Best Practices zur Sensibilisierung & Protektion gegenüber Ransomware in der Medizin

Schriftliches Artefakt SAT

Gruppe K: Ransomware in der Medizin

Hochschule Reutlingen Fakultät Informatik
Studiengang: Medien- und Kommunikations-Informatik

Martin Lauterbach, 810087

Luca Sebastian Schellhorn, 768425

Sebastian Vincent Schwarz, 768298

Abstract

Die fortschreitende Digitalisierung im Gesundheitswesen birgt neue Risiken: Ransomware und verbundene Phishing-Angriffe bedrohen die Integrität und Verfügbarkeit kritischer Daten. Mit der Verabschiedung des Digital-Gesetzes-DigiG und des Gesundheitsdatennutzungsgesetzes - GDNG durch den Deutschen Bundestag am 14. Dezember 2023 wurden wichtige Schritte zur Digitalisierung unternommen, die jedoch auch neue Angriffsflächen schaffen. Es werden praxisorientierte Strategien vorgestellt, die sowohl auf technologische Lösungen als auch auf die Schulung des Personals abzielen, um ein umfassendes Schutzkonzept gegen Ransomware-Angriffe zu entwickeln. Die Arbeit bietet einen Einblick in die Funktionsweise von Ransomware, identifiziert spezifische Risiken für das Gesundheitswesen und schlägt effektive Sensibilisierungs- und Präventionsmaßnahmen vor.

Stand: 23. Juni 2025

SoSe 2024

Inhaltsverzeichnis

1 Einleitung (Lauterbach) 1
1.1 Zielsetzung der Arbeit 1
1.2 Methodik und Aufbau der Arbeit 1

2 Grundlagen der Ransomware und KIS-Sicherheit (Schwarz) 2
2.1 Definition und Funktionsweise von Ransomware 2
2.2 Krankenhausinformationssystem 4

3 Sensibilisierung (Lauterbach) 5
3.1 Implementierung von Leitfäden zur Bedrohungsbehandlung 6
3.2 Social-Engineering 7
3.2.1 Methodiken 7
3.2.2 Links 8
3.2.3 Anhänge 9

4 Prävention (Schellhorn) 9
4.1 Einsatz von Antivirensoftware und Firewalls 10
4.2 Implementierung von Backupstrategien und Zugriffskontrollen 11
4.3 Spezifische Regulierungen bestehender Systeme 12

5 Schlussfolgerung und Ausblick (Schwarz & Schellhorn) 13
5.1 Empfehlungen für die Praxis 13
5.2 Ausblick auf zukünftige Forschungen 13

6 Quellverzeichnis 15
6.1 weitere Hilfsmittel 16

7 Erklärung zur wissenschaftlichen Arbeit 17

1 Einleitung (Lauterbach)

Am 14.Dezember 2023 verabschiedete der Deutsche Bundestag das Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz-DigiG)[1].
Dies geschah zusammen mit dem "Gesetz zur verbesserten Nutzung von Gesundheitsdaten"(Gesundheitsdatennutzungsgesetz - GDNG)[2]. Zielführend war die Beschleunigung der seit den frühen 2000er angestrebten Implementierung einer elektronischen Patientakte (ePA), sowie dem neueren elektronischem Rezept (E-Rezept). Diese Daten sollen geplant rein digital hinterlegt und zugreifbar gemacht werden.

Durch die zunehmende Digitalisierung des Gesundheitswesen steigt auch die Anzahl der Möglichkeiten durch Aktoren, Angriffe auf kritische IT-Systeme vorzunehmen, die nicht nur zu finanziellen Verlusten führen können, sondern auch das Wohl der Patienten gefährden, indem gesundheitskritische Maßnahmen temporär nicht mehr in geplanten Rahmen passieren können.

Ransomware, eine Form der Malware, die Daten verschlüsselt und Lösegeld für deren Freigabe fordert, hat sich als eine ernsthafte Bedrohung etabliert. Die Sensibilisierung gegenüber Ransomware-Angriffen ist daher von Bedeutung, um die Sicherheit patientenbezogener Daten und die Kontinuität der medizinischen Versorgung zu gewährleisten.

1.1 Zielsetzung der Arbeit

Das Ziel der Arbeit ist, Strategien vorzustellen, wie medizinisches Personal und IT-Abteilungen in Krankenhäusern für diese Bedrohungen sensibilisiert und entsprechende Präventionsmaßnahmen implementiert werden können.

1.2 Methodik und Aufbau der Arbeit

Die Arbeit ist strukturiert in die Bereiche des Bedrohungsverständnisses (der speziellen Gefahr der Ransomware sowie dem klinischen Umfeldes), der Sensibilisierung für Personal (Phishing und Social Engineering), sowie technischer Lösungen. Abschließend wird ein Rückblick auf die aufgestellte Thematik gezogen und eine mögliche zukünftige Entwicklung von Ransomware-Angriffen prognostiziert.

Durch eine systematische Literaturrecherche wurden wissenschaftliche Artikel der 2024 vorausgehenden 5 Jahren identifiziert und unserem Arbeitsziel hin analysiert.

2 Grundlagen der Ransomware und KIS-Sicherheit (Schwarz)

Ransomware wird definiert als eine Form von Schadsoftware, die darauf abzielt, den Zugriff auf Daten und Systeme zu blockieren oder einzuschränken, häufig durch Verschlüsselung, und die Freigabe dieser Ressourcen nur gegen Zahlung eines Lösegeldes ermöglicht [3, S.4]. Dies stellt einen Angriff auf das Sicherheitsziel der Verfügbarkeit dar und ist eine digitale Form der Erpressung [3, S.4]. Die erste dokumentierte Ransomware-Attacke ereignete sich im Jahr 1989 und zielte auf die Gesundheitsbranche ab [4]. Bis heute bleibt die Gesundheitsbranche ein primäres Ziel solcher Angriffe [5][6].

