Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Abschlussbericht Projekt CyberPraxMed – Sicherheit in Arztpraxen

Eine IT-Sicherheitsbetrachtung aktueller Arztpraxen mit Handlungsempfehlungen

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-di24@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2023

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
0.9	04.08.0223	Entwurf	Erster Entwurf für ein internes Review
0.91	31.08.2023	Entwurf 2	Bericht mit Änderungen nach dem ersten Review
0.92	07.09.2023	Entwurf 3	Einleitung durch Prof. Jedamzik erweitert
0.93	08.09.2023	Entwurf 4	Zusammenfassung durch Prof. Jedamzik erweitert
0.94	15.09.2023	First Final	Kleinere Anpassungen nach weiteren Reviews

Inhaltsverzeichnis

1 Einleitung 9
2 Projektauftrag 10
2.1 Auftragsgegenstand und Projektziele 10
2.2 Vorgehen und Aufbau der Studie 10
2.3 Projektteam 11
3 Zusammenfassung 12
4 Überblick der Arztpraxen 13
4.1 Beschreibung der Stichprobe 13
4.2 Charakteristiken der untersuchten Arztpraxen 15
4.3 Clusterung der Praxen 16
4.4 Beschreibung der Arztpraxen 17
5 Angreifer / Angriffe 19
5.1 Zufälliger Angreifer 19
5.2 Gezielte Angreifer 21
5.3 Kriminelle Organisationen 22
6 Übergreifende Fragestellungen 23
6.1 Auswertung nach Schwachstellenhäufigkeit / Cluster 23
6.2 Bewertung der statistischen Befunde 26
6.3 Ableitungen aus den Auswertungen 26
7 Übergreifende Lösungsansätze 26
7.1 Hilfestellung 27
7.2 Musterverträge für Dienstleister 27
7.3 Verbesserung von Schulungs- und Awareness-Angeboten 27
7.4 Bereitstellung eines prototypischen ISMS 27
8 Schwachstellen 27
8.1 PC mit angemeldetem Account 29
8.2 Sensible Daten auf externen Geräten 31
8.3 Unzureichende Betrachtung der DSGVO-Anforderungen 34
8.4 Fehlende Funktionstests der Backups 35
8.5 Unzureichende Awareness-Schulungen 37
8.6 Unsichere Entsorgung von IT-Geräten 40
8.7 Unzureichender Virenschutz 42
8.8 Unzureichende Verschlüsselung 44
8.9 Unverschlüsselte Backups 45
8.10 Ungesicherte Netzwerkdosen unbemerkt zugänglich 46
8.11 Verwendung fremder Datenträger 48

8.12 Unzureichendes Berechtigungsmanagement ... 50
8.13 Unsichere Anwendungen ... 51
8.14 Unzureichendes IT-Know-how ... 53
8.15 Ungesicherte Medizintechnik ... 54
8.16 Unzureichendes Patch- und Updatemanagement ... 57
8.17 Keine zentrale Verwaltung für IT-Systeme ... 59
8.18 Unzureichende Dokumentation der Infrastruktur ... 60
8.19 Potenziell unsichere Passwörter ... 61
8.20 Privatgeräte im Netzwerk ... 63
8.21 Fehlende Netzwerksegmentierung ... 64
8.22 Parallelbetrieb TI-Konnektor ... 66
8.23 Gemeinsam benutzte User-Konten ... 67
8.24 Unverschlüsselte E-Mail-Kommunikation ... 68
8.25 Fehlende Strukturierung der Informationssicherheit ... 70
8.26 Unsichere Netzwerkkonfiguration ... 71
9 Mögliche Schwachstellen ... 73
9.1 Unzureichende Sicherung öffentlich erreichbarer Ports ... 73
9.2 Unzureichendes Logging- und Monitoring-Konzept ... 73
9.3 Unsichere Praxisverwaltungs-Software ... 73
10 Anhang: Netzpläne ... 74
11 Anhang: Fragebogen ... 84
12 Anhang: Matrix – Schwachstellen/Praxis ... 101
13 Anhang: Checkliste für Arztpraxen ... 102
13.1 Onepager ... 104
14 Verweise ... 105

Abbildungsverzeichnis

Abbildung 1 – Vergleich der Anzahl der Mitarbeiterinnen und Mitarbeitern (inkl. Ärztinnen und Ärzten) von Praxen und Dienstleistern. 17
Abbildung 2 - Relative Häufigkeit der Schwachstellen in Abhängigkeit zur Fachlichkeit 23
Abbildung 3 - Relative Häufigkeit der Schwachstellen in Bezug auf Praxis-Größe 24
Abbildung 4 - Relative Häufigkeit der Schwachstellen in Bezug auf die Größe der Dienstleister 25
Abbildung 5 - Relative Verteilung von Schwachstellen nach Lokation 25
Abbildung 6 - Risiko-Matrix, die den Schweregrad / Schaden in einer Dimension und die Ausnutzbarkeit der Schwachstelle in der zweiten Dimension zeigt. 28
Abbildung 7 – Häufigkeit der Schwachstellen in Prozent 29

Abkürzungsverzeichnis

Abkürzung	Beschreibung
AD	Active Directory
BSI	Bundesamt für Sicherheit in der Informationstechnik
CyberPraxMed	Projekt Cyber-Sicherheit in Arztpraxen
DPI	Deep Paket Inspection
DSGVO	Datenschutzgrundverordnung
KV	Kassenärztliche Vereinigungen
MFA	Medizinische Fachangestellte
RAT	Remote Access Trojaner
RDP	Remote Desktop Protocol
TI	Telematikinfrastruktur
TOM	Technisch organisatorische Maßnahmen
VPN	Virtual Private Network

Glossar

Bezeichnung	Beschreibung
Anwendung	Als Anwendung(s-Software) werden Computerprogramme bezeichnet, die genutzt werden, um eine nützliche oder gewünschte, nicht systemtechnische Funktionalität zu bearbeiten oder zu unterstützen.
Client	Bei einem Client handelt es sich um einen Computer oder eine Software, die mit einem Server kommuniziert und von diesem Daten und spezielle Dienste in Anspruch nimmt.
DDoS	Der Distributed-Denial-of-Service (DDoS) Angriff ist ein „verteilter“ Denial-of-Service (DoS) Angriff, der wiederum eine Dienstblockade darstellt. Diese liegt vor, wenn ein angefragter Dienst nicht mehr bzw. nur noch stark eingeschränkt verfügbar ist.
ISMS	Ein Information Security Management System (ISMS) definiert Regeln und Methoden, um die Informationssicherheit in einem Unternehmen oder in einer Organisation zu gewährleisten.
IDS	Ein IDS (Intrusion Detection System) ist ein Gerät oder eine Software-Anwendung, die einen Administrator im Falle einer Security- oder Policy-Verletzung benachrichtigt.
IPS	Ein Intrusion Prevention System (IPS) ist eine automatisierte Netzwerksicherheitstechnologie, um das Netzwerk zu überwachen und auf potenzielle Bedrohungen zu reagieren.
Patch	Patch bezeichnet ein Software-Update für bestehende Anwendungen oder Betriebssysteme zur Behebung von Fehlern oder Sicherheitslücken.
Phishing	Unter dem Begriff Phishing versteht man Versuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben.
Reconnaissance	Reconnaissance, oder auch „Aufklärung”, bezeichnet die Informationsbeschaffung vor einem Angriff.
Schwachstelle	Schwachstellen sind inhärente Sicherheitslücken in einem System oder Netzwerk, die Cyberkriminelle für ihre Zwecke nutzen können.
Scope	Beschreibung des Fokus der Schwachstellenanalyse.
Social Engineering	Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum

Bezeichnung	Beschreibung
	Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.

1 Einleitung

Die Digitalisierung der Arztpraxen in Deutschland bringt zahlreiche Vorteile, etwa in Form eines schnelleren und effizienteren Zugriffs auf medizinische Fachdienste, mit sich. Dies erfordert eine sichere Anbindung der Praxen an das Internet. Diese Forderung besitzt allein deshalb schon höchste Priorität, da in Arztpraxen sensible Patientendaten gespeichert und verwaltet werden, auf die Berechtigte über das Internet remote zugreifen können sollen. Der Schutz dieser Daten ist von höchster Priorität. Gleichzeitig wird die Etablierung von Cyber-Sicherheit und Datensicherheit in Arztpraxen akuter und komplexer. In diesem Kontext ist die Anbindung von Arztpraxen an eine sichere Telematikinfrastruktur (TI) unerlässlich.

Die bisherige TI-Lösung, die auf VPN und spezielle Router, sogenannte Konnektoren setzt, hat sich als nicht ausreichend erwiesen, da in Arztpraxen häufig Internetverbindungen parallel zum Konnektor aufgebaut werden, wodurch – von speziell getrennten Netzwerken abgesehen - die Schutzwirkung des speziell gesicherten Konnektors beeinträchtigt werden kann. Darüber hinaus konnte in durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführten Projekten (eCare, ManiMed) nachgewiesen werden, dass es in vernetzten Medizinprodukten mitunter gefährliche Schwachstellen gibt, die eine Angreiferin oder ein Angreifer in einem kompromittierten Praxisnetzwerk gezielt ausnutzen könnte. Zudem wurden in den letzten Jahren in Arztpraxen vermehrt Sicherheitsprobleme durch Netzwerkkomponenten bekannt. In einem besonders schwerwiegenden Fall etwa waren aufgrund eines Fehlers in der Firmware eines Routers dreißigtausend Patientenakten sowie weitere vertrauliche interne Daten frei über das Internet zugänglich.

Die technische und operative Infrastruktur in Arztpraxen bildet das unverzichtbare Rückgrat für eine breite Palette von Dienstleistungen, angefangen bei der Patientenverwaltung und -aufnahme bis hin zur Diagnostik und Nachsorge. Mit dem kontinuierlichen Voranschreiten der Digitalisierung entsteht eine zunehmend komplexe und hoch vernetzte IT-Landschaft, die gleichzeitig eine Reihe von Herausforderungen im Bereich der Cyber-Sicherheit mit sich bringt.

Diese Studie hat das Ziel, den gegenwärtigen Sicherheitsstatus in deutschen Arztpraxen zu erheben, um auf diese Weise eine Reihe von dringenden Handlungsbedarfen innerhalb der Praxen sichtbar zu machen. Dieses Vorhaben wurde durch die Erkenntnisse aus früheren Untersuchungen inspiriert und unterstreicht die Notwendigkeit einer systematischen Überprüfung des IT-Sicherheitsniveaus sowie der IT-Ausstattung in deutschen Arztpraxen. Die Dringlichkeit und Notwendigkeit einer solchen Untersuchung ergeben sich aus verschiedenen Überlegungen, die im Folgenden skizziert werden:

1. Identifikation von Schwachstellen: Die geplante systematische Untersuchung soll es ermöglichen, potenzielle Schwachstellen sowohl in der Software als auch in der Hardware zu identifizieren. Dazu gehören Server, Netzwerkgeräte und medizinische Geräte, die als mögliche Angriffsziele für Cyberangriffe dienen könnten.
2. Standardisierung und Best Practices: Eine gründliche Analyse der Infrastruktur soll zur Entwicklung von Standards für bewährte Praktiken im Bereich der Cyber-Sicherheit und des Datenschutzes beitragen. Diese Standards können Arztpraxen als wertvolle Leitlinien dienen und die Implementierung von Sicherheitsmaßnahmen erleichtern.
3. Interoperabilität: Im Gesundheitswesen müssen verschiedene Akteure und Systeme reibungslos miteinander interagieren. Die Studie soll aufzeigen, ob die vorhandenen Systeme für einen sicheren Informationsaustausch gerüstet sind, ohne dabei die Integrität der Daten zu gefährden.
4. Überprüfung der technischen und organisatorische Maßnahmen die sich aus den typischen Compliance und rechtlichen Anforderungen ergeben (z.B. Datenschutz, Anforderungen der Kassenärtzlichen Vereinigung (KBV) etc.)
5. Reaktionsfähigkeit auf Sicherheitsvorfälle: Durch eine umfassende Untersuchung der technischen und operativen Infrastrukturen soll es möglich sein, die Fähigkeit von Arztpraxen zur angemessenen Reaktion auf Sicherheitsvorfälle zu bewerten. Dies umfasst Fragen zur Erkennung von Zwischenfällen, zur schnellen Isolation von Problemen und zur Wiederherstellung der Systeme.

Zusammenfassend richtet die Studie das Hauptaugenmerk darauf, ob und inwieweit Arztpraxen den grundlegenden Sicherheitsanforderungen entsprechen und wie widerstandsfähig sie gegenüber potenziellen Cyberangriffen sind. Die Ergebnisse der Studie sollen dazu beitragen, mögliche Schwachstellen zu identifizieren und somit zur Verbesserung der gesamten Sicherheitsarchitektur von Arztpraxen beitragen. Die gewonnenen Erkenntnisse können als Grundlage für die Weiterentwicklung von Sicherheitsarchitekturen der Telematik Infrastruktur (TI 2.0) dienen, die auf dem Zero-Trust-Prinzip basieren. Ein erhöhtes Sicherheitsniveau in Arztpraxen dient nicht nur dem Wohl der Patienten und des medizinischen Personals, sondern kann auch dazu beitragen, das Vertrauen in das Gesundheitssystem als Ganzes zu stärken.

2 Projektauftrag

2.1 Auftragsgegenstand und Projektziele

Der Projektauftrag bestand darin, das aktuelle Sicherheitsniveau in unterschiedlichen Typen von Arztpraxen anhand verschiedener Faktoren zu evaluieren. Als Projektziel war aus den gesammelten Informationen ein Bericht über die Sicherheit in Arztpraxen zu erarbeiten, der Empfehlungen zur Verbesserung der dortigen IT-Sicherheit beinhalten und zudem auch für Personen mit weniger fachlichem Hintergrundwissen verständlich sein sollte.

Die für die Evaluierung zu betrachtenden Faktoren wurden durch das BSI vorgegeben. Dazu zählten die grundsätzliche Struktur des Netzwerks der Arztpraxen sowie seine Komponenten, vorhandene Firewalls und die Anbindung an das Internet. Zu den Komponenten zählten insbesondere auch vernetzte medizinische Geräte. Außerdem war die IT-Kompetenz eines eventuell beauftragten IT-Dienstleisters, des Arztes und des Praxispersonals zu ermitteln.

2.2 Vorgehen und Aufbau der Studie

Zunächst wurde gemäß den Projektvorgaben eine Datenerhebung zur Ausstattung und Vernetzung von Arztpraxen unterschiedlicher Kategorien (Hausarztpraxen, Zahnarztpraxen, psychotherapeutische Praxen und radiologische Praxen[1]) in Form einer Umfrage durchgeführt, um Anhaltspunkte für aktuelle Systemlandschaften und eingesetzte technische Lösungen zu gewinnen. Die Auswahl der Arztpraxen und die Erstellung der Fragebögen wurde anhand der durch das BSI definierten Kriterien getroffen bzw. durchgeführt.

Die vorgegebenen Rahmenbedingungen machen deutlich, dass es in diesem Projekt nur darum gehen konnte, ein erstes, grobes Lagebild zur Situation der IT-Sicherheit in deutschen Arztpraxen zu gewinnen. Dies folgt bereits aus den Auswahlkriterien für die Teilnehmer der Studie. Es handelte sich nicht um eine zufällige Stichprobe, sondern die Teilnehmer waren selbstrekrutiert und erhielten zudem noch eine finanzielle Aufwandsentschädigung. Es liegt auf der Hand, dass sich das Antwortverhalten von Teilnehmern und Nicht-Teilnehmern unterscheidet, wenn es um eine Selbstauskunft bezüglich der IT-Sicherheit im eigenen Unternehmen geht. Aufgrund der daraus resultierenden Verzerrung des Ergebnisses muss davon ausgegangen werden, dass die Stichprobe kein Abbild der Grundgesamtheit darstellen kann.

Darüber hinaus deutet die vom BSI vorab getroffene Auswahl der Fachrichtung der zu untersuchenden Praxen darauf hin, dass die Richtung der Studie auf eine qualitative Bewertung der Ergebnisse zielt, da die statistische Signifikanz nicht ermittelt werden kann. Die Größenordnungen der in Deutschland ansässigen

[1] Trotz Aufwandsentschädigung war die Bereitschaft zur Teilnahme bei den angesprochenen Praxen sehr gering. So war es im Zeitraum der Untersuchung nicht möglich, eine dritte radiologische Praxis zur Teilnahme zu bewegen.

- Haus- und Allgemeinarztpraxen (ca. 25.000),
- Zahnarztpraxen (ca. 50.000),
- psychotherapeutischen Praxen (ca. 3000) und
- radiologischen Praxen (unter 1000),

aus denen jeweils drei auszuwählen waren (siehe Kapitel 4.1), liegen zu weit auseinander, um einen strengen, statistisch signifikanten quantitativen Vergleich zwischen den Kategorien anzustellen. Es sei an dieser Stelle jedoch vorweggenommen, dass die qualitative bzw. semi-quantitative Auswertung der Ergebnisse eine Reihe von wertvollen Hinweisen auf gegebenenfalls zukünftig durchzuführende Untersuchungen erbrachte.

Die durch die ausgefüllten Fragebögen und Interviews erfassten Daten wurden auf wiederkehrende Muster und Möglichkeiten zur Verallgemeinerbarkeit hin untersucht und kategorisiert. Die pro Praxis angefertigten Netzpläne dienten zur Identifizierung der zu untersuchenden Angriffsvektoren.

Daraufhin wurde unter Berücksichtigung typischer Angreiferprofile eine Sicherheitsanalyse durchgeführt, aus der sich der Bedrohungsstatus der teilnehmenden Arztpraxen bzw. Kategorien von Arztpraxen ergab. Die Sicherheitsanalyse enthält zu jedem Angriffsvektor Vorschläge für Mitigationsmaßnahmen und eine Abschätzung der jeweiligen Mitigationskosten und des verbleibenden Restrisikos.

Schließlich wurden aus den Ergebnissen der Sicherheitsanalyse Handlungsempfehlungen abgeleitet, die zur Erhöhung der Patientensicherheit und der Vertraulichkeit von Gesundheitsdaten in Arztpraxen geeignet sind. Als weitere Hilfestellung wurde eine entsprechende Checkliste erstellt, anhand derer eine Praxis unkompliziert prüfen kann, ob die erforderlichen Maßnahmen zur Beseitigung der gefundenen Schwachstellen implementiert sind.

Zusammenfassend wurden zur Erreichung der genannten Ziele die folgenden Schritte durchgeführt:

1. Datenerhebung zur Ausstattung, Vernetzung und Anwendung von IT-Sicherheitsmaßnahmen von Arztpraxen anhand eines Fragebogens: zunächst in einer, dann nach Verfeinerung des Fragebogens in weiteren Praxen.
2. Sicherheitsanalyse aller erhobenen Daten der Arztpraxen und der Zusammenstellung potenzieller Gefahren sowie möglicher Angreiferprofile.
3. Erstellung eines Ergebnisberichts mit Handlungsempfehlungen zur Erhöhung der IT-Sicherheit in Arztpraxen.

2.3 Projektteam

Das Projektteam bestand aus Mitarbeiterinnen und Mitarbeitern des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Bonn sowie der Bayerische TelemedAllianz GmbH, der DATATREE AG und der adesso SE.

Die Leitung des Projekts „CyberPraxMed – Sicherheit in Arztpraxen“ lag in den Händen der Mitarbeiterinnen und Mitarbeiter des BSI aus dem Referat DI 24 – Cyber-Sicherheit im Gesundheits- und Finanzwesen.

Die Bayerische TelemedAllianz GmbH und die DATATREE AG unterstützten das Projekt beratend und stellten dabei die Verbindung zu einschlägigen Praxen her bzw. lieferten Input für die Erstellung und Bewertung der Fragebögen sowie die Auswertung der Ergebnisse.

Mit der Projektdurchführung war die adesso SE beauftragt, ein IT-Dienstleister mit Hauptsitz in Dortmund. Zu ihren Geschäftsfeldern gehört allgemein das Themengebiet Informations- und IT-Sicherheit sowie speziell die Informationssicherheit im Gesundheitswesen neben einer breiten Palette weiterer Branchen.

3 Zusammenfassung

Die durchgeführte Studie – über eine nicht repräsentative Stichprobe – indiziert, dass im Bereich der Informations- und IT-Sicherheit in Arztpraxen großes Potenzial für Verbesserungen besteht.

In der Studie wurden 16 Praxen aus ländlichen und städtischen Regionen mit einer Größe von ein bis 150 Mitarbeiterinnen und Mitarbeitern aus den Kategorien allgemeinmedizinische, zahnärztliche, psychotherapeutische und radiologische Praxen, mittels eines Fragebogens und eines damit verbundenen Interviews mit dem IT-Dienstleister aus dem Projektteam, untersucht.

Im Rahmen dieser Studie wurden diverse Sicherheitsmängel festgestellt, die zügig behoben werden sollten. Bei den PCs war zu bemerken, dass sie oft eingeschaltet und mit einem aktiven Benutzerkonto angemeldet blieben, auch wenn sie nicht in Gebrauch waren. Dies birgt das Risiko, dass Unbefugte, sollten sie physischen Zugang zum PC haben, auf sensible Daten zugreifen könnten. Eine einfache Lösung wäre, automatische Sperrmechanismen oder Abmeldefunktionen nach einer bestimmten Inaktivitätszeit einzuführen. Weiterhin wurden sensible Patientendaten auf externen Speichermedien wie USB-Sticks und externen Festplatten gefunden. Der Verlust solcher Geräte könnte dazu führen, dass diese Daten in falsche Hände geraten. Es ist daher ratsam, derartige Daten nicht auf tragbaren Medien zu speichern oder sie zumindest zu verschlüsseln. Es zeigte sich außerdem, dass nicht alle Anforderungen der DSGVO von den Praxen berücksichtigt wurden. Nicht nur drohen hier hohe Bußgelder, sondern auch ein erheblicher Reputationsverlust. Um dem entgegenzuwirken, sollten externe Berater für Datenschutz engagiert oder entsprechende Schulungen durchgeführt werden.

Ein weiteres Problem besteht darin, dass zwar Backups erstellt, diese jedoch nicht auf ihre Funktionsfähigkeit überprüft wurden. Sollten diese Backups bei einem Datenverlust unbrauchbar sein, könnten wichtige Daten verloren gehen. Es ist unerlässlich, regelmäßige Funktionstests der Backups durchzuführen und sicherzustellen, dass sie an einem sicheren Ort aufbewahrt werden. Das Personal zeigte zudem Defizite in der IT-Sicherheit, da sie nicht ausreichend geschult waren. Schulungen und Weiterbildungen in diesem Bereich sind daher unabdingbar. Ähnlich problematisch ist die unsichere Entsorgung von IT-Geräten. Eine sicherere Methode wäre, die Daten professionell zu löschen oder die Geräte physisch zu zerstören.

Die PCs in den Praxen waren teilweise nicht mit aktuellen Virenschutzprogrammen ausgestattet oder hatten gar keinen Schutz. Eine regelmäßige Aktualisierung und Überprüfung des Virenschutzes ist hier essenziell. Auch in Bezug auf die Verschlüsselung gibt es Nachholbedarf: Daten, insbesondere Backups, wurden oft unverschlüsselt gespeichert, was sie bei einem Datenleck angreifbar macht. Eine Lösung wäre die Einführung einer Ende-zu-Ende-Verschlüsselung. Netzwerkanschlüsse in öffentlichen Bereichen waren zudem ungesichert, was bedeutet, dass externe Personen potenziell Geräte anschließen und auf das Netzwerk zugreifen könnten. Es sollte erwogen werden, diese Anschlüsse physisch zu sichern oder sie in private Bereiche zu verlegen.

Die Verwendung von externen Speichermedien, die nicht zur Praxis gehören, sowie ein unzureichendes Berechtigungsmanagement waren weitere Schwachstellen. Es sollte eine klare Richtlinie für die Nutzung von Speichermedien geben und ein System, das sicherstellt, dass jeder Mitarbeiter nur Zugriff auf die für seine Arbeit erforderlichen Daten hat. Einige der eingesetzten Softwarelösungen wiesen bekannte Sicherheitslücken auf. Es ist wichtig, regelmäßig nach Updates zu suchen und sicherzustellen, dass nur sichere Software verwendet wird.

Unzureichendes IT-Wissen, ungesicherte Medizintechnik und fehlendes Patch- und Updatemanagement waren ebenso Problembereiche. Schulungen, spezialisierte Sicherheitssoftware für medizinische Geräte und ein zentrales Management für IT-Systeme könnten hier Abhilfe schaffen. Die Liste der Probleme geht weiter mit mangelnder Netzwerksegmentierung, potenziell unsicheren Passwörtern und dem Einsatz von Privatgeräten im Netzwerk. Hier könnten die Einführung von stärkeren Passwortrichtlinien, die Trennung von professionellen und privaten Netzwerken sowie die Segmentierung des Netzwerks helfen. Der Parallelbetrieb des TI-Konnektors, gemeinsam genutzte Benutzerkonten und unverschlüsselte E-Mail-

Kommunikation waren ebenfalls Anlass zur Sorge. Lösungen könnten hier die strikte Trennung von Systemen, die Zuweisung individueller Benutzerkonten und die Nutzung verschlüsselter E-Mail-Dienste sein.

Im Rahmen dieses Projekts wurde festgestellt, dass sich in allen untersuchten Arztpraxen der Konnektor parallel zu einem nicht speziell gesicherten Router befand und dadurch seine Schutzwirkung nicht vollständig entfalten konnte. Dieses Ergebnis unterstreicht die Relevanz der Studie, da es auf ein generelles Problem in Bezug auf die Konnektorimplementierung in Arztpraxen hinweist. Die Feststellung eines parallelen Anschlusses hat Auswirkungen auf die Sicherheit und den Datenfluss innerhalb der Telematikinfrastruktur und sollte als Anregung für Diskussionen und Maßnahmen zur Verbesserung der IT-Sicherheit in Arztpraxen dienen.

Schließlich mangelt es oft an klaren Strukturen für die Informationssicherheit, einer sicheren Netzwerkkonfiguration und einer ordnungsgemäßen Sicherung öffentlich zugänglicher Ports. Es sollte ein klarer Rahmen für die Informationssicherheit erstellt, das Netzwerk regelmäßig überprüft und alle öffentlich zugänglichen Ports ordnungsgemäß gesichert werden.

Zusammenfassend zeigt sich, dass Arztpraxen in vielen Bereichen der IT-Sicherheit nachbessern sollten. Durch gezielte Maßnahmen und Schulungen kann ein hohes Sicherheitsniveau erreicht werden, das sowohl die Daten der Patienten als auch die Systeme der Praxis schützt.

Summarisch kann folgendes festgehalten werden:

- Die durch Fragebogen und Interviews erfassten Daten zeigen, dass über alle 16 Praxen der Studie hinweg einige zum Teil gravierende Schwachstellen vorhanden sind.
- Die Daten weisen auf deutliche Unterschiede hinsichtlich der Sicherheit in Bezug auf die Praxisgröße, die Größe des Dienstleisters oder die Fachlichkeit hin. Jedoch erreichen selbst diejenigen Praxen, die hier am besten abschneiden, kein akzeptables Niveau hinsichtlich der IT-Sicherheit.
- Die untersuchte Stichprobe stellt kein Abbild der Grundgesamtheit der Arztpraxen dar und erlaubt somit auch keine pauschale Verallgemeinerung auf alle Arztpraxen. Dennoch ist dieses Ergebnis alarmierend und impliziert die Forderung, dem Thema Sicherheit in Arztpraxen mehr Beachtung zu schenken.
- Die Analyse der erfassten Daten im Zusammenhang mit dem aktuellen IT-Sicherheitsniveau der Praxen lassen den Schluss zu, dass die Praxen und Dienstleister ohne externe Unterstützung bei der Umsetzung notwendiger Maßnahmen überfordert sein werden.
- Diese externe Unterstützung könnte z. B. über Angebote sowie zentral bereitgestellte Hilfestellungen – etwa durch Körperschaften des öffentlichen Rechts, wie z.B. Kassenärztliche Vereinigungen, Berufsverbände, Krankenkassen, das BSI oder private Anbieter– erfolgen und dabei behilflich sein, die Awareness der verantwortlichen Ärzte und das technische Knowhow der Dienstleister zu verbessern, aber auch die Umsetzung sicherheitsrelevanter Maßnahmen zu beschleunigen.

