FERDINAND PORSCHE
FERNFH

Entwicklung eines IT-Sicherheitskonzepts zur Reduzierung von Cyberangriffen um 50 %: Anwendung der OCTAVE-Methode in Kombination mit weiteren IT-Sicherheitsansätzen an der polnischen Schule des Jan III. Sobieski am Kollegium Kalksburg

Bachelorarbeit

eingereicht von: **mgr Dariusz Zarosa**
Matrikelnummer: 00452351

im Fachhochschul-Bachelorstudiengang Wirtschaftsinformatik (0470)
der Ferdinand Porsche FernFH

zur Erlangung des akademischen Grades <einer/eines>

Bachelor of Arts in Business

Betreuung und Beurteilung: Dipl.-Ing. Thomas Györgyfalvay, BA MBA

Wiener Neustadt, 06 2025

FERDINAND PORSCHE
FERNFH

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Bachelorarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

Wien, 03.06.2025

Dariusz Zarosa

Unterschrift

Die Kapitel 2 bis 5 der vorliegenden Bachelorarbeit wurden im Rahmen der Lehrveranstaltung „Bachelor Seminar 1“ eingereicht und am 11.04.2025 als Bachelorarbeit 1 angenommen.

Kurzzusammenfassung: Entwicklung eines IT-Sicherheitskonzepts zur Reduzierung von Cyberangriffen um 50 %: Anwendung der OCTAVE-Methode in Kombination mit weiteren IT-Sicherheitsansätzen an der polnischen Schule des Jan III. Sobieski am Kollegium Kalksburg

Im Rahmen dieser Bachelorarbeit wurde ein maßgeschneidertes IT-Sicherheitskonzept für die Polnische Schule Jan III Sobieski in Wien entwickelt, mit dem Ziel, die Anzahl von Cyberangriffen um mindestens 50 % zu reduzieren. Die Untersuchung basierte auf der Anwendung der OCTAVE-S-Methode, die durch Standards wie ISO/IEC 27001, NIST CSF, BSI-Grundschutz und das österreichische Informationssicherheitshandbuch erweitert wurde. Nach einer Analyse der bestehenden IT-Infrastruktur und dokumentierter Vorfälle wurden technische und organisatorische Maßnahmen umgesetzt, darunter Firewall-Konfiguration, VLAN-Segmentierung, Backup-Strategien, MFA und Awareness-Training. Basierend auf den Ergebnissen einer über drei Wochen andauernden Evaluation konnte eine Reduktion der Vorfälle um mehr als 65 Prozent sowie eine Reduktion der Schwachstellen um 90 Prozent verzeichnet werden. Die Wirksamkeit der implementierten Schutzmaßnahmen wurde durch Penetrationstests bestätigt. Die vorliegende Arbeit verdeutlicht, dass selbst unter restriktiven Ressourcen-bedingungen signifikante Sicherheitsverbesserungen erzielt werden können. Gleichzeitig wird betont, dass IT-Sicherheit als ein kontinuierlicher Prozess zu betrachten ist, für den regelmäßige Updates, Audits und Schulungen erforderlich sind. Die aufgestellte Hypothese konnte dabei eindeutig validiert werden.

Schlagwörter:

IT-Sicherheitskonzept Schule, Cybersecurity im Bildungswesen, OCTAVE-S Methode Beispiel, IT-Risikoanalyse Bildungsinstitution, Maßnahmen gegen Cyberangriffe Schule

Abstract: Development of an IT Security Concept to Reduce Cyberattacks by 50%: Application of the OCTAVE Method in Combination with Additional IT Security Approaches at the Polish School of Jan III Sobieski at Kollegium Kalksburg

This bachelor thesis presents the development and implementation of a customized IT security concept for the Polish School Jan III Sobieski in Vienna, aiming to reduce cyber incidents by at least 50%. The methodology is based on the OCTAVE-S framework, complemented by international and national standards such as ISO/IEC 27001, NIST CSF, the BSI IT Baseline Protection, and Austrian guidelines. Following an in-depth analysis of the existing IT infrastructure and documented security incidents, technical and organizational measures were implemented, including VLAN-based network segmentation, firewall and antivirus upgrades, backup strategies, and awareness training. Evaluation through incident tracking, vulnerability scans, and a penetration test revealed a 65% reduction in threats and a 90% decrease in vulnerabilities. User feedback confirmed high acceptance and minimal disruption to school operations. Despite the constraints imposed by limited financial and human resources, measurable improvements were achieved. As a result, the hypothesis was confirmed. Nevertheless, the study emphasises the necessity for constant monitoring, updating, and adaptation in view of the evolution of threats and institutional limitations.

Keywords:

School IT Security Concept, Cybersecurity in Education, OCTAVE-S Method Case Study, IT Risk Assessment in Educational Institutions, Cyberattack Mitigation Measures for Schools

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Bestätigung

Hiermit bestätigen wir, dass Herr **Zarosa** im Rahmen seiner Bachelorarbeit mit dem Titel:

„Entwicklung eines IT-Sicherheitskonzepts zur Reduzierung von Cyberangriffen um 50 % – Anwendung der OCTAVE-Methode in Kombination mit weiteren IT-Sicherheitsansätzen an der Polnischen Schule des Jan III. Sobieski am Kollegium Kalksburg“

zahlreiche Analysen, Gespräche und technische Maßnahmen im direkten Kontakt mit unserer Schule durchgeführt hat. Ziel war es, Schwachstellen zu identifizieren, Sicherheitsanforderungen zu definieren und konkrete Maßnahmen zur Verbesserung der IT-Sicherheit zu entwickeln.

Durchgeführte Aktivitäten:

Aktivität	Datum	Verantwortliche
Analyse IT-Landschaft	01.06.2024	IT - Verantwortlicher (D. Zarosa)
Vorfallanalyse Juni 2024	30.06.2024	IT - Verantwortlicher (D. Zarosa)
Gespräch 1: Identifizierung der organisatorischen Assets	14.03.2025	IT - Verantwortlicher (D. Zarosa), Bibliothekar (I. Szliter), Direktion (H. Kaczmarczyk)
Gespräch 2: Bewertung bestehenden Sicherheitsmaßnahmen	15.03.2025	IT - Verantwortlicher (D. Zarosa), Bibliothekar (I. Szliter), Direktion (H. Kaczmarczyk)
Vorfallanalyse April 2025	27.04.2025	IT - Verantwortlicher (D. Zarosa)
Gespräch 3: Festlegung von Sicherheitsanforderungen	29.04.2025	IT - Verantwortlicher (D. Zarosa), Lehrervertreter (I. Szliter), Direktion (H. Kaczmarczyk)

Technische Umsetzung:

Im Zeitraum Ende April bis Anfang Mai 2025 wurden folgende sicherheitsrelevante Komponenten mit nur minimaler Beeinträchtigung des Unterrichts erfolgreich in Betrieb genommen:

- **FortiGate 60F (Firewall)**
- **Cisco Catalyst 3750V2 Switch**
- **Cisco Meraki MR32 Access Point**
- **USV (Unterbrechungsfreie Stromversorgung, 1000 VA)**
- **ESET PROTECT (Endpoint-Sicherheitslösung)**

- **MyQ X Druckmanagement**

Die genannten Geräte wurden von Herrn Zarosa konfiguriert und getestet. Die Schule trägt für das erste Jahr keine Lizenzkosten. Alle Tests und Änderungen wurden mit Zustimmung der Schulleitung durchgeführt und transparent dokumentiert.

Dokumentation und Schulung:

Die vollständige technische und organisatorische Dokumentation wird bis September 2025 in unsere IT-Mappe eingepflegt. Darüber hinaus präsentierte Herr Zarosa im Mai eine vorläufige Analyse der bisherigen Ergebnisse.

Am 17.05.2025 fand ein einstündiger Workshop mit Lehrkräften statt, der praxisnahe IT-Sicherheitsaspekte behandelte. Ein zweiter, vertiefender Trainingsblock für Lehrkräfte und Schüler ist für Oktober 2025 geplant. Das genaue Datum wird im Laufe des Septembers festgelegt.

Dieses Dokument dient der offiziellen Bestätigung und kann bei Bedarf gegenüber Dritten (z. B. Hochschulen, Prüfungskommissionen) vorgelegt werden.

Mit freundlichen Grüßen
im Namen der Polnischen Schule des Jan III. Sobieski am Kollegium Kalksburg

...SCHULE UND LYZEUM
JAN III SOBIESKI
BEI
...ER POLNISCHEN
...OTSCHAFT IN WIEN
Promenadeweg 3
1238 Wien - Austria

DYREKTOR
Szkoły Polskiej im. Jana III Sobieskiego
przy Ambasadzie RP w Wiedniu
Hanna Kaczmarczyk

Wien, am 20.05.2025
[Unterschrift/Name der ausstellenden Person]

Danksagung

Für die Unterstützung während der Anfertigung dieser Bachelorarbeit möchte ich mich herzlich bei allen bedanken.

Mein besonderer Dank gilt Herrn Thomas Györgyfalvay. Er stand mir mit seinem Fachwissen und wertvollen Hinweisen zur Strukturierung der Arbeit stets zur Seite und begleitete mich fachlich wie methodisch.

Bedanken möchte ich mich auch bei der Leitung der Polnischen Schule Jan III Sobieski in Wien, insbesondere Frau Direktorin Hanna Kaczmarczyk sowie der Bibliotheksleiterin und stellvertretenden Direktorin, Frau Ilona Szliter, für die offene Zusammenarbeit, das entgegengebrachte Vertrauen und die Unterstützung bei der praktischen Umsetzung dieser Arbeit.

Ein besonderer Dank gilt auch meinen Eltern, die mir bei jedem Vorhaben mit Rat, Tat und Motivation zur Seite standen. Nicht zuletzt danke ich allen, die zur erfolgreichen Durchführung und Umsetzung des Projekts beigetragen haben.

1. Einleitung

1.1 Ausgangslage

Die polnische Schule Jan III Sobieski ist eine unabhängige Bildungsinstitution innerhalb des Kollegiums Kalksburg. Um den wachsenden Anforderungen an digitale Lernumgebungen und administrative Abläufe gerecht zu werden, wurde die IT-Infrastruktur der Schule grundlegend modernisiert. Zu den wesentlichen Neuerungen zählten:

- **Server:** Während der COVID-19-Pandemie (September 2020) installierte die Schule einen Server als zentrale Plattform für die Datenverwaltung und -speicherung. Er verwaltet sowohl Schul- als auch Bibliotheksdaten und führt regelmäßige Backups durch. Um diese Serverarchitektur zu schützen, wurde die Sicherheitssoftware Avast Essential Business Security eingesetzt, deren Lizenz jedoch im Februar 2025 abläuft. Dies bietet die Möglichkeit, ein umfassendes Sicherheitskonzept zu entwickeln, da bislang noch keine einheitlichen Sicherheitsrichtlinien vorhanden sind.
- **Switch:** Ein HP-Switch gewährleistet eine stabile und effiziente Datenübertragung zwischen den IT-Systemen und bildet das Rückgrat der schulischen Netzwerkinfrastruktur.
- **Arbeitsplätze:** In der Direktion und der Bibliothek wurden zwei neue Computer sowie zwei Laptops eingerichtet. Darüber hinaus wurde ein älteres Gerät modernisiert. Diese Systeme sind mit aktueller Software ausgestattet und unterstützen sowohl den Unterricht als auch administrative Aufgaben.
- **Drucker:** In verschiedenen Schulräumen wurden insgesamt vier netzwerkfähige Multifunktionsdrucker installiert, die sowohl Schwarzweiß- als auch Farbdrucke ermöglichen. Die Druckdienste sind für alle im Schulnetzwerk angemeldeten Geräte verfügbar, einschließlich Schul-PCs, Laptops und der von den Schülern verwendeten BYOD-Geräte (Bring Your Own Device). Schüler können Druckaufträge direkt von ihren Geräten aus versenden, solange diese mit dem Netzwerk verbunden sind. Darüber hinaus ist das Drucken von mobilen Geräten wie Tablets und Smartphones, ohne dass eine spezielle Software installiert werden muss, möglich. Die Verbindung erfolgt automatisch über das Schul-WLAN, sofern das Gerät ein unterstütztes Druckprotokoll verwendet. Unterstützt werden unter anderem folgende Protokolle:
    - **AirPrint (für Apple-Geräte)** entwickelt von Apple um das Drucken direkt aus iOS- und macOS-Apps zu ermöglichen, ohne dass Treiber oder zusätzliche Software erforderlich sind. Solange sich das Gerät im selben

Netzwerk wie ein AirPrint-kompatibler Drucker befindet, wird dieser automatisch erkannt.

- **Mopria Print Service (für Android-Geräte)** ist eine standardisierte Drucklösung für Android-Smartphones und -Tablets, die das Drucken aus nahezu jeder App ermöglicht, ohne eine spezielle Drucker-App zu benötigen. Mopria unterstützt zahlreiche Druckermodelle verschiedener Hersteller und ermöglicht das direkte Drucken über WLAN.

Die Druckfreigabe erfolgt auf direkte, mündliche Anfrage des Schülers beim Lehrer. Nach Zustimmung kann der Schüler den Druckvorgang selbstständig initiieren. Momentan gibt es keine zentrale Kontrolle oder Nachverfolgung der Ausdrucke. In Zukunft könnte dies jedoch durch ein Druckkontingent oder eine Benutzeranmeldung verbessert werden.

- **WLAN-Router:** Schüler und Lehrkräfte profitieren nun von einem neuen WLAN, das den Einsatz mobiler Geräte wie Tablets, Smartphones und interaktiver Whiteboards erleichtert. Darüber hinaus steht den Besuchern auch ein Gäste-WLAN zur Verfügung, das jedoch unverschlüsselt ist und somit ein potenzielles Sicherheitsrisiko darstellen kann. Zudem fungiert der WLAN-Router nicht nur als drahtloser Access Point für die Netzwerkgeräte, sondern stellt auch die Verbindung zum Internet (A1) bereit.
- **Interaktive Whiteboards:** Einige Klassenräume wurden mit modernen Whiteboards ausgestattet, die multimediale Inhalte unterstützen und den Unterricht interaktiver gestalten. Diese sind direkt ins Schulnetzwerk eingebunden und ermöglichen einen schnellen Zugriff auf digitale Lernressourcen.

Zur Veranschaulichung der zuvor beschriebenen IT-Komponenten und deren Vernetzung in der polnischen Schule wurde Abbildung 1 erstellt.

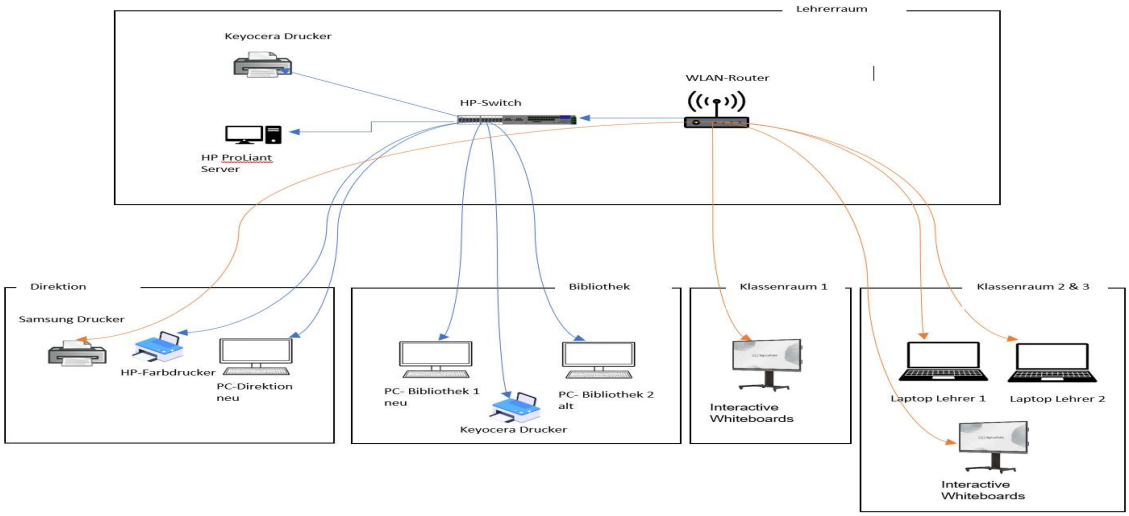

Abbildung 1 Bildliche Darstellung der aktuellen IT-Architektur der polnischen Schule.

1.2 Motivation für ein IT-Sicherheitskonzept

Trotz der Modernisierung der IT-Infrastruktur der Schule wurde der IT-Sicherheit weiterhin nicht genügend berücksichtigt. Finanzielle Einschränkungen führten dazu, dass nur grundlegende Schutzmaßnahmen umgesetzt wurden. Nach wie vor fehlen klare Richtlinien zur Sicherung sensibler Daten, den Schutz sowie Mechanismen zur Überwachung des Netzwerkzugriffs und zum Schutz der mobilen Geräte.

Innerhalb des vorliegenden Kontextes bezeichnen Richtlinien zur Sicherung sensibler Daten konkrete Vorgaben und Best Practices, mit deren Hilfe der Schutz personenbezogener und vertraulicher Informationen gewährleistet werden soll. Zu den entsprechenden Maßnahmen würden unter anderem die Klassifizierung sensibler Daten, die Zugriffsbeschränkungen, sichere Speichermethoden, die verschlüsselte Übertragung von Daten sowie regelmäßige Datensicherungen zählen. Darüber hinaus wird die Festlegung klarer Richtlinien für den Umgang mit externen Speichermedien, Cloud-Diensten und BYOD-Lösungen (Bring Your Own Device) empfohlen, um das Risiko eines Datenverlusts oder unbefugten Zugriffs zu verhindern bzw. zu minimieren.

Die jahrelange ehrenamtliche Verantwortung für die IT-Infrastruktur, sowie die maßgebliche Rolle bei der Modernisierung, verdeutlichen den dringenden Handlungsbedarf für ein umfassendes IT-Sicherheitskonzept. Ziel ist es, nicht nur die Sicherheit der bestehenden Infrastruktur zu verbessern, sondern auch ein Modell für andere Bildungsinstitutionen bereitzustellen, die bisher kein strukturiertes Sicherheitskonzept umgesetzt haben.

1.3 Problemstellung

Die IT-Sicherheit der polnischen Schule des Jan III. Sobieski erfordert dringende Aufmerksamkeit, insbesondere aufgrund einer deutlichen Zunahme von Cyberattacken im Juni 2024. Dies verdeutlicht, wie wichtig es ist, die bestehenden Schutzmaßnahmen zu optimieren, um die digitale Umgebung der Schule - sowohl für Schüler und Lehrkräfte als auch für alle Personen, die täglich mit den Systemen interagieren – sicherer zu gestalten. In diesem Zusammenhang existieren mehrere Herausforderungen, die gelöst werden müssen:

- **Schutz sensibler Daten:** Die Schule erhebt, bearbeitet und speichert personenbezogene Daten von Schülern, Lehrkräften und administrativen Mitarbeitern. Ohne die Implementierung adäquater Datenschutzrichtlinien und Sicherheitsmaßnahmen besteht das Risiko, dass diese Daten Dritten uneingeschränkt zugänglich gemacht werden oder sogar gestohlen werden.
- **Unsichere Netzwerkverbindungen:** Durch die gleichzeitige Nutzung des WLANs durch eine hohe Anzahl an Nutzern besteht, ohne angemessene Sicherheitsprotokolle, einerseits die Gefahr des unberechtigten Zugriffs auf das Netzwerk, andererseits die daraus resultierenden Cyberangriffe. Dabei stellt

insbesondere das unverschlüsselte WLAN für Gäste ein potenzielles Sicherheitsrisiko dar.

- **Fehlende Zugriffskontrollen:** Derzeit existiert keine klar definierte Richtlinie zur Zugangskontrolle. Das Schulgebäude ist während des Schulbetriebes für Gäste frei zugänglich, ohne jegliche Kontrolle. Ebenso ist die Bibliothek gelegentlich unbesetzt, was das Risiko eines unautorisierten Zugriffs auf die IT-Systeme erhöht.
- **Mangelnde regelmäßige Wartung und Updates:** Ohne regelmäßige Software-Updates entstehen Sicherheitslücken, welche von Angreifern ausgenutzt werden können. Derzeit fehlt ein verbindlicher Wartungsplan für IT-Komponenten und Software.
- **Fehlende Schulungen und Sensibilisierung:** Viele Lehrkräfte sind im Umgang mit modernen Technologien und Sicherheitsmaßnahmen nicht vertraut. Dies kann zu einer inkorrekten Nutzung von IT-Systemen führen und das Risiko von Cyberangriffen erhöhen, beispielsweise durch das unbewusste Öffnen von Phishing-E-Mails oder das Herunterladen von unsicherer Programme.

In den letzten beiden Juniwochen wurden an der Schule rund 50 Cybervorfälle registriert. Im Rahmen der Bachelorarbeit wird eine detaillierte Analyse durchgeführt, um die spezifischen Bedrohungen genauer zu erfassen. Unter den häufigsten Attacken waren

- **Malware-Infektionen**
- **Viren und Trojaner**
- **Phishing-Angriffe**

Da die bisherigen Maßnahmen nur einen minimalen Grundschutz bieten, ist die Entwicklung eines umfassenden Sicherheitskonzeptes dringend erforderlich. Dies soll auf der OCTAVE-Methode basieren und durch bewährte Sicherheitsstandards ergänzt werden.

1.4 Zielsetzung der Arbeit

Das Ziel dieser Bachelorarbeit ist es, zu zeigen, dass ein neu entwickeltes IT-Sicherheitskonzept, das die OCTAVE-Methode in Kombination mit weiteren IT-Sicherheitsansätzen anwendet, die Zahl der Cyberangriffe auf die IT-Infrastruktur der polnischen Schule des Jan III. Sobieski am Kollegium Kalksburg um mindestens 50 % reduziert. Dieses Konzept soll die IT-Infrastruktur der Schule schützen, Cyberangriffe minimieren und den Datenschutz erhöhen. Gleichzeitig soll es als Vorlage für ähnliche Bildungseinrichtungen dienen, die noch über keine Sicherheitsstrategie verfügen.

1.5 Forschungsfrage

Die Forschungsfrage, die mit dieser Arbeit beantwortet werden soll, lautet:

"Reduziert ein neu entwickeltes IT-Sicherheitskonzept, das die OCTAVE-Methode in Kombination mit weiteren IT-Sicherheitsansätzen anwendet, die Zahl der Cyberangriffe auf die IT-Infrastruktur der polnischen Schule des Jan III. Sobieski am Kollegium Kalksburg um mindestens 50 % ?

1.6 Hypothese

Angesichts der zunehmenden Bedrohung durch Cyber-Angriffe und der wachsenden Relevanz robuster IT-Sicherheitsmaßnahmen für Bildungsinstitutionen stellt sich die Frage, inwiefern die Kombination bewährter Sicherheitskonzepte zur Risikominimierung beitragen kann. Auf Basis dieser Überlegung wird nachfolgend die Hypothese formuliert:

"Ein neu entwickeltes IT-Sicherheitskonzept, das die OCTAVE-Methode in Kombination mit weiteren IT-Sicherheitsansätzen anwendet, reduziert die Zahl der Cyberangriffe auf die IT-Infrastruktur der polnischen Schule des Jan III. Sobieski am Kollegium Kalksburg um mindestens 50 %."

1.7 Methodische Vorgehensweise

Die methodische Vorgehensweise, um die formulierte Forschungsfrage zu beantworten, umfasst mehrere Schritte und lässt sich wie folgt unterteilen:

1. **Literaturrecherche und Theorie**

   Das Ziel ist die Schaffung eines guten theoretischen Rahmens für IT-Sicherheit, inklusive der OCTAVE-Methode, weiteren Sicherheitsansätzen wie ISO/IEC 27001 und allgemeinen Informationssicherheitsstandards.

   Im Rahmen dieser Phase werden auch die wissenschaftliche Literatur, Fachartikel und Fallstudien, die die Anwendung der OCTAVE-Methode in Bildungsinstitutionen beschreiben, analysiert.

2. **Analyse der aktuellen IT-Infrastruktur und der Sicherheit.**

   Zweck dieser Studie ist die Analyse und Bewertung der bestehenden IT-Infrastruktur und Sicherheitsmaßnahmen in der polnischen Schule von Jan III Sobieski.

   Um dies zu erreichen, wird wie folgt vorgegangen:

   - Analyse der IT-Infrastruktur, um mögliche Schwachstellen zu identifizieren.
   - Untersuchung von Cyberattacken, um Angriffsmuster und Schwachstellen zu ermitteln.

3. **Risikoanalyse und Bewertung von Risiken.**

Basierend auf der OCTAVE-Methode wird eine umfassende Risikoanalyse durchgeführt. Durch den Einsatz dieser Methode wird die Identifizierung kritischer Assets sowie die Klassifizierung potenzieller Bedrohungen und Schwachstellen möglich.

Das Verfahren, das hier typisch wäre, ist:

- Mittels der erwähnten Methode sollen kritische Assets ermittelt und potenzielle Bedrohungen und Schwachstellen klassifiziert werden.
- Bewertung der Risiken hinsichtlich ihrer möglichen Auswirkungen und Eintrittswahrscheinlichkeit, um Prioritäten für Sicherheitsmaßnahmen festzulegen.

4. **Entwicklung des IT-Sicherheitskonzepts**

Zur Entwicklung eines maßgeschneiderten IT-Sicherheitskonzeptes, das präzise auf die Bedürfnisse der Schule zugeschnitten ist, soll zunächst eine umfassende Risikoanalyse durchgeführt werden. Mittels dieser Analyse werden die relevanten Risiken evaluiert und darauf aufbauend konkrete Maßnahmen konzipiert, um die IT-Systeme der Schule optimal zu schützen. Dabei stehen folgende Schritte im Mittelpunkt:

- Die Ergebnisse der Risikoanalyse werden in ein Sicherheitskonzept eingearbeitet, das ergänzende Sicherheitsmaßnahmen (z. B. Zugangskontrolle, Netzwerksicherheit) und Sicherheitsstandards integriert.
- Konkrete Maßnahmen zur Verbesserung der IT-Sicherheit, die sowohl technische als auch organisatorische und personelle Aspekte umfassen.
- Ein Schulungsplan für Mitarbeiter und Studierende zur Stärkung des Sicherheitsbewusstseins.

5. **Implementierung und Evaluation von Maßnahmen**
   Im Rahmen der Evaluation wird die Wirksamkeit des entwickelten Sicherheitskonzepts ermittelt. Dafür werden ausgewählte Sicherheitsmaßnahmen in der Schule getestet und ihre Auswirkungen analysiert. Gemäß dem Forschungsansatz werden die Sicherheitsvorfälle erfasst und die Auswertung der Nutzerfeedbacks berücksichtigt. Basierend auf den gewonnenen Erkenntnissen erfolgt eine gezielte Anpassung und weitere Optimierung des Sicherheitskonzepts.
6. **Validierung**
   In einem weiteren Schritt wird nun die formulierte Hypothese überprüft und alternative Lösungsansätze untersucht, um die Forschungsfrage möglichst genau zu beantworten. Die bisherigen Ergebnisse werden zusammengefasst und daraus Schlussfolgerungen für die Effektivität des Sicherheitskonzeptes abgeleitet. Gleichzeitig werden die Grenzen der Studie analysiert, um mögliche Schwächen oder unbeantwortete Fragen zu ermitteln. Durch dieses

methodischen Vorgehen wird eine systematische und umfassende Bearbeitung der Forschungsfrage garantiert.

1.8 Aufbau der Arbeit

Die vorliegende Bachelorarbeit ist in zwei Abschnitte geteilt:

1. **Theoretischer Teil (Kapitel 2 bis 5)**

   Dieser Abschnitt legt das Fundament für die vorliegende Arbeit und beleuchtet wichtige Aspekte der IT-Sicherheit sowie die dazugehörigen Methoden und Standards.

   - In Kapitel 2 werden die zentralen Begriffe, Bedrohungsszenarien und Risiken der IT-Sicherheit klar definiert.
   - Kapitel 3 widmet sich der OCTAVE-Methode, wobei deren Ziele, Durchführung und spezifische Anwendung im Bildungsinstitutionen näher erläutert werden.
   - Kapitel 4 erörtert ergänzend weitere Ansätze zur IT-Sicherheit, wie etwa die Norm ISO/IEC 27001 sowie das NIST Cybersecurity Framework. Darüber hinaus wird analysiert, welche Synergien zwischen diesen Methoden bestehen.
   - Kapitel 5 setzt sich mit der aktuellen IT-Sicherheitslage im Bildungssektor auseinander. Mittels der Analyse von Fallstudien werden typische Bedrohungsszenarien diskutiert und daraus wertvolle Best Practices für Bildungsinstitutionen abgeleitet.

2. **Praktischer Teil (Kapitel 6 bis 10)**

   Dieser Teil befasst sich mit der Entwicklung eines IT-Sicherheitskonzepts für die polnische Schule Jan III Sobieski und dessen Umsetzung.

   - Kapitel 6 befasst sich mit dem methodischen Vorgehen zur Entwicklung, Umsetzung und Validierung eines IT-Sicherheitskonzepts für die Polnische Schule Jan III. Sobieski in Wien. Inhaltlich bildet es die Basis für den praktischen Teil der Arbeit und beschreibt detailliert, wie das Sicherheitskonzept von der Bestandsaufnahme der IT-Infrastruktur über die Risikobewertung bis hin zur Implementierung technischer und organisatorischer Maßnahmen sowie deren Evaluation aufgebaut worden ist.
   - Kapitel 7 analysiert die bestehende IT-Infrastruktur der Schule, dokumentiert und bewertet vorhandene Sicherheitsmaßnahmen sowie frühere Cyberangriffe.
   - In Kapitel 8 wird die OCTAVE-Methode zur Risikoanalyse angewendet, um kritische Assets zu identifizieren, deren Bedrohungspotenzial zu bewerten und Prioritäten für Sicherheitsmaßnahmen zu setzen.

- Kapitel 9 konzentriert sich auf die Entwicklung eines umfassenden IT-Sicherheitskonzepts, welches sowohl technische Maßnahmen, wie Netzwerksicherheit, Verschlüsselung und Zugangskontrollen, als auch organisatorische Aspekte, wie Richtlinien, Schulungen und Notfallpläne, berücksichtigt, um Risiken effektiv zu minimieren.
- Kapitel 10 fokussiert sich auf die Implementierung und Evaluierung des in Kapitel 9 entworfenen IT-Sicherheitskonzepts im Schulbetrieb. Im Rahmen dieses Prozesses erfolgt die schrittweise Implementierung und Evaluierung diverser Maßnahmen. Dies umfassen technische Komponenten wie Netzwerksegmentierung, Firewalls und Backup-Systeme sowie organisatorische Elemente wie Awareness-Training, Sicherheitsrichtlinien und Monitoring. Zur Ergänzung der Umsetzung werden Penetrationstests, Nutzerfeedback und eine Wirksamkeitsanalyse durchgeführt. Auf diese Weise soll die Zielerreichung – insbesondere die Reduktion von Cyberangriffen um mindestens 50 % – nachgewiesen und Optimierungspotenziale identifiziert werden.

3. Diskussion und Ausblicke (Kapitel 11)

Im abschließenden Kapitel erfolgt zunächst eine Zusammenfassung der gewonnenen Erkenntnisse, worauf eine Überprüfung der Forschungsfrage sowie eine Reflexion über die Limitationen der vorliegenden Arbeit folgt. Durch diesen klaren und strukturierten Aufbau wird eine fundierte Auseinandersetzung mit der Forschungsfrage gewährleistet, die eine umfassende Analyse und die Implementierung eines praxisnahen IT-Sicherheitskonzepts für Bildungsinstitutionen ermöglicht.

2. Grundlage der Informationssicherheit

Das zweite Kapitel dient dazu, die Grundlagen für die weiteren Abschnitte dieser Arbeit zu schaffen und die Bedeutung der IT-Sicherheit in Bildungseinrichtungen zu beleuchten. Zur besseren Verständnis der Maßnahmen, die dazu beitragen, kritische Informationen zu schützen und die Zuverlässigkeit von IT-Systemen zu gewährleisten, sollten sowohl technische als auch organisatorische Sicherheitsvorkehrungen berücksichtigt werden.

In diesem Kontext sollten ebenso die essenziellen Aspekte der IT-Sicherheit, wie den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen, berücksichtigt werden. "Vertraulichkeit" bedeutet dabei, dass lediglich autorisierte Personen Zugang zu sensiblen Informationen haben (Bishop 2004). "Integrität" bezieht sich auf die korrekte sowie unbeeinträchtigte Datenqualität, während "Verfügbarkeit" den uneingeschränkten Zugriff auf Systeme und ihre Inhalte gewährleistet (Siebenhandl 2011).

Unter dem Begriff "Schutz" wiederum werden alle Maßnahmen verstanden, die dazu dienen, unbefugten Zugriff, Datenverlust sowie andere Bedrohungen zu verhindern (Bruns 2022). "Sensible Daten" bezeichnen in diesem Kontext personenbezogene Informationen von Schülern und Lehrkräften, Prüfungsunterlagen oder vertrauliche Verwaltungsdaten (Priv.Doz. Dr. Lachmaye und Dr. Menzel 2015). Die "Zuverlässigkeit der IT-Infrastruktur" bedeutet, dass die Systeme sicher sind, stabil arbeiten und den täglichen Betrieb nicht beeinträchtigen (Paul 2023).

Im weiteren Verlauf wird die Bedeutung dieser Begriffe für die IT-Sicherheitsstrategie in Bildungseinrichtungen deutlich hervorgehoben und erläutert.

2.1 Einführung in die Informationssicherheit

Aktuelle Tendenzen zeigen, dass zentrale Bereiche wie Wirtschaft, Soziales und Bildung stark von Informationstechnologien beeinflusst werden. Diese Technologien beeinflussen nicht nur das Denken der Gesellschaft, sondern auch die Art und Weise der Kommunikation und des Informationsaustausches. Gleichzeitig bringt die fortschreitende Digitalisierung neue Bedrohungen mit sich, welche gezielt Schwachstellen in den Informationssystemen ausnutzen. Daher befassen sich aktuelle Analysen mit der Frage, wie diese Technologien zur Steuerung der Innovationsentwicklung und zur Optimierung zahlreicher Prozesse eingesetzt werden können, sondern auch mit den daraus resultierenden Sicherheitsrisiken. Ihr Priorität liegt auf dem Schutz sensibler Daten, wie personenbezogene Informationen, Finanztransaktionen und vertrauliche Dokumente, sowie kritischer Systeme, wie Serverinfrastrukturen und Kommunikationsnetzwerke.

2.1.1 Bedeutung der IT-Sicherheit

Die IT-Sicherheit kann als ein ganzheitlicher Ansatz, der alle notwendigen Maßnahmen zusammenführt, um Daten und Systeme vor unbefugtem Zugriff, Manipulation und Vernichtung zu schützen, definieren werden (N. Pohlmann 2024). Um ein Höchstmaß an Schutz sicherzustellen, werden aufeinander abgestimmte technische sowie organisatorische Maßnahmen notwendig, die eine sichere und zuverlässige IT-Infrastruktur gestalten. Dies bedeutet nicht nur einen umfassenden Schutz der Systeme vor Angriffen, sondern auch, die Aufrechterhaltung ihrer Verfügbarkeit und Funktionalität in jeder Situation (N. Pohlmann 2022).

Ein weiterer wesentlicher Aspekt ist die Sensibilisierung aller Nutzer, die in der Sicherheitskette oft als schwächstes Glied angesehen werden. Durch regelmäßige Schulungen und klare Richtlinien können potenzielle Risiken reduziert werden, die durch menschliche Fehler entstehen (Niederösterreich, Technologie- und InnovationsPartner 2023).

2.1.2 Die drei zentralen Prinzipien der IT-Sicherheit

Wie bereits in der Einleitung des zweiten Kapitels erläutert, basieren IT-Sicherheitskonzepte auf drei zentralen Säulen: **Vertraulichkeit, Integrität und Verfügbarkeit**. Diese drei Prinzipien bilden eine solide Grundlage für die Entwicklung effektiver Sicherheitsmaßnahmen (Rayanne 2023).

2.1.2.1 Vertraulichkeit

Die Vertraulichkeit garantiert, dass nur autorisierte Personen den Zugang zu sensiblen Daten wie Patientendaten im Gesundheitssektor, Kontoinformationen im Finanzwesen und Prüfungsunterlagen im Bildungswesen erhalten können (Wies 2024). Vor diesem Hintergrund ist es besonders wichtig zu verstehen, dass ein Datenleck nicht nur finanzielle Verluste, sondern auch schwerwiegende rechtliche Konsequenzen und erheblichen Imageverlust nach sich ziehen kann (Hirsch, et al. 2024).

Um solchen Bedrohungen effektiv vorzubeugen – und damit den Schutz von Daten zu gewährleisten – ist die Implementierung geeigneter Technologien und Sicherheits-maßnahmen, die die Vertraulichkeit von Informationen sicherstellen, unerlässlich. In diesem Kontext spielen moderne Verschlüsselungsalgorithmen wie AES (Advanced Encryption Standard) eine zentrale Rolle, da sie eine sichere Speicherung und Übertragung von Daten ermöglichen. Darüber hinaus erhöht die Multi-Faktor-Authentifizierung (MFA) die Sicherheit, indem sie eine zusätzliche Schutzebene schafft und das Risiko unbefugter Zugriffe minimiert (Nekkanti und NR 2022).

Die Bedeutung von AES zeigt sich vor allem darin, dass Informationen ohne den entsprechenden Schlüssel für den Angreifer unlesbar bleiben - selbst wenn der Angreifer Zugriff auf das System erhält. Darüber hinaus kommt den strikten Zugriffskontrollen eine

besondere Bedeutung zu, die einerseits durch Rollen- und Berechtigungskonzepte, sowie die Implementierung der MFA (z.B. Fingerabdruck oder Gesichtserkennung) erreicht wird (Nekkanti und NR 2022). Die dargestellten Beispiele verdeutlichen, dass die Kombination aus Verschlüsselungstechnologien wie AES und Maßnahmen zur Zugriffskontrolle wie MFA wesentliche Elemente eines umfassenden Datenschutzkonzepts darstellt und das Risiko von Datendiebstahl reduziert.

Trotz der Anwendung fortschrittlicher Sicherheitstechnologien sind weiterhin Bedrohungen zu verzeichnen, derer Ursache in der Regel menschliche Fehler, welche oft das schwächste Glied im Datenschutzsystem repräsentieren, sind. Besonders deutlich wird dies bei Phishing-Angriffen, die laut Untersuchungen von IDSA (Identity Defined Security Alliance) zu den häufigsten Methoden gehören, die die Vertraulichkeit von Informationen verletzen (Identity Defined Security Alliance 2023). Der Versand von täuschend echter E-Mails, die Benutzer dazu bringen, vertrauliche Zugangsdaten preiszugeben, können hier als Beispiel herangezogen werden. Um solchen Bedrohungen entgegenzuwirken, ist auch ein hohes Maß an Sicherheitsbewusstsein, welches durch gezielte Sensibilisierung und Schulung erreicht werden kann, unerlässlich (Kersten, Reuter und Schröder 2013). Folglich kann auch das Risiko solcher Angriffe effektiv und langfristig minimiert werden.

2.1.2.2 Integrität

Neben der Vertraulichkeit spielt auch die Integrität, die eng mit deren Unversehrtheit und Korrektheit zusammenhängt, eine entscheidende Rolle. Gemäß der Definition bedeutet Integrität, dass Daten nicht verändert werden und ihre ursprüngliche Form erhalten bleiben (Harmes 2024). An dieser Stelle sei hervorgehoben, dass schon kleinste Änderungen dieser Form insbesondere im Kontext von Geschäftsprozessen und Entscheidungsfindungen gravierende Konsequenzen haben könnten. Um die Integrität der Daten zu gewährleisten, kommen verschiedene Methoden zum Einsatz, darunter digitale Signaturen, Prüfsummen und Hash-Verfahren wie SHA (Secure Hash Algorithm) (Spitz, Pramateftakis und Swoboda 2011).

Prüfsummen sind mathematische Werte, die durch Algorithmen aus Ursprungsdateien berechnet werden. Sie fungieren als eine Art Fingerabdruck, mit dem man überprüfen kann, ob sich die Daten während der Übertragung oder Speicherung nicht verändert haben. Weicht die Prüfsumme der empfangenen Daten vom Original ab, dann bedeutet dies, dass die Daten beschädigt wurden oder ein Übertragungsfehler aufgetreten ist. Ein typisches Beispiel für den Einsatz dieser Verfahren ist CRC (Cyclic Redundancy Check), das häufig in Netzwerken oder Datenspeichern eingesetzt wird (Spitz, Pramateftakis und Swoboda 2011).

Ein verwandter, jedoch erheblich komplexerer Ansatz ist die Anwendung kryptografischer Hash-Funktionen, zu denen der "Secure Hash Algorithm" (SHA) zählt. Im Gegensatz zu Prüfsummen, die vorrangig der Fehlererkennung dienen, bieten krypto-

grafische Hash-Funktionen wie der SHA durch ihre mathematische Struktur einen zusätzlichen Schutz gegen Manipulationsversuche. Diese Verfahren wurden speziell entwickelt, um die Sicherheit und Integrität digitaler Daten zu gewährleisten und verfolgen dasselbe grundlegende Prinzip: die Transformation eines beliebigen Eingabewerts in eine eindeutige Ausgabe von fester Länge (Spitz, Pramateftakis und Swoboda 2011).

Es ist an dieser Stelle von Bedeutung, darauf hinzuweisen, dass der Anwendungsbereich des SHA über die reine Integritätsprüfung hinausgeht. So findet er unter anderem Verwendung bei der Erstellung digitaler Signaturen, der Verschlüsselung von Zertifikaten und der Sicherung von Passwörtern. Bereits geringfügige Änderungen an den ursprünglichen Daten führen zu einer signifikanten Abweichung des resultierenden Hash-Wertes, was die Robustheit dieser Methode gegen unbefugte Modifikationen unterstreicht (Wenzel-Benner und Wasserrab 2015).

Zu den prominentesten Versionen dieser Funktionalität gehören SHA-1, SHA-256 und SHA-512. Die Zahl hinter der Bezeichnung gibt dabei die Länge des Hash-Wertes in Bits an. Wie aktuelle Studien nahelegen, bevorzugen moderne sicherheitskritische Anwendungen insbesondere SHA-256 und SHA-512, da diese durch ihre längeren Ausgaben und komplexeren Algorithmen einen höheren Schutz gegen Angriffe bieten (Gitlan 2025), (Eckert 2013). Aus diesen Ausführungen lässt sich folgern, dass kryptografische Hash-Funktionen wie SHA nicht nur theoretisch, sondern auch praktisch eine unverzichtbare Komponente in der Sicherung sensibler Daten darstellen.

Eine weitere innovative Lösung zur Gewährleistung der Datenintegrität ist die Blockchain-Technologie. Sie gewährleistet, dass Daten sowohl bei der Übertragung als auch bei der Speicherung in ihrer ursprünglichen Form unverändert bleiben. Die Entwicklung neuer Sicherheitsmaßnahmen und die immer raffinierteren Techniken der Cyberkriminellen können jedoch dazu führen, dass selbst hochkomplexe Systeme wie cloudbasierte Netzwerke oder Blockchain-Lösungen mit modernen kryptografischen Mechanismen überlistet werden können (Groopman 2023).

Die vorliegende technologische Lösung ist ein herausragendes Beispiel für die Anwendung kryptografischer Verfahren zur Datensicherung und gleichzeitig ein dezentrales System zur Speicherung und Verwaltung von Informationen. Charakteristisch für dieses System ist die kontinuierlich wachsende Kette von Blöcken, auch bekannt als Blockchain. An dieser Stelle sei besonders hervorgehoben, dass jeder Block kryptografisch mit dem vorherigen verknüpft ist. Daraus folgt, dass die Daten eines Blocks, sobald dieser zur Kette hinzugefügt wurde, persistent sind und aufgrund der dezentralen Natur des Netzwerks nahezu unveränderbar bleiben, weil diese Chain nicht von zentralgebundenen Hauptserver sondern von einem Knoten (Netzwerk aus Computer) verteilt und verwaltet wird. Es lässt sich zweifellos sagen, dass diese Struktur auf einem besonders sicheren Prinzip basiert: Jede nachträgliche Modifikation würde eine Änderung aller nachfolgenden Blöcke erfordern, was mit einem enormen Aufwand

verbunden ist. Diese Eigenschaften unterstreichen die außergewöhnliche Widerstandsfähigkeit der Blockchain-Technologie gegen Manipulationen, was sie zu einem weit verbreiteten Werkzeug macht, das über das bloße Fundament von Kryptowährungen wie Bitcoin oder Ethereum hinausgeht (Bundesnetzagentur für Elektrizität, Gas,Telekommunikation, Post und Eisenbahnen 2021). Exemplarisch kann die Blockchain im Supply Chain Management eingesetzt werden, um vollständige Transparenz bei der Überwachung der Herkunft und des Warenflusses sowie im Gesundheitswesen, wo sie die sichere Speicherung und Freigabe medizinischer Daten ermöglicht, zu gewährleisten (Jede, Bensberg und Klein 2024).

Trotz hoher Sicherheit und Dezentralisierung sind potenzielle Schwachstellen dieser Technologie nicht ganz auszuschließen. Ein gutes Beispiel dafür ist der so genannte "51 %-Angriff", bei dem ein Angreifer/ Häcker die Kontrolle über die Mehrheit der Rechenleistung im Netzwerk ergreift und dadurch das Netzwerk manipulieren kann. Auch Schwachstellen in den Anwendungen, die auf der Blockchain basieren (wie z.B. Smart Contracts), können gleichermaßen von den Cyberkriminellen ausgenutzt werden. Daher ist es so wichtig, dass man die Blockchain und die Anwendungen sichert um dadurch Risiko zu minimiert und die Widerstandsfähigkeit der Systeme gegen Angriffe zu erhöhen (Groopman 2023).

2.1.2.3 Verfügbarkeit

Die Verfügbarkeit zielt darauf ab, den ständigen Zugriff auf Systeme und Daten zu gewährleisten. Sie ist die Grundlage für das reibungslose Funktionieren von Organisationen und Bildungseinrichtungen, da jeder Systemausfall schwerwiegende Folgen einschließlich Vertrauensverlust und Imageverlust, haben kann (Harmes 2024).

Distributed Denial-of-Service-Attacken (DDoS) sind eine der gängigsten Formen der Einschränkung des Systemzugangs. Bei solchen Attacken werden Systeme mit einer Flut von Anfragen bombardiert, was letztendlich zu einer Leistungsabnahme der Systemleistung und im Extremfall zu einem vollständigen Ausfall der Dienste führt (Rayanne 2023). Um solche Angriffe abzuwehren, sollten fortschrittliche Lösungen wie die Verteilung des Datenverkehrs zwischen verschiedenen Servern über Content Delivery eingesetzt werden, welche den Datenverkehr zwischen zahlreichen Servern aufteilen und dadurch das Risiko einer Überlastung minimieren (Wies 2024), (Eckert 2013), (Kienzle 2022).

2.1.3 Herausforderungen und Zukunftsperspektiven der IT-Sicherheit

Neue Herausforderungen für die IT-Sicherheit ergeben sich aus der Entwicklung von Technologien wie Cloud-Services, die Unternehmen Flexibilität und Skalierbarkeit bieten und es ihnen ermöglichen, ihre Ressourcen dynamisch an sich ändernde Anforderungen anzupassen (Bedner 2013). Der Einsatz dieser Lösungen zwingt Unternehmen, einen

besseren Datenschutz zu implementieren, einschließlich fortschrittlicher Verschlüsselung, regelmäßiger Sicherheitsaudits und strenger Zugriffs-richtlinien.

Ein weiterer bedeutender Problembereich, der auch nicht unerwähnt bleiben soll, ergibt sich insbesondere im Kontext der Remote-Arbeit aus der zunehmenden Nutzung mobiler Geräte und dem BYOD-Modell (Bring Your Own Device), das einerseits die Arbeitsflexibilität, andererseits aber auch die Möglichkeit von Cyberangriffen auf diese Geräte (Laptops, Notebooks, Smartphones, Tablets) erhöht. Um diese Geräte zu schützen, verpflichten sich viele Institutionen zur Implementierung oder zum Einsatz von Mobile Device Management Systemen (MDM), die den Zugriff auf die Daten von diesen Organisationen überwachen, aktualisieren und steuern (Sobota 2022).

Um die Effektivität von IT Sicherheit zu erhöhen und das Risiko menschlicher Fehler zu verringern, sollten Unternehmen und Bildungsinstitutionen in die Schulung ihrer Mitarbeiter investieren, damit die Bedrohungen wie Phishing, Malware oder unberechtigten Zugriff frühzeitig erkennen (Kersten, Reuter und Schröder 2013). Die Kombination der richtigen technologischen Tools mit den richtigen Trainings schafft eine umfassende und konsistente Schutzstrategie, die die Widerstandsfähigkeit eines Unternehmens bzw. einer Institution gegen moderne Cyberbedrohungen erhöht.

Zusammenfassend lässt sich sagen, dass die IT-Sicherheit ein dynamisches und herausforderndes Feld bleibt, welches kontinuierlich angepasst werden muss. Unternehmen, Organisationen und Bildungsinstitutionen müssen robuste Sicherheits-konzepte implementieren und ihre Systeme fortlaufend an neue Bedrohungen anpassen. Um die Sicherheit in einer zunehmend digitalisierten Welt zu gewährleisten, ist ein zukunftsorientierter Ansatz erforderlich, der sowohl präventive als auch innovative Lösungen berücksichtigt.

2.2 Überblick über Bedrohungen und Risiken in der IT

Die Grundprinzipien der IT-Sicherheit - Vertraulichkeit, Integrität und Verfügbarkeit - wurden bereits teilweise in Kapitel 2.1 erläutert. Diese Grundsätze bilden die Grundlage für den Schutz moderner IT-Infrastrukturen und dienen als Rahmen für die Entwicklung von Sicherheitsmaßnahmen. Es zeigt sich allerdings, dass die digitale Landschaft durch permanent neue Bedrohungen gekennzeichnet ist, die sowohl technischer als auch menschlicher Natur sein können. Um diesen Bedrohungen entgegenzuwirken, ist es notwendig, das Risiko im Kontext der IT-Sicherheit tiefer zu verstehen. So kann Risiko als eine Kombination aus der Wahrscheinlichkeit des Auftretens einer Bedrohung, die sich auf die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten und Systemen auswirkt, und den potenziellen Schäden, die sich aus diesem Ereignis ergeben können, definiert werden (Finanzmarktaufsichtsbehörde (FMA) 2018).

2.2.1 Definition von Risiko in Bezug auf IT-Sicherheit

Um Risiko im Kontext der IT-Sicherheit zu verstehen, ist es erforderlich, zwei Schlüsselkomponenten dieses Begriffs näher zu erläutern:

- **Eintrittswahrscheinlichkeit:** Die Eintrittswahrscheinlichkeit eines Risikos hängt von mehreren Faktoren ab, wie z. B. der Art des Risikos, der Sicherheitsinfrastruktur und bestehenden Schwachstellen.
- **Potentieller Schaden:** Dies ist nichts Anderes als mögliche Folgen, die finanzielle, rechtliche, betriebliche oder Reputationsschäden haben können. (Bundesamt für Sicherheit in der Informationstechnik 2017)

Aus der obigen Definition lässt sich einerseits eine Formel zur Berechnung des Risikos ableiten:

$$\boldsymbol{Risiko = potentieller\ Schaden\ x\ Eintrittswahrscheinlichkeit}$$

Andererseits bietet eine Risikoanalyse die Möglichkeit, Sicherheitsmaßnahmen dort einzusetzen, wo sie den größten Nutzen bringen können. Um die Berechnungen durchzuführen, müssen die beiden Werte (Schadenspotential, Eintrittswahrscheinlichkeit) noch klassifiziert werden. Hierbei empfiehlt es sich vier Schadensklassen zu definieren: **gering, mittel, hoch und kritisch**, um die Risiken entsprechend einzustufen (Stoiber 2019).

2.2.2 Malware als zentrale Bedrohung moderner IT-Systeme

Eine der Hauptbedrohungen moderner IT-Systeme stellt Schadsoftware, in der Fachliteratur auch als "Malware" bezeichnet, dar. Dieses Begriff fasst verschiedene Arten von schädlicher Software zusammen, die gezielt entwickelt wurden, um Systeme zu manipulieren, zu beschädigen oder sogar vollständig zu zerstören (IONOS Digital Guide 2024).

Um den Gefahren, die von solcher Software ausgehen, effektiv entgegenzuwirken, ist die Durchführung einer umfassenden Risikoanalyse notwendig. In diesem Zusammenhang sind zwei wesentliche Aspekte zu berücksichtigen:

- **Eintrittswahrscheinlichkeit**: Insbesondere bei unzureichenden Sicherheitsvorkehrungen, veralteter Software oder der Nutzung unsicherer Netzwerke ist die Wahrscheinlichkeit einer Malware-Attacke hoch.
- **Potentieller Schaden**: Je nach Art der Schadsoftware können gravierend sein. Dazu gehören Datenverlust und finanzielle Einbuße ebenso wie Imageverlust oder ein kompletter Systemcrash. (Siebenhandl 2011)

2.2.2.1 Varianten der Schadsoftware

Um die Funktionsweise von Schadsoftware besser zu verstehen und geeignete Schutzmaßnahmen zu implementieren, ist eine ausführliche Analyse von verschiedenen

Schadsoftwarearten notwendig. Zu den weit verbreitetsten und am stärksten etablierten Varianten zählen:

1. **Adware und Spyware** – schalten unerwünschte Werbung oder protokollieren heimlich Benutzerdaten, um an die vertrauliche Informationen zu gelangen.
2. **Viren** – infizieren Dateien und können durch eigene Replikation erhebliche Systemstörungen verursachen.
3. **Würmer** – verbreiten sich im Gegensatz zu Viren eigenständig über Netzwerke, ohne dass Nutzeraktivitäten erforderlich sind. Dieser Prozess der Schadsoftwareverbreitung binnen eines Netzwerks oder über verschiedene Systeme wird als Dispersion bezeichnet. Allerdings resultiert der tatsächliche Schaden, der durch Würmer verursacht wird, nicht aus ihrer Verbreitung selbst, sondern aus den Aktionen, die auf den infizierten Systemen ausgeführt werden. Hierzu zählen das Löschen von Daten, die Installation weiterer Schadsoftware oder das Überlasten von Netzwerken, infolgedessen ganze IT-Systeme lahm gelegt werden können. Aufgrund ihrer autonomen Verbreitungsfähigkeit sind Würmer in der Lage, in kürzester Zeit eine Vielzahl von Systemen zu infizieren und somit den potenziellen Schaden zu vervielfachen.
4. **Ransomware** – verschlüsseln die Daten und fordern für Wiederherstellung des Zugriffs Lösegeld von den Nutzern. (IONOS Digital Guide 2024), (Eckert 2013)

Eine der am meisten bagatellisierten Bedrohungen und zugleich eine der gängigsten Methoden, um vertraulichen Informationen wie Login- oder Kreditkartendaten zu stehlen, ist Phishing (Blumberg und Pohlmann 2006). Im Folgenden wird eine grobe Analyse der Phishing-Risiken dargelegt, die Eintrittswahrscheinlichkeit und potentieller Schaden berücksichtigt:

- **Eintrittswahrscheinlichkeit:** Diese Bedrohung ist einerseits aufgrund des unzureichenden Bewusstseins der Mitarbeiter, andererseits aufgrund der zunehmenden Komplexität von Phishing-Nachrichten und gefälschten Seiten hoch.
- **Potentieller Schaden:** Dieser kann sowohl finanzielle Natur, als auch Imageverlust sein. (Vayansky und Kumar 2018)

Phishing-Angriffe zielen auf die psychologischen Schwächen des Opfers ab, indem sie Ängste oder Druck erzeugen, um eine schnelle Handlung hervorzurufen. Einer der gefährlichsten Methoden ist das sogenannte Spear-Phishing, bei dem der Angriff gezielt gegen bestimmte Personengruppen oder Unternehmen gerichtet wird (Tzipora, Nasir und Oded 2015). Charakteristisch für diese Art des Phishings sind:

- **Sammeln von Informationen** – z. B. über soziale Medien oder professionelle Netzwerke. Der Angreifer sammelt detaillierte Informationen über das Angriffsziel.

- **Personalisierung** – E-Mails enthalten häufig Namen und Informationen über bekannte Personen oder Organisationen und können von den Benutzern als vertraulich und authentisch eingestuft werden.
- **Manipulation** – Opfer werden dazu gedrängt, bestimmte Aktionen wie das Öffnen schädlicher Links, die Offenlegung vertraulicher Informationen oder die Überweisung von Geldern durchzuführen. (Tzipora, Nasir und Oded 2015)

Dabei stellt sich auch die Frage, welche Strategien und Maßnahmen am effektivsten sind, um derartigen Angriffen entgegenzuwirken ?

Als Antwort auf diese Frage könnten folgende Maßnahmen vorgeschlagen werden:

- **Sensibilisierung und Schulung** – Eine gezielte Sensibilisierung der Benutzer für solche Angriffe ist erforderlich.
- **Technische Maßnahmen** – Der Einsatz von Spam-Filter, Multi-Faktor-Authentifizierung und E-Mail-Scanner kann dabei helfen, verdächtige Nachrichten rechtzeitig zu identifizieren.
- **Manuelle Überprüfung** – Die sorgfältige manuelle Überprüfung der Absenderadressen und des Inhalts der Nachricht durch die Mitarbeiter ist von entscheidender Bedeutung. Im Zweifelsfall sollte die IT-Abteilung kontaktiert werden. (Siebenhandl 2011)

2.2.2.2 Verbreitungsmethoden der Schadsoftware

Die Schadsoftware breitet sich durch verschiedene Kanäle aus und nutzt dabei sowohl technische als auch menschliche Schwachstellen. Zu den wichtigsten Verbreitungs-methoden zählen:

1. **E-Mail-Anhänge und Links:** Phishing- und Spear-Phishing-E-Mails enthalten in der Regel schädliche Links oder Anhänge, mit dem Ziel, Benutzer dazu zu verleiten, infizierte Dateien zu öffnen bzw. manipulierten Webseiten aufzurufen (Verbraucherzentrale NRW 2021).
2. **Drive-by-Downloads**: Die Installation von Schadsoftware erfolgt häufig heimlich über Webseiten oder durch infizierte Werbung, vor allem, wenn der Benutzer eine veraltete oder nicht aktualisierte Software nutzt (Cova, Kruegel und Vinga 2010).
3. **Exploit-Kits und Zero-Day-Exploits:** Exploit-Kits sind speziell entwickelte, automatisierte Tools, die darauf abzielen, Sicherheitslücken zu identifizieren und auszunutzen (Kurniawan und Fitriansyah 2018). Von besonderer Relevanz sind in diesem Zusammenhang die sogenannten Zero-Day-Exploits. Dabei handelt es sich um Schwachstellen, die von Angreifern entdeckt und ausgenutzt werden, bevor der Hersteller die Möglichkeit hat, eine Sicherheitsaktualisierung bereitzustellen (Waheed, et al. 2024).
4. **USB-Sticks und Speichermedien:** Externe Speichermedien, die mit Schad-software infiziert sind, können über Autostart-Funktionen oder manipulierte

Dateien zur Verbreitung schädlicher Software beitragen (Verbraucherzentrale NRW 2021). Das geschieht häufig durch eine unvorsichtige Nutzung externer Datenträger, vor allem innerhalb eines Firmennetzwerks.

5. **Soziale Netzwerke und Messenger:** Die Verbreitung schädlicher Hyperlinks oder Dateien erfolgt in vielen Fällen über kompromittierte Konten sowie mittels gezielter Social-Engineering-Techniken, welche das Vertrauen der Nutzer ausnutzen (Verbraucherzentrale NRW 2021).
6. **Infizierte Software-Downloads:** Kompromittierte oder manipulierte Programme aus unbekannten Quellen wie Torrents, kostenlosen Software oder unautorisierten App-Stores können Schadsoftware enthalten (Bundesamt für Sicherheit in der Informationstechnik 2024).
7. **Remote-Angriffe (RDP-Exploits):** Die Verbreitung von Schadsoftware kann auch durch Brute-Force-Angriffe erfolgen, bei denen automatisiert Passwörter ausprobiert werden, um Zugriff auf RDP-Sitzungen zu erhalten. Diese Methode ist besonders gefährlich, da sie Schwachstellen im Remote-Desktop-Protokoll ausnutzt, um unbefugten Zugriff auf Systeme zu erlangen. Solche Angriffe ermöglichen häufig die vollständige Kontrolle über die betroffenen Systeme und werden oft auch für Ransomware-Angriffe verwendet (Vitla 2024).