Die globale Bedrohung durch Ransomware hat sich seit der COVID-19 Pandemie deutlich erhöht[7]. Es werden mehr Fälle bekannt, in denen gestohlene Daten veröffentlicht werden. Das Veröffentlichen der Daten erhöht den Druck auf die Opfer, Lösegeld zu zahlen. Ransomware hat im Laufe der Zeit verschiedene Varianten entwickelt. Manche verschlüsseln Daten dauerhaft, selbst nach Entfernen des Schadprogramms. Diese Varianten verwenden oft sichere Verschlüsselungs-Algorithmen. Eine Entschlüsselung ist dann in der Regel unmöglich [3, S.4].

Für Kriminelle bieten Ransomware-Angriffe den Vorteil eines direkten Geldtransfers zwischen Opfer und Täter über anonyme Zahlungsmittel wie Bitcoin und Monero, im Gegensatz zu anderen Cyber-Angriffen, die Mittelsmänner oder Warenagenten erfordern [3, S.4]. Für Opfer unterscheidet sich Ransomware von anderen Arten von Schadsoftware wie Banking-Trojanern dadurch, dass der Schaden sofort eintritt und konkrete Konsequenzen hat, wie den Verlust von persönlichen oder geschäftlichen Daten [3, S.4].

2.1 Definition und Funktionsweise von Ransomware

In den letzten Jahren gab es einen exponentiellen Anstieg von Cyberangriffen [8]. Der gefährlichste Cyberangriff weltweit ist der Ransomware-Angriff [8]. Die Verschlüsselungstechnologie, die von den Angreifern verwendet wir, erschwert es den Opfern, ihre Daten ohne Zahlung des geforderten Lösegelds wiederherzustellen [9]. Dieser Umstand macht Ransomware zu einer Bedrohung für Einzelpersonen, Unternehmen und sogar staatliche Einrichtungen.

Unter den Ransomware-Angriffen sind zwei Hauptarten bekannt: Crypto Ransomware und Locker Ransomware. Bei einem Crypto-Ransomware-Angriff verschlüsseln die Angreifer Daten auf dem betroffenen Gerät. Im Gegensatz dazu blockiert Locker Ransomware nicht die Daten, sondern sperrt lediglich den Zugang zum betroffenen System des Opfers [8].

Ein zusätzliches Anliegen im Kontext von Ransomware-Angriffen betrifft das Internet der Dinge (IoT). Da IoT-Geräte zunehmend in unserem Alltag präsent sind und sensible

Daten verarbeiten, sind sie ebenfalls anfällig für solche Angriffe. Ransomware-Angriffe auf IoT-Geräte können nicht nur vorübergehenden Datenverlust verursachen, sondern auch dauerhafte Schäden, indem Informationen unwiederbringlich verloren gehen [9].

Die Hauptmotivation für Ransomware-Angriffe liegt im Streben nach finanziellen Gewinnen [3, S. 8-9]. Diese Angriffe werden durch die Bereitschaft von Opfern, Lösegelder zu zahlen, und die Verfügbarkeit von Cyber-Versicherungen unterstützt, insbesondere wenn die Sicherheitssysteme unzureichend sind. Opfer stehen vor einem Dilemma: Kooperation würde langfristig die Motivation für weitere Angriffe verringern, aber die individuelle Zahlung erhöht die Wahrscheinlichkeit zukünftiger Angriffe. Das Bundesamt für Sicherheit in der Informationstechnik stellt fest, dass Unternehmen aufgrund verschiedener Faktoren wie der Anzahl der betroffenen Rechner und der Wert der Daten im Visier von Ransomware stehen [3, S. 8-9].

Neben finanziellen Motiven können auch staatliche Akteure Ransomware einsetzen, um Sanktionen zu umgehen oder Devisen zu beschaffen. Sabotage ist eine weitere Motivation, die politisch oder wirtschaftlich motiviert sein kann und auf die Schädigung des Opfers abzielt. Es gibt auch Fälle, in denen Ransomware zur Ablenkung von Spionageoperationen oder aus anderen Gründen eingesetzt wurde, wie beispielsweise für Hacktivismus oder das Streben nach Aufmerksamkeit. Insgesamt lassen sich folgende Motivationen für Ransomware-Angriffe feststellen: finanzielle Gewinne, Sabotage, Ablenkung, Aufmerksamkeit und das Erreichen von Zielen von Hacktivisten. Vor der Verschlüsselung entwenden einige Cyberkriminelle Daten und setzen das Opfer unter Druck, indem sie mit ihrer Veröffentlichung drohen. Dies betrifft auch vertrauliche Geschäftsdaten, die vor Wettbewerbern geschützt werden müssen [3, S. 8-9].

Potenzielle Schäden durch Cyber-Sicherheitsvorfälle für Organisationen lassen sich in drei Hauptkategorien einteilen: Eigenschäden, Fremdschäden und Reputationsschäden. Eigenschäden umfassen Kosten durch Betriebsbeeinträchtigungen, Krisenreaktion und -beratung sowie forensische Untersuchungen und Wiederherstellungsaufwände. Fremdschäden treten auf, wenn rechtliche oder vertragliche Verpflichtungen gegenüber Dritten nicht erfüllt werden können, insbesondere bei Kritischen Infrastrukturen. Reputationsschäden entstehen durch den Verlust von Ansehen und Kunden aufgrund eines Angriffs, was zusätzliche Investitionen in Werbung und Kundenbindung erfordert[3, S. 6].

Die Schätzung der Kosten von Cyber-Sicherheitsvorfällen hängt von den individuellen Rahmenbedingungen und Gefährdungen einer Organisation ab. Erfolgreiche Ransomware-Angriffe können Schäden in allen genannten Kategorien verursachen. Das Ausmaß der Schäden ist stark von der technischen und organisatorischen Vorbereitung der betroffenen Organisation abhängig. Entscheidende Faktoren sind die Zeit bis zur Identifizierung des Vorfalls, die Effizienz bei der Identifizierung infizierter Geräte, die Verfügbarkeit

aktueller Backups, die Vorbereitung und Übung von Wiederherstellungsmaßnahmen sowie der Umfang der Daten- und Gerätebetroffenheit. Eine Infektion kann zu erhöhtem Arbeitsaufwand, temporären Ausfällen von Geschäftsprozessen und sogar zum Neuaufbau der gesamten IT-Infrastruktur führen. [3, S. 6-7].