4 Überblick der Arztpraxen

4.1 Beschreibung der Stichprobe

Die Stichprobe sollte ein möglichst breites Spektrum der Arztpraxen in Deutschland abdecken. Daher sollten die häufigsten zwei Praxisarten, Haus- und Allgemeinarztpraxen sowie Zahnarztpraxen, aber auch zwei spezielle Praxisarten, psychotherapeutische- und radiologische Praxen betrachtet werden. Von jeder dieser Praxisarten sollten mindestens drei in der Stichprobe enthalten sein.

Rahmenparameter

Die Studie hat folgende Rahmenparameter zur Grundlage:

In der Studie sollten folgende Kategorien von Praxen enthalten sein:

- Haus- und Allgemeinarztpraxen
- Zahnarztpraxen
- Psychotherapeutische Praxen
- Radiologische Praxen

Von jeder Praxiskategorie sollten mindestens drei Praxen in der Stichprobe enthalten sein. Dieses Ziel wurde allerdings im Fall der radiologischen Praxen nicht erreicht (siehe unten).

Die Praxen sollten eine Größe von bis zu fünf Ärztinnen und Ärzten aufweisen. Auch in diesem Punkt gibt es eine Abweichung. Vor allem Zahnarztpraxen und Radiologen waren teilweise größer.

Es sollte ein ausgewogenes Verhältnis von ländlichen und städtischen Praxen erreicht werden. Entsprechend wurden die Praxen ausgewählt, wobei die Einschätzung, ob eine Praxis als ländlich oder städtisch einzustufen war, von den Praxen selbst getroffen wurde.

Verwendete Stichprobe

In der Studie wurden insgesamt 16 Arztpraxen in Deutschland hinsichtlich ihrer Ausstattung und Vernetzungssysteme untersucht.

- Sechs Haus- und Allgemeinarztpraxen
- Fünf Zahnarztpraxen
- Drei psychotherapeutische Praxen
- Zwei radiologische Praxen

Die geographische Verteilung der befragten medizinischen Praxen erstreckt sich von Hamburg im Norden bis Nürnberg im Süden. Von den insgesamt 16 Praxen befinden sich 8 in ländlichen und 8 in städtischen Umgebungen.

Repräsentativität der Stichprobe

Diese Stichprobe ist aus statistischen Gesichtspunkten weder hinsichtlich der Stichprobengröße noch bezüglich der Verteilung über die unterschiedlichen fachlichen, geographischen oder anderen Merkmale repräsentativ. Die Aussagen der Stichprobe sind daher qualitativ und indikativ, erlauben aber durchaus eine erste Einschätzung der allgemeinen Situation im Hinblick auf die Informations- und IT-Sicherheit von Arztpraxen in Deutschland.

Vorgehen zur Auswahl bzw. Teilnahme an der Studie

Um genügend Teilnehmerinnen und Teilnehmer zu gewinnen, wurden als Zielansprechpartner die Ärztinnen und Ärzte mit einer pauschalen Aufwandsentschädigung von 1000 € entlohnt.

Die Ansprache der möglichen Praxen erfolgte über die Partner (Bayrische TelemedAllianz GmbH und die DATATREE AG) und war insoweit herausfordernd, als die Motivation der Teilnahme an der Studie bei den angefragten Praxen relativ gering war.

4.2 Charakteristiken der untersuchten Arztpraxen

Die statistischen Daten werden stark durch zwei Ausreißer (Praxis mit einem Mitarbeiter und Praxis mit 150 Angestellten) verzerrt. Daher wird im Folgenden jeweils der Median über die statistische Erhebung angegeben.

Patienten / Behandlungen pro Jahr

Die Praxen haben zwischen 200[2] und 600.000 Patientenstammdaten

- Durchschnitt: ~ 57.000
- Median: 5.000

Die Praxen behandeln zwischen 200 und 100.000 Patienten pro Jahr

- Durchschnitt: ~ 12.000
- Median: 16.000

Mitarbeiter

Die Anzahl Mitarbeiterinnen und Mitarbeitern der Praxen liegt zwischen 1 und 150, die Anzahl der Ärztinnen und Ärzte zwischen 1 und 21.

- Durchschnittliche Anzahl: 21,8 Mitarbeiterinnen und Mitarbeitern / 4,4 Ärztinnen und Ärzte
- Median: 7 Mitarbeiterinnen und Mitarbeitern / 3,5 Ärztinnen und Ärzte

Davon arbeiten etwas mehr als 95 % regelmäßig mit IT-Systemen.[3]

IT-Dienstleister

13 Praxen werden durch externe Dienstleister unterstützt, 3 Praxen beschäftigen keine Dienstleister, die IT-Administration erfolgt durch Mitarbeiterinnen und Mitarbeitern, Bekannte oder in einem Falle den Arzt selbst.

Die 13 Dienstleister haben zwischen 2 und 100 Mitarbeiterinnen und Mitarbeitern.

- Durchschnittliche Anzahl Mitarbeiterinnen und Mitarbeitern: 18,3
- Median: 2,5

Laut Angaben in den Fragebögen haben 14 Dienstleister keine zertifizierten Nachweise über die IT-Sicherheitsbefähigung der Mitarbeiterinnen und Mitarbeitern.

13 Dienstleister haben Remote-Zugriff auf die Systeme / Teile der Infrastruktur, davon die meisten Dienstleister nur per freigeschalteter Remote-Session.

Nur 2 Praxen gaben an, mehrere Dienstleister zu beschäftigen. Die restlichen 14 gaben nur einen einzigen Dienstleister an, daher werden diese Daten nicht weiter berücksichtigt.

Praxisverwaltungssoftware

Die Stichprobe ist dadurch gekennzeichnet, dass alle Praxen (bei einer Befragung wurde keine Angabe gemacht) unterschiedliche Softwareprodukte für die Praxisverwaltung verwenden. Dies ist ein Indikator für die Heterogenität des Marktes für diese Art von Software. Ohne dass eine genaue Untersuchung der Softwareprodukte durchgeführt wurde, ist die Vermutung zulässig, dass nicht alle Softwarehersteller

[2] Die befragten psychotherapeutischen Praxen haben einen deutlich kleineren Patientenstamm, als die anderen Praxen, die im Rahmen dieses Berichts befragt wurde. Es kann sich hier darüber hinaus noch um eine junge Praxis handeln. Dies wurde jedoch nicht abgefragt.

[3] Es sind teilweise Reinigungskräfte angestellt, die nicht mit den IT-Systemen arbeiten.

adäquate Sicherheitsmechanismen (Sicherheitsfunktionen, regelmäßige Patches etc.) implementieren bzw. bereitstellen. Die Vermutung wird auch durch die Tatsache unterstrichen, dass es laut Angaben nur bedingt automatisierte Prozesse oder Bereitstellung von Patches gibt (fünf Praxen machen laut Fragebogen Patches mehr oder weniger regelmäßig per Hand).

4.3 Clusterung der Praxen

Nach Auswertung der Fragebögen ergeben sich mögliche Clusterungen / Dimensionen für eine systematische Prüfung, inwieweit Schwachstellen von bestimmten Faktoren bestimmt werden. Diese sind:

- Fachlichkeit
- Größe der Praxis
- Größe der Dienstleister
- Ländliche oder städtische Praxis

Die Fachlichkeit hat – zumindest in der Stichprobe – eine hohe Korrelation mit der technischen Ausstattung, der IT-Infrastruktur, der Netzwerkarchitektur und der Anzahl der angeschlossenen medizinischen Geräte und wird deswegen als separate Dimension nicht weiter betrachtet.

Die Beschreibung der Beispielpraxen in Kapitel 4.4 orientiert sich an den Clustern der Fachlichkeit, da hier die größte Übereinstimmung innerhalb der Cluster gegeben ist.

Clusterung über die Fachlichkeit

Bezüglich der Fachlichkeit bieten sich natürlicherweise folgende Cluster an:

- Psychotherapeutische Praxen
- Allgemeinmediziner
- Zahnarztpraxen
- Radiologische Praxen

In diesen Clustern bedingen die fachlichen Themen, wie oben erwähnt, die IT-Ausstattung. Während psychotherapeutische Praxen eine sehr einfache Ausstattung haben (häufig nur ein Notebook und Kartenlesegeräte für die elektronische Gesundheitskarte und den elektronischen Heilberufsausweis), verfügen allgemeinmedizinische- sowie zahnärztliche Praxen über zusätzliche Server und medizinische Geräte, die auch häufig an die Netzwerke angeschlossen sind. Bei radiologischen Praxen steigt die Anzahl technischer und medizinischer Geräte und damit die Komplexität der Infrastruktur nochmals an.

Clusterung über die Praxisgröße

Die Größe der Praxen (Anzahl Patientinnen und Patienten, Mitarbeiterinnen und Mitarbeitern) hängt zwar auch bedingt von der Fachlichkeit ab, bietet sich aber als Cluster-Faktor an, da organisatorische Anforderungen an die Informationssicherheit (entsprechend der Stichprobe) mit der Praxisgröße korrelieren.

Mit einer Ausnahme (Praxis mit einem Mitarbeiter) befinden sich 11 der 16 Praxen in der Größe 4–15 Mitarbeiterinnen und Mitarbeitern (Durchschnitt 8 Mitarbeiterinnen und Mitarbeitern).

Das zweite Cluster bilden die größeren Arztpraxen (25–150 Mitarbeiterinnen und Mitarbeitern), wobei eine Praxis mit 150 Mitarbeiterinnen und Mitarbeitern heraussticht.

Die Größe des Patientenstamms korreliert mit der Größe der Arztpraxen und wird daher hier nicht weiter als eigener Faktor betrachtet.

Clusterung über die Dienstleistergröße

Bei den Dienstleistern sind drei Cluster erkennbar.

Bei den Dienstleistern sind drei Cluster erkennbar. Das erste Cluster bilden Praxen mit bedingter Dienstleisterunterstützung (Eigenverantwortung, Bekannter), das zweite Cluster Praxen mit Dienstleistern, die 1 – 3 Mitarbeiter haben (fünf Praxen), das dritte Cluster Praxen mit vier Dienstleistern, mit 35 bis 100 Mitarbeitern.

Wie im Diagramm zu sehen ist, korreliert die Dienstleistergröße nur bedingt mit der Praxisgröße.

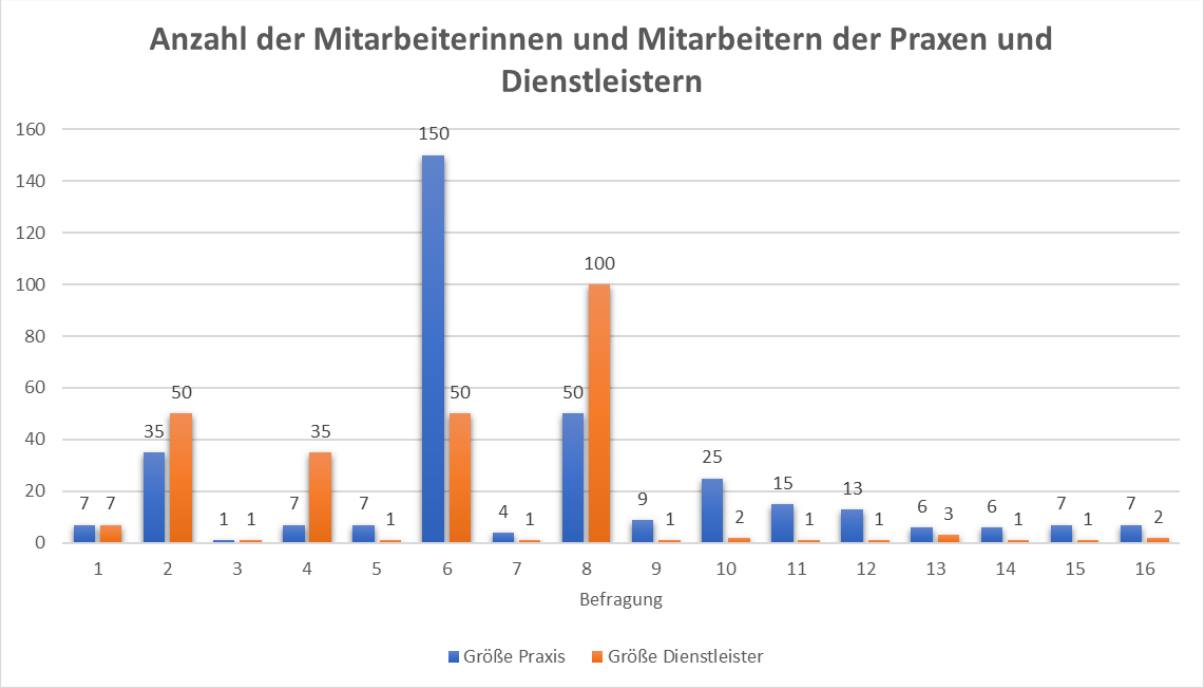


Abbildung 1 – Vergleich der Anzahl der Mitarbeiterinnen und Mitarbeitern (inkl. Ärztinnen und Ärzten) von Praxen und Dienstleistern.

Clusterung über die Lokation (ländlich, städtisch)

Die Praxen sind zu 50 % jeweils in ländlichen bzw. städtischen Umgebungen lokalisiert. Daraus ergeben sich natürlicherweise zwei Cluster: Ländliche Praxen und städtische Praxen.

4.4 Beschreibung der Arztpraxen

Im folgenden Text werden die drei Cluster bezüglich der Fachlichkeit anschaulicher beschrieben. Die Beispiele verallgemeinern die erhobenen Daten aus den Fragebögen nach den fachlichen Kategorien.

4.4.1 Psychotherapeutische Praxen

Die untersuchten psychotherapeutischen Praxen haben einen oder wenige Angestellte, die meist auch selbst Therapeutinnen und Therapeuten sind. Im Patientenstamm finden sich wenige hundert Patienten und es werden auch ähnlich viele Behandlungen pro Jahr durchgeführt. Wenn IT-Dienstleister eingesetzt werden, handelt es sich bei diesen um eher kleine Unternehmen mit 1–3 Mitarbeiterinnen und Mitarbeitern, die laut Angaben in den Fragebögen auch nicht spezifisch für IT-Sicherheitsthemen qualifiziert sind. Falls Remote-Zugriff möglich ist, geht das nur über die ausdrückliche Genehmigung der jeweiligen Praxis.

Die IT-Ausstattung der Praxen ist überschaubar, häufig sind nur Notebooks für die Therapeutinnen und Therapeuten, ein Kartenlesegerät und ein TI-Konnektor bzw. eine KV-Anbindung vorhanden. Typischerweise wird eine Verwaltungssoftware, die lokal installiert ist, eingesetzt. Die Geräte hängen parallel am selben Router / Internetzugang, es gibt keine dedizierten Netzwerkzonen. Die Geräte sind mit

einer Antivirensoftware versehen, das Patchen erfolgte jedoch in nur in einer der befragten Praxen regelmäßig. Die Therapeutinnen und Therapeuten kümmern sich häufig auch selbst um die IT, die Maßnahmen in der IT bzw. zur Sicherheit hängen daher auch stark von der IT-Affinität des Therapeuten ab. Datensicherungen werden laut Angaben täglich durchgeführt, in zwei von drei Fällen erfolgt auch eine Restore-Übung.

Patientinnen und Patienten befinden sich laut Angaben nie allein im Behandlungsraum, grundsätzlich wird viel Wert auf Anonymität, auch gegenüber anderen Patienten, gelegt.

4.4.2 Radiologie

Die Radiologie-Praxen in der Stichprobe sind bezüglich der Anzahl der Mitarbeiterinnen und Mitarbeiter, Ärztinnen und Ärzte sowie Patientinnen und Patienten deutlich größer als die anderen Praxen. Auffallend ist, dass die Radiologie-Praxen innerhalb der Stichprobe den höchsten Grad an Sicherheitsvorkehrungen haben bzw. das Thema Informations- und IT-Sicherheit am besten abdecken.

Die IT-Ausstattung ist umfangreicher und umfasst neben einer größeren Anzahl von Servern und Clients auch eine größere Anzahl medizinischer Geräte, die an das Netzwerk angeschlossen sind. Die größere der beiden befragten Praxen setzt zusätzlich mehrere Systeme zur automatisierten Bildauswertung ein. Die Praxen verfügen über zugangsbeschränkte Server-Räume, eine Praxis hat Server im Rechenzentrum eines Dienstleisters ausgelagert, zu dem eine dauerhafte VPN-Verbindung besteht. Die internen Netze sind entweder bereits segmentiert oder die Segmentierung ist geplant. Remote-Zugriffe für Mitarbeiterinnen und Mitarbeiter sind möglich und über VPN-Verbindungen eingerichtet. Dienstleister haben teilweise auch Zugriff auf die Netze und Geräte.

Die größere Praxis hat eigene IT-Mitarbeiterinnen und -Mitarbeitern und nutzt zusätzlich mehrere Dienstleister. Der Haupt-IT-Dienstleister ist weltweit aktiv und deckt die Themen DSGVO, inklusive TOMs bzw. allgemeine IT-Sicherheit innerhalb der Stichprobe am besten ab.

Die kleinere der befragten Praxen beschäftigt als Dienstleister ein kleines Unternehmen mit zwei Arbeitskräften, das für verhältnismäßig wenige Praxen tätig ist. Dennoch ist dieser Dienstleister im Gegensatz zu den anderen kleinen Dienstleistern in der Studie sowohl formal (Datenschutz etc.) als auch technisch besser bezüglich der IT-Sicherheit aufgestellt.

4.4.3 Allgemeinmediziner und Zahnärzte

Die allgemeinmedizinischen und zahnärztlichen Praxen sind relativ homogen, was die IT-Infrastruktur anbelangt. Typischerweise gibt es neben mehreren Clients jeweils einen Server, der sich in 50 % der Fälle in einem abgeschlossen, separaten Raum befindet. Die Unterstützung durch IT-Dienstleister ist jedoch heterogen, hier reicht die Bandbreite von keinem Dienstleister (Unterstützung durch einen Bekannten) bis zu professionellen Dienstleistern mit 15 Mitarbeiterinnen und Mitarbeitern. Der Remote-Zugriff durch Dienstleister wird jedoch in allen relevanten Fällen überwacht und ist nur nach Freischaltung möglich. Der Zugriff auf die Systeme erfolgt in mehreren Fällen durch generische Konten mit geteilten Zugangsdaten statt personalisierten Benutzerkonten.

In jeder der befragten Praxen hat eine Reinigungskraft physischen Zugang zu den Räumlichkeiten, auch außerhalb der Öffnungszeiten.

5 Angreifer / Angriffe

Das Spektrum möglicher IT-Angriffe auf Arztpraxen ist sehr groß und enthält prinzipiell alle möglichen Angreifertypen (vom Skript-Kiddie bis hin zu staatlichen Akteuren) sowie alle denkbaren Angriffsversuche (vom Einbruch bis hin zum DDoS-Angriff). Eine zielführende Analyse mit dem Ziel der Verbesserung der Sicherheit von Arztpraxen sollte sich jedoch auf die spezifischen Besonderheiten dieser Praxen beziehen. Daher werden nur drei relevante Angreifertypen im Detail behandelt:

- Zufällige Angreiferinnen und Angreifer, die situativ durch die Gelegenheit und die Möglichkeit eines Angriffes zu einem IT-Angriff verführt werden.
- Gezielte Angreiferinnen und Angreifer, die mit einem definierten Ziel (z. B. dem Ausspähen von Daten) geplante IT-Angriffe durchführen.
- Kriminelle Organisationen, die mit der Motivation des finanziellen Gewinns IT-Angriffe durchführen.

In der Analyse werden folgende Angreifer bewusst nicht näher betrachtet:

- Skript-Kiddie[4]s, da zum einen die Vermutung naheliegt, dass Arztpraxen kein primäres Ziel von Skript-Kiddies sind, zum anderen mögliche Schwachstellen für typische Angriffe von Skript-Kiddies vollständig durch die Angreifergruppe „Gezielte Angreifer“ abgedeckt sind.
- Hacktivisten, da Arztpraxen mit geringer Wahrscheinlichkeit im Fokus dieser Gruppen stehen und wiederum die möglichen Schwachstellen für Angriffe durch die Gruppe „Gezielte Angreifer“ abgedeckt sind.
- Staatliche Angreifer, da zwar durchaus Interesse an bestimmten Informationen über Patientinnen und Patienten vorliegen könnte, eine Absicherung gegen Angriffe dieser Gruppe jedoch weit über den angestrebten Basisschutz von Arztpraxen hinausgeht.

Die ausgewählten Angreifergruppen werden im Folgenden genauer beschrieben. Allgemein ist jedoch anzumerken, dass sowohl die Angreiferinnen und Angreifer als auch die Angriffe und Angriffspfade nicht trennscharf zu betrachten sind. Als Beispiel sei genannt, dass ein zufälliger Angreifer durchaus später auch kriminelle Absichten verfolgen kann, oder eine kriminelle Angreiferin oder ein krimineller Angreifer sich als Patientin oder Patient Zugang verschafft.

Eine weitere Dimension, die sich über diese drei Angreiferprofile verteilt, ist die Frage nach externen bzw. internen Angriffen. Generell können in allen drei Profilen Angriffe durch Interne (z. B. Mitarbeiterinnen und Mitarbeiter, Dienstleister) oder durch Externe (z. B. Patientinnen und Patienten oder anonyme Angreifer über das Internet) erfolgen. Das hat Einfluss auf die Möglichkeiten der jeweiligen Angreiferin oder des Angreifers – interne Mitarbeiterinnen und Mitarbeiter haben z. B. grundsätzlich mehr Zeit, Zugriffsmöglichkeiten und Berechtigungen, um Angriffe durchzuführen.

5.1 Zufälliger Angreifer

Know-how	Finanzielle Mittel	Erfolgschancen	Risiko
Niedrig	Niedrig	Mittel	Hoch

5.1.1 Angreiferprofil

Das Profil des zufälligen Angreifers ist sehr heterogen und umfasst ein sehr breites Spektrum innerhalb der Bevölkerung. Auch die Fähigkeiten dieser Angriffsgruppe sind vermutlich breit gestreut und reichen von geringen bzw. kaum vorhandenen IT-Kenntnissen bis hin zum ausgebildeten professionellen Hacker.

4 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf 2.1.1

Allerdings wird in diesem Profil eher von einer durchschnittlichen mitarbeitenden oder zu behandelnden Person ohne besondere Qualifikation für IT-Angriffe ausgegangen.

Wesentliche Mitglieder dieser Angriffsgruppe sind Patientinnen und Patienten, Mitarbeiterinnen und Mitarbeiter oder Dienstleister. Die Wahrscheinlichkeit eines Angriffes wird durch zwei wesentliche Faktoren bestimmt:

- die sehr hohe Anzahl an Praxen und Patientinnen und Patienten in Deutschland
- die Anzahl der erfassten Cybercrime-Fälle – in 2021 nach Polizeilicher Kriminalstatistik 146.363 Fälle (Bundeskriminalamt, 2021).

5.1.2 Motivation

Wesentliches Merkmal dieser Gruppe ist, dass ein Angriff eher durch die Möglichkeit bedingt wird und keine zielgerichtete Planung und Durchführung vorliegt.

Die Motivation eines Gelegenheitsangreifers kann sehr unterschiedlich sein, generell könnten folgende Motivationen vorhanden sein:

- Die Vermutung liegt nahe, dass die Hauptmotivation Neugier ist. D. h. eine Patientin oder ein Patient nutzt die Gelegenheit, Informationen über die Gesundheit für ihn interessanter Menschen (Nachbarn, Bekannte oder Freunde) zu erlangen.
- Eine weitere Motivation ist, durch das erlangte Wissen eine gewisse Macht über andere Menschen zu erlangen. Erpressungsversuche von Patientinnen und Patienten oder der Arztpraxis infolge dieser Macht sind nicht auszuschließen.
- Ein weiterer Motivationsfaktor könnte das Testen des eigenen Könnens sein.
- Auch die Gelegenheit, über Rezepte beispielsweise an Betäubungsmittel zu gelangen, kann eine Motivation sein.

5.1.3 Gelegenheit / Angriffspfade

Die Gelegenheit für zufällige Angriffe ergibt sich im Wesentlichen aus a) physischen Zugängen zur Praxis oder b) Online-Zugriffen auf Portale für Termine etc.

a) Physischer Zugang durch Patientinnen und Patienten:
    a. Patientinnen und Patienten verbringen häufig Wartezeiten in Räumen der Arztpraxis, ohne dass eine weitere Person im Raum ist. Dies trifft neben dem Wartezimmer auch für Labore und Behandlungsräume zu, vor allem wenn eine Praxis über mehrere Räume verfügt.
    b. Mögliche Angriffspfade sind dabei:
        i. Physischer Zugang zu Rechnern in diesen Räumen
        ii. Zugriff auf das WLAN der Praxis
        iii. Zugriff auf das LAN über ungeschützte Netzwerkdosen

b) Zugang durch Dienstleisterinnen und Dienstleister:
    a. Dienstleisterinnen und Dienstleister sind ebenfalls oft allein in entsprechenden Räumen der Praxis und haben somit Zugriff auf mögliches IT-Equipment. Dienstleister umfasst dabei z. B. Reinigungspersonal, aber auch Mitarbeiterinnen und Mitarbeitern von Haustechnikdiensten etc.
    b. Mögliche Angriffspfade:
        i. Physischer Zugang zu Rechnern
        ii. Direkter, eventuell privilegierter Zugang zu Computer-Systemen (z. B. IT-Dienstleister)

5.1.4 Chancen / Auswirkung des Angriffs

Die Chancen auf einen erfolgreichen Angriff sind hoch, d. h. eine Patientin oder ein Patient kann in einigen Minuten Wartezeit durchaus die digitalen Krankenakten mehrerer Patientinnen und Patienten einsehen

und eventuell sogar kopieren. Eine Dienstleisterin oder Dienstleister hat gegebenenfalls deutlich mehr Zeit und daher noch höhere Chancen auf einen erfolgreichen Angriff. Eine technische Dienstleisterin oder Dienstleister hat sehr i.d.R auch ein besseres Verständnis davon, wie Schwachstellen und interessante Daten gefunden werden und möglicherweise sogar Geräte dabei, die ihn oder sie dabei unterstützen.

Die Auswirkungen umfassen dabei folgende Eckpunkte:

a) Verlust der Vertraulichkeit: Einsicht in Patientendaten (Lesen, Foto des Bildschirms etc.)
b) Verlust von Integrität: Manipulation von Diagnosen, Rezepten
c) Verlust der Verfügbarkeit: Löschen von Datensätzen

Da es sich hier um besonders schützenswerte Daten handelt, können die finanziellen Auswirkungen hoch sein. Das gilt insbesondere dann, wenn fahrlässiges Verhalten (Patient allein mit ungesperrtem PC) zu einer Verletzung der Vertraulichkeit führt.

5.2 Gezielte Angreifer

Know-how	Finanzielle Mittel	Erfolgschancen	Risiko
Hoch	Mittel	Hoch	Hoch

5.2.1 Angreiferprofil

Gezielte Angreiferinnen und Angreifer haben typischerweise einen fundierten technischen Background und das Know-how, spezifische und komplexere IT-Angriffe durchzuführen. Die finanziellen Mittel und Ressourcen sind beschränkt, dürften aber durchaus auch für komplexere Angriffe ausreichen.

5.2.2 Motivation

Die Motivation für gezielte Angriffe ist wiederum sehr divers. D. h. die Bandbreite reicht von kriminellen Motiven (finanzielle Gewinne) bis hin zur motivierten hackenden Person, die „nur“ nachweisen möchte, dass ein Angriff möglich ist.

5.2.3 Gelegenheit / Angriffspfade

Speziell im Umfeld der Arztpraxen bietet sich auch für eine gezielte Angreiferin oder einen Angreifer der physische Zugang als Patientin oder Patient oder Dienstleisterin oder Dienstleister an (siehe auch oben).

Neben den physischen Zugriffen sind aus dieser Gruppe auch Remote-Angriffe über Portale, Webseiten etc. erwartbar.

Die Angriffsziele sind vielfältig:

- Patienteninformationssysteme
- Medizinische Geräte
- Personalverwaltungssysteme
- Abrechnungssysteme
- Informationssysteme wie Websites

5.2.4 Chancen / Auswirkung des Angriffs

Die Chancen, dass einer Computerexpertin oder einem Computerexperten ein erfolgreicher Angriff auf eine Praxis gelingt, sind als hoch einzuschätzen. Die Auswirkungen sind sehr vielfältig. Die möglichen Auswirkungen schließen unter anderem Reputationsschäden, finanzielle Schäden der Praxen sowie gesundheitliche Schäden der Patientinnen und Patienten sowie die Zerstörung von medizinischen Geräten und Servern ein.

