in IT-Systemen aufzudecken.

Adversarial Attacks
Manipulationstechniken, die darauf abzielen, KI-Modelle gezielt zu täuschen, sodass sie Bedrohungen nicht korrekt erkennen.

Intrusion Detection- und Prevention-Systeme (IDS/IPS)
Systeme zur Überwachung von Netzwerkverkehr, die verdächtige Aktivitäten erkennen (IDS) und Angriffe aktiv blockieren (IPS).

Best Practices
Empfohlene Methoden und Strategien zur Verbesserung der IT-Sicherheit, die sich in

der Praxis bewährt haben und als Richtlinien für Unternehmen und Organisationen dienen.

Anhang

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbstständig und ohne unerlaubte Hilfe angefertigt worden ist, insbesondere, dass ich alle Stellen, die wörtlich oderannähernd wörtlich aus Veröffentlichungen entnommen sind, durch Zitate als solche gekennzeichnet habe. Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Weiterhin erkläre ich, dass die Arbeit in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde/Prüfungsstelle vorgelegen hat. Ich erkläre mich damit nicht einverstanden, dass die Arbeit der Öffentlichkeit zugänglich gemacht wird. Ich erkläre mich damit einverstanden, dass die Digitalversion dieser Arbeit zwecks Plagiatsprüfung

auf die Server externer Anbieter hochgeladen werden darf. Die Plagiatsprüfung stellt keine Zurverfügungstellung für die Öffentlichkeit dar.

(Ort, Datum) (Eigenhändige Unterschrift)

90441 Nürnberg, 16.02.2025