2.2 Krankenhausinformationssystem

Ein Krankenhausinformationssystem (KIS) ist nicht eine einzige spezifische Software, sondern beschreibt die Gesamtheit aller eingesetzten Mittel zur Verwaltung von Daten und Informationen innerhalb eines Krankenhauses. Es umfasst computergestützte Systeme, deren einzelne Komponenten von verschiedenen Herstellern stammen können. Das KIS ermöglicht die zentrale Datenverwaltung und -weitergabe aus verschiedenen Netzwerken. Das KIS umfasst alle informationstechnologischen Systeme, die im Krankenhaus medizinische und administrative Daten erfassen, bearbeiten und weitergeben. Dabei integriert es Funktionen zur Datenbereitstellung auf Servern, Arbeitsplätzen und mobilen Geräten sowie traditionelle papierbasierte Dokumentations- und Kommunikationsmethoden. Der Begriff KIS bezieht sich in der Regel auf die computerbasierten Komponenten. [10, S. 249]

Patientendaten, die in KIS gespeichert sind, sind äußerst sensibel und bedürfen eines hohen Schutzes. Diese Daten enthalten persönliche Gesundheitsinformationen, die sowohl intim als auch für die weitere Behandlung relevant sind [11]. Die Veröffentlichung oder Manipulation dieser Daten kann schwerwiegende psychische Belastungen verursachen und zu Schäden für die Patienten führen. Im digitalen Zeitalter verschärft die Digitalisierung dieses Risiko noch weiter, da externe Angriffe oder unberechtigte Zugriffe auf große Mengen von Patientendaten erleichtert werden können. Mitarbeiter werden oft als Schwachstelle für solche Angriffe identifiziert, da sie durch Phishing-E-Mails oder das versehentliche Anschließen von USB-Sticks an das Netzwerk des Krankenhauses manipuliert werden können[12]. Es ist daher wichtig, technische Maßnahmen zu ergreifen, um solche Angriffe zu verhindern, wie beispielsweise die Sperrung von Schnittstellen für externe Geräte oder die Implementierung automatischer Anmeldesysteme, um den Zugang zu sensiblen Systemen zu kontrollieren. Darüber hinaus stellen auch die Zugangspunkte zum KIS eine potenzielle Schwachstelle dar, da ungeschützte Monitore oder mobile Visitenwagen unbefugten Zugriff ermöglichen können, wenn Mitarbeiter sich nicht ordnungsgemäß abmelden. Es ist daher wichtig, strenge Sicherheitsprotokolle zu implementieren, um den unberechtigten Zugriff auf Patientendaten zu verhindern [12].

Ein KIS ist anfällig für verschiedene Arten von Cyberangriffen, insbesondere für Ransomware-Angriffe, die in jüngster Zeit eine bedeutende Bedrohung für Computer- und Mobilgerätenutzer darstellen [5]. Die Einfallstore für solche Angriffe sind vielfältig und umfassen

verschiedene Methoden, die in der folgenden Tabelle 1 dargestellt sind:

Tabelle 1: Mögliche Angriffsarten und deren Beschreibung

Angriffsart	**Beschreibung**
Email-Phishing	Angreifer versenden bösartige Dateianhänge und URLs über E-Mails, um Daten zu exfiltrieren, Anmeldeinformationen zu stehlen und Ransomware einzuschleusen[10, S. 81].
Remote Desktop Protocol (RDP)	Angreifer nutzen Brute-Force-Angriffe, um sich über RDP-Zugriff zu verschaffen[5].
Exploit Kits	Toolkits, die Schwachstellen ausnutzen, indem sie bösartigen Code auf Websites platzieren, um Ransomware herunterzuladen und auszuführen[5].
Watering Hole Attacks	Angreifer injizieren bösartige Skripte auf häufig besuchten Websites, um Opfer zu infizieren[5].
Wechselmedien und USB	Angreifer erhalten physischen Zugang und schleusen Ransomware über infizierte Wechselmedien wie USB-Sticks ein[5].
Installation raubkopierter Software	Ransomware kann in heruntergeladener Software versteckt sein und so installiert werden[5].
Microsoft Office-Makros	Angreifer nutzen Makros in Office-Dokumenten, um Ransomware einzuschleusen[5].
Botnets	Botnets, gesteuert von einem Command-and-Control-Server, können Ransomware herunterladen und ausführen oder DDoS-Angriffe durchführen[5].
Brute-Force-Angriffe	Automatisierte Angriffe zum Erraten von Passwörtern, um Zugriff auf geschützte Gesundheitsinformationen zu erhalten. [13].

In den letzten Jahren ist die Anzahl der Ransomware-Angriffe angestiegen [5]. Gesundheitseinrichtungen sind zu einem wichtigen Ziel dieser Angriffe geworden [5].Daher ist es notwendig, dass KIS robuste Sicherheitsmaßnahmen implementieren, um sich wirksam gegen solche Angriffe zu schützen.

3 Sensibilisierung (Lauterbach)

Um der Gefahr durch Ransomware entgegenzuwirken, gibt es die Möglichkeit der Sensibilisierung (Schulung, Unterrichtung, klare Aushänge) von Mitarbeiter*innen. Dies soll helfen, wenn versucht wird, durch menschliche Einflussnahme einen Ransomware-Angriff zu begehen. Dies nennt sich Social Engineering, da anstatt auf einem rein tech-

nischen Weg, der Angriff einen Teil seiner Strategie auf die Menschen in einem System setzt. Diese werden dazu bewegt werden, Informationen preiszugeben oder sogenannte Schadsoftware direkt im System auszuführen. Phishing beschreibt diesbezüglich den Vorgang eines Angreifers, durch E-Mail-Verkehr sein Ziel dazu zu bewegen, für Ihn vorteilhafte Aktionen durchzuführen.
Diese Schulungen haben dabei Limitierungen. Es kann die Möglichkeit bestehen, dass Schulung das Lehrmaterial und die Gefahr nicht wirkungskräftig und langanhaltend an Mitarbeiter vermittelt. Die Alternative wäre es, Mitarbeiter nicht über die möglichen Gefahren und Wege eines Ransomware-Angriffes zu unterrichten, und Allein auf Ihr Vorwissen zu vertrauen. Die aufzuführenden sensibilisierenden Informationen und Strategien können dazu genutzt werden, zu versuchen, Mitarbeiter*innen laufend der Gefahr und Ihrer Rolle allzugegenwärtigen.