5.3 Kriminelle Organisationen

Know-how	Finanzielle Mittel	Erfolgschancen	Risiko
Hoch – Sehr hoch	Hoch	Hoch	Hoch

5.3.1 Angreiferprofil

Kriminelle Organisationen sind häufig sehr gut ausgestattete und motivierte Vereinigungen mit der Absicht, finanzielle Gewinne zu erzielen. Mit teilweise sehr gutem Know-how und „modernsten“ Tools sind diese Angreiferinnen und Angreifer bestens ausgestattet.

5.3.2 Motivation

Die wesentliche Motivation der kriminellen Organisationen ist finanzieller Gewinn. Dabei gehen diese Gruppen durchaus „wirtschaftlich“ vor, d. h. der Aufwand der Angriffe muss im Verhältnis zum möglichen Gewinn stehen.

Dass kriminelle Organisationen gezielt einzelne Praxen angreifen, ist denkbar, wird jedoch als nur bedingt wahrscheinlich betrachtet. Eher liegt die Vermutung nahe, dass Arztpraxen Opfer von Angriffswellen werden, d. h. eher zufällig in die Liste der Angriffsziele geraten. Ein Beispiel hierfür wäre, wenn eine E-Mail-Adresse einer Praxis bei einem Hack oder Leak entwendet und dann für einen Phishing Angriff genutzt werden würde.

5.3.3 Gelegenheit / Angriffspfade

Die Gelegenheit für gezielte Angriffe beschafft sich die kriminelle Organisation häufig durch eine Reconnaissance-Phase.

Hierbei werden in der Regel bekannte Schwachstellen durch gezielte Scans gefunden und ausgenutzt oder es werden Social-Engineering-Methoden wie Phishing eingesetzt.

5.3.4 Chancen / Auswirkung des Angriffs

Die Wahrscheinlichkeit dafür, dass ein Angriff aus Sicht einer Täterin oder eines Täters erfolgreich verläuft, ist hoch. Die Auswirkungen eines erfolgreichen Angriffs sind bei dieser Gruppe in der Regel hoch bis schwerwiegend. Ein erfolgreicher Diebstahl von Patientendaten und deren Veröffentlichung könnte die Reputation der betroffenen Praxen stark beinträchtigen. Auch die Zerstörung von Datensätzen und Infrastruktur kann dazu führen, dass Praxen über längere Zeit nicht mehr arbeitsfähig sind, was auch deren Fortbestand gefährden könnte.

6 Übergreifende Fragestellungen

Bei einer sehr kleinen, nicht repräsentativen Stichprobe ist eine statistische Auswertung grundsätzlich mit Zurückhaltung zu betrachten. Dennoch wurde der Vollständigkeit halber eine Auswertung der Daten nach den Clustern / Dimensionen gemäß Kapitel 4.3 durchgeführt. Die Ergebnisse in diesem Kapitel dienen somit als ergänzende Indikatoren dafür, ob gewisse Erwartungen durch die Daten bestätigt werden. Die Auswertung wurde auf Basis der relativen Häufigkeit des Vorhandenseins von Schwachstellen in den Praxen des jeweiligen Clusters durchgeführt. Für jede Schwachstelle wurde die Anzahl der Praxen im Cluster erfasst, in denen die betreffende Schwachstelle auftrat, und mit der Gesamtzahl der im Cluster befindlichen Praxen auf einen Wert zwischen 0 und 1 normiert. Dies ergibt die relative Häufigkeit der Schwachstellen im Cluster. Die folgenden Diagramme stellen somit die relativen Häufigkeiten der individuellen Schwachstellen dar, jeweils bezogen auf ein betrachtetes Cluster.

Als Vergleichswert über alle Schwachstellen dient der Mittelwert der relativen Häufigkeit über alle Schwachstellen. Diese Werte sind zu Beginn der folgenden Kapitel für die jeweiligen Cluster angegeben. Eine detaillierte Aufstellung der vorhandenen Schwachstellen bei allen teilnehmenden Praxen findet sich in Anhang 11.

6.1 Auswertung nach Schwachstellenhäufigkeit / Cluster

6.1.1 Auswertung nach Fachlichkeit:

Die relative Schwachstellenhäufigkeit bezogen auf die fachlichen Cluster ergibt sich wie folgt:

- Psychotherapeutische Praxen: 58 %
- Allgemeinmedizinerpraxen: 51 %
- Zahnarztpraxen: 58 %
- Radiologie-Praxen: 40 %

Die folgende Abbildung zeigt die relative Häufigkeit der einzelnen Schwachstellen bezogen auf die fachlichen Cluster.

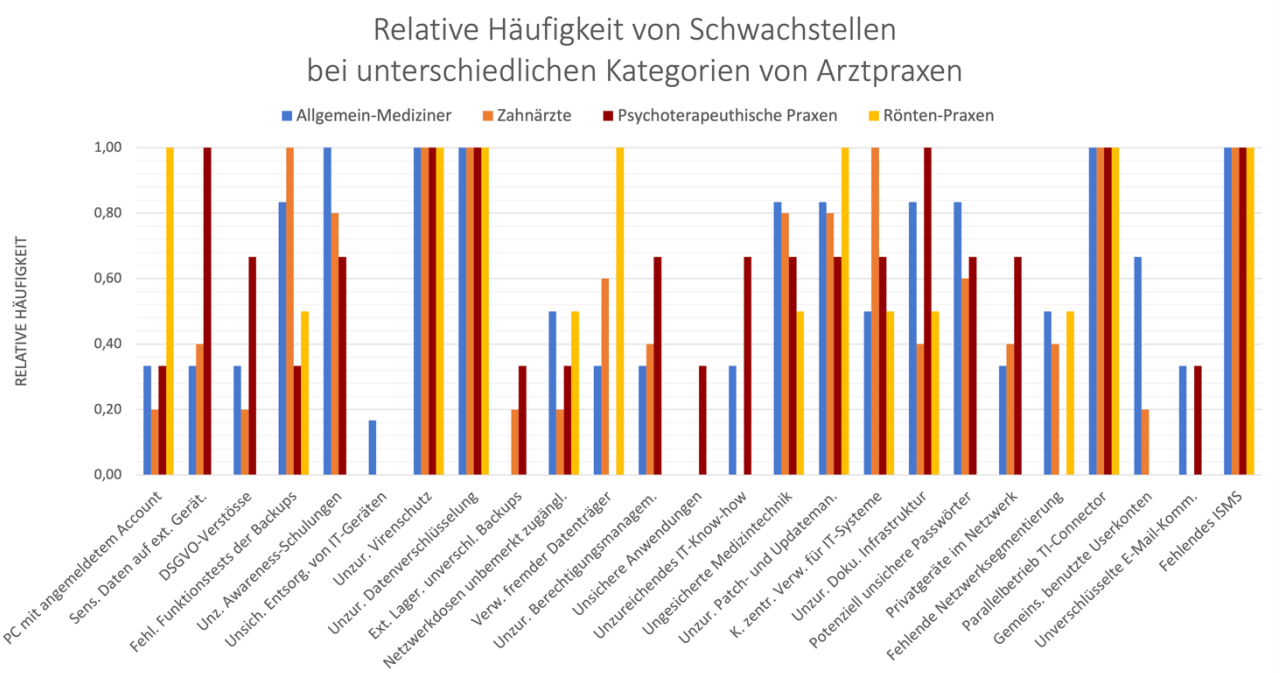


Abbildung 2 - Relative Häufigkeit der Schwachstellen in Abhängigkeit zur Fachlichkeit

6.1.2 Auswertung nach Praxisgröße

Die relative Schwachstellenhäufigkeit bezogen auf die Größe der Praxen ergibt sich wie folgt:

- Praxen mit bis zu 15 Mitarbeiterinnen und Mitarbeitern: 57 %
- Praxen mit mehr als 15 Mitarbeiterinnen und Mitarbeitern: 42 %

Die folgende Abbildung zeigt die relative Häufigkeit der einzelnen Schwachstellen bezogen auf die beiden Cluster zur Praxisgröße.

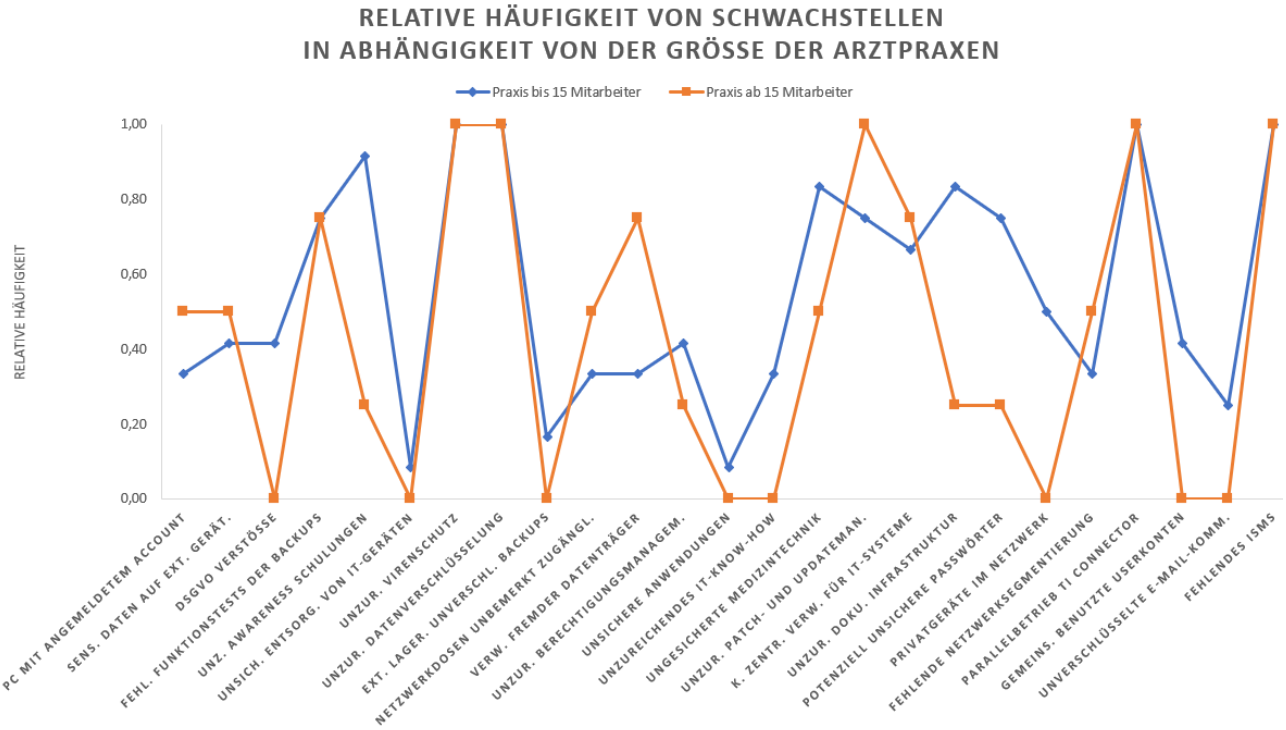


Abbildung 3 - Relative Häufigkeit der Schwachstellen in Bezug auf Praxis-Größe

6.1.3 Auswertung nach Größe der Dienstleister

Die relative Schwachstellenhäufigkeit bezogen auf die Größe der Dienstleister ergibt sich wie folgt:

- Kein dedizierter externer Dienstleister: 60 %
- Dienstleister mit bis zu 15 Mitarbeiterinnen und Mitarbeitern: 47 %
- Dienstleister mit über 15 Mitarbeiterinnen und Mitarbeitern: 46 %

Die folgende Abbildung zeigt die relative Häufigkeit der einzelnen Schwachstellen bezogen auf die Größe der IT- Dienstleister.

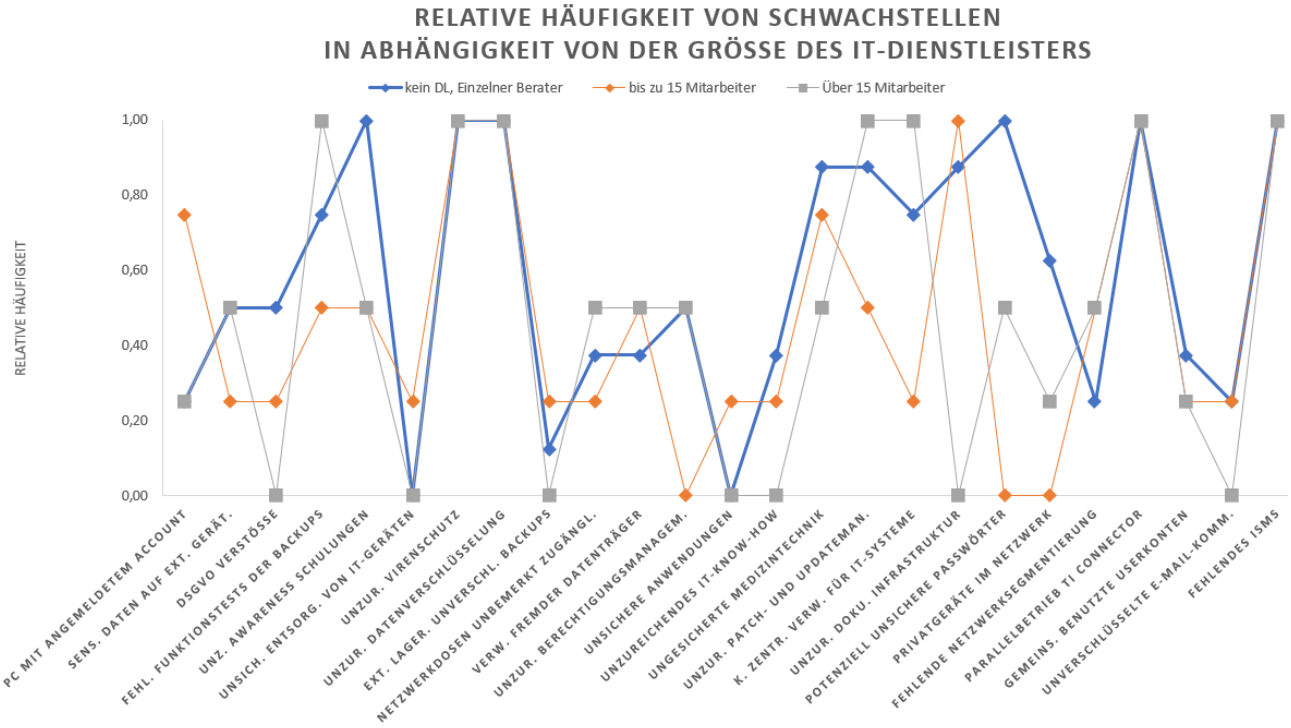


Abbildung 4 - Relative Häufigkeit der Schwachstellen in Bezug auf die Größe der Dienstleister

6.1.4 Auswertung nach Lokation

Die relative Schwachstellenhäufigkeit bezogen auf die Lokation ergibt sich wie folgt:

- Ländlich: 56 %
- Städtisch: 50 %

Die Verteilung der einzelnen Schwachstellen nach der Lokation ist in der folgenden Grafik dargestellt.

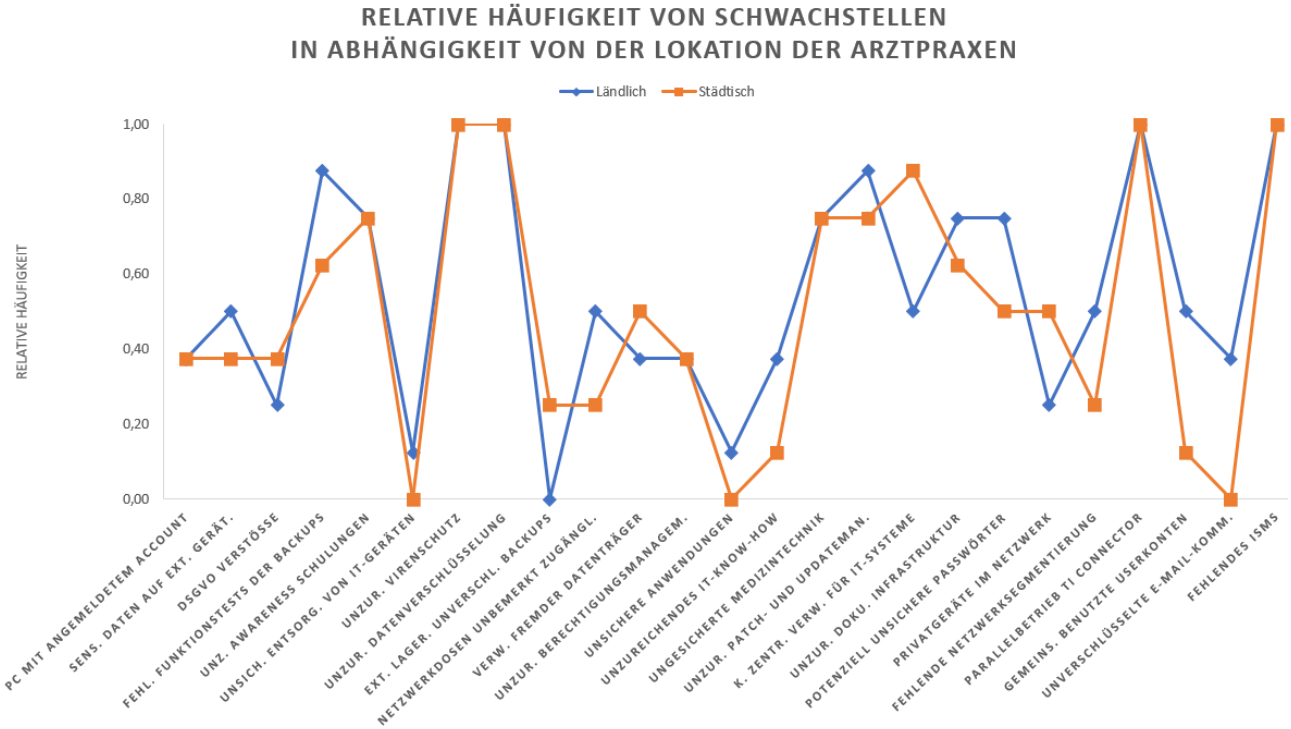


Abbildung 5 - Relative Verteilung von Schwachstellen nach Lokation

6.2 Bewertung der statistischen Befunde

Die Zahlen stützen folgende Erwartungen / Annahmen:

- Die Fachlichkeit hat – vermutlich auch aufgrund der notwendigen IT-Ausstattung – einen Einfluss auf die Qualität der Sicherheit. In der Stichprobe gibt es einen deutlichen Unterschied, wobei die Radiologie-Praxen die wenigsten, die psychotherapeutischen Praxen die meisten Schwachstellen aufweisen.
- Der erwartete Einfluss der Größe der Praxis wird bestätigt. Praxen mit mehr Mitarbeiterinnen und Mitarbeitern haben tendenziell weniger Schwachstellen. Die Datenbasis ist jedoch zu klein, um eine mögliche Korrelation zwischen Fachlichkeit und Größe der Praxis zu berechnen. Es ist jedoch unter Umständen möglich, dass eine der beiden Dimensionen (Größe oder Fachlichkeit) in der Realität ein größeres Gewicht hat als die andere Dimension.
- Die Größe des Dienstleisters hat nur insoweit spürbaren Einfluss, als semi-professionelle Ansätze (Eigenverantwortung, Bekannter etc.) schlechter abschneiden als professionelle Dienstleister. So sind Praxen, die keinen Dienstleister haben, im Mittelwert über alle Schwachstellen, in 60% der Fälle betroffen, bei einem Dienstleister mit bis zu 15 Mitarbeitern in 47% und über 15 Mitarbeitern in 46% betroffen.
- Die Lokation hat auf Basis der Daten nur einen kleinen Einfluss, was auch der Vorabeinschätzung entspricht. Im Mittelwert über alle Schwachstellen sind ländliche Praxen zu 56%, Städtische zu 50% betroffen.

6.3 Ableitungen aus den Auswertungen

Mit gebotener Vorsicht können aus den Zahlen und Auswertungen folgende Ableitungen getroffen werden:

- Die Größe bzw. Fachlichkeit der Praxen ist durch Maßnahmen per Definition nicht zu beeinflussen. Die bessere Situation bei den größeren Praxen bzw. bei Radiologie-Praxen dürfte sehr stark mit dem Einsatz dedizierter Mitarbeiter im IT-Umfeld zusammenhängen. Ein Modell, das sich kaum auf kleinere Praxen übertragen lässt.
- Der Einsatz eines professionellen Dienstleisters erscheint sinnvoll und könnte die Situation allgemein verbessern, jedoch scheint auch bei professionellen Dienstleistern noch genügend Verbesserungspotenzial zu bestehen.

7 Übergreifende Lösungsansätze

Die grundlegenden gesetzlichen Anforderungen an eine bessere Informations- und IT-Sicherheit in Praxen sind vorhanden (z. B. DSGVO, Gesetz zum Schutz von Patientendaten etc.). Eine Erweiterung um zusätzliche Regulatorien wird aktuell nicht als zielführend erachtet, da mehr Bürokratie nicht unmittelbar und kurzfristig die Sicherheit erhöhen würde und zudem die Kosten für die Umsetzung Gesetz – Verordnung – Prüfung und Prüfgrundlagen nicht unbeträchtlich wären.

In diesem Kapitel werden daher praxisnahe, umsetzbare Maßnahmen mit einer akzeptablen Kostenstruktur vorgeschlagen.

- Bereitstellung einer Hilfestellung
- Bereitstellung von Musterverträgen für Dienstleister
- Verbesserung der Schulungs- und Awareness-Angebote
- Bereitstellung eines prototypischen ISMS

Keine dieser Maßnahmen wäre vollkommen kostenfrei, jedoch ist durchaus eine gemischte Finanzierung durch das BSI, Kassenverbände, Arztverbände und die Arztpraxen selbst denkbar. Entsprechend den

vorgeschlagenen Maßnahmen wäre ein sinnvoller nächster Schritt, mögliche Kostenstrukturen und Finanzierungsvorschläge zu erarbeiten und abzustimmen.

7.1 Hilfestellung

Eine Maßnahmen- oder Checkliste löst per se natürlich noch keines der angesprochenen Probleme, jedoch könnte eine Hilfestellung – vor allem für kleinere Praxen und kleinere Dienstleister – die erkannten Schwachstellen adressieren. Die Kurzfassung einer möglichen Checkliste findet sich in Kapitel 13.1.

Die Hilfestellung sollte die wichtigsten Maßnahmen in verständlicher Form darstellen. Die Liste sollte so gestaltet werden, dass die Anforderungen auch als Anhang von Verträgen mit Dienstleistern verwendet werden können. Die technische Umsetzung sollte beispielhaft, aber herstellerneutral beschrieben werden. Die Liste sollte zentral verwaltet und aktualisiert auf einer Portalseite bereitgestellt werden.

7.2 Musterverträge für Dienstleister

Auf Basis der fehlenden AV-Vereinbarungen in verschiedenen Praxen wären Musterverträge für die Vereinbarung zwischen Praxis und Dienstleister hilfreich. Die Musterverträge könnten dabei vor allem die rechtlichen Grundlagen des Datenschutzes (DSGVO-Konformität) und speziell der entsprechenden Auftragsverarbeitung in kompakter Form abbilden und somit beiden Parteien Rechtssicherheit geben.

Auch hier wären eine zentrale Bereitstellung und Aktualisierung hilfreich.

7.3 Verbesserung von Schulungs- und Awareness-Angeboten

Ein wesentliches Problem ist das Fehlen der entsprechenden IT-Sicherheits-Kenntnisse. Die Bereitstellung kostengünstiger Schulungen für Mitarbeiter und Dienstleister mit einem dedizierten Fokus auf Arztpraxen könnte dieses Manko kompensieren.

7.4 Bereitstellung eines prototypischen ISMS

Vor allem größere Praxen könnten daran interessiert sein, das Thema IT-Sicherheit auf eine breitere Basis zu stellen. Wie die Analyse zeigt, sind die Fragestellungen in den Praxen – trotz einiger sehr divergenter Parameter – sehr ähnlich, sodass ein vordefiniertes Mini-ISMS, das mit einfachen Mitteln anpassbar ist, diese Lücke kostengünstig schließen könnte.

Mögliche Inhalte eines Mini-ISMS wären:

- Scope-Definition mit Zielen
- Richtlinie für Mitarbeiter und Dienstleister
- Richtlinie für Mindestmaßnahmen (Netzwerk-, Benutzer- und Berechtigungsmanagement etc.)

Das Mini-ISMS wäre dabei eine logische Erweiterung der Hilfestellung (siehe Kapitel 7.1).

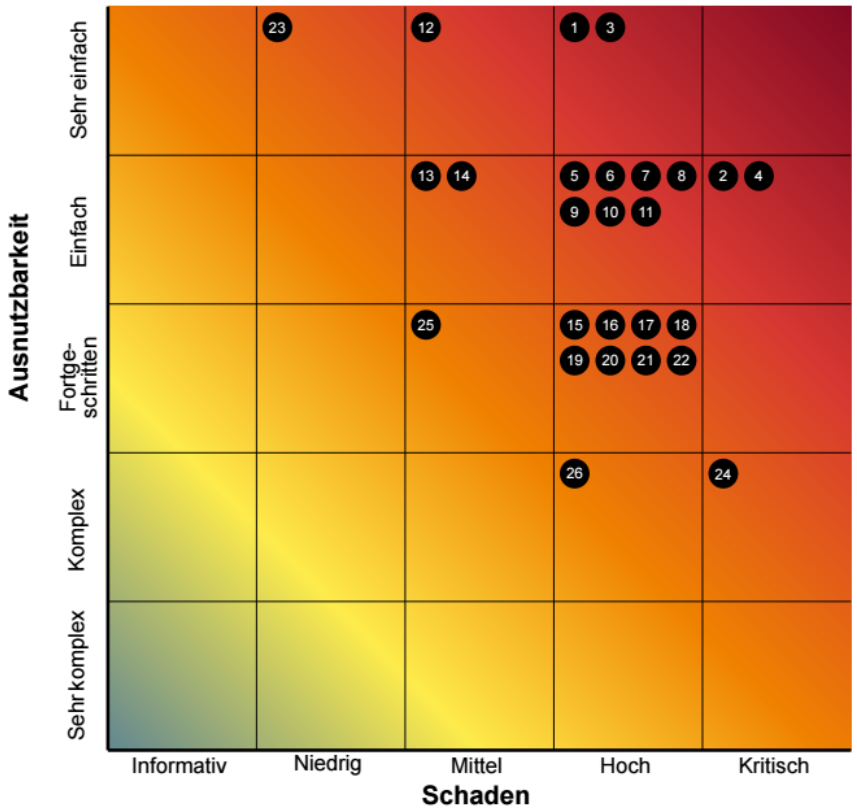
8 Schwachstellen

Die Analyse der Netzwerkinfrastruktur der evaluierten Arztpraxen bzw. die Beantwortung der Fragebögen hat einige Schwachstellen zum Vorschein gebracht. In diesem Abschnitt werden diese Schwachstellen im Einzelnen beschrieben, die potenziellen Auswirkungen im Falle der Ausnutzung der Schwachstellen dargelegt und Maßnahmen zur Beseitigung der Schwachstellen oder zumindest zur Reduzierung des aus den Schwachstellen resultierenden Risikos vorgeschlagen. Darüber hinaus wird qualitativ abgeschätzt, mit welchen Kosten durch die vorgeschlagenen Maßnahmen zu rechnen ist und welches Restrisiko jeweils verbleibt.

Die Ermittlung des Risikos erfolgt auf Basis des möglichen Schadens und der Ausnutzbarkeit der Schwachstellte. Eine Schwachstelle etwa, die sehr einfach ausnutzbar ist, hat ein erhöhtes Risiko, auch ausgenutzt zu werden.

Zu jedem Angriffsvektor – der die Ausnutzbarkeit beschreibt – wird auch die wahrscheinlichste Angreiferin oder Angreifer der definierten Angreiferprofile benannt.