2.2.3 Technische Risiken der IT-Infrastruktur

Eine weitere nicht zu unterschätzende Gefahr für IT-Systeme liegt in ihrer teils veralteten und nicht immer optimal gewarteten Infrastruktur, welche Hacker aufgrund technischer Mängel und Sicherheitslücken als Tür für Angriffe nutzen können. Die Folgen einer erfolgreichen Attacke können von kleinen Ausfälle bis zu Systemcrashs reichen und damit auch erhebliche finanzielle Verluste verursachen. Umso wichtiger ist es daher, Schwachstellen und mögliche Einfallstore in der bestehenden Netzwerkarchitektur durch eine gründliche Risikoeinschätzung genau unter die Lupe zu nehmen. Zu diesen Bedrohungsquellen gehören etwa:

- **Veraltete Systeme** – für die der Betreiber keinen technischen Support mehr anbietet.
- **Fehlende Aktualisierungen** – Systeme ohne regelmäßige Updates sind anfällig für Sicherheitslücken.
- **Ungesicherte Netzwerke** – sind solche, die schwache oder keine Verschlüsselung besitzen und dadurch das Risiko des unbefugten Zugriffs erhöhen.
- **Fehlkonfigurationen** – bei der Einrichtung und Konfiguration von Systemen und Anwendungen öffnen unabsichtlich neue Angriffsflächen. (Blumberg und Pohlmann 2006)

Besonders wichtig bei der Beseitigung dieser Schwachstellen sollte die Risiko-Priorisierung sein, um die Gefahr von Angriffen und Ausfällen zu minimieren.

2.2.4 Der menschliche Aspekt als Risikofaktor in der IT-Sicherheit

Ein zentrales Thema innerhalb der IT-Sicherheit, welches in diesem Kapitel noch erörtert wird, ist der menschliche Aspekt, weil die Fehlerhaftigkeiten, Fahrlässigkeit oder vorsätzliche Fehlhandlungen, die durch diesen Faktor hervorgerufen werden, zu gravierenden Konsequenzen führen können (A-SIT Zentrum für sichere Informationstechnologie - Austria 2024). Um die Auswirkungen des Faktors auf die Sicherheit von Systemen genauer zu verstehen, werden im Folgenden zentrale Einflussfaktoren analysiert:

- **Wahrscheinlichkeit** – eines Verstoßes gegen die Sicherheitsrichtlinien, sowohl absichtlich als auch unbeabsichtigt, ist aufgrund der Art der menschlichen Handlungen ziemlich hoch.
- **Potentieller Schaden** – dazu gehören Datenverlust, unbefugte Zugriff auf vertrauliche Informationen und ein langfristiger Imageverlust. (A-SIT Zentrum für sichere Informationstechnologie - Austria 2024)

Innere Bedrohungen stellen eine besonders schwer zu bewältigende Herausforderung dar, da sie häufig auf das Fehlverhalten von aktuellen oder ehemaligen Mitarbeitern zurückzuführen sind, die ihre Systemberechtigungen missbrauchen. (Kienzle 2022). Solche Taten können weitreichende Auswirkungen auf Unternehmen haben, daher ist es von äußerster Bedeutung, wirksame Vorsichtsmaßnahmen zu implementieren. Dazu gehören beispielsweise:

- **Systematische Schulungen** zur Sensibilisierung der Mitarbeiter für IT-Sicherheit.
- **Beschränkung des Zugriffs** auf Daten und Systeme auf das erforderliche Minimum.
- **Regelmäßige Berechtigungsprüfungen** zur Vermeidung nicht autorisierter Zugriffe. (Olaoye und Egon 2024)

Insbesondere im Kontext interner Bedrohungen ist eine umfassende Betrachtung bzw. Herangehensweise, der die Bildung, Kontrolle und klare Prozesse kombiniert, der Schlüssel zur wirksamen Risikominderung, die sich aus dem menschlichen Faktor ergibt.

2.2.5 Bedeutung der IT-Sicherheit für Bildungsinstitutionen

Der letzte Aspekt der Cybersicherheit, der hier behandelt wird, ist ihre Bedeutung für Bildungsinstitutionen, die unzählige sensible Daten verarbeiten und vor besonderen, komplexen Herausforderungen stehen. In diesem Zusammenhang bietet eine umfassende Risikoanalyse die Möglichkeit, sowohl die Wahrscheinlichkeit eines

Sicherheitsvorfalls als auch die daraus resultierenden potenziellen Schäden zu diskutieren, die im Folgenden näher erläutert werden:

- **Eintrittswahrscheinlichkeit** – Aufgrund der Nutzung privater Geräte, begrenzter IT-Ressourcen und offener Netzwerke sind Bildungsinstitutionen besonders anfällig für Angriffe.
- **Potentieller Schaden** – dazu gehört die Verletzung der Vertraulichkeit von Schüler- und Mitarbeiterdaten und die Störung des Unterrichtsprozesses. (Donaldson, Williams und Siegel 2018)

Um die oben genannten Risiken dieser Institutionen zu minimieren, müssen folgende Maßnahmen ergriffen werden:

- **Regelmäßige Schulungen** zur Sensibilisierung des Personals und der Studierenden für IT-Sicherheit werden, wie bereits mehrfach in diesem Abschnitt erwähnt, durchgeführt.
- **Firewalls und andere technische Lösungen** wie Antivirenprogramme oder sichere Netzwerkprotokolle werden verwendet.
- **Trennung kritischer Systeme** von allgemeinen Netzwerke. (Siebenhandl 2011), (N. Pohlmann 2022)

Zusammengefasst bedarf Cybersicherheit in Bildungsinstitutionen ständiger Adaptationen und Verbesserungen. In diesem Kontext ist eine gründliche Risikoeinschätzung eine Basis für effektive Schutzvorkehrungen, die sowohl die Eintrittswahrscheinlichkeit als auch potenzielle Schäden berücksichtigen. Erst die Kombination moderner Technologien, organisatorischer Maßnahmen und des Nutzerbewusstseins kann die IT-Sicherheitsprinzipien wie Vertraulichkeit, Integrität und Verfügbarkeit langfristig absichern.

3. OCTAVE-Methode

Dieses Kapitel konzentriert sich auf die OCTAVE-Methode, die eine entscheidende Rolle bei der Entwicklung von IT-Sicherheitskonzepten spielt. Diese Methode dient der Identifizierung von IT-Risiken und der Entwicklung geeigneter Maßnahmen zur Risikominimierung und wurde von der Carnegie Mellon University entwickelt (Paulsen 2012). Sie wird im Kontext ihrer Anwendung in Bildungseinrichtungen betrachtet und ausführlich in den folgenden Abschnitten behandelt:

- Grundlagen und Ziele der OCTAVE-Methode (sieh Abschnitt 3.1)
- Ablauf der OCTAVE-Methode (sieh Abschnitt 3.2)
- Anwendung der OCTAVE-Methode in Bildungsinstitutionen(sieh Abschnitt 3.3)

3.1 Grundlagen und Ziele der OCTAVE-Methode

Mitte der 1990er Jahre vom Carnegie Mellon Software-Engineering Institute entwickelte Methode zur Bewertung operativer Risiken, Ressourcen und Sicherheitslücken – die sogenannte OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation)* – ist ein bewährter, strukturierter Ansatz, der die Organisationen, einschließlich Bildungsinstitutionen, dabei unterstützt, Risiken im Kontext von IT-Sicherheit zu identifizieren und zu managen (Paulsen 2012). Der entscheidende Vorteil dieser Methode liegt in der Kombination verschiedener Perspektiven, bei der sowohl technische als auch organisatorische und menschliche Faktoren berücksichtigt werden. Hervorzuheben ist auch, dass diese Methode nicht nur ein umfassendes Sicherheitsprofil von Unternehmen erstellt, sondern auch die Grundlage für ein strategisches Management von IT-Sicherheitsrisiken bildet (Paulsen 2012). Dabei ist vor allem die hohe Flexibilität des Ansatzes von Bedeutung. Sie ermöglicht nicht nur die Anpassung an spezifische Anforderungen und dynamische Gegebenheiten, sondern unterstützt auch die effektive Umsetzung in verschiedenen Organisationsbereichen unter Berücksichtigung der individuellen Prioritäten und Bedürfnisse der jeweiligen Organisation (Alberts, et al. 2025). In diesem Zusammenhang konzentriert sich die Methode auf die Erreichung folgender Ziele:

- **Erkennung und Reduktion von Bedrohungen:** Basierend auf einer strukturierten Analyse von Schwachstellen und potenziellen Gefahren hilft diese Methode Organisationen, Sicherheitsrisiken zu identifizieren, zu bewerten und wirksame Maßnahmen zur Minimierung dieser Risiken zu entwickeln.
- **Identifikation kritischer Assets:** In dieser Phase werden Schlüsselressourcen wie Kundendatenbanken, IT-Infrastruktur oder geistiges Eigentum bewertet, die für den Unternehmenserfolg entscheidend sind.
- **Einbindung relevanter Beteiligter:** Dieser integrierte Ansatz ermöglicht fundierte Entscheidungen zu treffen und eine umfassende Analyse zu erhalten,

die auf der aktiven Beteiligung von Entscheidungsträgern und Experten aus unterschiedlichen Bereichen basiert. (Paulsen 2012)

Die Methode ist in drei klar definierte und aufeinander aufbauende Phasen gegliedert, wodurch eine systematische Bewertung ermöglicht wird:

- **Organisatorische Perspektive** – ermittelt potenzielle Bedrohungen sowie deren Signifikanz. Zusätzlich wird eine umfassende Analyse bestehender Sicherheitspraktiken durchgeführt, um Schwachstellen und Verbesserungspotenziale zu identifizieren. Das Hauptziel dieser Phase besteht darin, eine soliden Basis für die darauffolgenden Schritte zu schaffen.
- **Technologische Perspektive** – dient der Entwicklung geeigneter Sicherheitsstrategien, die zunächst eine Analyse der Verantwortlichkeiten und Prozesse innerhalb der IT-Abteilung verlangen sowie der Bedrohungen und Schwachstellen der Infrastruktur, die sich potenziell auf die identifizierten kritischen Ressourcen auswirken könnten.
- **Strategische Planung** – legt besonderen Wert auf die Entwicklung einer langfristigen Sicherheitsstrategie, die in enger Relation zu den Geschäftszielen der Organisation steht und auf identifizierten und priorisierten Bedrohungen basiert. Auf dieser Basis werden spezifische Schutzmaßnahmen erarbeitet. (Paulsen 2012)

Zum Abschluss werden spezifische Merkmale dieser Methode, die sie als besonders wirksam und adaptionsfähig machen, aufgezählt:

- **Anpassungsfähigkeit und Skalierbarkeit** – Die Methode ist an die Bedürfnisse und Strukturen unterschiedlicher Organisationen und Institutionen anpassbar. Des Weiteren ermöglicht sie eine effektive Risikobewertung, unabhängig von der Komplexität der Organisation.
- **Stärkung der Selbstorganisation** – Sie ermöglicht auch die selbständige Durchführung von Risikobewertungen und reduziert die Abhängigkeit von externen Experten. Dies resultiert im Endeffekt in einer Stärkung der Sicherheitskultur und in Kosteneinsparungen.
- **Ganzheitlicher Ansatz** – Octave berücksichtigt verschiedene Faktoren, darunter technische, organisatorische und menschliche, um ein umfassendes Sicherheitsprofil zu erstellen und fundierte Entscheidungen zu ermöglichen. (Alberts, et al. 2025)

Zusammenfassend lässt sich sagen, dass dieses Kapitel eine Einführung in die theoretischen Grundlagen der OCTAVE-Methode bietet (Paulsen 2012). Das Hauptziel dieser Methode besteht darin, die erforderlichen organisatorischen Ressourcen zu identifizieren, relevante Beteiligten einzubeziehen und wirksame Sicherheitsstrategien zu entwickeln (Paulsen 2012). Besonders hervorzuheben ist die Tatsache, dass sie durch ihren flexiblen Ansatz eine präzise Analyse und Sicherung von Vermögenswerten ermöglicht, indem sie gezielt auf die spezifischen Bedürfnisse und

Strukturen der Organisation eingeht. Darüber hinaus trägt diese Methode zur nachhaltigen Umsetzung der entwickelten Strategien bei und bildet somit eine solide Grundlage für das Sicherheitskonzept (Alberts, et al. 2025).

3.2 Ablauf der OCTAVE-Methode

Die Octave-Methode ermöglicht die methodische Identifikation, Analyse und Verwaltung von Informationssicherheitsrisiken. Wie in der einschlägigen Fachliteratur hervorgehoben wird, gliedert sie sich in drei aufeinander abgestimmte Phasen, die jeweils zu einer systematischen und ganzheitlichen Bewertung der Informations-sicherheit beitragen sollen (Caralli, et al. 2007). Jede dieser Phasen ist durch klar definierte Schritte gekennzeichnet, die die Ermittlung kritischer Vermögenswerte, das Auffinden von Bedrohungen und Schwachstellen sowie die Entwicklung risikosenkender Maßnahmen umfassen (Woody, et al. 2006). Wie in Abbildung 2 illustriert, zeigt der Prozess die übergreifenden Interaktionen zwischen den jeweiligen Phasen, wodurch die Methode einen nachhaltigen Beitrag zur Risikominimierung leisten kann (Paulsen 2012).

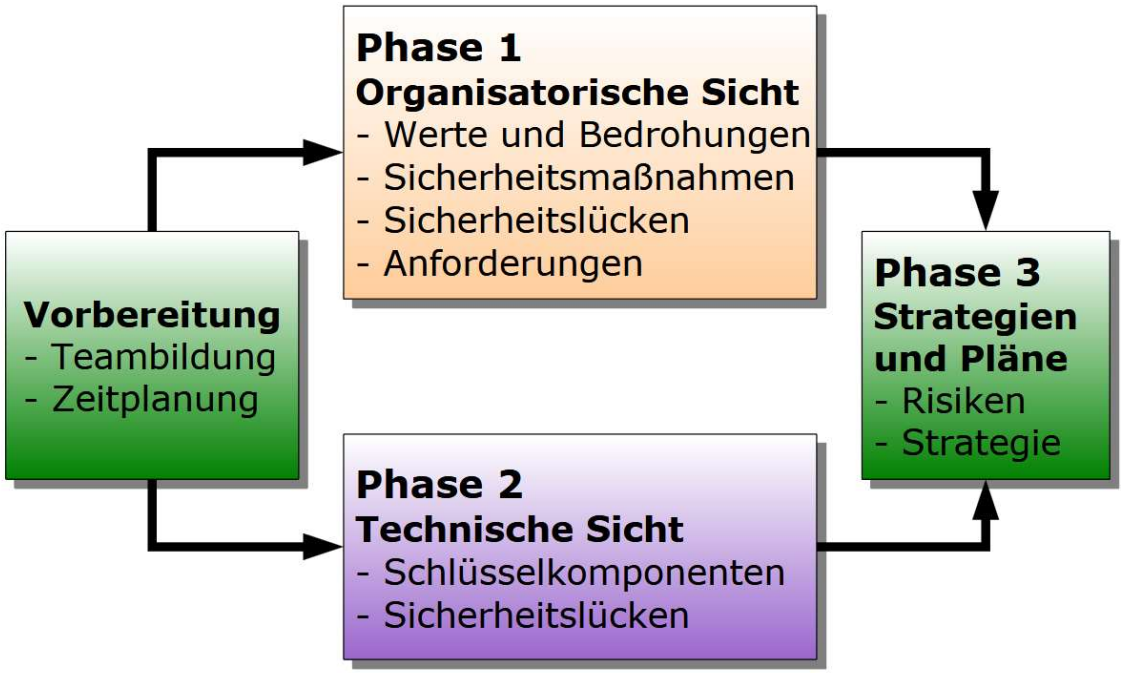

Abbildung 2 Drei wesentlichen Phasen der OCTAVE-Methode (Aust und Paulsen 2013).

Im Folgenden werden die drei Phasen näher erläutert, beginnend mit einer Analyse der Risiken für die wichtigsten Ressourcen der Organisation.

3.2.1 Phase 1: Organisatorische Sicht

In der initialen Phase der Octave Methode liegt die Identifikation und Evaluation kritischer Werte wie z.B. IT-Systeme, Kundendaten oder immaterielle Vermögenswerte einer Organisation, die sowohl physischer als auch technischer Natur sein können (Caralli, et al. 2007). Das Ziel dieser Phase ist es, die zentralen Fragestellungen zu erörtern, darunter:

- Welche Werte sind für die Organisation von größter Bedeutung?
- Welche Bedrohungen könnten diese Werte gefährden?
- Wie gut sind diese Werte durch bestehende Maßnahmen geschützt? (Paulsen 2012)

Die wichtigsten Meilensteine dieses Zyklus umfassen:

1. **Identifikation kritische Werte (Assets) und Bedrohungen:** Die Identifikation kritischer Vermögenswerte spielt eine entscheidende Rolle bei der Bestimmung der Sicherheitsanforderungen einer Organisation und der Entwicklung angemessener Schutzmaßnahmen. Diese Vermögenswerte sind Ressourcen, Informationen, Systeme oder Geschäftsprozesse, die für das reibungslose Funktionieren einer Organisation/Institution unabdingbar sind und deren Beeinträchtigung oder Kompromittierung bedeutende Auswirkungen auf ihre Funktionsfähigkeit und Sicherheit haben könnte (Woody, et al. 2006).
   Zu diesen Assets zählen unter anderem:
   - **Kundendatenbanken** – Aufbewahrung und Verwaltung sensibler Kundendaten, wobei deren Verlust zu Datenschutzverletzungen und Vertrauensverlust führen kann (Alberts, et al. 2025).
   - **Geistiges Eigentum** – darunter Patente, Forschungsdaten oder unternehmenskritische Innovationen – kann im Falle eines Diebstahls zu wirtschaftlichen Schäden verursachen.
   - **Finanzsysteme** – Buchhaltung, der Zahlungsverkehr sowie die Erstellung von Finanzberichten – sind für die wirtschaftliche Stabilität der Organisation von hoher Relevanz (Moya 2014).
   - **IT-Infrastruktur** – damit sind Server, Netzwerke und Cloud-Dienste gemeint, die als technische Basis für Geschäftsprozesse fungieren. Ausfälle oder Angriffe auf diese Infrastruktur können erheblichen Schaden anrichten (Moya 2014).
   - **Kommunikationsnetzwerke** – Interne und externe Kommunikationswege, die für den reibungslosen Informationsaustausch innerhalb der Organisation erforderlich sind (Moya 2014).

   Da diese Vermögenswerte bedeutend für die Funktionsfähigkeit und Sicherheit einer Organisation sind, ist es daher unabdingbar, die potenziellen Risiken, die sie gefährden könnten, systematisch zu analysieren. In diesem Zusammen-

hang spielen die Identifizierung und Bewertung von Bedrohungen ein wichtige Rolle.

Eine *Bedrohung* beschreibt ein potenzielles Ereignis oder eine Sicherheitslücke, welche potenziell zu einem Sicherheitsvorfall führen kann. Generell lassen sich Bedrohungen in zwei Kategorien unterteilen: externe und interne Bedrohungen. Zu den externen Bedrohungen zählen unter anderem Cyberangriffe, Malware, Phishing und Naturkatastrophen. Als interne Bedrohungen werden hingegen jene Gefahren bezeichnet, die durch das unverantwortliche Verhalten von Mitarbeiter, Sabotageakte oder unzureichende Zugriffskontrollen ausgelöst werden (Moya 2014). Das primäre Ziele der Bedrohungsanalyse besteht in der Ermittlung der potenziellen Auswirkungen dieser Bedrohungen auf die ermittelten kritischen Vermögenswerte sowie in der Bewertung der Eintrittswahrscheinlichkeit derartiger Ereignisse (C. C. Woody 2004).

2. **Vorhandene Sicherheitsmaßnahmen und -lücken:** Ein zentraler Aspekt dieses Meilensteins ist die Dokumentation bestehender Sicherheitsmaßnahmen sowie die Identifizierung von Sicherheitslücken auf organisatorischer Ebene. Der Abschluss dieses Schrittes erfolgt, sobald die Bedrohungsprofile für die Vermögenswerte fertiggestellt wurden (Alberts, et al. 2025). In diesem Kontext wird die Effektivität bestehender Maßnahmen wie: *Zugriffskontrollen, Passwortrichtlinien und Verschlüsselungstechniken* überprüft (Vukalovic und Delija 2015). Des Weiteren spielen in der Phase auch organisatorische Aspekte eine bedeutsame Rolle, zu denen klar definierte Sicherheitsrichtlinien und regelmäßige Awareness-Training für die Angestellte gehören. Diese Maßnahmen tragen dazu bei, Sicherheitsrisiken vorzeitig zu erkennen und das Bewusstsein für potenzielle Bedrohungen innerhalb der Organisation/Institution zu fördern. Eine umfassende Bewertung dieser Schutzmechanismen ermöglicht die Identifizierung möglicher Schwachstellen und die Implementierung entsprechender Verbesserungen (C. C. Woody 2004).

   Obwohl die bestehenden Sicherheitsmaßnahmen als ausreichend betrachtet werden, zeigt sich in der Praxis, dass diese häufig *Sicherheitslücken* enthalten. Solche Lücken werden als Mängel oder Schwachstellen in den Sicherheitsmaßnahmen definiert und können von Angreifern gezielt ausgenutzt werden, um beispielsweise IT-Systeme anzugreifen. Diese Lücken entstehen in der Regel durch unzureichende Implementierung von Schutzmaßnahmen oder einer geringen Sensibilisierung des Personals liegen (Bishop 2004).
   Als Beispiel kann hier die unzureichende Implementierung von Passwortrichtlinien oder unzureichende Zugriffskontrollen genannt werden, die es Angreifern unbefugten Zugriff auf Systeme zu erlangen, erleichtert (Moya 2014). Daher ist es von entscheidender Bedeutung, diese Sicherheitslücken systematisch zu identifizieren und zu beheben, um die Robustheit der Organisation gegenüber Cyberbedrohungen zu steigern.

3. **Anforderungen:** Im letzten Schritt der Phase erfolgt die Festlegung von Sicherheitsanforderungen, die zur Minimierung von Risiken erforderlich sind (Alberts, et al. 2025).

Der Abschluss der organisatorischen Analyse erfolgt erst nach Validierung der Bedrohungsprofile durch das Team, wobei dieser Schritt erst dann als abgeschlossen zu betrachten ist, wenn alle Profile abgestimmt, überprüft und umfassend dokumentiert sind (Alberts, et al. 2025).

3.2.2 Phase 2: Technische Sicht

In der zweiten Phase werden technologische Aspekte der Organisation analysiert. Im Mittelpunkt der Überlegungen stehen die Fragen welche Schwachstellen in der IT-Infrastruktur die kritischen Werte gefährden könnten und wie lassen sich diese Schwachstellen beheben? (Paulsen 2012)

Zentrale Aktivitäten dieser Phase umfassen:

- **Identifizierung der Schlüsselkomponenten:** Die Ermittlung der zentralen IT-Systeme, die in direktem Zusammenhang mit den in Phase 1 definierten kritischen Vermögenswerten stehen, ist ein wesentlicher Bestandteil des Prozesses. Zu den relevanten Komponenten zählen u.a. *Server, Netzwerke, Anwendungen, Datenbanken und Speicherlösungen*, die für den Betrieb der Organisation obligatorisch sind. Das Ziel dieses Schrittes liegt in der Erstellung eines umfassenden Inventars aller relevanten Systeme, um deren Bedeutung für die Organisation zu erfassen und potenzielle Sicherheitsrisiken frühzeitig zu erkennen. Der Meilenstein wird als abgeschlossen betrachtet, wenn eine vollständige Übersicht über sämtliche IT-Komponenten vorliegt, ihre Funktionen und Relevanz für die Organisation klar dokumentiert sind und die Verknüpfungen zwischen diesen Komponenten und den kritischen Vermögenswerten nachvollziehbar erfasst wurden (C. C. Woody 2004).
- **Bewertung von Sicherheitslücken:** Dieser Prozess beinhaltet eine detaillierte Analyse der Zugriffswege im Netzwerk sowie eine umfassende Prüfung der Robustheit der einzelnen Komponenten gegenüber potenziellen Angriffen (Caralli, et al. 2007). Zu diesem Zweck werden verschiedene Methoden angewandt, darunter Schwachstellenscans zur Aufdeckung bekannter Sicherheitslücken und Penetrationstests zur Simulation von Attacken unter realistischen Bedingungen (Zhang 2016). Des Weiteren wird eine Analyse der Zugriffskontrollen vorgenommen, um unberechtigte Zugriffe zu identifizieren, sowie eine Bewertung der Konfigurationen, die mögliche Fehlkonfigurationen oder unsichere Schnittstellen aufzeigen kann (Vukalovic und Delija 2015). Ein besonderer Schwerpunkt liegt auf der direkten Verknüpfung der identifizierten Schwachstellen mit den Bedrohungen aus Phase 1, dadurch wird

ersichtlich, welche Sicherheitslücken ein reales Risiko für die Organisation darstellen (Appiah, et al. 2018).

Der Meilenstein dieser Phase ist dann erreicht, wenn alle relevanten Schwachstellen dokumentiert sind, ihre potenziellen Auswirkungen auf die Geschäftsprozesse bewertet wurden und eine klare Zuordnung zu den bereits identifizierten Bedrohungen aus Phase 1 vollzogen wurde (Alberts, et al. 2025).

- **Abschluss der Technischen Analyse:** Im finalen Schritt der zweiten Phase erfolgt die Konsolidierung und Zusammenfassung der gewonnenen Erkenntnisse in einem umfassenden technischen Bericht. Dieser Bericht präsentiert eine detaillierte Übersicht über die identifizierten Schlüsselkomponenten, dokumentierte Sicherheitslücken sowie die damit verbundenen Risiken für die Organisation. Wesentlicher Bestandteil des Berichts ist eine klare und nachvollziehbare Darstellung der ermittelten Schwachstellen, welche durch eine strukturierte Zusammenfassung der Analyseergebnisse sichergestellt wird (Alberts, et al. 2025). Die identifizierten Risiken werden nach ihrer Priorität klassifiziert, um die Implementierung gezielter Maßnahmen zu ermöglichen. Zudem werden erste Empfehlungen für sicherheitssteigernde Maßnahmen gegeben, um potenzielle Bedrohungen zu minimieren (Țîțu, Pop und Ceocea 2019), (Alberts, et al. 2025).

  Diese Phase wird nach Abschluss des Berichts, dessen Vollständigkeit und Konsistenz durch die zuständigen Verantwortlichen geprüft und freigegeben wurde, für abgeschlossen erklärt (Moya 2014).

Mit dem Abschluss dieser Phase stehen alle notwendigen Informationen dafür bereit, dass in Phase 3 konkrete Sicherheitsmaßnahmen entwickelt und umgesetzt werden können.

Zusammenfassend lässt sich feststellen, dass diese Phase eine präzise Grundlage für die Entwicklung gezielter Gegenmaßnahmen bietet. Zur Veranschaulichung der Analyse der Schwachstellen der IT-Infrastruktur und Zugriffspfade kann eine visuelle Darstellung (Abbildung 3) als Unterstützung dienen. Diese Abbildung bietet eine Übersicht der Infrastruktur, der insbesondere die WLAN-Knoten hervorhebt, über die sowohl internen als auch externen Nutzer mit dem Netzwerk kommunizieren. Potenzielle Schwachstellen wurden hier rot markiert, da sie häufig einen Angriffspunkt in IT-Infrastrukturen sind. Diese Struktur bietet nun einen vollständigen Überblick über alle wichtigen Elemente und ihre Verbindungen.

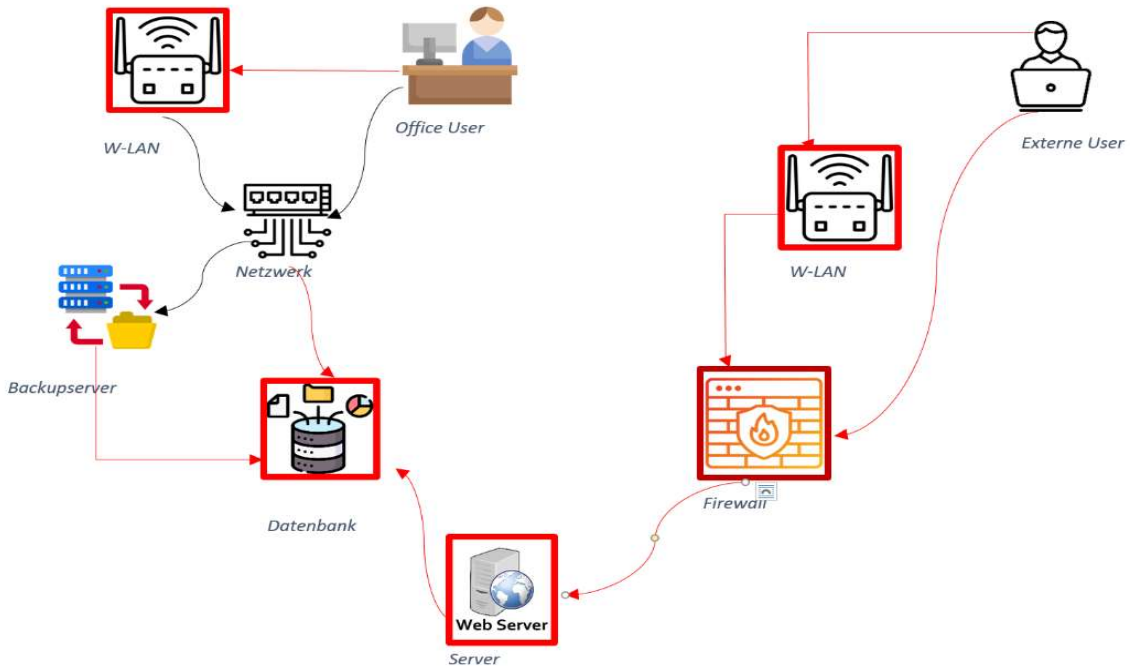

Abbildung 3 Eine schematische Darstellung der IT-Infrastruktur mit hervorgehobenen Schwachstellen und Zugriffspfaden

3.2.3 Phase 3: Strategien und Pläne

Die Erstellung und Implementierung der IT-Sicherheitsstrategie ist der letzte Prozessabschritt der Octave-Methode. Sie stützt sich auf eine methodische und strukturierte Vorgehensweise und umfasst die Entwicklung eines Maßnahmenplans, der sowohl kurzfristige als auch langfristige Ziele berücksichtigt (Caralli, et al. 2007).

Die wesentlichen Schritte in dieser Phase sind:

- **Risiko Priorisierung und Wahrscheinlichkeit des Auftretens:** Das Ziel dieses Vorgehens besteht in der konsistenten Einstufung der Risiken in die Kategorien niedrig, mittel oder hoch. Die Bewertung und Priorisierung der Risiken erfolgten anhand der Wahrscheinlichkeit des Auftretens eines Angriffs und der potenziellen Auswirkungen. Die zielgerichtete Allokation der verfügbaren Ressourcen wird durch die Fokussierung auf die dringendsten Risiken ermöglicht. In diesem Zusammenhang ist besonders hervorzuheben, dass durch die Priorisierung eine effiziente Risikominimierung gewährleistet werden kann (Alberts, et al. 2025).
- **Auswahl der Methoden zur Risikominimierung**: Ein wesentlicher Bestandteil dieser Phase besteht in der Prüfung und Auswahl geeigneter Techniken, die auf die spezifischen Bedrohungen innerhalb der Organisation abgestimmt sind (Alberts, et al. 2025). Dabei sind folgende Ansätze zur Risikominimierung sind zu berücksichtigen:

    - **Eliminierung des Risikos** wird beispielweise durch die vollständige Stilllegung eines gefährdeten Systems oder Außerbetriebnahme veralteter Software erreicht (Caralli, et al. 2007).
    - **Reduzierung des Risikos** erfolgt meistens durch Implementierung von Multi-Faktor-Authentifizierung (MFA), Verschlüsselung von Daten oder Netzwerksegmentierung (Stoneburner, Goguen und Feringa 2002).
    - **Übertragung des Risikos** wird durch Abschluss einer Cyber-Versicherung oder Outsourcing von Sicherheitsdienstleistungen an spezialisierte Unternehmen realisiert (Caralli, et al. 2007).
    - **Akzeptanz des Risikos** allerdings nur unter der Prämisse, dass die Kosten der Eliminierung des Sicherheitsfalles höher sind als der potenzielle Schaden, sowie unter der Voraussetzung einer kontinuierlichen Überwachung und Kontrolle (Caralli, et al. 2007).
- **Erstellung von Minderungsplänen** beinhaltet die Festlegung spezifischer Maßnahmen, benötigter Ressourcen und Zeitrahmen für deren Umsetzung. Das Ziel besteht darin, einen ordentlichen und koordinierten Prozess der Strategieimplementierung sicherzustellen. Dabei sollten diese Pläne realistisch, umsetzbar und auf die übergeordneten Sicherheitsziele der Organisation abgestimmt sein (Caralli, et al. 2007).
- **Identifikation notwendiger Änderungen in der Schutzstrategie** ermöglicht eine formale Anpassung der erforderlichen Maßnahmen zur Verbesserung der Sicherheit der Organisation. Dies geschieht basierend auf den Ergebnissen der Risikobewertung und der Planung von Gegenmaßnahmen (Alberts, et al. 2025). Ein wesentlicher Aspekt dieser Phase ist auch die Dokumentation der möglichen Auswirkungen auf die Mission der Organisation, sollte es zur Realisierung bestimmter Bedrohungsszenarien kommen, was bei der Planung der Geschäftskontinuität von großer Bedeutung ist. Die Erstellung von Bedrohungsprofilen umfasst die Auswahl kritischer Ressourcen, die Festlegung der Sicherheitsanforderungen für diese Ressourcen sowie die Identifikation potenzieller Bedrohungen, die ihnen begegnen könnten (Binus 2014).
- **Definition der weiteren Vorgehensweise** umfasst unmittelbar zu ergreifenden Maßnahmen zur Umsetzung der Sicherheitsstrategie sowie der Risikominderungspläne, mit dem Ziel, einen nahtlosen Übergang von der Planungs- zur Umsetzungsphase sicherzustellen (Alberts, et al. 2025). Nach der Identifizierung von Schwachstellen in der Infrastruktur widmet sich das Team der Analyse und Bewertung der mit den kritischen Vermögenswerten der Organisation assoziierten Risiken, um darauf aufbauend geeignete Gegenmaßnahmen zu entwickeln (Moya 2014).

Im Fokus der Betrachtungen dieser Phase stehen folgende Fragen:

- Welche Risiken sind von höchster Bedeutung?

- Welche Maßnahmen sind erforderlich, um die Risiken effektiv zu minimieren?
- Wie können die Ergebnisse einer kontinuierlichen Überprüfung und Optimierung unterzogen werden? (Paulsen 2012)

Die OCTAVE-Methode verdeutlicht, dass eine systematische und ganzheitliche Betrachtung von Sicherheitsrisiken unerlässlich ist. Darüber hinaus zeigt sich deutlich, dass die Methode für Organisationen unterschiedlicher Größe geeignet ist und somit eine breite Anwendbarkeit gewährleistet (Hom, et al. 2020). Dabei ist zu berücksichtigen, dass trotz der Implementierung einer Risikominimierungsstrategie stets ein gewisses Restrisiko bleibt, welches entweder in Kauf genommen oder weiter minimiert werden sollte (Caralli, et al. 2007). Zusammenfassend lässt sich sagen, dass in dieser Phase erarbeiteten Maßnahmenpläne eine Basis, die nicht nur aktuelle Bedrohungen adressiert, sondern auch zukünftige Herausforderungen im Bereich der Informationssicherheit erfolgreich bewältigen kann, schaffen. Diese Ergebnisse geben Anlass zur Annahme, dass OCTAVE eine unverzichtbare Methode für Organisationen darstellt, die ihre Sicherheitsstrategie optimieren möchten.

3.3 Anwendung der OCTAVE-Methode in Bildungsinstitutionen

In diesem Subkapitel werden die Herausforderungen der Digitalisierung in Bildungsinstitutionen sowie deren Auswirkungen auf die IT-Sicherheit untersucht. Die Basis für diese Analyse zur Risikominimierung in Bildungseinrichtungen, die sensible Daten wie Noten, Gesundheitsdaten oder Verwaltungsinformationen absichert, bildet die OCTAVE Allegro Methode (Gerardo und Fajar 2022). Die vorliegende Analyse stützt sich auf eine Fallstudie des Kalbis Instituts, die im "Journal of Information Systems and Informatics" veröffentlicht wurde.

3.3.1 Fallstudie des Kalbis Instituts

Im Fokus der Fallstudie, welche in Bildungsinstitution in Jakarta durchgeführt wurde und auf der oben beschriebenen Methode basiert, steht die Identifikation und Bewertung von Risiken, die sich durch die Digitalisierung in Bildungsinstitutionen ergeben. Im Rahmen der Analyse wurden insgesamt 24 Risikobereiche identifiziert, die in drei Kategorien eingeteilt werden konnten: Erstens die Risiken, welche **minimiert** und priorisiert (hoch) behandelt werden sollten, zweitens die **aufgeschobenen** Risiken mit mittlerer Priorität und drittens die Risiken, welche von der Organisation mit geringer Priorität **akzeptiert** werden (Gerardo und Fajar 2022).

Zu diesen identifizierten Risiken zählen:

Nr	Bereich der Bedenken	Kategorien	Priorität	Empfohlene Ansätze
1	Fehler bei der Eingabe von persönlichen Daten der Studierenden.	aufgeschobenen	mittel	Zunächst sollte ein Abstimmungsprozess mit der Geschäftsleitung erfolgen. Sofern dies realisierbar ist, empfiehlt sich eine Validierung im Formular sowie die Integration einer Bestätigungsfunktion. Mittels dieser Maßnahmen kann sichergestellt werden, dass der Beamte die Daten korrekt eingegeben hat und bereit ist, diese zu übermitteln.
2	Unzureichende Validierung bei der Vergabe von Benutzerzugriffen.	aufgeschobenen	mittel	Zunächst sollte ein Abstimmungsprozess mit der Geschäftsleitung erfolgen. Sofern dies realisierbar ist, empfiehlt sich eine Validierung im Formular sowie die Integration einer Bestätigungsfunktion. Mittels dieser Maßnahmen kann sichergestellt werden, dass der Beamte die Daten korrekt eingegeben hat und bereit ist, diese zu übermitteln.
3	Fehlkonfigurationen auf dem Webserver.	aufgeschobenen	mittel	Im ersten Schritt wird ein Gespräch mit der Geschäftsleitung geführt, um die Rahmenbedingungen für die weitere Vorgehensweise zu definieren. Anschließend wird, sofern es möglich ist, entweder ein Überwachungssystem für den Server implementiert oder eine alternative Serverlösung für das System recherchiert.
4	Verlust physischer Formulare während des Transports.	aufgeschobenen	mittel	Vorab ist eine Abstimmung mit der Geschäftsleitung erforderlich, um gegebenenfalls ein Verfahren zu etablieren, das die Speicherung der vorgelegten Formulare präzise regelt.
5	Fehlerhafte Vergabe von Benutzerkonten.	aufgeschobenen	mittel	Zunächst ist eine Abstimmung mit der Geschäftsleitung erforderlich. Darüber hinaus ist die Implementierung eines Verfahrens zu empfehlen, das eine erneute Überprüfung des Namens des Studierenden auf dem Konto sowie des Namens des empfangenden Studierenden ermöglicht.
6	Schwachstellen aufgrund unzureichender Firewall-Konfigurationen.	minimiert	hoch	Um die Sicherheit von Systemen zu gewährleisten, empfiehlt es sich, Best Practice zu implementieren und sich an anerkannte Entwicklungsstandards zu orientieren. Darüber hinaus sollten Firewalls sowie Sicherheitsrichtlinien auf den Servern und im Netzwerk regelmäßig überprüft werden. Durch kontinuierliche Sicherheitsaudits können Schwachstellen frühzeitig erkannt und behoben werden.

7	Cyberangriffe auf das Rechenzentrum.	minimiert	hoch	Regelmäßige Sicherheitsaudits des Systems sind durchzuführen, wobei auch die Firewall-Konfigurationen auf den Servern zu überprüfen sind. Zudem wird empfohlen, eine Kopie des Servers zu erstellen, um einen Backup-Server bereitzustellen.
8	Absichtliche Weitergabe sensibler Daten an Dritte.	minimiert	hoch	Um die Effizienz und Validität des Informationsflusses zu gewährleisten, ist es empfehlenswert, die Verteilung der Informationen über den Studierendenservice zu koordinieren und diesen Prozess erneut zu überprüfen. Zudem ist es von großer Bedeutung, einen transparenten Informationsfluss an die Studierenden durch den Studierendenservice zu gewährleisten.
9	Benutzer vergessen, sich von öffentlichen Geräten abzumelden.	aufgeschobenen	mittel	Im ersten Schritt ist eine Abstimmung mit der Geschäftsleitung erforderlich. Im Anschluss daran, sofern dies realisierbar ist, sollte eine Schulung durchgeführt werden, um den Studierenden die Bedeutung des Datenschutzes zu verdeutlichen.
10	Fehler bei Systemaktualisierungen.	aufgeschobenen	mittel	Die Abstimmung mit der Geschäftsleitung ist dabei ein wesentlicher Aspekt. Darüber hinaus ist, sofern es die Umstände erlauben, eine umfassende Prüfung der Implementierung und des Systemablaufs zu empfehlen, um die reibungslose Funktion des Systems sicherzustellen.
11	Ungenauigkeiten bei der Eingabe von Anwesenheitsdaten.	akzeptiert	gering	Für die Übermittlung einer Abwesenheitsmeldung von Studierenden wäre die Einführung einer zusätzlichen Validierung und Bestätigung vorteilhaft.
12	Systemfehler bei der Verarbeitung von Anwesenheitsdaten.	aufgeschobenen	mittel	Eine Abstimmung mit der Geschäftsleitung sollte zunächst erfolgen. Im Anschluss daran ist eine erneute interne Überprüfung und Testung des Systems durchzuführen, um dessen einwandfreie Funktionsweise sicherzustellen. Treten dabei Probleme auf, sind diese durch ein Update des Systems zu beheben. Anschließend sind weitere Tests durchzuführen, bevor das System "GO-Live" geht.
13	Falsche Vergabe von Zugriffsrechten.	akzeptiert	gering	Bei Einreichung eines Zugriffsrechten für einen bestimmten Benutzer sollte eine Bestätigung an den zuständigen Mitarbeiter gesendet werden.
14	Fehler bei der Eingabe von Noten.	akzeptiert	gering	Vor dem Absenden des Formulars ist eine Validierung und Bestätigung vorzunehmen.
15	Systemfehler, die zu vertauschten Noten führen.	akzeptiert	gering	Um die Qualität der Anwendung zu gewährleisten, wird empfohlen, diese vor der Bereitstellung auf dem Produktionsserver einer weiteren Überprüfung zu unterziehen und den Testprozess zu wiederholen.

16	Fehler bei der Erstellung von Stundenplänen.	akzeptiert	gering	Vor dem Absenden des Studienplänen wird darum ersucht, eine Validierung und Bestätigung durchführen zu lassen.
17	Konflikte zwischen den Stundenplänen von Lehrenden und Studierenden.	akzeptiert	gering	In Erwägung der Notwendigkeit einer erneuten Überprüfung der Daten vor der Einreichung ist die Übermittlung einer Bestätigung als Erinnerung eine mögliche Maßnahme.
18	Fehler bei der Eingabe persönlicher Daten von Lehrenden.	akzeptiert	gering	Vor dem Absenden des Formulars wird darum ersucht, eine Validierung und Bestätigung durchführen zu lassen.
19	Verlust von Mitarbeiterformularen durch die Personalabteilung.	aufgeschobenen	mittel	Eine Konsultation mit der Geschäftsleitung ist zu empfehlen, gefolgt von der Festlegung eines Verfahrens, das die Speicherung und den Aufbewahrungsort der eingereichten Formulare eindeutig definiert.
20	Falsche Vergabe von Zugriffsrechten an Lehrende.	akzeptiert	gering	Bei der Vergabe von Zugriffsrechten an Lehrende ist zu berücksichtigen, dass dafür berechtigte Personal eine Bestätigung einholt.
21	Absichtliche Weitergabe personenbezogener Daten von Lehrenden.	minimiert	hoch	Die Datenverteilung durch den Lehrenden-Service sollte nach Möglichkeit transparent gestaltet werden.
22	Fehler bei der Eingabe von Semesterplänen.	akzeptiert	gering	Im Zuge der Einreichung der Semesterpläne in das System wird eine Bestätigung an den Leiter des Lehrteams empfohlen.
23	Nutzung veralteter Lehrmaterialien ohne Überprüfung.	akzeptiert	gering	Es wird empfohlen, ein Team zu bilden, das das Lehrmaterial eines Fachs überprüft, um sicherzustellen, dass es den aktuellen Anforderungen entspricht und für das Fach relevant ist.
24	Bereitstellung nicht relevanter Inhalte für Lehrveranstaltungen	akzeptiert	gering	Die Inhalte der Lehrveranstaltungen sind zunächst einer gründlichen Überprüfung zu unterziehen. Gegebenenfalls ist eine erneute Überprüfung durchzuführen, bevor die Inhalte an die IT-Abteilung weitergeleitet werden.

Tabelle 1 Überblick über 24 Risikobereichen mit Kategorien, Priorität und empfohlenen Ansätzen (Gerardo und Fajar 2022), (Moya 2014)

In Anbetracht der obigen Ergebnisse, die den Wissenschaftlern mittels der OCTAVE-Allegro-Methode bei der Durchführung der Risikobewertung behilflich war, lässt sich Folgendes feststellen:

- 4 Risiken müssen minimiert werden
- 9 Risiken erfordern eine Diskussion mit der obersten Geschäftsleitung
- 11 Risiken wurden von der Institution akzeptiert. (Gerardo und Fajar 2022)

Ein besonderer Schwerpunkt bei der Studie wurde auf die systematische Anwendung von OCTAVE Allegro Arbeitsblättern gelegt, um Schwachstellen und potenzielle Bedrohungen zu evaluieren (Gerardo und Fajar 2022). Darüber hinaus wurden die drei größten Risikofaktoren in der Institution identifiziert:

- **Menschen,**
- **veraltete Systeme**
- **und unzureichende Infrastruktur.** (Moya 2014)

3.3.2 Maßnahmen zur Risikominimierung

Basierend auf diesen Erkenntnissen der Fallstudie in Jakarta lassen sich folgende Maßnahmen ableiten, um die identifizierten Risiken zu minimieren:

- **Regelmäßige Sicherheitsaudits**: Diese Überprüfungen werden jährlich für die gesamte IT Infrastruktur durchgeführt um die Schwachstellen zu erkennen und zu beheben (Moya 2014).
- **Standardisierung des Quellcodes**: An dieser Stelle erfolgt die Implementierung verbindlicher Standards für die Entwicklung und Pflege von Software, einschließlich Code-Reviews und Versionskontrollen. Die Einführung von Checklisten für Entwickler stellt eine mögliche Lösung dar, um die Implementierung gefährlicher Routinen zu verhindern (Gerardo und Fajar 2022).
- **Überprüfung der Firewall-Konfigurationen**: Netzwerksicherheitsrichtlinien der Institutionen sollte regelmäßig aktualisiert und überprüft werden, um Angriffe abzuwehren bzw. zu verhindern (Titus, et al. 2023).
- **Benutzerschulungen**: Diese Trainings umfassten praxisnahe Checklisten sowie Workshops und sind auf Bedürfnisse von Lehrkräften und Verwaltungspersonal zugeschnittenen. Ziel dieser Maßnahmen ist die Vermittlung grundlegender Sicherheitspraktiken, wie zum Beispiel der Schutz von Passwörtern und die Erkennung von Phishing-Angriffen (Moya 2014).

Besonders bemerkenswert dabei ist, dass kurzfristige Verbesserungen bereits durch die Einführung standardisierter Sicherheitsrichtlinien und regelmäßiger Schulungen erzielt wurden. Um allerdings den spezifischen Herausforderungen gerecht zu werden, waren weiterführende Anpassungen notwendig, die die jeweiligen Bedingungen in den Schulen berücksichtigen. In diesem Zusammenhang spielen insbesondere kostengünstige Anwendungen eine zentrale Rolle. Hierzu zählen z. B:

- **OpenVAS** - ermöglicht Schwachstellenüberprüfungen.
- **ClamAV** - ist ein kostenloser Antivirenschutz.
- **pfSense** - ist Open-Source-Firewall dient als zur Sicherung des Netzwerks. (Detken 2019)

Die Fallstudie am Kalbis Institute beweist, dass auch mit beschränkten Ressourcen Verbesserungen der Cybersicherheit möglich sind (Gerardo und Fajar 2022). Besonders wertvoll scheint der strukturierte Ansatz der dargelegten Methode zu sein, die es möglich macht die Risiken systematisch und rechtzeitig zu erkennen und geeignete präventive Maßnahmen einzuleiten. Die Fallstudie unterstreicht, dass die Kombination der pragmatischen und technischen Lösungen sowie Schulungen zur Verbesserung der Sicherheit führt (Gerardo und Fajar 2022).

Die bisherigen Erkenntnisse bezüglich der OCTAVE-Methode weisen darauf hin, dass es sich um einen vielversprechenden Ansatz zur Risikominimierung handelt. In der einleitenden Phase der Implementierung dieser Methode sollten Schulen ihre wichtigsten Ressourcen, wie persönliche Daten oder Testergebnisse, identifizieren (Titus, et al. 2023). Basierend auf dieser Analyse lassen sich potenzielle Risiken, wie unberechtigter Zugriff oder Datenverlust, identifizieren und daraus resultierend geeignete Gegenmaßnahmen ableiten. Zu diesen Maßnahmen gehören:

- **Ende-zu-Ende-Verschlüsselung** – zur Sicherung der Daten sowohl bei der Übertragung als auch in der Cloud.
- **Multi-Faktor-Authentifizierung** – um unbefugte Zugriffe zu verhindern.
- **Regelmäßige Sicherheitsüberprüfungen** – damit genutzten Dienste den aktuellen Sicherheitsstandards entsprechen. (C. C. Woody 2004)

3.3.3 DSGVO und Datenschutz in Bildungsinstitutionen

Die Datenschutz-Grundverordnung (DSGVO) ergänzt die hier die Beiträge und die Reflexion der Fallstudie. Die DSGVO definiert klare Vorgaben für die Erhebung und Verarbeitung von Daten durch Bildungseinrichtungen und legt fest, dass ausschließlich die für die Erfüllung der jeweiligen Zwecke erforderlichen Informationen erfasst werden dürfen. Dies umfasst Prüfungsergebnisse, Gesundheitsdaten und Kontaktdaten der Eltern. Dabei ist auch zu berücksichtigen, dass für die Verarbeitung dieser Daten eine ausdrückliche Zustimmung der Eltern oder volljährigen Schüler/innen erforderlich ist (Sobota 2022). Um die Einhaltung der Datensicherheit in der Bildungs-institutionen sicherzustellen, sind umfassende Maßnahmen erforderlich, darunter:

- Technische Lösungen wie Datenverschlüsselung, regelmäßige System-Updates der Systeme, eingeschränkte und gut dokumentierte Zugriffsrechte.
- Gesetzliche Regelungen. (Sobota 2022)

Des Weiteren gewinnen die verstärkte Nutzung von Cloud-Plattformen und die Durchführung von Online-Prüfungen im Kontext des E-Learnings zunehmend an Bedeutung. Diese Entwicklungen sorgen jedoch für neue Herausforderungen, welche insbesondere in den folgenden Bereichen zu sehen sind:

- **Datenlecks** – verursacht durch unsichere Cloud-Dienste (Zugriff von Dritten).
- **Unzureichende Verschlüsselung** – erleichtert die Angriffe und den Identitäts-diebstahl.
- **Manipulationen z. B. bei Online-Prüfungen** – durch fehlende Authentifizierung.
- **Verfügbarkeit des Clouddienstes** – verbunden mit dem Risiko eines Ausfalls oder einer Überlastung des Dienstes**.** (Sobota 2022)

Zusammenfassend lässt sich sagen, dass die OCTAVE-Methode einen flexiblen und effektiven Ansatz bietet, um Sicherheitslücken systematisch zu identifizieren und zu beheben. Die dargestellten Ergebnisse stützen die Hypothese, dass Bildungs-institutionen durch Integration kostengünstiger Tools, praxisnaher Schulungen und

die strikter Einhaltung der DSGVO ihre IT-Sicherheit nachhaltig verbessern können (Gerardo und Fajar 2022). Diese Erkenntnisse liefern einen wertvollen Impuls für weitere Bildungseinrichtungen, die mit ähnlichen Herausforderungen konfrontiert sind.

4. Weitere Methoden und Standards der IT-Sicherheit

Zur wirksameren Bekämpfung der vielfältigen und komplexen Bedrohungen in einer digitalen Welt haben sich verschiedene Methoden und Standards, die von Organisationen zur effektiven Sicherung ihrer IT-Systeme und Daten eingesetzt werden, herauskristallisiert. In diesem Kapitel werden die gängigsten Ansätze besprochen, die eine strukturierte und erfolgreiche Implementierung von Informationssicherheits-maßnahmen unterstützen. Neben der bereits näher erklärte OCTAVE-Methode bieten auch andere Methoden und internationale Standards wie ISO/IEC 27001 und das NIST Cybersecurity Framework (CSF), die in diesem Abschnitt vorgestellt werden, spezifische Strategien zur Risikobewertung und -bewältigung. Hierbei werden auch nationale Konzepte wie das BSI IT-Grundschutz-Kompendium und das Österreichische Informationssicherheitshandbuch präsentiert, die praktische Lösungen mit lokaler Relevanz anbieten. Die Kombination der beschriebenen Ansätze ermöglicht die Schaffung von Synergien. Dies wiederum erlaubt die Entwicklung einer umfassenden Sicherheitsstrategie, die auf die spezifischen Bedürfnisse der jeweiligen Organisation bzw. Institution angepasst werden kann.

4.1 Überblick über gängige IT-Sicherheitsansätze

Aufgrund der zunehmenden Anzahl auftretender Angriffe auf Datenverarbeitungs-systeme erlangt die Konzeption eines angemessenen IT-Sicherheitskonzepts zur Gewährleistung der Informationssicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Daten gegenwärtig hohe Bedeutung (Bundesamt für Sicherheit in der Informationstechnik 2017). Sie umfasst sowohl technische als auch organisatorische (Isele, et al. 2017). Besonders im Bildungskontext scheint dieses Thematik auf Grund der Speicherung von hochsensible Daten von Schülern und Lehrkräften besonderes relevant zu sein.

4.1.1 Das Prinzip der minimalen Rechtevergabe

Ein fundierter Ansatz der moderne IT-Sicherheitsstrategien ist das Prinzip der minimalen Rechtevergabe (engl. Least Privilege), welches besagt, dass Anwendern und Systemen einzig jene Zugriffsrechte gewährt werden sollten, die für die Erfüllung ihrer Aufgaben unbedingt notwendig sind (Bundesamt für Sicherheit in der Informationstechnik 2017). Das genannte Prinzip ist darauf gerichtet, mögliche Gefahren und Schäden, welche im Falle eines erfolgreichen Angriffs auftreten könnten, zu reduzieren.

Bei der praktischen Umsetzung dieses Prinzips könnten verschiedene Herangehensweisen zur Auswahl, gestellt werden, darunter:

- **Rollenbasiertes Zugriffsmanagement:** Er gestattet eine zielgerichtete Distribution von Rechten und eine präzise Zuordnung von Rollen.

- **Regelmäßige Überprüfungen:** Diese dienen dazu, redundante oder veraltete Berechtigungen zu identifizieren und zu löschen.
- **Technische Lösungen:** Diese Werkzeuge/Tools wie z.B. LDAP (Lightweight Directory Access Protocol) oder Active Directory erleichtern die effiziente Verwaltung von Berechtigungen und setzen das Prinzip der minimalen Rechtevergabe praktisch um. (Bundesamt für Sicherheit in der Informationstechnik 2017)

Um das Least Privilege im Kontext der Bildungsinstitutionen genauer zu veranschaulichen wurde ein konkretes Beispiel dargestellt: Einen Lehrer werden ausschließlich die Zugriffsrechte auf die Daten jener Klassen verleihen, die er unterrichtet. Zudem wird durch regelmäßige Überprüfungen seitens der Administratoren sichergestellt, dass diese Rechte aktuell bleiben (Bundeskanzleramt Österreich 2023).

4.1.2 IT-Grundschutz-Kompendium und nationale Ansätze

Das IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) bietet Leitfaden zur Identifizierung und Minimierung von Risiken und stellt praxisnahe sowie erprobte Sicherheitsmaßnahmen der IT- Infrastruktur bereit (Bundesamt für Sicherheit in der Informationstechnik 2000).

Die zentralen Inhalte dieses Kompendiums umfassen:

- **Schutzbedarfsermittlung:** Analyse der zu schutzbedürftigen Werte und Systeme sowie deren spezifischer Schutzanforderungen.
- **Risikomanagement:** Bewertung von Schwachstellen, Bedrohungen und Wahrscheinlichkeiten von Angriffen.
- **Maßnahmenkataloge:** Richtlinien zur Umsetzung technischer, organisatorischer und infrastruktureller Maßnahmen. (Bundesamt für Sicherheit in der Informationstechnik 2000)

Das österreichische Bildungsministerium hingegen nutzt die BSI-Standards als Grundlage, hat jedoch eine eigene Lösung entwickelt: das sogenannte "Österreichische Informationssicherheitshandbuch". Dieses Handbuch ist speziell an die österreichischen Gegebenheiten und Umstände angepasst (Bundeskanzleramt Österreich 2023). Basierend auf einer Risikoanalyse und durch die Kombination bewährter Sicherheitsmethoden können im österreichischen Bildungssektor spezifische Lösungen flexibel umgesetzt werden. Zu diesen praxisnahen Lösungen gehören:

1. **Modularer Ansatz für IT-Sicherheit** ermöglicht die Anpassung von IT-Sicherheitsmaßnahmen an diverse Arten von Bildungsinstitutionen und Organisationen (Blumberg und Pohlmann 2006).
2. **Leitfäden und Checklisten** bieten detaillierte Leitlinien für die Implementierung von Sicherheitsmaßnahmen und erleichtern deren sukzessive Umsetzung durch klar definierte Abläufe (Blumberg und Pohlmann 2006).

3. **Integration von Datenschutz und IT-Sicherheit** stellt sicher, dass technische Anforderungen sowie Datenschutzbestimmungen konsistent sind und die ordnungsgemäße Datenverwaltung unterstützen (Blumberg und Pohlmann 2006).
4. **Datenschutz- und Compliance-Richtlinien** helfen Bildungsinstitutionen wie Schulen und Universitäten bei der Einhaltung vom DSVGO (Strohmeyer 2018).
5. **Integriertes Risikomanagement**, das die Institutionen bei der Identifizierung und Minimierung von Informationsrisiken unterstützt (Blumberg und Pohlmann 2006).

4.1.3 Technische und organisatorische Maßnahmen

Allerdings reicht theoretisches Wissen allein nicht aus, um einen umfassenden Schutz zu gewährleisten. Vielmehr sind konkrete technische und organisatorische Maßnahmen erforderlich, um ein effektives IT-Sicherheitskonzept zu etablieren. Diese enge Verzahnung stellt sicher, dass potenzielle Schwachstellen ganzheitlich adressiert werden:

1. **Technische Maßnahmen:**
   - **Firewalls und Netzwerksicherheitslösungen** – schützen vor unerlaubtem Zugriff und externen Angriffen.
   - **Verschlüsselung** – stellt die Integrität und Vertraulichkeit von Daten sowohl während der Übertragung als auch bei der Speicherung, sicher.
   - **Intrusion Detection Systeme (IDS)** – identifizieren unzulässige Netzwerk-aktivitäten sowie ermöglichen einer rechtzeitigen Reaktion auf potenzielle Bedrohungen (Bundesamt für Sicherheit in der Informationstechnik 2017), (Isele, et al. 2017).
2. **Organisatorische Maßnahmen:**
   - **Sensibilisierung durch Schulungen** – Etwa durch Simulationen von Phishing-Angriffen, um das Sicherheitsbewusstsein zu stärken (Bundeskanzleramt Österreich 2023).
   - **Notfallpläne –** beinhaltet eine effiziente Reaktion auf Sicherheitsvorfälle ihre Bewertung und Behebung sowie die Implementierung von Notfallstrategien zur Reduzierung potenzielle Schäden von Cyber-Angriffen (Isele, et al. 2017).
   - **Regelmäßige Audits** – sorgen für die Einhaltung der Sicherheitsrichtlinien und dokumentieren die Ergebnisse hinsichtlich kontinuierlicher Verbesse-rungen (Bundesamt für Sicherheit in der Informationstechnik 2017).