3.1 Implementierung von Leitfäden zur Bedrohungsbehandlung

Ein laut Oles 2023 in der wissenschaftlichen Literatur oft benanntes Prozedere, für den vollumfänglichem Umgang mit der Bedrohung unerlaubten Zugriffes, bis hin zu festgestellten Angriffen, hier beidsam für die Gefahr von Ransomware, ist PICERL der Organisation SANS.org.

*Vorbereitung (**P**reparation)*
Im Schritt der Vorbereitung sind Strategien wie die Sensibilisierung der Mitarbeiter sowie die Implementierung von technischen Regeln im Vordergrund.
Für technische Implementierungen von Präventionen als Teil der Vorbereitung (Preparation) siehe Kapitel 4: Prävention.

*Erkennung (**I**dentification)*
Der Schritt der Identifikation weitet sich auf das stetige informieren nach aufkommenden Sicherheitslücken in genutzten Systemen aus. Er beinhaltet die kontinuierliche Suche, Dokumentation und Researche nach verdächtigem Verhalten. [14, S. 36]

*Eindämmung (**C**ontainment)*
Das Eindämmen beinhaltet das Isolieren des von der Sicherheitslücke oder dem bereits von Verschlüsselung betroffenem Teil des Systems vom Zugriff auf den Rest des

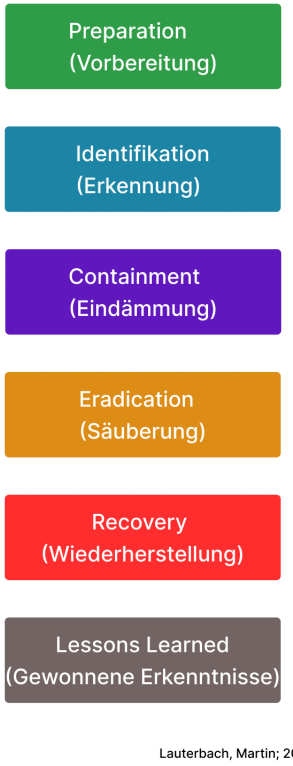

Abbildung 1: PICERL: incident response framework, erstellt von Lauterbach. Nach Oles 2023 [14, S. 34]

Netzwerks.[14, S. 37]

*Beseitigung (**E**radication)*

Dateien und Prozesse, welche unerlaubt Vorgegangen sind, können gelöscht werden.[14, S. 38]

*Erholung (**R**ecovery)*

Es kann sicher gestellt werden, dass die wiederhergestellten Strukturen keine weiteren Sicherheitsrisiken beinhalten. [14, S. 39][15, S. 188]

*Aufarbeitung (**L**essons Learned)*

Im letzten Teil des Schematas soll gelernt werden, welche Schlüsse aus dem Angriff gezogen werden können: Wie konnte der Ransomware-Angriff geschehen, wie kann das System verbessert werden und wie wird der Leitfaden in Zukunft fortgesetzt.[14, S. 40]

3.2 Social-Engineering

Phishing-E-Mails täuschen oft legitime Kommunikation vor, um Nutzer dazu zu verleiten, schädliche Anhänge zu öffnen oder auf gefälschte Links zu klicken. Dies kann Malware mit erhöhter Berechtigung auszuführen, oder das Ziel mit bekannten Interfaces vortäuschen, Benutzernamen und Passwörter an den Angreifer zu übermitteln.[15, S. 64]Dieses Nutzen von Mitarbeiter*innen als Teil der Angriffs-Kette nennt sich Social-Engineering.

Sensibilisierungen können darauf abzielen, Mitarbeiter darüber aufzuklären, wie sie verdächtige E-Mails erkennen können, indem sie auf ungewöhnliche Absenderadressen, Rechtschreibfehler, unerwartete Anfragen nach persönlichen oder vertraulichen Informationen und andere verdächtige Merkmale achten.

Ein Grundpfeiler der Sensibilisierung kann dementsprechend das ständige vor-augenhalten sein, dass man als Nutzer zuerst denken, dann klicken soll, wenn es um verdächtige E-Mails geht.[14, S. 35]

3.2.1 Methodiken

Das Social-Engineering setzt sich aus mehreren Methoden zusammen. Eine Mehrzahl an Beispielen bezieht sich hier auf monetäre Betrüge. Jede einzelne dieser Maschen kann jedoch genutzt werden, einen Benutzer dazu zu bringen, einem Angreifer Zugriff auf sensible Server und Daten zu geben.[14, S. 24][15, S. 80]

Eine Methode, wie ein Angreifer seinem Ziel vortäuscht in einem Vertrauensverhältnis zu stehen, ist die Nutzung eines dem Ziel bekanntem, dem Angreifer zur Verfügung stehendem, Accounts, oder eines Accounts, wessen Adresse sich einem vertrauenswürdigem Accounts ähnelt. Dies kann ermöglichen, dass Ziel mit höherer Wahrscheinlichkeit zum gewünschten Effekt hin zu bringen. Diese Ziel kann vom 'Aushelfen durch ein wenig Geld' hin zu dem Preisgeben von Informationen reichen. [14, S. 24]