Die folgende Grafik zeigt eine Verteilung der insgesamt 25 erfassten Schwachstellen. Die Darstellung basiert auf einer Risiko-Matrix, die den Schweregrad / Schaden in einer Dimension und die Ausnutzbarkeit der Schwachstelle in der zweiten Dimension zeigt:



Nr.	Schwachstelle
1	PC mit angemeldetem Account
2	Sens. Daten auf ext. Gerät.
3	DSGVO Verstösse
4	Fehl. Funktionstests der Backups
5	Unz. Awareness Schulungen
6	Unsich. Entsorg. von IT-Geräten
7	Unzur. Virenschutz
8	Unzur. Datenverschlüsselung
9	Ext. Lager. unverschl. Backups
10	Unges. Netzwerkdosen öffentl.
11	Verw. fremder Datenträger
12	Unzur. Berechtigungsmanagem.
13	Unsichere Anwendungen
14	Unzureichendes IT-Know-how
15	Ungesicherte Medizintechnik
16	Unzur. Patch- und Updateman.
17	K. zentr. Verw. für IT-Systeme
18	Unzur. Doku. Infrastruktur
19	Potenziell unsichere Passwörter
20	Privatgeräte im Netzwerk
21	Fehlende Netzwerksegmentierung
22	Parallelbetrieb TI Connector
23	Gemeins. benutzte Userkonten
24	Unverschlüsselte E-Mail-Komm.
25	Fehlendes ISMS
26	Unsichere Netzwerkkonfig.

Abbildung 6 - Risiko-Matrix, die den Schweregrad / Schaden in einer Dimension und die Ausnutzbarkeit der Schwachstelle in der zweiten Dimension zeigt.

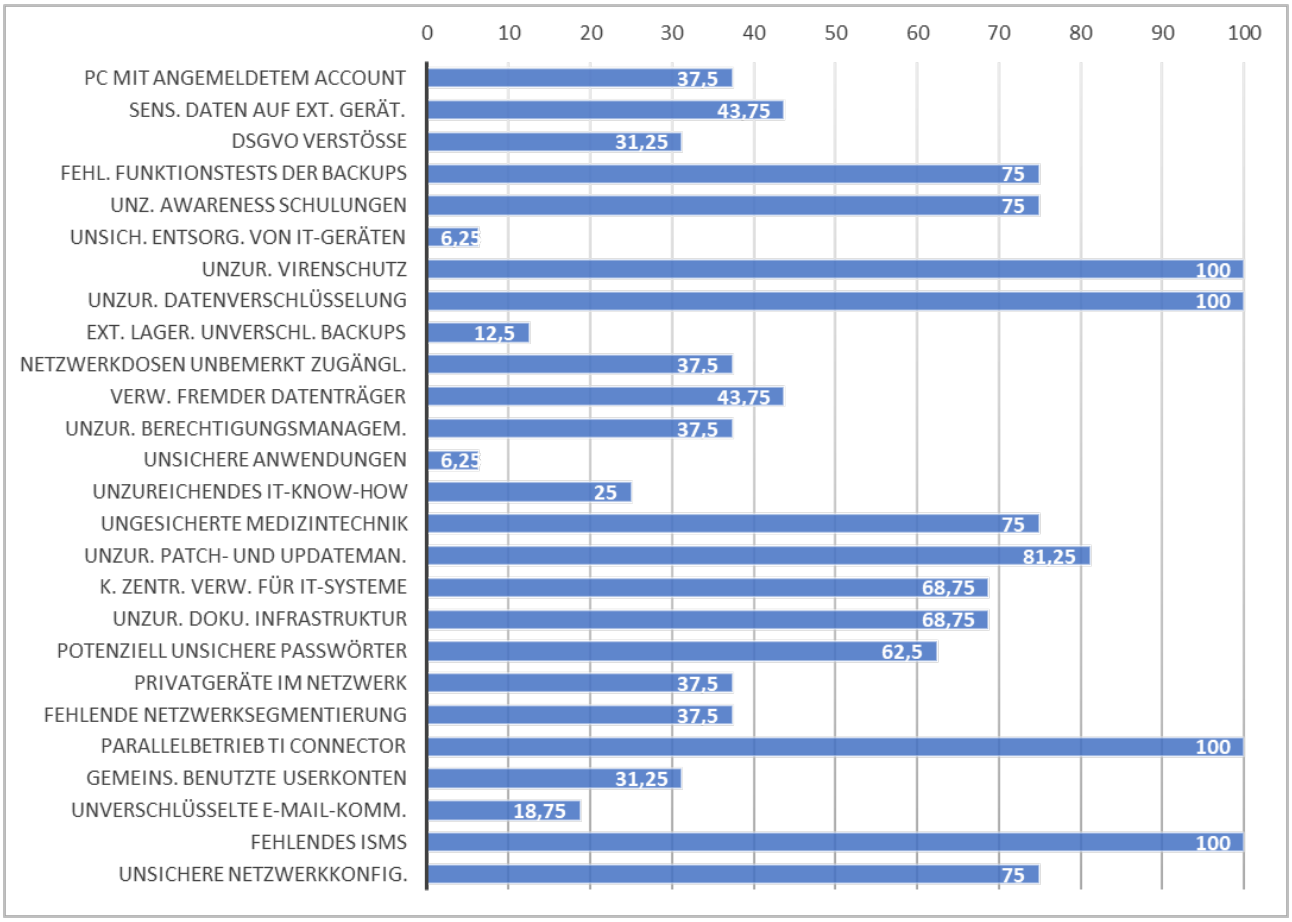


Abbildung 7 – Häufigkeit der Schwachstellen in Prozent

Die Schwachstellen werden im Einzelnen in den nächsten Abschnitten detailliert beschrieben.

8.1 PC mit angemeldetem Account

8.1.1 Beschreibung der Schwachstelle

Ein nicht gesperrter PC mit angemeldetem User ist ein leichtes Ziel. Das gilt umso mehr, wenn sich eine Patientin oder ein Patient oder eine Dienstleisterin oder ein Dienstleister allein in einem entsprechenden Raum befindet. Ohne Aufwand kann die Angreiferin oder der Angreifer dann auf Daten zugreifen und diese lesen, verändern oder löschen – dabei können alle Aktionen durchgeführt werden, für die der angemeldete Account Rechte besitzt. Darüber hinaus ist auch ein Angriff mittels der Installation von Schadsoftware, Keylogger oder Ähnlichem denkbar.

Siehe auch CWE-306 (The MITRE Corporation, 2023)

8.1.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragenbogen 6 von 16 (37,5 %) Arztpraxen mitgeteilt, dass es möglich sei, Zugang zu einem nicht gesperrten PC zu erlangen.

Entsprechend ist den Verantwortlichen der Praxen diese Schwachstelle in der Regel bekannt, jedoch deuten einzelne Kommentare darauf hin, dass durch eine Sperrung des PCs der Ablauf der Praxis dadurch zu stark gestört und daher bewusst auf eine automatisierte Sperre des Accounts beim Verlassen des Arbeitsplatzes verzichtet würde.

8.1.3 Auswirkung bei Ausnutzung der Schwachstelle

Das Risiko ist abhängig von den Berechtigungen des angemeldeten Users. Da dies oft der einzig genutzte Account ist, sind umfassende Berechtigungen, z. B. für das Extrahieren, Manipulieren oder Löschen aller Daten, möglich. Mit administrativen Berechtigungen können auch tiefergehende Manipulationen auf Betriebssystemebene durchgeführt werden. Auch die Installation eines Remote Access Trojaners (RAT) ist möglich, um später in Ruhe und ohne das Risiko, entdeckt zu werden, den Angriff fortzuführen.

Potenzieller Schaden: Hoch

8.1.4 Angriffsvektor

Vorbedingungen: Unbeaufsichtigter PC mit angemeldetem User in einem für Externe zugänglichen Bereich

Angriffspfad: Unbeaufsichtigter Zugriff durch Patienten oder Dienstleister, z. B. während einer Wartezeit im Besprechungszimmer oder der Durchführung von Dienstleistungen (Reinigung, technische Maßnahmen etc.)

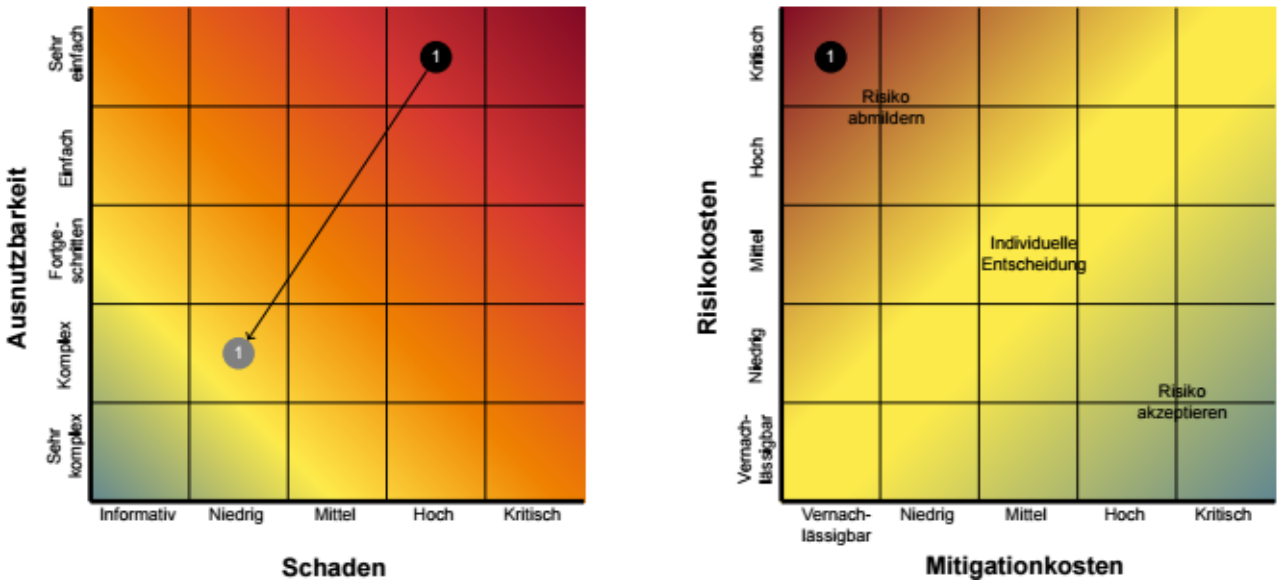
Wahrscheinlichster Angreifer: Zufälliger Angreifer

Angriffskomplexität: Sehr einfach

8.1.5 Mögliche abmildernde Maßnahmen

8.1.5.1 Sperren des PCs

Graphische Risikodarstellung



Beschreibung

PCs sollten immer gesperrt werden, wenn sie unbeaufsichtigt zurückgelassen werden, da sich unbefugte Personen potenziell Zugang zu den betroffenen PCs verschaffen könnten. Eine zu ergreifende Maßnahme besteht darin, automatische Bildschirmsperren einzurichten, die nach einer festzulegenden Zeit der Inaktivität ansprechen. Zudem sollten die Benutzer, wenn Sie den Arbeitsplatz verlassen, den PC sperren. Schließlich sollten regelmäßige Sicherheitsschulungen für das Personal durchgeführt werden, um das Bewusstsein für die Risiken und die Bedeutung der Datensicherheit zu erhöhen.

Verantwortliche, die diese Schwachstelle bewusst in Kauf nehmen, sollten auf die möglicherweise grobe Fahrlässigkeit dieser Entscheidung hingewiesen werden.

Siehe auch: SYS.2.1.A1 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

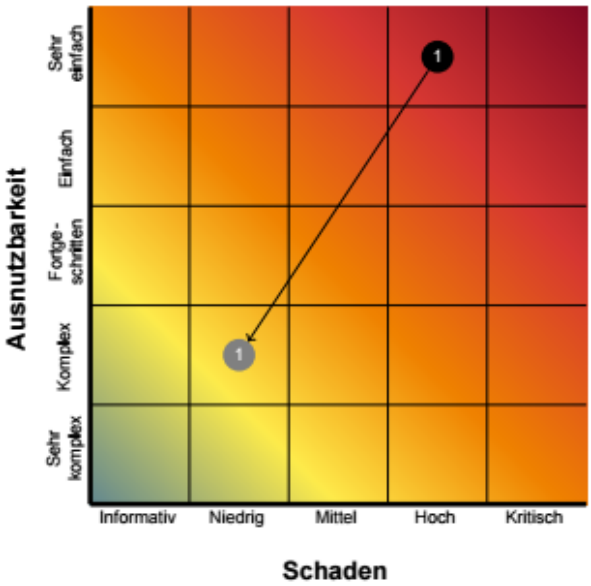
Für die Maßnahme selbst entstehen keine direkten Kosten (eventuell für Awareness-Maßnahmen). Es können jedoch Kosten für Maßnahmen entstehen, die die Anmeldung bzw. das Entsperren erleichtern, wie Smartcards oder biometrische Hardware.

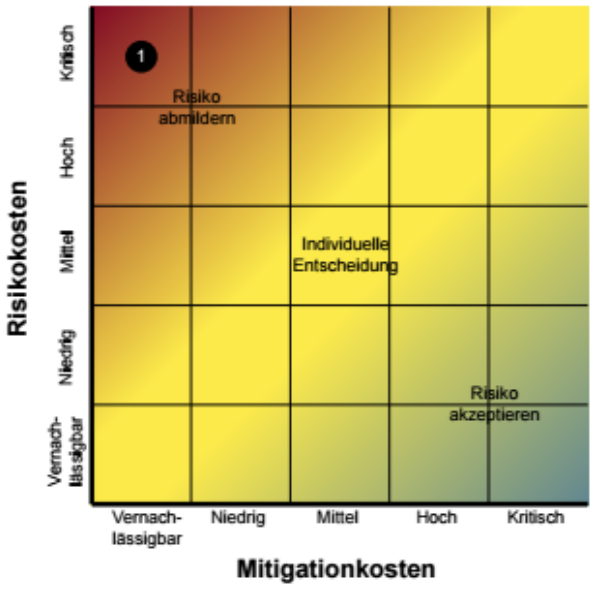
Verbleibendes Restrisiko

Das Restrisiko ist bei einem gesperrten PC gering.

8.1.5.2 Blockieren von ungenutzten USB-Ports

Graphische Risikodarstellung





Beschreibung

USB-Ports, die ungenutzt und im Zugriff fremder Personen sind, sollten deaktiviert bzw. gesperrt werden. Dadurch wird verhindert, dass Unbefugte USB-Geräte anschließen und in Schaden verursachender Weise verwenden können.

Kostenabschätzung

Für die Deaktivierung / Sperrung der Ports entstehen vernachlässigbare Kosten. Es können höhere Kosten für Software anfallen, falls an den Ports bestimmte Geräte freigeschaltet werden sollen während andere blockiert bleiben.

Verbleibendes Restrisiko

Das Restrisiko ist gering.

8.2 Sensible Daten auf externen Geräten

8.2.1 Beschreibung der Schwachstelle

Sensible Daten werden zur Arbeit im Home-Office auf externen Geräten gespeichert. Die Überführung auf diese geschieht über unverschlüsselte Speichermedien sowie VPNs (Virtual Private Network). Die Sicherheit von individuellen Geräten wie Privatgeräten ist hierbei nicht feststellbar und stellt daher ein hohes Risiko dar. Ebenso kann nicht ausgeschlossen werden, dass andere Personen im Haushalt dasselbe Gerät nutzen und somit ebenso Zugriff auf die Daten haben.

Siehe auch CWE-841 (The MITRE Corporation, 2023)

8.2.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 9 von 16 Arztpraxen mitgeteilt, dass sie VPN (Virtual Private Network) oder RDP-Verbindungen zum Netz der Praxis eingerichtet haben. Zwei der Arztpraxen laden Daten auf private Gerät, um sie zu bearbeiten. Eine Praxis benutzt für die Übertragung auf externe Geräte USB-Sticks. Somit besteht diese Schwachstelle in der Summe bei 12 von 16 Praxen (75 %).

8.2.3 Auswirkung bei Ausnutzung der Schwachstelle

Unsichere Systeme können eine Preisgabe von sensiblen Informationen an unberechtigte Personen zur Folge haben. Zudem besteht eine Gefährdung der Integrität der Daten sowie deren Verfügbarkeit.

Potenzieller Schaden: Hoch

8.2.4 Angriffsvektor

Vorbedingungen: Speicherung der Daten auf unsicherem Privatsystem

Angriffspfad:

- Fremdzugriff auf Privatsystem
- Verlust der Datenträger

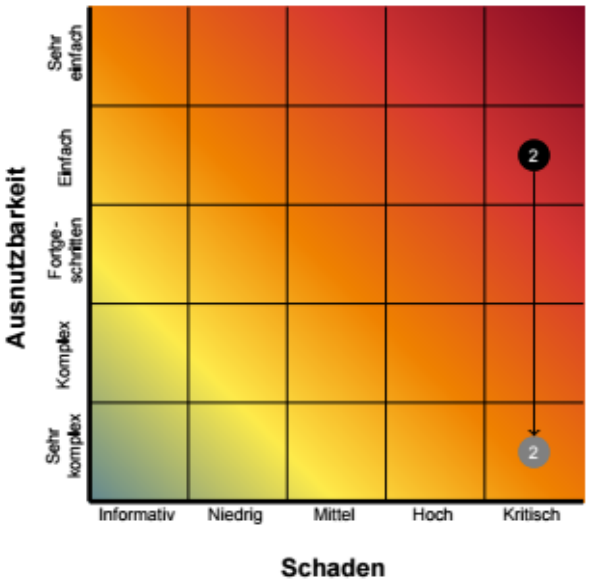
Wahrscheinlichster Angreifer: Zufälliger Angreifer

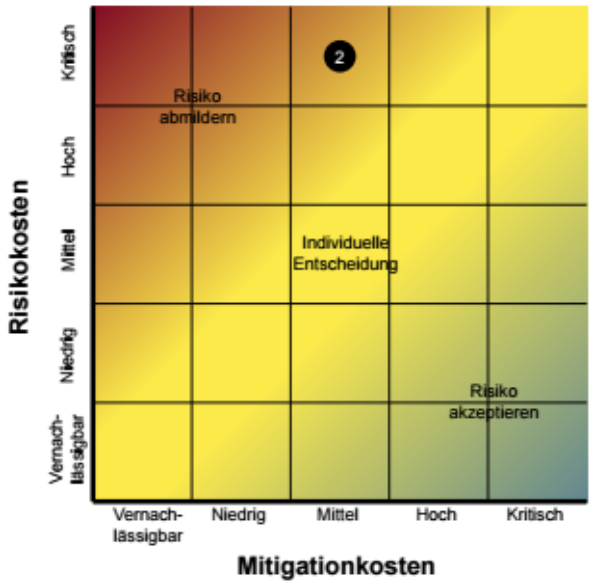
Angriffskomplexität: Sehr einfach

8.2.5 Mögliche abmildernde Maßnahmen

8.2.5.1 Verwendung von Mobile Device Management

Graphische Risikodarstellung





Beschreibung

Sensible Daten, wie Patientenakten oder ähnliche Dokumente sowie Geschäftsdokumente im Allgemeinen, sollten nur auf betrieblich verwalteten Systemen bearbeitet werden. Eine mögliche Lösung wäre die Einrichtung einer Mobile Device Management (MDM) Lösung, damit diese Geräte zentral verwaltet werden können.

Hierbei ist auch auf eine entsprechende Konfiguration und Sicherheit zu achten.
Es ist wichtig, eine strikte Richtlinie für das Home-Office zu implementieren, die das Speichern

sensibler Daten auf persönlichen, nicht verwalteten Geräten verbietet. Stattdessen sollte die Nutzung von verschlüsselten verwalteten Geräten und sicheren, durch das Unternehmen bereitgestellten VPNs zur Übertragung von Daten verpflichtend sein. Zudem sollten klare Regeln für die Nutzung und den Zugriff auf diese Geräte im häuslichen Umfeld festgelegt werden.

Siehe auch: INF.8.A1 ff. (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

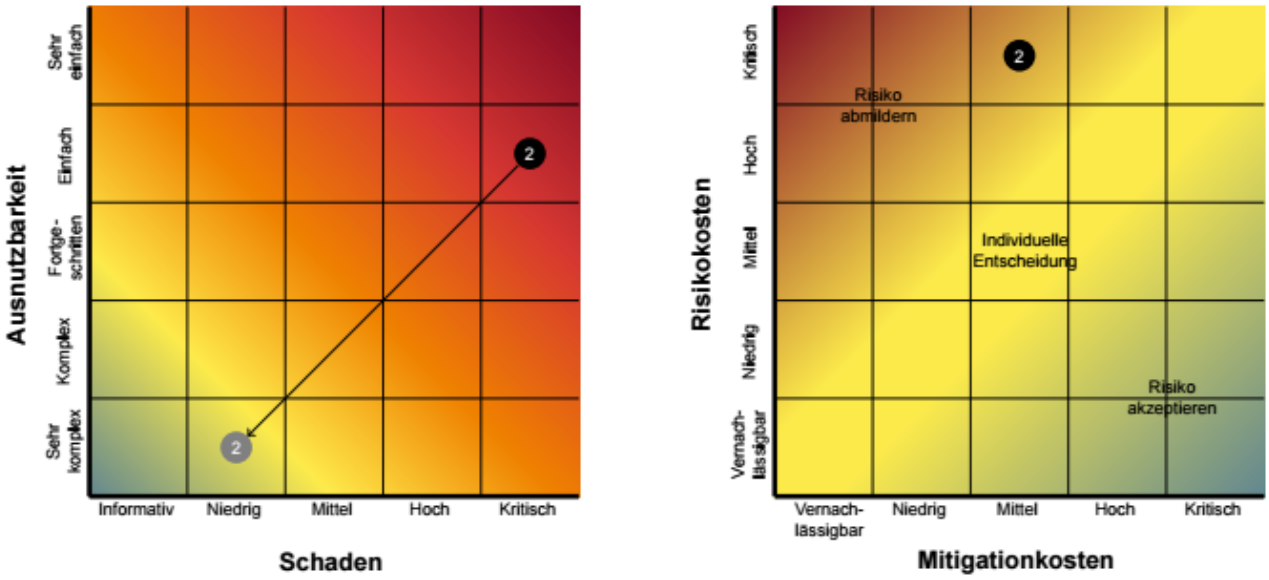
Es fallen mittlere bis hohe Kosten durch die Beschaffung und Einrichtung der MDM-Lösung an.

Verbleibendes Restrisiko

Das verbleibende Restrisiko ist gering.

8.2.5.2 Verwendung von DPI und SSL Inspection

Graphische Risikodarstellung



Beschreibung

Die Verwendung von Deep Packet Inspection (DPI) sowie SSL Inspection erhöht den Schutz im Netzwerk. Dabei werden nicht nur die Metadaten der Kommunikation analysiert, sondern auch die konkreten Inhalte. Ferner wird durch die SSL Inspection auch verschlüsselte Kommunikation, wie bei der Verbindung zu HTTPS-Seiten, betrachtet.

Dadurch kann bereits der Download von Schadcode verhindert werden.

Kostenabschätzung

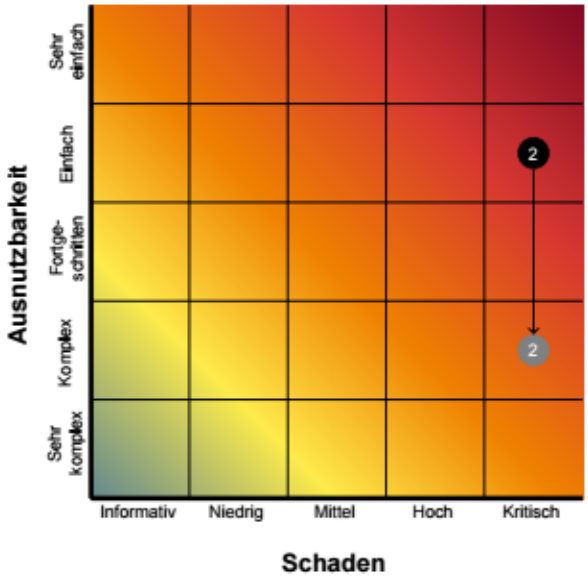
Es entstehen niedrige Kosten durch die Einrichtung sowie eventuell zusätzliche Kosten, sollten DPI und SSL Inspection durch die bestehenden Systeme nicht unterstützt werden.

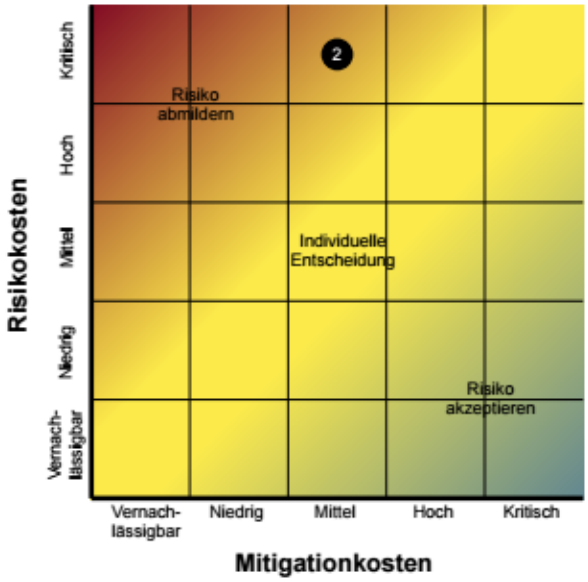
Verbleibendes Restrisiko

Das Restrisiko ist gering.

8.2.5.3 Awareness-Maßnahmen

Graphische Risikodarstellung





Beschreibung

Die Durchführung regelmäßiger Schulungen und Informationsveranstaltungen zur Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheitsthemen ist entscheidend. Diese sollten sich hier auf den Umgang mit sensiblen Daten konzentrieren.

Aber auch ein sicheres Online-Verhalten, der Umgang mit verdächtigen E-Mails und die Bedeutung von Sicherheitsprotokollen sollten beachtet werden.

Siehe auch: ORP.3.A6 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Es entstehen mittlere Kosten durch die Schulungen.

Verbleibendes Restrisiko

Das Restrisiko hängt vom Problembewusstsein der Mitarbeiter ab.

8.3 Unzureichende Betrachtung der DSGVO-Anforderungen

8.3.1 Beschreibung der Schwachstelle

Fehlendes Wissen und mangelnde Betreuung der Datenschutzthemen sowie fehlende Verträge zur Auftragsdatenverarbeitung mit Dienstleistern können zu DSGVO-Verstößen führen.

8.3.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 4 von 16 (25 %) Arztpraxen mitgeteilt, dass sie keine Rechtsgrundlage für die Erhebung bzw. Verarbeitung der Patientendaten kennen. In drei Praxen (18,75 %) gibt es niemanden, der für DSGVO-Themen verantwortlich ist.

8.3.3 Auswirkung bei Ausnutzung der Schwachstelle

Neben den Verstößen gegen die DSGVO, die zu empfindlichen Geldbußen führen können, sind auch notwendige Maßnahmen (TOMs) nicht als Anforderung dokumentiert und Bestandteil der Verträge und damit gegebenenfalls beim Dienstleister nicht umgesetzt.