Ein hervorragendes Beispiel für die Verbindung von technischen und organisatorischen Maßnahmen in Schulen ist die Lehrerfortbildung. Dabei geht es nicht nur um den sicheren Umgang mit Firewalls und Verschlüsselungstechnologien, sondern auch um deren Einbindung in die Entwicklung eines Notfallplans. So werden technische Sicherheitsmaßnahmen nicht isoliert betrachtet, sondern als integraler Bestandteil eines

umfassenden Sicherheitskonzeptes (Kienzle 2022). Das Ziel dieses Planes ist, im Falle der Fälle eine schnelle und effektive Gegenreaktion auf den eingetroffenen Ernstfall zu ermöglichen.

4.1.4 Praktische Anwendungsfälle

Die Implementierung dieser Maßnahmen lässt sich anhand konkreter Beispiele veranschaulichen:

- **Datenleck** – das die sensiblen Schülerdaten öffentlich zugänglich machen würden, könnten durch Regelmäßige Audits sowie die Anwendung des Prinzips der minimalen Rechtevergabe verhindert werden (Isele, et al. 2017).
- **Phishing-Angriff** – im Kampf gegen E-Mail-Betrug und damit verbundenen Risiken sollten einerseits die Lehrkräfte durch Schulungen sensibilisiert und anderseits strikte Passwortstrategie eingeführt werden (Bundeskanzleramt Österreich 2023).

Die in dem vorliegenden Subkapitel beschriebenen Sicherheitsansätze bieten eine fundierte Grundlage für ein modernes IT-Sicherheitskonzept. Sie beinhalten das Prinzip der minimalen Rechtevergabe sowie das IT-Grundschutz-Kompendium und das österreichische Informationssicherheitshandbuch. Insbesondere im Bildungskontext tragen sie zur Identifikation und Minimierung von Schwachstellen bei. Zusammenfassend lässt sich festhalten, dass durch die gezielte Kombination technischer und organisatorischer Maßnahmen eine sichere Umgebung geschaffen werden kann, die den Schutz sensibler Daten sicherstellt und das Vertrauen aller Beteiligten stärkt.

4.2 ISO/IEC 27001

Die Informationen sind für Betrieb eines Unternehmens unerlässlich, um einen reibungslosen Ablauf sicherzustellen, gesetzliche Vorgaben einzuhalten und das Vertrauen der Kunden zu bewahren. Solche Internationale Standards wie ISO/IEC 27001 fördern die Implementierung und Verwaltung von Informationssicherheits-Managementsystemen (ISMS). Die vorliegende Norm definiert die Rahmenbedingungen für die Implementierung, den Betrieb und die kontinuierliche Optimierung eines ISMS für Organisationen (Wijayarathne 2022).

Hierbei wird das Hauptziel dieser Standards in der Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationsressourcen gesehen, die in analoger oder digitaler Form vorliegen können (Ewuga, et al. 2023). Eine besondere Bedeutung der Informationssicherheit lässt sich in Bildungsinstitutionen (Schulen), wo eine Vielzahl sensibler Daten verarbeitet wird, sehen. Insbesondere Schulen, die oft mit solchen Informationen arbeiten und über begrenzte Ressourcen verfügen, können von der

strukturierten Implementierung eines ISMS nach ISO/IEC 27001 profitieren (Wijayarathne 2022).

4.2.1 Charakteristische Merkmale des ISO/IEC 27001 Standards

Zur besseren Veranschaulichung der Anwendungsmöglichkeiten dieses Standards können folgende Merkmale definiert werden:

- **Flexibilität:** Dieser Standard kann an die spezifischen Anforderungen jeder Organisation adaptiert werden. Diese Charakteristik ermöglicht die Implementierung einer maßgeschneiderten Lösung in bestehende Organisationsstrukturen.
- **Prozessansatz:** "Plan-Do-Check-Act" (PDCA)-Modell gestatte eine kontinuierliche Optimierung des ISMS. Dies stellt sicher, dass das Sicherheitsniveau laufend analysiert, evaluiert und verbessert wird.
- **Integration:** Der Standard kann mit anderen Managementsystemen wie ISO 9001 oder ISO 14001 kombiniert werden. Für Schulen, die bereits ein Qualitätsmanagementsystem nach ISO 9001 etabliert haben, ergeben sich in den Bereichen Dokumentation, Prozessgestaltung und Compliance neue Synergien, die genutzt werden können (Wijayarathne 2022), (ISO/ICE 2005).

4.2.2 Vorteile für Bildungsinstitutionen

In Anbetracht der verstärkten Verwendung digitaler Plattformen und Technologien in Bildungseinrichtungen gewinnt der Schutz sensibler Daten immer mehr an Bedeutung. Die Implementierung von ISO/IEC 27001 bietet in diesem Zusammenhang einige Vorteile wie z. B.:

- **Erhöhter Datenschutz:** Aufgrund der zunehmenden regulatorischen Anforderungen ist die Einhaltung strenger Datenschutzrichtlinien, wie der DSGVO, von hoher Relevanz, um Rechtssicherheit zu gewährleisten, weshalb durch den Einsatz dieser Norm personenbezogene Daten vor Missbrauch geschützt werden.
- **Risikominimierung:** Eine systematische Risikoanalyse und -bewertung ist essentiell, um Bedrohungen wie Phishing oder Ransomware frühzeitig zu erkennen und geeignete Schutzmaßnahmen zu etablieren. Damit kann die Wahrscheinlichkeit eines Cyberangriffs deutlich reduziert werden.
- **Sensibilisierung und Schulung:** Ein zentraler Bestandteil von ISO/IEC 27001 sind Schulungen und Sensibilisierungsmaßnahmen, die das Sicherheitsbewusstsein innerhalb der Organisation fördern. Regelmäßige Schulungen können dazu beitragen, dass Sicherheitsrisiken durch menschliche Fehler minimiert werden.
- **Vertrauensbildung:** Demzufolge stärkt eine Zertifizierung nach ISO/IEC 27001 das Vertrauen von Schülern, Eltern sowie Behörden in die Sicherheits-

maßnahmen der Bildungsinstitution. Ein zertifiziertes ISMS wird als Nachweis für ein hohes Maß an Datenschutz und Sicherheitsbewusstsein betrachtet. (PD – Berater der öffentlichen Hand GmbH 2023)

4.2.3 Umsetzung in Institutionen mit begrenzten Ressourcen

Zudem ist bei der Bearbeitung dieses Abschnitts auch der finanzielle Aspekt in den Schulen bzw. Bildungsinstitutionen zu berücksichtigen. Institutionen dieser Art verfügen in der Regel über eingeschränkte finanzielle und personelle Ressourcen. Aus diesem Grund erfolgt die Implementierung von ISO/IEC 27001 in der Regel in mehreren Phasen. Diese umfassen:

1. **Security Awareness Training:** Mitarbeiter müssen für grundlegende Sicherheitsaspekte sensibilisiert werden. Dies bildet auch die Basis für ein effektives Sicherheitsmanagementsystem.
2. **Risikobewertung:** Kritische Schwachstellen in der IT-Infrastruktur werden identifiziert. Hierbei sind sowohl technische als auch organisatorische Aspekte zu berücksichtigen.
3. **Grundlegende Sicherheitsmaßnahmen:** Als erste Schutzebene werden die Einführung von Passwortmanagement, Zugriffsbeschränkungen und regelmäßigen Backups vorgenommen, da diese Maßnahmen von größter Bedeutung für den Grundschutz der IT-Infrastruktur sind.
4. **Erweiterte Sicherheitsmaßnahmen:** Implementierung eines strukturierten ISMS nach ISO/IEC 27001. Dazu gehören die Definition von Sicherheitsrichtlinien, Maßnahmen zur Netzwerküberwachung sowie die Einführung eines Vorfallmanagementsystems.
5. **Regelmäßige Audits und Verbesserungen:** Dies beinhaltet die regelmäßige Durchführung von Audits sowie kontinuierliche Verbesserungen der Sicherheitsprozesse. Die Effektivität des ISMS wird durch regelmäßige Audits evaluiert und kontinuierlich optimiert. (Ewuga, et al. 2023)

4.2.4 Förderprogramme

Die Implementierung von IT-Sicherheitsstandards wie ISO/IEC 27001 ist für viele Bildungseinrichtungen eine große finanzielle Belastung. Um diese Herausforderung zu meistern, nutzen viele Institutionen staatliche oder private Förderprogramme. Solche finanziellen Unterstützungsmaßnahmen erleichtern die Implementierung und Umsetzung von Sicherheitsmaßnahmen und verbessern langfristig die digitale Infrastruktur. Im Folgenden werden einige der wichtigsten Fördermöglichkeiten aufgezählt:

- **EU-Förderprogramme:** Diesbezüglich seien der "InvestEU" sowie der "Digital Education Action Plan" der EU als hervorragende Beispiele genannt, die finanzielle Mittel für digitale Bildungsinitiativen bereitstellen und auf diese Weise einen Beitrag zur Gewährleistung der IT-Sicherheit in Bildungs-

institutionen leisten (European Commision 2020), (Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs 2021).

- **Nationale Programme:** In Deutschland fördert das Bundesministerium für Bildung und Forschung (BMBF) IT-Sicherheitsmaßnahmen in erwähnten Institutionen. Dadurch können finanzielle Belastungen für die Einführung eines ISMS reduziert werden (Bundesministerium für Bildung, Wissenschaft und Forschung 2021).
- **Landesspezifische Programme:** In Österreich unterstützt die Initiative "Digitale Schule" als auch "Sicher im Netz - Safer Internet in der Schule" oder "Förderprogramm Cyber Security Schecks" des Bildungsministeriums Investitionen in IT-Sicherheit. Vor allem kleinere Schulen mit begrenztem Budget können von solcher Programmen profitieren (Bundesministerium für Bildung, Wissenschaft und Forschung nd), (Bundesministerium für Bildung, Wissenschaft und Forschung 2025), (Bundesministerium für Finanzen n.d.).

4.2.5 Herausforderungen bei der Implementierung

Nicht unerwähnt soll es bleiben, dass es trotz der zahlreichen Vorteile auch einige Herausforderungen gibt, beispielsweise:

- **Kosten:** Die finanziellen Belastungen, die mit der Implementierung und Zertifizierung verbunden sind, sind in der Regel beträchtlich. Förderungsprogramme können jedoch behilflich sein um diese Belastung zu reduzieren.
- **Akzeptanz durch Mitarbeiter:** Um Sicherheitslücken durch menschliche Fehler zu reduzieren bzw. zu vermeiden, sollten nicht nur intensive Schulungen angeboten, sondern auch die Mitarbeiter frühzeitig eingebunden werden. Ohne eine Mitarbeiterakzeptanz innerhalb der Organisation bleibt die Wirksamkeit des ISMS begrenzt.
- **Veraltete IT-Infrastruktur:** Laut Anforderungen von ISO/IEC 27001 muss die bestehende IT-Systeme Systemtechnisch aktuell sein. Dies stellt insbesondere für Bildungseinrichtungen mit begrenzten IT-Ressourcen eine Herausforderung dar. (Stoiber 2019)

Die Implementierung von ISO/IEC 27001 könnte für die polnische Schule in Kalksburg von wesentlicher Bedeutung sein. Dabei ist zu bemerken, dass die Implementierung eines effektiven ISMS zwar nicht direkt den gesetzlichen Anforderungen entspricht, jedoch einen wichtigen Beitrag zur Schaffung einer sicheren digitalen Lernumgebung leisten kann. Die Implementierung eines nach ISO/IEC 27001 zertifizierten Systems würde die Schule nicht nur auf die aktuellen gesetzlichen Anforderungen vorbereiten sondern auch auf die zukünftigen.

4.3 NIST

Das vom National Institute of Standards and Technology (NIST) entwickelte Cybersecurity Framework (CSF) bietet einen etablierten und flexiblen Ansatz, der Firmen und Institutionen ein systematisches Vorgehen bei der Erkennung und Bewertung ihrer Cyber-Abwehrkapazitäten ermöglicht. Dieses wurde ursprünglich als Modell für den Schutz kritischer Infrastrukturen in den USA entwickelt, allerdings konnte seine Wirksamkeit auch in vielen anderen Bereichen über kritische Infrastrukturen hinaus eindeutig nachgewiesen werden (FedTech 2019). Ein besonderes Aufmerksamkeit wurde dem Bildungssektor gewidmet, der zunehmend zu einem attraktiven Ziel für Cyberkriminelle geworden ist.

Darüber hinaus ist in diesem Abschnitt auch die grundlegende Struktur des CSF NIST analysiert worden, die fünf Schlüsselfunktionen beinhaltet: *Identifikation, Schutz, Erkennung, Reaktion und Wiederherstellung* (National Institute of Standards and Technology 2024). Diese Funktionen umfassen den gesamten Sicherheitszyklus von der Risikoanalyse über die Implementierung von Schutzmaßnahmen bis hin zur Reaktion auf Sicherheitsvorfälle und deren wirksame Bewältigung.

Insbesondere für Bildungsinstitutionen ist NIST von großer Bedeutung, da es dazu beiträgt, Cyber-Risiken gezielt zu minimieren und die Resilienz gegenüber Bedrohungen zu erhöhen. Die Implementierung des Frameworks für Bildungseinrichtungen wie Schulen und Hochschulen erscheint somit als ein wesentlicher Aspekt, der nicht nur vorteilhaft, sondern angesichts des zunehmenden Risikos von Cyberangriffen sogar notwendig ist.

4.3.1 Die fünf grundlegenden Funktionen des NIST CSF

Im Folgenden werden die fünf zentralen Elemente näher erläutert:

1. **Identifizieren:** Mittels dieser Funktion erfolgt die strukturierte Erfassung und Evaluation von Risiken sowie die Identifikation kritischer Ressourcen und potenzieller Bedrohungen. Diese umfasst die Erstellung eines IT-Inventars sowie die Festlegung der Risikotoleranz einer Einrichtung. Wie bereits in früheren Teilen dieser Arbeit festgestellt wurde, bildet eine präzise Risikoanalyse die Basis für effiziente Sicherheitsmaßnahmen (National Institute of Standards and Technology 2024).
2. **Schützen**: Das Ziel dieser Funktion besteht darin, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu sicherstellen, wobei insbesondere die Verschlüsselung, Zugriffskontrollen und die Implementierung sicherer Systemkonfigurationen von Bedeutung sind (National Institute of Standards and Technology 2018).
3. **Erkennen:** Eine zentrale Rolle spielt dabei die frühzeitige Identifikation von Risiken. Dies erfolgt durch die Analyse von Protokolldaten wie auch die

Erkennung möglicher Schwachstellen. Daraus ergibt sich die Notwendigkeit, geeignete Monitoring-Mechanismen zu implementieren (Gopstein, et al. 2020).

4. **Reagieren:** Diese Funktion zielt darauf ab, die Auswirkungen von Sicherheitsvorfällen zu minimieren. Um dieses Ziel zu erreichen, sollten Maßnahmen wie Eskalationsverfahren, Vorfallmanagementprozesse und Notfallkommunikation etabliert werden. In der praktischen Anwendung konnte festgestellt werden, dass eine systematisch konzipierte Reaktionsstrategie dazu beitragen kann, die Schäden zu minimieren (National Institute of Standards and Technology 2024).
5. **Wiederherstellen:** Hierbei handelt es sich um eine Aktivität, welche regulären IT-Betrieb nach einem Sicherheitsvorfall wiederherstellt. Darüber hinaus ist eine sorgfältige Überarbeitung und Optimierung der bestehenden Sicherheitsrichtlinien erforderlich, um potenzielle Risiken zukünftig zu minimieren. Ferner ermöglicht eine detaillierte Analyse aufgetretene Vorfälle wertvolle Erkenntnisse für die Entwicklung entsprechender Schutzmaßnahmen (Gopstein, et al. 2020).

4.3.2 Anwendung des NIST CSF im Bildungssektor

Das NIST CSF stellt durch seine Flexibilität eine ausgezeichnete Grundlage dar, um die Herausforderungen der Bildungsinstitutionen erfolgreich zu meistern. Vor allem drei wesentliche Elemente machen das Framework besonders attraktiv für diesen Bereich:

- **Flexibilität:** Ein wesentlicher Vorteil dieses Frameworks ist, dass es an die Bedürfnissen der einzelnen Bildungsinstitutionen angepasst werden kann (National Institute of Standards and Technology 2018).
- **Integration:** NIST kann in die bestehenden Sicherheitsrichtlinien der Institution integriert werden und hilft bei der Behebung existierender Schwachstellen (Gopstein, et al. 2020).
- **Kosteneffizienz:** Da die Umsetzung nicht zwingend das gesamte Framework umfassen muss, können Institutionen maßgeschneiderte Sicherheitsschutzmaßnahmen, ohne ihre Budgetgrenze zu überschreiten, implementieren lassen (Alshar'e 2023).

Für die effektive Implementierung des NIST CSF in Bildungsinstitutionen sind folgende Aspekte relevant:

- **Institutionen/Organisationen mit begrenztem Budget**: Kleine Schulen haben die Möglichkeit, dieses Framework zu nutzen, sollten jedoch mit weniger komplexen Maßnahmen beginnen. Hierzu zählen z. B. regelmäßige Sicherheitsupdates, verstärkte Zugriffskontrollen für Lehrkräfte und Schüler sowie Schulungen zu Phishing-Angriffen.

- **Besonders relevante Risiken für Schulen:**
    - **Phishing:** Gezielte Angriffe auf Lehrkräfte und Schüler über E-Mail oder manipulierte Websites.
    - **Ransomware:** Verschlüsselung sensibler Daten (Schülerakten oder Verwaltungsinformationen).
    - **Schutz personenbezogener Daten:** Einhaltung der DSGVO, vor allem beim Umgang mit sensiblen Schüler- und Lehrerdaten. (Harjinder, et al. 2023)
- **Einfache Maßnahmen zur Implementierung:**
    - **Schulungen:** Regelmäßige Awareness-Trainings für Lehrkräften und Schülern (Harjinder, et al. 2023).
    - **Zugriffskontrollen:** Einführung sicherer Passwortrichtlinien und Multi-Faktor-Authentifizierung (National Institute of Standards and Technology 2018).
    - **Notfallpläne:** Entwicklung sowie die regelmäßige Aktualisierung von Reaktionsplänen im Falle von Cyberangriffen (Isele, et al. 2017).

4.3.3 Förderprogramme für Schulen

Wie bereits im Subkapitel ISO/IEC 27001 erwähnt, bestehen auch in diesem Fall für Bildungsinstitutionen, welche die Implementierung des NIST CSF in Erwägung ziehen, diverse Fördermöglichkeiten, die hier nur aufgezählt aber nicht näher erläutert werden:

- **EU-Förderprogramme für Cybersicherheit** (Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs 2021)
- **Nationale Förderprogramme** (Bundesministerium für Bildung, Wissenschaft und Forschung 2021)
- **Kooperationen mit IT-Sicherheitsunternehmen** (Bundesministerium für Bildung, Wissenschaft und Forschung 2025).

Zusammenfassend kann festgehalten werden, dass für Bildungseinrichtungen das NIST CSF als strategische Basis zum effektiven Schutz vor diversen Cyber-Angriffen sinnvoll ist. Dabei sind insbesondere die folgenden Vorteile zu berücksichtigen, die das Framework zu bieten hat: Einerseits sorgt es für eine strukturierte IT-Sicherheitsverwaltung und andererseits ist es flexibel genug, um auf individuelle Bedürfnisse der Institutionen/Organisationen adäquat reagieren zu können.

Dabei ist hervorzuheben, dass die Implementierung der Sicherheitsmaßnahmen in Bildungsinstitutionen schrittweise erfolgen kann, ohne dass hohe Kosten für den Einsatz entstehen. Des Weiteren wurde aufgezeigt, dass die Sensibilisierung des pädagogischen Personals für Cybersicherheit durch Schulungen als vorbeugende Maßnahme geeignet ist, wobei dadurch die Bewusstseinsbildung in Bezug auf Sicherheitsfragen wesentlich gestärkt wird .

Nicht zuletzt ermöglicht das NIST CSF eine nachhaltige Kultur der IT-Sicherheit, indem es den kontinuierlichen Optimierungsprozess fördert. Im Hinblick auf die zunehmende Risikolandschaft ist die Implementierung eines solchen Frameworks in Bildungsinstitutionen nicht nur ratsam, sondern zwingend erforderlich.

4.4 Vergleich und Synergien zwischen den Methoden

Zu den zentralen Herausforderungen moderner Organisationen gehört die Sicherstellung der Informationssicherheit. Im Zuge der Digitalisierungsprozesse und der damit verbundenen Cyberrisiken sind Unternehmen und Institutionen gefordert, effektive Sicherheitsmaßnahmen zu etablieren. In diesem Zusammenhang haben sich verschiedene Methoden und Standards durchgesetzt, die Organisationen dabei unterstützen, IT-Risiken zu identifizieren, zu bewerten und zu handhaben.

Im Folgenden werden die relevanten Sicherheitsansätze – ISO/IEC 27001, das NIST Cybersecurity Framework (CSF), die OCTAVE-Methode sowie BSI IT-Grundschutz und das Österreichische Informationssicherheitshandbuch – miteinander verglichen. Durch diesen Vergleich sollen einerseits die jeweiligen Synergiepotenziale aufgezeigt werden um eine fundierte Einschätzung über die kombinierte Anwendung dieser Ansätze zu ermöglichen, andererseits soll erörtert werden, inwiefern diese Methoden komplementär zueinander genutzt werden können, um eine ganzheitliche Sicherheitsstrategie zu entwickeln.

Im Rahmen der vorliegenden Arbeit sollen die Synergie näher erläutert werden, um das Thema dieses Subkapitels zu verdeutlichen. Der Begriff wird vom griechischen Wort *"synergos"* abgeleitet, was sinngemäß mit "zusammenarbeitend" oder "gemeinsam wirksam" übersetzt werden kann. In der Management- und Wirtschaftsliteratur wird der Begriff als *"die vorteilhafte Interaktion verschiedener Elemente mit dem Ziel, durch deren Zusammenwirken einen größeren Nutzen zu erzielen, als es die einzelnen Elemente für sich genommen ermöglichen würden"* (Hax und Majflut 1991) beschrieben.

In der IT-Sicherheit bedeutet dies Terminus, dass verschiedene Sicherheitsansätze nicht isoliert, sondern gezielt miteinander kombiniert werden sollten. Durch diese Verknüpfung können die Stärken additiv genutzt und mögliche Schwächen einzelner Maßnahmen kompensiert werden. Daraus lässt sich ableiten, dass mehrere konkret ausgearbeitete Sicherheitskonzepte in einer Wiese kombiniert werden sollten, sodass sich ihre Funktionalitäten ergänzen und die dadurch konzipierte Sicherheitsstrategie effizienter, umfassender und nachhaltiger wird. Ein solcher Ansatz könnte dazu beitragen, dass die Widerstandsfähigkeit gegenüber potenziellen Bedrohungen gesteigert und ein höheres Sicherheitsniveau erzielt wird.

Des Weiteren weist ein ausführlicher Vergleich der in vorigen Kapiteln präsentierten Methoden darauf hin, dass sie alle einem risikobezogenen Ansatz entsprechen, sich jedoch in ihren jeweiligen Merkmalen und Anforderungen an die Umsetzung

unterscheiden. Die nachfolgende Tabelle 2 enthält eine kompakte Übersicht über die relevanten Merkmale der einzelnen Methoden.

Merkmal	ISO/IEC 27001	NIST CSF	OCTAVE-Methode	BSI IT-Grundschutz /Österreichische Informationssicherheitshandbuch
Fokus	Informationssicherheitsmanagement	Cyberrisiko-management	Organisatorische Risiken	Kombination von Standards
Flexibilität	Hoch anpassbar	Sehr flexibel	Fokussiert auf Assets	National angepasst
Zertifikate	Ja	Nein	Nein	Nein
Kosten	Höher	Mittlere Kosten	Gering	Gering
Anwendung	Branchenunabhängig	Sektoren-übergreifend	Gut geeignet für KMUs und Bildungseinrichtungen	National

Tabelle 2 Vergleich zwischen IT-Sicherheitsansätzen

Aus der vorliegenden Übersicht geht hervor, dass die Anwendungsbereiche und der Implementierungsaufwand der verschiedenen Methoden bedeutende Unterschiede aufweisen. Während einige Ansätze eine flexible Nutzung ermöglichen, verlangt die Implementierung der ISO/IEC 27001 eine Zertifizierung, da es sich um einen international anerkannten Standard handelt, welcher die Einführung eines Informationssicherheitsmanagementsystems (ISMS) erfordert (Alshar'e 2023). Demgegenüber stellt das NIST CSF eine nicht verpflichtende Alternative dar, welche es Organisationen erlaubt, den Einsatzbereich und die Anwendung des CSF zu definieren. Die OCTAVE-Methode hingegen ist ein Instrument des Risikomanagements, das sich auf organisatorische, technische und menschliche Risiken fokussiert. Als weitere praxisorientierte Minimalschutzmaßnahmen lassen sich der IT-Grundschutz und das Österreichische Informationssicherheitshandbuch nennen, die unter anderem für den Schutz von Institutionen in Deutschland und Österreich eingesetzt werden können.

Trotz des Potenzials einer isolierten Anwendung einzelner Sicherheitsansätze zur Risikominderung, ist eine umfassende Risikominderung erst durch eine Kombination dieser Methoden möglich. In diesem Zusammenhang sind die folgenden Synergien von besonderer Relevanz:

1. **Kombination von ISO/IEC 27001 und NIST CSF:** Bei näherer Betrachtung dieser Kombination wird festgestellt, dass ISO/IEC 27001 eine formale Grundlage für ein ISMS schafft, während NIST CSF praxisorientierte Handlungsempfehlungen zur operativen Umsetzung liefert. Die Verbindung der beiden Ansätze führt dazu, dass Institutionen sowohl regulatorische

Anforderungen erfüllen als auch eine praxisnahe Umsetzung von Sicherheitsmaßnahmen sicherstellen können (Alshar'e 2023).

2. **Ergänzung durch OCTAVE:** Mit der OCTAVE-Methode legt ein besonderer Fokus auf die Einbeziehung des Personals sowie der organisatorischen Aspekte. Insbesondere Institutionen, die im Bildungssektor sowie in kleinen und mittleren Unternehmen (KMUs) profitieren von dieser Methode. Durch die Stärkung des Bewusstseins sowie Einbeziehung von Entscheidungsträgern wird die nachhaltige Umsetzung von Informationssicherheitsstrategien gefördert (Gerardo und Fajar 2022).
3. **IT-Grundschutz und nationale Sicherheitsrichtlinien:** Der BSI IT-Grundschutz ebenso wie das Österreichische Informationssicherheits-handbuch basieren auf international etablierten Sicherheitskonzepten, ergänzen diese jedoch mit praxisorientierten Lösungen, die spezifischen Erfordernisse nationaler Institutionen zugeschnitten sind und die bereits in dem Überblick zu den Methoden (Kapitel 4.1) thematisiert wurden. Diese Konzepte zielen darauf ab, die Effizienz beim Ressourceneinsatz zu verbessern, indem sie erprobte Sicherheitsmaßnahmen mit landes-spezifischen Bedingungen kombinieren (Bundesamt für Sicherheit in der Informationstechnik 2017), (Bundeskanzleramt Österreich 2023).

Basierend auf den Erkenntnissen der Synergien die in diesem Kapitel behandelt wurden, lässt sich festhalten, dass kein Ansatz existiert, der die Gewährleistung maximaler Sicherheit ermöglicht. Stattdessen bedarf die Entwicklung einer Strategie vor allem einer Orientierung an den jeweiligen Rahmenbedingungen sowie einer Kombination diverser Ansätze. Dies verdeutlicht, dass eine solche Strategie dynamisch und anpassungsfähig konzipiert sein muss und gleichermaßen technische, organisatorische sowie personelle Aspekte der Informationssicherheit berücksichtigen sollte. Vorteilhaft ist in diesem Zusammenhang die Kombination formaler Standards (ISO/IEC 27001) mit praxisnahen Frameworks (NIST CSF) sowie organisatorischen Methoden (OCTAVE). Eine solche Kombination ermöglicht eine ganzheitliche Betrachtung der IT-Sicherheit, die sowohl die strategische Steuerung als auch die praktische Umsetzung berücksichtigt. Demnach entsteht ein effektives Sicherheitskonzept nicht durch die Wahl einer einzelnen Methode, sondern durch die sinnvolle Kombination der Stärken verschiedener Ansätze.

5. Aktuelle Sicherheitslage in Bildungsinstitutionen

Allen Bildungsinstitutionen, die immer häufiger auf digitale Systeme – von digitalen Lehrplattformen über interaktive didaktische Technologien bis hin zu cloudbasierten Verwaltungssystemen – angewiesen sind, bietet dieser Trend zweifellos neue Chancen für die Modernisierung des Lehrens und Lernens, gleichzeitig birgt er aber auch ernste Sicherheitsrisiken. Die Häufigkeit und das Ausmaß von Cyberangriffen auf Schulen, Hochschulen und Universitäten haben in den letzten Jahren zugenommen. Zu den gefährlichsten davon zählen Bedrohungen wie Ransomware, Phishing und Datenlecks.

Doch nicht allein gezielte Attacken der Cyberkriminellen von außen sind eine ernstzunehmende Bedrohung für Bildungsinstitutionen, sondern auch interne Schwachstellen, unsichere Passwörter, veraltete Software oder mangelndes Bewusstsein für IT-Risiken bei Lehrenden und Lernenden machen sie anfälliger für Cyberangriffe. Eine unzureichende Sicherheitsstrategie gefährdet nicht nur den Schutz der sensiblen Daten von Schülern und Lehrern – im schlimmsten Fall kann sie auch den gesamten Betrieb von Schulen oder Hochschulen lahmlegen.

In diesem Abschnitt wird auch ein Überblick über die aktuelle Bedrohungslage dieser Institutionen vorgelegt. Abschließend wird anhand von praxisnahen Beispielen aufgezeigt, wie Bildungsinstitutionen ihre IT-Sicherheit verbessern und damit ihre Resilienz gegenüber modernen Cyber-Bedrohungen erhöhen können.

5.1 Typische Bedrohungsszenarien und Schutzmaßnahmen

Die Bildungsinstitutionen sind wegen der großen Menge an sensiblen Daten, die in ihren Datenbanken gespeichert sind, häufig Ziel von Cyber-Angriffen. Einige dieser Bedrohungen wurden bereits in Kapitel 2 diskutiert und werden hier nur in Bezug auf Bildungssektoren noch einmal angesprochen und ergänzt.

5.1.1 Typische Bedrohungsszenarien

Im folgenden Subkapitel werden typische Bedrohungsszenarien präsentiert, die speziell in digitalen Lernumgebungen auftreten und Bildungsinstitutionen vor besondere Herausforderungen stellen. Zu diesen Szenarien gehören unter anderem:

- **Sicherheitslücken in veralteten Programmen und Betriebssystemen** werden von Angreifern häufig ausgenutzt, um Schadsoftware einzuschleusen oder Zugriff auf sensible Daten zu erhalten (Huber 2023). Bei dieser weit verbreiteten Angriffsmethode werden bekannte Schwachstellen ausgenützt, um unbemerkt in Systeme einzudringen.
- **Phishing-Angriffe** machen etwa 30 % aller Cyberbedrohungen aus und zielen darauf ab, sensible Informationen wie Login-Daten abzufangen (Gurinaviciute 2024). Besonders perfide dabei ist, dass sich Angreifer oft als vertrauenswürdige

Institutionen ausgeben und so psychologischen Druck auf die Opfer ausüben, um diese zur Preisgabe vertraulicher Daten zu bewegen.

- **Zero-Trust-Ansätze** sind notwendig, da kein Benutzer und kein Gerät automatisch als vertrauenswürdig angesehen werden kann und ein nicht autorisierter Zugriff schwerwiegende Folgen für die Bildungseinrichtungen haben kann. Dieses Modell basiert auf dem Prinzip "Vertrauen ist gut, Kontrolle ist besser", wobei jede Zugriffsanfrage unabhängig davon, ob sie aus dem internen Netzwerk oder externen Quellen stammt, verifiziert wird (Bundesamt für Sicherheit in der Informationstechnik 2023).
- **Ransomware-Angriffe** können Bildungseinrichtungen erheblich schädigen, indem sie Daten verschlüsseln und Lösegeld fordern (Kaspersky Labs GmbH 2024). Diese Art von Angriffen ist besonders problematisch, da nicht nur der Zugriff auf wichtige Daten blockiert, sondern auch oft Lösegeld verlangt wird.
- **Fehlende IT-Sicherheitsrichtlinien** machen Schulen zu interessanten Zielen für Cyber-Angriffe. Mangels klar definierter Richtlinien zur Erkennung und Reaktion auf Bedrohungen führt dazu, dass Bildungsorganisationen oft nicht in der Lage sind, angemessen auf Angriffe zu reagieren (Prema und Kumar 2019).
- **DDoS-Angriffe**, die sich auf digitale Lernplattformen beziehen, beeinflussen deutlich den Schulbetrieb und tragen dazu bei, dass Schüler und Lehrer durch starke Überlastung von Servern auf wichtige digitale Ressourcen nicht mehr zugreifen können (Jawaid 2022).

5.1.2 Schutzmaßnahmen zur Abwehr von Cyberbedrohungen

Die beschriebenen Bedrohungen verdeutlichen die vielfältigen und ernstzunehmenden Risiken, vor denen Bildungsinstitutionen im Kontext der Cybersicherheit stehen. Von gezielten Angriffen wie Ransomware und Phishing bis hin zu infrastrukturellen Schwachstellen, die durch veraltete Systeme oder fehlende Sicherheitsrichtlinien entstehen, wird die Verfügbarkeit und Integrität digitaler Lernumgebungen bedroht.

Um diesen Bedrohungen wirksam vorzubeugen, sind gezielt Schutzmaßnahmen erforderlich, die sowohl präventive als auch reaktive Sicherheitsstrategien umfassen. Aus diesem Grund werden folgende zentrale Maßnahmen zur Abwehr von Cyber-bedrohungen näher erläutert:

- **Regelmäßige Updates und Sicherheitspatches** stellen sicher, dass bereits länger bekannte Schwachstellen geschlossen werden. Wicht ist es dabei, dass einerseits alle Systeme immer auf dem neuesten Stand sind und anderseits die Endpunkt-Security Lösungen, die Schadprogramme frühzeitig erkennen und beseitigen. Auf diese Weise wird verhindert, dass Schwachstellen missbraucht werden, bevor sie behoben sind (Bundesamt für Sicherheit in der Informationstechnik 2018).

- **MFA**, wie in Kapitel 2 erwähnt, bietet einen ergänzenden Schutz für Benutzerkonten, indem zusätzlich zum Passwort eine zweite Schutzstufe wie ein Einmal-Passwort (OTP) oder eine biometrische Verifikation verlangt wird (Rieß-Marchive 2021).
- **KI-basierte E-Mail-Filter** untersuchen E-Mails auf verdächtige Elemente wie Inhalt, Absender und Hyperlinks. So können sie betrügerische Phishing-E-Mails erkennen und blockieren, bevor sie den Nutzer erreichen. Dies gelingt vor allem durch den Einsatz von maschinellem Lernen, das Muster erkennt, die für schädliche Inhalte charakteristisch sind (Ott 2024).
- **"Least Privilege"** reduziert das Risiko von Missbrauch von Daten sowie unberechtigtem Zugriff, indem Nutzer nur die Zugriffsrechte erhalten, die für sie notwendig sind. Des Weiteren ermöglichen Audit-Protokolle und das Echtzeit-Monitoring eine umgehende Identifizierung und Reaktion auf verdächtige Aktivitäten, wodurch eine genaue Protokollierung sicherstellt, dass keine unautorisierten Änderungen vorgenommen werden können (Bundesamt für Sicherheit in der Informationstechnik 2017).
- **Backup-Strategien nach der 3-2-1-Regel** dienen dem Schutz vor Datenverlust durch Ransomware. Basierend auf der Regel werden drei Kopien der Daten auf zwei verschiedenen Speichermedien erstellt werden, wobei eine Kopie offline aufbewahrt werden muss. Darüber hinaus werden regelmäßige Tests der Recovery-Fähigkeit durchgeführt um einerseits sicherzustellen, dass die Backups im Notfall sehr schnell wiederherstellbar sind und anderseits, dass der Zugriff auf die Daten auch bei einem Ransomware-Angriff weiterhin erhalten bleibt (Rieß-Marchive 2021).
- **Klare Sicherheitsrichtlinien** helfen bei der Definition von klaren Rollen- und Rechtemanagementstrukturen, regelmäßige Sicherheitsaudits sowie Penetrationstest bzw. Schwachstellenscans, um Schwachstellen frühzeitig zu erkennen und zu beseitigen (C. C. Woody 2004). Durch die Festlegung solcher Richtlinien kann ein einheitliches Sicherheitslevel in der gesamten Institution sichergestellt werden.
- **Firewalls mit Deep Packet Inspection (DPI) Technologie** sind in der Lage, den Datenverkehr genau zu überwachen. So können beispielweise frühzeitig verdächtige Muster oder Datenpakete erkannt und Angriffe abgewehrt werden. Im Gegensatz zu herkömmlichen Firewalls ermöglichen sie nicht nur die Überprüfung der IP-Adressen, sondern auch die Überprüfung des Inhalts der Daten (Houyoux 2023).
- **Intrusion Detection and Prevention Systeme (IDS/IPS)** überprüfen in Echtzeit das Netzwerk auf unberechtigte Zugriffsversuche und verdächtige Aktivitäten. Währenddessen werden durch IDS verdächtige Muster identifiziert und durch IPS Angriffe aktiv abgewehrt. Beide dienen als Frühwarnsysteme und agieren sofort, um Bedrohungen abzuwehren (Houyoux 2023).

- **Cloud-DDoS-Schutzdienste** filtern sowohl eingehenden als auch ausgehenden Datenverkehr sowie Zugriffsraten und überwachen ungewöhnlich hohe Raten, um sicherzustellen, dass legitime Benutzer weiterhin auf den Dienst zugreifen können. Dies wird durch intelligente Algorithmen erreicht, die zwischen normalen und gefährlichen Anfragen unterscheiden können (Dare und Kanungo 2024).

Zusammenfassend lässt sich festhalten, dass eine umfassend konzipierte IT-Sicherheitsstrategie, die sowohl präventive als auch reaktive Maßnahmen berücksichtigt, von entscheidender Relevanz für Bildungsinstitutionen ist. Nur auf diese Weise kann den kontinuierlich sich wandelnden Bedrohungen wirkungsvoll entgegengetreten und die Resilienz gegenüber Cyberangriffen nachhaltig gestärkt werden.

5.2 Fallstudien und Best Practices

Das Subkapitel 5.2 dieser Bachelorarbeit befasst sich mit den Fallstudien und Lösungsansätzen zur IT-Sicherheit in Bildungsinstitutionen, insbesondere Schulen. Der Schwerpunkt der Untersuchungen liegt auf der Übertragbarkeit bewährter Sicherheitsstrategien auf andere Institutionen/Organisationen. Basierend auf diesen Studien wurden Best Practices identifiziert, die auf verschiedene Schulen und Bildungseinrichtungen übertragbar sind. Des Weiteren wurden Faktoren analysiert, die zu einer erfolgreichen Umsetzung von Sicherheitsmaßnahmen beitragen können. Diese Studien behandelten verschiedene Aspekte der IT-Sicherheit, wie z. B. Ransomware-Attacken, BYOD, Content Filterung und Netzwerksicherheit.

5.2.1 Fallstudie 1: Cybersicherheitsprogramm an einer Sekundarschule in Arizona

Ein hervorragendes Beispiel für eine erfolgreiche Implementierung von Cybersicherheitsprogrammen in Schulen stellt ein vier Jahre dauernde Programm einer High School in Arizona dar. Der Fokus dieser Studie liegt auf der Implementierung von Cybersecurity-Bildung im K-12-Bereich, d. h. vom Kindergarten bis zur Oberschule, mit dem Ziel, den Fachkräftemangel in diesem Bereich zu verringern und das Sicherheitsbewusstsein zu stärken. Eine wesentliche Herausforderung besteht in der ungleichen Verfügbarkeit von Ressourcen in den verschiedenen Schulbezirken (Wagner und Alharthi 2024).

Im Schuljahr 2019/2020 wurde an der Basha High School ein Cybersecurity-Programm etabliert, das zu Beginn 60 Schüler umfasste und bis zum Jahr 2022/2023 auf 154 Teilnehmer angestiegen ist. Die Zahl der Absolventen stieg von einem im Jahr 2020 auf 17 im Jahr 2023. Das Programm kombiniert akademische Lehrinhalte mit praxisorientierten Lehrmethoden und umfasst zehn duale Kurse, darunter Netzwerksicherheit und Linux-Betriebssysteme. Darüber hinaus ergänzt die Initiative ihr Angebot durch

Cybersecurity-Camps wie Cyber-Patriot, Zertifizierungen (wie CompTIA A+ und Security+) und Praktikumsmöglichkeiten. Trotz dieser positiven Entwicklungen ergeben sich dennoch einige Herausforderungen wie: Die Rekrutierung von qualifizierten Lehrkräften, die oft in die Industrie wechseln (Wagner und Alharthi 2024)

Die anfänglichen Investitionen in diesem Programm von 32.000 USD ermöglichten die Schaffung einer isolierten Netzwerkinfrastruktur, in der jedoch technische Einschränkungen, insbesondere durch begrenzte Rechnerleistung, bestehen. Aktuell stehen drei Klassenzimmer und ein Career and Technical Education-Labor zur Verfügung, jedoch fehlen spezialisierte "Cyber-Ranges" dh. Umgebung die für praktische Übungen und Simulationen erforderlich (Wagner und Alharthi 2024).

Das Programm erleichtert den Zugang zu Hochschulen, beispielsweise zum "Chandler-Gilbert Community College" oder zur "University of Arizona", und eröffnet vielfältige berufliche Perspektiven in der IT-Branche, im Militär oder über entsprechende Zertifizierungen. Dennoch gibt es weiterhin Einschränkungen. Hierzu zählen: Das Fehlen verbindlicher K-12-Cybersecurity-Standards bis zum Jahr 2021, erschwerte Implementierung aufgrund administrativer Prozesse sowie ungleicher Zugang zu Ressourcen für sozial benachteiligte Schüler (Wagner und Alharthi 2024).

Zur Überwindung dieser Probleme werden folgende Lösungsansätze empfohlen: Eine intensivere Zusammenarbeit mit der Industrie, die Förderung kreativer Problemlösungsansätze sowie der Austausch mit anderen Bildungsprogrammen (Wagner und Alharthi 2024).

Die Fallstudie demonstriert, dass die Implementierung von Cybersecurity-Programmen in Schulen möglich ist, allerdings sind langfristig zusätzliche Ressourcen, qualifizierte Lehrkräfte und strukturelle Unterstützung erforderlich. Die Ergebnisse zeigen, dass die Integration von Cybersicherheit in den Lehrplan nicht nur die IT-Kompetenzen der Schüler verbessert, sondern auch einen wichtigen Beitrag zum Schutz der Schulnetzwerke leistet. Das Programm zielt darauf ab, Schüler für Cybersicherheits-risiken zu sensibilisieren und ihre Karrierechancen durch eine fundierte Ausbildung in diesem Bereich zu erhöhen (Wagner und Alharthi 2024).

5.2.2 Fallstudie 2: Sicherheitsherausforderungen bei digitalen Lernplattformen

In der heutigen modernen Bildungslandschaft sind digitale Lernplattformen wie "Moodle" und "Zoom" fest etabliert und nahezu unverzichtbar. Sie ermöglichen eine flexible und effiziente Gestaltung des Lehr- und Lernprozesses, bringen jedoch zugleich hohe Sicherheitsrisiken mit sich. Diese Fallstudie analysiert die wesentlichen Bedrohungen, denen digitale Bildungsplattformen ausgesetzt sind, und präsentiert geeignete Schutzmaßnahmen. Basierend auf den Erkenntnissen aus vorliegender Studie lassen sich mehrere Schwachstellen, die digitale Lernplattformen anfällig machen, identifizieren:

- **Brute-Force-Angriffe auf Zugangsdaten:** Eine Vielzahl von Lernplattformen verwendet herkömmliche Passwort-Authentifizierungsmethoden, die durch Brute-Force-Angriffe überwunden werden können. Bei diesen Angriffen versuchen Angreifer, Passwortkombinationen systematisch durchzuprobieren, bis unbefugter Zugriff auf Benutzerkonten erlangt wird.
- **Session Hijacking:** Mithilfe dieser Attacken können Angreifer eine aktive Sitzung übernehmen und so Zugriff auf sensible Informationen und administrative Funktionen erlangen. Insbesondere die Lernplattform Moodle ist von dieser Angriffsform betroffen.
- **Zoom-Bombing und Remote-Code-Ausführung**: Auf der Plattform Zoom kommt es zu unerwünschten Störungen durch unautorisierte Benutzer, die auch als "Zoom-Bombing" bezeichnet werden. Zudem sind Sicherheitslücken bekannt, die es Angreifern ermöglichen, Schadcode auf den Geräten der Nutzer zu installieren und auszuführen.
- **Cross-Site-Scripting-Angriffen:** Dieser Angriffstyp bezieht sich auf Einschleusen von bösartigem Code in Webanwendungen, mit dem Ziel, Benutzerdaten zu stehlen oder gefälschte Login-Seiten für Phishing-Angriffe zu erzeugen.
- **Malware und DDoS-Angriffe:** Während der Pandemie wurde eine Zunahme der Cyberangriffe auf Bildungseinrichtungen beobachtet, wobei DDoS-Angriffe (die 2020 um 550 % zunahmen) eine besondere Rolle spielten. Dies führte zu einer Störung des Unterrichts und der Funktionsfähigkeit digitaler Lernplattformen. (Salvador Ruiz, Llerena Alvarez und Dai Nguyen 2021)

Um solchen Angriffen entgegen zu wirken, ist ein ganzheitlicher Ansatz erforderlich, der technische, organisatorische und präventive Sicherheitsmaßnahmen miteinander kombiniert. Folgende Strategien haben sich als besonders effektive Schutzmaßnahmen erwiesen:

- **Kryptographie zur Sicherstellung der Vertraulichkeit und Integrität:** Die Implementierung moderner Verschlüsselungstechnologien, wie TLS und AES ist von großer Bedeutung, um die Vertraulichkeit von Informationen zu sichern.
- **Biometrische Authentifizierung und MFA:** Durch die Implementierung von MFA oder biometrischen Verfahren wie Fingerabdruck- und Gesichtserkennung lässt sich das Risiko unerlaubter Zugriffe reduzieren.
- **Intrusion Detection Systems (IDS) und Firewalls:** Durch den Einsatz von Netzwerksicherheitslösungen wie IDS und Firewalls ist es möglich, verdächtige Aktivitäten innerhalb der Lernplattformen rechtzeitig zu erkennen und abzuwehren.

- **Digitale Wasserzeichen zur Identifizierung von Datenlecks:** Die Nutzung ermöglicht die Nachvollziehung der Herkunft von Datenlecks und verhindert gleichzeitig den unautorisierten Zugriff auf vertrauliche Inhalte.
- **Regelmäßige Software-Updates und Sicherheits-Patches:** Kontinuierliche Wartung und Aktualisierung der Plattformen ist unerlässlich, da ein Großteil der genannten Sicherheitslücken aus veralteter oder unzureichend gesicherter Software resultiert.
- **Ein proaktives Sicherheitsmanagementmodell:** Dies beinhaltet die Implementierung eines fortlaufenden Sicherheitsmanagementprozesses, welcher die Phasen: Plan, Implementierung, Evaluierung und Wartung umfasst. Ein solcher Ansatz ermöglicht eine dynamische Anpassung an neue Bedrohungen. (Salvador Ruiz, Llerena Alvarez und Dai Nguyen 2021)

Zusammenfassend verdeutlicht die Fallstudie, dass die Nutzung digitaler Lernplattformen in der modernen Bildung eine bedeutende Rolle spielt, gleichzeitig aber auch erhebliche Sicherheitsrisiken mit sich trägt. In der Konsequenz wird deutlich, dass allein ein reaktives Vorgehen nicht ausreichend ist, sondern eine Kombination aus präventiven Sicherheitsmaßnahmen und einem ganzheitlichen Ansatz erforderlich ist, um die Integrität, Verfügbarkeit und Vertraulichkeit digitaler Bildungsressourcen zu schützen.

5.2.3 Fallstudie 3: Cybersicherheitsbewusstsein bei Lehrkräften

In der Studie "Cyber security awareness among primary school teachers" wird dargelegt, dass der technologische Fortschritt und die progressive Vernetzung der Gesellschaft das Risiko von Datendiebstahl und Identitätsmissbrauch erhöhen. Dieser Aspekt ist insbesondere für Schüler, die einen großen Teil ihrer Zeit im Internet verbringen, von hoher Relevanz. Zudem wurde festgestellt, dass das Bewusstsein für Cybersicherheit unter Grundschullehrkräften stark variiert. Als Einflussfaktoren werden dabei insbesondere das Geschlecht, die Unterrichtssprache, der Schultyp (staatlich oder privat), die Berufserfahrung und die Bildungsqualifikation der Lehrkräfte genannt. Die vorliegende Untersuchung wurde mit einer Stichprobe von 120 Lehrkräften aus 30 Schulen in Indien durchgeführt. Die Ergebnisse zeigen signifikante Unterschiede im Bewusstsein für Cybersicherheit. Insbesondere männliche Lehrkräfte, Lehrer an Englisch-Mittelschulen sowie an privaten Schulen mit weniger als fünf Jahren Berufserfahrung und Abschluss auf der Sekundarstufe hatten ein deutlich höheres Sicherheitsbewusstsein als ihre Vergleichsgruppen. (Prema und Kumar 2019)

Die Studie betont auch die zunehmende Relevanz des Cybersicherheitsbewusstseins angesichts zunehmender Risiken wie Identitätsdiebstahl und betont die Notwendigkeit einer gezielten Schulung von Lehrkräften, um Schüler und die Gesellschaft besser zu schützen. In diesem Zusammenhang wird die Verwendung sicherer Passwörter, der Schutz sensibler Daten, der Einsatz von Antiviren-Software und die Vermeidung unbekannter Downloads empfohlen. Darüber hinaus weist die Studie auf die

Notwendigkeit hin, Cybersicherheitsbildung in das Schulsystem zu integrieren, um die zukünftigen Risiken zu minimieren und eine sichere digitale Lernumgebung zu gewährleisten. (Prema und Kumar 2019)

5.2.4 Fallstudie 4: Umgang mit Ransomware-Angriffen

Laut einer Analyse von "Kaspersky" wird die Thematik der steigenden Cyberangriffe auf Bildungsinstitutionen untersucht. Dabei wird ersichtlich, dass die Zahl der Angriffe auf diese Institutionen weltweit zunimmt. Besonders hervorzuheben ist in diesem Kontext der Bildungssektor der USA, der mittlerweile zu den an den stärksten betroffenen Bereichen zählt. Auch in Großbritannien ist ein Anstieg der Attacken auf Schulen um 55 % zwischen 2022 und 2023 ersichtlich. Diese Entwicklung ist ein Anlass zur Reflexion darüber, aus welchen Gründen Schulen für Cyberkriminelle ein so attraktives Ziel darstellen. Als Ursache ist hier die zunehmende Digitalisierung der Schulen zu nennen, die zu einer Speicherung großer Mengen sensibler Daten führt. Zudem erschweren begrenzte finanzielle Ressourcen und unzureichende Schutzmaßnahmen eine effektive Absicherung, wodurch Bildungseinrichtungen besonders anfällig für Cyberangriffe sind (Kaspersky Labs GmbH 2024). Dies wird auch durch eine Vielzahl von Cyberangriffen auf Schulen ersichtlich, welche die zunehmend drohende Bedrohungslage veranschaulichen, darunter beispielweise:

- **Highline Public Schools (USA):** Als Konsequenz eines Cyberangriffs wurden 34 Schulen geschlossen, über 17.000 Schüler waren betroffen.
- **Singapur:** Der Angriff eines Hackers führte zur Löschung der Daten von 13.000 im Unterricht verwendeten iPads und Chromebooks.
- **Toronto District School Board in Kanada:** Nach einem Ransomware-Angriff waren nahezu 600 Schulen lahmgelegt.
- **Western Sydney University in Australien**: Durch einen Hackerangriff wurde die IT-Infrastruktur der Universität beeinträchtigt, die über 35.000 Studierende betreut. (Kaspersky Labs GmbH 2024)

Um solche Vorfälle zukünftig zu verhindern, sollten Bildungsinstitutionen adäquate Maßnahmen zur Cybersicherheit implementieren. Diese Problematik ist insbesondere im Kontext der Nutzung unsicherer Software für Privatanwender relevant. Aus präventiver Sicht wird der Einsatz geeigneter Sicherheitslösungen für kleine und mittlere Unternehmen (KMU) empfohlen. Als Beispiel kann hier Kaspersky Small Office Security genannt werden, die neben Schutz vor Malware auch automatische Backups und ein Passwort-Management bietet. Des Weiteren ist die Schulung des Lehrpersonals als ein weiterer wesentlicher Faktor zu betrachten. Zur Stärkung des Bewusstseins für Cybergefahren und zur proaktiven Prävention von Angriffen können Plattformen wie die Kaspersky Automated Security Awareness Plattform eingesetzt werden (Kaspersky Labs GmbH 2024).

Zusammenfassend lässt sich sagen, dass Cyberangriffe auf Bildungsinstitutionen nicht nur die Daten, sondern auch den reibungslosen Ablauf des Unterrichts gefährden können. Diese Erkenntnis verdeutlicht die Notwendigkeit effektiver Schutzmaßnahmen in Form von robuster Sicherheitssoftware und gezielten Schulungen für Lehrkräfte und Schüler, um die Sicherheit und den reibungslosen Ablauf des Unterrichts in Zukunft zu gewährleisten.

5.2.5 Best Practices

Im Rahmen der vorliegenden Arbeit können aus den in Unterkapitel 5.2.4 präsentierten Studien die nachfolgenden Best Practices abgeleitet werden:

- **Regelmäßige Sicherheits-Audits:** Um Sicherheitslücken frühzeitig erkennen und beheben zu können, sollten Bildungsinstitutionen ihre Netzwerke regelmäßig kontrollieren. Um Schwachstellen effizienter zu ermitteln, können auch automatisierte Sicherheitsscans behilflich sein. Wie Studie von Kaspersky darstellte, ermöglichen regelmäßige Audits eine präzisere Risikoanalyse und tragen zur kontinuierlichen Verbesserung der Sicherheitsmaßnahmen bei (Kaspersky Labs GmbH 2024).
- **Sensibilisierung durch Bildung:** Dauerhafte Bildungsaktivitäten auf allen Ebenen, von Schülern über Lehrer bis hin zu Verwaltungsangestellten, sind unabdingbar. Des Weiteren müssen solche Awareness-Programme sowohl theoretische als auch praktische Komponenten enthalten. Durch die Einführung standardisierter Trainings kann in der gesamten Institution ein einheitliches Sicherheitsbewusstsein geschaffen werden (Ondrušková und Pospíšil 2023), (Prema und Kumar 2019).
- **Modernes Cyber Security Framework:** Durch die Integration moderner Technologien wie MFA, Verschlüsselung und anderer Sicherheitsprotokolle wird die Sicherheit deutlich erhöht. Hierbei ist der Einsatz von Content Filterung von besonderer Bedeutung, um unerwünschte oder potenziell gefährliche Inhalte in Schulnetzwerken zu sperren. Des Weiteren wird deutlich, dass eine anpassungsfähige Sicherheitsstrategie, die auf aktuelle Bedrohungen eingeht, für den langfristigen Schutz digitaler Bildungsinstitutionen entscheidend ist (Almagro, et al. 2020).

Aus den vorliegenden Studien und Best Practices ergeben sich klare Handlungsempfehlungen für Schulen und andere Bildungseinrichtungen hinsichtlich der IT-Sicherheit. In Anbetracht der zunehmenden Cyber-Bedrohungen ist ein entschlossenes Handeln unabdingbar, um Netzwerke und sensible Daten nachhaltig zu schützen. Zu diesem Zweck sind technische Maßnahmen wie Firewalls und Passwortmanager erforderlich, welche Sicherheitslücken schließen und Angriffe erschweren.

Allerdings ist der Einsatz moderner Schutzsysteme allein nicht ausreichend. Eine effektive Sicherheitsstrategie erfordert ein ganzheitliches Konzept, das technische

und organisatorische Maßnahmen miteinander verbindet. Neben leistungsstarken IT-Sicherheitslösungen sind klare Richtlinien für den Umgang mit digitalen Systemen und regelmäßige Schulungen von großer Bedeutung, um das Bewusstsein für potenzielle Bedrohungen in der gesamten Schulumgebung zu schärfen. Nur durch diese Kombination von technischen und organisatorischen Maßnahmen kann langfristig ein hohes Niveau an Sicherheit garantiert werden.

5.3 Herausforderungen und Lösungsansätze

Die Digitalisierung stellt Bildungsinstitutionen vor große Herausforderungen, bietet aber gleichzeitig zahlreiche Chancen – von der Digitalisierung des Unterrichts über die Nutzung moderner Bildungsplattformen bis hin zur Zusammenarbeit im digitalen Lernumfeld. Dies betrifft insbesondere den Bereich der IT-Sicherheit, wo die Anzahl der Cyber-Angriffe auf Bildungsinstitutionen, welche sensible Daten von Studierenden, Lehrenden und Verwaltungsprozessen aufbewahren, stetig zunimmt. Laut "IT-Daily.net" notiert beispielwies der Bildungssektor an 3100 Angriffe pro Woche was ungefähr 37 % mehr ist als Jahr davor (Check Point Software Technologies Ltd 2024). In diesem Fall kann ein Mangel an angemessenen Sicherheitsmaßnahmen zu Datenverlust, Systemausfällen und sogar Identitätsdiebstahl führen, was ernsthafte Konsequenzen haben kann (Bundesamt für Sicherheit in der Informationstechnik n.d.).

Im Interesse der Hochschule selbst, der Studierenden und ihrer Eltern ist es notwendig, solche Szenarien zu verhindern und daher wirksame Maßnahmen zur Verbesserung der Sicherheit zu treffen. Dabei müssen sowohl sensible Daten als auch die langfristige Sicherheit der Systeme geschützt werden, was sowohl interne als auch externe Sicherheitsmaßnahmen erfordert. Im folgenden Unterkapitel werden verschiedene Ansätze zur Bewältigung dieser Herausforderungen vorgestellt und auf die in Kapitel 5.2 diskutierten Best Practices verwiesen, welche verdeutlichen, wie Bildungsinstitutionen die IT-Sicherheit effektiv stärken können.

Im Folgenden werden daher verschiedene Lösungsansätze aufgelistet, die zur nachhaltigen Sicherung der IT-Infrastruktur in Bildungseinrichtungen einen Beitrag leisten können:

1. **Finanzielle Engpässe** – sie betreffen vor allem kleinere Bildungsinstitutionen, die bei der Anschaffung von IT-Ausrüstung und Software sowie bei der Anstellung von qualifiziertem Personal auf finanzielle Unterstützung des Staates angewiesen sind. Demzufolge sind folgende Lösungen denkbar:
    - Die Relevanz von Finanzierungsunterstützung liegt insbesondere in staatlichen Förderprogrammen, die Bildungsinstitutionen gezielt in ihrer IT-Sicherheitsstrategie fördern können (Cybersicherheit, Nationales Koordinierungszentrum n.d.).

- Public-Private-Partnerships (PPP) zur Bereitstellung von Unternehmensressourcen (European Union Agency for Cybersecurity n.d.).
- Cyber-Versicherungen zum Schutz vor finanziellen Schäden durch Cyber-Attacken (Wirtschaftskammer Österreich 2024).