Ein Eindringling könnte auch versuchen, durch die Nutzung von Emotionen den Nutzer zum schnellen und undurchdachtem Handeln zu bringen. Oftmals wird hier Scham, Schuld und Dringlichkeit genutzt. Der Nutzer möchte zum Beispiel nicht, dass eine vom Angreifer vorgetäuschte Chance verloren geht oder, dass persönliche Informationen preisgegeben werden, und fühlt sich daher gedrängt, dem Ziel des Angreifers entgegenzukommen. [14, S. 25]
Damit verbunden ist auch die Taktik, dass ein Angreifers durch attraktive, weit unter dem normalen Marktpreis liegenden, Angeboten versucht, einen Nutzer dazu zu bringen, zum Beispiel zu erst eine kleine Summe Geld zu senden, um dann die große Summe Geld zurückzubekommen. [14, S. 25]
Eine Möglichkeit, bei Verdacht den Betrugsversuch aufzudecken, ist die Aufforderung der Identitätsbestätigung. Wenn der Sender dies nicht zufriedenstellend ausführen kann, liegt der Verdacht nahe, dass es sich bei der E-Mail um einen Pishing-Versuch handelt. [14, S. 26]
Auch wenn diese Methodiken ein weites Feld von Betrugsmaschen abdeckt, haben sich diese Angriffstechniken in der Vergangenheit weiterentwickelt und Oles (2023) prognostiziert, dass sich Diese weiter entwickeln werden.[14, S. 28] Er behauptet zusätzlich, dass keine einzelne vollständige Liste an Methoden existiert. [14, S. 28]
Die Methodiken zeigen, dass selbst Mitarbeiter*innen, die kürzlich geschult worden sind, und diese Schulung aufnehmen konnten, jederzeit Ziel und Opfer eines Phishing-Angriffes werden können. Auf der einen Seite versuchen die Methoden, grundlegende Emotionen hervorzurufen, die es dem Ziel schwer machen können, jeden Link zu überprüfen, jede Information abzuwägen und jede Datei zu scannen. Auf der anderen Seite stehen die Schulungen und Sensibilisierungen, welche nicht jedem Mitarbeiter gleich langanhaltend sensbibilisieren können.

3.2.2 Links

Ein in einer E-Mail befindlicher Link kann auf mehreren Weisen auftreten. Ein textbasierter Link kann durch ein sogenannter Verkürzer (englisch: shortner) wie 'bit.ly' maskiert sein, was es für den Empfänger erschwert, den Betrugsfall zu erkennen. Ein Link kann sich zudem eingebettet in einem Bild befinden, welches sich zum Beispiel bei einem Drücken öffnet. Zudem ist es Möglich, dass ein schädlicher Link sich in den 'Abmelden'-Fußzeichen einer Email befindet, oder eingebettet als 'Hier', was den Link selbst obfusziert.
Auf der geöffneten Webseite kann dann Informationen gesammelt oder Code ausgeführt werden. [14, S. 53–58]
Eine Prävention, dass auf diese Links nicht ohne Kontrolle gedrückt wird, kann durch Sensibilisierung der Mitarbeiter durch Weiterbildungen vorliegen. Da zuvor genannte Limitierungen gelten - dass nicht zwingend lang-anhaltend geschult worden sein kann -

ist technisch in vielen Anwendung ein sogenanntes Link-Hovering vorzufinden. Wie der Name suggeriert, kann ein Link ohne dessen Ausführung in der Regel angezeigt werden, indem je nach Anbieter: Auf Desktop-Anwendungen durch ein Halten des Zeigers über dem Link, und auf Smartphones, durch das lange Gedrückt-halten des Links. Hier kann es die Möglichkeit geben, dass ein Nutzer einen Link analysieren kann.[14, S. 61]
Es gibt verschiedene online-tools (Stand: 15/04/2024), die es ermöglichen, einen Link zu scannen, bevor man Ihn auf dem eigenen Gerät nutzt. Oles (2023) nennt hier die folgenden Webseiten: 'VirusTotal', 'urlscan.io' und 'urlvoid.com'. [14, S. 70–74]

3.2.3 Anhänge

Wenn eine Methode des Social-Enginnering effektiv am Ziel genutzt wird, kann die Möglichkeit bestehen, dass geschultes Personal schädliche Anhänge ausführt, trotz Allvergegenwärtigung vor Phishing-Gefahr. [14, S. 77]
Strategien, die sich geschulte Mitarbeiter*innen laut Oles (2023) dennoch fragen können:
'Würde der Absender dieses Dateiformat senden?'
'Habe ich nach diesem Dateiformat gebeten?'
'Benötige ich diese Information?'
'Stimmt der Anhang mit dem Inhalt der Email überein?'
[14, S. 78]
Ein sogenanntes dynamisches Analysieren kann durch den Nutzer durchgeführt werden. Dies geschieht, indem die Datei anstatt direkt ausgeführt, lokal gespeichert und dann auf bestimmten Webseiten hochgeladen analysiert wird. Genannt werden kann hier laut Oles (2023) (Stand: 15/0/2024): "www.virustotal.com", "www.any.run", "www.hybrid-analysis.com"[14, S. 61]

4 Prävention (Schellhorn)

Viele Computer sind von hochentwickelten Ransomware-Programmen infiziert, aber Schutzmaßnahmen sind nicht immer effektiv.[16] Den Besitzern von Computersystemen bleibt daher häufig nur noch die Lösegeldzahlung übrig.[16] Der erste Schritt zum Schutz gegen Ransomware-Angriffe ist die Vorbeugung. Für die Entwicklung wirksamer Schutzmaßnahmen ist es von Bedeutung, zu erforschen, wie sie funktionieren.[16]
Zur Vorbeugung und Absicherung eines Computersystems vor Ransomware-Angriffen existieren einige effektive Maßnahmen. Die meisten davon sind in der Vorbeugungsphase hilfreich. Investitionen in Sicherheitswissen und Sicherheitsprogramme können dazu beitragen, schwerwiegende Schäden und finanzielle Schäden zu vermeiden. Es ist leichter, vorzubeugen, als später wieder herzustellen.[16]
Der renommierte Cybersicherheitsspezialist S. Morgan sagt dass, Lösegeldzahlungen

die geringste Kostenkomponente darstellen. Daher ist Prävention zwar wichtig und unumgänglich, aber auch sehr teuer.[16]
Die zuverlässigste und effektivste Methode zum Schutz persönlicher Daten, Informationen und des gesamten Computersystems besteht jedoch in der Kombination verschiedener Werkzeuge: Wissen, Software und Vorsicht.[16] Die besten Präventionsmaßnahmen gegen Ransomware-Angriffe sollten in drei Bereiche organisiert sein: Die Entwicklung von Programmen, die eine professionelle Managementprüfung potenzieller Risiken und Bedrohungen durch Ransomware-Angriffe ermöglichen, die Analyse jeder Datei und jedes Computers.[16] Die Entwicklung spezieller Filter für eingehende E-Mails und heruntergeladene Dateien, die Ransomware-Bedrohungen erkennen können. Unternehmen sollten sich für die Organisation von Schulungsprogrammen zum Schutz vor Ransomware-Angriffen für ihre Mitarbeiter interessieren. [16]