Potenzieller Schaden: Hoch

8.3.4 Angriffsvektor

Vorbedingungen: Keine organisatorischen und vertraglichen Regelungen für die Umsetzung der DSGVO

Angriffspfad: Compliance-Verstoß / kein Angriff

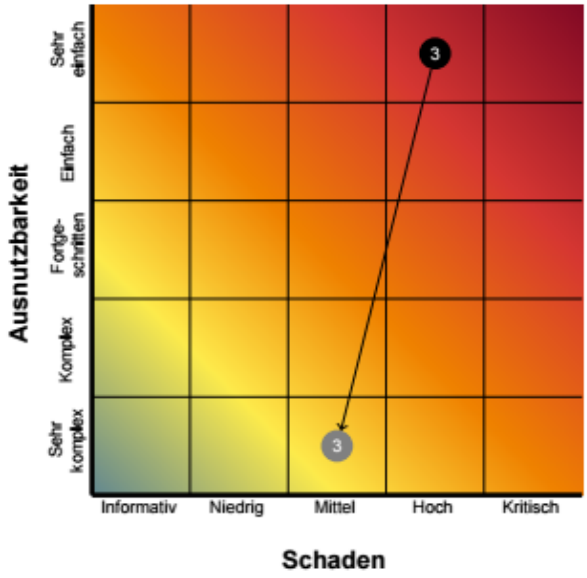
Wahrscheinlichster Angreifer: Nicht relevant

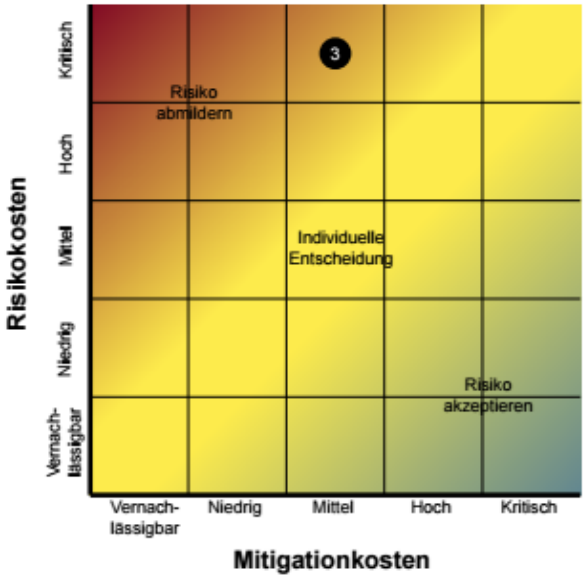
Angriffskomplexität: Nicht relevant

8.3.5 Mögliche abmildernde Maßnahmen

8.3.5.1 Beachtung und Einhaltung entsprechender gesetzlicher Vorgaben

Graphische Risikodarstellung





Beschreibung

> Datenschutzthemen müssen entweder selbst ausreichend betrachtet oder durch einen Dienstleister betreut und sichergestellt werden. Dennoch ist eine Schulung zu Datenschutzthemen und DSGVO-Vorschriften für alle Mitarbeiterinnen und Mitarbeiter unerlässlich.
> Zudem sollten alle Verträge mit Dienstleistern sorgfältig geprüft und entsprechende Klauseln zur Auftragsdatenverarbeitung aufgenommen werden, um die Einhaltung der DSGVO sicherzustellen.
>
> Siehe auch: CON.2.A1 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Es entstehen mittlere Kosten.

Verbleibendes Restrisiko

> Das verbleibende Restrisiko ist vernachlässigbar.

8.4 Fehlende Funktionstests der Backups

8.4.1 Beschreibung der Schwachstelle

Es besteht in allen Praxen eine Backupstrategie, jedoch wird die Wiederherstellbarkeit der erstellten Backups in den wenigsten Fällen tatsächlich geprüft.

8.4.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 12 von 16 Arztpraxen mitgeteilt, dass sie die Funktion ihrer Backups nicht oder nur in unregelmäßigen Zeitabständen testen. Das ergibt eine Quote von 75 %.

8.4.3 Auswirkung bei Ausnutzung der Schwachstelle

Sollte das Wiederherstellen von Daten aus einem zuvor erstellen Backup notwendig werden, besteht die Gefahr, dass das Backup nicht funktionstüchtig ist.

Potenzieller Schaden: Kritisch

8.4.4 Angriffsvektor

Vorbedingungen: Wiederherstellung aus Backup erforderlich

Angriffspfad: Keiner

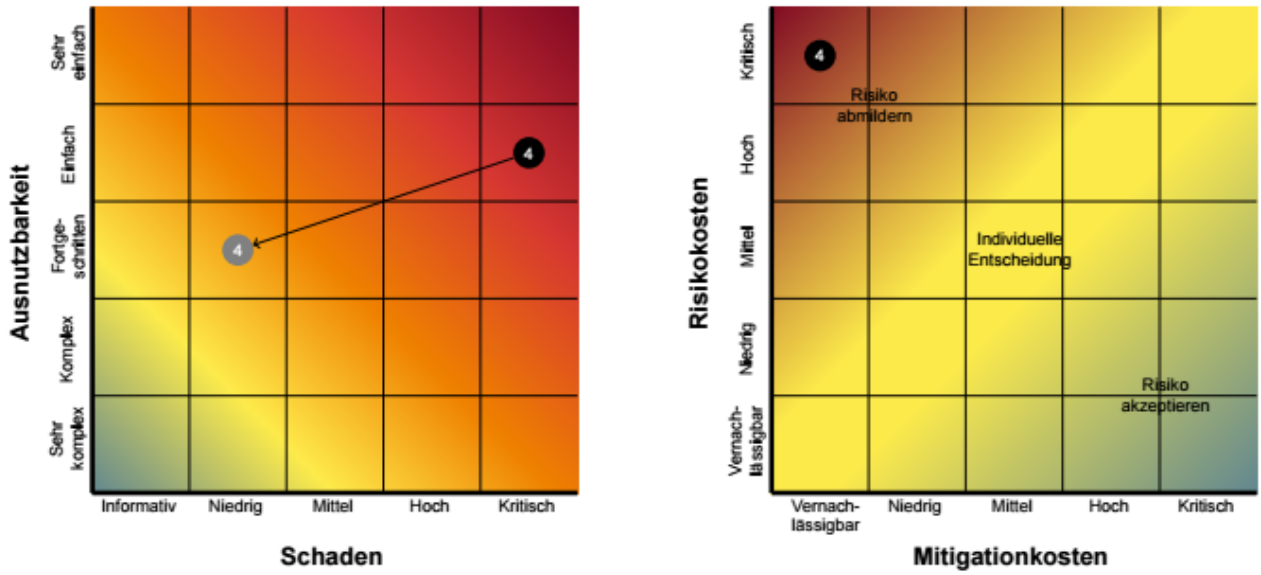
Wahrscheinlichster Angreifer: Trifft nicht zu.

Angriffskomplexität: Einfach

8.4.5 Mögliche abmildernde Maßnahmen

8.4.5.1 Funktionstests der Backups

Graphische Risikodarstellung



Beschreibung

Es sollten regelmäßig Funktionstests der erstellten Backups durchgeführt werden, um sicherzustellen, dass diese im Wiederherstellungsfall einsatzfähig sind.

Siehe auch: CON.3.A15 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Backup-Funktionstests verursachen in der Regel einen sehr geringen Kostenaufwand.

Verbleibendes Restrisiko

Das Restrisiko ist gering.

8.5 Unzureichende Awareness-Schulungen

8.5.1 Beschreibung der Schwachstelle

Unzureichende Awareness kann zu fehlerhafter Bedienung der IT-Systeme führen. Dazu gehören das wahllose Laden von und Navigieren in Internetseiten unbekannten Ursprungs und das sorglose Anklicken von Links oder Öffnen von Anhängen in E-Mails ungeprüfter Herkunft. Aber auch E-Mails von bekannten Absendern können schadhaft sein, beispielsweise wenn der Account des Absenders kompromittiert wurde. Daher sollte immer geprüft werden, ob die E-Mail erwartet wurde, Anhänge nötig sind und bei Links, ob die URL zum Absender passt.

8.5.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 12 von 16 Arztpraxen mitgeteilt, dass sie keine oder nur unregelmäßige (Awareness-)Schulungen für ihre Mitarbeiterinnen und Mitarbeiter angeboten haben. Das sind 75 % aller Arztpraxen.

8.5.3 Auswirkung bei Ausnutzung der Schwachstelle

Durch das Öffnen von Webseiten oder das Ausführen heruntergeladener bzw. per E-Mail empfangener Dateien kann es zu einer Kompromittierung der IT-Systeme kommen.

Potenzieller Schaden: Hoch

8.5.4 Angriffsvektor

Vorbedingungen: Fehlende Awareness

Angriffspfad:

- Phishing-E-Mail
- Manipulierte Website

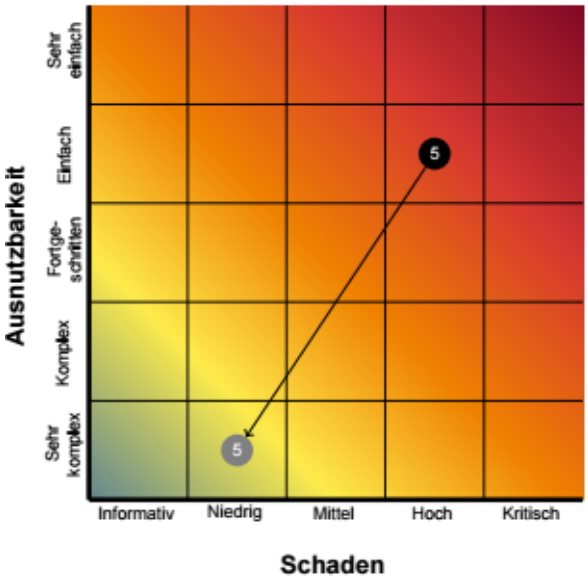
Wahrscheinlichster Angreifer: Kriminelle Organisationen

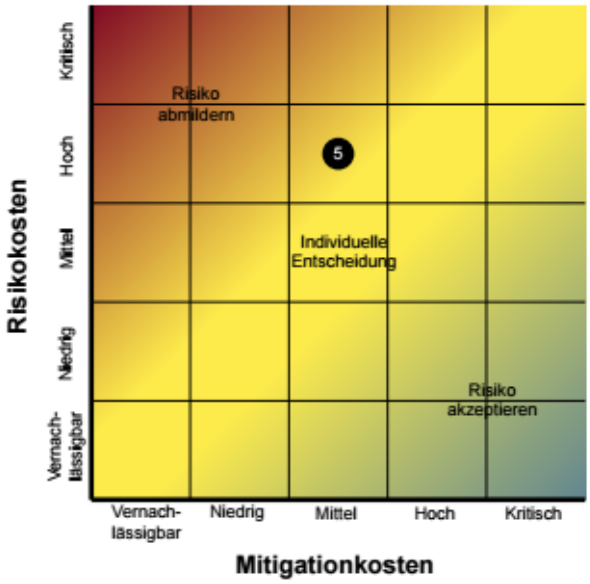
Angriffskomplexität: Einfach

8.5.5 Mögliche abmildernde Maßnahmen

8.5.5.1 Awareness-Schulungen für die Mitarbeiter

Graphische Risikodarstellung





Beschreibung

Die Durchführung regelmäßiger Schulungen und Informationsveranstaltungen zur Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheitsthemen ist entscheidend. Diese sollten sich auf sicheres Online-Verhalten, den Umgang mit verdächtigen E-Mails und die Bedeutung von Sicherheitsprotokollen konzentrieren.

Siehe auch: ORP.3.A6 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

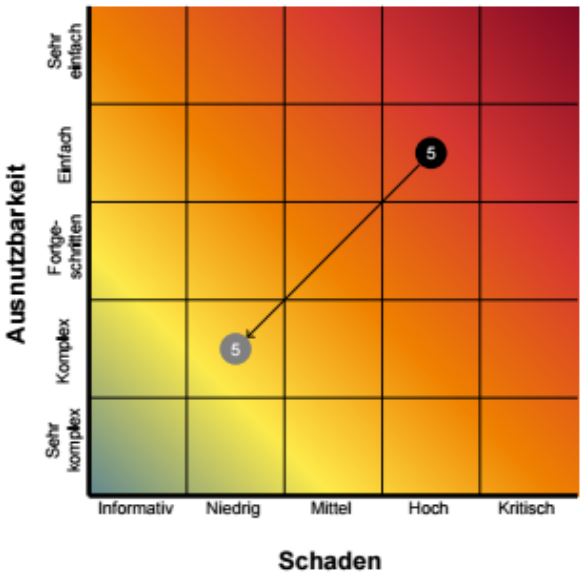
Es entstehen mittlere Kosten durch die Schulungen.

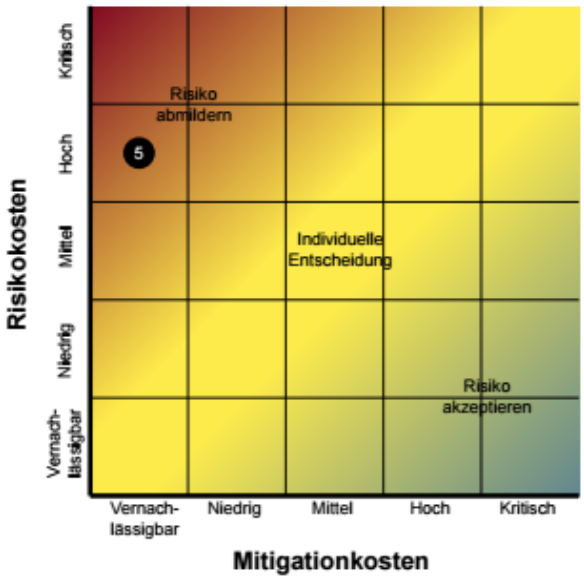
Verbleibendes Restrisiko

Das Restrisiko hängt vom Problembewusstsein der Mitarbeiterinnen und Mitarbeiter ab. Bei Mitarbeiterinnen und Mitarbeitern mit einem ausgeprägten und durch regelmäßige Awareness-Schulungen aufgefrischten Problembewusstsein ist das verbleibende Restrisiko niedrig. Ansonsten müssten weiterführende Maßnahmen wie z. B. entsprechende Dienstanweisungen in Erwägung gezogen werden.

8.5.5.2 Einschränken der Benutzerrechte

Graphische Risikodarstellung





Beschreibung

Die Vergabe der Rechte eines Accounts nach dem Least-Privilege-Prinzip (PoLP) reduziert die Auswirkungen eines erfolgreichen Angriffs oder erschwert diesen zumindest.

Siehe auch: ORP.4.A7 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

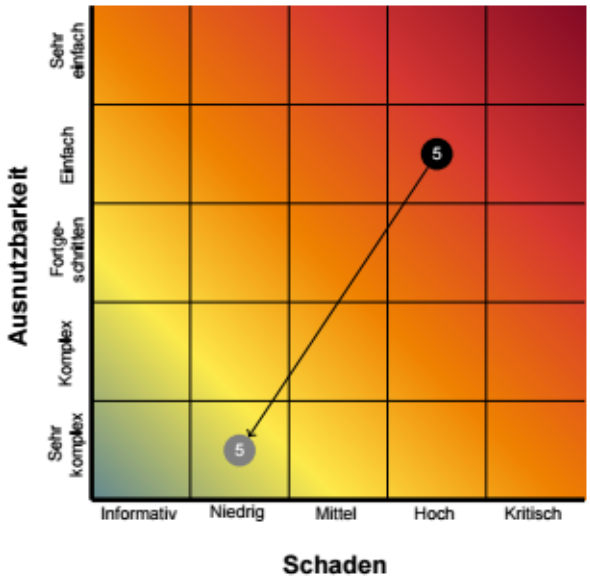
Es entstehen hauptsächlich Kosten durch den Verwaltungsaufwand für die persönlichen Konten.

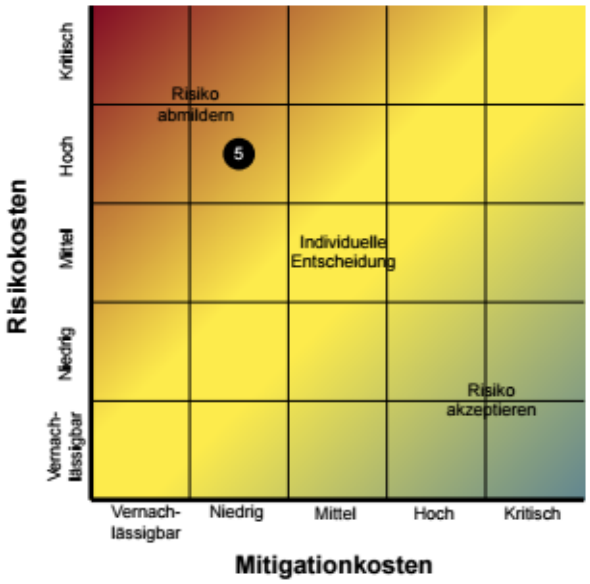
Verbleibendes Restrisiko

Es verbleibt ein geringes Restrisiko, abhängig von den tatsächlichen Berechtigungen.

8.5.5.3 Verwenden von Deep Packet Inspection

Graphische Risikodarstellung





Beschreibung

Die Verwendung von Deep Packet Inspection (DPI) erhöht den Schutz im Netzwerk. Dabei werden nicht nur die Metadaten der Kommunikation analysiert, sondern auch die konkreten Inhalte.

Siehe auch: NET.3.2.A22 ff. (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Es entstehen niedrige Kosten durch die Einrichtung und das Testen sowie evtl. zusätzliche Kosten, sollte DPI durch die bestehenden Systeme nicht unterstützt werden.

Verbleibendes Restrisiko

Das Restrisiko ist gering.

8.6 Unsichere Entsorgung von IT-Geräten

8.6.1 Beschreibung der Schwachstelle

Auf Datenträgern von Altgeräten befinden sich mitunter noch vertrauliche Informationen wie Patientendaten, Finanzdaten oder Kennwörter. Diese können insbesondere nach einfachen Löschvorgängen wiederhergestellt und missbraucht werden.

Siehe auch CWE-212 (The MITRE Corporation, 2023)

8.6.2 Herkunft / Nachweise

Es wurden keine konkreten Fragen nach der Entsorgung von Altgeräten gestellt, auf einem Fragebogen wurde jedoch als Kommentar mitgeteilt, dass kein Prozess zur Entsorgung vorhanden ist.

8.6.3 Auswirkung bei Ausnutzung der Schwachstelle

Werden vermeintlich gelöschte Patientendaten oder vertrauliche Interna der Praxis auf einem Altgerät wiederhergestellt, kommen verschiedene Möglichkeiten der Ausnutzung in Betracht:

- Diskreditierung der Praxis oder Patienten
- Erpressung der Praxis oder Patienten
- Erleichterung eines Angriffs auf Accounts oder Geräte der Praxis

Potenzieller Schaden: Hoch

8.6.4 Angriffsvektor

Vorbedingungen: Eine Angreiferin oder ein Angreifer erhält Zugriff auf Datenträger, die unverschlüsselt und unzureichend gelöscht sind. Die Bandbreite der Möglichkeiten ist hier groß, in Betracht kommt zum Beispiel der unabsichtliche Erwerb über Internet-Auktionen oder auch das Abgreifen der Hardware während des Entsorgungsprozesses.

Angriffspfad: Erwerb oder Diebstahl von Altgeräten oder Datenträgern

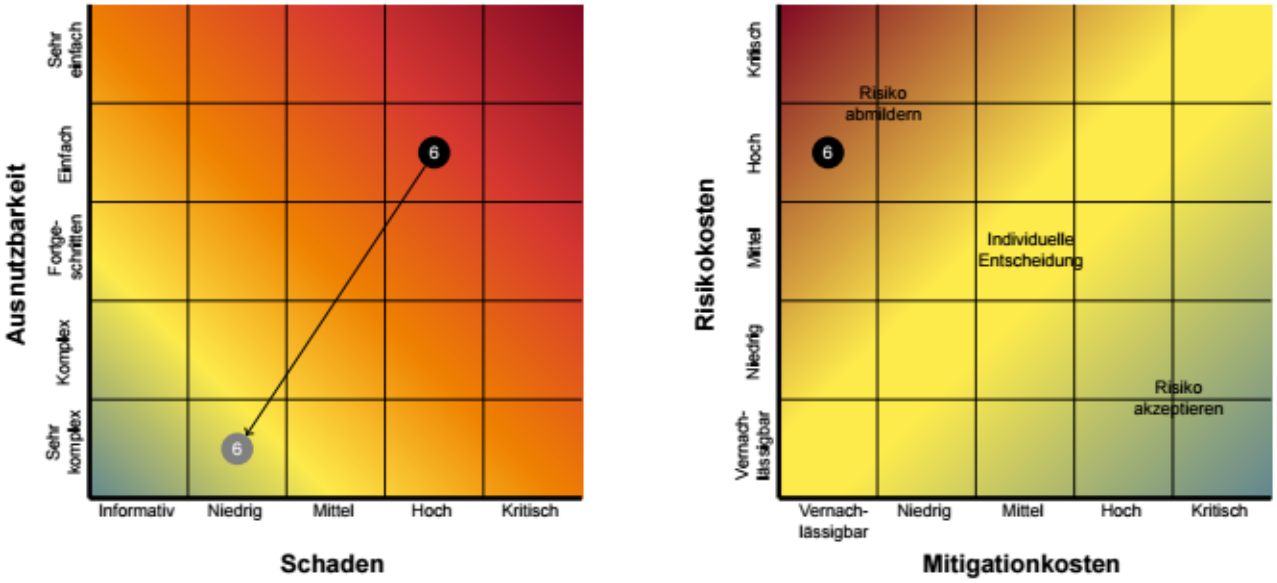
Wahrscheinlichster Angreifer: Zufälliger Angreifer

Angriffskomplexität: Einfach

8.6.5 Mögliche abmildernde Maßnahmen

8.6.5.1 Nutzung zertifizierter Datenlöschverfahren

Graphische Risikodarstellung



Beschreibung

Um dieses Risiko zu minimieren, sollten alle Datenträger vor dem Ausmustern eines Altgeräts mittels zertifizierter Datenlöschverfahren vollständig und unwiederbringlich gelöscht werden. Zusätzlich ist es sinnvoll, die physische Vernichtung von Datenträgern in Betracht zu ziehen, um einen zusätzlichen Schutz gegen Datenmissbrauch zu bieten. Eventuell ist die Einbindung eines externen Dienstleisters sinnvoll.

Siehe auch: CON.6.A2 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

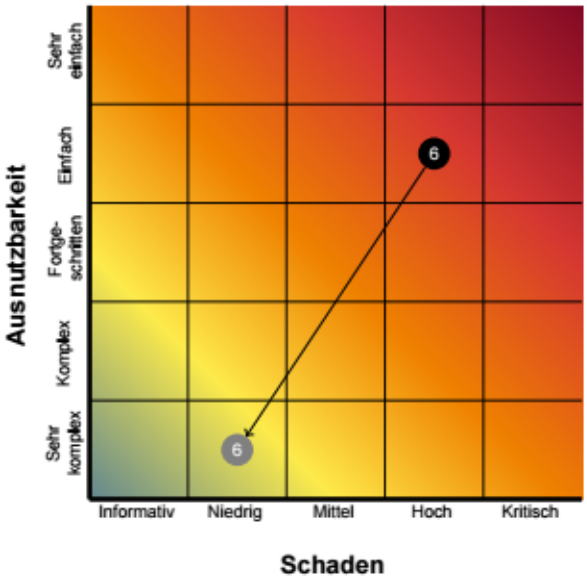
Es entstehen geringe Kosten durch die Beauftragung.

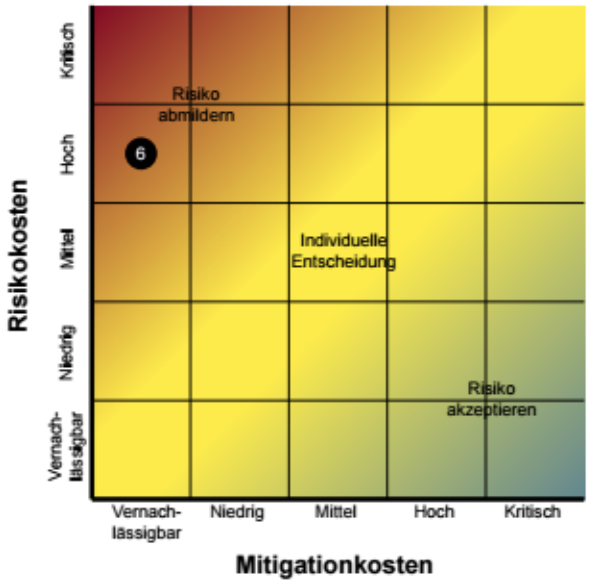
Verbleibendes Restrisiko

Das Restrisiko ist vernachlässigbar.

8.6.5.2 Verschlüsselung aller Datenträger

Graphische Risikodarstellung





Beschreibung

> Um die Sicherheit von Daten zu gewährleisten, sollte eine vollständige Festplattenverschlüsselung (Full Disk Encryption) auf allen IT-Systemen implementiert werden. Dies schützt die Daten auch bei der Entsorgung.
>
> Siehe auch: CON.1.A1 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Da inzwischen nahezu alle Systeme Datenträgerverschlüsselung unterstützen, sollten die Kosten vernachlässigbar sein.

Verbleibendes Restrisiko

> Bei unzureichenden Verschlüsselungsverfahren bleibt das Risiko, dass Daten zwar nicht sofort, aber in der Zukunft entschlüsselt werden können.

8.7 Unzureichender Virenschutz

8.7.1 Beschreibung der Schwachstelle

Es existiert kein ausreichender Virenschutz. Dieser ist jedoch unerlässlich, wenn IT-Systeme Zugriff auf Internet-Ressourcen haben oder das Einlesen fremder Datenträger gestatten.

Siehe auch CWE-358 (The MITRE Corporation, 2023)

8.7.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 9 von 16 Arztpraxen mitgeteilt, dass sie keine zentral verwaltete Antivirensoftware für ihre Geräte einsetzen, zwei weitere haben dies nicht vollständig umgesetzt. 12 Arztpraxen teilten mit, dass sie keine Standard-Antivirensoftware nutzen. Insgesamt haben fünf Praxen und damit 31,25 % der Teilnehmer angegeben, keinen Virenschutz einzusetzen.

8.7.3 Auswirkung bei Ausnutzung der Schwachstelle

Bei einem unzureichenden Schutz vor Viren besteht das Risiko, dass Viren und Malware nicht erkannt werden und sich frei im Praxisnetzwerk verteilen. Die hieraus resultierenden Folgen können vielfältig sein

und reichen von Verschlüsselung der Daten durch Ransomware über Manipulationen oder Extraktionen von Daten bis hin zur Integration der Praxissysteme in ein Botnetz.

Potenzieller Schaden: Hoch

8.7.4 Angriffsvektor

Vorbedingungen: Virenschutz nicht vorhanden oder nicht aktuell

Angriffspfad:

- Social Engineering über E-Mails mit Anhängen oder Links
- Infektion über infizierte Geräte z. B. USB

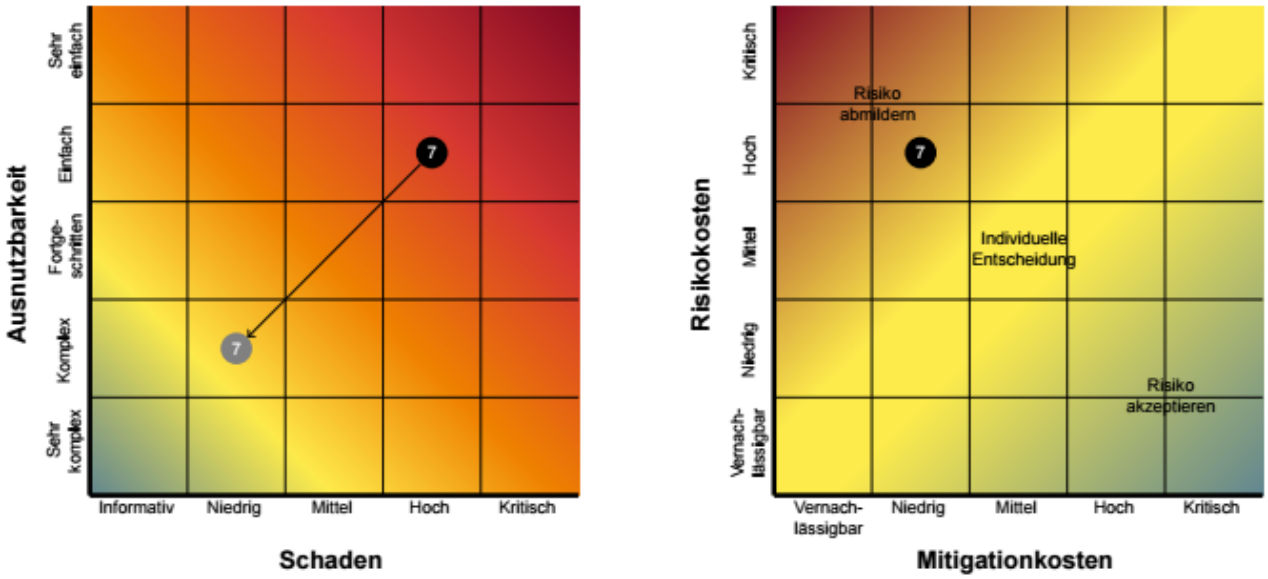
Wahrscheinlichster Angreifer: Kriminelle Organisationen

Angriffskomplexität: Einfach

8.7.5 Mögliche abmildernde Maßnahmen

8.7.5.1 Einsatz einer verwalteten Virenschutzlösung

Graphische Risikodarstellung



Beschreibung

Um einen ausreichenden Schutz vor Viren und Malware zu erlangen, sollte eine verwaltete Virenschutzlösung implementiert werden. Diese bietet eine kontinuierliche Überwachung der Systeme und gewährleistet eine Aktualität der Definitionsdateien. Dabei sollte die Lösung ebenfalls eine heuristische Analyse unterstützen, um auch neue oder modifizierte Schadsoftware erkennen zu können.