2. **Mangelndes technisches Know-how und Trainingsbedarf** – wie aus den Fallstudien in Kapitel 5.2 hervorgeht, sind Trainingsprogramme und Sensibilisierungsschulungen für eine effektive IT-Sicherheitsstrategie von entscheidender Bedeutung. Best Practices beinhalten:
   - Regelmäßige Schulungen und Workshops sind wichtige Bestandteile einer nachhaltigen Sicherheitskultur. Sie fördern die Bewusstseinsbildung für IT-Sicherheitsrisiken und liefern konkrete Maßnahmen.
   - Interaktive Lernansätze unterstützen ein besseres Verständnis von IT-Sicherheit.
   - Aus Sicht der Experten sind praxisorientierte Szenarien entscheidend, um das Sicherheitsbewusstsein zu schärfen und die Sicherheitskompetenz zu erweitern (Almagro, et al. 2020).
3. Die **Sicherheit von digitalen Lernplattformen** – beispielsweise Moodle und Zoom ist zwar unabdingbar, beinhaltet aber auch Sicherheitsrisiken, die bereits in Kapitel 5.2 näher erläutert wurden. Diese Risiken lassen sich durch eine Kombination von technischen und organisatorischen Maßnahmen minimieren. Hierzu gehören:
   - DSGVO – konforme Datenschutzrichtlinien (Sobota 2022).
   - Biometrische Authentifizierung, Verschlüsselung sowie Digitales Wasserzeichen (Hierbei handelt es sich um eine Technik zur Markierung digitaler Inhalte, die sowohl sichtbare als auch unsichtbare Form annehmen kann. Dazu zählen beispielsweise Bilder, Videos oder Dokumente) (Salvador Ruiz, Llerena Alvarez und Dai Nguyen 2021) .
   - Zero-Trust-Architekturen gewährleisten eine umfassende Zugriffs-kontrolle und damit eine strenge Regelung des Datenzugriffs (Bundesamt für Sicherheit in der Informationstechnik 2023).
4. **BYOD** – Die Verwendung privater Geräte in Bildungsinstitutionen stellt ein erhöhtes Risiko dar, das in Kapitel 5.2 ausführlich behandelt bzw. betont wurde. Bewährte Praktiken sind in diesem Fall (Ferdous 2022):
   - Trennung von privaten und institutionellen IT-Systemen durch segmentierte Netzwerke.
   - Erforderliche Sicherheitssoftware wie Firewalls und VPNs.
   - Rollenbasierte Zugriffskontrolle (RBAC) zur Minimierung des Risikos von unbefugten Zugriffen.
5. **Notfall- und Krisenmanagement** (gemäß den zuvor erarbeiteten Fallstudien in Kapitel 5.2) – ist für die effektive Abwehr von Cyber-Bedrohungen wichtig. Die dafür notwendigen Bestandteile sind z. B. (Kirvan 2024):

- Incident-Response-Pläne, d. h. Notfallpläne
- Eskalationsregeln: Offene Krisenkommunikation, um relevante Parteien schnell und effizient zu informieren
- Regelmäßige Notfallübungen, um Reaktionszeiten zu verkürzen und Schäden zu minimieren.

6. **Datenschutzanforderungen für Bildungseinrichtungen** – die Bildungsinstitutionen sind verpflichtet, die strengen Datenschutzanforderungen der DSGVO und der nationalen Gesetze einzuhalten. Folgende Grundsätze sind wichtig (Sobota 2022):
   - Einwilligung und Transparenz: Grundsätze für die datenschutzkonforme Verarbeitung personenbezogener Daten.
   - Datenminimierung: Speicherung nur der absolut notwendigen Daten.
   - Recht auf Löschung: Möglichkeit, nicht mehr benötigte Daten zu löschen.
   - Datenschutz-Folgenabschätzung: Bewertung möglicher Datenschutzrisiken vor der Einführung neuer IT-Systeme.
   - Technische und organisatorische Maßnahmen wie Verschlüsselung und Zugriffskontrollen sind für den Schutz sensibler Daten unerlässlich.

In Kapitel 5.2 wurde bereits darauf hingewiesen, dass im Bildungswesen eine erfolgreiche IT-Sicherheitsstrategie nicht nur von technischen Lösungen, sondern auch von einer sorgfältigen Planung sowie aufgeklärten und gut eingeschulten Personal, abhängt. Von wesentlicher Bedeutung sind in diesem Zusammenhang eine fundierte Finanzplanung, regelmäßige Schulungen, wirksame Schutzmaßnahmen und ein klar definiertes Notfallmanagement.

Erkenntnisse der Fallstudien zeigen auch, dass Bildungseinrichtungen, die gezielt bewährte Best Practices anwenden, in der Lage sind, Cyber-Bedrohungen effektiver abzuwehren und sensible Daten besser zu schützen.

6. Methodische Vorgehen des praktischen Teils

Das vorliegende Kapitel widmet sich den methodischen Grundlagen zur Entwicklung, Implementierung und Validierung eines IT-Sicherheitskonzepts für die polnischen Schule des Jan III. Sobieski am Gymnasium Kalksburg. Angestrebt wird dabei ein systematisch aufgebautes, nachvollziehbares und praxisorientiertes Konzept, das die Reduktion erfassten Cyberangriffe um mindestens 50 % ermöglicht und die Sicherheit sensibler Daten – insbesondere von Schülern und Lehrkräften – erhöht sowie die Netzwerksicherheit langfristig verbessert.

Das methodische Vorgehen basiert auf einem mehrstufigen Verfahren, das sich an den in Kapitel 1.7 dargestellten Phasen orientiert und sowohl internationale als auch nationale Standards einbezieht. Dabei werden neben der OCTAVE-Methode auch Elemente der ISO/IEC 27001, des NIST CSF sowie des BSI-Grundschutzes und des Österreichischen Informationssicherheitshandbuchs berücksichtigt.

Die Konkretisierung dieses methodischen Rahmens und die Beschreibung der Vorgehensweise in den fünf zentralen Schritten von der Bestandsaufnahme über die Risikoanalyse bis hin zur Bewertung wird im nachfolgenden Subkapitel 6.1 präsentiert. Darauf aufbauend erfolgt in den Kapiteln 7 bis 10 die praktische Umsetzung.

6.1 Überblick über die methodische Vorgehensweise

In diesem Unterkapitel werden zuerst die methodischen Rahmen für die praktische Umsetzung des IT-Sicherheitskonzepts, die in den Kapiteln 7 bis 10 beschrieben werden, dargestellt. Diese Rahmenbedingungen basieren auf der OCTAVE-Methode (Operationally Critical Threat, Asset, and Vulnerability Evaluation) und werden durch internationale und nationale Standards (ISO/IEC 27001, NIST CSF, BSI-Grundschutzkompendium, Österreichisches Informationssicherheitshandbuch) ergänzt. Durch diese Kombination wird sichergestellt, dass sowohl technische als auch organisatorische Maßnahmen berücksichtigt werden, wobei ein besonderer Fokus auf die Anforderungen und Ressourcenbeschränkungen von Bildungsinstitutionen gelegt wird (vgl. Kapitel 3 und 4).

Der Ansatz gliedert sich in fünf verschiedene Phasen:

1. **Analyse der bestehenden IT-Infrastruktur:** Bestandsaufnahme der IT-Komponenten und Identifikation von kritischen Schwachstellen.
2. **Risikobewertung:** Priorisierung der Assets und Bewertung der Bedrohungen basierend auf OCTAVE.
3. **Entwicklung eines maßgeschneiderten Sicherheitskonzeptes:** Erarbeitung konkreter technischer und organisatorischer Maßnahmen.
4. **Implementierung:** Umsetzung der Sicherheitsmaßnahmen unter Berücksichtigung eines möglichst störungsfreien Betriebs.

5. **Evaluation:** Überprüfung der Wirksamkeit der getroffenen Maßnahmen anhand vordefinierter Erfolgskriterien (siehe Kapitel 6.5).

Für eine bessere Veranschaulichung des strukturierten Vorgehens ist Abbildung 4 als Flussdiagramm dargestellt welches die fünf Phasen der praktischen Umsetzung des IT-Sicherheitskonzepts bildlich präsentiert wird. Das Diagramm illustriert den schrittweisen Aufbau: von der Analyse der bestehenden IT-Infrastruktur über die Risikobewertung und Konzeptentwicklung bis hin zur Implementierung und abschließenden Evaluation.

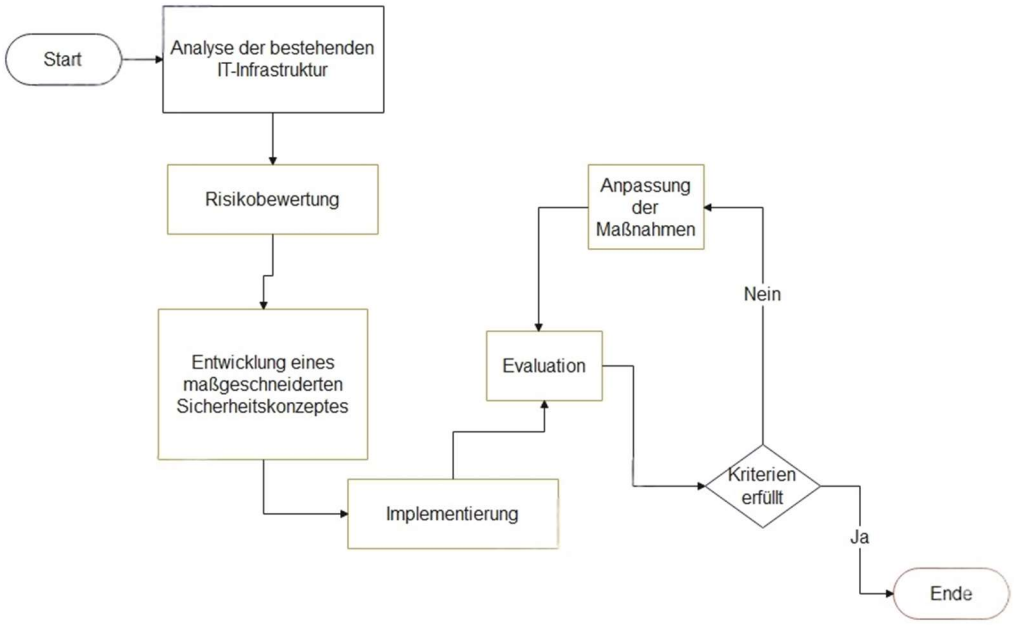

Abbildung 4 Methodischer Ablauf der Umsetzung des IT-Sicherheitskonzepts

6.2 Abgrenzung und Zielsetzung des praktischen Teils

In diesem Abschnitt wird der Fokus auf die IT-Infrastruktur der Polnischen Schule Jan III Sobieski in Wien gelegt, wie in Kapitel 1.1 beschrieben. Im Rahmen der Untersuchung wurden der zentrale Server, ein HP-Switch, stationäre Arbeitsplätze, Multifunktionsdrucker, WLAN-Router, interaktive Whiteboards sowie genutzte Cloud-Dienste analysiert. Diese Systeme werden im Hinblick auf ihre Sicherheitsanforderungen einer Analyse unterzogen, um darauf aufbauend gezielte Schutzmaßnahmen zu entwickeln.

Im Rahmen der Abgrenzung wurden Aspekte der physischen Sicherheit, wie etwa Einbruchschutz oder Zugangskontrollen, bewusst ausgeschlossen, da sie nicht direkt der Verantwortung der IT-Verantwortlichen als auch der Direktion unterliegen. Auch die relevanten juristischen Rahmenbedingungen, insbesondere die Datenschutz-Grundverordnung (DSGVO), werden insoweit berücksichtigt, sofern eine unmittelbare Auswirkung auf die IT-Infrastruktur und deren Schutzmaßnahmen festgestellt werden

kann. Dies ist beispielsweise bei der Datenverschlüsselung oder dem Zugriffsschutz der Fall.

Das Ziel dieser praxisorientierten Studie besteht in der Entwicklung eines IT-Sicherheitskonzeptes, das auf den in Kapitel 1 formulierten Forschungsfrage und Hypothese basiert und auf den festgelegten drei Ebenen wirksam ist:

- **Reduktion der Cybervorfälle:** Mindestens 50 % Verringerung gegenüber der Baseline und von 63 Vorfällen (Juni 2024).
- **Schutz sensibler Daten:** Technische (Verschlüsselung) und organisatorische Maßnahmen (Zugriffskontrollen).
- **Erhöhung der Netzwerksicherheit:** Behebung spezifischer Schwachstellen (Gäste-WLAN, Antivirus-Software).

Durch diese Maßnahmen soll nicht nur ein kurzfristiger Sicherheitsstandard an der Schule erreicht werden, sondern es wird auch ein langfristiger, übertragbarer Sicherheitsrahmen geschaffen, welcher als Referenz für andere Bildungsinstitutionen dienen kann. Um die Effektivität der technischen und organisatorischen Maßnahmen zu steigern, wird angestrebt, das Sicherheitsbewusstsein des Lehrpersonals und der Lernenden durch regelmäßige Schulungen und klar definierte Verhaltensrichtlinien zu stärken.

6.3 Verwendete Analysemethoden

Im Subkapitel 6.3 werden die Analysemethoden näher erläutert, die zur Erfassung der aktuellen Sicherheitslage der Schule verwendet werden und als Grundlage für das Sicherheitskonzept dienen. Zur umfassenden Erfassung der Sicherheitslage wurde ein Methodenmix aus verschiedenen Zur umfassenden und differenzierten Erfassung der Sicherheitslage wurde ein Methodenmix aus mehreren Ansätzen gewählt:

- **OCTAVE-Methode (vgl. Kapitel 3.2):**
  - Organisatorische Analyse (kritische Vermögenswerte, bestehende Praktiken).
  - Technische Analyse (Netzwerkarchitektur, Schwachstellen).
  - Strategieentwicklung (Risiko-Priorisierung, Maßnahmenableitung). (Alberts, et al. 2025)
- **Qualitative Methoden:**
  - Interviews/ Gespräche mit Schulleitung, Bibliothekpersonal und IT-Verantwortlichen (Erfassung organisatorischer Risiken).
  - Umfragen unter Lehrkräften zur Einschätzung des Sicherheits-bewusstseins.
- **Fallanalyse:** Untersuchung der dokumentierten 63 Cyberangriffe vom Juni 2024 (Muster, Schwachstellen, Gegenmaßnahmen).
- **Technische Werkzeuge:**

- OpenVAS oder ESET PROTECT zur Schwachstellenerkennung.
- ARMITAGE - Metasploit Framework (Penetrationstest um Schwachstellen in Netzwerken, Systemen oder Anwendungen aufzudecken).
- Checklisten (z.B. BSI-Grundschutz) für strukturierte Erfassung.

Diese Kombination liefert ein umfassendes Bild der Sicherheitslage und dient als Grundlage für gezielte Maßnahmen.

6.4 Ablauf der praktischen Umsetzung

In diesem Subkapitel wird der chronologische und operative Ablauf der Implementierung eines IT-Sicherheitskonzepts beleuchtet. Die praktische Umsetzung des Sicherheitskonzeptes erfolgt in mehreren klar definierten Phasen:

- **Phase 1 – Datenerhebung und Aufbereitung:**
  - IT-Inventarisierung und kurze Nutzerbefragungen.
  - Projektzeitplan definieren.
- **Phase 2 – Risikoanalyse:**
  - OCTAVE-Anwendung zur systematischen Risikobewertung.
- **Phase 3 – Entwicklung des Sicherheitskonzepts:**
  - Technische Maßnahmen (Verschlüsselung, Firewalls, VLANs, MFA).
  - Organisatorische Maßnahmen (Passwortmanagement, Schulungen).
- **Phase 4 – Implementierung:**
  - Konkrete Umsetzungsschritte (sicheres WLAN, Antivirus-Software-Update).
  - Schulung der Lehrer.
  - Umsetzungsdauer mit definierten Phasen.
- **Phase 5 – Monitoring:**
  - Einrichtung von Monitoring-System.
  - Penetrationstest
  - Nutzerfeedback zur Akzeptanz der Maßnahmen.

6.5 Validierungsansatz und Erfolgskriterien

Das Subkapitel 6.5 fokussiert sich auf der Evaluierung der Effektivität und Praxistauglichkeit des präsentierten Sicherheitskonzepts. Die Validierung dieser Studie erfolgt durch eine Kombination unterschiedlicher Methoden, die sowohl quantitative als auch qualitative Aspekte berücksichtigen. Im Rahmen dessen erfolgt die Definition messbarer Erfolgskriterien, welche als Fundament für die Bewertung dienen. Zur Überprüfung der Wirksamkeit des Sicherheitskonzepts werden drei Hauptansätze verfolgt:

- **Vorher-Nachher-Vergleich von Cybervorfällen**: Im Rahmen der Untersuchung wird ein Vergleich der Häufigkeit und Relevanz von Cybervorfällen vor und nach der Implementierung des Sicherheitskonzepts durchgeführt. Die dokumentierten

Sicherheitsvorfälle vom Juni 2024 sollen hier als Ausgangsbasis dienen. Der Beobachtungszeitraum umfasst jeweils drei bis vier Wochen vor und nach der Umsetzung der Maßnahmen. Diese Analyse gestattet die Messung der unmittelbaren Wirkung der implementierten Schutzmaßnahmen auf die Reduktion von Sicherheitsvorfällen.

- **Nutzerfeedback:** Die Beurteilung der Akzeptanz und Praxistauglichkeit der Sicherheitsmaßnahmen soll durch ein Feedback von Lehrenden erfolgen. Die Erhebung von Daten zu den Aspekten Benutzerfreundlichkeit, Verständlichkeit und subjektiv wahrgenommene Sicherheit erfolgt mittels strukturierter Umfrage. Ein hohes Maß an Akzeptanz ist entscheidend, um eine dauerhafte Umsetzung und Einhaltung der Sicherheitsvorgaben zu gewährleisten.
- **Penetrationstest:** Um die Robustheit der technischen Sicherheitsmaßnahmen zu prüfen, wird auch ein Penetrationstest durchgeführt. Diese simulieren gezielten Angriff auf das System, um Schwachstellen in der Infrastruktur, den Anwendungen und den Konfigurationen zu erkennen. Die Resultate der Tests werden wertvolle Erkenntnisse über die Wirksamkeit der implementierten Schutzmaßnahmen liefern sowie Verbesserungspotenziale offenbaren.

Die Wirksamkeit des Sicherheitskonzepts wird anhand folgender Kriterien bewertet:

- **Reduktion der Sicherheitsvorfälle um mindestens 50 %**: Gemäß der in dieser Bachelorarbeit aufgestellten Hypothese kann die Erreichung dieses Ziels als ausreichender Beweis betrachtet werden. Durch den Vorher-Nachher-Vergleich soll eine signifikante Reduktion der Anzahl und Schwere von Cybervorfällen evident werden.
- **Reduktion kritischer Schwachstellen um 50 %**: Mithilfe ESET Schwachstellenscan soll die Anzahl kritischer Schwachstellen im System reduziert werden, was dazu beitragen soll, dass die Angriffsflächen begrenzt werden.
- **Systemverfügbarkeit von 99 %**: Die implementierten Maßnahmen dürfen die Verfügbarkeit der Systeme nicht beeinträchtigen, sondern sollen eine unterbrechungsfreie Nutzung gewährleisten.
- **Gestärktes Sicherheitsbewusstsein**: Das Nutzerfeedback soll dazu beitragen, das Bewusstsein für IT-Sicherheitsfragen sowohl bei Lehrenden als auch bei Lernenden zu erhöhen. Dies wird durch regelmäßige Schulungen unterstützt.
- **Etablierung eines regelmäßigen Audit - Zyklus und Update - Managements**: Die Einführung eines strukturierten Prozesses für wiederkehrende Sicherheitsaudits und zeitnahe Systemupdates soll die langfristige Wirksamkeit des Konzepts sichern.

Die Umsetzung des Sicherheitskonzepts ist durch begrenzte finanzielle Mittel und eingeschränktes Personalengagement herausfordernd. Um diesen Einschränkungen zu begegnen, werden folgende Optimierungsvorschläge der Direktion unterbreitet:

- **Nutzung von Förderprogrammen**: Vor allem im Bereich der Lizenzverlängerung sollte zusammen mit der Direktion ein Plan erarbeitet werden, um Fördermöglichkeiten auf nationaler Ebene sowie über die polnische Botschaft oder polnische Lehrerverbände zu prüfen. Ziel ist es, finanzielle Mittel für die Aufrechterhaltung der Sicherheitsmaßnahmen zu sichern.
- **Priorisierung von Maßnahmen**: Eine schrittweise Umsetzung, die sich auf die kritischsten Schwachstellen konzentriert, ermöglicht eine effiziente Ressourcennutzung und erzielt frühzeitig sichtbare Ergebnisse.

Die Evaluierung des Sicherheitskonzepts erfolgt auf Basis einer Kombination aus Vorher-Nachher-Vergleich, Nutzerfeedback und Penetrationstest, welche eine umfassende Bewertung der Wirksamkeit ermöglicht. Die in diesem Zusammenhang definierten Erfolgskriterien umfassen eine Reihe von Aspekten, darunter die Reduktion von Sicherheitsvorfällen und Schwachstellen, die Steigerung der Systemverfügbarkeit sowie die Stärkung des Sicherheitsbewusstseins. Diese Kriterien bieten klare Orientierungspunkte für die Bewertung der Effektivität der getroffenen Maßnahmen. Die Berücksichtigung einschränkender Faktoren sowie die vorgeschlagenen Optimierungsmaßnahmen zielen auf eine realistische und nachhaltige Umsetzung des Konzepts ab.

7. Analyse der bestehenden IT-Infrastruktur

Die IT-Infrastruktur der Schule von Jan III Sobieski Schule in Kalksburg ist eine zentrale Säule für den Unterrichtsbetrieb und die administrative Verwaltung. Die wachsende Abhängigkeit von digitalen Technologien bietet sowohl Chancen als auch Risiken. Deshalb ist es notwendig, eine detaillierte Analyse der bestehenden IT-Struktur durchzuführen, um Schwachstellen zu identifizieren, Sicherheitsmaßnahmen zu evaluieren und die digitale Widerstandsfähigkeit der Schule zu stärken. Das vorliegende Kapitel hat zum Ziel, die aktuelle IT-Landschaft der Schule zu erfassen, vorhandene Sicherheitsmaßnahmen zu identifizieren, potenzielle Schwachstellen zu dokumentieren und vergangene Cyber-Angriffe zu analysieren. Diese umfassende Analyse bildet die Grundlage für gezielte Optimierungsmaßnahmen und die Entwicklung eines nachhaltigen IT-Sicherheitskonzeptes:

7.1 Beschreibung der aktuellen IT-Architektur

7.2 Vorhandene Sicherheitsmaßnahmen (IST-Zustand)

7.3 Analyse bisheriger Cyberangriffe

7.4 Identifikation von Schwachstelle und Risiken (Grobe IST-Bewertung)

Diese Analyse dient als Basis für die spätere Entwicklung eines verbesserten IT-Sicherheitskonzepts, dass die digitale Sicherheit der Schule nachhaltig erhöht und ihre Widerstandsfähigkeit gegenüber Cyberbedrohungen stärkt.

7.1 Beschreibung der aktuellen IT-Architektur

Die Polnische Schule Jan III Sobieski, eine unabhängige Bildungseinrichtung innerhalb des Kollegiums Kalksburg, hat ihre IT-Infrastruktur in den letzten Jahren, insbesondere während der COVID-19-Pandemie, grundlegend modernisiert. Ziel dieser Modernisierung war, den gestiegenen Anforderungen an digitale Lernumgebungen, administrative Abläufe und IT-Sicherheit gerecht zu werden. Die aktuelle IT-Landschaft der Schule umfasst eine breite Palette an Hardware- und Softwarekomponenten, die sowohl den Unterricht als auch die Verwaltung unterstützen. In diesem Kapitel findet eine detaillierte Beschreibung der räumlichen Struktur, der Hardware- und Software-Ausstattung sowie der Netzwerkinfrastruktur. Hierbei werden auch bestehende Schwächen analysiert, Optimierungspotenziale identifiziert und geplante Erweiterungen vorgestellt, die dazu dienen sollen, die Infrastruktur zukunftssicher zu gestalten. Darüber hinaus werden neue Aspekte wie Nachhaltigkeit, Schulungsmaßnahmen und Cloud-Integration berücksichtigt, um eine umfassende Bewertung der IT-Landschaft zu ermöglichen.

7.1.1 Räumliche Struktur der IT-Infrastruktur

Die Polnische Schule nutzt ausschließlich die Räumlichkeiten im vierten Stock des Kollegiums Kalksburg. Die IT-Infrastruktur ist strategisch auf verschiedene Räume verteilt, um eine effiziente Nutzung für Unterricht und Verwaltung zu gewährleisten. Die folgenden Räume sind mit IT-Technologie ausgestattet:

- **Klassenzimmer:** Vier Klassenzimmer sind mit IT-Ausstattung versehen. Zwei dieser Räume verfügen über interaktive Whiteboards und Schul-Laptops, die den Unterricht durch den Zugriff auf digitale Lernressourcen interaktiver gestalten. Diese Räume sind zentrale Knotenpunkte für digitale Bildung.
- **Bibliothek**: Die Bibliothek ist mit zwei stationären PCs ausgestattet, die für die Verwaltung des Bibliotheksmanagementsystems und die Nutzung durch Schüler und Lehrkräfte dienen.
- **Lehrerzimmer:** Ein PC steht dem Lehrpersonal für administrative Aufgaben, Unterrichtsvorbereitung und die Nutzung von Online-Ressourcen zur Verfügung.
- **Direktionszimmer:** Ein Verwaltungs-PC unterstützt die organisatorischen Aufgaben der Schulleitung, einschließlich der Verwaltung von Schülerdaten und der Kommunikation mit externen Partnern.
- **Flurbereich/Halle:** Dieser Bereich dient als gemeinschaftlich genutzter Raum.

Ein Nebengebäude im Hof des Kollegiums ist derzeit nicht in die IT-Infrastruktur eingebunden und wird daher nicht von der IT-Betreuung abgedeckt. Die räumliche Struktur ist darauf ausgelegt, eine optimale Nutzung der IT-Ressourcen zu ermöglichen, wobei die Klassenzimmer und die Bibliothek als zentrale Bereiche für digitale Bildung fungieren. Zukünftig könnte die Integration des Nebengebäudes in die IT-Infrastruktur in Betracht gezogen werden, um die Kapazitäten der Schule zu erweitern.

7.1.2 Hardwareausstattung

Die Hardware-Ausstattung der Schule wurde gezielt modernisiert, um den Anforderungen einer zeitgemäßen Bildungseinrichtung gerecht zu werden. Sie umfasst Server, Netzwerkkomponenten, Drucker, Peripheriegeräte, Rechner und mobile Geräte.

7.1.2.1 Server und Netzwerkinfrastruktur

Die Netzwerkinfrastruktur bildet das Rückgrat der IT-Landschaft und gewährleistet eine stabile Datenübertragung sowie eine sichere Datenverwaltung. Die zentralen Komponenten sind:

- **HPE ProLiant MicroServer Gen10 Plus:** Installiert im September 2020, dient dieser Server als zentrale Plattform für die Datenverwaltung und -speicherung. Mit einem Intel Xeon E-2224 Prozessor (3,4 GHz), 16 GB RAM und SATA-Speicher verwaltet er Schul- und Bibliotheksdaten und führt regelmäßige Backups durch. Die Backup-Strategie umfasst tägliche inkrementelle und wöchentliche vollständige Backups, um Datenverluste zu minimieren.

- **HP 1410-24G J9561A:** Dieser 24-Port Gigabit-Switch ermöglicht eine schnelle und zuverlässige Datenübertragung zwischen den IT-Systemen, aber unterstützt leider keine VLANs (Virtual Local Area Networks) zur Segmentierung des Netzwerks.
- **Linksys EA7500 Max-Stream AC1900:** Der WLAN-Router bietet drahtlosen Netzwerkzugriff für Schüler, Lehrkräfte und Besucher. Er fungiert als Internet-Gateway (Anbieter A1) und unterstützt die Nutzung mobiler Geräte wie Tablets, Smartphones und interaktiver Whiteboards. Ein unverschlüsseltes Gäste-WLAN stellt jedoch ein Sicherheitsrisiko dar.
- **Devolo Powerline-Adapter:** Diese Adapter nutzen Stromleitungen zur Netzwerkübertragung, und erweitern so die WLAN-Abdeckung in Bereichen mit schwachem Signal. An diesem Gerät häng ein Kyocera Farbdrucker, der sich im hinteren Eck der Bibliothek befindet.
- **Serverschrank:** Ein dedizierter Serverschrank mit Kühlung und Temperatur-überwachung schützt die Server-Hardware vor Überhitzung und sorgt für eine stabile Betriebsumgebung.

Die Netzwerkinfrastruktur ermöglicht eine nahtlose Integration von stationären und mobilen Geräten und unterstützt moderne Unterrichtsmethoden wie BYOD (Bring Your Own Device).

7.1.2.2 Drucker und Peripheriegeräte

Die Schule verfügt über eine Vielzahl von Druck- und Peripheriegeräten, die den täglichen Betrieb unterstützen:

- **Multifunktionsdrucker:** Vier netzwerkfähige Drucker (Kyocera 3550, Kyocera 5526, HP Envy 4500 Serie, Samsung 2020) ermöglichen Schwarzweiß- und Farbdrucke. Sie sind für alle im Schulnetzwerk angemeldeten Geräte zugänglich, einschließlich Schul-PCs, Laptops und BYOD-Geräten. Unterstützte Druckprotokolle umfassen:
    - **AirPrint:** Ermöglicht das Drucken von Apple-Geräten ohne zusätzliche Software, sofern sie sich im selben Netzwerk befinden.
    - **Mopria Print Service:** Bietet eine standardisierte Drucklösung für Android-Geräte, die das Drucken aus nahezu jeder App ohne spezielle Drucker-Apps ermöglicht.
- **Projektor (Acer):** Unterstützt Präsentationen und die Darstellung multimedialer Inhalte in Klassenzimmern oder im Flurbereich.

Die Druckfreigabe erfolgt derzeit auf mündliche Anfrage der Schüler beim Lehrer, ohne zentrale Kontrolle oder Nachverfolgung. Dies birgt das Risiko von Missbrauch und ineffizienter Ressourcennutzung. Ein zentrales Druckmanagementsystem, wie Paper-

Cut oder MyQ X, könnte eingeführt werden, um Druckkontingente zuzuweisen und die Nutzung zu überwachen.

7.1.3 Betreibsysteme und Software

Die Softwarelandschaft der Schule ist auf die Unterstützung von Unterricht und Verwaltung ausgelegt und umfasst Betriebssysteme sowie spezialisierte Anwendungen:

- **Betriebssysteme:**
  - **Server:** Windows Server 2016 bildet die Grundlage für die zentrale Datenverwaltung und Backup-Prozesse.
  - **PCs und Laptops:** Windows 10 Pro wird auf allen stationären und mobilen Geräten eingesetzt, um eine einheitliche Benutzererfahrung zu gewährleisten.
  - **Mobile Endgeräte:** Schüler und Lehrkräfte nutzen iOS- und Android-Geräte, die über das Schul-WLAN in das Netzwerk eingebunden sind und Druckaufträge senden können.
- **Spezialisierte Software/ Anwendungen:**
  - **Oracle Database:** Wird für das Bibliotheksmanagementsystem MOL NET von Firma VULCAN eingesetzt, um Bibliotheksdaten effizient zu verwalten.
  - **Microsoft Office Pakete:** Unterstützten administrative Aufgaben und die Erstellung von Unterrichtsmaterialien.
  - **Avast:** Diese Antivirenlösung schützt die Serverarchitektur, wobei die Lizenz im Februar 2025 ausläuft. Der Ablauf bietet die Gelegenheit, ein umfassendes Sicherheitskonzept zu entwickeln.
  - **E-Klassenbuch:** Webbasierte Anwendung, dass die Noten, Anwesenheitslisten und andere schulische Informationen der Schüler der Polnische Schule zentral speichert und verwaltet.

7.1.4 Geplante Erweiterungen der IT-Infrastruktur

Um die IT-Sicherheit, Netzwerkstabilität und Effizienz weiter zu verbessern, sind folgende Maßnahmen geplant:

- **Austausch des Linksys-Routers:** Der aktuelle Router soll durch einen Cisco 819G-4G-GA-K9 M2M ersetzt werden, um die Netzwerkstabilität und -geschwindigkeit zu erhöhen.
- **Fortigate - 60F:** Eine Firewall-Lösung zur Abwehr von Bedrohungen wie Malware oder unbefugten Zugriffen.
- **Cisco 3750V2 Switch:** Ein leistungsstärkerer Switch zur Verbesserung der Netzwerkleistung und Skalierbarkeit, der unterstützt VLANs (Virtual Local Area Networks) zur Segmentierung des Netzwerks.

- **Cisco Access Point MERAKI MR32:** Ein neuer Access Point zur Verbesserung der WLAN-Abdeckung und -leistung. Beinhalte auch die Möglichkeit der Netzwerk-segmentierung
- **USV 1000 VA:** Eine unterbrechungsfreie Stromversorgung für den Server, um Datenverluste bei Stromausfällen zu verhindern.
- **ESET PROTECT:** Eine Sicherheitssoftware zur Schwachstellenanalyse und Optimierung der IT-Sicherheit, die nach Ablauf der Avast-Lizenz implementiert werden könnte.

7.2 Vorhandene Sicherheitsmaßnahmen (IST-Zustand)

Die IT-Infrastruktur der Polnischen Schule Jan III Sobieski verfügt über grundlegende Sicherheitsmaßnahmen, die primär auf den Schutz der Serverarchitektur und die Aufrechterhaltung der Betriebsfähigkeit abzielen. Dieses Subkapitel beschreibt die aktuell eingesetzten Schutzmechanismen ohne deren Wirksamkeit zu bewerten und bietet zugleich eine deskriptive Übersicht über die bestehenden Maßnahmen, um den IST-Zustand der IT-Sicherheit zu dokumentieren:

1. **Antivirensoftware:** Die Schule nutzt Avast als zentrale Sicherheitssoftware für den HPE ProLiant MicroServer Gen 10 Plus. Diese Software wurde im September 2020 installiert und schützt die Serverarchitektur vor Malware, Viren und anderen Bedrohungen. Die Lizenz für Avast läuft Ende Februar 2025 aus. Eine Erweiterung auf Client-Systeme oder mobile Endgeräte ist derzeit nicht erfolgt.
2. **Backup-Strategie:** Auf dem Server werden regelmäßige Backups durchgeführt um die Datenverluste zu minimieren. Die Backup-Strategie umfasst die Erstellung eines täglichen vollständigen Backups und dient der Sicherung von Daten, die auf dem Server gespeichert sind. Diese Daten umfassen sowohl schulische als auch Bibliotheksinformationen. Zu diesem Zeitpunkt existieren jedoch keine dokumentierten Richtlinien, welche die Häufigkeit, die Speicherorte oder die Verfahren zur Wiederherstellung von Daten festlegen.
3. **Netzwerkzugang und WLAN:** Der Netzwerkzugang der Schule wird durch einen Linksys EA7500 Max-Stream Router bereitgestellt. Über diesen Router wird sowohl den Schülern als auch den Lehrkräften sowie den Gästen der Schule der Zugriff auf das Internet sowie auf das interne Schulnetzwerk ermöglicht. Gäste-WLAN ist unverschlüsselt und kann ohne Authentifizierung genutzt werden. Jedoch für das interne WLAN, das von den Lehrkräften und Schülern genutzt wird, ist ein Passwort erforderlich, allerdings werden hier keine weiteren Sicherheits-mechanismen wie WPA3-Verschlüsselung, MAC-Adressfilterung oder Netzwerksegmentierung eingesetzt. Somit besteht im vorliegenden Kontext ein erhöhtes Risiko unbefugter Zugriffe sowie einer unzureichenden Trennung zwischen internen und externen Endgeräten. Darüber hinaus bieten

die vorhandenen Hardwarekomponenten keine Funktionalitäten zur Netzwerkanalyse, zur Nutzerüberwachung oder zur gezielten Reduzierung des Datenverkehrs.

4. **Druckmanagement:** In der Schule werden derzeit vier netzwerkfähige Drucker eingesetzt (Kyocera 3550, Kyocera 5526, HP Envy sowie Samsung 2020), die über das Schulnetzwerk für sämtliche angemeldeten Geräte erreichbar sind. Dies umfasst auch private Endgeräte im Rahmen des Bring Your Own Device (BYOD)-Konzepts. Drückaufträge von Schüler erfordern eine mündliche Freigabe von Lehrer, jedoch gibt es keine technische Authentifizierung oder Nachverfolgung der Druckaktivtäten. Die eingesetzten Drucksysteme unterstützen moderne Protokolle wie AirPrint und Mopria Print, wodurch ein mobiles Drucken ohne zusätzliche Software ermöglicht wird – unter der Voraussetzung, dass das jeweilige Gerät mit dem Schul-WLAN verbunden ist. Auch hierbei wird keine zentrale Kontrolle der Druckvorgänge eingesetzt.
5. **Benutzerverwaltung und Zugriff:** Active Directory ist vorhanden und dient zur zentralen Benutzerverwaltung auf dem Windows Server 2016. Die Benutzerkonten für Lehrkräfte und Direktion als auch der Verwaltung werden darüber verwaltet. Jedoch ist die Nutzung des Active Directory bislang nicht umfassend auf mobile Geräte oder BYOD ausgeweitet worden. Auch ein klares Rollen und Rechtevergabe für unterschiedliche Benutzergruppen ist nur in Basis form vorhanden.
6. **Physische Sicherheitsmaßnahmen:** Der Server ist in einem Serverschrank untergebracht, der mit Kühlung und Temperaturüberwachung ausgerüstet ist um die Betriebsstabilität der Server zu gewährleisten. Es gibt keine Dokumentierte physische Zugriffskontrolle für Lehrerzimmer wo der Server sich befinden. Das Schulgebäude ist während Betriebes für Gäste, Schuler und Lehrer frei zugänglich und Bibliothek ist gelegentlich unbesetzt.
7. **Schulungen und Sensibilisierung:** Bis dato wurden keine systematischen Schulungen oder Sensibilisierungsmaßnahmen für Lehrkräfte oder Schüler im Bereich der IT-Sicherheit durchgeführt. Kenntnis im sicheren Umgang mit digitalen Medien und Bedrohungserkennung wie zum Beispiel Phishing sind unterschiedlich ausgeprägt und abhängig zum großenteil von individuellen Erfahrungen der Personal. Eine Sicherheitskultur im Umgang mit IT-Systemen ist bislang nicht in diese Bildungsinstitution verankert.

Diese kurze Erfassung zeigt, dass sich die vorhandenen Sicherheitsmaßnahmen auf ein Minimum bzw. auf eine Basisabsicherung der Server beschränken. Das vorhandene Active Directory stelle eine gute Grundlage dar, jedoch der potenzial von ihr wird nicht vollständig genutzt. Darüber hinaus die fehlende Netzwerksegmentierung und das Fehlen technischen Zugangskontrollen stellen erhebliche Schwachstellen dar. Derzeit fehlen sowohl strukturierte Prozesse als auch technische Kontrollmechanismen, um den Datenschutz, die Netzwerksicherheit und einen verantwortungsvollen Umgang

mit IT-Ressourcen effektiv zu gewährleisten. Diese Ausgangslage unterstreicht den dringenden Handlungsbedarf für die Entwicklung eines zukunftsorientierten IT-Sicherheitskonzepts. Aufgrund begrenzter Ressourcen können jedoch einige Aspekte, wie beispielsweise die Implementierung von Zugangskontrollen, im Rahmen dieser Studie nicht umfassend behandelt werden. Dennoch werden diese Punkte dokumentiert, um ihre Relevanz für zukünftige Maßnahmen zu betonen.

7.3 Analyse bisheriger Cyberangriffe

In diesem Kapitel soll eine eingehende Analyse der Sicherheitsvorfälle, die im Juni 2024 sowie in der dreiwöchigen Periode vom 7. Bis 27.April 2025 registriert wurden, durchgeführt werden. Dabei liegt der Fokus auf den Vorfällen, die vor der Umstellung der IT-Architektur in einer polnischen Schule stattfanden. Primär werden Malware-Infektionen, Viren, Trojaner und Phishing-Angriffe analysiert. Das Hauptziel besteht darin, Angriffsmuster zu identifizieren, die Effektivität der bestehenden Sicherheits-maßnahmen zu evaluieren und die dringende Notwendigkeit zu betonen, die IT-Sicherheitsvorkehrungen in schulisches Umfeld zu optimieren.

Die Resultate werden für beide analysierten Zeiträume separat dargestellt und beinhalten grafische Darstellungen der betroffenen Geräte, diverser Bedrohungstypen sowie Informationen zu den Bedrohungen, systematisiert nach ihrer Häufigkeit. Diese Analyse ist von großer Bedeutung, um Schwachstellen der IT-Systemen von Schulen zu identifizieren und zukunftsorientierte Sicherheitsstrategien zu entwickeln.

7.3.1 Übersicht der Vorfälle Juni 2024

Im Juni 2024 wurden insgesamt mehr als 60 Cybervorfälle registriert und dokumentiert. Diese Vorfälle betrafen sowohl Geräte von Verwaltung (Dyrekcja-PC01) als auch von Lehrern (Nauczyciel-LP01, Nauczyciel-LP02), Schülern (Uczen-PC01) und dem Bibliothekspersonal (Biblioteka-PC01). Die identifizierten Bedrohungen konnten verschiedenen Typen zugeordnet werden, darunter Spyware, Adware, Trojaner, Ransomware, Würmer, Phishing-Versuche und Netzwerkangriffe wie ARP-Spoofing. In zahlreichen Fällen waren die eingesetzten Schutzmechanismen nicht ausreichend wirksam, sodass die Angriffe nicht erfolgreich abgewehrt werden konnten.
Im Rahmen der Vorfallanalyse wurden die erfassten Ereignisse systematisch zu spezifischen Bedrohungstypen zugeordnet. Die daraus resultierende Verteilung verdeutlicht das Auftreten der jeweiligen Kategorien im Beobachtungszeitraum:

- **Netzwerk (ARP Spoofing):** Insgesamt wurden 32 Vorfälle dokumentiert, wobei der Großteil auf die Computer Biblioteka-PC01 (11 Fälle), Nauczyciel-LP01 (10 Fälle) und Dyrekcja-PC01 (6 Fälle) verteilt ist. Diese Vorfälle lassen auf einen Versuch schließen, den Netzwerkverkehr zu kompromittieren und sensible Daten zu erlangen.

- **Phishing:** Zu den registrierten Vorfällen zählen zehn Vorfälle, die die Nauczyciel-LP01, Nauczyciel-LP02, Dyrekcja-PC01, Biblioteka-PC01 und Uczen-PC01 betrafen. Die genannten Angriffe erfolgten mittels E-Mails, die von vertrauenswürdigen Unternehmen wie Amazon und Microsoft imitiert wurden.
- **Spyware:** Fünf Vorfälle sind gegen Dyrekcja-PC01 und Uczen-PC01 festgestellt worden. Die Bedrohungen, wie etwa Spyware: KeyloggerX-gen und DataStealer, waren darauf ausgerichtet, Benutzerinteraktionen oder Daten zu kompromittieren.
- **Adware:** Des Weiteren wurden vier Vorfälle dokumentiert, die Dyrekcja-PC01, Biblioteka-PC01 und Uczen-PC01 betroffen haben. Bedrohungen wie Adware: PopUpGen und Adware: BannerX hatten einen negativen Einfluss auf das Nutzererlebnis und führten zu einer erhöhten Wahrscheinlichkeit weiterer Infektionen.
- **Trojaner:** Vier Fälle, die primär Uczen-PC01 Computer betrafen (Trojan: BankerX-gen, Trojan: DropperX-gen) wurden dokumentiert. Diese Vorfälle weisen auf den Versuch zusätzliche bösartige Payloads zu installieren, hin.
- **Ransomware:** Es wurden vier Vorfälle dokumentiert, die Dyrekcja-PC01 und Nauczyciel-LP01 bedrohten. Bei diesen Vorfällen kam eine Ransomware zum Einsatz, die den Bezeichnungen "Ransom: Locky" und "Ransom: WannaCry" trugen. Diese Ransomware stellte ein erhebliches Risiko für die Datenintegrität dar.
- **Würmer:** In vier dokumentierten Vorfällen wurde der Fokus auf die Rechner Dyrekcja-PC01 und Uczen-PC01 gerichtet, die mit den Schadprogrammen "Worm: Conficker" und "Worm: Blaster" infiziert wurden. Diese waren darauf ausgelegt, sich im Netzwerk zu verbreiten.

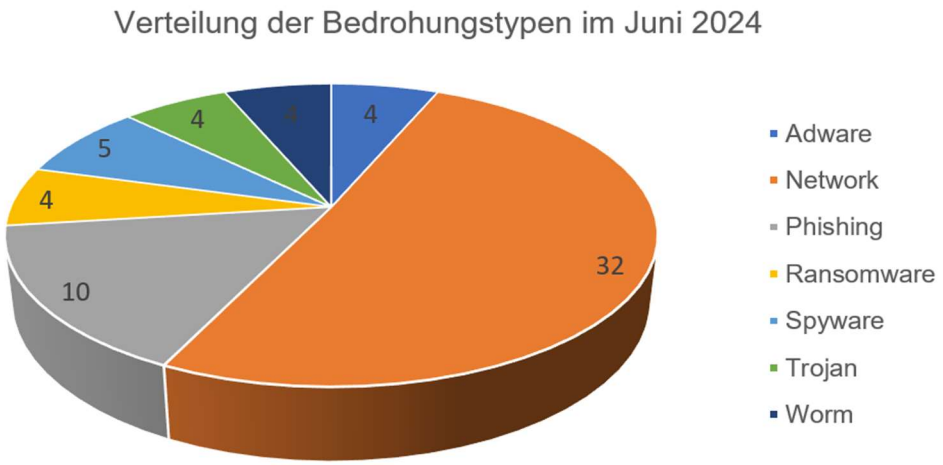

Abbildung 5 Verteilung der Bedrohungstypen im Juni 2024

7.3.1.1 Gerätbezogene Schwachstellen im Juni 2024

Am häufigsten wurde das Gerät Dyrekcja-PC01 von insgesamt 15 verschiedenen Vorfällen betroffen, darunter Ransomware, Spyware, Adware, Würmer, Phishing und ARP-Spoofing. Dies lässt die Vermutung zu, dass administrative Geräte, die sensible Daten enthalten, als hochprioritäre Ziele angesehen werden. Bei Biblioteka-PC01 wurden 12 Vorfälle verzeichnet, wobei der Schwerpunkt auf ARP-Spoofing lag.

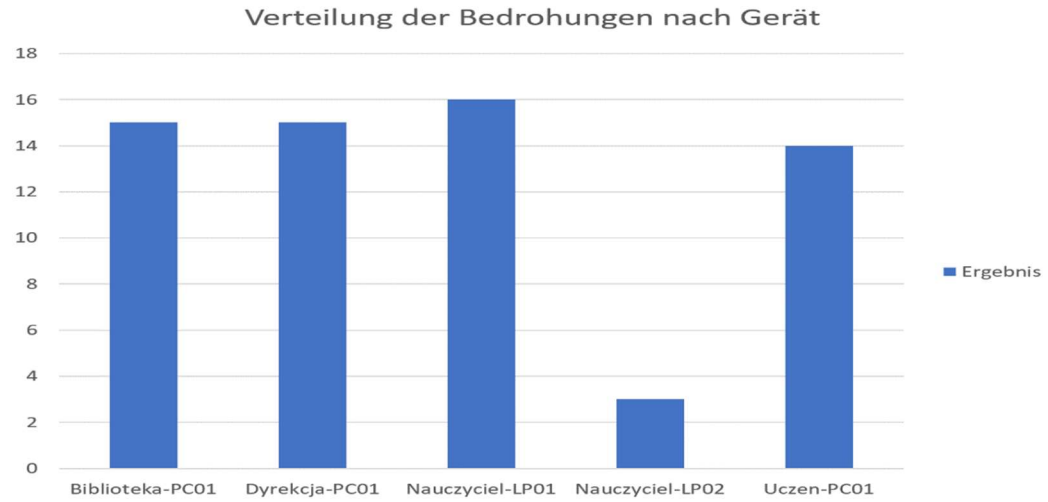

Abbildung 6 Gerätbezogene Bedrohungsverteilung

Dies lässt auf Schwachstellen im Netzwerk von gemeinsam genutzten Umgebungen schließen. Im Falle von Uczen-PC01 wurden insgesamt 11 Vorfälle registriert, die eine Mischung aus Trojanern, Spyware, Würmern, Adware, Phishing und ARP-Spoofing umfassten. Dies reflektiert die Anfälligkeit von Schülergeräten für schadhafte Downloads und Social Engineering. Auch die Lehrergeräte (Nauczyciel-LP01, Nauczyciel-LP02) waren von den Angriffen betroffen, insbesondere durch Phishing und ARP-Spoofing. Dies lässt auf eine unzureichende E-Mail-Filterung und einen unzureichenden Netzwerkschutz schließen.

7.3.1.2 Bedrohungshäufigkeit im Juni 2024

Nachfolgende Tabelle präsentiert eine Übersicht über die an den häufigsten dokumentierten Angriffen im Juni 2024.

Bedrohungen	Anzahl
Adware:BannerX [Adw]	1
Adware:ClickerX [Adw]	1
Adware:PopAdX [Adw]	1
Adware:PopUpGen [Adw]	1
ARP:Spoofing	32
Phishing:Amazon [Phish]	3

Phishing:BankAustria [Phish]	1
Phishing:Dropbox [Phish]	2
Phishing:Groupon [Phish]	1
Phishing:MicrosoftEmail [Phish]	3
Ransom:CryptoLock [Rns]	1
Ransom:Locky [Rns]	1
Ransom:Ryuk [Rns]	1
Ransom:WannaCry [Rns]	1
Spyware:DataStealer [Spy]	1
Spyware:KeyloggerX-gen [Spy]	1
Spyware:LoggerZ-gen [Spy]	1
Spyware:MonitorX-gen [Spy]	1
Spyware:TrackerZ-gen [Spy]	1
Trojan:AgentX-gen [Trj]	1
Trojan:BankerX-gen [Trj]	1
Trojan:DropperX-gen [Trj]	1
Trojan:StealerX-gen [Trj]	1
Worm:AutoRun [Wrm]	1
Worm:Blaster [Wrm]	1
Worm:Conficker [Wrm]	1
Worm:SpreadX [Wrm]	1

Tabelle 3 Häufigste Bedrohungen im Juni 2024

Der Inhalt der obigen Tabelle wird auch in Form eines Diagramms dargestellt, um die Informationen übersichtlicher zu präsentieren.

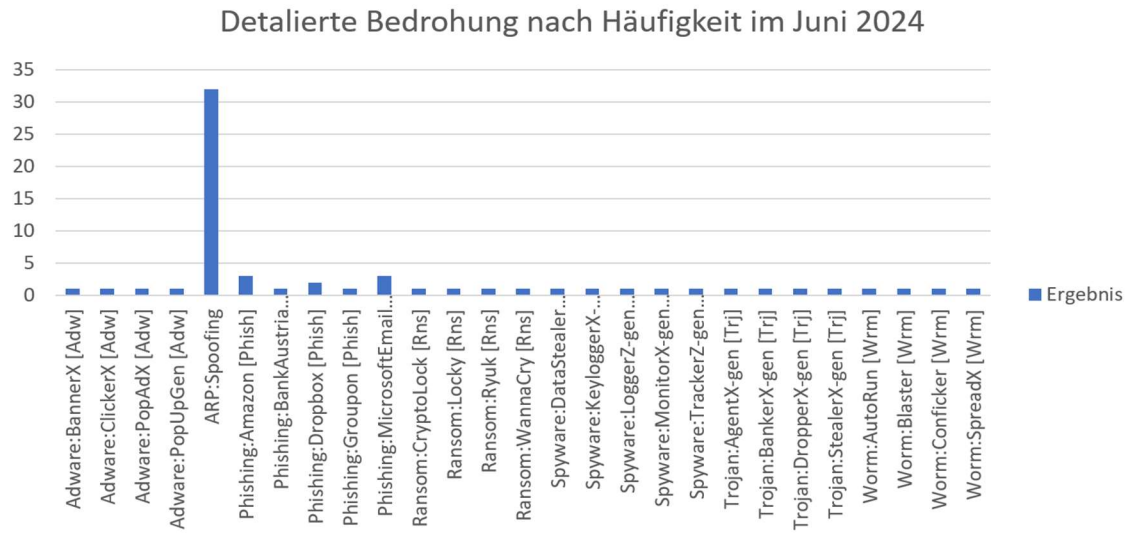

Abbildung 7 Genaue Bedrohungen und ihre Häufigkeit im Juni 2024

7.3.2 Übersicht der Vorfälle von 07.04. bis 27.04.2025

In der dreiwöchigen Beobachtungsperiode vom 07.04. bis 27.04.2025 wurden insgesamt 94 Vorfälle dokumentiert. Die betroffenen Geräte umfassten: Dyrekcja-PC01, Biblioteka-PC01, Uczen-PC01 sowie die Lehrergeräte Nauczyciel-LP01 und Nauczyciel-LP02, aber auch Server PLS-AUT. Die identifizierten Bedrohungen konnten in die Kategorien Adware, Phishing, netzwerkbasiertes ARP-Spoofing und Malware klassifiziert werden. Basierend auf den zuvor identifizierten Bedrohungskategorien können die beobachteten Vorfälle wie folgt dargestellt werden:

- **Adware:** Insgesamt wurden 21 Vorfälle dokumentiert, wobei der Anteil der registrierten AdwareTypen wie: PopUpGen, BannerX, ClickerX und PopAdX größer war. Die Geräte Dyrekcja-PC01 und Biblioteka-PC01 waren mit neun bzw. sieben Vorfällen besonders stark betroffen. Diese Adware tarnten sich in der Regel als Software-Installer, die zwar nach außen hin legitim erscheinen, jedoch in Wirklichkeit schädliche Software enthielten.
- **Phishing:** Aus der dokumentierten Gesamtheit der Fälle wurden 22 Phishing-Vorfälle identifiziert, die alle Geräte betrafen. Die vorliegende Untersuchung befasst sich mit einer spezifischen Form der Cyber-Angriffe, die sich durch die Nachahmung von E-Mails bekannter Unternehmen wie UPS, T-Mobile und DHL auszeichnet. Diesbezüglich besonders betroffen waren Dyrekcja-PC01 und Biblioteka-PC01 mit jeweils 6 Vorfällen, was auf eine Verbreitung von Social-Engineering-Versuchen hindeutet.
- **Netzwerk (ARP-Spoofing):** In dem untersuchten Zeitraum wurden insgesamt 26 Vorfälle registriert, wobei der Großteil der Vorfälle, nämlich 12 Vorfälle, auf den Server PLS-AUT entfiel. Dies lässt auf gezielte Angriffe auf die Server-infrastruktur schließen.
- **Malware:** Insgesamt kam es zu 4 Vorfällen, die alle die Malware-Kategorie PDF:MalwareX-gen [Drp] betrafen. Die betroffenen Geräte waren Nauczyciel-LP01, Biblioteka-PC01, Dyrekcja-PC01 und Nauczyciel-LP02, wobei die Malware in PDF-Dateien mit pädagogischen Titeln eingebettet waren.

Unterhalb dieser Analyse befindet sich eine Grafik, die die Verteilung der Gefahren für den Zeitraum vom 07. Bis 27. April 2025 zeigt.

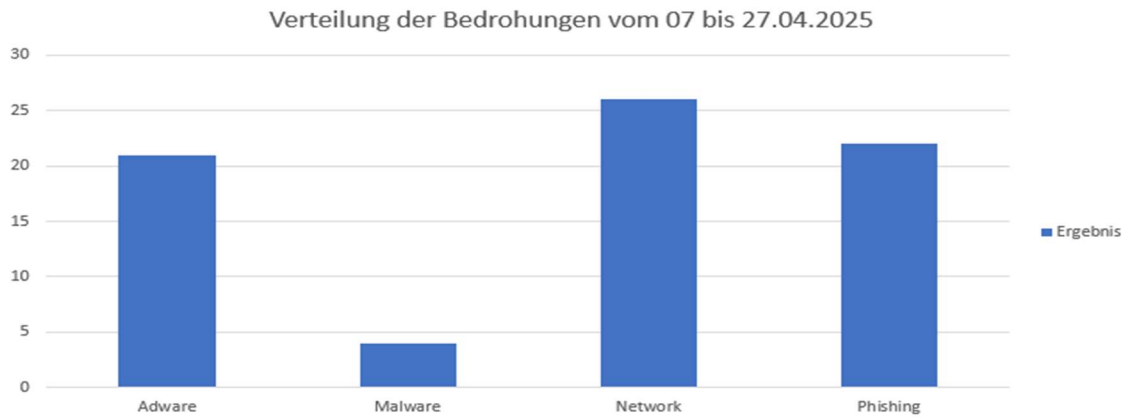

Abbildung 8 Verteilung der Bedrohungen vom 07.04. bis 27.04.2025

7.3.2.1 Gerätbezogene Schwachstellen in dem Zeitraum 07. bis 27.04.2025

Aus den vorliegenden Daten geht hervor, dass die Dyrektion-PC01 insgesamt 17 Vorfälle verzeichnete, darunter Adware, Phishing, Network und Malware. Dies unterstreicht, dass der Dyrektion-PC01 als primäres Ziel der Angriffe angesehen wird. Die Uczen-PC01 wurde Opfer von 9 Vorfällen, die eine Mischung aus Adware und Phishing umfassten. Dies verweist auf anhaltende Schwachstellen in gemeinsam genutzten Geräten. Der Server PLS-AUT war von 13 Vorfällen des ARP-Spoofing betroffen, was auf Versuche hindeutet, die Sicherheit kritischer Infrastrukturen zu gefährden. Biblioteka-PC01 verzeichnete 12 und Nauczyciel-LP01 – 13 Vorfälle, die hauptsächlich Adware, Malware, Network und Phishing betrafen, während Nauczyciel-LP02 – 8 Vorfälle registrierte, darunter Adware, Network und Malware. Die wiederholte Beobachtung von PDF basierter Malware deutet darauf hin, dass Cyber-kriminelle das Vertrauen in pädagogische Materialien gezielt ausnutzen.

Im Anschluss daran ist eine Grafik zusehen, die die gerätespezifische Verteilung der Bedrohungen vom 07. Bis 27. April 2025 anschaulich darstellt.

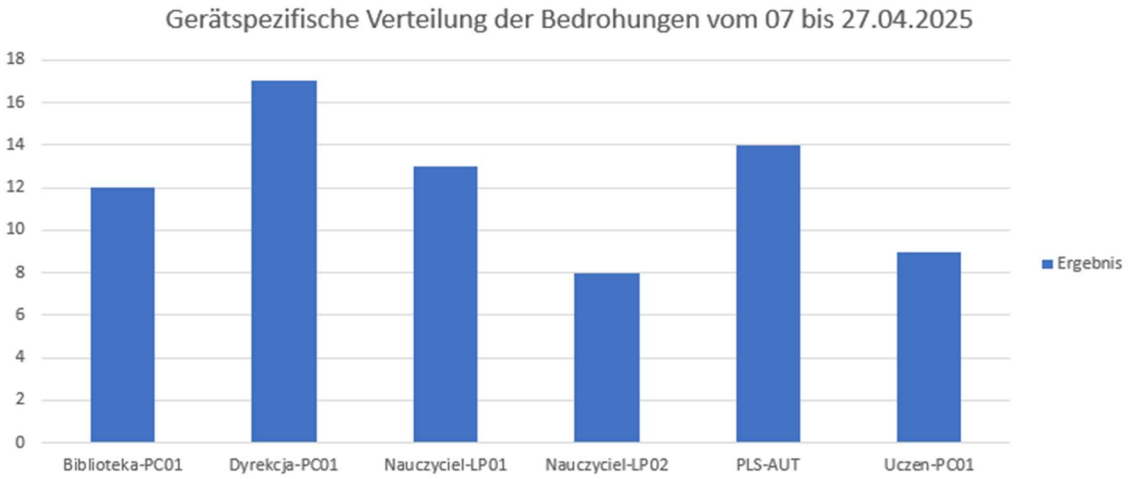

Abbildung 9 Gerätbezogene Bedrohungsverteilung im April 2025

7.3.2.2 Häufigkeit der Bedrohungen 07.04. bis 27.04.2025

Im Rahmen der vorliegenden Evaluierung wird ein umfassender Überblick über die häufigsten Bedrohungen für den Zeitraum 07. Bis 27. April 2025 präsentiert. Die folgende Tabelle 4 gibt einen detaillierten Übersicht über die identifizierten Bedrohungen, während Abbildung 9 eine visuelle Darstellung der Verteilung der häufigsten Bedrohungen auf die einzelnen Geräten bereitstellt.