4.1 Einsatz von Antivirensoftware und Firewalls

Neue Varianten von Schadsoftware werden nicht sofort durch herkömmliche Antiviren-Signaturen erkannt. Daher ist es ratsam, alle verfügbaren Module professioneller Antivirensoftware zu nutzen, um Infektionen zu verhindern.[17, S.13] Insbesondere hostbasierte Intrusion Prevention (IPS)-Module und Cloud-Dienste können wirksam sein, um Ransomware zu bekämpfen, was erklärt, warum die Erkennung an Gateways oft weniger effektiv ist als auf Endgeräten.[17, S.13]
Zusätzliche Antiviren (AV)-Module können die Ausführung oder Verbreitung von Malware unterbinden, indem sie verdächtiges Verhalten blockieren. Kunden mit Supportverträgen sollten ihre AV-Hersteller nach zusätzlichen Schutzmöglichkeiten und Konfigurationshinweisen fragen.[17, S.13]
Der Begriff Virenschutz ist veraltet und umfasst nicht mehr das gesamte Produktportfolio, das in Enterprise-Umgebungen benötigt wird. Eine umfassende IT-Sicherheitsarchitektur ist erforderlich, die Endgeräte, Server, Gateways und spezielle Anwendungen wie Webserver, E-Mails und Datenbanken umfasst.
Es muss unabhängig vom Betriebssystem geprüft werden, ob professionelle Viren-Schutzprogramme für den Einsatz in Unternehmen und Behörden erforderlich sind. Enterprise-Produkte bieten erweiterte Konfigurationsmöglichkeiten und zentrale Administration. Die Aktualisierung auf die neueste Programmversion ist ebenfalls wichtig, da neue Erkennungsverfahren oft nur in aktuellen Versionen integriert sind.
Wenn verdächtige Aktivitäten von Virenschutz-Lösungen gemeldet werden, sollten diesen unbedingt nachgegangen werden.
Viele aktuelle Schadprogramme auf Windows-Systemen verlassen sich auf PowerShell, um ihr schädliches Potenzial zu entfalten. Durch Einschränkungen der PowerShell kann die Ausführung des Schadcodes häufig verhindert werden.[17, S.13]
Es ist jedoch wichtig, die Auswirkungen solcher Maßnahmen auf den regulären Betrieb

zu prüfen. Zum Beispiel kann der „ConstrainedLanguage Mode“ in PowerShell aktiviert werden, um bestimmte Befehle und Funktionen zu blockieren, obwohl dieser Modus möglicherweise umgangen werden kann.
Darüber hinaus kann der Internetzugriff für PowerShell über eine Firewall blockiert werden, was viele Schadprogramme einschränkt, da sie oft weitere Module oder zusätzliche Schadprogramme nachladen müssen.
Zusätzlich zur Beschränkung ist es ratsam, das Logging aller PowerShell-Befehle (via GPO) zu aktivieren, um die Aktionen von Angreifern im Nachhinein nachvollziehen zu können. [17, S.13]

4.2 Implementierung von Backupstrategien und Zugriffskontrollen

Backups sind eine Schutzmaßnahme, um im Falle eines Ransomware-Angriffs die Datenverfügbarkeit und einen zügigen Betriebsfortschritt sicherzustellen. Jede Organisation sollte ein Datensicherungskonzept implementieren, das verschiedene Backup-Methoden wie Cloud oder NAS berücksichtigt. Je nach Unternehmensgröße kann es ratsam sein, lediglich Server- und Netzlaufwerksdaten zu sichern und bei Infektionen Clients neu einzurichten, um den Verlust wichtiger Daten zu vermeiden.[17, S.8]
Es ist zu prüfen, ob neben den Inhaltsdaten auch Konfigurationen gesichert werden sollten. Angreifer suchen zunehmend nach Backups und verschlüsseln diese zusammen mit Produktivsystemen. Man kann eine Offline-Kopie zu sichern, um sie vor Remote-Angriffen zu schützen. Diese Trennung sollte regelmäßig überprüft werden, um sicherzustellen, dass keine unerlaubten Zugriffe erfolgen.[17, S.8]
Neben dem Schutz vor Ransomware bieten Backups auch Sicherheit vor physischen Bedrohungen wie Brand oder Hochwasser, indem Kopien an verschiedenen geografischen Standorten verteilt werden. Eine sorgfältige Planung und Vorbereitung der Wiederanlauf- und Wiederherstellungsprozesse ist unerlässlich und sollte regelmäßig getestet werden, um mögliche Komplikationen frühzeitig zu erkennen.[17, S.8]
Es ist wichtig zu überprüfen, ob die Backups mit Malware infiziert sein könnten, bevor sie wiederhergestellt werden. Bei der Wiederherstellung sollten Kopien der Backups oder Write-Blocker verwendet werden, insbesondere wenn nicht ausgeschlossen werden kann, dass die Systeme infiziert sind. Beachten Sie jedoch, dass Backups nicht vor dem Abfließen verschiedener Daten schützen können, die Angreifer möglicherweise kopieren und veröffentlichen.[17, S.8]
Die Implementierung von Zugriffskontrollen ist von entscheidender Bedeutung für die Sicherheit eines Netzwerks. Bei allen externen Zugriffspunkten wird eine Multi-Faktor-Authentifizierung verwendet, insbesondere für administrative Zugänge. Darüber hinaus verfügt nur eine begrenzte Anzahl von Administratoren über hoch privilegierte Konten im Active Directory. Diese Administratoren verwenden separate, besonders geschützte Clients für ihre administrativen Aufgaben, um das Risiko von Kompromittierungen zu