Siehe auch: OPS.1.1.4.A5 ff. (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Die Kosten für eine Virenschutzlösung sind niedrig bis mittel, abhängig von der Anzahl und Art der Geräte.

Verbleibendes Restrisiko

Es verbleibt ein geringes Risiko, dass neue oder verschlüsselte Viren nicht erkannt werden.

8.8 Unzureichende Verschlüsselung

8.8.1 Beschreibung der Schwachstelle

Datenträger in den IT-Systemen sind nicht verschlüsselt.

Siehe auch CWE-311 (The MITRE Corporation, 2023)

8.8.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen alle Arztpraxen mitgeteilt, dass sie keine Festplattenverschlüsselung umgesetzt haben.

8.8.3 Auswirkung bei Ausnutzung der Schwachstelle

Gelangt eine Angreiferin oder ein Angreifer an unverschlüsselte Datenträger, kann er diese gänzlich nutzen. Dabei gibt es verschiedene Möglichkeiten:

- Diskreditierung der Praxis oder Patienten
- Erpressung der Praxis oder Patienten
- Erleichterung eines Angriffs auf Accounts oder Geräte der Praxis

Potenzieller Schaden: Hoch

8.8.4 Angriffsvektor

Vorbedingungen: Angreifer erlangt Zugriff auf unverschlüsselte Datenträger.

Angriffspfad: Lesen oder Ändern von Daten

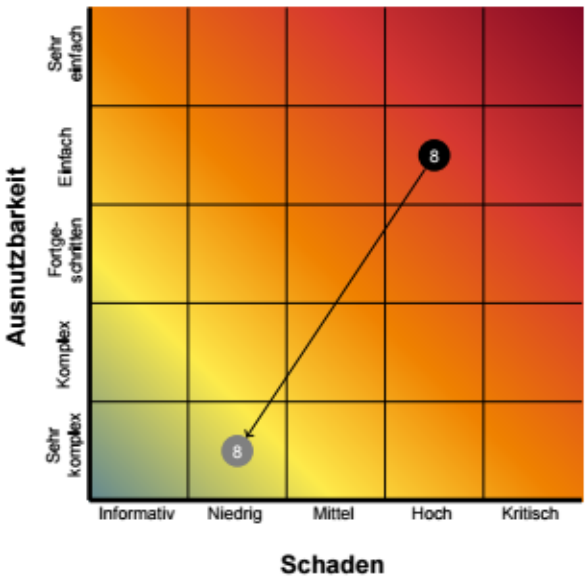
Wahrscheinlichster Angreifer: Gezielter Angreifer

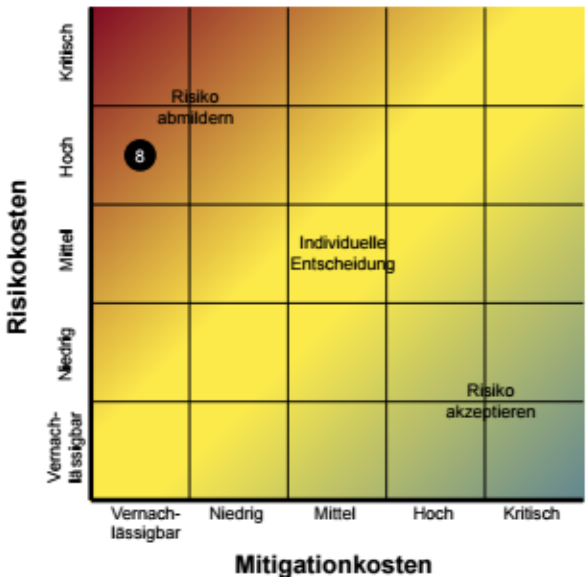
Angriffskomplexität: Einfach

8.8.5 Mögliche abmildernde Maßnahmen

8.8.5.1 Verschlüsselung

Graphische Risikodarstellung





Beschreibung

Um die Sicherheit von Daten zu gewährleisten, sollte eine vollständige Festplattenverschlüsselung (Full Disk Encryption) auf allen IT-Systemen implementiert werden. Dies schützt die Daten, selbst wenn der physische Datenträger gestohlen oder kompromittiert wird.
Dies gilt insbesondere für sensible Daten. Ein Mindestschutz sollte die hardwarenahe Festplattenverschlüsselung sein, sehr kritische Daten sollten gegebenenfalls noch auf Datenbank- oder Anwendungs-Ebene verschlüsselt werden.

Die Verschlüsselung der Festplatten kann z. B. über eine AD-Gruppenrichtlinie zentral gesteuert werden.

Siehe auch: CON.1.A1 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Die Kosten sind vernachlässigbar, falls eine hardwarenahe Verschlüsselung ausreichend ist.

Verbleibendes Restrisiko

Bei unzureichenden Verschlüsselungsverfahren bleibt zudem ein Risiko, dass Daten zwar nicht sofort, aber in der Zukunft entschlüsselt werden können.

8.9 Unverschlüsselte Backups

8.9.1 Beschreibung der Schwachstelle

Werden Backups nicht verschlüsselt, können die darin enthaltenen Daten Unbefugten in die Hände fallen. Das gilt insbesondere dann, wenn die Backups in diesem Zustand transportiert und extern gelagert werden.

Siehe auch CWE-311 (The MITRE Corporation, 2023)

8.9.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 2 von 16 und damit 12,5 % der Arztpraxen mitgeteilt, dass Backups unverschlüsselt gelagert werden. Zusätzlich gaben beide Praxen an, dass diese Backups mitgenommen und extern gelagert werden.

8.9.3 Auswirkung bei Ausnutzung der Schwachstelle

Gelangt eine unbefugte Person an unverschlüsselte Daten, kann er diese sofort nutzen. Dabei gibt es verschiedene Möglichkeiten:

- Diskreditierung der Praxis oder Patienten
- Erpressung der Praxis oder Patienten
- Erleichterung eines Angriffs auf Accounts oder Geräte der Praxis

Potenzieller Schaden: Hoch

8.9.4 Angriffsvektor

Vorbedingungen: Verlust oder Diebstahl unverschlüsselter Backup-Dateien

Angriffspfad: Zugriff auf die extern gelagerten Backups

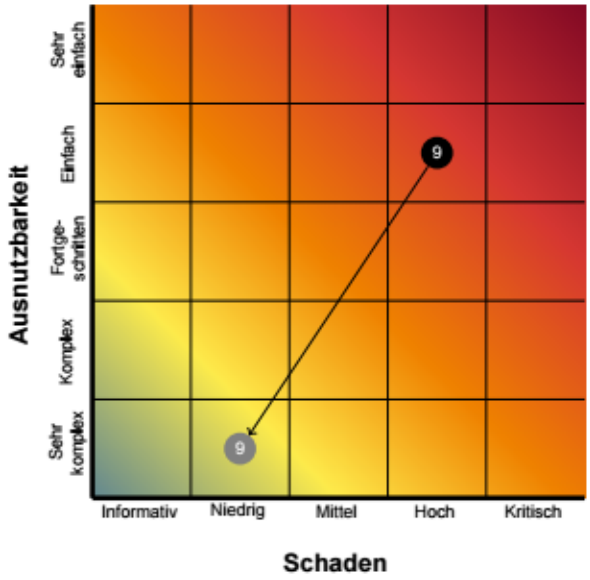
Wahrscheinlichster Angreifer: Zufälliger Angreifer

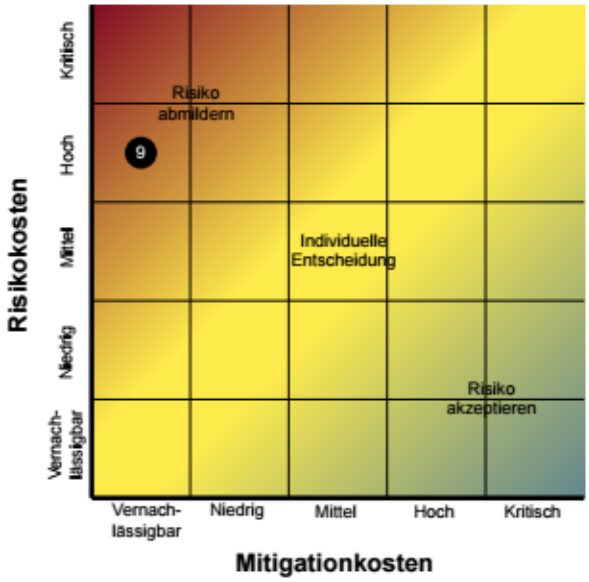
Angriffskomplexität: Einfach

8.9.5 Mögliche abmildernde Maßnahmen

8.9.5.1 Verschlüsselung – Backup oder Datenträger

Graphische Risikodarstellung





Beschreibung

> Alle Daten sollten verschlüsselt werden, insbesondere sensible Daten und Backups. Dies hat gerade beim Transport von Daten höchste Priorität.
>
> Siehe auch: CON.3.A13 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Die Kosten sind vernachlässigbar.

Verbleibendes Restrisiko

> Es bleibt ein geringes Restrisiko, dass die Daten – abhängig vom verwendeten Verschlüsselungsalgorithmus und -verfahren – entschlüsselt werden können.

8.10 Ungesicherte Netzwerkdosen unbemerkt zugänglich

8.10.1 Beschreibung der Schwachstelle

Wenn eine Angreiferin oder ein Angreifer Zugriff auf eine ungesicherte Netzwerkdose erlangt, ist ein erfolgreicher Angriff sehr wahrscheinlich.

Siehe auch CWE-284 (The MITRE Corporation, 2023)

8.10.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 6 von 16 Arztpraxen mitgeteilt, dass sie offene oder nicht besonders geschützte Netzwerkdosen in ihrer Praxis haben. Diese Schwachstelle besteht daher bei 37,5 % der Praxen.

8.10.3 Auswirkung bei Ausnutzung der Schwachstelle

Kann eine Angreiferin oder ein Angreifer direkt auf das Netzwerk zugreifen, hat er eine Vielzahl von Möglichkeiten, die Geräte in diesem Netzwerk anzugreifen. Er oder sie kann sowohl bestehende

Schwachstellen der IT-Systeme ausnutzen als auch den Traffic in diesem Netzwerk mitlesen und manipulieren.

Potenzieller Schaden: Hoch

8.10.4 Angriffsvektor

Vorbedingungen: Zugriff auf eine ungeschützte Netzwerkdose

Angriffspfad: Anschluss eines Netzwerkgeräts – Scan der Netzwerkumgebung – Suche nach offenen Ports, Schwachstellen – Exploitation der Schwachstellen

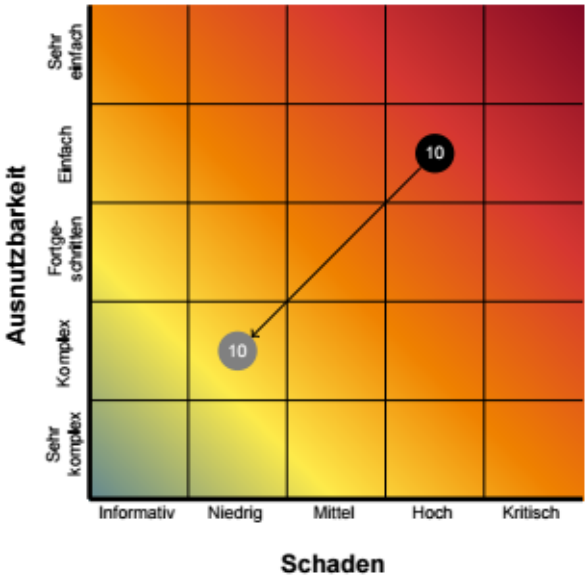
Wahrscheinlichster Angreifer: Gezielte Angreifer

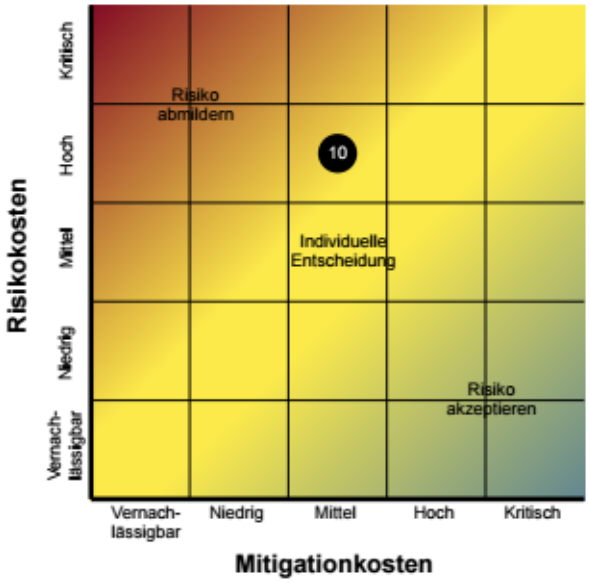
Angriffskomplexität: Einfach

8.10.5 Mögliche abmildernde Maßnahmen

8.10.5.1 Netzwerkdosen schützen

Graphische Risikodarstellung





Beschreibung

Alle Netzwerkdosen sollten physisch und technisch vor unbefugtem Zugriff geschützt sein, z. B. durch Network-Access-Kontrolle.

Siehe auch: NET.3.4.A2 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

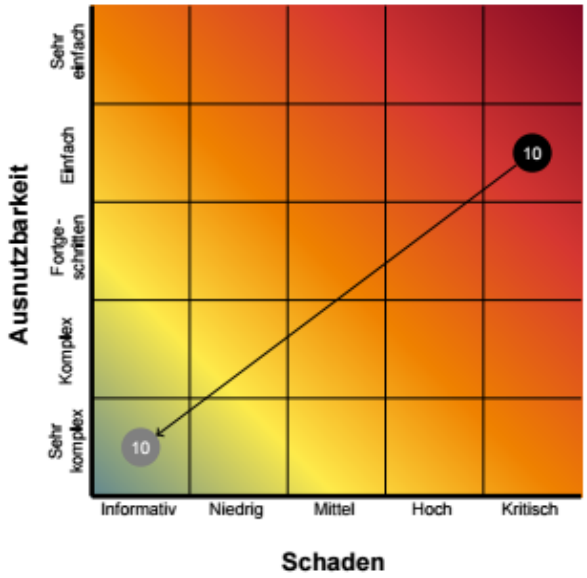
Sollte die eingesetzte Netzwerk-Hardware Schutzmechanismen nicht unterstützen, entstehen mittlere Kosten.

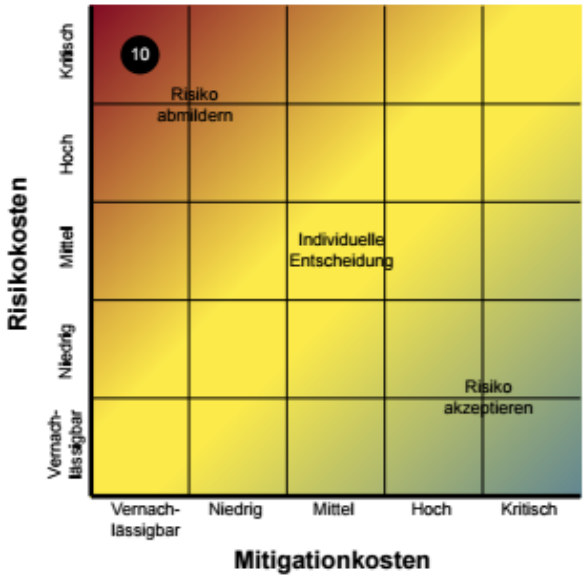
Verbleibendes Restrisiko

Es verbleibt ein niedriges Risiko.

8.10.5.2 Ungenutzte Netzwerkdosen stilllegen

Graphische Risikodarstellung





Beschreibung

Ungenutzte Dosen sollten stillgelegt werden.

Kostenabschätzung

Es entstehen geringe Kosten.

Verbleibendes Restrisiko

Stillgelegte Dosen bieten keine Angriffsfläche, daher geht von ihnen kein Risiko aus.

8.11 Verwendung fremder Datenträger

8.11.1 Beschreibung der Schwachstelle

Über ein fremdes Medium können Viren und Malware eingeschleust werden.

8.11.2 Herkunft / Nachweise

In den Fragebögen gaben 7 von 16 Praxen, also 43,75 % an, Datenträger wie CDs, DVDs oder auch USB-Sticks einzulesen.

8.11.3 Auswirkung bei Ausnutzung der Schwachstelle

Bei der Infektion eines Systems durch Datenträger können sowohl Daten manipuliert, exfiltriert sowie verschlüsselt oder direkt vernichtet werden. Darüber hinaus ist nach einer erfolgreichen Kompromittierung auch die Ausweitung auf andere Systeme möglich.

Potenzieller Schaden: Hoch

8.11.4 Angriffsvektor

Vorbedingungen: Nutzen fremder, infizierter Datenträger

Angriffspfad: Offenes Laufwerk oder offener Port

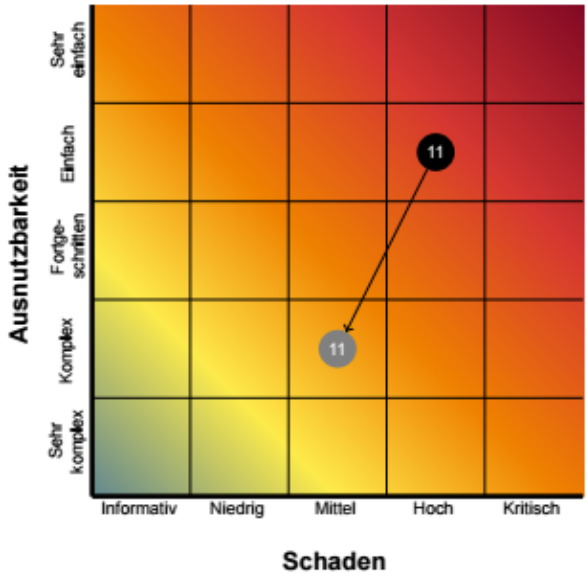
Wahrscheinlichster Angreifer: Gezielte Angreifer

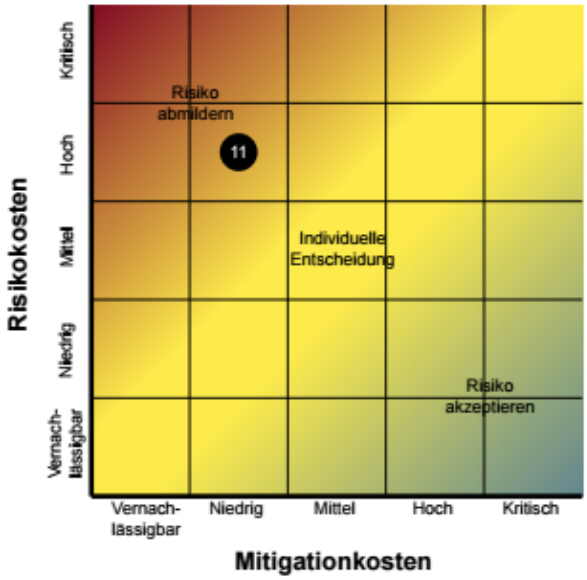
Angriffskomplexität: Einfach

8.11.5 Mögliche abmildernde Maßnahmen

8.11.5.1 Nur Datenträger von vertrauenswürdigen Quellen nutzen

Graphische Risikodarstellung





Beschreibung

Nur Datenträger, die direkt von anderen Praxen kommen, sollten eingelesen werden.

Siehe auch: SYS.4.5.A4 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

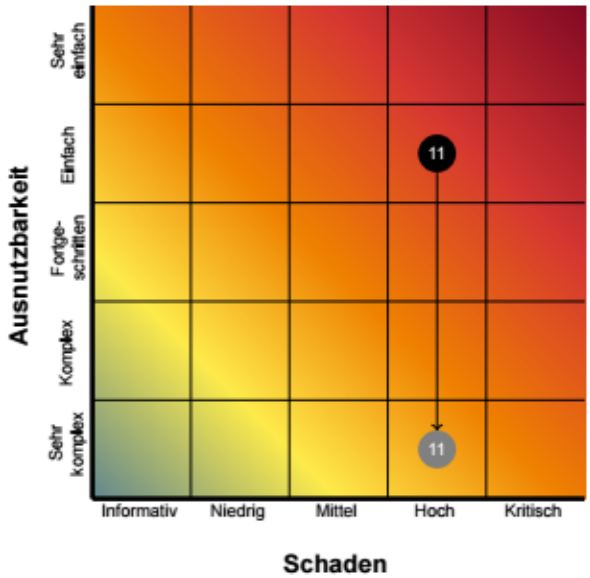
Es entstehen geringe Kosten.

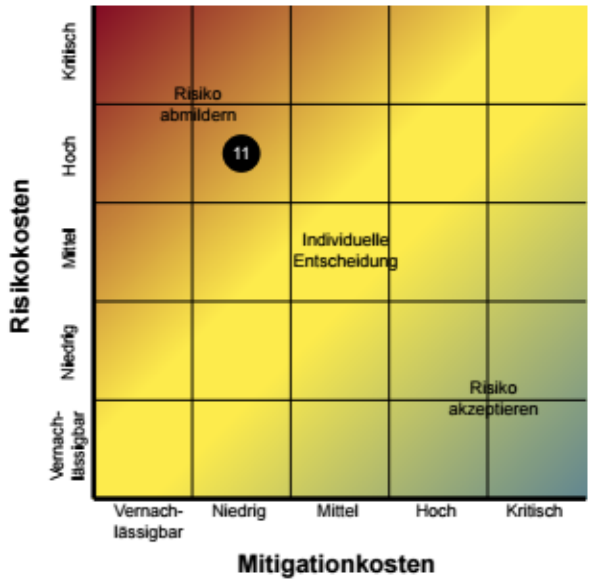
Verbleibendes Restrisiko

Es bleibt ein geringes Restrisiko.

8.11.5.2 Datenträger vor der Nutzung scannen

Graphische Risikodarstellung





Beschreibung

Datenträger sollten vor der Nutzung erst an einem unabhängigen, isolierten Gerät auf Schadsoftware gescannt werden.

Siehe auch: SYS.4.5.A12 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Es entstehen evtl. geringe Kosten durch die Beschaffung und Einrichtung eines dedizierten Computers zum Scannen.

Verbleibendes Restrisiko

Es bleibt ein geringes Restrisiko.

8.12 Unzureichendes Berechtigungsmanagement

8.12.1 Beschreibung der Schwachstelle

Es existiert kein Berechtigungs- oder Rollenkonzept, das die spezifischen Berechtigungen für Gruppen oder Individuen definiert. Jeder Benutzer verfügt über dieselben, meist sehr umfangreichen Berechtigungen, die in den meisten Fällen, über die zur Erledigung der betrieblichen Aufgaben benötigten Berechtigungen hinaus gehen.

Siehe auch CWE-732 (The MITRE Corporation, 2023)

8.12.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 5 von 16 Arztpraxen mitgeteilt, dass den Mitarbeitenden keine gesonderten Rollen zugewiesen werden. Damit haben in 31,25 % der Fälle User bzw. Accounts mehr Rechte als benötigt.

8.12.3 Auswirkung bei Ausnutzung der Schwachstelle

Ein fehlendes oder mangelndes Berechtigungsmanagement hat zur Folge, dass jedes Benutzerkonto über dasselbe Potenzial, Schaden zu verursachen, verfügt. Eine Kompromittierung hätte somit immer die höchstmögliche Auswirkung auf das Gesamtsystem, unabhängig davon, welches Benutzerkonto betroffen ist.
Die Vergabe von nicht benötigten Berechtigungen an Personen mit unzureichendem technischem Fachwissen kann außerdem zu unbeabsichtigten Aktionen mit nachhaltiger Wirkung auf Daten oder Systeme führen.

Potenzieller Schaden: Mittel

8.12.4 Angriffsvektor

Vorbedingungen: Zugriff auf ein Benutzerkonto

Angriffspfad: Ausnutzung der nicht benötigten Privilegien für unautorisierte Aktionen

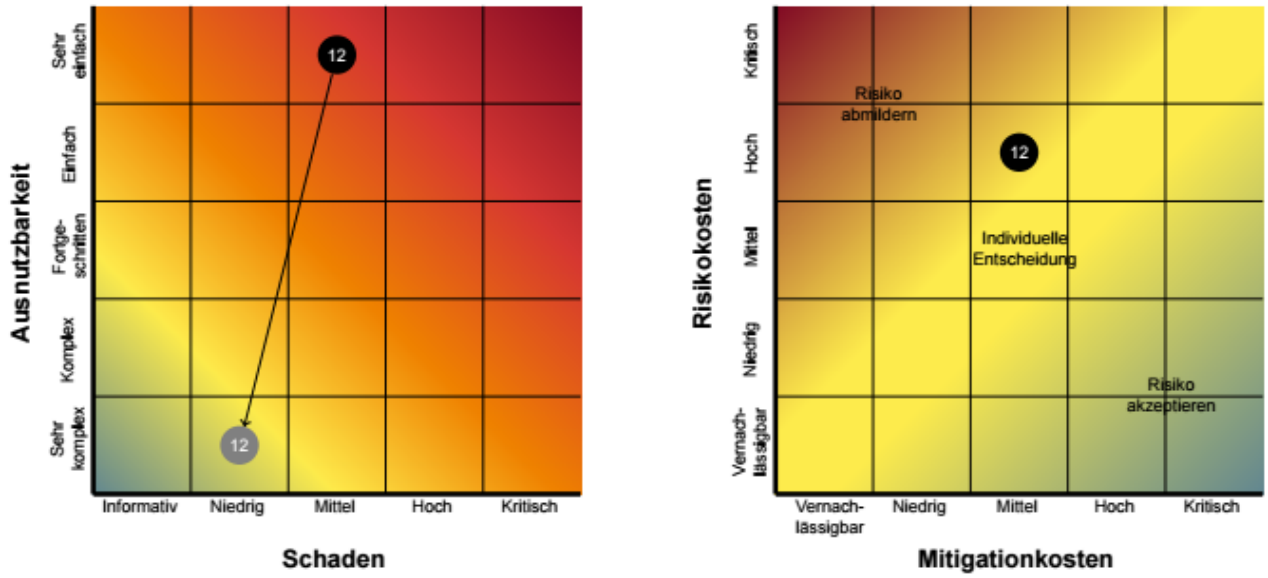
Wahrscheinlichster Angreifer: zufälliger Angreifer

Angriffskomplexität: Sehr einfach

8.12.5 Mögliche abmildernde Maßnahmen

8.12.5.1 Least-Privilege-Prinzip (PoLP)

Graphische Risikodarstellung



Beschreibung

> Autorisierungen sollten immer nach dem Prinzip der geringsten Rechte vergeben werden. Jedes Benutzerkonto sollte also nur über die Rechte verfügen, die die zugehörige Benutzerin oder der Benutzer für die Erledigung seiner betrieblichen Aufgaben benötigt. Dadurch können die Auswirkungen durch eine Kompromittierung eingeschränkt und das Risiko durch versehentliche Eingriffe in Daten oder Systeme minimiert werden.
>
> Siehe auch: ORP.4.A7 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Es entstehen mittlere Kosten durch den Planungs- und Implementierungsaufwand.

Verbleibendes Restrisiko

> Das Restrisiko ist vernachlässigbar.

8.13 Unsichere Anwendungen

8.13.1 Beschreibung der Schwachstelle

Es werden teilweise selbst entwickelte Lösungen zum Speichern und Bearbeiten von Patientendaten verwendet. Hierbei ist das Risiko von Sicherheitslücken und Implementationsfehlern im Vergleich zu verfügbaren, erprobten Lösungen sehr hoch.

Siehe auch CWE-657 (The MITRE Corporation, 2023)

8.13.2 Herkunft / Nachweise

In einem Fall, also 6,25 % wurde in den Fragebögen angegeben, dass selbst entwickelte Access-Datenbanken zum Einsatz kommen.

8.13.3 Auswirkung bei Ausnutzung der Schwachstelle

Unsichere Software oder unsichere Implementierung von Software kann unbefugten Zugriff auf Patientendaten ermöglichen. Darüber hinaus ist auch die Verfügbarkeit bei selbst entwickelten Anwendungen nicht sichergestellt.