Bedohungsdetails	Anzahl
Adware:BannerX [Adw]	7
Adware:ClickerX [Adw]	5
Adware:PopAdX [Adw]	4
Adware:PopUpGen [Adw]	5
ARP:Spoofing	26
PDF:MalwareX-gen [Drp]	4
Phishing:Amazon [Phish]	1
Phishing:Email [Phish]	17
Phishing: Survey [Phish]	4

Tabelle 4 Häufigste Bedrohungen vom 07.04. bis 27.04.2025

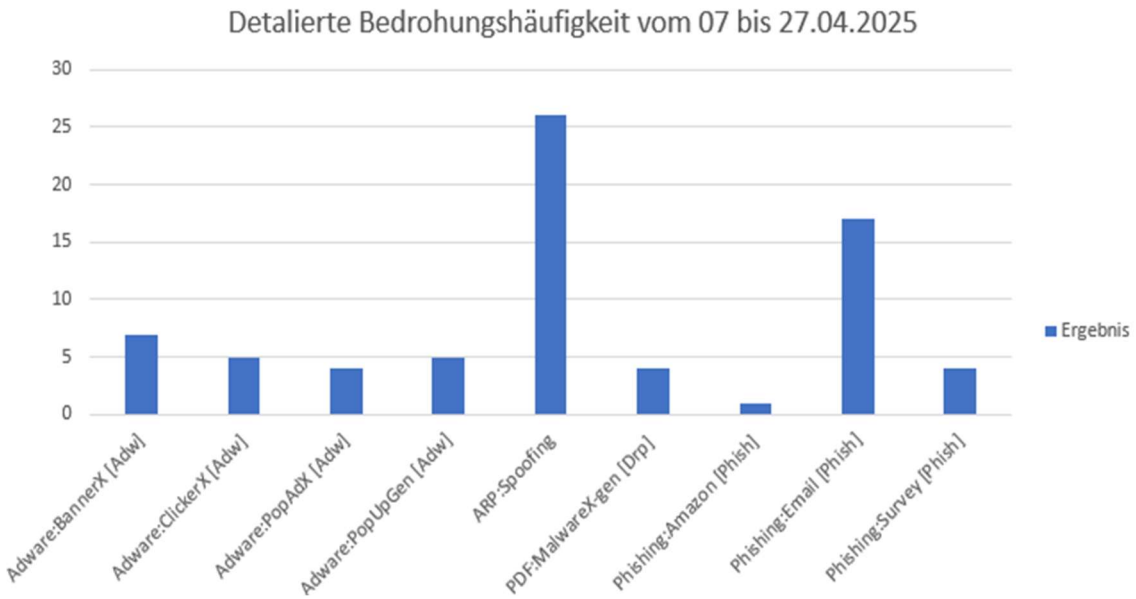

Abbildung 10 Bedrohungen und ihre Häufigkeit vom 07.04. bis 27.04.2025

7.3.2.3 Erkannte Angriffsmuster und Sicherheitslücken

Die durchgeführte Untersuchung hat zahlreiche wiederkehrende Angriffsmuster sowie Schwachstellen gezeigt. Die wichtigsten Erkenntnisse lassen sich wie folgt zusammenfassen:

- **Social Engineering durch Phishing:** In beiden Beobachtungszeiträumen war eine hohe Anzahl an Phishing-Angriffen zu verzeichnen. Insbesondere E-Mails, welche den Anschein erweckten, von vertrauenswürdigen Marken wie Amazon, Microsoft, BLIK, T-Mobile oder UPS zu stammen, wurden in diesem Zusammenhang besonders häufig genutzt. Ein konkretes Beispiel ist in Abbildung 11 dargestellt: Die Abbildung zeigt eine Phishing-Mail, die als Werbebotschaft für die "Urodzinowa Blikomania" (10 Jahre BLIK) getarnt ist. Dies beinhaltet eine Aufforderung zur Registrierung und das Versprechen hoher Geldgewinne. Das E-Mail wurde am 15. April 2025 an E-Mail-Adresse der Schule versendet und beinhaltete bekannte Designelemente und Logos, um Glaubwürdigkeit vorzutäuschen.

Abbildung 11 Phishing-Mail an die Polnische Schule Jan III Sobieski in Form einer BLIK-Werbung

Dies zeigt deutlich, dass Benutzerfehler eine wichtige Rolle spielen, da anscheinend E-Mail-Filterung die Gefahren bösartiger E-Mails nicht komplett beseitigen kann.

- **Bösartige Software Downloads:** In der Schul-PCs tarnten sich Adware und Trojaner häufig als legitime Software wie PDFConverterProX.msi.

Besonders auffällig ist, dass bei Insgesamt von 136 Vorfällen (Juni 2024 und April 2025) 92 also ca. 67,65 % in beiden Zeiträumen nicht abgewehrt wurden, was eindeutig auf

unzureichende Sicherheitsmaßnahmen hinweist. Auch die Vorfälle vom April 2025 sind ein Hinweis darauf, dass vorhandene Sicherheitstools wie Antivirensoftware oder Firewall keinen ausreichenden Schutz bieten oder standardgemäß nicht robust genug eingerichtet sind. Das wiederholte Auftreten von Bedrohungen wie Adware: PopUpGen und Phishing: E-Mail auf verschiedenen Geräten und über verschiedene Zeiträume lässt darauf schließen, dass proaktive Abwehrmaßnahmen nicht ausgeführt wurden. Darüber hinaus weist das Fehlen von Netzwerk-basierten Schutzmaßnahmen gegen ARP-Spoofing auf weitere Schwachstellen in Intrusion Detection und Prevention Systemen hin.

7.4 Identifikation von Schwachstelle und Risiken (Grobe IST-Bewertung)

Die vorliegende Grobanalyse der bestehenden IT-Infrastruktur der Polnischen Schule Jan III Sobieski offenbart Schwachstellen, welche einer zeitnahen Bearbeitung, um die digitale Robustheit der Einrichtung gezielt zu stärken, erzwingen. Als Grundlage dieser Bewertung dienen die in den vorangegangenen Abschnitten des siebten Kapitels dokumentierten technischen Komponenten sowie organisatorischen Faktoren. Die in Tabelle 5 zusammengefassten Schwachstellen werden in der weiteren Folge einer Schadenspotenzialanalyse unterzogen.

Schwachstellen	Beschreibung	Risiko
offen Gäste-WLAN	unautorisierte Zugriff auf das Schulnetz	Angriffe auf Geräte, Datenlecks
fehlende Drucker Authentifizierung	Unkontrollierte Zugriff auf Drucker und kein Drucknachweis	Ressourcen Verschwendung bzw. Schwund
unkontrollierte BYOD	Schülergeräte werden ohne Sicherheitsüberprüfung ins Netzwerk integriert	Malware-Infektionen
Fehlende physische Zutrittskontrollen	Räume wie Bibliothek oder Lehrerzimmer sind frei zugänglich	Manipulation, Datendiebstall möglich
Veraltete Software/ Patchmanagement	Einige Geräte die sich länger außer Netzwerk befinden Nauczycile-LP01 und LP02 nutzen Software ohne regelmäßige Updates	Exploit-Risiko
Fehlende User Sensibilisierungsmaßnahmen	höhere Anfälligkeit gegen Phishing und Malware	Social Engineering, Ransomware, Trojaner
keine Netzwerksegmentierung	alle Gräte befinden sich an einem und gleichen Segment	Schneller Ausbreitung von Angriffen und Infektionen
Fehlende Richtlinien für Datenwiederherstellung	Es gibt Backups aber keine definierter Recovery-Prozess	Längere Ausfallzeiten bzw. Datenverluste

Tabelle 5 Identifizierter Schwachstellen

Zur übersichtlichen Darstellung der Schwachstellen (Tabelle 6) wird eine Bewertung eines Schadenspotenzial auf einer Skala von hoch, mittel und Kritisch erstellt.

Schwachstellen	Schadenspotenzial
offen Gäste-WLAN	Hoch
fehlende Drucker Authentifizierung	Mittel
unkontrollierte BYOD	Mittel
Fehlende physische Zutrittskontrollen	Hoch
Veraltete Software/ Patchmanagement	Hoch
Fehlende User Sensibilisierungsmaßnahmen	Hoch
keine Netzwerksegmentierung	Hoch
Fehlende Richtlinien für Datenwiederherstellung	Hoch

Tabelle 6 Darstellung der Schwachstellen

Diese grobe IST-Bewertung zeigt, dass die IT-Infrastruktur der Polnischen Schule des Jan III Sobieski einige Schwachstellen aufweist, die sowohl die Sicherheit als auch die Stabilität der Systeme gefährden. Besonders kritisch sind:

- das unverschlüsselte Gäste-WLAN
- fehlende Zugangskontrollen,
- ungeregelte BYOD Nutzung,
- veraltete Software und mangelndes Awareness der Benutzer.

Alle diese Faktoren erhöhen die Vulnerabilität gegen Cyberangriffen, wie die Vorfälle im Juni 2024 und April 2025 bewiesen haben. Zu den möglichen Risiken in diesem Zusammenhang zählen Datenverluste, unbefugte Zugriffe, Netzwerkausfälle, Imageschäden sowie hohe Kosten. Die in diesem Kapitel dargelegte Evaluierung sollte ein Fundament für die anschließende Risikoanalyse (vgl. Kapitel 8), die auf der OCTAVE-S Methode basiert, bilden.

8. Anwendung der Octave-Methode

Polnische Schule des Jan III Sobieski an der Botschaft der Republik Polen in Wien ist seit 1977 eine Bildungsinstitution des polnischen Auslandsschulwesens. Sie bietet Unterricht in polnischer Sprache, Geschichte und Geographie sowie Vorschulerziehung für die Klassen I bis III an. Die Schule wird vom polnischen Bildungsministerium verwaltet und vom Zentrum für die Entwicklung des Auslandsschulwesens (ORPEG) beaufsichtigt und finanziell unterstützt. Der Unterricht findet einmal wöchentlich von Dienstag bis Samstag statt. Trotz begrenzter Ressourcen spielt die Informationstechnologie sowohl im Unterricht als auch in der Verwaltung eine zentrale Rolle. Diese organisatorischen Rahmenbedingungen der Schule wirken sich direkt auf die Verfügbarkeit von Ressourcen, Personal und IT-Unterstützung aus und sollten beider Sicherheitsanalyse unbedingt berücksichtigt werden.

8.1 Phase 1: Organisatorische Sicht

Die Umsetzung der OCTAVE-S - Methode in der ersten Phase dient der systematischen Identifizierung und Bewertung von Assets, Sicherheitspraktiken und Bedrohungen. Diese Phase bildet auch die Grundlage für die nachfolgende Phase 2, die sich mit Technischen Sicht befasst, sowie für die Phase 3, die Strategie und Plänen gewidmet ist. Die praktische Durchführung erfolgte in polnischer Sprache unter Verwendung von Materialien aus dem offiziellen OCTAVE-S-Dokument.

8.1.1 Durchführungszeitplan für die Phase 1

Um die Transparenz der Analysen in Phase 1 sicherzustellen, bedarf es eines Zeitplans, der die wesentlichen Schritte und deren zeitliche Abfolge (Tabelle 7) übersichtlich darstellt.

Aktivität	Datum	Verantwortliche
Analyse IT-Landschaft	01.06.2024	IT - Verantwortlicher (D. Zarosa)
Vorfallanalyse Juni 2024	30.06.2024	IT - Verantwortlicher (D. Zarosa)
Gespräch 1: Identifizierung der organisatorischen Assets	14.03.2025	IT - Verantwortlicher (D. Zarosa), Bibliothekar (I. Szliter), Direktion (H. Kaczmarczyk)
Gespräch 2: Bewertung bestehenden Sicherheitsmaßnahmen	15.03.2025	IT - Verantwortlicher (D. Zarosa), Bibliothekar (I. Szliter), Direktion (H. Kaczmarczyk)
Vorfallanalyse April 2025	27.04.2025	IT - Verantwortlicher (D. Zarosa)
Gespräch 3: Festlegung von Sicherheitsanforderungen	29.04.2025	IT - Verantwortlicher (D. Zarosa), Lehrervertreter (I. Szliter), Direktion (H. Kaczmarczyk)

Tabelle 7 Durchführungszeitplan der OCTAVE-S Phase 1

8.1.2 Definition der Bewertungskriterien

Im Anschluss an den Zeitplan für Phase 1 werden Kriterien für die Bewertung der Auswirkungen potenzieller Sicherheitsvorfälle oder Risiken vorgestellt, die eine Einschätzung der Auswirkungen potenzieller Sicherheitsvorfälle auf die Schule ermöglichen. Diese Kriterien bilden die Basis für die darauffolgende Risikoanalyse und die Priorisierung der Bedrohungen. Um die potenziellen Auswirkungen von Sicherheitsvorfällen zu bewerten, wurden die Kriterien basierend auf dem OCTAVE-S "Impact Evaluation Criteria Worksheet" ausgearbeitet und in der Tabelle zusammengefasst (Alberts, et al. 2025).

Kriterium	Kritisch	Mittel	Gering
Datenschutz	Verlust sensibler Daten sowohl von Schüler als auch Lehrer oder Verwaltungspersonal	Zugriff auf interne, aber nicht sensible Daten	Zugriff auf öffentliche zugängliche Daten
Unterrichtsausfall	Unterrichtausfall über mehrere Wochen	Ausfall einzelner Tage oder Unterrichtsmodule	kurzzeitige Unterbrechung
Image-Schaden	Medienberichte, diplomatische Folgen	interne Unzufriedenheit, Beschwerden	Einzelfälle
Kosten	über 2000 € (Wiederherstellung, Ausfälle)	von 500€ - 2000€	unter 500€

Tabelle 8 Kriterien für die Bewertung der Auswirkungen potenzieller Sicherheitsvorfälle oder Risiken. (Alberts, et al. 2025)

8.1.3 Bewertung bestehenden Sicherheitsmaßnahmen

Im Folgenden werden die bestehenden Sicherheitsmaßnahmen untersucht und mögliche Lücken aufgezeigt. Die Evaluation der IT-Sicherheitsbereiche erfolgt auf Basis des "Security Practices Worksheet" der OCTAVE-S Methode und umfasst die Verwendung eines Ampelsystems – die darunter aufgeklärt und in der Tabelle 9 abgebildet wird – zur Darstellung des Sicherheitsstatus, der dadurch transparent und nach vollziehbar wird (Alberts, et al. 2025):

- **Rot** signalisiert kritische Schwachstellen, bei denen dringender Handlungsbedarf hinsichtlich unzureichender oder fehlender Maßnahmen besteht.
- **Gelb** hingegen weist daraufhin, dass teilweise Maßnahmen vorhanden sind, die jedoch verbessert oder ergänzt werde müssen
- **Grün** wird verwendet, um anzuzeigen, dass starke und effektive Sicherheitsvorkehrungen implementiert wurden, welche den geltenden Standards entsprechen.

Bereich	IT-Beschreibung	Bewertung
Antivirenschutz	Litzen läuft im Februar 2025 ab.	
Backup	Täglich jedoch kein dokumentierter Wiederherstellungsprozess	
LAN/WLAN-Sicherheit	Gäste-WLAN offen, keine VLANs, keine Protokolle	
Zugriffkontrollen	Keine MFA	
Schulung & Awareness	keine IT-Schulungen	
Netzwerk	keine Segmentierung, keine Intrusion Detection	
Druckmanagement	keine technische Freigabe oder Login	

Tabelle 9 Bewertung der IT-Sicherheitsmaßnahmen nach Ampelsystem

8.1.4 Identifizierung der organisatorischen Assets

Nach Festlegung der Bewertungskriterien werden im vorliegenden Teil die wichtigen organisatorischen Ressourcen der Schule ermittelt. Diese Ressourcen stellen die Basis für die weiterführende Analyse im Rahmen der OCTAVE-S Methode dar. Im Rahmen eines organisierten Gesprächs, in dem das "Asset Identification Worksheet" (Alberts, et al. 2025) als Hilfsmittel diente, konnten die folgenden organisatorischen Ressourcen identifiziert werden:

Asset ID	Kategorie	Beschreibung	Verantwortlich
A01	Bildung	Lehrbetrieb, Schülereinteilung	Direktion (H.Kaczmarczyk)
A02	Verwaltung	Schülerakten, Zeugnisse, Kommunikation mit ORPEG	Direktion (H. Kaczmarczyk)
A03	Bibliothek	Physische und digitale Ressourcen (Bücher, Datenbank), Bibliotheks-PCs, Recherche	Bibliothekarin (I. Szliter), Direktion (H. Kaczmarczyk)
A04	IT-Infrastruktur	Server, WLAN, Drucker, Netzwerk, BYOD, Whiteboard, usw.	IT- Verantwortlicher (D. Zarosa)
A05	Räumliche Infrastruktur	Schulgebäude, physische Zugang	Direktion (H. Kaczmarczyk)
A06	Personalressourcen	informelle Prozesse	Direktion (H. Kaczmarczyk)
A07	Kommunikation	E-Mail, Digitale Klassenbuch, Plattformen	Lehrervertreter (I. Szliter), Direktion (H. Kaczmarczyk)

Tabelle 10 Übersicht der organisatorischen Schlüsselressourcen der Schule. (Alberts, et al. 2025)

8.1.5 Auswahl kritischer Assets

Aufbauend auf den Erkenntnissen aus Überschicht der organisatorischen Schlüsselressourcen in Abschnitt 8.1.4 fokussiert sich im Rahmen der ersten Phase der OCTAVE-S Methode dieser Abschnitt auf die Identifikation der kritischen Assets der Schule. Diese Assets sind von hoher Relevanz für den Schulbetrieb und ihr Schutz ist von zentraler Bedeutung, um die zuvor identifizierten Schwachstellen zu adressieren. Die kritischen Vermögenswerte wurden in einer strukturierten Gesprächsrunde mit der Schulleitung, dem IT-Personal und dem Bibliothekspersonal unter Verwendung der Informationen aus Kapitel 7 und des "Critical Asset Indentification Worksheet" ermittelt und in darauf folgenden Tabellen dargestellt (Alberts, et al. 2025).

Step 6	**Step 7**
Critical Asset	**Rationale for Selection**
What is the critical System	**Why is this system critical to the organization**
Schülerdaten	Zentrale personenbezogene Daten notwendig für Verwaltung, Zeugniserstellung und rechtliche Verpflichtungen.
Step 8	
Description	
Who Users the system	**Who is responsible for the system**
Schulleitung, Lehrkräfte, Bibliothekpersonal	IT-Verantwortlicher
Step 9	
Related Assets	
Which assets are related to this system?	
Information	**Services and Application**
Name, Geburtsdatum, Noten, Kontakte, Gesundheitsinformationen, Adressdaten, Schulhistorie	Server, Dyrekcja-PC01, Benutzerkonten, Internet, Papierarchive
Other	
Authentifizierung und Datenablage Software	
Step 10	**Step 11**
Security Requirements	**Most Important security requirements**
What are the security requirements for this system	**Which security requirement is most important for this system**
Vertraulichkeit (Confidentiality): Schülerdaten enthalten sensible personenbezogene Informationen. Zugriff darf ausschließlich berechtigten Verwaltungs- und Lehrkräften über gesicherte Benutzerkonten gewährt werden. Integrität (Integrity): Noten, Stammdaten und	Vertraulichkeit (Confidentiality)

Kontaktinformationen müssen korrekt gespeichert werden, da sie rechtlich und pädagogisch relevant sind. Verfügbarkeit (Availability): Die Daten müssen während der Schulzeiten durchgängig zugänglich sein, insbesondere für Direktion und Klassenleitung.	

Tabelle 11 Kritisches Asset "Schülerdaten" – Analyse gemäß OCTAVE-S (Schritte 6 – 11). (Alberts, et al. 2025)

Step 6	**Step 7**
Critical Asset	**Rationale for Selection**
What is the critical System	**Why is this system critical to the organization**
Bibliothekdatenbank	Die Verwaltung der Ausleihe und Rückgabe, Medienrecherche sowie Mahnungen erfolgt digital über die Bibliothekdatenbank.
Step 8	
Description	
Who Users the system	**Who is responsible for the system**
Bibliothekspersonal, Schüler:innen, Lehrkräfte, andere mit der Schule nicht verbunden Erwachsene	Bibliothekarin und IT-Verantwortlicher, FA. VULCAN
Step 9	
Related Assets	
Which assets are related to this system?	
Information	**Services and Application**
Ausleihhistorie, Medienverzeichnis, Persönliche Informationen wie, Kontakt Daten, Adresse, Telefonnummer usw.	Server, Bibliotek-PC01, Internet
Other	
Bibliotheken Software (VULCAN)	
Step 10	**Step 11**
Security Requirements	**Most Important security requirements**
What are the security requirements for this system	**Which security requirement is most important for this system**
Vertraulichkeit: Schüler ausleihen und Mahndaten dürfen nur von autorisiertem Bibliothekspersonal eingesehen werden. Integrität: Falsche oder doppelte Ausleihbuchungen würden das System	Integrität (Integrity)

unbrauchbar machen und die Schüler benachteiligen. Verfügbarkeit: Die Daten müssen während der Schulzeiten durchgängig zugänglich sein, insbesondere für Bibliothekarin, Lehrer und Schüller	

Tabelle 12 Kritisches Asset "Bibliothekdatenbank" – Analyse gemäß OCTAVE-S (Schritte 6 – 11). (Alberts, et al. 2025)

Step 6	**Step 7**
Critical Asset	**Rationale for Selection**
What is the critical System	**Why is this system critical to the organization**
Lehrmaterialien	Basis für die Unterrichtsplanung, Hausarbeiten und digitale Lernmöglichkeiten.
Step 8	
Description	
Who Users the system	**Who is responsible for the system**
Lehrkräfte, Schüler	Lehrkräfte und IT-Verantwortlicher
Step 9	
Related Assets	
Which assets are related to this system?	
Information	**Services and Application**
Unterrichtsinhalte, Dateien, Übungen, Lehrkonzepte, Prüfungen	Cloud-Dienste (One Drive, Dropbox), Dateiablage
Other	
Sharing-Ordner, Nauczyciel-LP01, Nauczyciel-LP02, Bibliotek-PC01, Dyrekcja-PC01, WLAN, Whiteboard	
Step 10	**Step 11**
Security Requirements	**Most Important security requirements**
What are the security requirements for this system	**Which security requirement is most important for this system**
Vertraulichkeit: Interne Materialien wie Prüfungen oder unveröffentlichte Konzepte dürfen nicht von Schüler eingesehen werden.	Verfügbarkeit (Availability)

Integrität: Dateien dürfen nicht manipuliert oder versehentlich überschrieben werden – insbesondere bei Prüfungen und offiziellen Unterlagen. Verfügbarkeit: Lehrpersonal sollte jederzeit Zugang zu Unterrichtsmaterialien haben – sowohl online als auch auf ihren Geräten–besonders vor und während der Lehrveranstaltungen.	

Tabelle 13 Kritisches Asset "Lehrmaterialien" – Analyse gemäß OCTAVE-S (Schritte 6 – 11). (Alberts, et al. 2025)

Step 6	**Step 7**
Critical Asset	**Rationale for Selection**
What is the critical System	**Why is this system critical to the organization**
E-Mail-Kommunikation	Die Kommunikation zwischen Lehrkräften, Direktion, Eltern und externen Stellen erfolgt überwiegend über E-Mail.
Step 8	
Description	
Who Users the system	**Who is responsible for the system**
Lehrkräfte, Direktion, Bibliothekarin IT.	IT-Verantwortliche bzw. externer Provider (z. B. Microsoft, Gmail oder ORPEG).
Step 9	
Related Assets	
Which assets are related to this system?	
Information	**Services and Application**
Dienstliche Nachrichten, Bestellungen und damit verbunden Finanzinformationen, Schülerbezogen Informationen, Anmeldeinformationen	E-Mail-Dienst (Outlook, Gmail)
Other	
Dyrekcja-PC01, Bibliotek-PC01, Nauczyciel-LP01, Nauczyciel-LP02)	
Step 10	**Step 11**
Security Requirements	**Most Important security requirements**
What are the security requirements for this system	**Which security requirement is most important for this system**
Vertraulichkeit: Kommunikation kann sensible Daten enthalten – Verschlüsselung und Zugangsschutz sind nötig.	Vertraulichkeit (Confidentiality)

Integrität: Nachrichten dürfen nicht manipuliert werden. Verfügbarkeit: Zugang zur Mailkommunikation ist während Schulzeiten zwingend erforderlich.	

Tabelle 14 Kritisches Asset "E-Mail-Kommunikation" – Analyse gemäß OCTAVE-S (Schritte 6 - 11). (Alberts, et al. 2025)

Step 6	**Step 7**
Critical Asset	**Rationale for Selection**
What is the critical System	**Why is this system critical to the organization**
Shared-Ordner	Gemeinsame Ablage von Unterrichts- und Verwaltungs- uns Schülerdokumenten sowie Bibliotheksbestandes.
Step 8	
Description	
Who Users the system	**Who is responsible for the system**
Lehrkräfte, Bibliothekarin, Direktion	IT-Verantwortlicher
Step 9	
Related Assets	
Which assets are related to this system?	
Information	**Services and Application**
Lehrmaterialien, Formulare, Schülerdokumenten sowie Bibliotheksbestandes	Netzlaufwerke
Other	
Server, Benutzerkonten	
Step 10	**Step 11**
Security Requirements	**Most Important security requirements**
What are the security requirements for this system	**Which security requirement is most important for this system**
Vertraulichkeit: Gemeinsame Ordner dürfen nur für die vorgesehenen Benutzergruppen wie Lehrer, oder Direktion zugänglich sein. Die Zugriffsrechte sind regelmäßig zu überprüfen.	Vertraulichkeit (Confidentiality)

Integrität: Unbefugte Änderungen oder das versehentliche Löschen wichtiger Dateien sollten durch den Einsatz von Versionskontrollsystemen oder Backup verhindert werden. Verfügbarkeit: Die Dateien sollten jederzeit zugänglich sein, sowohl lokal als auch über Schulnetzwerk.	

Tabelle 15 Kritisches Asset "Sharde-Ordner" – Analyse gemäß OCTAVE-S (Schritte 6 - 11). (Alberts, et al. 2025)

Step 6	**Step 7**
Critical Asset	**Rationale for Selection**
What is the critical System	**Why is this system critical to the organization**
Benutzerkonten	Der Zugang zu sämtlichen IT-Systemen erfolgt über Benutzerkonten, wie zum Beispiel für E-Mail, digitales Klassenbuch und Netzwerkzugang.
Step 8	
Description	
Who Users the system	**Who is responsible for the system**
Lehrkräfte, Direktion, Bibliothek, Schüler	IT-Verantwortlicher
Step 9	
Related Assets	
Which assets are related to this system?	
Information	**Services and Application**
Zugangsdaten, Rollenrechte	Active Directory, Gruppenrichtlinien
Other	
Dyrekcja-PC01, Server PLS-AUT, Uczen-PC01, Nauczyciel-PC02, Nauczyciel-LP02, Bibliothek_PC01 WLAN, Drucker, Filesharing, E-Mail	
Step 10	**Step 11**
Security Requirements	**Most Important security requirements**
What are the security requirements for this system	**Which security requirement is most important for this system**
Vertraulichkeit: Nur die betreffende Person sollte Zugang zu ihrem eigenen Konto haben. Es ist ratsam, starke Passwörter zu verwenden und die Zwei-Faktor-Authentifizierung zu aktivieren.	Integrität (Integrity)

Integrität: Die Rollen- und Rechte vergabe muss korrekt sein, damit kein unbefugter Zugriff auf das System möglich ist. Verfügbarkeit: Die Daten müssen während der Schulzeiten durchgängig zugänglich sein, insbesondere für Bibliothekarin, Lehrer und Schüller	

Tabelle 16 Kritisches Asset "Benutzerkonten" – Analyse gemäß OCTAVE-S (Schritte 6 -11) (Alberts, et al. 2025)

Step 6	**Step 7**
Critical Asset	**Rationale for Selection**
What is the critical System	**Why is this system critical to the organization**
LAN/WLAN-Infrastruktur	Viele Dienste wie E-Klassenbuch, Whiteboard, Druck und Kommunikation sind auf LAN und WLAN-Zugang angewiesen.
Step 8	
Description	
Who Users the system	**Who is responsible for the system**
Bibliothekpersonal, Lehrkräfte, Direktion, Schüler, Gäste	IT-Verantwortlicher
Step 9	
Related Assets	
Which assets are related to this system?	
Information	**Services and Application**
Zugangsdaten, Authentifizierungsinformationen	DHCP, DNS, Server, Firewall
Other	
WLAN-Access Point, Server, Benutzerkonten, Whiteboard, mobile Geräte	
Step 10	**Step 11**
Security Requirements	**Most Important security requirements**
What are the security requirements for this system	**Which security requirement is most important for this system**
Vertraulichkeit: WLAN muss durch WPA2/WPA3-Standard und getrennte Netze für Schüler und Lehrer oder Gäste abgesichert sein	Verfügbarkeit (Availability)

Integrität: Netzwerkverkehr darf nicht manipuliert oder überwacht werden können–Schutz vor Man-in-the-Middle-Angriffen. Verfügbarkeit: WLAN muss überall verfügbar, stabil und leistungsfähig sein-vor allem in Klassenräumen und Lehrerzimmern.	

Tabelle 17 Kritisches Asset "LAN/WLAN-Infrastruktur" – Analyse gemäß OCTAVE-S (Schritte 6 - 11). (Alberts, et al. 2025)

Step 6	**Step 7**
Critical Asset	**Rationale for Selection**
What is the critical System	**Why is this system critical to the organization**
E-Klassenbuch	Alle administrativen Aufgaben im Zusammenhang mit dem Unterricht (z.B. Anwesenheit, Noten, Kommentare) werden online über das E-Klassenbuch abgewickelt. Ein Ausfall dieses Systems würde den Schulalltag stark beeinträchtigen.
Step 8	
Description	
Who Users the system	**Who is responsible for the system**
Lehrkräfte, Direktion	IT-Verantwortlicher, Software Anbieter (extern)
Step 9	
Related Assets	
Which assets are related to this system?	
Information	**Services and Application**
Schülerdaten, Noten, Fehlzeiten	E-Klassenbuch Webanwendung
Other	
Dyrekcja-PC01, Server PLS-AUT, Nauczyciel-PC02, Nauczyciel-LP02, WLAN-Infrastruktur, E-Mail-Kommunikation, Internetverbindung, Benutzerkonten	
Step 10	**Step 11**
Security Requirements	**Most Important security requirements**
What are the security requirements for this system	**Which security requirement is most important for this system**
Vertraulichkeit: Informationen über Schüler, ihre Noten und Anmerkungen dürfen nur von befugten	Integrität (Integrity)

Lehrkräften eingesehen werden. Der Zugriff ist zu protokolieren. Integrität: Falsche oder manipulierte Noten gefährden den Schulerfolg. Änderungen müssen revisionssicher dokumentiert sein. Verfügbarkeit: Das System muss jederzeit im Unterricht und zur Zeugniserstellung erreichbar sein. Kurze Offline-Zeiten sind erlaubt.	

Tabelle 18 Kritisches Asset "E-Klassenbuch" – Analyse gemäß OCTAVE-S (Schritte 6 - 11)

Step 6	**Step 7**
Critical Asset	**Rationale for Selection**
What is the critical System	**Why is this system critical to the organization**
Drucker	Der Druck von Zeugnissen, Unterlagen und Lehrmaterialien spielt eine entscheidende Rolle in zahlreichen Prozessen.
Step 8	
Description	
Who Users the system	**Who is responsible for the system**
Bibliothekspersonal, Lehrkräfte, Direktion	IT-Verantwortlicher
Step 9	
Related Assets	
Which assets are related to this system?	
Information	**Services and Application**
Druckdaten (z. B. Zeugnisse, Prüfungen, Lehrmaterialien)	Druckserver
Other	
Netzwerk, Dyrekcja-PC01, Server PLS-AUT, Nauczyciel-PC02, Nauczyciel-LP02, Bibliothek-PC01, mobile Geräte	
Step 10	**Step 11**
Security Requirements	**Most Important security requirements**
What are the security requirements for this system	**Which security requirement is most important for this system**
Vertraulichkeit: Ausdrucke mit sensiblen Daten (z. B. Zeugnisse, Listen) dürfen nicht unbeaufsichtigt im Ausgabefach liegen	Verfügbarkeit (Availability)

Integrität: Druckaufträge müssen unverändert und vollständig gedruckt werden. Verfügbarkeit: Drucker müssen zuverlässig funktionieren, insbesondere vor der Zeugnisausgabe und vor Veranstaltungen. Ersatzgeräte oder Notfalldrucker sind vorgesehen (HP Envy Tintenstrahldrucker).	

Tabelle 19 Kritisches Asset "Drucker" – Analyse gemäß OCTAVE-S (Schritte 6 - 11). (Alberts, et al. 2025)

Auf Basis dieser Analyse findet eine Bewertung statt, die die Relevanz der identifizierten Assets für den Schulbetrieb in Bezug auf die Sicherheitsanforderungen Vertraulichkeit, Integrität und Verfügbarkeit priorisiert, um darauf aufbauend gezielte Schutzmaßnahmen abzuleiten.

Asset-ID	Asset	Vertraulichkeit	Integrität	Verfügbarkeit	Kritikalität
KA01	Schüller Daten	Hoch	Hoch	Hoch	Sehr Hoch
KA02	Bibliothekdatenbank	Hoch	Hoch	Hoch	Sehr Hoch
KA03	Lehrmaterialien	Mittel	Hoch	Mittel	Hoch
KA04	E-Mail-Kommunikation	Hoch	Mittel	Mittel	Hoch
KA05	Shared-Ordner	Mittel	Hoch	Hoch	Hoch
KA06	Benutzerkonten	Hoch	Hoch	Hoch	Sehr Hoch
KA07	LAN/WLAN-Infrastruktur	Mittel	Hoch	Hoch	Hoch
KA08	E-Klassenbuch	Mittel	Hoch	Hoch	Hoch
KA09	Drucker	Mittel	Mittel	Mittel	Mittel

Tabelle 20 Einschätzung der Vertraulichkeit, Integrität, Verfügbarkeit und Kritikalität schulischer Assets. (Alberts, et al. 2025)

8.1.6 Assets Visualisierung

Zur Verbesserung der Übersichtlichkeit und Kommunikation wurde eine visuelle Darstellung der identifizierten kritischen Ressourcen erstellt. Die Abbildung 12 verdeutlicht die zentrale Bedeutung der IT-Infrastruktur und deren Verknüpfung mit den Bildungsprozessen:

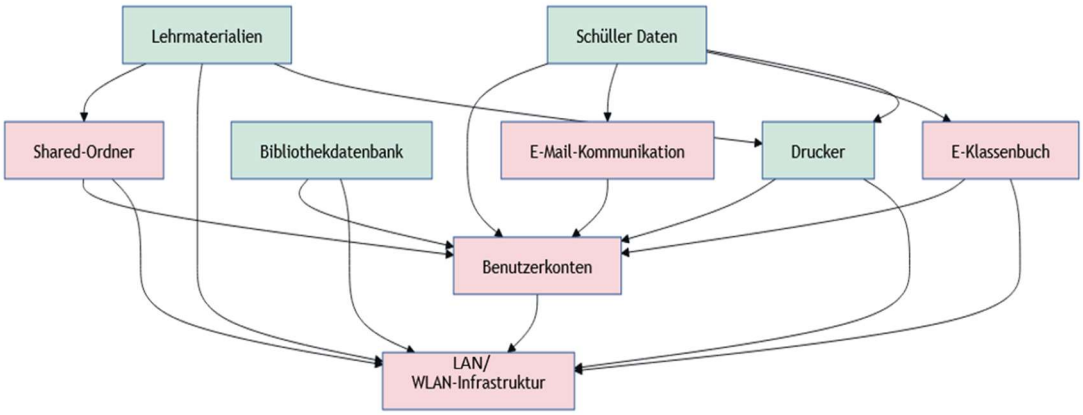

Abbildung 12 Darstellung der Asset-Abhängigkeiten im Rahmen der IT-Sicherheitsanalyse (OCTAVE-S Phase 1)

8.1.7 Bedrohungsanalyse

In dieser Phase werden konkrete Bedrohungen wie Ransomware, Phishing und unautorisierte Zugriffe, die bereits in Kapitel 7 angesprochen wurden, erneut identifiziert und bewertet. Grundlage hierfür sind reale Vorfälle aus Juni 2024 und April 2025 sowie Erkenntnisse ausgeführten Gesprächen. Aufbauend auf diesen Ereignissen wird die Analyse präzisiert bzw. verfeinert.

Bedrohung	Häufigkeit	Auswirkung	Priorität
APR-Spoofing	Hoch	Hoch	Kritisch
Physhing (BYOD)	Hoch	Hoch	Kritisch
Ransomware	Mittel	Hoch	Hoch
Trojaner	Mittel	Hoch	Hoch
PDF-Malware	Mittel	Mittel	Mittel
offenes WLAN	Hoch	Hoch	Kritisch

Tabelle 21 IT-Bedrohungen gemäß OCTAVE-S – Identifizierte Risiken und Priorisierung

8.1.8 Festlegung von Sicherheitsanforderungen

Auf Basis der identifizierten Bedrohungen und Schwachstellen werden nun spezifische technische und organisatorische Sicherheitsmaßnahmen formuliert. Ziel dieser Anforderungen ist die Sicherheit der polnische Schule nachhaltig zu erhöhen.

Maßnahme	Zweck
MFA für kritische Zugänge	Absicherung gegen Kontoübernahem
VLAN-Segmentierung	Trennung von BYOD (Schüler), Lehrer, Whiteboard und Gästen
MAC-Filter	Kontrolle der Zugriffe
Firewall (FORTIGATE)	Netzwerküberwachung und Attacken Abwehr

ESET PROTECT	Endproint Protection, Schwachstellenanalyse, Intrusion Detection
Patchmanagement	Regelmäßige Update von aller Systemen (ESET PROTECT)
Awareness-Trainings	Phishing-Abwehrt. Password Erstellung, Sichere Nutzung des Internets und Medien
MyQ X-Druckkontrolle	Authentifizierung bei Druckvorgängen
AES Verschlüsselung	Schutz von Daten auf dem Server (ESET Full Disk Encryption)
USV für Server	Schutz gegen Stromausfall und Datenverlust

Tabelle 22 IT-Sicherheitsmaßnahmen zur Steigerung der IT-Sicherheit an der Polnischen Schule des Jan III Sobieski.

8.1.9 Risikoprofile

Die nachfolgenden Risikoprofile bieten eine übersichtliche und an der Praxisorientierte Evaluierung potenzieller Gefahren, die zentrale IT-Assets der Polnischen Schule Jan III Sobieski betreffen. Diese wurden gemäß der OCTAVE-S Methode entwickelt und basieren auf realen Vorfällen.

Hierbei werden sowohl Bedrohungen durch interne als auch externe Akteure mit physischem oder elektronischem Zugang innerhalb der bestehenden Systemarchitektur berücksichtigt. Das Ziel der im Folgenden beschriebenen Risikoprofile besteht darin, kritische Schwachpunkte der Schul-IT evident zu machen, um daraus konkrete Handlungsempfehlungen abzuleiten, die darauf abzielen, das Risiko zu minimieren und die Widerstands- bzw. Resilienz der IT zu erhöhen. Jedes Risikoprofil beinhaltet die betroffenen Assets, potenzielle Motive für Angriffe oder Schäden, die daraus resultierenden Konsequenzen sowie die Anzahl erfasster Vorfälle, die auf früheren Daten basieren (Alberts, et al. 2025).

8.1.9.1 Risikoprofil – Menschliche Akteure mit Netzwerkzugang

In diesem Risikoprofil werden Bedrohungen analysiert, die durch menschliche Akteure entstehen, die legitimen oder unautorisierten Zugang zu IT-Systemen über das schulische Netzwerk besitzen. Zu den relevanten Akteuren zählen Lehrkräfte, Direktion, Bibliothekar, Schüler (BYOD) sowie externe Gäste oder potenzielle Angreifer.

Asset	Actor Type	Kategorie des Handelns	Motive	Outcome	Historical Occurrences
Schülerdaten	Insider	Insiders acting accidentally	Unabsichtlich	Offenlegung, Modifikation	3 Vorfälle intern unabsichtlich
Schülerdaten	Insider	Insiders acting deliberately	Absichtlich	Offenlegung, Modifikation	1 Vorfall intern absichtlich
Schülerdaten	Outsider	Outsiders acting deliberately	Absichtlich	Offenlegung, Verlust	1 Vorfälle extern absichtlich

E-Mail-Kommunikation	Outsider	Outsiders acting deliberately	Absichtlich	Offenlegung, Modifikation	22 Phishing-Vorfälle extern absichtlich
Shared-Ordner	Insider	Insiders acting accidentally	Unabsichtlich	Modifikation, Verlust	2 Vorfälle intern unabsichtlich
Shared-Ordner	Outsider	Outsiders acting deliberately	Absichtlich	Offenlegung, Verlust	0 Vorfälle extern absichtlich
Benutzerkonten	Outsider	Outsiders acting deliberately	Absichtlich	Offenlegung, Modifikation	0 Vorfälle extern absichtlich
WLAN-Infrastruktur	Outsider	Outsiders acting deliberately	Absichtlich	Offenlegung, Unterbrechung	26 Vorfälle extern absichtlich
E-Klassenbuch	Insider	Insiders acting accidentally	Unabsichtlich	Modifikation, Verlust	2 Vorfälle intern unabsichtlich
E-Klassenbuch	Outsider	Outsiders acting deliberately	Absichtlich	Offenlegung, Modifikation	0 Vorfälle extern absichtlich

Tabelle 23 Bedrohungen die von menschlichen Akteure mit Netzwerkzugang ausgehen. (Alberts, et al. 2025)

Die obere Tabelle gibt einen Überblick über die identifizierten Bedrohungen und deren Bewertung. Im Folgenden werden die spezifischen Risiken durch interne und externe Akteure, die sowohl unbeabsichtigte als auch vorsätzliche Handlungen umfassen, näher erläutert:

- **Unabsichtliche Handlungen (Insider):**
  - **E-Klassenbuch:** Bis dato konnten nur 2 Fälle festgestellt werden, wo ein Lehrer versehentlich unter dem falschen Schülernamen ein falscher Note erzeugte. In einem anderen Fall wurde eine Jahresnote durch Synchronisierungsprobleme mit dem Klassenbuch gelöscht. Keine externen Vorfälle dokumentiert: Das Risiko eines Brute-Force-Zugriffs auf das Online-Klassenbuch wurde jedoch technisch als hoch eingestuft.
  - **Shared-Ordner:** Eine Lehrer hat versehentlich und ohne Vorwarnung bestehende Dateien im Shared-Ordner ersetzt. Ein betroffenes Dokument war eine unterschriebene Ausflugserlaubnis eines Schülers, welches ohne Backup gelöscht wurde.
- **Absichtliche Handlungen (Outsider):**
  - **WLAN-Infrastruktur:** In zwei dokumentierten Fällen wurde ARP-Spoofing innerhalb des Gäste-WLANs durchgeführt, um Anmeldedaten über gefälschte DNS-Weiterleitungen abzugreifen. Die restlichen 26 Fälle betrafen massiven Datenverkehr durch unautorisierte Geräte, die Angriffe im Netzwerk simulierten.
  - **E-Mail-Kommunikation:** Es wurden 22 Fälle von gefälschten E-Mails von Microsoft, BLIK, PayPal, UPS usw. registriert. Zwei Empfänger

klickten auf Links und speicherten Malware auf dem Computer. (Alberts, et al. 2025)

Potenzielle Auswirkungen dieser Bedrohungen wurden anhand folgender Kriterien bewertet:

- **Modifikation:** Fehlerhafte Eingaben oder absichtliche Manipulationen beeinträchtigen die Datenintegrität der Schülerdaten.
- **Verlust:** Das versehentliche oder absichtliche Löschen von Daten oder Dokumenten kann den täglichen Betrieb erheblich stören.
- **Modifikation:** Eingaben in E-Klassenbuch, Bibliothekdatenbank oder Shared-Ordner können zu falschen Bewertungen, Datenverwirrung oder Verwaltungsproblemen führen.
- **Unterbrechung:** Störungen im WLAN oder bei synchronisierten Systemen E-Klassenbuch behindern den Unterrichtsalltag erheblich.
- **Offenlegung:** Besonders kritisch ist die Offenlegung sensibler personenbezogener Daten, da sie sowohl gegen die DSGVO verstößt als auch das Vertrauen der Betroffenen Schülerin die Institution nachhaltig schädigen kann. (Alberts, et al. 2025)

8.1.9.2 Risikoprofil – Menschliche Akteure mit physischen Zugang

Im weiteren Verlauf erfolgt eine Fokussierung auf physische Bedrohungsszenarien, mit dem Ziel, die potenziellen Auswirkungen einer umfassenden Analyse zu unterziehen. Zur Veranschaulichung wurden zwei zentrale organisatorische Ressourcen der Polnischen Schule Jan III Sobieski herangezogen: die Bibliotheksdatenbank und der Drucker. Sowohl das eine als auch das andere System wird im schulischen Alltag häufig verwendet, jedoch besteht bei dem Fehlen geeigneter Kontrollmechanismen einer Sicherheitsrisiko. Auch in bestehender Übersicht werden die verschiedenen Arten von Akteuren, Handlungen, Motiven, möglichen Auswirkungen und Vorfällen in der Vergangenheit sowie Bedrohungen behandelt, wie sie in Tabelle 23 im Subkapitel 8.1.9.1 bereits dargestellt worden sind. Dabei wird sowohl auf unbeabsichtigte als auch auf vorsätzliche Handlungen eingegangen. (Alberts, et al. 2025)

Asset	Actor Type	Kategorie des Handelns	Motive	Outcome	Historical Occurrences
Bibliothekdatenbank	Insider	Insiders acting accidentally	Unabsichtlich	Modifikation, Verlust	3 Vorfälle intern
Bibliothekdatenbank	Outsider	Outsiders acting deliberately	Absichtlich	Offenlegung, Verlust	1 Vorfälle extern
Drucker	Insider	Insiders acting accidentally	Unabsichtlich	Verlust, Modifikation	3 Vorfälle intern

Tabelle 24 Bedrohungen die von menschlichen Akteure mit physischen Zugang ausgehen. (Alberts, et al. 2025)

Die genannten Handlungen können wir wie folgt erläutern, um die spezifischen Risiken und Szenarien klarer darzustellen:

- **Unabsichtliche Handlungen (Insider)**
  - **Bibliothekdatenbank:** Drei interne Vorfälle wurden dokumentiert, bei denen das Bibliothekspersonal versehentlich Daten in der Bibliothek-datenbank löschte bzw. fehlerhaft eingab, wobei die fehlerhafte Bedienung der Software von der Firma VULCAN als Ursache identifiziert wurde. Ein konkretes Beispiel ist das Löschen einer Ausleihhistorie aufgrund eines Bedienfehlers, welches zu Verwirrung bei der Rückgabe von Bücher führte.
  - **Drucker:** In drei Fällen wurden interne Vorfälle dokumentiert, die das unbeabsichtigte Drucken sensibler Dokumente betrafen. Diese blieben im Ausgabefach liegen und wurden potenziell von Unbefugten eingesehen. Darüber hinaus wurde auch das versehentliche Löschen von Druck-aufträgen von Nutzer verzeichnet. (Alberts, et al. 2025)
- **Absichtliche Handlungen(Outsider):**
  - **Bibliothekdatenbank**: Die Analyse ergab, dass sich derzeit ein einzelner Fall dieser Art ereignete – ein Besucher schlich sich hinter die Bibliothekarin und konnte auf einem Bibliothek-PC Schüler Kontakt Daten einsehen.
  - **Drucker**: Obwohl keine dokumentierten externen Vorfälle vorliegen, besteht das Risiko, dass ein Eindringling Druckaufträge mit sensiblen Daten, wie beispielsweise Prüfungen, absichtlich abfängt oder die Hardware beschädigt. (Alberts, et al. 2025)

In diesem Zusammenhang können wir folgende potenzielle Auswirkungen (Impact Values) festlegen:

- **Modifikation:** Das Risiko für unbeabsichtigte Änderungen, fehlerhafte Eingaben in der Bibliothekdatenbank oder vorsätzliche Manipulationen resultiert in einer Gefährdung der Integrität der Daten. Dies kann zu Fehlern in der Bibliotheks-verwaltung oder unzuverlässigen Druckaufträgen führen.
- **Verlust:** Datenverlust, der etwa durch das Löschen von Bibliotheksdaten oder Druckaufträgen entsteht, würde den Betrieb stören, da wichtige Informationen nicht mehr verfügbar wären.
- **Offenlegung:** Die Bibliothekdatenbank ist in diesem Zusammenhang als besonders kritisch zu betrachten, da in diesem Kontext sensible Schülerdaten, wie Kontaktdaten, offen gelegt werden könnten. Dies kann rechtliche Konsequenzen nach sich ziehen, wie beispielsweise einen Datenschutzverstoß oder Reputationsschäden. (Alberts, et al. 2025)

8.1.9.3 Risikoprofil – Systemprobleme

Das "System Problem Worksheet" analysiert technische Risiken, die den Schulbetrieb der Polnische Schule Jan III Sobieski beeinträchtigen können, insbesondere durch Software sowie Schadsoftware. Die nachfolgende Tabelle gibt einen Überblick über die betroffenen Assets, die Art der aufgetretenen Probleme, die potenziellen Auswirkungen sowie die Anzahl der dokumentierten Vorfälle im April 2025.

Asset	Problem Type	Outcome	Historical Occurrences
E-Klassenbuch	Software defects	Verlust, Modifikation	2 Vorfälle
E-Mail-Kommunikation	Software defects	Verlust, Modifikation	2 Vorfälle
Lehrmaterialien	Software defects	Verlust, Modifikation	2 Vorfälle
Lehrmaterialien	Malicious code	Verlust, Modifikation	4 Vorfälle

Tabelle 25 Risikoprofil – Systemprobleme: Identifizierte Schwachstellen und historische Ereignisse (Alberts, et al. 2025)

Zur besseren Verständlichkeit werden im Folgenden Vorfälle erläutert, die die konkreten Auswirkungen der identifizierten Systemprobleme auf den Schulalltag belegen. Diese realen Ereignisse bilden die Grundlage für die Risikobewertung technischer Schwachstellen:

- **Software Defects:** In der jüngeren Vergangenheit traten beim E-Klassenbuch zwei dokumentierte Vorfälle auf, bei denen Softwarefehler zu temporärem Datenverlust nicht gespeicherte Noten oder Modifikationen fehlerhafte Anzeige von Fehlzeiten führten. Auch bei der E-Mail-Kommunikation kam es zu zwei Fällen von Dateninkonsistenz oder-verlust durch fehlerhafte Synchronisation mit dem Mailserver. Bei den Lehrmaterialien verursachte ein Shared-Ordner Kapazität Problem im Server, den Verlust von Arbeitsdateien, wodurch der Unterrichtsablauf beeinträchtigt wurde.
- **Malicious Code:** Besonders kritisch sind vier dokumentierte Vorfälle mit infizierten ORPEG PDF-Dateien, die über Direktion in das System gelangen konnten. Diese führten zu Datenverlust wie und beschädigte Lehrdokumente sowie zu unautorisierten Modifikationen, wodurch die Integrität der Lehrmaterialien ernsthaft gefährdet wurde. (Alberts, et al. 2025)

Die anschließende Zusammenfassung veranschaulicht die zentralen Auswirkungen von Softwarefehlern und Schadsoftware. Darüber hinaus verdeutlicht sie, wie technische Störungen die Arbeitsfähigkeit der Lehrkräfte, die Integrität schulischer Prozesse sowie die Verfügbarkeit kritischer Daten beeinträchtigen können:

- **Verlust:** Datenverluste, wie das unbeabsichtigte Löschen von Noten oder Unterrichtsdateien, führten zu erheblichen Unterbrechungen im Schulalltag. In solchen Fällen mussten Lehrkräfte auf manuelle Wiederherstellung zurückgreifen.

- **Modifikation:** Unbeabsichtigte oder böswillige Änderungen von Daten durch Softwarefehler oder Schadsoftware stellten eine Bedrohung für die pädagogische und rechtliche Integrität dar. So kann etwa eine fehlerhafte Noteneintragung im E-Klassenbuch rechtliche Folgen und Beschwerden von Eltern nach sich ziehen (In unseren Fällen ist keine dieser Konsequenzen aufgetreten). (Alberts, et al. 2025)

Die aufgezeichneten Vorfälle verdeutlichen, dass Sicherheitslücken in der Software sowie unzureichende Schutzmaßnahmen gegen Malware ein nicht zu unterschätzendes Risiko darstellen. Die Zunahme von Angriffen, die durch mit BYOD-Geräten assoziierte schadhafte Software initiiert werden, verdeutlicht die Relevanz technischer Lösungen, wie etwa die VLAN-Segmentierung, Antivirenprogramme und Patchmanagement, sowie organisatorischer Ansätze, wie etwa Schulungen zur Sensibilisierung für Lehrer und Schüler.

8.2 Phase 2: Technische Sicht

In der zweiten Phase der OCTAVE-S Methode wird der Fokus auf die technische Perspektive der IT-Infrastruktur gerichtet. Das Ziel besteht darin, konkrete Schwachstellen in Systemen, Anwendungen und Netzwerken zu identifizieren und deren Risiken methodisch zu bewerten. Die in Kapitel 7 und 8.1 gewonnenen Erkenntnisse bilden die Grundlage für diese technische Analyse. Im Rahmen dieser Untersuchung werden einzelne IT-Komponenten analysiert, Bedrohungen systematisch zu geordnet und priorisierte Sicherheitslücken identifiziert. Im Rahmen der vorliegenden Bewertung erfolgt auch eine Prüfung der Zugangspfade zu kritischen Vermögenswerten. Darüber hinaus wird eine Analyse technologiebezogener Prozesse durchgeführt. Abschließend erfolgt eine strukturierte Verknüpfung mit den OCTAVE-S Schritte 17 bis 21 (Alberts, et al. 2025).

8.2.1 Schlüsselkomponenten der Infrastruktur

Aufbauend auf der in Phase 1 vollzogenen Evaluation der organisatorischen Assets sowie der identifizierten Sicherheitsanforderungen richtet sich der Fokus der zweiten Phase der OCTAVE-S Methode nun auf die konkrete technische Implementierung. Die Analyse der Schlüsselkomponenten der IT-Infrastruktur dient dazu, bestehende technische Schwachstellen zu identifizieren, potenzielle Angriffspunkte für Bedrohungen zu ermitteln um daraus resultierend notwendige Sicherheitsmaßnahmen abzuleiten (Alberts, et al. 2025).

Der Fokus liegt hierbei auf den Systemen, die für den Schulbetrieb von Relevanz sind, insbesondere unter Berücksichtigung der zuvor priorisierten kritischen Vermögenswerte wie Schülerdaten, Bibliotheksdatenbank, E-Klassenbuch oder E-Mail-Kommunikation.

Die nachfolgende Übersicht fasst die wesentlichen Schlüsselkomponenten der derzeitigen und zukünftigen IT-Infrastruktur zusammen.

Komponente	Beschreibung
Server	HPE ProLiant MicroServer Gen10 Plus, zentraler Speicher- und Backup-Knoten
Switch	HP 1410-24G J9561A, kein VLAN-Support, ersetzt durch Cisco 3750V2
WLAN-Router	Linksys EA7500, keine Verschlüsselung für Gäste-WLAN, geplant: Cisco 819G-4G-GA-K9
Firewall	Derzeit nicht vorhanden, geplant: FortiGate-60F
Endgeräte	Schul-PCs (Windows 10), Laptops, mobile BYOD-Geräte (iOS, Android)
Drucker	Kyocera, HP, Samsung; alle netzwerkfähig, ohne Authentifizierung geplant: MyQ X
WLAN-Infrastruktur	Devolo-Powerline, WLAN-Ausbau mit APs MERAKI MR32 geplant
Cloud-Dienste	OneDrive, Dropbox für Lehrmaterialien
Software	Windows Server 2016, Oracle DB (Bibliothek), Microsoft Office, Avast Anitivirus (auslaufend)

Tabelle 26 Übersicht der IT – Schlüsselkomponenten (Alberts, et al. 2025)

Diese Komponenten bilden das Rückgrat der schulischen IT-Infrastruktur und gelten sowohl als Ziel möglicher Bedrohungen (z.B. durch Ransomware oder unautorisierte Zugriffe) als auch als Hebel für Verbesserungsmaßnahmen. Die detaillierte Bewertung der einzelnen Systeme erfolgt im nächsten Abschnitt im Rahmen der systematischen Schwachstellenanalyse und Risiko Priorisierung.

8.2.2 Prüfung der Zugangspfade zu kritischen Assets

Im Anschluss an die Identifikation technischer Schwachstellen erfolgt unter Bezugnahme auf Schritt 17 der OCTAVE-S Methode eine detaillierte Analyse der Zugangspfade zu den in Kapitel 8.1 ermittelten kritischen Assets. Das Ziel besteht darin, die vorhandene Sicherheitsarchitektur der Zugriffsmöglichkeiten zu überprüfen und potenzielle Schwachstellen in den Bereichen Authentifizierung, Verschlüsselung und Zugriffskontrolle aufzuzeigen (Alberts, et al. 2025).

Im Rahmen der Analyse wird insbesondere untersucht, ob die bestehenden Zugangsmöglichkeiten den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit gerecht werden. Die entsprechenden Definitionen sind in den Tabellen 11 bis 19 aufgeführt. In die Bewertung fließen sowohl interne Netzwerke – Shared-Ordner, Serverzugriffe – als auch externe Plattformen wie Webzugriffe auf das E-Klassenbuch oder Cloud-Dienste ein.

Die Tabelle 27 präsentiert eine Übersicht über die Zugangspfade der wichtigsten Assets unter Berücksichtigung zentraler Schutzmechanismen:

Asset	Zugangspfad	Authentifizierung	Verschlüsselung	Zugriffskontrolle
Schülerdaten	Server → Dyrekcja-PC01 / OneDrive	Passwort (AD)	Nein	Teilweise
Bibliotheksdatenbank	Bibliothek-PC01 → Oracle DB	lokal	Nein	Nein
E-Klassenbuch	Extern via Web	Benutzername & Passwort	HTTPS	Nein
Lehrmaterialien	Dropbox, OneDrive	lokal	Nein	Nein
Shared-Ordner	Netzlaufwerk / WLAN	AD / lokal	Nein	Teilweise
LAN/WLAN-Infrastruktur	WLAN-Access-Points / Linksys EA7500	WLAN-Passwort (teilweise)	Nein (offenes Gäste-WLAN)	Nein (keine Netztrennung, keine VLANs)
Benutzerkonten	Login → AD / lokale Geräte / Dienste	Benutzername & Passwort	Nein (keine 2FA)	Teilweise (Gruppenrichtlinien)
E-Mail-Kommunikation	Outlook / Gmail / ORPEG-Mail (Web, IMAP)	Passwort	HTTPS / TLS (je nach Anbieter)	Eingeschränkt (Clientabhängig)
Drucksysteme	LAN → Netzwerkdrucker (Kyocera, HP, Samsung)	Keine / lokal	Nein	Nein (kein Login, keine Authentifizierung)
Remote-Zugriff (Admin)	TeamViewer / Splashtop	Passwort / Code	Nein / teilweise (abhängig von Tool)	Keine zentrale Verwaltung

Tabelle 27 Übersicht über die Zugangspfade der Assets (Alberts, et al. 2025)

Dieses Übersicht verdeutlicht, dass insbesondere im Hinblick auf die drahtlose Infrastruktur dringender Handlungsbedarf besteht. Denn es mangelt sowohl an Verschlüsselung als auch an einer Netzwerksegmentierung, welche für die Gewährleistung der Sicherheit sensibler Daten in Netzwerken als unabdingbar zu betrachten ist. Dies deckt sich mit den bereits in Kapitel 8.1.7 und 8.1.8 festgestellten Bedrohungsszenarien (offenes WLAN, BYOD-Risiken) und unterstreicht die Notwendigkeit geplanter Maßnahmen wie VLAN-Segmentierung, Verschlüsselung und MAC-Adresse-Filterung.

8.2.3 Identifikation technischer Schwachstellen

Im Rahmen von Schritt 18 der OCTAVE-S Methode erfolgt eine gezielte Identifikation technischer Schwachstellen innerhalb der bestehenden IT-Infrastruktur. Die vorliegende Evaluation stützt sich auf die Erkenntnisse aus der Analyse der Zugangspfade (Kapitel 8.2.2) sowie auf dokumentierte reale Vorfälle an der Schule in den Jahren 2024 und 2025 (vgl. Kapitel 8.1.9).