minimieren.[17, S.8]
Die Netzwerksegmentierung trägt dazu bei, Schäden zu begrenzen, da sie die Ausbreitung von Ransomware auf benachbarte Systeme einschränkt. Insbesondere ist die sichere Verwendung von Administrator-Konten entscheidend, da sie einen zentralen Bestandteil des Sicherheitskonzepts darstellen. Die Begrenzung von Client-zu-Client-Verbindungen kann die Ausbreitung von Angriffen erheblich verlangsamen.[17, S.8]
Eine bedarfsgerechte Konzeption des Active Directory kann das Risiko eines übergreifenden Vorfalls erheblich reduzieren. Durch die Unterteilung in verschiedene Ebenen mit Zugriffseinschränkungen können Rechte innerhalb des Netzwerks effektiv kontrolliert werden. Die Verwendung von Active Directories mit separaten Forests"kann die Ausbreitung von Malware über verschiedene Organisationseinheiten hinweg begrenzen.[17, S.8]
Die erfolgreiche Umsetzung dieser Maßnahmen erfordert sorgfältige Planung und Umsetzung. Es ist wichtig, dass diese Schritte nicht trivial sind, da sie die Grundlage für eine effektive Netzwerksicherheit bilden. [17, S.8]

4.3 Spezifische Regulierungen bestehender Systeme

Sicherheit von Windows-PCs und Servern kann durch einfache, aber wichtige Einstellungen erheblich verbessert werden. Häufige Angriffsvektoren auf Windows-Systeme sind bestimmte Funktionen oder Dienste, die standardmäßig inaktiv oder unkonfiguriert sind und von vielen Benutzern nicht bekannt oder genutzt werden. Durch das Abschalten dieser Einfallstore kann die IT-Sicherheit erheblich gestärkt werden, auch wenn dies möglicherweise zu geringfügigen Einschränkungen führen kann.[10, S. 53]
Sicherheitsexperten versuchen, die Angriffsfläche des Systems zu reduzieren oder sie ganz zu eliminieren, indem sie Funktionen oder Dienste abschalten, die nicht benötigt werden.[10, S. 53] Dies kann dazu führen, dass Angriffe, die diese Technik nutzen wollen, ins Leere laufen. Überprüfung der Standardeinstellungen: Die Standardeinstellungen des Betriebssystems sind oft unsicher, um mehr auf die Bequemlichkeit des Benutzers zugeschnitten zu sein. Es ist wichtig, regelmäßig zu überprüfen, ob die Einstellungen noch gültig sind. [10, S. 53-54]

Sicherheit durch Vermeidung von Funktionen

Abschalten von JavaScript in Adobe Reader: Die Funktion JavaScript-in-PDF-ausführen wird kaum benötigt und kann daher abgeschaltet werden. Dies verhindert die Ausführung von Objekten in PDF-Dokumenten, die über OLE oder Makros Schaden anrichten können.[10, S. 54] Vermeidung von Makros: In vielen Unternehmen sind Makros gängige Praxis, da sie viele Arbeitsschritte vereinfachen oder beschleunigen. Allerdings wird oft die Dokumentation und Maßnahmen zur Qualitätssicherung "vergessen". Es ist ratsam, Makros von unbekannten Quellen zu vermeiden. Sicherheit im Web und E-Mail Härtung von Web- und E-Mail-Zugriff: Nicht nur Schad-Software,

sondern auch User-Tracking und Lauschangriffe sollen abgeblockt werden. Dies kann erreicht werden, indem die Software stets auf dem neuesten Stand gehalten und nicht benötigte Software komplett deinstalliert wird. Passwort-Verwaltung absichern: Die Passwort-Verwaltung in den Browser-Einstellungen sollte deaktiviert werden. Externe Passwort-Manager bieten sich als sichere Alternative an. [10, S. 54-55]

Speichermedien

USB-Sticks und andere externe Speichermedien werden für den Datentransport verwendet. Um die Daten vor unbefugtem Zugriff zu schützen, sollte die Verschlüsselung der Daten beim Schreiben auf den USB-Stick aktiviert werden. Diese Maßnahmen helfen, die Sicherheit von Windows-PCs und Servern zu verbessern und die Angriffsfläche zu reduzieren. Es ist wichtig, diese Einstellungen regelmäßig zu überprüfen, da durch (automatische) Updates der Applikationen und des Betriebssystems wieder die (unsicheren) Standardeinstellungen gesetzt werden könnten. [10, S. 57]

5 Schlussfolgerung und Ausblick (Schwarz & Schellhorn)

Die Analyse der Ransomware-Bedrohung im Gesundheitswesen hat gezeigt, dass die Sicherheit von Patientendaten und kritischen IT-Systemen eine dringende Angelegenheit ist. Die Digitalisierung bietet zwar zahlreiche Vorteile, birgt jedoch auch Risiken. Ransomware-Angriffe sind eine ernsthafte Gefahr, die nicht ignoriert werden darf. Die Sensibilisierung von Mitarbeitern, die Implementierung robuster Backupstrategien und die gezielte Abschaltung unnötiger Funktionen sind entscheidende Schritte zur Stärkung der Resilienz gegenüber solchen Angriffen.

5.1 Empfehlungen für die Praxis

In der Praxis sollten mehrere Empfehlungen umgesetzt werden, um die Cybersicherheit im Gesundheitswesen zu verbessern. Zunächst sind regelmäßige Schulungen und Sensibilisierungsmaßnahmen für medizinisches Personal und IT-Abteilungen unerlässlich, um das Bewusstsein für potenzielle Cybersecurity-Risiken zu schärfen. Darüber hinaus sind eine durchdachte Backupstrategie und strenge Zugriffskontrollen notwendig, damit die Datenverfügbarkeit sichergestellt und im Falle eines Angriffs eine schnelle Wiederherstellung der Systeme gewährleistet werden kann. Nicht zuletzt sind spezifische Regulierungen und Sicherheitsmaßnahmen wie die Deaktivierung unnötiger Funktionen und Dienste sowie die Anwendung von Sicherheitsrichtlinien für bestehende Systeme entscheidend, um die Cyber-Resilienz im Gesundheitswesen zu erhöhen.