Potenzieller Schaden: Hoch

8.13.4 Angriffsvektor

Vorbedingungen: Selbst entworfene Lösung unsicher

Angriffspfad: Netzwerkzugriff, Ausnutzen der vorhandenen Schwachstellen

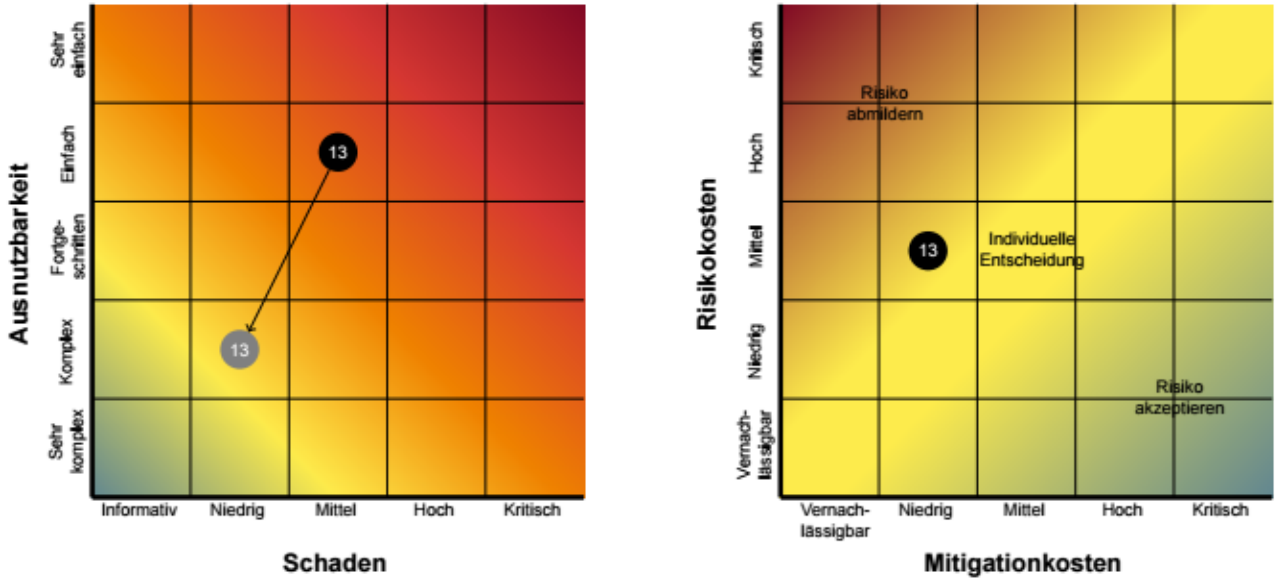
Wahrscheinlichster Angreifer: Gezielte Angreifer

Angriffskomplexität: Mittel

8.13.5 Mögliche abmildernde Maßnahmen

8.13.5.1 Nutzung erprobter Lösungen

Graphische Risikodarstellung



Beschreibung

> Selbst entwickelte Anwendungen können anfällig für Sicherheitslücken sein, wenn die Entwickler nicht über ausreichende Sicherheitskenntnisse verfügen. Zudem ist die Verfügbarkeit nicht sichergestellt. Es gibt bereits eine Vielzahl bestehender Lösungen zur Speicherung und Bearbeitung von Patientendaten, welche das Risiko minimieren. Diese Lösungen sollten für den jeweiligen Anwendungsfall evaluiert und implementiert werden.
>
> Siehe auch: APP.6.A7 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Die Kosten setzten sich aus dem Aufwand der Evaluierung verschiedener Lösungen sowie deren Implementierung zusammen. Möglicherweise fallen hier zusätzlich Lizenzkosten an.

Verbleibendes Restrisiko

> Das verbleibende Restrisiko niedrig.

8.14 Unzureichendes IT-Know-how

8.14.1 Beschreibung der Schwachstelle

Unzureichendes Know-how kann zu fehlerhafter Einrichtung und Konfiguration der Systeme führen und damit Angriffe erleichtern.

8.14.2 Herkunft / Nachweise

Gemäß den Angaben wird die IT bei einer Praxis durch eine Medizinische Fachangestellte (MFA) mit IT-Hintergrund, bei einer anderen durch einen Bekannten, der in einem nicht näher ausgeführten IT-Bereich arbeitet, und bei einer dritten durch einen Arzt selbst betreut. In zwei Fällen wurden Dienstleister ohne jede Zertifizierung beauftragt. Somit sind 31,25 % betroffen.

8.14.3 Auswirkung bei Ausnutzung der Schwachstelle

Fehlerhafte Einrichtung und Wartung der IT-Systeme und Netzwerke können dazu führen, dass Sicherheitslücken nicht geschlossen werden und zusätzlich die Angriffsfläche erhöht wird. Darüber hinaus ist es fraglich, ob eine Mitarbeiterin oder ein Mitarbeiter mit anderem Fokus (MFA, Arzt) auch ausreichend Zeit investiert, sich über aktuelle Themen und Bedrohungen zu informieren, und proaktiv Verbesserungen vornimmt.

Potenzieller Schaden: Hoch

8.14.4 Angriffsvektor

Vorbedingungen: Fehlerhafte Einrichtung und Wartung der IT-Systeme oder Netzwerke.

Angriffspfad: Ausnutzung möglicher Schwachstellen durch einen Angriff über Netzwerke oder lokal.

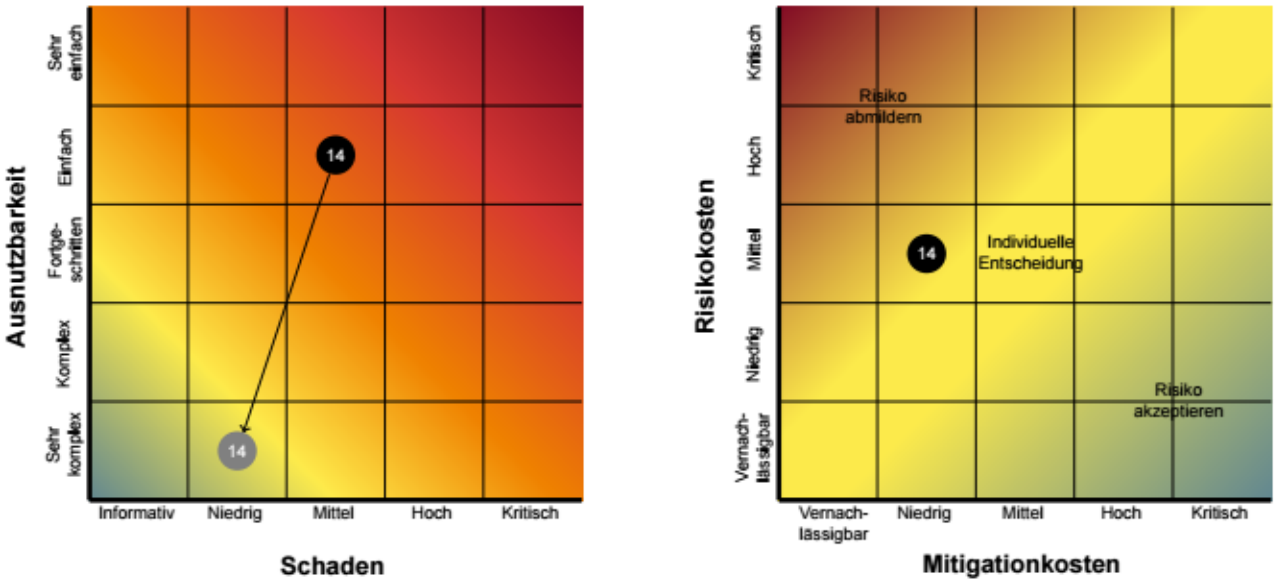
Wahrscheinlichster Angreifer: Gezielte Angreifer

Angriffskomplexität: Einfach

8.14.5 Mögliche abmildernde Maßnahmen

8.14.5.1 Überprüfung der IT-Systeme durch fachliche Experten

Graphische Risikodarstellung



Beschreibung

Die Konfiguration sollte professionell geprüft und anhand vorhandener Hardening Guides optimiert werden.

Siehe auch: SYS.1.1.A6 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

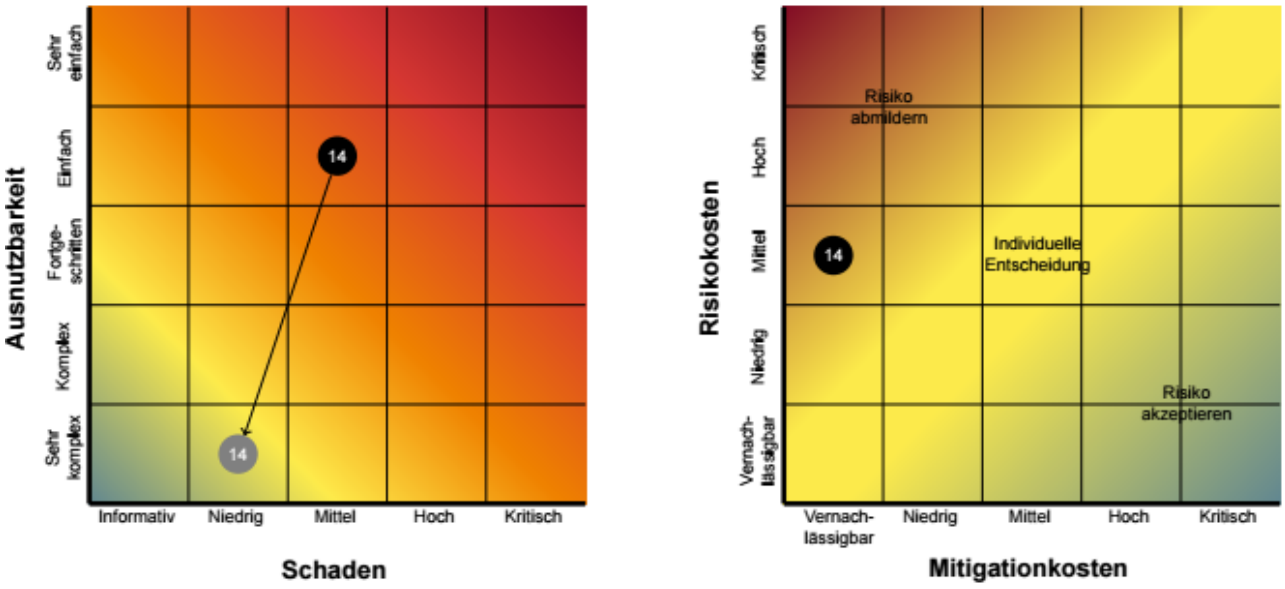
Abhängig von der aktuellen Lage können mittlere bis hohe Kosten entstehen.

Verbleibendes Restrisiko

Das verbleibende Restrisiko ist vernachlässigbar.

8.14.5.2 Aus- und Weiterbildung von Personal forcieren

Graphische Risikodarstellung



Beschreibung

Es ist wichtig, dass nur qualifizierte IT-Fachleute oder geschulte Mitarbeiterinnen und Mitarbeiter für die Einrichtung und Konfiguration der Systeme verantwortlich sind. Darüber hinaus sollte regelmäßige Fortbildung angeboten werden, um das technische Wissen der Mitarbeiterinnen und Mitarbeiter aktuell zu halten und sicherzustellen, dass sie über die neuesten Sicherheitsbestimmungen informiert sind.

Kostenabschätzung

Für die Ausbildung der Mitarbeiterinnen und Mitarbeiter von Dienstleistern sollten für die Praxis keine Kosten entstehen. Ein Wechsel zu einem kompetenteren Dienstleister kann jedoch die Kosten erhöhen. Sollten die IT-Systeme vom Praxispersonal betreut werden, entstehen mittlere bis hohe Kosten für die Ausbildungsmaßnahmen.

Verbleibendes Restrisiko

Das verbleibende Restrisiko ist vernachlässigbar.

8.15 Ungesicherte Medizintechnik

8.15.1 Beschreibung der Schwachstelle

Die medizintechnischen Geräte sind häufig nicht vor Angriffen über das lokale Netzwerk gesichert. Dabei kann es sich um generelle Schwachstellen wie ungesicherte Schnittstellen und veraltete Softwarestände, aber auch um Standardkennwörter handeln, die frei im Internet verfügbar sind.

Siehe auch CWE-693 (The MITRE Corporation, 2023)

8.15.2 Herkunft / Nachweise

Gemäß den Fragenbögen haben nur 25 %, also 4 von 16 Arztpraxen mitgeteilt, dass sie Antivirensoftware für ihre medizinische Geräte einsetzen. Von den 12 Praxen, in denen kein Virenschutz für die Medizingeräte eingesetzt wird, haben 3 keine Netzwerksegmentierung, was das Risiko noch weiter erhöht.

8.15.3 Auswirkung bei Ausnutzung der Schwachstelle

Die Auswirkungen können von Kompromittierung bis hin zu Sperrung oder Beschädigung der Medizintechnik reichen. Bei einer Kompromittierung können auch weitere Geräte im selben Netzwerk angegriffen werden (Lateral Movement).

Potenzieller Schaden: Hoch

8.15.4 Angriffsvektor

Vorbedingungen:

- Die Netzwerkschnittstellen der Medizintechnik sind im Netz erreichbar. Die Software hat selbst Schwachstellen in der Implementierung. Es existieren keine oder kaum netzbasierte Schutzmechanismen wie dedizierte Firewalls oder Einbrucherkennungssysteme.
- Zugriff auf das interne Netzwerk

Angriffspfad: Der Angriff erfolgt entweder direkt über das Netzwerk oder nach einem erfolgreichen Angriff von außen, nachdem Zugriff auf ein anderes Gerät (z. B. einen Client) in diesem Netzwerk erlangt wurde.

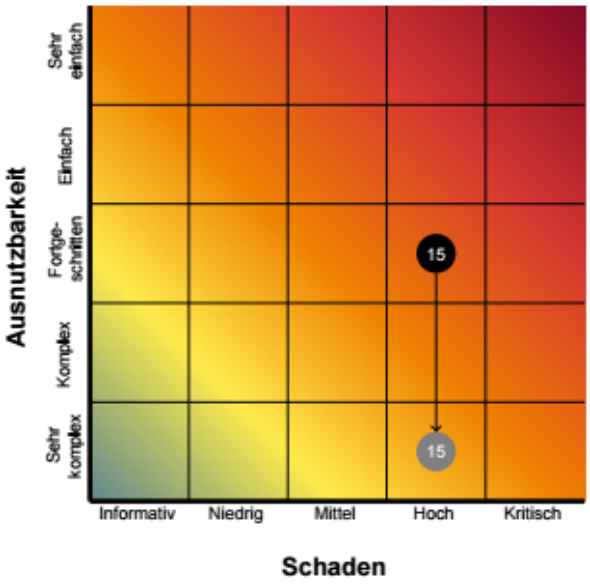
Wahrscheinlichster Angreifer: Gezielte Angreifer

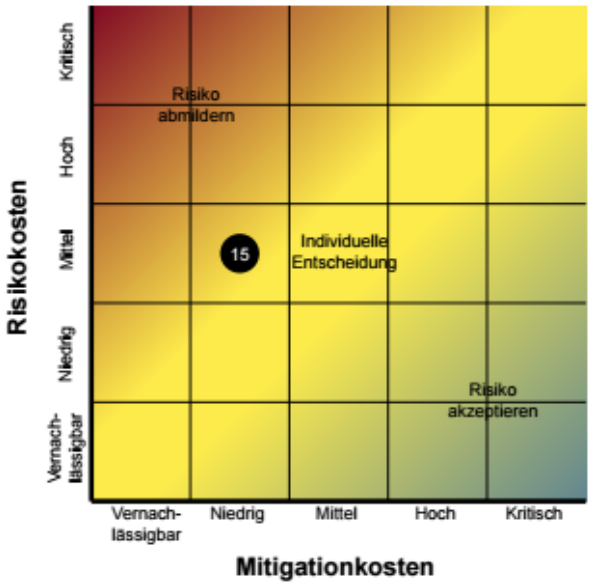
Angriffskomplexität: Mittel

8.15.5 Mögliche abmildernde Maßnahmen

8.15.5.1 Ändern von Standardkennwörtern

Graphische Risikodarstellung





Beschreibung

Ändern von Standardkennwörtern, falls die Medizintechnik den Zugriff über Authentifizierungsmechanismen absichert.

Siehe auch: ORP.4.A8 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

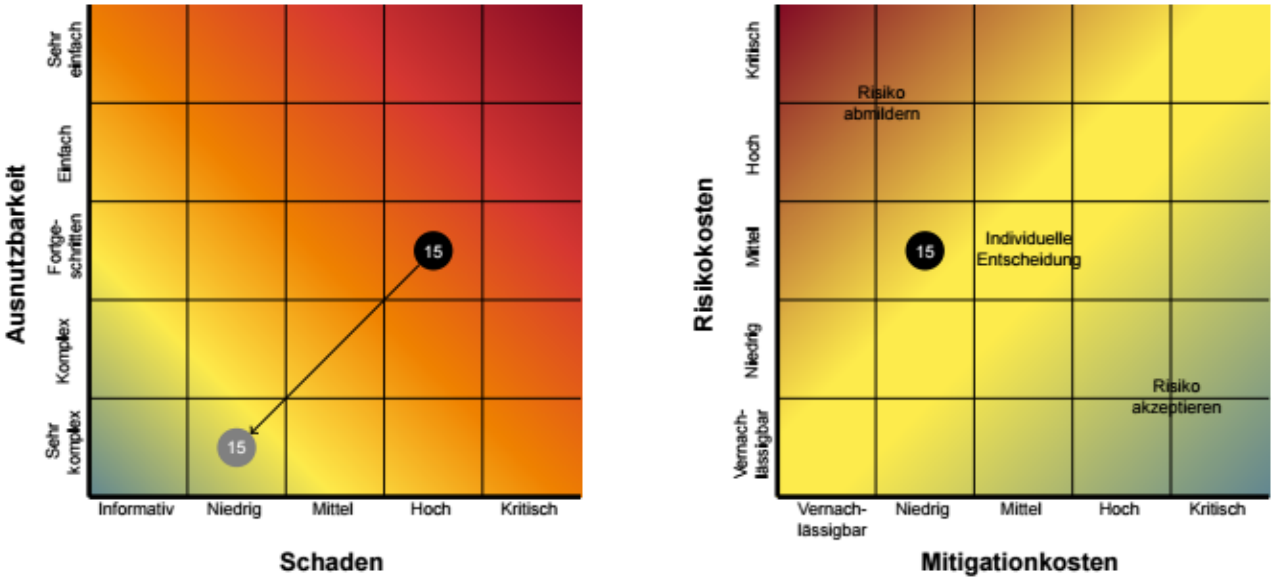
Die Kosten sind gering.

Verbleibendes Restrisiko

Das Ändern des Standardkennwortes hilft, wenn von einem sicheren Gerät ausgegangen werden kann. Es verbleiben aber die anderen oben genannten Risiken.

8.15.5.2 Patchen

Graphische Risikodarstellung



Beschreibung

Es ist entscheidend, dass alle medizintechnischen Geräte regelmäßig auf Updates und Patches überprüft werden, um sicherzustellen, dass sie auf dem neuesten Stand sind und bekannte Sicherheitslücken geschlossen sind.

Siehe auch: OPS.1.1.3.A15 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

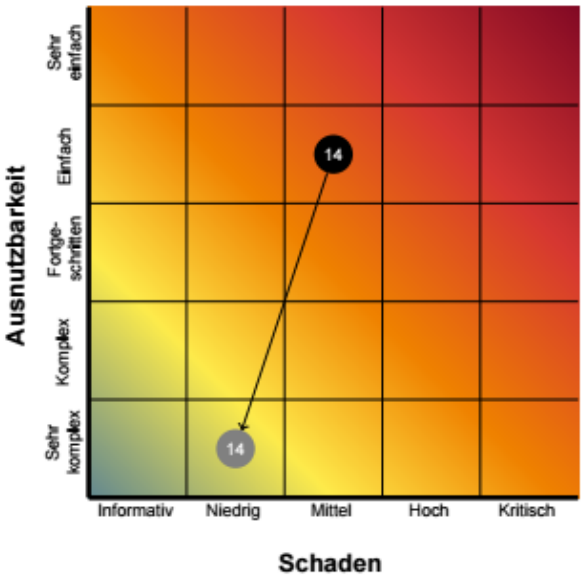
Es entstehen geringe Kosten für die regelmäßige Aktualisierung der jeweiligen Systeme.

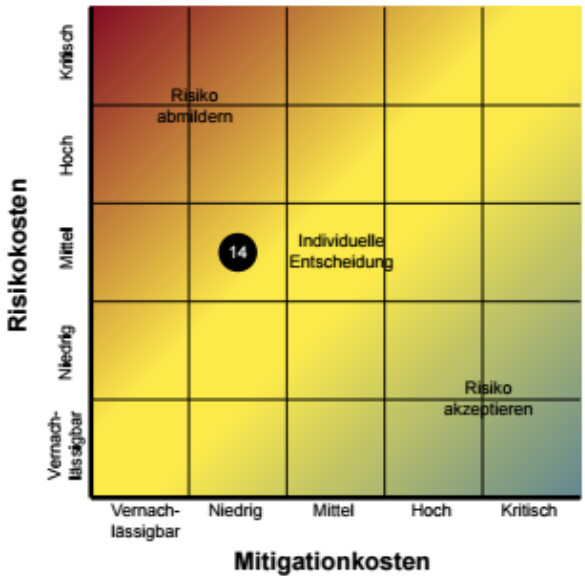
Verbleibendes Restrisiko

Das Restrisiko ist in erster Linie abhängig von der Aktualität der Patches und dem Sicherheitsfokus des Herstellers sowie der zuverlässigen Aktualisierung durch die Verantwortlichen.

8.15.5.3 Netzwerksegmentierung

Graphische Risikodarstellung





Beschreibung

> Als zusätzliche Maßnahme wird empfohlen, die Medizintechnik in ein eigenes Netzwerksegment mit eigenen Schutzmechanismen und Firewall-Regeln umzuziehen, um einen Übergriff zu erschweren. Dies bietet sowohl einen Schutz bei kompromittierten IT-Geräten als auch bei kompromittierter Medizintechnik. Diese Maßnahme ist insbesondere angezeigt, wenn durch den Hersteller keine Updates zur Verfügung gestellt werden.
>
> Siehe auch: NET.1.1.A4 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Hier fallen Kosten für die Einrichtung des Netzwerksegments und der Firewall-Regeln als auch für das Testen an. Kosten für Hardware können zusätzlich anfallen, falls die bestehenden Geräte eine Segmentierung nicht unterstützen.

Verbleibendes Restrisiko

> Das Restrisiko ist maßgeblich davon abhängig, welche Kommunikationsverbindungen für den benötigten Funktionsumfang nötig sind und inwieweit man die Kommunikation zwischen den Netzsegmenten einschränken kann.

8.16 Unzureichendes Patch- und Updatemanagement

8.16.1 Beschreibung der Schwachstelle

In 13 der befragten Praxen ist kein bzw. ein unzureichendes Patch- und Updatemanagement implementiert. D. h. teilweise finden unregelmäßige Updates statt, teilweise gibt es keine Updates für die Systeme.

Siehe auch CWE-1277 (The MITRE Corporation, 2023)

8.16.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 11 von 16 Arztpraxen mitgeteilt, dass sie keinen definierten Prozess zum Patch- und Updatemanagement umgesetzt haben. Damit weisen 68,75 % der Praxen einen unklaren Patch-Stand auf. Zieht man nur die Medizintechnik in Betracht, sind es sogar 13 Praxen, also 81,25 %.

8.16.3 Auswirkung bei Ausnutzung der Schwachstelle

Ein System, das bezüglich der Sicherheit nicht auf dem aktuellen Stand gehalten wird, ist leichter zu kompromittieren, da es bereits bekannte und ausnutzbare Schwachstellen enthalten kann.

Potenzieller Schaden: Hoch

8.16.4 Angriffsvektor

Vorbedingungen: Ungepatchtes, anfälliges System

Angriffspfad: Ausnutzung der Schwachstellen über einen Netzwerk- oder lokalen Angriff

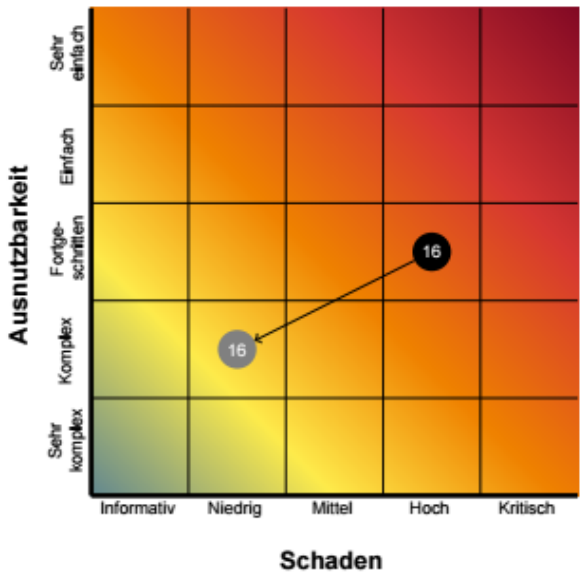
Wahrscheinlichster Angreifer: Gezielte Angreifer

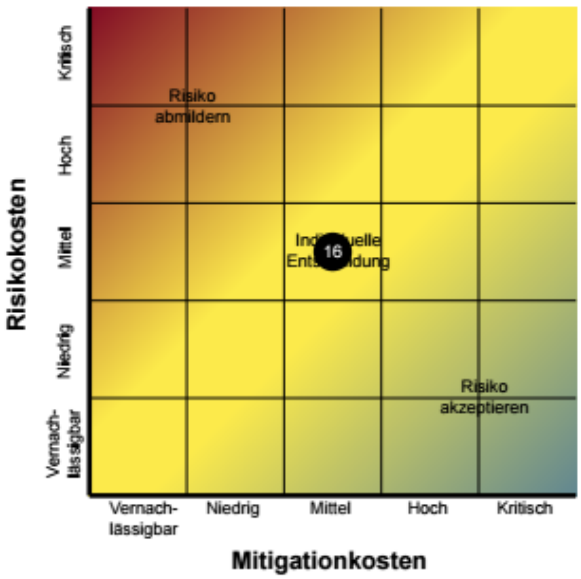
Angriffskomplexität: Mittel

8.16.5 Mögliche abmildernde Maßnahmen

8.16.5.1 Patchmanagement

Graphische Risikodarstellung





Beschreibung

> Die Einführung eines regelmäßigen und strukturierten Patch- und Update-Managements ist dringend erforderlich, um alle Systeme auf dem neuesten Stand zu halten und bekannte Sicherheitslücken zu schließen. Automatisierte Update-Prozesse könnten hierbei helfen, den Arbeitsaufwand zu reduzieren und gleichzeitig die Systemsicherheit zu erhöhen.
>
> Siehe auch: OPS.1.1.3.A3 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Es entstehen mittlere Kosten durch die Einrichtung, die aber durch den reduzierten manuellen Aufwand kompensiert werden.

Verbleibendes Restrisiko

> Es verbleibt ein niedriges Restrisiko durch Zero-Day-Exploits.

8.17 Keine zentrale Verwaltung für IT-Systeme

8.17.1 Beschreibung der Schwachstelle

Ohne zentrale Verwaltung von IT-Systemen, die eine einfache und einheitliche Konfiguration der angeschlossenen Systeme und Geräte ermöglicht, besteht das Risiko von unsicheren Konfigurationen.

8.17.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 8 von 16 Arztpraxen mitgeteilt, dass keine zentrale Verwaltung ihrer Systeme und Endgeräte existiert. Bei 3 weiteren Praxen ist eine zentrale Verwaltung nur unvollständig implementiert. Damit weisen 68,75 % der Praxen diese Schwachstelle auf.

8.17.3 Auswirkung bei Ausnutzung der Schwachstelle

Schwachstellen, die durch fehlende oder fehlerhafte Konfigurationen entstehen, können ausgenutzt werden, was zu einer Kompromittierung der Systeme führen kann.