Das Ziel dieses Schrittes besteht darin, die Schwächen und technische Fehlkonfigurationen offenzulegen, die den Schutz kritischer Assets – wie Schülerdaten, Lehrmaterialien oder das E-Klassenbuch – gefährden (Alberts, et al. 2025). Die nachfolgende Tabelle fasst zentrale Schwach-stellen zusammen, benennt die Ursachen und zeigt die damit verbundenen Bedrohungs-szenarien auf:

Schwachstelle	Beschreibung	Ursache	Bedrohung
Offenes Gäste-WLAN	Keine Verschlüsselung, keine Zugangskontrolle	Veraltete Router-Konfiguration	Man-in-the-Middle Attacken, unautorisierter Zugriffe
Fehlende VLAN-Segmentierung	Kein Schutz zwischen Lehrer-, Schüler- und Gäste- und Lokalen Netz	Veralteter Switch	Ausbreitung von Malware, ARP Spoofing
Veraltete Software	Fehlende Patches auf Lehrer-Notebooks	Kein zentrales Patchmanagement	Exploits, Ransomware
Ungeschützte Drucker	Kein Login, direkter Zugriff auf Netzwerkfreigaben	Kein zentrales Managementsystem	Datenverlust, unautorisierte Nutzung
Fehlende Firewall	Keine Paketfilterung, keine Abwehrmaßnahmen	Ressourcenmangel	Ransomware, DDoS
Kein Intrusion Detection	Keine Erkennung bei Zugriffen oder Anomalien	Fehlende Monitoring-Infrastruktur	Datenabfluss, unbemerkte Angriffe
Unkontrolliertes BYOD	Keine Kontrolle über mobile Geräte	Offene WLAN-Infrastruktur	Einschleusung von Malware
Keine Datenverschlüsselung	PC und Laptopdateien ungeschützt	Fehlende Standards, fehlende Awareness	Datenlecks bei Diebstahl oder Zugriff

Tabelle 28 Technische Schwachstellen gemäß OCTAVE-S Schritt 18 (Alberts, et al. 2025)

8.2.4 Zuordnung der Bedrohungen zu technischen Komponenten

Basierend auf der Identifikation technischer Schwachstellen erfolgt in Schritt 19 der OCTAVE-S Methode eine Zuordnung spezifischer Bedrohungen zu den betroffenen IT-Komponenten. Das Ziel dieses Schrittes besteht darin, die potenziellen Angriffspunkte innerhalb der technischen Infrastruktur präzise zu lokalisieren und dadurch zielgerichtete Schutzmaßnahmen zu ermöglichen (Alberts, et al. 2025).

Die nachfolgende Tabelle präsentiert eine Übersicht über die Relevanz verschiedener Bedrohungen für spezifische IT-Komponente. Die Zuordnung erfolgt anhand der in Kapitel 8.2.3 erörterten Schwachstellen und unzureichender Konfigurationen. Die vorliegende Untersuchung stützt sich auf eine Kombination aus technischen Beobachtungen und dokumentierten Vorfällen an der Schule (vgl. Kapitel 8.1.9).

Bedrohung	Komponente	Begründung
Ransomware	Server, Nauczyciel-LPs, Dyrekcja-PC, Biblioteka-PC	Fehlende Updates, fehlende Firewall, zentrale Datenhaltung
Phishing	BYOD, E-Mail-System	Offenes WLAN, keine Schulungen, kein E-Mail-Filter
DDoS	Router, Access Point, WLAN, Switch	Keine aktive Abwehr, keine Trennung, keine Lastverteilung
ARP Spoofing	Switch, Netzwerkstruktur	Keine Segmentierung, ungeschütztes internes LAN

PDF-Malware	Nauczyciel-LPs, Dyrekcja-PC, Biblioteka-PC, Uczen-PC	Kein Filter, keine AV-Integration im Dateisystem
Trojaner	BYOD, geteilte Geräte, Nauczyciel-LPs, Dyrekcja-PC, Biblioteka-PC, Uczen-PC	Keine Richtlinien, keine Kontrolle über App-Installationen

Tabelle 29 Übersicht über verschiedener Bedrohungen für spezifische IT-Komponente. (Alberts, et al. 2025)

8.2.5 Bewertung der Sicherheitslücken

Bei der Risikobewertung gemäß OCTAVE-S Schritt 20 findet eine Einstufung der identifizierten technischen Schwachstellen anhand zwei zentraler Kriterien statt:

- **Eintrittswahrscheinlichkeit** ist definiert als die Wahrscheinlichkeit, dass eine Schwachstelle in einem System ausgenutzt wird.
- **Schadenspotenzial** gibt Aufschluss darüber, welche Schäden sich im Falle einer Kompromittierung ergeben könnten (Alberts, et al. 2025).

Diese Bewertung bildet die Basis für die Priorisierung im Kontext des Risiko-managements und die Ableitung geeigneter Maßnahmen. Hierbei werden sowohl dokumentierte Vorfälle (vgl. Kapitel 8.1.9) als auch technische Analysen der IT-Infrastruktur (vgl. Kapitel 8.2.3 und 8.2.4) berücksichtigt. Die daraus abgeleiteten Risikowerte bilden eine zentrale Entscheidungsgrundlage für die Umsetzung technischer und organisatorischer Schutzmaßnahmen in Phase 3 der OCTAVE-S Methode.

Schwachstelle	Eintrittswahrscheinlichkeit	Schadenspotenzial	Gesamtrisiko
Offenes Gäste-WLAN	Hoch	Hoch	Kritisch
Keine VLAN-Segmentierung	Hoch	Hoch	Kritisch
Veraltete Software	Mittel	Hoch	Hoch
Ungeschützte Drucker	Mittel	Mittel	Mittel
Fehlende Firewall	Hoch	Hoch	Kritisch
Kein IDS	Hoch	Hoch	Kritisch
Unkontrollierte BYODs	Hoch	Hoch	Kritisch
Keine Datenver-schlüsselung	Mittel	Hoch	Hoch

Tabelle 30 Bewertung technischer Schwachstellen nach Eintrittswahr-scheinlichkeit und Schadenspotenzial (Alberts, et al. 2025)

Die Analyse ergibt, dass insbesondere Schwächen in der Netzwerksicherheit, mangelhafte Segmentierung, keine vorhandene Firewall, ungeschütztes WLAN sowie das Fehlen zentraler Kontrollsysteme (IDS) als bedenklich zu betrachten sind. Sie stellen eine potenzielle Gefahr für die Vertraulichkeit, Integrität und Verfügbarkeit dar und sollten daher oberste Priorität bezüglich der Bearbeitung erhalten.

8.2.6 Analyse technologiebezogener Prozesse

Schritt 21 der OCTAVE-S Methode umfasst die gezielte Prozessanalyse der sicherheits-relevanten technischen Abläufe innerhalb der IT-Infrastruktur von der polnischen Schule. Dabei liegt der Fokus auf alltäglichen IT-Prozessen, die potenziell zu einer Gefahr für

kritischer Systeme und Daten werden können. Dies kann durch eine fehlende Automatisierung oder eine unzureichende Kontrolle geschehen. (Alberts, et al. 2025)

Die Evaluation erfolgt unter Berücksichtigung der in Kapitel 8.2.5 identifizierten Risiken sowie der infrastrukturellen Gegebenheiten der Schule. Das Ziel besteht darin, operative Schwächen transparent zu machen, die trotz vorhandener Technik die Wirksamkeit der IT-Sicherheit beeinträchtigen. Die nachfolgende Tabelle stellt die wichtigsten IT-Prozesse zusammen und benennt konkrete sicherheitsrelevante Probleme:

Prozess	Beschreibung	Sicherheitsproblem
Backup	Lokal auf Server, keine Externe-Speicherung	Keine Recovery-Tests, kein Desasterplan
Software-Updates	Manuell, dezentral	Verzögerte Updates, keine Patchmanagement
Benutzerverwaltung	AD vorhanden, aber eingeschränkt	Fehlende Rollentrennung, keine MFA
Logging / Monitoring	Nicht implementiert	Keine Angriffserkennung, keine Protokollierung
WLAN-Zugang	Offen für Gäste, kein Trennungskonzept	Keine Gastkontrolle, keine VLANs
Druckausgabe	Manuelle Freigabe	Keine Nachverfolgung, keine Zugriffsbeschränkung

Tabelle 31 Schwachstellenanalyse alltäglicher IT-Prozesse in der Schulumgebung (Alberts, et al. 2025)

8.2.7 Referenz der OCTAVE-S Schritte

Zur klaren Gliederung wie auch nachvollziehbaren Methode der durchgeführten technischen Sicherheitsbewertung wird nachfolgend eine Zusammenfassung der in Phase 2 behandelten Themen in Bezug auf die Schritte 17 bis 21 der OCTAVE-S Methode präsentiert (Alberts, et al. 2025).

Die vorliegende Einordnung veranschaulicht, welche Subkapitel die methodische Bausteine der OCTAVE-S repräsentieren und dient als Orientierungshilfe für die anschließende Analyse in Phase 3 (Strategie und Planung).

OCTAVE-S Schritt	Umsetzung im Subkapitel
Schritt 17	Siehe 8.2.2 – Zugangspfade zu kritischen Assets
Schritt 18	Siehe 8.2.3 – Technische Schwachstellen
Schritt 19	Siehe 8.2.4 – Bedrohungszuordnung
Schritt 20	Siehe 8.2.5 – Risikobewertung und Dokumentation
Schritt 21	Siehe 8.2.6 – Analyse technikbezogener Prozesse

Tabelle 32 Zuordnung der Subkapitelinhalte zu den OCTAVE-S Schritten der Phase 2

8.2.8 Priorisierung der Maßnahmen

Basierend auf der in den früheren Kapiteln durch geführten technischen Schwachstellen- und Bedrohungsanalyse (vgl. Kapitel 8.2.3 bis 8.2.6) werden im Rahmen von OCTAVE-S Schritt 21 präzise Sicherheitsmaßnahmen priorisiert (Alberts, et al. 2025). Die nachfolgende Tabelle zeigt, welche Maßnahmen mit welcher Dringlichkeit

umzusetzen sind, um die identifizierten Risiken wirksam zu minimieren und die IT-Sicherheit der Schule nachhaltig zu stärken:

Maßnahme	Priorität	Betroffene Komponenten
Einführung FortiGate-60F	Sehr Hoch	WLAN, Internetzugänge, Server
VLAN mit Cisco 3750	Sehr Hoch	Netzwerksegmentierung
Einführung von Patchmanagement ESET PROTECT	Hoch	Biblioteka-PCs, Server, Nauczyciel-LPs, Dyrekcja-PC
Druckermanagementsystem MyQ X	Mittel	Drucker, LAN
WLAN-Verschlüsselung & Trennung	Sehr Hoch	Gäste-WLAN, interne Netze
ESET PROTECT als zentrale AV-Lösung	Hoch	Server, Endgeräte
BYOD-Regelung (Richtlinie & Trennung)	Hoch	WLAN, mobile Geräte
Awareness-Training für Lehrer	Hoch	E-Mail, Umgang mit Dateien, Passworte, BYOD-Schutz

Tabelle 33 Priorisierung sicherheitsrelevanter Maßnahmen. (Alberts, et al. 2025)

Die technische Analyse in Phase 2 der OCTAVE-S Methode hat Sicherheitslücken in der IT-Infrastruktur der Polnischen Schule Jan III Sobieski, die eine potenzielle Bedrohung für den Schulbetrieb darstellen, offenbart. Als besonders kritisch sind hier das ungeschützte Gäste-WLAN, die fehlende Netzwerksegmentierung sowie der unkontrollierte Einsatz privater Geräte (BYOD) gesehen.

Die in diesem Kapitel abgeleiteten Maßnahmen – insbesondere die Implementierung einer Firewall, die Einführung von VLANs sowie ein zentrales Patch- und Antivirenmanagement – müssen mit höchster Priorität umgesetzt werden, um die digitale Robustheit der Schule zu stärken und zukünftige Angriffe wirksam abzuwehren.

Die aus diese Analyse gewonnene Erkenntnisse dienen als Fundament für die dritte Phase der OCTAVE-S Methode, in welcher ein spezifischer Sicherheitsplan entwickelt wird, der sowohl technische als auch organisatorische Maßnahmen beinhaltet und auf den Rahmenbedingungen des schulischen Kontexts basiert.

8.3 Phase 3: Strategie und Pläne

In Phase 3 der OCTAVE-S Methode erfolgt eine systematische Bewertung der zuvor identifizierten Risiken. Darauf basierend wird eine realistische, effiziente und ressourcenschonende Sicherheitsstrategie erarbeitet. Die Polnische Schule Jan III Sobieski dient dabei als praktisches Anwendungsbeispiel. Die vorliegende Phase unterteilt sich in zwei Prozesse: Im Rahmen der Identifikation und Analyse von Risiken (Schritte 22 - 24) sowie der Entwicklung von Schutzstrategien und Maßnahmenplänen (Schritte 25 - 30). (Alberts, et al. 2025)

8.3.1 Identifikation und Analyse von Risiken

Der Prozess beinhaltet die Erfassung und systematische Evaluation von Bedrohungen, die in den Phasen 1 und 2 identifiziert wurden. Demzufolge besteht das Ziel darin,

verlässliche Aussagen bezüglich der Bedrohungslage der Polnischen Schule treffen zu können, um darauf aufbauend zielgerichtete Schutzmaßnahmen zu entwickeln.

8.3.1.1 Bewertung der Auswirkungen

Die Bewertung der Auswirkungen potenzieller Bedrohungen erfolgt anhand der in Kapitel 8.1.2 definierten Kriterien. Die vorliegende Problematik umfasst mehrere Faktoren, darunter Datenschutzbestimmungen, finanzielle Aspekte, der Imageschaden sowie der Unterrichtsausfall. Aus den dokumentierten Vorfällen aus den Monaten Juni 2024 und April 2025 wird die Grundlage für die weitere Analyse geschaffen, während die technische IST-Bewertung (Kapitel 7.4) als zusätzliche Informationsquelle dient. Dies dient dazu, potenziellen Schaden zu ermitteln, die durch reale Angriffsszenarien auf die kritischen Ressourcen der Schule verursachen werden können.

Die nachfolgende Tabelle präsentiert eine Übersicht über die identifizierten zentralen Bedrohungen, die betroffenen Systeme und ihre Auswirkungen auf Polnischen Schule:

Bedrohung	Kritisches Asset	Auswirkung	Bewertung
ARP-Spoofing	WLAN, Server, Bibliothek	Netzwerkausfall, unbefugter Zugriff auf Datenströme, Störung der Online-Recherche	Hoch
Ransomware	Server, E-Klassenbuch	Datenverschlüsselung, Verlust von Schülerakten, hohe Wiederherstellungskosten, Unterrichtsausfall	Kritisch
Phishing	E-Mail-Kommunikation, Benutzerkonten	Kontoübernahmen, Datenlecks, Vertrauensverlust bei Eltern und Partnerinstitutionen	Hoch
PDF-Malware	Lehrer-/Direktion und Bibliothek, Shared-Ordner	Schadcode durch getarnte Inhalte, Verlust oder Manipulation von Lehrmaterialien	Mittel
Unautorisierte Druckaufträge	Zeugnisse, Schülerlisten, Drucksysteme	Ausdruck sensibler Dokumente ohne Kontrolle, Datenschutzverletzungen	Hoch

Tabelle 34 Bedrohungen, betroffene Systeme und deren spezifische Auswirkungen im schulischen Kontext. (Alberts, et al. 2025)

Ergänzende Informationen zur Bewertung im Schulkontext:

- **ARP-Spoofing** stellte im Juni 2024 mit 32 dokumentierten Vorfällen eine massive Bedrohung dar –insbesondere in gemeinsam genutzten Räumen wie der Bibliothek. Dies beeinträchtigt nicht nur den Datenschutz, sondern auch das Vertrauen in schulinterne Recherchesysteme.
- **Ransomware-Attacken** auf den Direktion-PC und Server zeigen, wie eng organisatorische und technische Assets miteinander verbunden sind. Eine Kompromittierung betrifft hier unmittelbar den Unterricht, die Zeugnisvergabe und zentrale Verwaltungsprozesse – was in einer Auslandsschule wie der Sobieski-Schule diplomatische Folgen haben könnte.

- **Phishing** hat sich besonders durch gefälschte E-Mails von Unternehmen wie Microsoft, BLIK und Amazon verbreitet – insbesondere gefährlich, da viele Lehrkräfte E-Mails auch privat am selben Gerätempfangen.
- **PDF-Malware** wurde als "ORPEG-Dokument" getarnten Dateien eingeschleust, was eine gezielte Attacke auf das Vertrauen in offizielle Quellen darstellt. Diese Angriffsform verdeutlicht, wie leicht die Lehrer durch scheinbar authentisch gestaltete Unterrichtsmaterialien getäuscht werden können.
- **Fehlender Druckernachweis** birgt ein besonders hohes Risiko, da Zeugnisse oder interne Schülerlisten unbeaufsichtigt ausgedruckt werden können – ein klarer Verstoß gegen Datenschutzrichtlinien.

Diese Bewertung verdeutlicht die Dringlichkeit gezielter Schutzmaßnahmen insbesondere bei den Bereichen Netzwerksicherheit, Druckmanagement und digitaler Kommunikation. Sie bildet die Grundlage für die Auswahl und Priorisierung der in Kapitel 8.3.2 zu entwickelnden Schutzstrategien.

8.3.1.2 Festlegung von der Bewertungskriterien für die Eintrittswahrscheinlichkeit

Die Einschätzung der Eintrittswahrscheinlichkeit wird anhand definierter Kriterien vorgenommen, welche auf den betrieblichen Kontext der Polnischen Schule Jan III Sobieski zugeschnitten sind. Die vorliegende Analyse stützt sich auf eine Kombination aus empirischen Beobachtungen und technischen Bewertungen, die in den vorigen Kapiteln dokumentiert wurden.

Bei der Bewertung wurden folgende Einflussfaktoren berücksichtigt:

- Anzahl von dokumentierten Vorfällen
- Reifegrad technischer Schutzmaßnahmen
- Sensibilisierung der Benutzer
- Architektonische und physische Sicherheit. (Alberts, et al. 2025)

Dabei wurden die zuvor aufgestellten Kriterien auf die in Kapitel 8.3.1.1 untersuchten Bedrohungen angewendet. Die Resultate sind in Tabelle 35 zusammengefasst.

Bedrohung	Häufigkeit	Technische Maßnahmen	Awareness /Schulung	Architektur/Physische Sicherheit	Gesamteinschätzung
ARP-Spoofing	Hoch	Unzureichend	Keine	Schwach	Hoch
Ransomware	Mittel	Teilweise	Keine	Schwach	Mittel
Phishing	Hoch	Unzureichend	Keine	Schwach	Hoch
PDF-Malware	Mittel	Teilweise	Keine	Teilwiese	Mittel
Unautorisierte Druckaufträge	Mittel	Fehlend	Keine	Schwach	Mittel

Tabelle 35 Matrix zur Einschätzung der Eintrittswahrscheinlichkeit je Bedrohung (farblich codiert)

Die Matrix verdeutlicht, dass Bedrohungen wie ARP-Spoofing und Phishing aufgrund häufiger Vorfälle, fehlender technischer Barrieren und unzureichender Awareness ein

besonders hohes Risiko darstellen. Auch eine effektive Abwehr von Ransomware und PDF-Malware ist bei bestehender Infrastruktur nicht immer gewährleistet.

Diese Einschätzung bildet die Grundlage für die nachfolgende Priorisierung von Schutzmaßnahmen (Kapitel 8.3.2) und findet Eingang in die abschließende Risikobewertung laut OCTAVE-S Methode.

8.3.1.3 Bewertung der Eintrittswahrscheinlichkeit

In Anlehnung an die in Kapitel 8.3.1.2 festgelegten Kriterien erfolgt an dieser Stelle die konkrete Einstufung der Eintrittswahrscheinlichkeit für die analysierten Bedrohungen. Zu diesem Zweck wird eine dreistufige Skala (hoch, mittel, gering) eingesetzt. Die daraus resultierenden Ableitungen basieren auf Erkenntnissen aus technischen Bewertungen, dokumentierten Vorfällen und strukturellen Schwachstellen der IT-Infrastruktur der Schule.

Bedrohung	Eintrittswahrscheinlichkeit	Kurzbegründung
ARP-Spoofing	Hoch	Wiederholt aufgetreten, keine Netzsegmentierung, offenes WLAN
Ransomware	Mittel	Teilschutz durch AV vorhanden, jedoch fehlende Firewall und ungepatchte Systeme
Phishing	Hoch	Hohe Fallzahl, fehlende technischen Filter, keine Awareness Trainings
PDF-Malware	Mittel	Vorkommen erkannt, aber niedriger Umfang, keine Inhaltserkennung aktiv
Unautorisierte Druckaufträge	Hoch	Keine Zugangskontrollen, Nutzung durch alle über das Netzwerk

Tabelle 36 Einschätzung der Eintrittswahrscheinlichkeit analysierter Bedrohungen. (Alberts, et al. 2025)

Die vorliegende Bewertung (Tabelle 36) findet jeweils im Kontext der schulischen Infrastruktur statt und leistet einen Beitrag zur anschließenden Priorisierung im Rahmen der Risikobewertung in Kapitel 8.3.2. Eine erneute Darstellung der Ursachen oder technischen Grundlagen wird an dieser Stelle bewusst vermieden, da diese bereits in vorigen Abschnitten ausführlich behandelt wurden.

8.3.2 Entwicklung von Schutzstrategien und Maßnahmenplänen

Aufbauend auf der zuvor durchgeführten Risikobewertung (Kapitel 8.3.1) werden im folgenden Schritt gezielt Schutzmaßnahmen formuliert, priorisiert und in Umsetzungspläne überführt. Dementsprechend liegt der Fokus auf denjenigen Bedrohungen, die im Kontext der Polnischen Schule Jan III Sobieski eine besonders hohe Kritikalität aufweisen. Als besonders relevante Kategorien sind in diesem Zusammenhang insbesondere netzwerkbasierte Angriffe, Phishing, unkontrollierte Gerätezugriffe sowie fehlende Authentifizierungsmechanismen zu nennen.

Dieser Prozess umfasst laut OCTAVE-S Methode folgende Schritte:

- Beschreibung der aktuellen Schutzstrategie

- Ableitung konkreter Maßnahmen aus Bedrohungs- und Schwachstellenprofilen
- Definition der Verantwortlichkeit und Prioritäten
- Planung der Umsetzungsschritten. (Alberts, et al. 2025)

8.3.2.1 Beschreibung der aktuellen Schutzstrategie

Die gegenwärtige Sicherheitsstrategie der Polnischen Schule Jan III Sobieski hat eine einfache Struktur, die sich aus der bestehenden Infrastruktur und den verfügbaren Ressourcen ergibt. Im Zuge von OCTAVE-S Schritt 25 wird analysiert, welche Sicherheitsmaßnahmen momentan durchgeführt werden, wo Defizite bestehen und in welchem Maße ein systematischer Schutzansatz vorhanden ist (Alberts, et al. 2025).

Technische Schutzmaßnahmen

- **Antivirensoftware:** Derzeit ist Avast Business Security auf dem Server installiert. Die Software bietet einen Basisschutz gegen bekannte Malware-Typen. Die Lizenz läuft jedoch im Februar 2025 aus, eine Verlängerung ist nicht vorgesehen, da eine Migration auf ESET PROTECT angedacht ist.
- **Datensicherung:** Es wird ein tägliches Backup des Servers durchgeführt (lokal, inkrementell), jedoch ohne dokumentiertes Wiederherstellungskonzept oder externe Sicherungskopie. Automatisierung und Notfallpläne fehlen.
- **Netzwerkzugriff:** Der Zugang zum Haupt-WLAN ist mit einem Passwort geschützt, wobei dieses regelmäßig an neue Schüler kommuniziert wird. Gäste-WLAN ist unverschlüsselt und ohne Authentifizierung verfügbar. Eine Netzwerk-segmentierung findet nicht statt.
- **Zugriffschutz:** Die Benutzerverwaltung erfolgt zentral über Active Directory, jedoch ohne Zwei-Faktor-Authentifizierung oder vollständige Rollentrennung. Auf mobilen Endgeräten (BYOD) ist die Nutzung nicht angebunden und erfolgt unkontrolliert.
- **Physischer Schutz:** Der Server ist in einem abgeschlossenen Serverschrank mit Kühlung untergebracht. Räumlicher Zugriff auf Geräte ist jedoch nicht systematisch geregelt (z. B. unbesetzte Bibliothek, Lehrerzimmer mit Server-zugang). (Alberts, et al. 2025)

Organisatorische Maßnahmen

- **Passwortrichtlinien und Benutzerrollen**: Es existieren einfache Passwort-richtlinien (Mindestlänge, Regelmäßigkeit), die jedoch nicht konsequent durchgesetzt werden. Rollen- und Rechtevergaben sind vorhanden, aber nicht vollständig auf unterschiedliche Benutzergruppen abgestimmt.
- **Bewusstseinsbildung:** Strukturelle Schulungen zur IT-Sicherheit wurden bislang nicht durchgeführt. Kenntnisse im sicheren Umgang mit E-Mail, Internet und Geräten beruhen auf individueller Vorerfahrung der Lehrkräfte. (Alberts, et al. 2025)

Nach den Richtlinien der dritten Phase (Strategieentwicklung) der OCTAVE-S Methode lässt sich die derzeitige Sicherheitsstrategie wie folgt beschreiben:

- Es existiert kein konsolidierter Plan, der technische, organisatorische und personelle Sicherheitsmaßnahmen integriert.
- Die gegenwärtigen Ansätze reagieren lediglich auf Vorfälle und sind nicht präventiv; sie streben nur einen grundlegenden Schutz an und lassen viele bedeutende Ressourcen unberücksichtigt (vgl. Kapitel 8. 1. 5).
- Die Sicherheitsstrategie ist nicht dokumentiert, wird nicht regelmäßig evaluiert und enthält keine klaren Sicherheitsziele. (Alberts, et al. 2025)

8.3.2.2 Ableitung der Schutzmaßnahmen

Basierend auf den in Kapitel 8.3.1 identifizierten Risiken sowie der in 8.3.2.1 dokumentierten unzureichenden Schutzstrategie werden in diesem Arbeitsschritt konkrete Maßnahmen abgeleitet, die sowohl technisch als auch organisatorisch eine Risikoreduktion bewirken sollen. Die Selektion richtete sich nach den Kriterien der Wirksamkeit, Umsetzbarkeit im Schulkontext und Ressourcenschonung, wie sie in der OCTAVE-S Phase 3 (Schritte 25 - 30) gefordert sind (Alberts, et al. 2025).

Zu diesem Zweck werden Maßnahmen ergriffen, die mehrere Schwachstellen simultan adressieren, vorhandene Lücken systematisch schließen und an die tatsächliche Bedrohungslage der Schule adaptieren.

Im Folgenden werden ausgewählte prioritäre Schutzmaßnahmen dargelegt:

- **Integration einer FortiGate 60F Firewall:** Die Integration der FortiGate-Firewall als Ersatz für den bisherigen Router ermöglicht eine detaillierte Steuerung des Datenverkehrs (Deep Packet Inspection, Webfilter, VPN, Intrusion Detection). Diese Technologie fungiert als eine zentrale Verteidigungslinie, gegen netzwerkbasierte Angriffe, wie ARP-Spoofing, unerwünschte Zugriffe und Malware.
- **VLAN-Segmentierung mittels Cisco Catalyst 3750V2:** Die Netzwerksegmentierung dient der Unterteilung des Schulnetzes in klar abgegrenzte Zonen: VLAN 10 Server, VLAN 20 Computers, VLAN 30 Drucker, VLAN 3 Lehrer, VLAN 4 Schüler, VLAN 5 Gäste, VLAN 6 Whiteboard, VLAN 40 Access Point, VLAN 50 Other Devices. Dadurch kann die spätere Ausbreitung potenzieller Gefahren verhindert und ein kontrollierter Zugriff auf wichtigen Schulsysteme wie Server, Klassenbuch, Bibliothekdatenbank usw. sichergestellt werden.
- **ESET PROTECT als ein zentrales Schwachstellen- und Patchmanagement System:** Die vorliegende Endpoint-Security-Lösung ersetzt bisherige Einzelplatzlösung (Avast). ESET PROTECT gewährleistet nicht nur Schutz vor Malware, sondern bietet auch zentrale Überwachung von Updates, automatisierte Schwachstellenerkennung und Sicherheitsrichtlinien. Letzteres stellt eine entscheidende Maßnahme gegen Ransomware und PDF-Malware dar.

- **Zwei-Faktor-Authentifizierung (MFA) für AD-Konten:** Zur Erhöhung des Schutzes sensibler Benutzerkonten ist eine Ergänzung des bestehenden Active Directory um eine MFA ESET PROTEC Lösung zu empfehlen. In erster Linie profitieren Direktion oder die Bibliothekarin von einer effektiven Absicherung gegen Phishing- und Brute-Force-Angriffe.
- **Einführung eines Druckmanagementsystems MyQ X: Diese** Maßnahme ersetzt die bisherige unkontrollierte Druckfreigabe. Demnach erhalten ausschließlich authentifizierte Benutzer Zugriff auf sensible Druckaufträge, wie Zeugnisse oder Schülerlisten. Durch die Implementierung dieser Maßnahme wird eine Steigerung der Datensicherheit im Druckprozess erzielt. Zudem wird durch die Einführung von Druckkontingenten eine Reduktion der Betriebskosten bewirkt.

Die Auswahl der Maßnahmen erfolgte unter Berücksichtigung der tatsächlichen Schulbedürfnisse, der Umsetzbarkeit im gegebenen finanziellen und personellen Rahmen und der Nutzung bestehender Ressourcen. Zudem erfüllen sie die zentralen Anforderungen der OCTAVE-S Methode:

- Gezielte Risikoreduktion für kritische Assets wie Schülerdaten, Lehrmaterialien, E-Mail-Kommunikation und Druckprozesse
- Harmonisierung technischer und organisatorischer Schutzmaßnahmen
- Erhöhung der Robustheit ohne Beeinträchtigung des regulären Unterrichts-betriebs. (Alberts, et al. 2025)

Die so konzipierten Maßnahmen formen das Rückgrat strategischer Umsetzungspläne, die in Kapitel 8.3.2.3 entwickelt werden. Beschreibung der aktuellen Schutzstrategie

8.3.2.3 Planung der Umsetzungsschritten

Die im vorherigen Abschnitt (8. 3. 2. 2) beschriebenen Sicherheitsvorkehrungen sind in konkrete, durchführbare Maßnahmen zu überführen, um die IT-Sicherheit an der Schule langfristig zu verbessern. Im Rahmen der OCTAVE-S-Methode wird in diesem Schritt (Schritt 27) die technische Machbarkeit, die organisatorischen Fähigkeiten, die Zuständigkeiten des Personals sowie die verfügbaren zeitlichen Ressourcen berücksichtigt. (Alberts, et al. 2025)

Hierbei wird der Fokus auf eine stufenweise Implementierung gelegt, die sich am Schuljahresverlauf orientiert. Einerseits wird dadurch der laufende Betrieb nicht beeinträchtigt, andererseits wird die Komplexität für das IT-Personal sowie die Lehrkräfte in einem angemessenen Rahmen gehalten.

Maßnahme	Zuständigkeit	Geplanter Zeitraum	Priorität
FortiGate-Firewall einrichten	IT-Verantwortlicher	April 2025	Sehr hoch
VLAN-Setup mit Cisco 3750	IT-Verantwortlicher	April 2025	Sehr hoch

ESET PROTECT ausrollen	IT-Verantwortlicher	April 2025	Hoch
MyQ X-Druckmanagement integrieren	IT-Verantwortlicher	Mai – Juni 2025	Mittel
MFA für Lehrpersonal einführen	IT-Verantwortlicher, Direktion	September 2025	Hoch

Tabelle 37 Umsetzungsschritte der priorisierten Schutzmaßnahmen

Die Maßnahmen wurden in zeitlicher Hinsicht gestaffelt, sodass:

- kritische infrastrukturelle Verbesserungen (Firewall, VLAN) vor dem Sommersemester abgeschlossen sind, um das Fundament für weitere Sicherheitsmechanismen zu schaffen,
- softwaregestützte Prozesse (Antivirenlösung, Druckmanagement) erfolgen im Zeitraum Mai/Juni,
- organisatorische Veränderungen wie die Einführung der Zwei-Faktor-Authentifizierung mit dem neuen Schuljahr erfolgen, um eine frühzeitige Schulung des Personals zu ermöglichen. (Alberts, et al. 2025)

In der vorliegenden Planung wurde berücksichtigt, dass die Installation ausschließlich an ausgewählten Tagen pro Woche (Dienstag – Samstag) machbar wäre. Darüber hinaus fand eine Abstimmung mit der Direktion und dem Bibliothekspersonal statt, um eine Unterbrechung des Unterrichts sowie Bibliothek zu vermeiden.

8.3.2.4 Identifizierung notwendige Änderungen

Im Rahmen von OCTAVE-S Step 28 wird evaluiert, ob und inwiefern eine Anpassung der bestehenden IT-Sicherheitsstrategie erforderlich ist, um den identifizierten Bedrohungen und Schwachstellen (Kap. 8.3.1) wirksam entgegenzuwirken (Alberts, et al. 2025). In diesem Kontext sind nicht nur technische Erweiterungen von Relevanz, sondern eine grundlegende Reorientierung – ein Wandel vom reaktiven Grundschutz hin zu einem präventiv ausgerichteten, strategisch eingebetteten Schutzmodell, das sowohl technischen als auch organisatorischen Anforderungen entspricht.

Die bisherige Sicherheitsstrategie der Polnischen Schule Jan III Sobieski in Wien konzentrierte sich primär auf Minimallösungen. Dies umfasst die Implementierung von Antivirenschutz (Avast), die Verwendung von Passwörtern im Active Directory und die Einrichtung von einfachen Backup-Routinen. Dennoch bieten diese keinen ausreichenden Schutz vor den im Rahmen der Bedrohungsanalyse identifizierten Risiken wie ARP-Spoofing, Ransomware oder Phishing (vgl. Kapitel 8.3.1). Besonders hervorzuheben ist das Fehlen zentraler Steuerungselemente, wie etwa Netzwerk-segmentierung, kontrollierte Druckprozesse, eine zentrale Update-Verwaltung oder einheitliche Zugriffsrichtlinien.

Darüber hinaus ist festzustellen, dass keine Sensibilisierungsstrategie für Lehrkräfte und Direktion vorliegt. Dies ist insbesondere in Hinblick auf dokumentierte Phishing-Vorfälle (vgl. Kapitel 7.3.2) als gravierendes Problem zu betrachten.

Die neue Strategie, die durch die OCTAVE-S Analyse ausgearbeitet wurde, modifiziert diesen Ansatz und ergänzt ihn um die folgenden drei strategischen Dimensionen:

Schutzdimension	Neuer strategischer Fokus
1. Netzwerkschutz	Einführung von VLAN-Segmentierung und FortiGate-Firewall zur aktiven Trennung und Überwachung von Netzverkehr
2. Endgerätesicherheit	Einsatz von ESET PROTECT mit zentralem Schwachstellenmanagement, inklusive Patch- und Policy-Steuerung
3. Sicherheitskultur & Training	Start eines strukturierten Sensibilisierungsprogramms für Lehrkräfte ab Herbst 2025, Fokus auf Phishing, Passwortschutz und sichere Dateiverwaltung

Tabelle 38 Drei strategische Schutzdimensionen. (Alberts, et al. 2025)

Die vorliegende Neuausrichtung zielt darauf ab, die digitale Widerstandsfähigkeit der Schule gegenüber realen Bedrohungsszenarien messbar zu erhöhen, während gleichzeitig die vorhandenen Ressourcen (personell, finanziell, zeitlich) effizient genutzt werden.

Im schulischen Kontext orientiert sich die erweiterte Strategie an den organisatorischen und betrieblichen Besonderheiten der Schule, insbesondere an folgenden Aspekten:

- der beschränkten Präsenzzeiten im Gebäude (Dienstag bis Samstag),
- der ehrenamtlich geführten IT-Betreuung,
- sowie der Nutzung heterogener Endgeräte (BYOD, Schul-PC und Laptops, mobile Geräte).

8.3.2.5 Nächste Schritte

Aufbauend auf der in Kapitel 8.3.2.3 dargestellten Zeitplanung wurden folgende nächste Schritte definiert, um die Strategien und Maßnahmen innerhalb des laufenden Schuljahres abzusichern:

Maßnahme	Ziel	Zeitraum
Präsentation der Strategie vor der Schulleitung	Transparente Kommunikation der geplanten Sicherheitsarchitektur und Herbeiführung formaler Zustimmung zu Implementierung (z. B. für Firewall, Softwarelizenzen)	März/April 2025
Pilotbetrieb der neuen Komponenten	Technische Tests unter Realbedingungen (Firewall, VLAN, ESET, MyQ X Druckmanagement)	ab Mai 2025

Begleitende Dokumentation und Konfigurationshandbuch	Erstellung technischer Dokumente für Wartung, Betrieb und Übergabe	bis Juli 2025

Tabelle 39 Strategien und Maßnahmen innerhalb des laufenden Schuljahres

Die Implementierung dieser Schritte stellt sicher, dass sich die Maßnahmen nicht ausschließlich auf der theoretischen Ebene manifestieren, sondern im schulischen Alltag effektiv angewendet werden.

Zu diesem Zweck ist für das zweite Quartal 2026 ein internes Sicherheits-Audit vorgesehen, um die Effektivität der implementierten Maßnahmen zu evaluieren. Dieses soll:

- prüfen, ob die installierten Schutzmechanismen korrekt arbeiten,
- das Nutzerverhalten und die Wirksamkeit der Schulungsmaßnahmen evaluieren,
- potenzielle neue Schwachstellen identifizieren.

Das Audit wird auf Grundlage eines standardisierten Prüfkatalogs (bspw. BSI) durchgeführt. Die Ergebnisse fließen in einen Evaluationsbericht, der als Grundlage für eine mögliche Nachjustierung der IT-Sicherheitsstrategie dienen wird.

9. Entwicklung eines maßgeschneiderten IT-Sicherheitskonzepts

Die Analyse der bestehenden IT-Infrastruktur der Polnischen Schule Jan III Sobieski (Kapitel 7) und die darauf aufbauende, strukturierte Risikobewertung mithilfe der OCTAVE-Methode (Kapitel 8) haben eine Vielzahl von Schwachstellen und Risiken identifiziert, die die digitale Sicherheit der Schule erheblich gefährden. Auf Basis dieser Erkenntnisse entwickelt dieses Kapitel ein praxisnahes und umsetzbares IT-Sicherheitskonzept, das speziell auf die Bedürfnisse und Rahmenbedingungen der Schule zugeschnitten ist. Das Konzept integriert technische und organisatorische Maßnahmen, die aufeinander abgestimmt sind und sich an bewährten Sicherheitsstandards ausrichten, ohne die begrenzten Ressourcen der Schule zu überschreiten. Dieses Konzept verbleibt auf der Ebene der Planung und beschreibt Maßnahmen, Standards und Verfahren, ohne deren spätere Implementierung oder Wirkung vorwegzunehmen.

Das Ziel des Konzepts besteht in der Reduktion der Anzahl an Cybervorfällen um mindestens 50%, wie die historische Analyse der Vorfälle von Juni 2024 und April 2025 (Kapitel 7.3) unterstreicht. Das Konzept berücksichtigt die spezifischen Herausforderungen der Schule, wie das unverschlüsselte Gäste-WLAN, das Fehlen klarer Zugriffsregelungen, die unkontrollierte Nutzung von BYOD-Geräten und das eingeschränkte Sicherheitsbewusstsein von Lehrkräften und Schülern. Die Maßnahmen sind so konzipiert, dass sie sowohl die digitale Resilienz der Schule stärken als auch die Anforderungen an den Schulbetrieb erfüllen.

9.1 Technische Schutzmaßnahmen zur Stärkung der IT-Sicherheit

In den Kapiteln 7 und 8 wurden technische Schwachstellen sowie potenzielle Risiken im Netzwerk, der Zugriffskontrolle und dem Datenmanagement ermittelt. Dies unterstreicht die Dringlichkeit, den digitalen Schutz der Polnischen Schule Jan III Sobieski zu verstärken. In diesem Abschnitt wird das Ziel verfolgt, technische Maßnahmen gezielt darzustellen, die zur Stärkung der IT-Infrastruktur beitragen und eine belastbare Sicherheitsarchitektur etablieren.

Die in diesem Zusammenhang vorgeschlagenen Maßnahmen wurden an den in der OCTAVE-S Methode entwickelten Schutzbedarfen kritischer Assets ausgerichtet, wobei insbesondere Schülerdaten, digitale Verwaltungsprozesse und Lernplattformen berücksichtigt wurden. Zugleich wurden auch die praktischen Anforderungen des Schulalltags in die Überlegungen einbezogen.

Die nachfolgenden Unterkapitel behandeln zentrale sicherheitstechnische Problemfelder:

- den Aufbau einer resilienten Netzwerksicherheit (9.1.1),
- die Einführung Zugriffskontrollen und Authentifizierung (9.1.2),
- den gezielten Schutz sensibler Daten (9.1.3).

9.1.1 Netzwerksicherheit

Die Netzwerkinfrastruktur der Schule stellt gemäß den dokumentierten Vorfällen des ARP-Spoofing (vgl. Kapitel 7.3) einen zentralen Angriffspunkt dar. Aufbauend auf den in Kapitel 7.1.4 dargestellten technischen Maßnahmen zur Ersetzung der Netzwerkkomponenten werden im Folgenden konkrete sicherheitsstrategische Schritte formuliert, um die Angriffsfläche zu minimieren und die Integrität des Schulnetzwerks dauerhaft zu stärken:

- **Netzwerkperimeter absichern durch professionelle Firewall:** Die Einführung einer Next-Generation-Firewall mit integrierter Intrusion Detection und Prevention (IDS/IPS) bildet die Grundlage für einen aktiven Schutz vor Bedrohungen wie Malware, DDoS-Angriffen und unautorisierten Zugriffen. In Kombination mit einem zentralen Logging-System (vgl. Kapitel 8.3.1) ermöglicht sie die Echtzeiterkennung verdächtiger Aktivitäten und den gezielten Schutz kritischer Assets wie Schülerdaten, E-Klassenbuch und Bibliothekdatenbank.
- **Segmentierung des Netzwerks zur Begrenzung interner Bedrohungen:** Die in Kapitel 7.1.4 vorgesehene Umstellung auf VLAN-fähige Infrastruktur schafft die Voraussetzung für eine logische Trennung von Benutzergruppen. Durch die strukturierte Segmentierung – für Lehrkräfte, Schüler, Gäste und Serversysteme, Whiteboards, Access Point, Drucker und Other Devices – wird die horizontale Ausbreitung von Angriffen innerhalb des Netzwerks – wie im Fall von ARP-Spoofing – wirksam eingebremst. Die Segmentierung trägt dazu bei, privilegierte Bereiche vom allgemeinen Datenverkehr abzukoppeln und gezielte Sicherheitsrichtlinien durchzusetzen.
- **Sicheres WLAN durch Verschlüsselung und Zugangskontrolle:** Die Schwachstelle des unverschlüsselten Gäste-WLANs, wie in Kapitel 7.4 thematisiert, wird durch den Einsatz MAC-Filterung, Zugangsbeschränkungen gezielt adressiert. Die technische Realisierung dieser Maßnahme wurde bereits in Kapitel 7.1.4 dargestellt. Aus der Perspektive der Sicherheitspolitik ist sie von zentraler Bedeutung, um potenzielle Schwachstellen, die externe Angreifer ausnutzen könnten, wirksam zu schließen.
- **Monitoring und regelmäßige Analyse der Netzwerkaktivität:** Zusätzlich zu den technischen Maßnahmen wird ein kontinuierliches Netzwerkmonitoring etabliert. Ziel ist die frühzeitige Erkennung ungewöhnlicher Muster, etwa bei ARP-Spoofing oder Zugriffsversuchen. Durch die systematische Auswertung von Logdaten lassen sich Angriffe nicht nur rekonstruieren, sondern auch präventiv

erkennen. Die Verantwortung für die Überwachung und Analyse liegt beim IT-Verantwortlichen, der auf dieser Basis gezielte Maßnahmen einleiten kann.

9.1.2 Zugriffskontrollen und Authentifizierung

Gemäß Kapitel 7.3 stellen unbefugte Zugriffe, insbesondere durch BYOD-Geräte und unzureichend gesicherte Benutzerkonten, ein hohes Risiko dar. Die nachfolgenden Maßnahmen dienen der Regulierung und dem Schutz des Zugriffs auf kritische Systeme:

1. **Rollenbasierte Zugriffskontrolle (RBAC):** Das bestehende Active Directory (Kapitel 7.2) wird um eine rollenbasierte Zugriffskontrolle für Server, Netzwerkkomponenten und Drucker erweitert (Ferdous 2022). Die folgenden Rollen werden definiert :
    - **Administratoren:** Vollzugriff auf Server und Netzwerkeinstellungen (IT-Verantwortlicher).
    - **Lehrer**: Zugriff auf Lehrmaterialien, E-Klassenbuch, Shared-Ordner und Drucker.
    - **Bibliothek**: Zugriff auf Bibliothekdatenbank, Drucker, Shared-Ordner.
    - **Direktion:** Zugriff auf Schülerdaten, Lehrmaterialien, Shared-Ordner und Schülerdaten.
    - **Schüler:** Eingeschränkter Zugriff auf Bibliotheksdatenbank und Schüler-WLAN. Die Rechtevergabe wird regelmäßig überprüft, um unbefugte Zugriffe zu verhindern.
2. **Multi-Faktor-Authentifizierung (MFA):** Für privilegierte Nutzergruppen (Direktion, Bibliothek, IT-Administratoren) wird eine MFA eingeführt, die auf einer Kombination aus Passwort und einem zweiten Faktor (ESET Secure Authentication) basiert. Dies soll die kritische Systeme wie den HPE ProLiant MicroServer, aufbewahrte Schülerdaten und das E-Klassenbuch vor Konto-übernahmen, insbesondere durch Phishing-Angriffe schützen.
3. **BYOD-Richtlinie und Gerätekontrolle:** BYOD-Richtlinie wird vorerfasst, um die Nutzung privater Geräte im Schulnetzwerk sicher zu gestalten. Die Richtlinie umfasst folgende Aspekte:
    - **Registrierung:** Alle BYOD-Geräte müssen beim IT-Verantwortlichen registriert werden, wobei Geräteinformationen (z. B. MAC-Adresse, Gerätetyp) erfasst werden.
    - **Sicherheitsprüfung:** Bevor eine Netzwerkintegration stattfindet, müssen die betreffenden Geräte einer Sicherheitsprüfung unterzogen werden. Im Rahmen dieser Prüfung wird die Installation aktueller Antiviren-Software, die Installation aktueller Betriebssystem-Updates sowie das Vorhandensein nicht genehmigter Anwendungen überprüft.

- **Authentifizierung:** Der Cisco MERAKI MR32 Access Point wird durch den IT-Verantwortlichen mit der Funktion der Authentifizierung konfiguriert. Diese Authentifizierung erfolgt entweder über Google oder über einen gesponserten Gastzugang (Gäste).
- **Netzwerkbeschränkungen:** BYOD-Geräte werden ausschließlich in VLAN 4 (Schüler) oder VLAN 5 (Gäste) angebunden, mit eingeschränktem Zugriff auf interne Systeme wie Server oder Schüler-daten.
- **Nutzungsregeln:** Die Nutzung von BYOD-Geräten für die Speicherung sensibler Daten ist untersagt.
- **Sanktionen:** Bei Verstoß gegen die Richtlinie (unbefugte Software) wird der Netzwerkzugriff gesperrt, bis die Konformität wiederhergestellt ist. Die Richtlinie wird an alle Schüler, alle Lehrkräfte sowie die Schulleitung kommuniziert und wird als integraler Bestandteil in den Leitfaden für sichere IT-Nutzung aufgenommen.

4. **Druckmanagement mit Authentifizierung (MyQ X):** Im Rahmen der Implementierung des Druckmanagementsystems MyQ X erfolgt eine sichere Verwaltung der vorhandenen Druckerpool, welche die Modelle Kyocera, HP und Samsung umfasst. Das Programm MyQ X bietet folgende Funktionalitäten:
    - **Benutzerauthentifizierung:** Druckaufträge werden nur nach Authentifizierung am Drucker freigegeben, entweder über Benutzerkonten (via Active Directory) oder PIN-Codes, die individuell vergeben werden. Dies verhindert unbefugtes Drucken sensibler Dokumente wie Zeugnisse oder Verwaltungsunterlagen.
    - **Quotenkontrolle**: Schüler erhalten monatliche Druckkontingente (20 Seiten), um Missbrauch zu verhindern. Lehrkräfte und Direktion (ca. 1000 Seiten) haben höhere Kontingente basierend auf ihren Rollen.
    - **Protokollierung:** Das Programm MyQ X protokolliert sämtliche Druckaktivitäten, wobei die protokollierten Informationen die Benutzer, den Zeitpunkt und den Dokumententyp umfassen. Die Überprüfung dieser Logs erfolgt durch den IT-Verantwortlichen Quartalmäßig mit dem Ziel der Identifizierung ungewöhnlicher Aktivitäten wie übermäßige Druckaufträge.
    - **Datenschutz:** MyQ X löscht temporäre Druckaufträge automatisch nach 24 Stunden, um die Gefahr von Datenlecks zu reduzieren. Die Implementierung von MyQ X wurde im Mai durchgeführt, allerdings erfolgt die intensive Schulung der Lehrkräfte, der Schulleitung sowie des Bibliothekspersonals erst im Juli und September 2025.

Diese Maßnahmen stärken die Zugriffssicherheit und reduzieren das Risiko von Social-Engineering-Angriffen und unbefugten Zugriffen, die in Kapitel 7.3 als häufige Bedrohungen identifiziert wurden.

9.1.3 Schutz sensibler Daten

Die Vertraulichkeit, Integrität und Verfügbarkeit von sensiblen Daten, wie beispielsweise Schülerakten, Noten und Verwaltungsinformationen, ist ein zentrales Schutzgut, dessen Gewährleistung von großer Bedeutung ist. Die nachfolgenden Maßnahmen adressieren die in Kapitel 7.2 und 7.4 beschriebenen Schwächen in der Datenverschlüsselung und Backup-Strategie:

1. **Datenverschlüsselung**: Zu diesem Zweck wird der Einsatz einer FIPS 140-2-validierten 256-Bit-AES-Verschlüsselung durch ESET PROTECT empfohlen. Für die Verschlüsselung sensibler Daten auf dem HPE ProLiant MicroServer, Dryrekcja-PC01, Biblioteka-PC01, Nauczyciel-LP01, LP02 in der Oracle-Datenbank (Bibliothekdatenbank) sowie auf Netzlaufwerken wird FIPS 140-2 verwendet. Dabei wird ESET PROTECT ENCRYPTION als zentrale Verschlüsselungslösung eingesetzt und bietet folgende Features:
    - **Festplattenverschlüsselung:** Vollständige Verschlüsselung der Festplatten auf dem HPE ProLiant MicroServer und Dryrekcja-PC01, Biblioteka-PC01, Nauczyciel-LP01, LP02 um Daten bei physischem Diebstahl zu schützen.
    - **Datei- und Ordner-Verschlüsselung:** Sensible Dateien wie Schülerdaten, Noten, Zeugnisse werden individuell verschlüsselt, mit Zugriff nur für autorisierte Benutzer über RBAC (Kapitel 9.1.2). (Ferdous 2022)
    - **E-Mail-Schutz:** ESET PROTECT bietet auch einen E-Mail-Schutz, wodurch Datenlecks während der Übertragung vermieden werden können.
    - **Zentrales Management:** Der IT-Verantwortliche verwaltet Verschlüsselungsschlüssel über die ESET PROTECT Konsole, mit regelmäßiger Rotation der Schlüssel (alle sechs bis neun Monate) und Backup der Schlüssel auf einem sicheren, physisch getrennten Medium.
2. **Automatisierte und verschlüsselte Backups**: Die bestehende Backup-Strategie (tägliche vollständige Backups, Kapitel 7.2) wird durch eine automatisierte und verschlüsselte Lösung ergänzt. Backups werden auf einem dedizierten, physisch getrennten Speichermedium gespeichert. Die Backup-Daten werden mit AES-256 verschlüsselt, und ein dokumentierter Wiederherstellungsprozess wird erstellt, um im Falle von Ransomware-Angriffen eine schnelle Datenwiederherstellung zu gewährleisten.
3. **Unterbrechungsfreie Stromversorgung (USV):** Eine USV mit 1000 VA (Kapitel 7.1.4) wird für den HPE ProLiant MicroServer installiert, um Datenverluste bei

Stromausfällen zu verhindern. Dies erhöht die Verfügbarkeit kritischer Systeme und schützt vor physischen Schäden an der Hardware.

4. **Datenwiederherstellungsrichtlinien:** In diesem Zusammenhang wird ein dokumentiertes Verfahren zur Wiederherstellung kritischer Daten eingeführt, das regelmäßige Integritätsprüfungen und Wiederherstellungstests umfasst. Das Ziel besteht in der Sicherstellung der Verfügbarkeit im Notfall sowie der Schließung der in Kapitel 7.4 identifizierten Sicherheitslücke. Laut der vorliegenden Richtlinie sind Backups mindestens täglich durchzuführen, verschlüsselt zu speichern und an einem physisch getrennten Ort aufzubewahren. Zudem werden Zuständigkeiten klar geregelt und Notfallkontakte (IT-Verantwortlicher) definiert, um im Ernstfall eine schnelle Wiederherstellung zu garantieren.

Diese Maßnahmen gewährleisten den Schutz sensibler Daten vor unbefugtem Zugriff und Verlust, insbesondere in Szenarien wie Ransomware-Angriffen, die in Kapitel 7.3 als Bedrohung dokumentiert wurden.

9.2 Organisatorische Maßnahmen zur Erhöhung der IT-Sicherheit

Neben den technischen Aspekten spielen auch organisatorische Maßnahmen eine bedeutsame Rolle bei der Etablierung einer nachhaltigen Sicherheitskultur binnen der Schule. Diese Maßnahmen berücksichtigen die in Kapitel 7.2 und 7.4 identifizierten Schwachstellen, wie das mangelnde Sicherheitsbewusstsein und die unzureichenden Richtlinien, sowie stellen sicher, dass jegliche relevanten Aspekte eines umfassenden Sicherheitskonzepts berücksichtigt werden.

9.2.1 Sensibilisierung und Schulungen

Der Mangel an systematischen Schulungen für Lehrkräfte und Schüler (Kapitel 7.2) erhöht die Anfälligkeit für Phishing- und Social-Engineering-Angriffe. Das Ziel der folgenden Maßnahmen besteht in der Stärkung des Sicherheitsbewusstseins durch:

1. **Regelmäßige Awareness-Trainings:** Ab Mai 2025 werden halbjährige Schulungen für Lehrkräfte und Schüler eingeführt. Die Themen die diese Schulungen abdecken sind: Phishing-Erkennung, sichere Passworterstellung, verantwortungsvoller Umgang mit BYOD-Geräten und sichere Nutzung des Internets. Die Trainings werden in Zusammenarbeit mit einem internen IT-Verantwortlichen durchgeführt.
2. **Leitfaden für sichere Nutzung der IT-Systeme:** Gemäß der geltenden Bestimmungen verpflichten sich alle Nutzer der schulischen IT-Systeme zur sicheren Handhabung von Passwörtern (mit einer Mindestfrequenz von drei Monaten zur Änderung, dürfen nicht wiederverwendet oder auf unsicheren

Geräten gespeichert werden), zum sensiblen Umgang mit personenbezogenen Daten sowie zur Vorsicht bei der Nutzung von E-Mails und des Internets. Die Nutzung schulischer Geräte und Software ist ausschließlich nach erfolgter Freigabe durch den IT-Verantwortlichen erlaubt. Im Falle von Sicherheitsvorfällen und Auffälligkeiten ist eine unverzügliche Meldung an den IT-Verantwortlichen vorgesehen. Dabei wird das Ziel verfolgt, durch verantwortungsvolles Verhalten die IT-Sicherheit im Schulalltag langfristig zu stärken.

3. **BYOD-Nutzung:** Die Verwendung privater Geräte ist ausschließlich nach erfolgter Registrierung und einer Sicherheitsprüfung auf Viren sowie Updates im Schulnetzwerk gestattet. Die Speicherung sensibler Daten auf BYOD-Geräten ist nicht gestattet.
4. **Druckmanagement:** Die Ausführung von Druckaufträgen ist ausschließlich nach erfolgter Authentifizierung über MyQ X möglich. Für vertrauliche Dokumente gilt eine sofortige Abholpflicht.
5. **Sicherheitsvorfälle:** Verdächtige Aktivitäten wie Phishing-E-Mails, ungewöhnliches Systemverhalten müssen unverzüglich dem IT-Verantwortlichen gemeldet werden.
6. **Datenschutz:** Gemäß der geltenden Bestimmungen ist die Weitergabe sensibler Daten an Dritte strengstens untersagt. Die Nutzung von Cloud-Diensten für schulbezogene Daten ist ausschließlich genehmigten Diensten wie OneDrive oder Dropbox gestattet. Der Leitfaden sowie die gesamte Dokumentation werden bis spätestens Juli 2025 in gedruckter Form an die Direktion übermittelt und in Schulungen präsentiert. Des Weiteren erfolgt eine jährliche Aktualisierung dieser Leitfaden.

9.2.2 Transkription einer durchgeführten IT-Sicherheitsschulung zur Sensibilisierung von Lehrkräften

Titel: Transkription der Schulung zur Cybersicherheit für Lehrkräfte (Kurzfassung)

Datum: 17.05.2025

Ort: Polnische Schule Jan III. Sobieski in Wien

Leitung: Dariusz Zarosa (T)

Hinweis: Die Schulung wurde in polnischer Sprache durchgeführt. Dieses Dokument enthält eine deutsche Zusammenfassung des Transkripts, strukturiert und nummeriert für den Überblick.

Legende:

T = Trainer

L = Lehrkraft (diverse)

D = Direktorin (H. Kaczmarczyk)

003: Einführung

004: T: Guten Tag! Mein Name ist Dariusz Zarosa. Ich unterstütze das IT-Team unserer Schule und kümmere mich um digitale Sicherheit. Heute besprechen wir gemeinsam zentrale Aspekte wie Passwörter, mobile Geräte und E-Mail-Sicherheit.

005: T: Wie jede gute Präsentation hat auch diese eine Gliederung – sie dient uns als Leitfaden von Bedrohungen bis zur Reaktion auf Vorfälle.

006: Warum diese Schulung?

007: T: Zwischen Juni 2024 und April 2025 wurden 136 Sicherheitsvorfälle registriert – über 67 % konnten nicht abgewehrt werden. Hauptprobleme: Adware (PopUpGen), Phishing-Mails.

008: T: Antivirenprogramme und Firewalls genügen nicht. Es fehlen proaktive Maßnahmen wie Netzwerkschutz und Segmentierung. Laut DSGVO müssen Schülerdaten geschützt werden.

009: D: Müssen alle Datenschutzverletzungen gemeldet werden?

010: T: Ja, laut DSGVO ist jede Datenpanne meldepflichtig, auch unbeabsichtigte.

011: Passwörter – erste Verteidigungslinie

012: T: Ein starkes Passwort schützt E-Mail, Schulnetzwerk und digitale Klassenbücher.

013: T: Es sollte mindestens 12 Zeichen lang sein, Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Keine Namen oder Geburtstage!

014: L: Kann ich den Namen meines Kindes im Passwort verwenden?

015: T: Lieber nicht – zu leicht zu erraten. Beispiel: Statt 'ania123' → 'HerbataDla4!ZCynamonem'

016: Strategien zur Passwort-Merkfähigkeit

017: T: Starke Passwörter sind schwer zu merken – daher ein paar Tricks:

018: T: 1. Anfangsbuchstaben-Methode: 'Meine Oma backt den besten Kuchen...' → 'MobdbK!24'

019: T: 2. Kreative Sätze mit Symbolen: 'Kaffee um 7 ist mein Treibstoff' → 'Kaffee@7=Treibstoff'

020: T: 3. Visuelle Assoziationen: z. B. 'Grüne_Katze_99!'