5.2 Ausblick auf zukünftige Forschungen

Die Entwicklung von Ransomware erfordert kontinuierliche Forschung und Innovation. Zukünftige Arbeiten sollten sich auf die Verbesserung von Erkennungs- und Präven-

tionsmethoden konzentrieren, um mit den sich wandelnden Angriffsmustern Schritt zu halten. Ethische Aspekte des Datenschutzes im Gesundheitswesen sollten ebenfalls weiter untersucht werden, um die Rechte der Patienten zu wahren.

6 Quellverzeichnis

Literatur

[1] Bundesministerium für Gesundheit, *Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)*, https://www.bundesgesundheitsministerium.de/ministerium/gesetze-und-verordnungen/guv-20-lp/digig, Zugriff am 30. April 2024, 2024.

[2] Bundesministerium für Gesundheit, *Gesundheitsdatennutzungsgesetz (GDNG)*, https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/gesundheitsdatennutzungsgesetz.html, Zugriff am 30. April 2024, 2024.

[3] Bundesamt für Sicherheit in der Informationstechnik, *Ransomware Bedrohungslage*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf, Zugriff am 05. Mai 2024, 2022.

[4] A. Ferreira, „Why Ransomware Needs A Human Touch“, in *2018 International Carnahan Conference on Security Technology (ICCST)*, 2018, S. 1–5. DOI: 10.1109/CCST.2018.8585650.

[5] N. Thamer und R. Alubady, „A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research“, in *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, 2021, S. 210–216. DOI: 10.1109/BICITS51482.2021.9509877.

[6] N. Thamer und R. Alubady, „Security against Ransomware Attack in Medical Healthcare Records Using Blockchain Technology“, in *2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT)*, 2022, S. 111–117. DOI: 10.1109/CSCTIT56299.2022.10145717.

[7] S. Sarowa, B. Bhanot, V. Kumar und M. Kumar, „Analysis of Attack Patterns and Cyber Threats in Healthcare Sector“, in *2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT)*, 2023, S. 160–165. DOI: 10.1109/DICCT56244.2023.10110141.

[8] Ekta und U. Bansal, „A Review on Ransomware Attack“, in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, 2021, S. 221–226. DOI: 10.1109/ICSCCC51823.2021.9478148.

[9] P. K, B. Nataraj und P. Duraisamy, „An Investigation on Attacks in Application Layer Protocols and Ransomeware Threats in Internet of Things“, in *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Bd. 1, 2023, S. 668–672. DOI: 10.1109/ICACCS57279.2023.10112669.

[10] S. F. Martin Darms Stefan Haßfeld, *IT-Sicherheit und Datenschutz im Gesundheitswesen*, en, 1. Aufl. Wiesbaden: Springer Vieweg, Jan. 2019, ISBN: 978-3-658-21589-7. Adresse: https://link.springer.com/book/10.1007/978-3-658-21589-7.

[11] R. Zhang, D. Chen und X. Shang, „Privacy preserving for patients' information: A knowledge-constrained access control model for hospital information systems", in *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, 2016, S. 921–926. DOI: 10.1109/INDIN.2016.7819293.

[12] R. Strametz, „Patientensicherheit 4.0", *Heilberufe*, Jg. 70, Nr. 12, S. 24–26, Nov. 2018. DOI: 10.1007/s00058-018-3802-2. Adresse: http://dx.doi.org/10.1007/s00058-018-3802-2.

[13] A. K. Sekar, R. Ramakrishnan, A. Ganesh und T. Kiruthiga, „Emerging Cyber Security and Brute Force Attacks in Hospital Management Information Systems", in *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, 2023, S. 421–426. DOI: 10.1109/SmartTechCon57526.2023.10391825.

[14] N. Oles, *How to Catch a Phish*, en, 1. Aufl. Berkeley, CA: Apress Berkeley, CA, Juni 2023, ISBN: 978-1-4842-9361-4. Adresse: https://link.springer.com/book/10.1007/978-1-4842-9361-4.

[15] J. M. Kizza, „Security Threats and Threat Motives to Computer Networks", en, in *Guide to Computer Network Security*, J. M. Kizza, Hrsg., Cham: Springer International Publishing, 2024, S. 63–87, ISBN: 978-3-031-47549-8. DOI: 10.1007/978-3-031-47549-8_3. Adresse: https://doi.org/10.1007/978-3-031-47549-8_3 (besucht am 15. 04. 2024).

[16] Antonina Farion-Melnyk, Viktoria Rozheliu, Tetiana Slipchenko, Serhiy Banakh, Mykhailyna Farion, Oksana Bilan, *Ransomware Attacks: Risks, Protection and Prevention Measures*, https://ieeexplore.ieee.org/document/9548507, Zugriff am 04. Mai 2024, 2021.

[17] Bundesamt für Sicherheit in der Informationstechnik, *Maßnahmenkatalog Ransomware*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.pdf, Zugriff am 05. Mai 2024, 2022.

6.1 weitere Hilfsmittel

7 Erklärung zur wissenschaftlichen Arbeit

Ich versichere hiermit, die Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt, die wörtlich oder inhaltlich übernommenen Stellen als solche kenntlich gemacht und die Allgemeine Studien- und Prüfungsordnung für das Bachelor- und Masterstudium der Hochschule Reutlingen, die fachspezifische Studien- und Prüfungsordnung und die Regeln zur Sicherung der guten wissenschaftlichen Praxis der Hochschule Reutlingen beachtet zu haben.
Diese Arbeit oder Teile dieser Arbeit sind weder Bestandteil einer anderen Prüfungsleistung an dieser noch an einer anderen wissenschaftlichen Institution.
Jegliche Ähnlichkeit ist allein gleicher Aufgabenstellung verschuldet. Andere Lösungsansätze wurden weder für die Bearbeitung der einzelnen Aufgaben oder der endgültigen Hausarbeit genutzt.

Martin Lauterbach
Reutlingen, 23. Juni 2025

Luca Sebastian Schellhorn
Reutlingen, 23. Juni 2025

Sebastian Vincent Schwarz
Reutlingen, 23. Juni 2025