021: T: 4. Sprachmix: z. B. 'IchMagPizza4Dinner!'

022: Passwortmanager und Praxistipps

023: T: Passwortmanager wie Bitwarden oder KeePassXC helfen, sichere Passwörter zu verwalten – ein starkes Hauptpasswort genügt.

024: L: Ist es nicht gefährlich, alle Passwörter an einem Ort zu speichern?

025: T: Nein, sofern ein starkes Masterpasswort und Zwei-Faktor-Authentifizierung verwendet werden.

026: T: Geben Sie keine Passwörter weiter. Schreiben Sie diese nicht auf Zettel. Bei Verdacht: Passwort ändern.

027: Mobile Geräte

028: T: Smartphones sind kleine Computer – mit Zugang zu E-Mail, Schulapps und sensiblen Daten.

029: T: Absicherung durch PIN, Fingerabdruck, Gesichtserkennung, Bildschirmsperre.

030: T: Kein öffentliches WLAN für Schulzugänge – stattdessen VPN nutzen. Nur Apps aus offiziellen Stores.

031: E-Mail-Sicherheit

032: T: Phishing ist der häufigste Angriffsweg – Mails, die täuschend echt aussehen.

033: T: Typische Merkmale: Zeitdruck, unbekannte Absender, seltsame Anhänge. Verdachtsfälle an IT melden.

034: Phishing-Demonstration

035: T: Wir schauen jetzt ein kurzes, lautloses Video, das einen realistischen Phishing-Angriff zeigt.

036: T: Video-Link: https://www.youtube.com/watch?v=sS3mZVCARZg

037: T: Eine Person erhält eine E-Mail, klickt auf den Link, gibt Daten ein – alles passiert schnell und wirkt harmlos.

038: T: Sie erkennt die falsche URL nicht und gibt ihr Passwort ein. Ein klassischer Fehler.

039: T: Im Video gibt die Person zusätzlich persönliche Daten an – Lieblingsband, Meinungen. Das zeigt, wie gefährlich Unwissenheit sein kann.

040: Analyse von Phishing-E-Mails

041: T: Wir analysieren zwei Beispiele – angeblich von Microsoft und PayPal.

042: T: Sie sehen professionell aus, doch der Link führt zu einer gefälschten Domain.

043: T: Die Absenderadresse endet nicht auf microsoft.com, sondern auf @email-records.com – verdächtig.

044: T: Die PayPal-Mail enthält eine ZIP-Datei und warnt vor verdächtigem Zugriff – ebenfalls eine Falle.

045: T: Gemeinsam prüften wir: Absenderadresse, Sprache, Druck, Anhangstyp, visuelle Abweichungen.

046: L: Kann man Phishing immer an der Mailadresse erkennen?

047: T: Leider nein. Im Zweifel: Nicht klicken – IT kontaktieren.

048: D: Was tun, wenn jemand bereits Daten eingegeben hat?

049: T: Keine Panik – sofort Passwort ändern, IT informieren, Beweise nicht löschen. Auch andere Konten absichern, falls Passwort mehrfach verwendet wurde.

050: Was Lehrkräfte beachten sollten

051: T: Keine Schülerdaten unverschlüsselt versenden. Keine Speicherung auf privaten Geräten.

052: T: Nur verschlüsselte, vertrauenswürdige USB-Sticks nutzen. Keine Login-Daten offenlassen. Keine Schülerfotos ohne Zustimmung.

053: Reaktion auf Vorfälle

054: T: Bei einem Vorfall: Gerät vom Netz trennen, Passwort ändern, Vorfall melden – Beweise sichern.

055: Zusammenfassung

056: T: Starke Passwörter, E-Mail-Vorsicht, Geräteschutz – das sind unsere drei Säulen.

057: T: Bei Unsicherheiten: lieber fragen. Gemeinsam schaffen wir ein sicheres digitales Umfeld.

058: T: Danke für Ihre Aufmerksamkeit. Bitte nehmen Sie am Quiz auf Quizizz teil: https://quizizz.com/admin/activity/classic/682d5ac855d225234d326b2b

9.2.3 Sicherheitsrichtlinien und Notfallpläne

Ergänzend zu den in Kapitel 9.1 dargestellten technischen Schutzmaßnahmen und der in den Kapiteln 9.2.1 bis 9.2.2 beschriebenen Sensibilisierung der Nutzer bilden verbindliche Richtlinien und ein klar strukturierter Notfallplan das organisatorische Rückgrat der IT-Sicherheitsarchitektur. Die Analyse in Kapitel 7.2 hat aufgezeigt, dass es einer unzureichenden Dokumentation von Richtlinien und nicht definierten Prozessen im Krisenfall mangelt. Zur Schließung vorhandener Sicherheitslücken wurde

ein übergreifendes Regelwerk in Form von IT-Sicherheitsrichtlinien erarbeitet, welches verbindliche Leitlinien für den täglichen IT-Betrieb sowie strukturierte Maßnahmen zur Reaktion auf Cybervorfälle definiert. Das Ziel dieser Richtlinien ist die Gewährleistung des sicheren Einsatzes sämtlicher IT-Ressourcen im schulischen Umfeld. Sie umfasst unter anderem folgende Punkte:

- **BYOD-Nutzung:** Registrierung und Sicherheitsprüfung aller mobilen Geräte vor Netzwerkintegration; Verpflichtung zur Installation aktueller Antivirensoftware und Betriebssystem-Updates.
- **Passwortvorgaben**: Mindestens 12 Zeichen, Kombination aus Groß und Kleinbuchstaben Zahlen und Sonderzeichen, empfohlene Methode für Password Erstellung – Kreative Sätze mit Symbolen, regelmäßige Passwortänderung alle drei Monate.
- **Druckregelungen:** Verpflichtende Authentifizierung über MyQ X für alle Druckaufträge.
- **Umgang mit mobilen Endgeräten:** Verbot der Installation nicht genehmigter Anwendungen auf Schulgeräten (Firewall Regel für die Anwendungen); Einschränkung des Zugriffs auf externe Cloud-Dienste außerhalb der genehmigten Plattformen (OneDrive, Dropbox).
- **Datenschutzrichtlinie:** Darüber hinaus wird eine spezifische Datenschutzrichtlinie als Anhang zur IT-Sicherheitsrichtlinie ergänzt, die folgende Vorgaben enthält:
    - **Datenminimierung:** Es werden nur die personenbezogenen Daten erhoben, die für den schulischen Zweck unbedingt erforderlich sind Name, Geburtsdatum, Noten für das E-Klassenbuch.
    - **Zweckbindung:** Daten dürfen nur für den ursprünglich angegebenen Zweck verwendet werden wie Verwaltung von Schülerakten, Erstellung von Zeugnissen und nicht für andere Zwecke weiterverarbeitet werden.
    - **Rechte der Betroffenen:** Laut der DSGVO steht Schüler, Eltern und Lehrer ein Recht auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung ihrer Daten zu. Zudem wird ein Prozess definiert, der die Bearbeitung von Anfragen innerhalb eines Zeitrahmens von 30 Tagen vorsieht (Europäische, Datenschutz-Grundverordnung (DSGVO), Art. 12–18 2018).
    - **Aufbewahrung und Löschung:** Im Kontext der Schule, die sensible Daten wie Schülerdaten, Bibliotheksdaten, E-Mail-Kommunikation und das E-Klassenbuch verarbeitet (Kapitel 8.1.5), sind folgende Aspekte zu beachten:
        - **Klassenbuch:** Das elektronische Klassenbuch muss 5 Jahre aufbewahrt werden (Rozporządzenie MEN 2017, § 22) (Minister Edukacji 2017). Danach müssen die Daten gelöscht oder archiviert werden, um die Vertraulichkeit gemäß Kapitel 8.1.2 zu gewährleisten.

- **Schülerdaten:** Daten wie Namen, Geburtsdaten oder Zeugnisse, Schülerbeurteilungsbögen müssen 50 Jahre aufbewahrt werden, um Ersatzzeugnisse ausstellen zu können (Minister Edukacji 2017). Dies ist relevant für die Verwaltung und den Schutz vor Datenlecks, die in Kapitel 7.3 dokumentiert wurden.
- **Lehrer- und Verwaltungsdaten:** Lohnabrechnungen (5 - 10 Jahre) (Marszałek Sejmu, Obwieszczenie z dnia 4 listopada 2022 r. w sprawie ogłoszenia jednolitego tekstu ustawy o rachunkowości 2023), Dienstzeugnisse und Sozial-versicherungsdaten müssen von 10 bis 50 Jahre (Minister Rodziny 2018), (R. P. Marszałek Sejmu 2023) aufbewahrt werden.
- **Gäste-WLAN-Zugangsdaten:** Im Zusammenhang mit einem gesponserten Gastzugang (Kapitel 8.1.10) könnten temporäre Zugangsdaten (Benutzerdaten, MAC-Adressen) erhoben werden. Diese sollten nach Ende des Gastbesuchs gemäß DSGVO gelöscht werden. (Europäische, Datenschutz-Grundverordnung (DSGVO), Art. 5 – Grundsätze 2018)
- Ein Löschprotokoll wird geführt, um die Einhaltung nachzuweisen.

Zur strukturierten Bewältigung von IT-Sicherheitsvorfällen wird in diesem Abschnitt auch ein Notfall- und Wiederanlaufplan ausgearbeitet. Dieser beschreibt konkrete Vorgehensweisen für typische Bedrohungsszenarien wie Datenverlust, Netzwerkausfälle oder Ransomware-Angriffe und umfasst die folgenden Maßnahmen:

- **Datenverlust:** Sofortige Isolation betroffener Systeme; Wiederherstellung aus verschlüsselten Backups gemäß dem dokumentierten Wiederherstellungsprozess (Kapitel 9.1.3); Benachrichtigung der Schulleitung innerhalb von 24 Stunden.
- **Netzwerkausfall:** Aktivierung eines Offline-Modus für das E-Klassenbuch; Nutzung von USV-gestützten Servern zur Aufrechterhaltung kritischer Funktionen; Zusammenarbeit mit einem externen Partner (Internetserviceprovider) zur Fehlerbehebung.
- **Ransomware-Angriff:** Abschaltung aller betroffenen Geräte; Analyse FortiGate-60F Firewall-Logs um die Angriffsvektoren zu identifizieren; Wiederherstellung der Daten aus Backup, falls möglich Meldung an die Behörden.
- **Datenschutzvorfälle:** Es wird ein Prozess etabliert, der die Meldung von Datenschutzvorfällen regelt und dabei die folgenden Schritte umfasst:
    - **Erkennung:** Identifikation eines Vorfalls (Datenleck, unbefugter Zugriff) durch Logs, Nutzermeldungen oder Audits.
    - **Bewertung:** Analyse des Vorfalls durch den IT-Verantwortlichen innerhalb von 24 Stunden, um den Umfang, die betroffenen Daten und die potenziellen Auswirkungen zu bestimmen.
    - **Kommunikation:** Gemäß Art. 34 DSGVO werden alle betroffenen Personen, wie beispielsweise Eltern, Schüler, Bibliothekare und die Direktion, im Falle

eines hohen Risikos durch ein Datenleck unverzüglich informiert (Europäische, Datenschutz-Grundverordnung (DSGVO), Art. 34 2018). Zur Sicher-stellung der angemessenen Vorbereitung des Personals finden ab Oktober halbjährlich Workshops in Form von regelmäßigen Simulationen von Notfallszenarien statt. Der Plan wird halbjährlich revidiert, um neue Bedrohungen und technische Innovationen zu berücksichtigen.

- **Patchmanagement-Prozess:** Die Einrichtung eines zentralen Patchmanagementprozesses gewährleistet, dass eine regelmäßige Distribution der neuesten Sicherheitsupdates für alle Geräte, einschließlich Server, PCs und Laptops, erfolgt. Der IT-Verantwortliche überwacht die Updates mit Hilfe von ESET PROTECT und dokumentiert deren Installation, damit die in Kapitel 7.4 identifizierte Schwachstelle veralteter Software behoben werden kann.

9.2.4 Physische Sicherheitsmaßnahmen

Die Analyse der bestehenden IT-Sicherheitslage offenbarte insbesondere im Bereich der physischen Zugangskontrollen signifikante Schwachstellen. Wie in Kapitel 7.2 bereits dargelegt, mangelt es derzeit an strukturierten Maßnahmen zur Zugangsbeschränkung in sensiblen Bereichen wie dem Lehrerzimmer oder der Schulbibliothek. Es konnte nachgewiesen werden, dass diese Lücke das Risiko unbefugter Zugriffe, von Datendiebstahl sowie von Manipulationshandlungen an IT-Infrastruktur und personenbezogenen Daten erhöht. (Alberts, et al. 2025)

Zur Minimierung von Risiken wird zunächst eine organisatorische Maßnahme implementiert, die den physikalischen Schutz dieser Räume verbessert. Konkret wird festgelegt, dass das Lehrerzimmer sowie die Bibliothek während unterrichtsfreier Zeiten und grundsätzlich bei Abwesenheit von Aufsichtspersonen verschlossen zu halten sind.

Diese Maßnahme dient nicht nur der Einhaltung grundlegender Datenschutzvorgaben, sondern auch der Gewährleistung eines kontrollierten physischen Zugangs zu IT-relevanten Bereichen der Schule. In diesem Zusammenhang ist es von großer Bedeutung, darauf hinzuweisen, dass organisatorische Schutzmaßnahmen in Bildungsinstitutionen, in denen IT-Geräte häufig für mehrere Personen gleichzeitig zugänglich sind und in denen zudem oft mehrere Personen gleichzeitig tätig sind, einen wesentlichen Bestandteil der Sicherheitsarchitektur darstellen. Darüber hinaus kann angemerkt werden, dass in einem weiteren Schritt die Einführung der Videoüberwachung unter Berücksichtigung datenschutzrechtlicher Rahmenbedingungen – geprüft werden sollte.

9.2.5 Einbindung Stakeholder

Die erfolgreiche Umsetzung eines Sicherheitskonzepts bedingt die aktive Einbindung sämtlicher relevanter Stakeholder, einschließlich Direktion, Lehrer, Schüler und Eltern,

um die Akzeptanz und Kooperation zu fördern (Alberts, et al. 2025). Dies wird durch folgende Maßnahmen sichergestellt:

- **Kommunikationsstrategie:** In diesem Zusammenhang wird eine schulbezogene Kommunikationsstrategie konzipiert, die darauf abzielt, alle relevanten Stakeholder an der Stärkung der Cybersicherheit zu beteiligen
- **Schüler:** Ab dem Monat Oktober werden Trainingsmaßnahmen in halbjährlichem Rhythmus durchgeführt, die darauf abzielen, das Interesse an der Thematik der IT-Sicherheit zu fördern. Es wurde zu dem beschlossen, dass quartalsweise ein "Cyber-Bulletin" in Form eines Aushangs veröffentlicht wird, welches über aktuelle Bedrohungen und entsprechende Gegenmaßnahmen, wie die Erkennung von Phishing E-Mails, informiert.
- **Lehrkräfte:** In periodischen Abständen werden Informationen vorübergehend über die WhatsApp-Gruppe, hinsichtlich Sicherheitsrichtlinien, den Leitfaden und Vorfallmeldungen versandt.
- **Direktion:** Vorgesehen ist, dass quartalsweise Berichte über aktuelle Vorfälle und Investitionsbedarfe an Direktion vorgelegt werden.

Darüber hinaus werden spezifische Schulungen für die Schulleitung sowie das Bibliothekspersonal eingeführt, um deren Rolle bei der Umsetzung und Unterstützung des Sicherheitskonzepts zu stärken. Im Rahmen dieser Schulungen werden unteranderem folgende Inhalte behandelt:

- Grundkenntnisse der Cybersicherheit im schulischen Kontext
- Handlungsleitfäden für die Reaktion auf Sicherheitsvorfälle
- Datenschutzgrundlagen und physische Schutzmaßnahmen
- Kommunikation in Krisensituationen
- Verantwortlichkeiten im Rahmen des internen Sicherheitsmanagements

Diese Maßnahmen zielen darauf ab, die Akzeptanz des Konzepts zu fördern und die in Kapitel 7.2 festgestellte mangelnde Sicherheitskultur durch eine enge Zusammenarbeit aller Beteiligten zu kompensieren.

9.2.6 Ressourcen Planung und Kosten

Erstellung eines umfassenden Sicherheitskonzepts erfordert die Berücksichtigung der finanziellen und personellen Ressourcen, die für die Umsetzung notwendig sind. Der nachfolgende Plan beinhaltet die geschätzten Kosten für die Jahre 2025/26 sowie die Lizenzierungskosten für das Jahr 2026/27.

Die Kosten, die im Rahmen der Umsetzung des praktischen Teils der Bachelorarbeit entstanden sind, wurden vom Autor dieser Arbeit getragen.

Maßnahme	Kategorie	Kosten (EUR)	von Schule getragen 2025/26 (EUR)	Kosten 2026/27 (EUR)
FortiGate-60F Firewall Lizenz (General überholt)	Hardware	€ 480,00	€ -	€ -
FortiGate-60F Firewall Lizenz 1 Jahr	Lizenz	€ 467,00	€ -	€ 467,00
Cisco 3750V2 Switch (General überholt)	Hardware	€ 150,00	€ -	€ -
Cisco 819G-4G-GA-K9 Router	Hardware	€ 160,00	€ -	€ -
Cisco MERAKI MR32 Access Point (General überholt)	Hardware	€ 150,00	€ -	€ -
Cisco MERAKI MR32 Cloud Lizenz MR-Enterprise	Lizenz	€ 80,00		
MyQ X Druckmanagementsystem (1 Jahr Testlizenz)	Lizenz	€ -	€ -	€ 1 500,00
ESET PROTECT (inkl. ENCRYPTION, 7 Nutzer im Jahr 2026 Erweiterung auf 20 Nutzer)	Software	€ 360,00	€ -	€ 860,00
USV (1000 VA)	Hardware	€ 100,00	€ -	
Jährliche Sicherheitsaudits (IT-Verantwortliche)	Dienstleistung	€ -	€ -	
Awareness-Trainings (halbjährlich, IT-Verantwortliche)	Dienstleistung	€ -	€ -	
Gesamt		**€ 1 947,00**	**€ -**	**€ 2 827,00**

Tabelle 40 Überblick über die Kosten 2025/26 und 2026/27

Die Allokation von Ressourcen aus der Tabelle erfolgt anhand des Prinzips der Priorisierung sicherheitskritischer Maßnahmen. Investitionen, die einen hohen Sicherheitsgewinn versprechen, wie beispielsweise die Einführung einer professionellen Firewall, die VLAN-Segmentierung sowie die Verschlüsselung sensibler Daten, werden dabei vorrangig umgesetzt. Die Verantwortung für die Umsetzung und die kontinuierliche technische Betreuung dieser Maßnahmen obliegt dem IT-Verantwortlichen der Schule. Zu seinen Aufgaben gehören die Konfiguration der Firewall, die Durchführung von Sicherheitsaudits, das Management des MyQ X – Drucksystems sowie das Patch-management.

Im Hinblick auf die langfristige Gewährleistung der Betriebsfähigkeit der Sicherheits-architektur werden gegenwärtig Gespräche mit der Schulleitung hinsichtlich geeigneter Finanzierungsmöglichkeiten geführt. Das Ziel besteht darin, ein zuverlässiges Modell zu entwickeln, das es der Schule ermöglicht, die laufenden Lizenzkosten – insbesondere ab dem Jahr 2026/27 – auch unter externer Unterstützung zu tragen. In diesem Kontext wird evaluiert, inwiefern Fördermittel seitens des ORPEG, des Elternvereins oder

alternativer nationaler Initiativen in Polen genutzt werden könnten, um die Infrastruktur finanziell abzusichern. Im Herbst 2025 werden der Schule eine detaillierte Kostenaufstellung sowie ein Vorschlag zur mittelfristigen Finanzierungsstrategie präsentiert.

9.3 Integration ausgewählten Aspekten aus Sicherheitsstandards (ISO/ BSI / NIST / Österreichisches Informationssicherheitshandbuch)

Die Realisierung eines umfassenden IT-Sicherheitskonzepts erfordert die Berücksichtigung zentraler Anforderungen internationaler Sicherheitsstandards, die über die Ergebnisse der OCTAVE-S Methode hinausgehen. Die vorliegende Analyse ergänzt die OCTAVE-Analyse insbesondere in den Bereichen strukturiertes Risiko-management, Sicherheitsfunktionen, technische und organisatorische Maßnahmen sowie regulatorische Mindeststandards. Im Folgenden werden diese Aspekte für die Polnische Schule Jan III Sobieski in Wien konkretisiert und in die Praxis integriert.

9.3.1 Strukturierter Risikomanagement (ISO/IEC 27001)

Obwohl in OCTAVE-S bereits eine Bedrohungsanalyse durchgeführt wird, wird im ISO/IEC 27001 ein fortlaufender, systematischer Risikomanagementprozess gefordert. Für den schulischen Kontext bedeutet dies:

- **Implementierung eines jährlichen Risikoreviews** an der Polnischen Schule Jan III Sobieski in Wien dient der systematischen Neubewertung und Priorisierung von IT-Risiken auf Grundlage aktueller Bedrohungen. Zu diesen zählen etwa die zunehmende BYOD-Nutzung durch Lehrkräfte. Darüber hinaus werden auch organisatorische Veränderungen im Schulbetrieb berücksichtigt. Gemäß der vorliegenden Informationen soll das Risikoreview-Protokoll folgende Inhalte umfassen: Ein Deckblatt mit dem Datum und den beteiligten Personen (Direktorin, der IT-Verantwortliche und Bibliothek Personal haben eine aktualisierte Liste der relevanten IT-Systeme (Server, Backup HDD, WLAN, Bibliothekdatenbank, E-Klassenbuch, private Endgeräte) anzufertigen. Des Weiteren ist eine Risikotabelle mit aktueller Bewertung der identifizierten Risiken zu erstellen. Darüber hinaus ist eine Übersicht über den Umsetzungsstand geplanter Sicherheitsmaßnahmen zu verfassen. Bei verbleibenden Restrisiken – etwa im Zusammenhang mit der privaten Gerätenutzung – ist eine dokumentierte Risikozulassung durch die Schulleitung erforderlich. Schließlich ist eine Liste offener Punkte und empfohlener Maßnahmen für das Folgejahr zu erstellen. (International Organization 2022)
- Im Rahmen des **Risikomanagementprozesses** ist es unerlässlich, dass die Schulleitung über die verbleibenden Restrisiken informiert wird und deren bewusste Akzeptanz dokumentiert. Dieses Vorgehen sollte insbesondere bei der

kontrollierten Nutzung privater Endgeräte (BYOD) durch Lehrer erfolgen. Gemäß der aktuellen Regelung ist die Nutzung privater Endgeräte wie Notebooks und Tablets durch das Lehrpersonal im Schuljahr 2024/25 gestattet. Dies gilt unter der Voraussetzung, dass die Geräte mit einem aktuellen Antivirenprogramm ausgestattet sind und dienstliche Daten ausschließlich über verschlüsselter E-Mail-Kommunikation verarbeitet/versendet werden. Obwohl dieses Vorgehen mit einem gewissen Restrisiko (bei Geräteverlust oder unsicheren WLAN-Verbindungen zu Hause) verbunden ist, hat die Schulleitung dieses Risiko nach Abwägung aller Faktoren akzeptiert. Diese Risiko kann künftig im IT-Risikoprotokoll dokumentiert werden. (International Organization 2022)

Diese Maßnahmen tragen zur Etablierung einer nachhaltigen Sicherheitskultur bei, die auf einem kontinuierlichen Verbesserungsprozess basiert.

9.3.2 Zuordnung Maßnahmen zu Sicherheitsfunktionen (NIST)

Zur Sicherstellung einer hohen Nachvollziehbarkeit, Priorisierung und Steuerung der IT-Sicherheitsmaßnahmen an der Polnischen Schule Jan III Sobieski in Wien erfolgt eine strukturierte Zuordnung der Maßnahmen zu den fünf Funktionsbereichen des NIST Cybersecurity Frameworks. In der vorliegenden Untersuchung wurden lediglich drei Aspekte berücksichtigt, da die übrigen im Rahmen von OCTAVE-S abgedeckt wurden:

1. **Identifizieren (Identify):** In diesem Bereich wird Erstellung und laufende Pflege eines IT-Asset-Verzeichnisses stattfinden. Es wird eine Liste mit eingesetzte Hardware – Schulserver, Whiteboard, Projetkoren, Backup-System, Access Point, Lehrerlaptops – Softwarelösungen – Office, Microsoft Teams, MOL NET von Firma Vulcan, Digitale Signatur Software – sowie digitale Dienste wie das elektronische Klassenbuch umfasst. Die Verantwortung für die Erstellung und Aktualisierung des Verzeichnisses liegt beim IT-Verantwortlichen und wird im Rahmen des jährlichen Risikoreviews durchgeführt. Darüber hinaus erfolgt eine Kategorisierung der in der Schule verarbeiteten Informationen nach ihrem jeweiligen Schutzbedarf:
    a. besonders schützenswerte personenbezogene Daten (Schülerdaten, Leistungsbeurteilungen),
    b. vertrauliche Verwaltungsdaten (Budget, Mitarbeiterinformationen),
    c. öffentlich zugängliche Inhalte (Webseite, allgemeine Informationen). (National Institute of Standards and Technology 2024)
2. **Erkennen (Detect):** Diese umfasst die Protokollierung und regelmäßige Auswertung administrativer Zugriffe auf sicherheitskritische Systeme wie den Schulserver, das E-Klassenbuch sowie den MERAKI Access Point und die Bibliothekdatenbank. Die Analyse der Logdateien hat sich insbesondere auf die Identifizierung ungewöhnlicher Zugriffsmuster zu fokussieren. Als Indikatoren

für derartige Muster sind insbesondere unübliche Zeitpunkte für Zugriffe auf die Daten, wie beispielsweise der Login außerhalb der Unterrichtszeiten (Di - Sa nach 20 Uhr), sowie wiederholte Fehlversuche zu werten. Die Verantwortung hinsichtlich der Kontrolle obliegt dem internen IT-Verantwortlichen, während die Wahrnehmung eventueller Auffälligkeiten an die Direktion delegiert wird. (National Institute of Standards and Technology 2024)

3. **Reagieren (Respond):** Eine weitere Aufgabe besteht in der Definition und Dokumentation einer Eskalationskette für sicherheitsrelevante Vorfälle wie Datenverlust, Virenbefall oder unbefugten Zugriff. Im Falle eines Vorfalls wird folgende Reihenfolge befolgt:
    a. Die Meldung an den IT-Verantwortlichen der Schule ist obligatorisch.
    b. Die Direktorin ist unverzüglich zu informieren.
    c. Zudem ist im Bedarfsfall eine Kontaktaufnahme mit einem externen Datenschutzbeauftragten (bspw. ORPEG) zur Prüfung von Meldepflichten.
    d. Im Bedarfsfall ist eine Information der betroffenen Personen (Eltern, Lehrer Schüler)unvermeidlich. (National Institute of Standards and Technology 2024)

9.3.3 Berücksichtigung von Mindeststandards (BSI)

Der BSI IT-Grundschutz stellt auch für kleinere Organisationen wie Schulen konkrete Umsetzungshilfen bereit. Das Sicherheitskonzept der Schule wird durch folgende Aspekte ergänzt:

1. **Minimalbenutzerkonzept an der Polnischen Schule Jan III Sobieski in Wien**
   An der Polnischen Schule Jan III Sobieski erfolgte die Implementierung eines entsprechenden Konzepts, welches die standardmäßige Einrichtung von Benutzern Konten für das Lehrpersonal und das Verwaltungspersonal ohne Administratorrechte vorsieht. Diese Einschränkung findet Anwendung auf sämtliche Schulgeräte, insbesondere jedoch auf Personal Computer in Lehrerzimmern, Verwaltungsbüros und Unterrichtsräumen. Diese Maßnahme zielt darauf ab, die Installation unerwünschter Software zu unterbinden und die Manipulation sicherheitsrelevanter Systemeinstellungen ohne entsprechende Freigabe zu verhindern.
   Für administrative Aufgaben, wie beispielsweise die Installation von Treibern oder Softwareupdates, werden benutzerdefinierte Administratorkonten bereitgestellt, auf die ausschließlich der IT-Verantwortliche Zugriff hat. Temporäre Vergaben von erhöhten Rechten erfolgen ausschließlich nach dokumentierter Genehmigung und werden im Protokollsystem vermerkt.
   Darüber hinaus wird die Nutzung privater Endgeräte von Lehrkräften bzw. Schüler (BYOD) eingeschränkt, indem eine Verbindung mit internen Netzlaufwerken, dem Server oder sensiblen Applikationen wie dem E-Klassen-

buch nicht gestattet ist. Der Zugang erfolgt ausschließlich über das schulische VLAN 3 (Lehrer) oder VLAN 4 (Schüler) mit Internetzugriff, jedoch ohne Zugriff auf interne Ressourcen. (Bundesamt für Sicherheit in der Informationstechnik 2017)

Dieses Konzept unterliegt einer jährlichen Überprüfung im Rahmen des Risikoreviews (vgl. Kapitel 9.3.1) mit dem Ziel der Anpassung an neue technische Entwicklungen oder organisatorische Änderungen, sofern diese als erforderlich erachtet werden.

2. **Regelung zur USB-Stick-Nutzung**

   Wechselmedien wie USB-Sticks sind ein häufig genutztes, jedoch auch kritisches Element in der IT-Infrastruktur. Einerseits können sie Schadsoftware einschleusen, andererseits ermöglichen sie unbemerkten Datenabfluss. Mit Hilfe von BSI IT-Grundschutz wurde an der Schule eine Weisung zur sicheren Nutzung von USB-Sticks verfasst, die Folgende Aspekte berücksichtigt:

   - Die zentralen Schulgeräte, primär in der Bibliothek, Direktion oder im Serverraum, sind bereits so konfiguriert, dass USB-Ports entweder vollständig deaktiviert oder lediglich mit dem Passwort des Administrators zugänglich sind.
   - Die Nutzung von USB-Sticks durch Lehrkräfte in Schul-Laptops ist nur dann gestattet, wenn diese als vertrauenswürdig Quelle eingestuft werden und auf dem Endgerät ein aktueller Virenschutz installiert ist. Im Rahmen des halbjährigen Awareness Trainings erfolgt eine Sensibilisierung zu dem Thema.
   - Die Zulässigkeit der USB-Nutzung beschränkt sich auf:
     - Nutzung zur Präsentation im Unterricht,
     - Datentransfer für schulische Veranstaltungen (Eltern-abende).
   - Für datenschutzsensible Inhalte, insbesondere personenbezogene Schülerdaten, ist die Nutzung von USB-Sticks untersagt. Hier sind ausschließlich sichere Cloudlösungen wie OneDrive oder Dopbox empfohlen. (Bundesamt für Sicherheit in der Informationstechnik 2017)

9.3.4 Berücksichtigung von österreichische Empfehlungen

Neben den internationalen Standards ISO/IEC 27001 und NIST Cybersecurity Framework bieten auch die österreichischen Empfehlungen aus dem "Sicherheitshandbuch" wichtige Maßnahmen zur Stärkung der IT-Sicherheit der Polnischen Schule Jan III Sobieski in Wien, die direkt in der Praxis umgesetzt werden können. Im Folgenden werden ausgewählte Aspekte erörtert, die in der bisherigen Sicherheitsplanung der Polnischen Schule Jan III Sobieski in Wien noch nicht berücksichtigt wurden, jedoch für den konkreten Schulbetrieb von Bedeutung sind:

1. **Verwendung mobile Geräte**

Für den sicheren Umgang mit mobilen IT-Geräten wie Lehrer-Laptops, Tablets und Handys soll eine Regelung erstellt werden, die ab dem neuen Schuljahr angewendet werden soll. Sie sollte für alle Anwender solcher Geräte festgelegt werden und folgendes beinhalten:

- Geräte dürfen nur von berechtigten Personen verwendet werden.
- Geräte sind bei Transport außerhalb des Schulgebäudes passwortgeschützt und nach Möglichkeit verschlüsselt aufzubewahren.
- keine Aufbewahrung in Fahrzeugen, insbesondere nicht sichtbar und unbeaufsichtigt.
- Bei Verlust oder Diebstahl ist unverzüglich der IT-Verantwortliche zu informieren. (Bundeskanzleramt Österreich 2023)

2. **Einweisung von Direktion und Bibliothekpersonal in grundlegende Sicherheitsabläufe**

   Die Direktion und das Bibliothekspersonal spielen eine zentrale Rolle im Schulalltag, auch außerhalb der Präsenzzeiten von technischem Personal. Um im Falle physischer Sicherheitsvorfälle angemessen reagieren zu können, wird eine strukturierte Einweisung in sicherheitsrelevante Abläufe eingeführt. Diese erfolgt jährlich zu Schuljahresbeginn sowie bei Personalwechsel durch den IT-Verantwortlichen.

   Folgende Bereiche sind Inhalt der Einweisung:

   a) Verhalten bei physischem Einbruch beinhaltet:
      - Sofortige Alarmierung der Polizei über Notruf 133, ohne selbständige Sicherungsversuche.
      - Keine Berührung verdächtiger Gegenstände oder Manipulationen an Türen, Fenstern oder IT-Geräten.
      - Räumung von folgenden Räumen: Bibliothek, Direktion, Lehrer-raum sowie Klassenzimmern nach Feststellung eines Einbruchs.
      - Warten auf das Eintreffen der Polizei außerhalb des Gebäudes.
      - Meldung an die IT-Verantwortlichen und Erstellung eines kurzen schriftlichen Bericht über dem Vorfall durch die Direktion.

   b) Vorgehen bei Diebstahl von IT-Geräten
      - Sofortige Meldung an die Direktion (falls Bibliothek betroffen) oder umgekehrt.
      - Falls möglich: Dokumentation der Seriennummer und Geräte-eigenschaften (Nauczyciel LP01, Lenovo und Windows-Kontoname).
      - Information an IT-Verantwortlichen zur:
        - Sperrung der Benutzerkonten
        - Prüfung etwaiger Datenverluste (Schülerdaten, Zugänge),

        - Einleitung Nachbearbeitung (Protokollierung).
    - Meldung an die Versicherung, falls erforderlich.

c) Meldung verdächtiger Personen oder Aktivitäten

    - Jede verdächtige bemerkte Person im Bereich Lehrerraum, Bibliothek oder Direktion außerhalb der Öffnungszeiten oder durch unbefugte Personen ist zu melden.
    - In keinem Fall die Person konfrontieren

d) Notfallkontaktübersicht

    - Ein aktualisiertes Notfallblatt mit allen wichtigen Kontakten wird im Sekretariat, der Direktion und der Bibliothek sichtbar und in digitaler Form hinterlegt. Es enthält:
        - Polizei / Feuerwehr / Rettung (133/122/144)
        - Direktion (inkl. Vertretung)
        - Nummer zum IT-Verantwortlichen

Damit neue technische oder organisatorische Entwicklungen berücksichtigt werden, werden die Inhalte dieser Einweisung jährlich evaluiert und aktualisiert (Bundeskanzleramt Österreich 2023). Neue Mitarbeiter der polnischen Schule werden in einem kurzen Einweisungs-gespräch mit den wichtigsten Informationen von der Direktion versorgt.

3. Erweiterung zur Verwendung mobile Geräte

Da viele Lehrer private Smartphones oder Tablets am Arbeitsplatz nutzen, braucht es klare Nutzungsempfehlungen seitens der IT-Verantwortlichen. Die Polnische Schule orientiert sich dabei an folgenden österreichischen Empfehlungen:

- Die dienstliche Nutzung privater Geräte ist ohne Mobile Device Management (MDM) untersagt.
- Die Verwendung von nicht abgesicherten Messenger-Diensten (WhatsApp) zur Übermittlung sensibler Schülerdaten ist verboten.
- Alternative Kanäle für Kommunikation werden noch geprüft und müssen mit ORPEG konsultiert werden, da eventuell die Module des bestehenden E-Klassenbuchs um eine solche Funktionalität erweitert werden können (in Gespräch mit Direktion). (Bundeskanzleramt Österreich 2023)

Lehrkräfte bekommen zu Beginn des neuen Schuljahres ein Informationsblatt zur datenschutzkonformen Kommunikation. Ab dann wird die Einhaltung dieser Regelungen auch im Rahmen der regel-mäßigen IT-Checks überprüft.

10. Umsetzungsplan und Evaluation der Maßnahmen

Nach der Konzeptionsphase in Kapitel 9 widmet sich dieses Kapitel der Umsetzung und Evaluation der entwickelten Maßnahmen im realen Schulbetrieb der Polnischen Schule Jan III Sobieski. Die Umsetzung der meisten vorgeschlagenen Schutzmechanismen erfolgte zwischen dem 07.04.2025 und dem 18.05.2025 unter realistischen Bedingungen. Anschließend wurden sie getestet und hinsichtlich ihrer Wirksamkeit analysiert. Die Ergebnisse dienen dazu, konkrete Erkenntnisse über die Effektivität des IT-Sicherheitskonzepts zu gewinnen, Optimierungspotenziale zu identifizieren und zu überprüfen, ob das zentrale Projektziel – die Reduzierung von Cyberangriffen um 50 % – erreicht wurde. Der Prozess umfasst eine strukturierte Planung, eine umfassende Bewertung der Wirksamkeit anhand valider Daten und die kontinuierliche Überwachung und Verbesserung.

10.1 Planung der Umsetzung

Die fortschreitende Digitalisierung bietet Bildungseinrichtungen ein breites Spektrum an Möglichkeiten, darunter die Integration digital unterstützter Lehrmethoden, den Einsatz moderner Lernplattformen sowie die Förderung kollaborativer virtueller Lernumgebungen. Gleichzeitig sind mit der Nutzung dieser Technologie Herausforderungen verbunden, insbesondere im Bereich der IT-Sicherheit. Schulen sind als Institutionen dafür zuständig, sensible Daten von Schüler, Lehrern und Verwaltungsmitarbeitenden zu verwalten. Dies macht sie zu einem attraktiven Ziel für Cyberangriffe. Für Bildungseinrichtungen, die über begrenzte finanzielle und personelle Ressourcen verfügen, gestaltet sich die Entwicklung eines umfassenden IT-Sicherheitskonzepts als komplexe Aufgabe. Sie erfordert eine strategische Planung technischer, organisatorischer und personeller Maßnahmen.

Im Rahmen der Vorbereitung der Implementierung eines IT-Sicherheitskonzepts wurde im Juni 2024 eine systematische Erhebung sicherheitsrelevanter IT-Vorfälle an der Polnischen Schule Jan III Sobieski in Wien durchgeführt. In der vorliegenden Untersuchung wurden 63 Vorfälle dokumentiert, die Schwachstellen in der bestehenden IT-Infrastruktur sowie im Umgang mit sicherheitskritischen Szenarien aufzeigten. Die vorliegende Analyse diente als Fundament für die Erstellung eines strukturierten IT-Sicherheitskonzepts, welches in fünf Phasen unterteilt ist. Das Ziel dieses Konzepts besteht in der Gewährleistung der Akzeptanz im schulischen Umfeld sowie der Sicherstellung eines reibungslosen Schulbetriebs. Die Implementierung der Maßnahmen ist für einen Zeitraum von sieben Monaten – von März bis September 2025 – vorgesehen.

Die Planung der Umsetzung basiert auf einem fünfphasigen Implementierungsmodell, das eine schrittweise Einführung der Sicherheitsmaßnahmen vorsieht. In der vorliegenden Tabelle 41 wird eine strukturierte Übersicht über diese Projektphasen präsentiert, inklusive der jeweiligen Zeiträume. Diese Zeiträume stellen zugleich die

Basis für die Visualisierung dar, welche den zeitlichen Verlauf der Implementierung des IT-Sicherheitskonzepts veranschaulicht.

Phase	Bezeichnung	Zeitraum	Status
1	Sofortmaßnahmen & Risikoanalyse (OCTAVE-S)	März – April 2025	abgeschlossen
2	Netzwerksegmentierung & Backup	April – Mai 2025	abgeschlossen
3	Organisatorische Maßnahmen	Mai – September 2025	Großteils umgesetzt
4	Abschlussanalyse & Wirksamkeitskontrolle	April – Mai 2025	abgeschlossen
5	Monitoring, Nutzerfeedback und Schulung	Mai – September 2025	Großteils umgesetzt

Tabelle 41 Überblick über die fünf Phasen der Umsetzung

Die Abbildung 13 veranschaulicht den zeitlichen Ablauf der fünf zentralen Phasen der Umsetzung des IT-Sicherheitskonzepts an der Polnischen Schule Jan III Sobieski in Wien. Die Projektabfolge, -dauer sowie zeitliche Überlappungen der einzelnen Projektabschnitte und Maßnahmen von März 2025 bis Ende September 2025 werden in Form eines Gantt-Diagramms dargestellt.

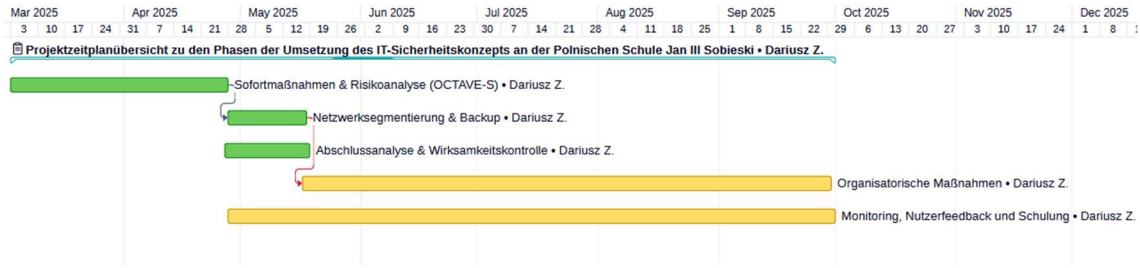

Abbildung 13 Projektzeitplanübersicht zu den Phasen der Umsetzung des IT-Sicherheitskonzepts an der Polnischen Schule Jan III Sobieski.

Die grünen Balken markieren bereits vollständig abgeschlossene Phasen:

- **Phase 1:** Die Sofortmaßnahmen sowie die initiale Risikoanalyse gemäß OCTAVE-S wurden im März und April 2025 vollständig durchgeführt.
- **Phase 2:** Die technische Umsetzung der Netzwerksegmentierung und die Einrichtung von Backups erfolgten unmittelbar danach im Zeitraum April bis Mai 2025.
- **Phase 4:** Die Abschlussanalyse und eine erste Evaluation der Wirksamkeit wurden parallel zur Phase 2 bereits im Mai 2025 abgeschlossen.

Die orangefarbenen Balken zeigen Maßnahmen an, die größtenteils umgesetzt sind, bei denen jedoch vereinzelte Restarbeiten oder Optimierungen noch ausstehen:

- **Phase 3** wurden Schulungen und Sensibilisierungsmaßnahmen durchgeführt sowie der erste Entwurf für die IT-Sicherheitsrichtlinie erstellt. Einige dieser Richtlinien, insbesondere zu den Themen BYOD-Nutzung, Passwortsicherheit

und USB-Gebrauch, wurden von der Schulleitung jedoch nur partiell freigegeben. Die Einführung der verbindlichen Sicherheitsrichtlinien erfolgt daher erst zum Beginn des Schuljahres 2025/26 im September 2025.

- In der **fünften Phase** wurde eine dreiwöchige Beobachtungsperiode (27.04. – 18.05.2025) durchgeführt und abgeschlossen. Im Rahmen der Untersuchung wurde die Wirksamkeit unter regulären Bedingungen eingeführten Sicherheitsmaßnahmen überprüft. Allerdings ist für eine verlässliche Evaluation der Resilienz der IT-Architektur unter variierenden Belastungsszenarien (wie beispielsweise Prüfungszeiten oder Elternsprechtage) eine Verlängerung des Monitorings bis Herbst 2025 vorgesehen

10.2 Umsetzung des Sicherheitskonzepts in Schulbetrieb

Die Implementierung des Sicherheitskonzepts wurde gemäß der in Kapitel 10.1 beschriebenen Phasenstruktur vorgenommen und ist in Abbildung 14 visuell dargestellt.

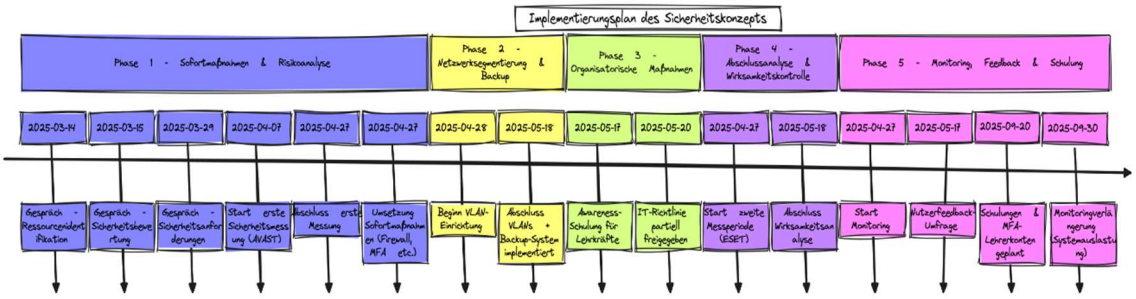

Abbildung 14 Implementierungsplan des Sicherheitskonzept

Die nachfolgenden Ausführungen erläutern die wesentlichen Maßnahmen und deren Umsetzung in Bezug auf die fünf Phasen des Sicherheitskonzepts:

Phase 1: Sofortmaßnahmen & Risikoanalyse (März – April 2025)

Im Zeitraum vom 14. bis zum 29. März 2025 wurden drei geplante Gespräche zwischen der Direktion, die Bibliothekarin/Lehrervertreterin, dem IT-Verantwortlichen durchgeführt. Diese dienten der Identifikation organisatorischer Ressourcen (14.03.), der Bewertung bestehender Sicherheitsmaßnahmen (15.03.) sowie der Festlegung konkreter Sicherheitsanforderungen (29.04.) (vgl. Kapitel 8).

Parallel dazu wurde vom 07.04. bis zum 27.04.2025 die erste Messung der sicherheitsrelevanten Vorfälle mithilfe von AVAST durchgeführt. Ausgehend von dieser Beobachtung wurden spätere Vergleiche durchgeführt. Basierend auf diesen Erkenntnissen wurden folgende Sofortmaßnahmen umgesetzt:

- Austausch veralteter Hardware und Einführung einer FortiGate-60F Firewall mit IDS/IPS-Funktionen,
- Erneuerung der Netzwerkstruktur durch Cisco MERAKI MR32 Access Points,

- Einrichtung der SSIDs: PLS-Lehrer, PLS-Schüler, PLS-Gäste, PLS-Whiteboard mit limitiertem Zugang,
- Einführung der Druckmanagementlösung MyQ X,
- Umsetzung der Multi-Faktor-Authentifizierung (MFA) für Direktion, Bibliothek und IT-Administratorenkonten.

Phase 2: Netzwerksegmentierung & Backup (April – Mai 2025)

Die Realisierung dieser Phase wurde zwischen dem 28. April und dem 18. Mai 2025 abgeschlossen. Im Zuge dessen erfolgte die Einrichtung von VLANs für acht unterschiedliche Nutzergruppen, darunter Lehrer, Schüler, Gäste, Server, Drucker, PCs, Whiteboards und sonstige Geräte. Die Implementierung dieser VLANs diente der Trennung der Netzkommunikation sowie der gezielten Durchsetzung von Sicherheitsrichtlinien. Die Implementierung eines dreifachen Backup-Systems stellt eine wesentliche Ergänzung dar:

- zwei interne Festplatten.
- eine externe verschlüsselte Festplatte (die in der Schule Breits vorhanden war),
- tägliche inkrementelle und wöchentliche vollständige Backups.

Phase 3: Organisatorische Maßnahmen (Mai – September 2025)

Am 17. Mai 2025 wurde Awareness-Schulung für Lehrer durchgeführt, die sich mit den Themen Phishing, Passwortsicherheit und mobile Geräte auseinandersetzte. Zudem wurde die IT-Sicherheitsrichtlinie konzipiert, jedoch lediglich partiell durch die Direktion freigegeben. Die vollständige Umsetzung der Richtlinie ist für September 2025 vorgesehen. Im Folgenden werden bereits umgesetzte Bestandteile aufgeführt:

- verbindliche Passwortanforderungen für Lehrer, Direktion, Bibliothek
- sichere Nutzung von USB-Sticks in Direktion und Bibliothek,
- Sichere Nutzung der IT-Systeme
- Verhalten im Falle eines Phishing-Angriffs

Phase 4: Abschlussanalyse & Wirksamkeitskontrolle (April – Mai 2025)

Zwischen dem 27. April und dem 18. Mai 2025 wurde eine zweite Messperiode für IT-Sicherheitsvorfälle festgesetzt und unter Einsatz von ESET PROTECT durchgeführt. Die Resultate der Untersuchung lassen sich wie folgt zusammenfassen:

- Rückgang sicherheitsrelevanter Ereignisse von 63 (Basis Juni 2024) auf 22 (Messung April/Mai 2025),
- vollständige automatische Bereinigung aller Bedrohungen,
- Verbesserung von 65 %,

Phase 5: Monitoring, Nutzerfeedback & Schulung (Mai – September 2025)

Die dreiwöchige Monitoring-Phase (27.04. – 18.05.) ergab eine klare Verbesserung der Sicherheitslage. Für eine fundierte Bewertung bei hoher Systemauslastung

(z. B. Prüfungszeiten) wird das Monitoring bis Oktober 2025 fortgesetzt. Für September 2025 geplant:

- Einführung der MFA für Lehrerkonten,
- vertiefende Schulungen für MyQ X.

Ergänzend zur technischen Evaluation wurde im Rahmen der Phase 5 auch die Nutzerperspektive berücksichtigt. Zu diesem Zweck wurde am 17. Mai 2025 eine anonyme Umfrage durchgeführt, die wertvolle Rückmeldungen zur Akzeptanz der Umsetzungen bzw. Awareness Training lieferte:

- 70 % der Teilnehmenden Lehrer empfand das Awareness-Training als besonders hilfreich bei der Erkennung sicherheitsrelevanter Bedrohungen wie Phishing.
- 70 % empfinden MyQ X als technisch anspruchsvoll.
- 80 % berichteten von keiner Einschränkung im Schulbetrieb während Implementierung der technischen Maßnahmen.

Darüber hinaus wird der IT-Verantwortliche künftig vierteljährlich CERT- und herstellerbasierte Sicherheitsberichte erstellen. Ferner befindet sich die Integration eines zentralen Log-Systems für FortiGate und ESET in Vorbereitung, um sicherheitsrelevante Ereignisse noch präziser analysieren zu können.

10.3 Bewertung der Umsetzung und Wirksamkeit

In diesem Subkapitel erfolgt eine Evaluierung der Wirksamkeit der implementierten IT-Sicherheitsmaßnahmen an der Polnischen Schule Jan III Sobieski in Wien. In diesem Kontext wird der Fokus auf die Evaluierung der Effektivität des Sicherheitskonzepts implementierten technischen und organisatorischen Maßnahmen gelegt um deren Beitrag zu einer nachweisbaren Verbesserung der Sicherheitslage bestimmen zu können. Zu diesem Zweck werden verschiedene quantitative und qualitative Indikatoren herangezogen, darunter die Entwicklung sicherheitsrelevanter Vorfälle, die Ergebnisse systematischer Schwachstellenscans sowie die Rückmeldungen der Nutzer im Rahmen einer strukturierten Umfrage. Die Analyse wird durch die Auswertung eines Penetrationstests ergänzt, der unter realitätsnahen Bedingungen durchgeführt wurde. Die nachfolgenden Abschnitte liefern eine empirisch fundierte Grundlage zur Einschätzung der Effektivität und Akzeptanz der implementierten Schutzmaßnahmen.

10.3.1 Bewertung der Umsetzung und Wirksamkeit

Zur Bewertung der Wirksamkeit der eingeführten IT-Sicherheitsmaßnahmen wurde eine Analyse zweier Beobachtungsperioden miteinander verglichen. Der Fokus lag dabei auf der Häufigkeit und Art der registrierten Sicherheitsvorfälle vor und nach der Umsetzung der technischen Teil des Konzepts.

In der ersten Beobachtungsperiode (BP1) vom 07.04. bis 27.04.2025 wurden an der Polnischen Schule Jan III Sobieski insgesamt 73 sicherheitsrelevante Vorfälle von AVAST registriert, was einem Durchschnitt von mehr als 24 Vorfällen pro Woche entspricht. Zu den erfassten Bedrohungen zählten unter anderem Phishing-Versuche, Schadsoftware (Malware) und gezielte Netzwerkangriffe wie ARP-Spoofing. Rund 68 % dieser Vorfälle konnten vom zuvor eingesetzten Antivirenprogramm nicht erfolgreich erkannt oder abgewehrt werden. In der Periode (BP2) vom 27.04. bis zum 18. 05. 2025 ergab der ESET PROTECT-Sicherheitsbericht ein deutlich verbessertes Bild. Insgesamt wurden in BP2 – 22 sicherheitsrelevante Ereignisse identifiziert, das sind rund 7,3 pro Woche. Dabei wurden sämtliche Bedrohungen automatisch erkannt und vollständig durch ESET PROTECT bereinigt.

Eine detaillierte Übersicht über die identifizierten Bedrohungen ist in Tabelle 42 zu finden, während Abbildung 15 eine visuelle Darstellung der Tagesübersicht über Bedrohungen bereitstellt.

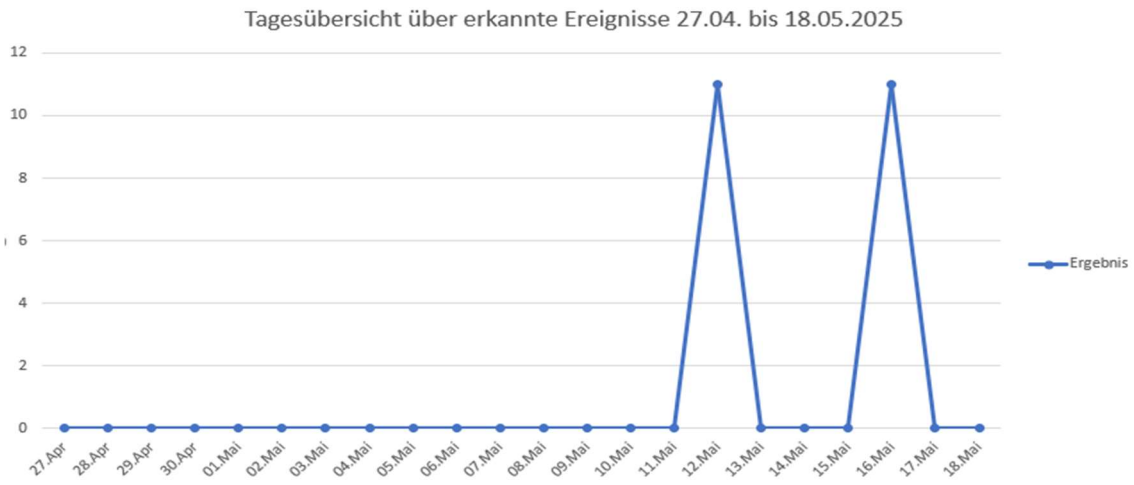

Abbildung 15 Tagesübersicht über Bedrohungen von 27.04. bis 18.05.2025

Ereignisname	Anzahl
Win32/Toolbar.Conduit	2
Win32/Toolbar.Montiera.AL	1
Win32/Toolbar.Montiera.B	1
Win32/Toolbar.Visicom.A	2
Win32/Toolbar.Visicom.B	1
Win32/Toolbar.Visicom.C	1
Win32/uTorrent.C	2
Win32/Visicom.A	4
Win32/Visicom.C	2
Win64/Pokki.A	2

Win64/Pokki.B	3
Win64/Pokki.C	1

Tabelle 42 Häufigste Bedrohungen vom 27.04. bis 18.05.2025

Bei den identifizierten IT-Sicherheitsmaßnahmen wurde die Anzahl der registrierten Sicherheitsvorfälle vor und nach der Implementierung verglichen, um deren Effektivität zu bewerten. Dies entspricht einer Reduktion um 41 in Vergleich zum Juni 2024 (BJ) und 51 zum April 2025 (BP1), was im ersten Vergleich zum BJ einer Verbesserung von ca. 65,08 % entspricht. Diese wurde nach folgender Formel berechnet:

$$\text{Verbesserung zum BJ} = \left(\frac{\text{BJ} - \text{BP2}}{\text{BJ}}\right) x\ 100$$

$$\text{Verbesserung zum BJ} = \left(\frac{63 - 22}{63}\right) x\ 100\ \approx 65{,}08\ \%$$

$$\text{Verbesserung zum BP1} = \left(\frac{\text{BP1} - \text{BP2}}{\text{BP1}}\right) x\ 100$$

$$\text{Verbesserung zum BP1} = \left(\frac{73 - 22}{73}\right) x\ 100\ \approx 69{,}86\ \%$$

Dieses Ergebnis bestätigt die Wirksamkeit der Maßnahmen. Insbesondere die Einführung technischer Lösungen und Sicherheitsrichtlinien sowie die verstärkte Kontrolle von Endgeräten zeigten eindeutige Wirkung.

10.3.1.1 Evaluation von Schwachstellenscan (Vulnerability Scan)

Neben der quantitativen Auswertung der Sicherheitsvorfälle wurde nach Implementierung der Schutzmaßnahmen ein Schwachstellenscan (Vulnerability Scan) mit ESET PROTECT durchgeführt. Zu diesem Zweck wurden zwei Zeitpunkte miteinander verglichen: ein einmaliger Scan (VS1) vom 26.04.2025 sowie ein kontinuierlicher Echtzeit-Scan (VES1) im Zeitraum vom 27.04. bis 18.05.2025.

Die Resultate beider Scans sind in Abbildung 16 und 17 dargestellt und weisen auf strukturelle Schwächen in der IT-Architektur der Polnischen Schule Jan III Sobieski hin. Der Vergleich zeigt auch, inwieweit die implementierten (technischen) Maßnahmen zur Reduktion kritischer Schwachstellen beigetragen haben und an welchen Stellen weiterhin Optimierungspotenzial bestehen.

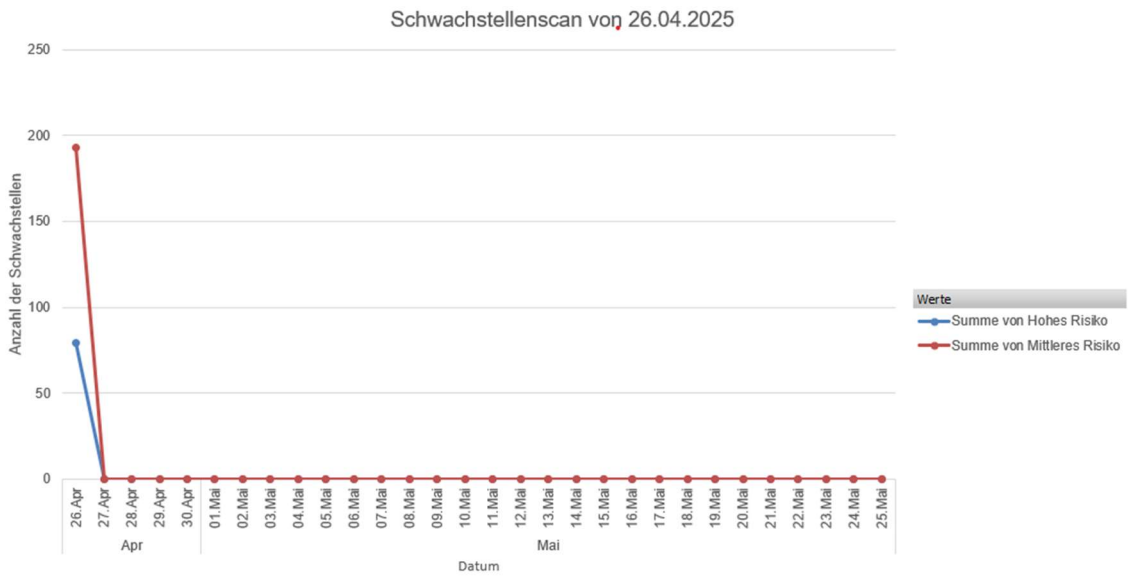

Abbildung 16 Einmaliger Schwachstellenscan vom 26.04.2025

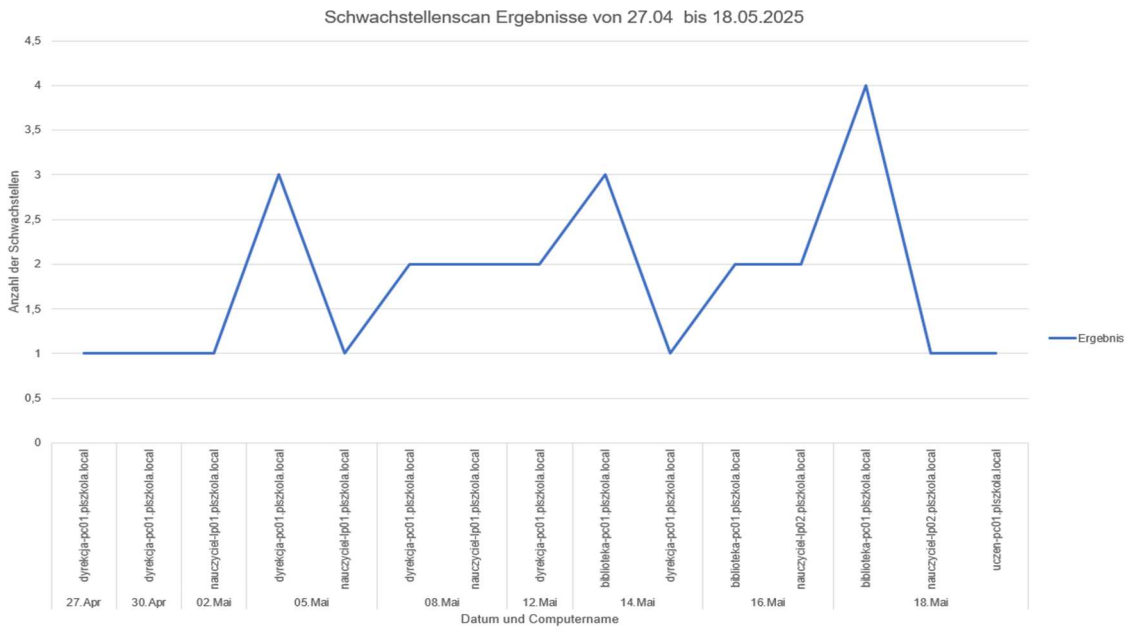

Abbildung 17 Schwachstellenscan Ergebnisse von 27.04. bis 18.05.2025

Im Zuge der durchgeführten Schwachstellenscans konnten sicherheitsrelevante Schwachstellen identifiziert werden. Beim ersten Scan am 26. April 2025 wurden 272 Schwachstellen identifiziert, wobei im Rahmen des Echtzeit-Schwachstellenscans während der dreiwöchigen Beobachtungsphase zwischen dem 27. April und dem 18. Mai 2025 nur noch 27 Schwachstellen verzeichnet wurden.

Gemäß der vorliegenden Daten lässt sich die prozentuale Verbesserung wie folgt berechnen:

$$\text{Verbesserung} = \left(\frac{\text{VS1} - \text{VES1}}{\text{VS1}}\right) x\ 100$$

$$\text{Verbesserung} = \left(\frac{272 - 27}{272}\right) x\ 100\ \approx 90{,}07\ \%$$

Durch den Einsatz von ESET PROTECT konnten viele schwerwiegende Schwachstellen automatisiert erkannt und behoben werden. Dabei handelte es sich insbesondere um sicherheitskritische Lücken in veralteten Versionen von Microsoft Office, Windows Defender sowie TeamViewer. Die Implementierung der signifikantesten Sicherheitsupdates erfolgte erfolgreich, wodurch eine Reihe von potenziellen Angriffsvektoren geschlossen werden konnte.

Die verbleibenden 27 Schwachstellen sind in erster Linie auf nicht aktualisierte Softwarekomponenten zurückzuführen. Diese stellen zwar ein moderates Risiko dar, müssen jedoch kontinuierlich beobachtet und aktualisiert werden.

Diese Ergebnisse unterstreichen einerseits die Effektivität der implementierten technischen Maßnahmen, andererseits verdeutlichen sie jedoch die Notwendigkeit einer kontinuierlichen Verbesserung und regelmäßigen Überprüfung der IT-Sicherheitsinfrastruktur, um das erreichte Sicherheitsniveau aufrechtzuerhalten und weiter zu stärken.

10.3.1.2 Evaluation der Akzeptanz – Ergebnisse der Feedback

Damit die Implementierung technischer und organisatorischer Sicherheitsmaßnahmen erfolgreich ist, ist die Akzeptanz durch die Endnutzer von größter Bedeutung. Hierbei wurde im Rahmen der Einführung des IT-Sicherheitskonzepts an der Polnischen Schule Jan III Sobieski in Wien am 17. Mai 2025 direkt am Ende des ersten Awareness-Trainings eine Umfrage mit dem Ziel, die Benutzerfreundlichkeit, Verständlichkeit und das subjektiv empfundene Sicherheitsniveau zu evaluieren, durchgeführt.

Zu diesem Zweck wurde ein strukturierter Fragebogen eingesetzt, der sowohl geschlossene Fragen zur quantitativen Auswertung als auch offene Fragen für individuelle Rückmeldungen beinhaltete. Demzufolge fokussierte sich die vorliegende Untersuchung auf folgende Fragestellungen:

A. Geschlossene Fragen:

- Ich empfinde die umgesetzten Sicherheitsmaßnahmen/Richtlinien insgesamt als sinnvoll und notwendig.
- Die Umsetzung der Maßnahmen hat meinen Unterrichtsalltag negativ beeinflusst.
- Die Bedienung des neuen Drucksystems (MyQ X) ist für mich...
    - sehr einfach / eher einfach / neutral / eher schwierig / sehr schwierig
- Die Nutzung der VLAN-Netzwerke (z. B. WLAN-Zugänge) ist für mich...

    - sehr klar und logisch / eher verständlich / neutral / eher verwirrend / sehr verwirrend
- Das Awareness-Training zur Cybersicherheit war für mich hilfreich.
- Ich fühle mich ausreichend informiert über die neue IT-Richtlinien der Schule.
- Ich fühle mich durch die umgesetzten Maßnahmen sicherer im Umgang mit digitalen Medien.
- Ich weiß, wie ich mich im Fall eines Sicherheitsvorfalls verhalten muss.
- Die Nutzung von BYOD-Geräten ist für mich nachvollziehbar geregelt.

B. Offene Fragen:

- Was war für Sie besonders hilfreich an den neuen Sicherheitsmaßnahmen?
- Wo sehen Sie noch Verbesserungsbedarf?

Insgesamt wurden zehn auswertbare Rückmeldungen analysiert, die folgendes ergaben:

- **Wirksamkeit des Awareness-Trainings:** Die Auswertung der Umfrage ergab, dass 70 % der Aussage "Das Awareness-Training zur Cybersicherheit war für mich hilfreich" mit "Stimme voll zu" zustimmten. Dieses Resultat unterstreicht die unmittelbare Wirksamkeit der Schulung und verdeutlicht, dass die Inhalte verständlich vermittelt wurden.
- **Benutzerfreundlichkeit des Druckmanagementsystems MyQ X:** In 70 % der Fälle wurde das Druckmanagementsystem MyQ X von den befragten Lehrkräften als "eher schwierig" oder "sehr schwierig" in der Benutzung beurteilt. Dies lässt auf einen dringenden Bedarf an Training und Schulung schließen, um die Benutzerfreundlichkeit des Systems zu verbessern und die Akzeptanz zu erhöhen.
- **Alltagstauglichkeit der Sicherheitsmaßnahmen**: Acht von zehn Lehrer d. h. 80 % teilten mit, dass die implementierten Sicherheitsmaßnahmen keine negativen Auswirkungen auf ihren Schulalltag hatte. Dies lässt den Schluss, dass die Maßnahmen erfolgreich in den Schulalltag integriert wurden, ohne dabei den Unterrichtsablauf zu beeinträchtigen.

Darüber hinaus wurden weitere Ergebnisse erzielt:

- **Gefühl der Sicherheit:** 60 % der Befragten berichteten, dass sie sich durch einführte technisch als auch organisatorische Maßnahmen sicherer bei der Nutzung des Schulsystem fühlen.
- **Informationsstand zu Sicherheitsrichtlinien:** Sechs von zehn Lehrer (60 %) fühlen sich gut über die neue Sicherheitsrichtlinien informiert.
- **Verhalten bei Sicherheitsvorfällen:** Die Messung ergab, dass 70 % wissen, wie sie sich im Falle eines Sicherheitsvorfalls wie Phishing-Angriff verhalten sollen.
- **Verständlichkeit der VLAN-Zugänge:** Acht von zehn Befragten (80 %) empfinden die VLAN-Zugänge als "klar" oder "eher verständlich".

Ein weiterer Aspekt, der in diesem Zusammenhang berücksichtigt wurde, ist die Systemverfügbarkeit, die Aufgrund der gezielten Planung und Umsetzung der technischen Maßnahmen außerhalb der regulären Schulbetriebszeiten gewährleistet werden konnte. Dies impliziert, dass der Unterrichtsbetrieb zu keinem Zeitpunkt signifikant beeinträchtigt wurde. In Anbetracht dieser Tatsache wird die Annahme getroffen, dass dieses Systemverfügbarkeitskriterium zu 99 % erfüllt wurde. Zudem wurde ein jährliches Audit der IT-Architektur im Maßnahmenplan verankert, um eine strukturierte Nachkontrolle sicherzustellen. Damit wird das Prinzip der kontinuierlichen Verbesserung umgesetzt und die Langfristigkeit sowie die Wirksamkeit des Sicherheits-konzepts gewährleistet.

10.3.2 Penetrationstest

Als Teil des IT-Sicherheitskonzepts für die Polnische Schule Jan III Sobieski in Wien erfolgte ein kurzer, einfacher Penetrationstest unter kontrollierten Rahmenbedingungen. Der Fokus des Tests lag auf der Nachstellung realer Angriffsszenarien unter Verwendung des Armitage Metasploit Frameworks in der Version 6 (msf6). Die Evaluierung zielte darauf ab, die Wirksamkeit der implementierten Schutzmaßnahmen gegen bekannte Schwachstellen zu bewerten.

10.3.2.1 Methodik des Tests

Das Metasploit Framework ist eine modulare Open-Source-Plattform, die für die Durchführung von Schwachstellenanalysen, Exploits und Payload-Tests genutzt wird. Das Werkzeug findet weltweit Anwendung bei IT-Sicherheitsanalysten, die damit Angriffe auf IT-Infrastrukturen unter kontrollierten Bedingungen simulieren. Armitage ergänzt msf6 um eine grafische Benutzeroberfläche, die insbesondere bei der Koordination mehrerer Hosts, Sessions und Exploits eine signifikante Erleichterung darstellt (Messner 2015).

Ein beispielhafter Ablauf beginnt in der Regel mit dem Laden eines Moduls wie z. B.:

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 > set RHOSTS 192.168.10.XX
msf6 > run
```

Abbildung 18 Beispiel für Metasploit Port Scan

In diesem Kontext findet das Modul "portscan/tcp" Anwendung, um die Erreichbarkeit spezifischer Dienste auf dem Zielsystem zu evaluieren. Die Abkürzung "RHOSTS" bezeichnet die Zieladresse(n), während der Begriff "run" die Ausführung des Scans einleitet. Im Rahmen dieses Tests wurden u. a. folgende Module eingesetzt:

- **auxiliary/scanner/portscan/tcp:** TCP-Portscanner zur Identifikation erreichbarer Dienste.
- **auxiliary/scanner/ldap/ldap_login:** Modul zum Testen von LDAP-Authentifizierungen auf schwache Zugangsdaten.

- **exploit/windows/smb/ms17_010_eternalblue:** Exploit für die Sicherheitslücke MS17-010 (EternalBlue), welcher bei ungepatchten Systemen eine Remote-Code-Ausführung ermöglicht.
- **auxiliary/scanner/http/http_methods**: HTTP-Scanner um unterstützte Web-methoden wie GET, POST, DELETE auf einem Webserver zu identifizieren.
- **auxiliary/spoof/arp/arp_poisoning:** Modul zur Durchführung eines ARP-Spoofing-Angriffs im lokalen Netzwerk. (Messner 2015)

Bei der Analyse wurden die nachfolgenden fünf Netzsegmente auf potenzielle Schwachstellen überprüft:

- 192.168.10.0/24 – Server
- 192.168.20.0/24 – Clients
- 192.168.50.0/24 – Other Devices
- 192.168.3.0/24 – PLS-Lehrer
- 192.168.4.0/24 – PLS-Schüler

Bei der Durchführung der Tests wurden folgende technische Parameter berücksichtigt:

- **Anzahl gleichzeitiger Threads:** 24 (zur Beschleunigung der Scanvorgänge)
- **Untersuchter Portbereich:** Ports 1–1000 (Standardports gängiger Dienste und Protokolle)

10.3.2.2 Test Ergebnisse

In den darauffolgenden Punkten werden die Resultate der Penetrationstestanalyse aller in Kapitel 10.4.1 analysierten Subnetze fragmentarisch präsentieren. Um die Sicherheit vertraulicher Informationen, konkret im Hinblick auf Netzwerksicherheit, zu gewährleisten, wurden die Daten in dieser Auswertung partiell anonymisiert. Gleichzeitig wird durch die Darstellung der Ergebnisse, eine klare und übersichtliche Darstellung des Zustands der Zielsysteme sichergestellt, die in folgenden Punkten zusammengefasst wurden:

a) **LDAP Authentifizierungsversuche:**
   Im Rahmen des ersten Tests wurde mit dem Modul "ldap_login" evaluiert, ob Zielsysteme gegenüber unsicheren oder anonymen Authentifizierungs-versuchen über LDAP (Lightweight Directory Access Protocol) verwundbar sind (Metasploit 2024). Dieser Begriff bezeichnet ein Netzwerkprotokoll, das zur Abfrage und Verwaltung von Verzeichnisdiensten wie Benutzer- und Gruppen-informationen dient. Häufig findet es die Verwendung in Active-Directory-Umgebung und ermöglicht – bei unzureichender Konfiguration – auch

ungesicherte anonyme Zugriffe (Red 2022). Hierbei wurde untersucht, ob diese potenzielle Schwachstelle im System ausgenutzt werden kann.

```
msf6 > use auxiliary/scanner/ldap/ldap_login
msf6 auxiliary(scanner/ldap/ldap_login) > set RHOSTS 192.168.20.XX
msf6 auxiliary(scanner/ldap/ldap_login) > set ANONYMOUS_LOGIN true
msf6 auxiliary(scanner/ldap/ldap_login) > run
[*] 192.168.20.XX:389 - Starting LDAP login sweep...
[-] 192.168.20.XX:389 - Bind attempt failed: Invalid credentials (49)
[*] 192.168.20.XX:389 - 0 valid LDAP credentials found
```

Abbildung 19 ARMITAGE Metasploit-Scan (ldap_login) – Authentifizierungsprüfung auf 192.168.20.XX

```
msf6 > use auxiliary/scanner/ldap/ldap_login
msf6 auxiliary(scanner/ldap/ldap_login) > set RHOSTS 192.168.50.XX
msf6 auxiliary(scanner/ldap/ldap_login) > set ANONYMOUS_LOGIN true
msf6 auxiliary(scanner/ldap/ldap_login) > run
[*] 192.168.20.XX:389 - Starting LDAP login sweep...
[-] 192.168.20.XX:389 - Bind attempt failed: Invalid credentials (49)
[*] 192.168.20.XX:389 - 0 valid LDAP credentials found
```

Abbildung 20 ARMITAGE Metasploit-Scan (ldap_login) – Authentifizierungsprüfung auf 192.168.50.XX

Diese Rückmeldung des Tests zeigt, dass der Server keine anonymen Abfragen akzeptiert und somit gegen unautorisierte Zugriffe auf Benutzer- oder Gruppeninformationen geschützt ist.

b) SMB Exploits – EternalBlue:

In der vorliegenden Evaluation wird analysiert, inwiefern Systeme gegenüber der kritischen SMBv1-Sicherheitslücke MS17-010 anfällig sind (Shivanandhan 2025). Die Schwachstelle wurde im Jahr 2017 durch eine Veröffentlichung seitens der NSA bekannt und ermöglichte unter anderem die globalen Angriffe "WannaCry" und "NotPetya" (Burdova 2020). Der Exploit nutzt eine fehlerhafte Speicherverwaltung im SMB-Dienst, um Code aus der Ferne auszuführen, wobei keine Authentifizierung erfolgt.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.10.X
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] 192.168.10.X:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.X:445 - Rex::ConnectionTimeout
[*] 192.168.10.X:445 - The target is not vulnerable.
```

Abbildung 21 ARMITAGE Metasploit-Scan (ms17_010_eternalblue) auf 192.168.10.X

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.20.XX
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] 192.168.20.XX:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.20.XX:445 - Rex::ConnectionTimeout
[*] 192.168.20.XX:445 - The target is not vulnerable.
```

Abbildung 22 ARMITAGE Metasploit-Scan (ms17_010_eternalblue) auf 192.168.20.XX

Zielsysteme reagierten mit Timeouts oder meldeten, dass sie nicht verwundbar sind. Die Lücke ist durch Patches geschlossen bzw. durch Firewalls blockiert.

c) HTTP-Analyse:

Mittels dieses Tests wurde evaluiert, ob Webserver gefährliche HTTP-Methoden wie PUT oder DELETE unterstützen, die potenziell zur Manipulation genutzt werden können (Messner 2015).

```
msf6 > use auxiliary/scanner/http/http_methods
msf6 auxiliary(scanner/http/http_methods) > set RHOSTS 192.168.20.XX
[*] Supported Methods: GET HEAD
[*] Scanned 1 of 1 hosts (100% complete)
```

Abbildung 23 ARMITAGE Metasploit-Scan (http_methods) auf 192.168.20.XX

Zusammenfassend lässt sich feststellen, von unsicheren HTTP-Methoden wie PUT, DELETE oder TRACE die nicht erkannt wurden geht kein Risiko aus.

d) TCP-Portscan:

Durch den Einsatz des TCP-Portscanners wurden die im Netzwerk verfügbaren Dienste analysiert, um potenzielle Schwachstellen zu identifizieren (Messner 2015).

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.10.X/24
msf6 auxiliary(scanner/portscan/tcp) > run
```

Abbildung 24 ARMITAGE Metasploit Port Scan auf 192.168.10.X

Erkannte Dienste:

- 80 (HTTP)
- 443 (HTTPS)
- 445 (SMB)
- 389 (LDAP)
- 88 (Kerberos)

Alle anderen Ports sind blockiert oder geschlossen. Gleiche Ergebnisse wurden für die IP-Adressen 192.168.20.XX, 192.168.3.XXX, 192.168.4.XX sowie 192.168.50.XX erzielt.

e) **ARP-Spoofing:**
Abschließend wurde ein "Man-in-the-Middle-Angriff" in Form von "ARP-Poisoning" simuliert (Messner 2015). Das Ziel bestand darin, den Datenverkehr durch gefälschte ARP-Antworten zu umleiten und zu analysieren.

```
msf6 > use auxiliary/spoof/arp/arp_poisoning
set RHOSTS 192.168.10.X
set GATEWAY 192.168.10.X
set INTERFACE eth0
set SNAPLEN 65535
set PCAPFILE /tmp/testcapture.pcap
run
[*] ARP poisoning started...
[-] No packets captured. Possible switched network or mitigation active.
```

Abbildung 25 ARMITAGE Metasploit-Scan (arp_poisoning) auf 192.168.10.X

```
msf6 > use auxiliary/spoof/arp/arp_poisoning
set RHOSTS 192.168.3.XXX
set GATEWAY 192.168.3.X
set INTERFACE eth0
set SNAPLEN 65535
set PCAPFILE /tmp/testcapture.pcap
run
[*] ARP poisoning started...
[-] No packets captured. Possible switched network or mitigation active.
```

Abbildung 26 ARMITAGE Metasploit-Scan (arp_poisoning) auf 192.168.3.XXX

Auch in diesem Fall war der Angriff wirkungslos und trotz laufender ARP-Manipulation konnte dank VLANs mit aktiver Port-Security kein Datenverkehr abgefangen werden.

Die Ergebnisse zeigen, dass keine gängigen Exploits erfolgreich ausgenutzt werden konnten. Weder über SMB, LDAP noch durch Man-in-the-Middle-Techniken konnten die getesteten Systeme kompromittiert werden. Der Einsatz des Metasploit Frameworks demonstrierte, dass gängige Angriffsvektoren durch konfigurationsbasierte Schutzmaßnahmen erfolgreich abgewehrt werden konnten.

10.4 Kontinuierliche Überwachung und Verbesserung

Ein IT-Sicherheitskonzept ist kein starres Dokument, sondern muss dynamisch an neue Bedrohungen und technologische Entwicklungen angepasst werden. In diesem Subkapitel werden Maßnahmen zur kontinuierlichen Überwachung und Verbesserung der IT-Sicherheit beschrieben, um die langfristige Resilienz der Schule zu gewährleisten:

1. **Regelmäßige Sicherheitsaudits:** Jedes Jahr führt der IT-Verantwortliche ein Sicherheitsaudit durch, um die Wirksamkeit der implementierten Maßnahmen zu

überprüfen. Dies umfasst Penetrationstests, Schwachstellenscans und die Überprüfung der Netzwerksicherheit, der Firewall-Konfiguration und der VLAN-Segmentierung.

2. **Incident Monitoring und Reporting:** Es wird eine zentrale Datenbank aufgebaut, um Sicherheitsvorfälle zu erfassen und zu analysieren. Die Datenbank basiert auf den Logs der FortiGate-60F-Firewall und der ESET-PROTECT-Lösung, um Trends zu erkennen und proaktive Maßnahmen abzuleiten.
3. **Feedback-Schleifen und Lessons Learned:** Nach jedem dokumentierten Sicherheitsvorfall wird eine Nachbesprechung mit der Direktion, dem Bibliothekspersonal und den Lehrern organisiert, um die Ursachen zu analysieren und Verbesserungsmaßnahmen abzuleiten. Die Ergebnisse fließen in die Aktualisierung der IT-Sicherheitsrichtlinie und der Awareness-Trainings ein.
4. **Technologie- und Bedrohungsüberwachung:** Der IT-Verantwortliche wurde beauftragt, vierteljährlich Berichte über neue Cyberbedrohungen und Sicherheitsupdates zu erstellen. Diese Berichte basieren auf CERT-Berichten und Hersteller-Updates für die Produkte von Cisco und Fortinet. Dadurch kann die Schule auf aktuelle Bedrohungslagen rechtzeitig reagieren.

Diese Maßnahmen adressieren die in Kapitel 7.3 dokumentierten wiederkehrenden Angriffe wie ARP-Spoofing und Phishing und stellen sicher, dass das Konzept dynamisch bleibt und auf neue Bedrohungen flexibel eingehen kann.

11. Diskussion und Abschluss

In diesem abschließenden Kapitel der Bachelorarbeit werden die zentralen Ergebnisse zusammengefasst, reflektiert und in einen größeren Zusammenhang gestellt. Dabei steht die kritische Bewertung der Wirksamkeit des entwickelten IT-Sicherheitskonzepts für die Polnische Schule Jan III Sobieski in Wien basierend auf den gewonnenen Erkenntnissen im Vordergrund. Darüber hinaus werden die Grenzen der Arbeit klar benannt, um sowohl methodische als auch praktische Probleme transparent darzustellen.

Dieses Kapitel gliedert sich in drei Abschnitte:

11.1 bietet eine kompakte Zusammenfassung der wesentlichen Forschungsergebnisse.
11.2 widmet sich der Validierung der Hypothese.
11.3 beleuchtet die Limitationen der Arbeit.

11.1 Zusammenfassung der Forschungsergebnisse

Das Ziel dieser Bachelorarbeit war die Entwicklung eines umfassenden IT-Sicherheitskonzepts für die Polnische Schule Jan III. Sobieski am Kollegium Kalksburg, das die OCTAVE-Methode mit weiteren IT-Sicherheitsansätzen kombiniert. Dieses Konzept hat zum Ziel, die Anzahl erfolgreicher Cyberangriffe auf die IT-Infrastruktur der Schule um mindestens 50 % zu reduzieren. Um dieses Ziel zu realisieren, wurde ein ganzheitlicher Ansatz verfolgt, der technische, organisatorische und personelle Maßnahmen integriert und auf einer fundierten Risikoanalyse basiert.

Zunächst erfolgte eine theoretische Erarbeitung der relevanten Konzepte und Prinzipien der Informationssicherheit (Kapitel 2), einschließlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sowie aktueller Bedrohungsszenarien im Bildungsbereich. In Kapitel 3 wurde die OCTAVE-S-Methode als zentrale Analysemethode präsentiert, ergänzt durch relevante internationale und nationale Standards wie ISO/IEC 27001, das NIST Cybersecurity Framework, den BSI-Grundschutz sowie das österreichische Informationssicherheitshandbuch (Kapitel 4).

In Kapitel 5 wurden spezifische Bedrohungsszenarien für Bildungseinrichtungen analysiert, die in der Regel auf unzureichend geschützte Infrastrukturen und ein mangelndes Sicherheitsbewusstsein zurückzuführen sind. In Kapitel 6 wurde das methodische Vorgehen zur Erstellung und Umsetzung eines Sicherheitskonzepts anhand eines Phasenmodells erörtert, welches die Planung, Durchführung und Evaluation umfasst.

Aus der Analyse der bestehenden IT-Infrastruktur der Schule in Kapitel 7 ergeben sich eine Reihe kritischer Schwachstellen: mangelhafte Netzwerksegmentierung, veraltete Hardware, fehlende Multifaktor-Authentifizierung, unzureichende Backup-

Strategien sowie unklare Verantwortlichkeiten im Sicherheitsmanagement. Darüber hinaus wurden konkrete Sicherheitsvorfälle aus den Jahren 2024 und 2025 dokumentiert, die als Ausgangsbasis für die Risikobewertung dienten.

Im achten Kapitel wurde die Anwendung der sogenannten OCTAVE-S Methode thematisiert. In der ersten Phase wurden die kritischsten Assets identifiziert (z. B. Schülerdaten, E-Klassenbuch, WLAN, Benutzerkonten), potenzielle Bedrohungen und Schwachstellen analysiert sowie spezifische Sicherheitsanforderungen formuliert. Die Risikoprofile dieser Assets dienten als Fundament für die strategische Maßnahmenplanung.

In Kapitel 9 wurde die technische und organisatorische Umsetzung des Sicherheitskonzepts beschrieben. Hierzu zählten unter anderem:

- die Implementierung einer FortiGate 60F Firewall mit IDS/IPS,
- der Austausch veralteter Geräte,
- die Einrichtung VLAN-basierter Netzwerksegmente für unterschiedliche Nutzergruppen,
- die Einführung eines dreifachen Backup-Systems,
- die Umsetzung der Multifaktor-Authentifizierung (MFA) für sensible Bereiche,
- sowie organisatorische Maßnahmen wie Awareness-Schulungen und IT-Sicherheitsrichtlinien.

Die Implementierung wurde in fünf Projektphasen unterteil und im Rahmen von Kapitel 10 einer umfangreichen Evaluation unterzogen. Die Resultate deuten auf eine signifikante Verbesserung der IT-Sicherheitslage hin:

- Die Anzahl sicherheitsrelevanter Vorfälle reduzierte sich von 63 im Juni 2024 auf 22 im Mai 2025. Dies entspricht einer Verbesserung von 65,08 %.
- Im Vergleich zur ersten Beobachtungsperiode mit AVAST im April 2025 (73 Vorfälle) konnte die ESET PROTECT-Analyse in der zweiten Periode (22 Vorfälle) eine Reduktion von 69,86 % dokumentieren.
- Ein durchgeführter Schwachstellenscan zeigte eine Reduktion von 272 auf 27 erkannte Sicherheitslücken, was eine Verbesserung von 90,07 % entspricht.
- Penetrationstests mit dem Metasploit-Framework zeigten, dass gängige Angriffe wie SMB-Exploits (EternalBlue), ARP-Spoofing oder unsichere HTTP-Methoden durch die implementierten Maßnahmen erfolgreich abgewehrt wurden.
- Die eingesetzten VLANs und Port-Security verhinderten erfolgreich Man-in-the-Middle-Angriffe.

Auch die Benutzerakzeptanz wurde evaluiert:

- 70 % der Lehrer fanden das Awareness-Training hilfreich zur Erkennung sicherheitsrelevanter Bedrohungen.
- 80 % gaben an, dass die technischen Maßnahmen den Schulbetrieb nicht beeinträchtigt haben.

- Die Benutzerfreundlichkeit des neuen Drucksystems MyQ X wurde hingegen von 70 % der Lehrkräfte als "eher schwierig" bewertet, was auf einen Schulungsbedarf hinweist.

Darüber hinaus wird mit der Implementierung eines zentralen Log-Systems, der Etablierung regelmäßiger Sicherheitsaudits sowie vierteljährlicher CERT-Berichte ein strukturierter Rahmen für die kontinuierliche Verbesserung der Sicherheitsarchitektur geschaffen.

Aus der in dieser Arbeit durchgeführten Auswertungen und Analysen geht hervor, dass ein mit begrenzten Ressourcen umsetzbares Sicherheitskonzept nachweisliche Verbesserungen bewirken kann. Das angestrebte Ziel dieser Arbeit, eine Reduktion von Cyberangriffen um mindestens 50 %, wurde mit einer Übertreffung von über 65 % (vgl. Kapitel 10.3) erreicht. Zudem wurde ein nachhaltiger Grundstein für ein verstärktes Sicherheitsbewusstsein sowie eine resiliente IT-Infrastruktur im schulischen Umfeld gelegt.

11.2 Validierung der Hypothese

Für die vorliegende Arbeit wurde folgende Hypothese aufgestellt:

"Ein neu entwickeltes IT-Sicherheitskonzept, das die OCTAVE-Methode in Kombination mit weiteren IT-Sicherheitsansätzen anwendet, reduziert die Zahl der Cyberangriffe auf die IT-Infrastruktur der polnischen Schule des Jan III. Sobieski am Kollegium Kalksburg um mindestens 50 %."

Zur Überprüfung der zuvor aufgestellten Hypothese wurde im Rahmen der vorliegenden Arbeit ein Sicherheitskonzept für die Polnische Schule Jan III Sobieski in Wien entwickelt, schrittweise implementiert (Kapitel 9) und einer umfassenden Evaluation unterzogen (Kapitel 10).

Die Resultate der durchgeführten Analysen belegen die Wirksamkeit der implementierten Maßnahmen eindeutig:

- **Reduktion von Cybervorfällen:** Die Anzahl der dokumentierten sicherheitsrelevanten Vorfälle sank von 63 (Basis Juni 2024) auf 22 (nach Implementierung im Mai 2025). Dies entspricht einer Reduktion um 65,08 %, die deutlich über dem in der Hypothese geforderten Wert von 50 % liegt.
- **Vergleich der beiden Beobachtungsperioden:** Zwischen dem 7. und 27. April 2025 (BP1) wurden 73 sicherheitsrelevante Ereignisse gezählt. In der darauf-folgenden Beobachtungsphase vom 27. April bis zum 18. Mai 2025 (BP2) reduzierte sich diese Zahl auf 22. Das entspricht einer Verbesserung um 69,86 % gegenüber der ersten Phase.
- **Ergebnisse der Schwachstellenscans:** Der initiale Schwachstellenscan (VS1) vom 26.04.2025 wies 272 Sicherheitslücken auf. Der Echtzeit-Scan vom 27.04.

bis 18.05.2025 (VES1) zeigte nur noch 27 relevante Schwachstellen – eine Verbesserung von 90,07 %.

- **Penetrationstests:** Im Rahmen realistischer Angriffssimulationen mit dem Metasploit-Framework konnten keine Schwachstellen erfolgreich ausgenutzt werden. Die getesteten Systeme reagierten stabil auf SMB-Exploits, ARP-Spoofing, Portscans und HTTP-Methoden-Analysen. Auch LDAP-Authentifizierungen konnten nicht missbraucht werden.
- **Benutzerperspektive:** Zusätzlich belegt die durchgeführte Umfrage unter Lehrkräften, dass die Sicherheitsmaßnahmen überwiegend akzeptiert wurden und als hilfreich wahrgenommen wurden. 70 % der Lehrkräfte empfanden das Awareness-Training als nützlich, 80 % berichteten von keinen Beeinträchtigungen im Schulalltag und 60 % fühlen sich durch die Maßnahmen sicherer im Umgang mit digitalen Medien.

Auf Basis dieser Daten konnte die Hypothese bestätigt werden. Die Kombination aus technischen Schutzvorkehrungen wie Firewall, VLAN, MFA, Backup, organisatorischen Maßnahmen (Sicherheitsrichtlinien, Schulungen, Monitoring) und der aktiven Beteiligung aller relevanten Stakeholder führte zu einer nachweislichen Verbesserung der Sicherheitslage. Die angestrebte Reduktion der erfolgreichen Cyberangriffe um mindestens 50 Prozent wurde nicht nur erreicht, sondern überschritten.

Demnach lässt sich schlussfolgern, dass ein IT-Sicherheitskonzept, welches risikobasiert, strukturiert und in Bezug auf den Bildungskontext entwickelt wurde, selbst bei limitierten Ressourcen, in einer Bildungsinstitution zu einer messbaren Wirkung führt und die Resilienz der IT-Infrastruktur erhöht.

11.3 Limitationen der Arbeit

Abgesehen von den positiven Resultaten dieser Arbeit – insbesondere der messbaren Reduktion von Cybervorfällen und der erfolgreichen Implementierung technischer wie organisatorischer Schutzmaßnahmen – bestehen mehrere relevante Limitationen, welche aus wissenschaftlicher Perspektive beleuchtet werden müssen. Diese betreffen sowohl methodische, personelle und finanzielle Aspekte als auch inhaltliche und übertragbare Rahmenbedingungen:

1. **Zeitliche und personelle Belastung:** Die Umsetzung wurde vollständig nebenberuflich durchgeführt. Dies erforderte ein hohes Maß an Eigenorganisation, insbesondere bei technischen Installationen, Konfigurationen und der Durchführung von Schulungen. Besonders herausfordernd waren die Planungsgespräche für die OCTAVE-Phase 1, da viele schulische Akteure (Lehrer, Direktion, Bibliothekspersonal) mehrere Rollen gleichzeitig ausüben und häufig kurzfristig vertreten werden mussten. Dies erschwerte die Koordination.

2. **Finanzierung:** Die Finanzierung des Projekts erfolgte aus privaten Mitteln des Autors, was zu eingeschränkten Wahlmöglichkeiten bei der Auswahl professioneller Systeme und Lizenzen führte. Infolgedessen wurde ein bewusster Fokus auf den Einsatz gebrauchter Geräte sowie auf Open-Source- bzw. kostengünstige Lizenzen gelegt. Auf diese Weise konnten betriebsfähige Lösungen umgesetzt werden, allerdings schränkte das Budget die Wahlfreiheit bei Systemen ein.
3. **Umfang und Tiefe der Standards**: Integraler Bestandteil dieser Arbeit war die OCTAVE-S Methode in Kombination mit ausgewählten Elementen der ISO/IEC 27001, des NIST Cybersecurity Frameworks, des BSI IT-Grundschutzes sowie des Österreichischen Informationssicherheitshandbuchs. Die angestrebte Interdisziplinarität sollte ein realistisches und zugleich anschlussfähiges Konzept sicherstellen. Jedoch wurde diese Breite auf Kosten der Tiefe erreicht: Einige Standards konnten nicht umfassend behandelt werden und es stand keine ausreichende Zeit für eine vollständige systematische Umsetzung, z. B. nach ISO 27001. In zukünftigen Studien sollte daher der Fokus auf OCTAVE-S mit ergänzenden Elementen aus dem BSI-Grundschutz gelegt werden, um methodische Ansätze zu vertiefen.
4. **Evaluation über begrenzten Zeitraum:** Aufgrund der Kurzfristigkeit der Analysen erlauben die gewonnenen Erkenntnisse, die den Rückgang von Bedrohungen um ca. 65 % und Schwachstellen um 90 % feststellten, keine validen Aussagen über die langfristige Wirksamkeit oder Nachhaltigkeit der getroffenen Maßnahmen. Für eine valide Evaluierung der Wirksamkeit von Awareness-Trainings und des tatsächlichen Verhaltens bei zukünftigen Angriffsszenarien ist ein deutlich längerer Evaluationszeitraum erforderlich.
5. **Eingeschränkte Generalisierbarkeit:** Aufgrund der starken Orientierung an den spezifischen Gegebenheiten der Polnischen Schule Jan III Sobieski ist eine Übertragung der entwickelten Maßnahmen auf andere Schulen nur bedingt möglich. Eine Übertragung auf andere Schulen erfordert Anpassungen hinsichtlich Infrastruktur, Personalstruktur und finanzieller Ressourcen.
6. **Dynamik der Angriffstechniken:** Die rasche Weiterentwicklung von Angriffs-techniken, Exploit-Methoden und Malware erfordert eine kontinuierliche Anpassung und Weiterentwicklung des IT-Sicherheitskonzepts. Dabei ist zu berücksichtigen, dass die in dieser Arbeit dokumentierten Ergebnisse nur eine Momentaufnahme (Mai 2025) repräsentieren. Angesichts der Dynamik der Cyberbedrohungslage – insbesondere im Bildungssektor – ist davon auszugehen, dass neue Angriffsmethoden oder Schwachstellen auftreten werden, die heute noch nicht bekannt sind. Nur durch regelmäßige Audits, Schulungen und Updates kann die Wirksamkeit des vorliegenden Konzepts langfristig gewährleistet werden.

Abschließend lässt sich festhalten, dass diese Arbeit bedeutende Ansätze für die Entwicklung eines praxisnahen Sicherheitskonzept im Bildungsbereich bietet, besonders unter realistischen Rahmenbedingungen und mit limitierten Ressourcen.
Die identifizierten Limitationen legen nahe, dass nachhaltige IT-Sicherheit nicht als singuläres Projekt, sondern als kontinuierlicher Prozess betrachtet werden sollte. Daher kann diese Arbeit als Grundstein verstanden werden, der einer kontinuierlichen Weiterentwicklung bedarf.

Literaturverzeichnis

Alberts, Christopher, Audrey Dorofee, James Stevens, und Carol Woody. *OCTAVE ® - S Implementation Guide, Version 1.0.* Pittsburg: Carnegie Mellon Software Engineering Institute, 2025.

Almagro, Luis , et al. *CYBERSECURITY EDUCATION: Planning for the Future Through Workforce Development.* 09 2020.

Alshar'e, Marwan. „Cyber Security Framework Selection: Comparison of NIST and ISO/IEC 27001." *Applied Computing Journal*, 2023: 245-255.

Appiah, Vincent, Michael Asante, Isaac Kofi Nti, und Owusu Nyarko-Boateng. „Survey of Websites and Web Application Security Threats Using Vulnerability Assessment." *Journal of Computer Science*, 2018: 1341-1354.

A-SIT Zentrum für sichere Informationstechnologie - Austria. *Der Faktor Mensch in der IT-Sicherheit: Unachtsamkeit als größtes Cyber-Risiko.* IKT-Sicherheitsportal, 04. 10 2024.

Aust, Christian, und Chirstian Paulsen. *Werte- und prozessorientierte Risikoanalyse mit OCTAVE.* Berlin: TeleTrusT Information Security Professional, 2013.

Bedner, Mark. *Cloud Computing: Technik, Sicherheit und rechtliche Gestaltung.* Kassel: kassel university press GmbH, 2013.

Binus, Stephanus. „Implementation Octave-S and ISO 27001 Controls in Risk Managment Information Systems." *ComTech* 5 (2014): 685-693.

Bishop, Matt. *Introduction to Computer Security.* Addison-Wesley Professional, 2004.

Blumberg, Hartmut, und Norbert Pohlmann. *Der IT-Sicherheitsleitfaden.* Heidelberg: Redline GmbH, 2006.

Bruns, Larissa. *Informationssicherheit im Überblick: Definition, Schutzziele, Maßnahmen.* 09. 06 2022. https://www.dataguard.de/blog/informationssicherheit (Zugriff am 05. 02 2025).

Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise." Bonn, 2000.

Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-1 – Managementsysteme für Informationssicherheit (ISMS)." Bonn, 2017.

Bundesamt für Sicherheit in der Informationstechnik. „BSI-Standard 200-2: IT-Grundschutz-Methodik." Bonn, 2017.

—. *Identitätsdiebstahl durch Datenleaks und Doxing.* n.d. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-

Kriminalitaet/Identitaetsdiebstahl/identitaetsdiebstahl_node.html (Zugriff am 06. 02 2025).

—. *Management von Schwachstellen und Sicherheitsupdates.* 11. 07 2018. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_093.pdf?__blob=publicationFile&v=1 (Zugriff am 07. 02 2025).

—. „Positionspapier Zero Trust 2023." 26. 06 2023. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeLeitlinien/Zero-Trust/Zero-Trust_04072023.pdf?__blob=publicationFile&v=4 (Zugriff am 07. 02 2025).

—. *Schadprogramme.* 2024. https://www.bsi.bund.de/dok/6596284 (Zugriff am 05. 03 2025).

Bundeskanzleramt Österreich. *Österreichisches Informationssicherheitshandbuch.* Version 4.4.0. Herausgeber: Bundeskanzleramt. Wien, 2023.

Bundesministerium für Bildung, Wissenschaft und Forschung. „Digital. Sicher. Souverän." Bonn, 2021.

—. *Digitale Bildung.* 2025. https://www.bmbwf.gv.at/Themen/schule/zrp/dibi.html (Zugriff am 07. 02 2025).

—. *Sicher im Netz - Safer Internet in der Schule.* nd. https://www.bmbwf.gv.at/Themen/schule/schulpraxis/pwi/pa/saferinternet.html (Zugriff am 07. 02 2025).

Bundesministerium für Finanzen. *Förderprogramm Cyber Security Schecks.* n.d. https://transparenzportal.gv.at/tdb/tp/leistung/1065069.html (Zugriff am 07. 02 2025).

Bundesnetzagentur für Elektrizität, Gas,Telekommunikation, Post und Eisenbahnen. „Die Blockchain-Technologie Grundlagen, Potenziale und Herausforderungen." Herausgeber: Referat 121 - Digitalisierung und und Internetplattformen. 06 2021. https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Blockchain/Links_Dokumente/einfuehrung_bc.pdf?__blob=publicationFile&v=1 (Zugriff am 05. 02 2025).

Burdova, Carly. *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?* 18. 06 2020.

Caralli, A. Richard, F. James Stevens, R. Lisa Young, und R. William Willson. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* Technical Report, Carnegie Mellon University, 2007.

Check Point Software Technologies Ltd. *Mehr Cyberangriffe auf deutsche Bildungseinrichtungen.* 19. 08 2024. https://blog.checkpoint.com/research/check-point-research-warns-every-day-is-a-school-day-for-cybercriminals-with-the-education-sector-as-the-top-target-in-2024/ (Zugriff am 07. 02 2025).

Cova, Marco, Christopher Kruegel, und Giovanni Vinga. „Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code.“ *WWW '10: Proceedings of the 19th international conference on World wide web.* New York: Association for Computing Machinery, 2010. 281-290.

Cybersicherheit, Nationales Koordinierungszentrum. *Förderungen.* n.d. https://www.ncc.gv.at/community/foerderungen.html (Zugriff am 07. 02 2025).

Dare, Johnson, und Kanungo Satyantaoo Kanungo. *Cloud-Based Solutions for Distributed DDoS Protection.* 10 2024. https://www.researchgate.net/publication/384639025_CLOUD-BASED_SOLUTIONS_FOR_DISTRIBUTED_DDOS_PROTECTION (Zugriff am 07. 02 2025).

Detken, Kai-Oliver. *Unternehmensschutz: IT-Monitoring und Security Information and Event Management (SIEM) für den Mittelstand.* Bremmen: DECOIT GmbH, 2019, 1-16.

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs. *InvestEU.* 2021. https://investeu.europa.eu/index_en (Zugriff am 06. 03 2025).

Donaldson, Scott, Chris Williams, und Stanley Siegel. *Understanding Security Issues.* Boston/Berlin: De Gruyter, Incorporated, 2018.

Eckert, Claudia. *IT-Sicherheit.* München: Oldenburg Verlag, 2013.

Europäische, Union. *Datenschutz-Grundverordnung (DSGVO), Art. 12–18.* 2018. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679 (Zugriff am 18. 05 2025).

—. *Datenschutz-Grundverordnung (DSGVO), Art. 34.* 2018. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679 (Zugriff am 18. 05 2025).

—. *Datenschutz-Grundverordnung (DSGVO), Art. 5 – Grundsätze.* 25. 05 2018. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679 (Zugriff am 18. 05 2025).

European Commision. *Digital Education Action Plan.* 30. 09 2020. https://education.ec.europa.eu/focus-topics/digital-education/action-plan (Zugriff am 07. 02 2025).

European Union Agency for Cybersecurity. *Public Private Partnerships (PPPs).* n.d. https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies-0/public-private (Zugriff am 07. 02 2025).

Ewuga, Kuzankah Sarah , Efe Zainab Egieya, Adedolapo Omotosho, und Oluwatoyin Abimbola Adegbite. „ISO 27001 In Banking: An Evaluation Of Its Implementation And Effectiveness In Nhancing Information Security.“ *Finance & Accounting Research Journal*, 2023: 405-425.

FedTech. *NIST Cybersecurity Framework: What Is It and What Does It Mean for Feds?* 06. 09 2019. https://fedtechmagazine.com/article/2019/09/nist-cybersecurity-framework-what-it-and-what-does-it-mean-feds-perfcon (Zugriff am 07. 02 2025).

Ferdous, Bilquis. „Cyber Security Risks of Bring Your Own Device (BYOD) Practice in Workplace and Strategies to Address the Risks.“ *International Journal of Science Academic Research*, 2022: 4554-4558.

Finanzmarktaufsichtsbehörde (FMA). „ FMA-Leitfaden IT-Sicherheit in Wertpapierdienstleistungsunternehmen und Wertpapierfirmen.“ 2018.

Gerardo, Vicientius, und Ahmad Nurul Fajar. „Academic IS Risk Management using OCTAVE Allegro in Educational Institution.“ *Journal of Information Systems and Informatics* Vol. 4, No. 3 (09 2022): 687-708.

Gitlan, Dionisie. *SHA-1 vs. SHA-2 vs. SHA-256 vs. SHA-512 Hash-Algorithmen.* 28. 02 2025. https://www.ssldragon.com/de/blog/sha1-sha2-sha256-sha-512 (Zugriff am 04. 03 2025).

Gopstein, Avi, Cuong Nguyen, Cheyney O"Fallon, Nelson Hastings, und David Wollmann. *DRAFT NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0.* U.S. Department of Commerce, 2020.

Groopman, Jessica. *Blockchain: Die wichtigsten Sicherheitsrisiken im Überblick.* 14. 08 2023. https://www.computerweekly.com/de/tipp/Blockchain-Die-wichtigsten-Sicherheitsrisiken-im-Ueberblick (Zugriff am 05. 02 2025).

Gurinaviciute, Juta. „What Cybersecurity Threats Does The Education Sector.“ *Forbes Technology Council*, 2024.

Harjinder, Singh Lallie, Andrew Thompson, Elzbieta Titis, und Paul Stephens. *Understanding Cyber Threats Against the Universities, Colleges, and Schools.* Cornell University, 2023.

Harmes, Tobias. *Die drei Schutzziele der Informationssicherheit.* 10. 06 2024. https://rz10.de/it-security/drei-schutzziele-der-informationssicherheit/ (Zugriff am 05. 02 2025).

Hax, Alando C., und Nicolas S. Majflut. *The Strategy Concept and Process: A Pragmatic Approach.* NJ: Prentice Hal: Englewood Cliffs, 1991.

Hirsch, Theresa, Johanna Berndorfer, Willibald Krenn, und Florian Lorber. *CyberGuide. Anforderungen von KMU zur Cybersicherheit.* Wien: Bundesministerium für Finanzen, 2024.

Hom, Jane, Boonsri Anong, Rii Kim Boem, Kyoung Lee Choi, und Kenita Zelina. „The Octave Allegro Method in Risk Management Assessment of Educational Institutions." *Aptisi Transactions on Technopreneurship (ATT)* Vol.2 No.2 (2020): 167-177.

Houyoux, Patrick. „IDS - IPS - DPI - FIREWALL Die Schlüsselelemente der Abwehr von Cyberangriffen verstehen." *GLOBAL SECURITY MAG*, 2023.

Huber, Jakob. *Bildungseinrichtungen wirkungsvoll vor digitalen Sicherheitsrisiken schützen.* 09. 02 2023. https://www.microsoft.com/de-de/industry/blog/education/2023/02/09/bildungseinrichtungen-wirkungsvoll-vor-digitalen-sicherheitsrisiken-schuetzen/ (Zugriff am 07. 02 2025).

Identity Defined Security Alliance. *Trends in Identity Security: A Survey of IT Security and Identity Professionals.* 2023. https://www.idsalliance.org (Zugriff am 05. 02 2025).

International Organization, for Standardization. *ISO/IEC 27001:2022(en) – Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements.* Geneva: ISO, 2022.

IONOS Digital Guide. *Malware.* 14. 11 2024. https://www.ionos.at/digitalguide/server/sicherheit/malware/ (Zugriff am 05. 02 2025).

Isele, Christoph, et al. *Leitfaden für die Erstellung eines IT-Sicherheitskonzeptes.* Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS), Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen", ZTG Zentrum für Telematik und Telemedizin GmbH (ZTG), 2017, 6-40.

ISO/ICE. *International Standard ISO/IEC 27001.* 15. 10 2005. https://www.telekom.mk/download/iso/ISO%2027001%202005%20Standard.pdf (Zugriff am 07. 02 2025).

Jawaid, Adnan Syed. „Cyber Security Threats to Educational Institutes: A Growing Concern for the New Era of Cybersecurity." *SvedbergOpen* Volume 2 (2022): 12-17.

Jede, Andreas, Frank Bensberg, und Tabea Klein. „Blockchain-Technologie im Supply Chain Management : Anwendungspotenziale und Kompetenzlücken."

Herausgeber: Wiesbaden : Springer Fachmedien. *HMD : Praxis der Wirtschaftsinformatik* 61 (2024): 266-283.

Kaspersky Labs GmbH . *Schule und Cyberbedrohungen.* 09. 10 2024. https://www.kaspersky.de/blog/how-to-protect-schools-from-cyberthreats/31698/ (Zugriff am 07. 02 2025).

Kersten, Heinrich, Jürgen Reuter, und Klaus Werner Schröder. *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz.* Wiesbaden: Springer Fachmedien, 2013.

Kienzle, Moritz Valentin. *Sensibilisierung und Schulung von Informationssicherheit für Lehrkräfte an öffentlichen Schulen: Studie zur gegenwärtigen Umsetzung und Entwicklung eines Konzepts für die Zukunft. Master's thesis.* Bremen: Faculty of Mathematics and Computer Science / Digital Media, 2022.

Kirvan, Paul. „How to build an incident response plan, with examples, template." Herausgeber: TechTarget. *Search Securtiy*, 10 2024.

Kurniawan, Ade, und Ahmad Fitriansyah. „What is Exploit Kit and How Does it Work?" *International Journal of Pure and Applied Mathematics*, 2018: 509-516.

Marszałek Sejmu, Rzeczypospolitej Polskiej. „Obwieszczenie z dnia 25 maja 2023 r. w sprawie ogłoszenia jednolitego tekstu ustawy o systemie ubezpieczeń społecznych." Dz.U. 2023, poz. 1230, 2023.

Marszałek Sejmu, Rzeczypospolitej Polskiej. „Obwieszczenie z dnia 4 listopada 2022 r. w sprawie ogłoszenia jednolitego tekstu ustawy o rachunkowości." Dziennik Ustaw 2023, poz. 120, 2023.

Messner, Michael. *Hacking mit Metasploit. Das umfassende Handbuch zu Penetration Testing und Measploit.* Heidelberg: d.punkt.verlag GmbH, 2015.

Metasploit, Documentation Team. *LDAP Workflows.* 15. 05 2024.

Minister Edukacji, Narodowej. „Rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia dokumentacji przebiegu nauczania.." Dziennik Ustaw, 2017.

Minister Rodziny, Pracy i Polityki Społecznej. „Rozporządzenie z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej." Dz.U. 2018, poz. 2369, 2018.

Moya, Moses. *Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems.* University of South Africa, 2014.

National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity.* 16. 04 2018. https://doi.org/10.6028/NIST.CSWP.04162018 (Zugriff am 09. 06 2025).

—. *Ramy cyberbezpieczeństwa wg NIST (CSF) 2.0.* 26. 02 2024. https://doi.org/10.6028/NIST.CSWP.29.pol (Zugriff am 07. 02 2025).

Nekkanti, Anusha, und Suma NR. „A Review on Secured File Systems Using Multi-Factor Authentication and Visual Cryptography in Cloud Environments.“ *International Research Journal of Modernization in Engineering Technology and Science*, 06 2022: 4433-4436.

Niederösterreich, Technologie- und InnovationsPartner. *Bedrohungen der Cybersicherheit auf dem Vormarsch – Unternehmen verstärken ihre Abwehrmaßnahmen.* 2023. https://www.tip-noe.at/news/bedrohungen-der-cybersicherheit/ (Zugriff am 05. 02 2025).

Olaoye, Favour, und Axel Egon. „Insider Threat Detection and Prevention.“ *Journal of Cyber Security*, 2024.

Ondrušková, Dana, und Richard Pospíšil. „The good practices for implementation of cyber security.“ *Contemporary Educational Technology* 15, Nr. no.3 (05 2023): 1-16.

Ott, Marc. *Die Zukunft der Unternehmens-Kommunikation: KI-basierte erweiterte E-Mail-Sicherheit.* Herausgeber: OS systems AG. 19. 01 2024.

Paul, Kirvan. *reliability of computers.* 03 2023. https://www.techtarget.com/whatis/definition/reliability (Zugriff am 05. 02 2025).

Paulsen, Christian. *Die OCTAVE-Risikoanalysemethode als selbstgesteuerter Einstieg ins Informationssicherheitsmanagement.* 5. DFN-Forum Kommunikationstechnologien – Verteilte Systeme im Wissenschaftsbereich, Bonn: Gesellschaft für Informatik e.V, 2012, 129-134.

PD – Berater der öffentlichen Hand GmbH. *Einführung in die Informationssicherheit für Schulen Handreichung für Schulträger und Schulen.* 31. 01 2023. https://www.pd-g.de/assets/Aktuell-im-Fokus/Schul-IT-Navigator/Einfuehrung_in_die_Informationssicherheit_fuer_Schulen_V1.0.pdf (Zugriff am 07. 02 2025).

Pohlmann, Norbert. *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung.* Bd. 2nd. Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2022.

—. „Cybersicherheit, IT-Sicherheit und Informationssicherheit – Definition und Abgrenzung.“ *IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz*, 02 2024.

Prema, Appan Kali, und Neresh V. Kumar. „Cyber security awareness among primary school teachers.“ *Journal of Social Sciences Review*, 2019: 17-20.

Priv.Doz. Dr. Lachmaye, Konrad, und Thomas Dr. Menzel. *Datenschutz für die digitale Schülerverwaltung.* Wien: Bundesministerium für Bildung und Frauen, 2015.

Rayanne, Azevedo. *Vulnerabilities, Threats & Risk: The Importance of Information Security in Your Organization.* 13. 10 2023. https://www.linkedin.com/pulse/vulnerabilities-threats-risk-importance-information-rayanne/ (Zugriff am 05. 02 2025).

Red, Hat. *What is LDAP Authentication?* 03. 06 2022. https://www.redhat.com/en/topics/security/what-is-ldap-authentication (Zugriff am 18. 05 2025).

Rieß-Marchive, Ulrike. „Expertenempfehlungen für Ransomware-Schutz von Backups." Herausgeber: TechTarget. *ComputerWeekly.de*, 07 2021.

Salvador Ruiz, Lourdes Cecilia, Lenin Carlos Llerena Alvarez, und Phuoc Huu Dai Nguyen. „Digital Education: Security Challenges and Best Practices." *Security Science Journal*, 12 2021: 65-76.

Shivanandhan , Manish. „How to Exploit the EternalBlue Vulnerability on Windows – A Step-by-Step Guide." 13. 03 2025.

Siebenhandl, Manuel. *Schaffung eines nachhaltigen IT-Security Managementkonzepts für kleine und mittlere Unternehmen. Master's thesis.* Wien: Universität Wien, 2011.

Sobota, Michael. *Datenschutz und IT-Sicherheit in der Schule.* Augsburg: Auer Verlag, 2022.

Spitz, Stephan, Michael Pramateftakis, und Joachim Swoboda. *Kryptographie und IT-Sicherheit.* 2. Wiesbanden: Vieweg +Teubner Verlag, 2011.

Stoiber, Regina. *Risikoanalyse durchführen – mit Muster / Vorlage und Beispiel.* 28. 04 2019. https://regina-stoiber.com/2019/04/28/risikoanalyse-durchfuehren-mit-muster-vorlage-und-beispiel/ (Zugriff am 05. 02 2025).

Stoneburner, Gary, Alice Goguen, und Alexis Feringa. *Risk Management Guid for Information Technology System.* Washington: U.S. Goverment Printing Office, 2002.

Strohmeyer, Heidrun. „Empfehlungen zur Nutzung digitaler Technologie an Schulstandorten." Bundesministerium für Bildung, Wissenschaft und Forschung, Wien, 2018.

Țîțu, Mihail Aurel, Bianca Alina Pop, und Costel Ceocea. „Risk Assessment of Physical Security within a Technologized Knowledge Based Organization." *MATEC Web of Conferences* 299, Nr. 04005 (2019).

Titus, Kristanto, Akhasni Setyo Prayoga Riza, Muhammad Nasrullah, Mustafa Kamal, und Wahyudidin S. „Risk Management for New Student Admission Information Systems at Higher Education using the Octave Allegroch." *IAIC International Conference Series*, 2023: 106-114.

Tzipora, Halevi, Memon Nasir, und Nov Oded. „Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks." *SSRN Electronic Journal*, 2015.

Vayansky, Ike, und Sathish Kumar. „Phishing – challenges and solutions." *Computer Freund & Security*, 2018: 15-20.

Verbraucherzentrale NRW. *Schadprogramme.* 2021. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Brosch_DINlang_Schadprogramme.pdf?__blob=publicationFile&v=10 (Zugriff am 06. 03 2025).

Vitla, Surendra. „Unsecured Remote Desktop Protocol (RDP) Access: A Gateway for Ransomware Attacks and Corporate Extortion." *Journal of Computer Science and Technology Studies*, 2024: 150-165.

Vukalovic, Jakob, und Damir Delija. „Advanced Persistent Threats - detection and defense." *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2015: 1324-1330.

Wagner, Paul, und Dalal Alharthi. „Comprehensive Cybersecurity Programs: Case-Study Analysis of a Four-Year Cybersecurity Program at a Secondary Education Institution in Arizona." *Cybersecurity Pedagogy and Practice Journal*, 04 2024: 37-63.

Waheed, Azheen, Bhavish Seegolam, Mohammad Faizaan Jowaheer, Chloe Lai Xin Sze, Ethan Teo Feng Hua, und Siva Raja Sindiramutty. „Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure." *Preprints*, 2024.

Wenzel-Benner, Christian, und Daniel Wasserrab. „Kryptographische Hashfunktionen: Historie, Angriffe und aktuell sichere Standards." European Mathematical Information Service, Rülzheim, 2015.

Wies, Eric. *Die vier wichtigsten Schutzziele der Informationssicherheit.* Herausgeber: BRANDMAUER IT. 17. 09 2024.

Wijayarathne, Senesh. *ISO 27001 Implementation.* 12 2022. https://www.researchgate.net/publication/372523436_ISO_27001_Implementation (Zugriff am 07. 02 2025).

Wirtschaftskammer Österreich. *Cyber-Versicherungen: Das Risiko einfach auslagern?* 03. 10 2024. https://www.wko.at/it-sicherheit/cyber-versicherungen-das-risiko-einfach-auslagern (Zugriff am 06. 02 2025).

Woody, C. Carol. *Applying Security Risk Management to Internet Connectivity in K-12 Schools and School Districts.* Graduate School of Computer and Information Sciences Nova Southeastern University, 2004.

Woody, Carol, Johnathan Coleman, Michael Fancher, Carol Myers, und Lisa Young. *Applying OCTAVE: Practitioners Report.* Technical Note, Carnagie Mellon University, 2006.

Zhang, Chenxiang. „Study on Security and Protection Strategy of Computer Network Information.“ Herausgeber: Atlantis Press. *Proceedings of the 2nd International Conference on Electronics, Network and Computer Engineering (ICENCE 2016)*, 2016.