Potenzieller Schaden: Hoch

8.17.4 Angriffsvektor

Vorbedingungen: Schwachstellen durch fehlerhafte Konfiguration

Angriffspfad: Ausnutzung der fehlerhaften Konfigurationen

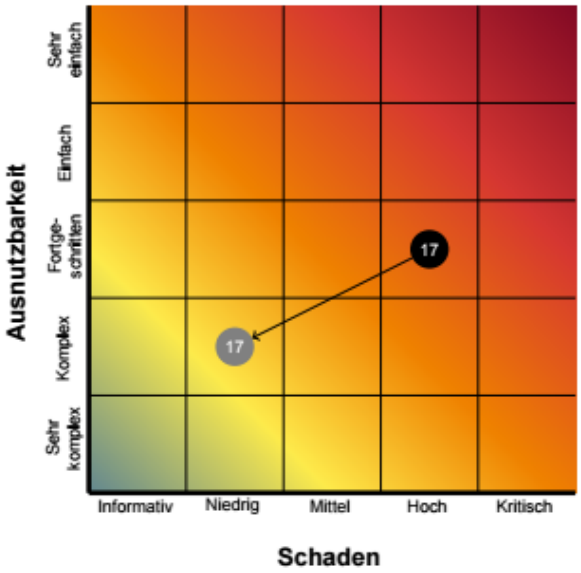
Wahrscheinlichster Angreifer: Gezielte Angreifer

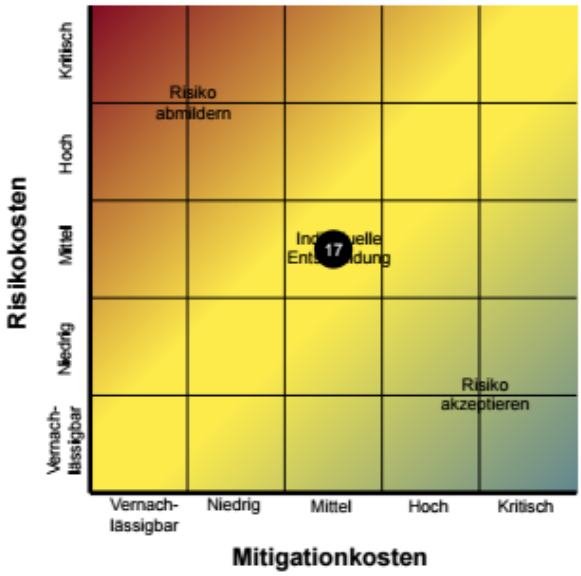
Angriffskomplexität: Mittel

8.17.5 Mögliche abmildernde Maßnahmen

8.17.5.1 Zentrale Verwaltung

Graphische Risikodarstellung





Beschreibung

> Konfigurationen sollten vor allem bei größeren Praxen zentral verwaltet werden, damit eine einheitliche Konfiguration gewährleistet werden kann. Der Fokus sollte dabei auf der Einhaltung einschlägiger Sicherheitsstandards liegen und anhand von Best Practices überprüft werden.

Siehe auch: OPS.1.1.7.A14 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Es entstehen mittlere Kosten.

Verbleibendes Restrisiko

Das Restrisiko bei einer einheitlichen, sicheren Konfiguration ist vernachlässigbar.

8.18 Unzureichende Dokumentation der Infrastruktur

8.18.1 Beschreibung der Schwachstelle

Eine unzureichende Dokumentation erschwert die Analyse der Sicherheit der Infrastruktur, was zu unerkannten Schwachstellen führen kann.

Siehe auch CWE-1059 (The MITRE Corporation, 2023)

8.18.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 11 von 16 Arztpraxen mitgeteilt, dass sie ihre Infrastruktur nicht oder nur teilweise dokumentiert haben. Das sind 68,75 % der Praxen.

8.18.3 Auswirkung bei Ausnutzung der Schwachstelle

Schwachstellen, die nicht erkannt werden, können nicht behoben werden. Dadurch wird ein erfolgreicher Angriff erleichtert.

Potenzieller Schaden: Hoch

8.18.4 Angriffsvektor

Vorbedingungen: Schwachstellen werden mangels Dokumentation nicht erkannt.

Angriffspfad: Keiner

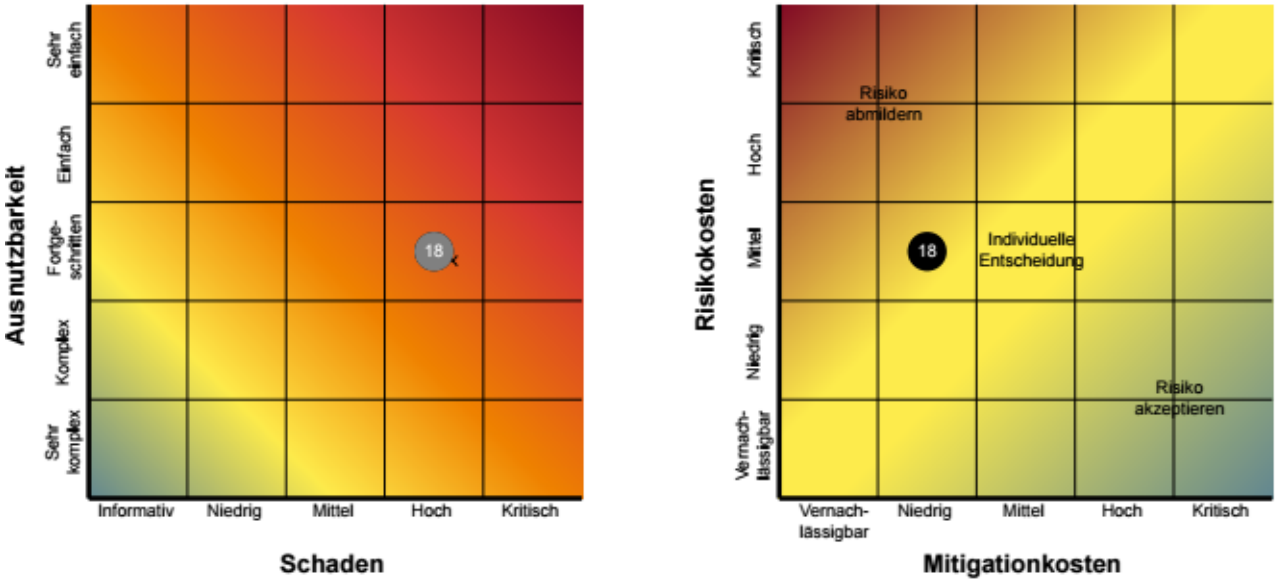
Wahrscheinlichster Angreifer: Gezielte Angreifer

Angriffskomplexität: Mittel

8.18.5 Mögliche abmildernde Maßnahmen

8.18.5.1 Infrastruktur dokumentieren

Graphische Risikodarstellung



Beschreibung

> Eine Umfassende Dokumentation der Infrastruktur ermöglicht die bessere Einschätzung von Schwachstellen. Probleme können frühzeitig besser erkannt werden und Angriffe können besser eingegrenzt werden.

Kostenabschätzung

> Es entstehen niedrige Kosten.

Verbleibendes Restrisiko

> Die Dokumentation reduziert nicht das Risiko, erleichtert aber die Erkennung von Problemen.

8.19 Potenziell unsichere Passwörter

8.19.1 Beschreibung der Schwachstelle

Unsichere Passwörter erleichtern deren Erraten und damit das Erlangen der Kontrolle über den Account.

Siehe auch CWE-521 (The MITRE Corporation, 2023)

8.19.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 10 von 16 Arztpraxen mitgeteilt, dass keine Passwortrichtlinie existiert. Das sind 62,5 % der Praxen.

8.19.3 Auswirkung bei Ausnutzung der Schwachstelle

Das Risiko ist abhängig davon, von welchem Account das Kennwort erraten werden kann. Bei personalisierten Konten ist das Risiko geringer als bei gemeinsam genutzten, bei normalen Usern geringer als bei Administratoren.

Potenzieller Schaden: Hoch

8.19.4 Angriffsvektor

Vorbedingungen: Unsichere Passwort-Policy

Angriffspfad: Anmeldeversuche über das Netzwerk oder am Gerät (z. B. Passwort-Guessing oder Brute-Force-Angriffe)

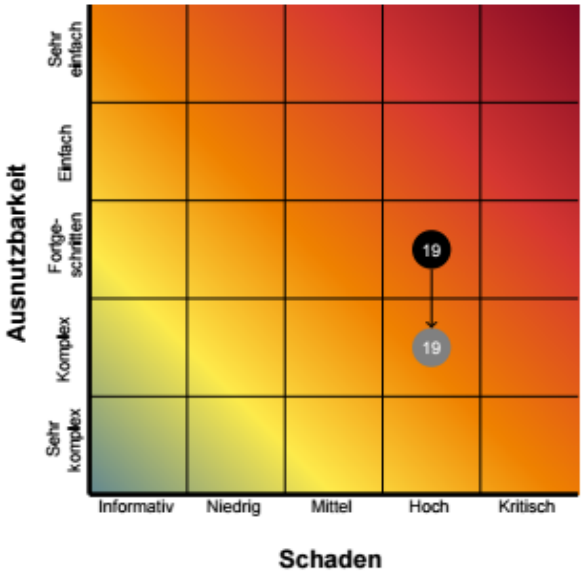
Wahrscheinlichster Angreifer: Gezielte Angreifer

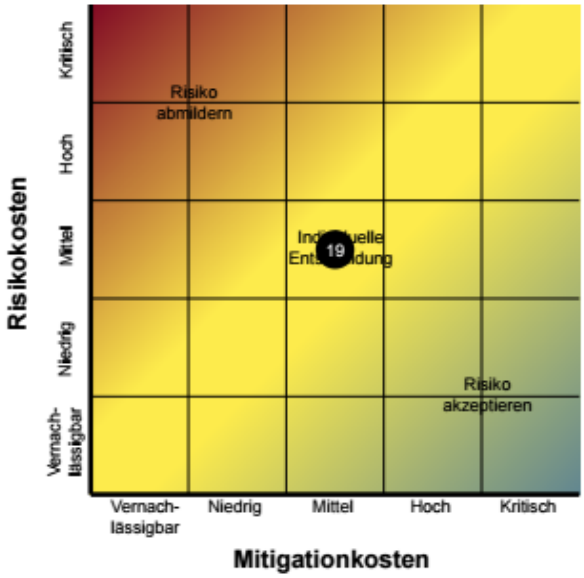
Angriffskomplexität: Mittel

8.19.5 Mögliche abmildernde Maßnahmen

8.19.5.1 Kennwortkomplexität erzwingen

Graphische Risikodarstellung





Beschreibung

Kennwörter sollten eine ausreichende Länge und Komplexität besitzen. Die Komplexität sollte über Richtlinien erzwungen werden. Es sollten keine Standartkennwörter verwendet werden. Die empfohlen Passwortlänge für Wortfolgen liegt bei 20 bis 25. Für Passwörter mit erweiterten Zeichenarten (Zahlen und Sonderzeichen) wird eine Länge von 8 bis 12 empfohlen. Zudem sollte die Sicherheit der Accounts über eine Zwei-Faktor-Authentisierung erhöht werden.

Darüber hinaus sollten Kennwörter regelmäßig, mindestens jährlich geändert werden. Auch dies kann über eine Richtlinie erzwungen werden.

Siehe auch: ORP.4.A8 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

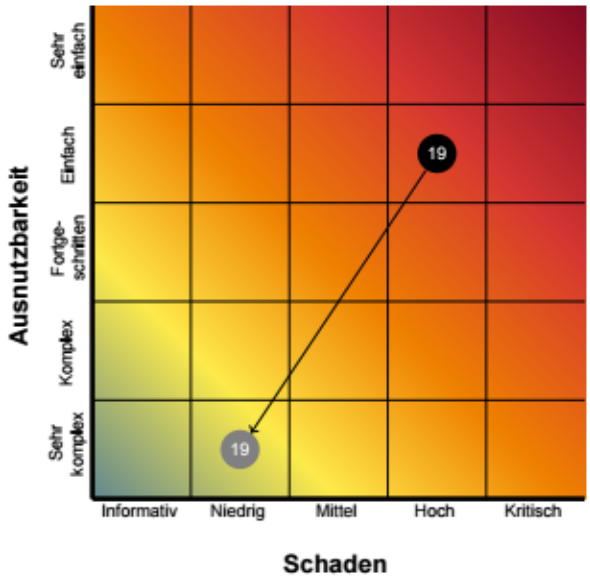
Es entstehen geringe Kosten.

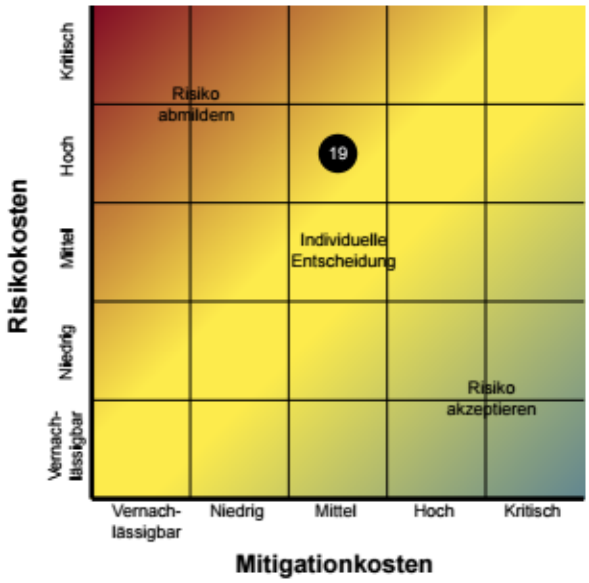
Verbleibendes Restrisiko

Es verbleibt ein mittleres Restrisiko.

8.19.5.2 Zwei-Faktor-Authentisierung

Graphische Risikodarstellung





Beschreibung

> Ein zweiter Faktor erhöht die Sicherheit der Accounts zusätzlich und hilft auch, wenn Kennwörter erraten oder entwendet wurden.
>
> Siehe auch: ORP.4.A21 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Es entstehen mittlere Kosten.

Verbleibendes Restrisiko

> Das verbleibende Restrisiko ist vernachlässigbar.

8.20 Privatgeräte im Netzwerk

8.20.1 Beschreibung der Schwachstelle

In einigen Praxen sind Privatgeräte im Einsatz, die sich im selben Netzwerk befinden, in dem auch die Praxistechnik angesiedelt ist.

8.20.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 6 von 16 Arztpraxen, also 37,5 % mitgeteilt, dass sie private Geräte im Netzwerk eingebunden haben.

8.20.3 Auswirkung bei Ausnutzung der Schwachstelle

Die Sicherheit von Privatgeräten kann nicht gewährleistet werden. Durch ein kompromittiertes Gerät im Netzwerk sind auch alle anderen Geräte gefährdet.

Potenzieller Schaden: Hoch

8.20.4 Angriffsvektor

Vorbedingungen: Kompromittiertes Privatgerät im Netzwerk

Angriffspfad: Angriffe über das Netzwerk

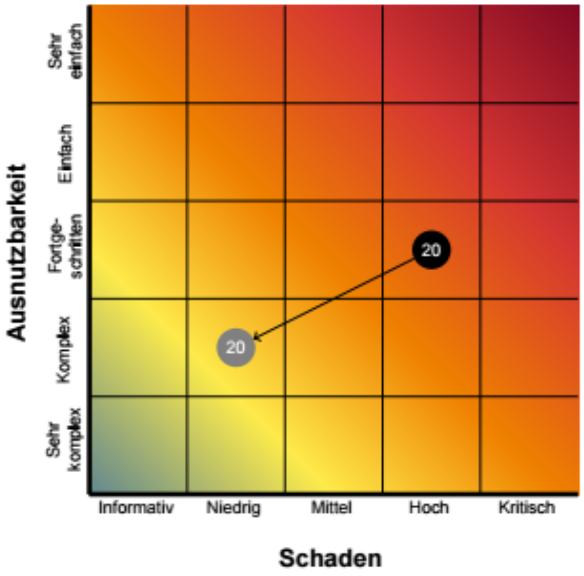
Wahrscheinlichster Angreifer: Gezielte Angreifer

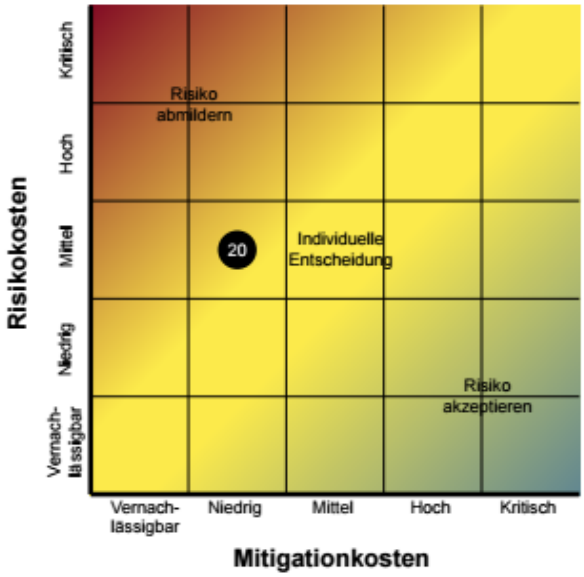
Angriffskomplexität: Fortgeschritten

8.20.5 Mögliche abmildernde Maßnahmen

8.20.5.1 Eigenes Netzwerk für Privatgeräte

Graphische Risikodarstellung





Beschreibung

> Privatgeräte sollten nur in abgetrennten Netzen zugelassen werden, aus denen keine Verbindung in die internen Praxisnetzwerke möglich ist.
>
> Siehe auch: NET.1.1.A6 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Es entstehen geringe Kosten durch die Einrichtung getrennter Netzwerke / WLANs und gegebenenfalls zusätzliche Kosten, falls die bestehende Hardware ausgetauscht werden muss.

Verbleibendes Restrisiko

> Es verbleibt ein geringes Restrisiko.

8.21 Fehlende Netzwerksegmentierung

8.21.1 Beschreibung der Schwachstelle

In einigen Praxen gibt es keine Trennung der Netzwerke. Das betrifft sowohl die Trennung zwischen LAN und WLAN als auch die Trennung zwischen Medizin- und IT-Geräten.

Siehe auch CWE-653 (The MITRE Corporation, 2023)

8.21.2 Herkunft / Nachweise

Von den befragten Arztpraxen gaben 6, also 37,5 % an, dass sie keine Netzwerksegmentierung konfiguriert haben.

8.21.3 Auswirkung bei Ausnutzung der Schwachstelle

Die Segmentierung von Netzwerken erschwert die Verbreitung im Netzwerk, sollte eines der Geräte kompromittiert sein. Dies ist umso wichtiger, falls Geräte mit unklarem Patch-Stand oder Virenschutz im Einsatz sind. Bei einer fehlenden Segmentierung fehlt dieser Schutz.

Potenzieller Schaden: Hoch

8.21.4 Angriffsvektor

Vorbedingungen: Kompromittiertes Gerät im Netzwerk

Angriffspfad: Angriffe über das Netzwerk

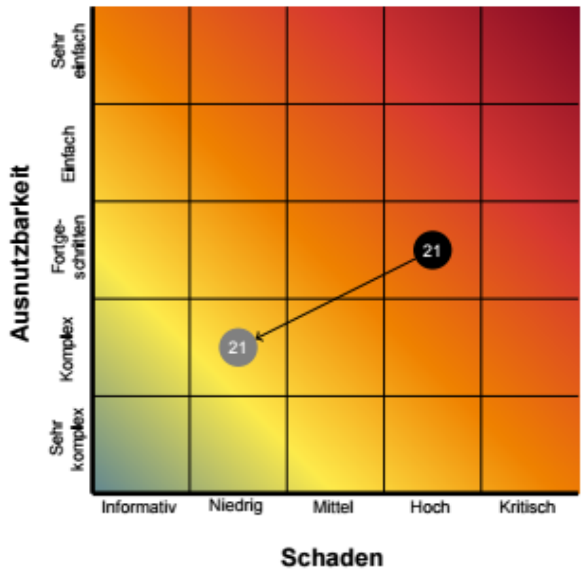
Wahrscheinlichster Angreifer: Gezielte Angreifer

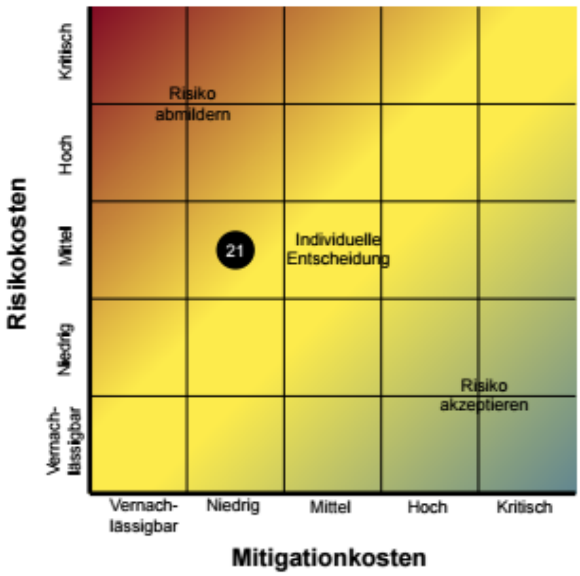
Angriffskomplexität: Fortgeschritten

8.21.5 Mögliche abmildernde Maßnahmen

8.21.5.1 Segmentierung implementieren

Graphische Risikodarstellung





Beschreibung

> Für unterschiedliche Gerätearten sollten eigene Netzwerksegmente angelegt werden. Zwischen den Segmenten sollte der Traffic kontrolliert und eingeschränkt werden.
>
> Siehe auch: NET.1.1.A4 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Es entstehen geringe Kosten durch die Einrichtung getrennter Netzwerke / WLANs und gegebenenfalls zusätzliche Kosten, falls die bestehende Hardware ausgetauscht werden muss.

Verbleibendes Restrisiko

> Es verbleibt ein geringes Restrisiko.

8.22 Parallelbetrieb TI-Konnektor

8.22.1 Beschreibung der Schwachstelle

In den Praxen wird der TI-Konnektor parallel zur restlichen Hardware eingesetzt. Dadurch kann eine Verbindung sowohl über den Router, als auch den TI-Konnektor möglich sein. Hierbei wird die Schutzfunktion des Konnektors umgangen.

8.22.2 Herkunft / Nachweise

Laut den Netzwerkplänen der Praxen, ist der TI-Konnektor in allen Fällen parallel zu weiterer Netzwerkhardware wie Clients und Medizingeräten im Einsatz.

8.22.3 Auswirkung bei Ausnutzung der Schwachstelle

Durch den parallelen Einsatz des TI-Konnektors sind Geräte, die eigentlich geschützt sein sollten, potentiell auch ungeschützt über das restliche Netzwerk erreichbar oder auch direkt mit dem Internet verbunden.

Potenzieller Schaden: Hoch

8.22.4 Angriffsvektor

Vorbedingungen: Zugriff auf ein Gerät im Netzwerk

Angriffspfad: Direkter Zugriff über das Netzwerk

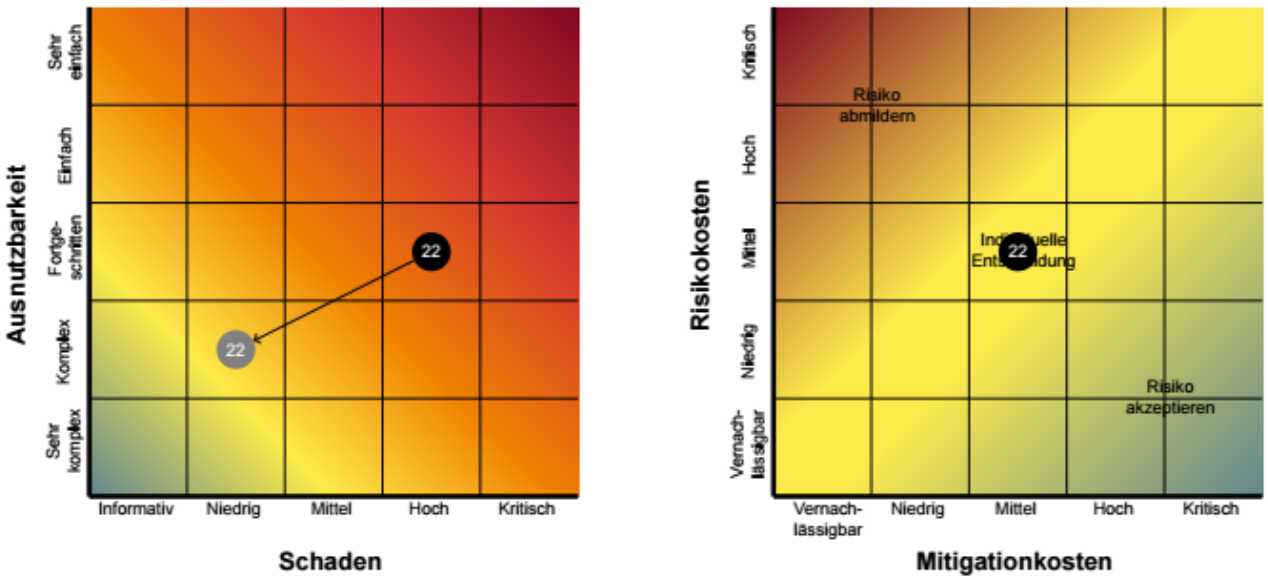
Wahrscheinlichster Angreifer: Gezielte Angreifer

Angriffskomplexität: Fortgeschritten

8.22.5 Mögliche abmildernde Maßnahmen

8.22.5.1 Segmentierung

Graphische Risikodarstellung



Beschreibung

> Geräte mit unterschiedlichem Schutzbedarf müssen sich in unterschiedlichen Netzwerken befinden, damit ein Zugriff untereinander nicht möglich ist. Daher sollten alle Praxisgeräte nur über den TI-

Konnektor als Gateway mit dem Internet verbunden sein. Externe Geräte sollten sich in einem eigenen Netzwerk befinden, dass komplett vom Praxisnetzwerk abgetrennt ist,

Siehe auch: NET.1.1.A6 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Es entstehen geringe Kosten durch die Trennung der Netzwerke und gegebenenfalls zusätzliche Kosten, falls bestehende Hardware ausgetauscht werden muss.

Verbleibendes Restrisiko

Es verbleibt ein geringes Restrisiko.

8.23 Gemeinsam benutzte User-Konten

8.23.1 Beschreibung der Schwachstelle

Zur Reduzierung des Verwaltungsaufwands wird in vielen Praxen von mehreren Mitarbeiterinnen und Mitarbeitern dasselbe Benutzerkonto verwendet.

8.23.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 4 von 16 Arztpraxen mitgeteilt, dass entweder nur ein gemeinsamer Account für alle angestellten Personen existiert oder dasselbe Passwort für verschiedene Benutzer gesetzt wurde. Bei einer weiteren Praxis haben zwar die Ärzte personalisierte Konten, die übrigen Mitarbeiterinnen und Mitarbeiter teilen sich jedoch einen gemeinsamen Account. Damit ist bei 31,25 % der Praxen eine Zuordnung nicht möglich.

8.23.3 Auswirkung bei Ausnutzung der Schwachstelle

Durch die Nutzung gemeinsamer Accounts können individuelle Aktivitäten nicht nachvollzogen werden. Darüber hinaus ist eine schnelle Sperrung des betreffenden Accounts nicht möglich, wenn dieser kompromittiert ist.

Potenzieller Schaden: Niedrig

8.23.4 Angriffsvektor

Vorbedingungen: Zugriff auf den gemeinsamen Account

Angriffspfad: Durchführung von nicht autorisierten Aktionen unter der Anonymität des gemeinsamen Kontos

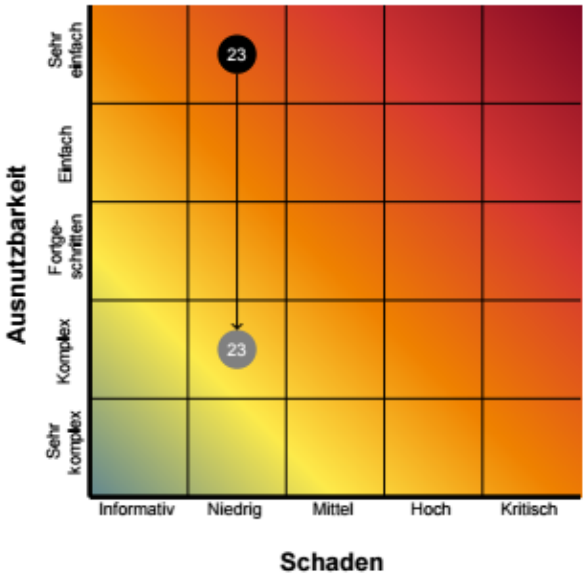
Wahrscheinlichster Angreifer: Gezielte Angreifer

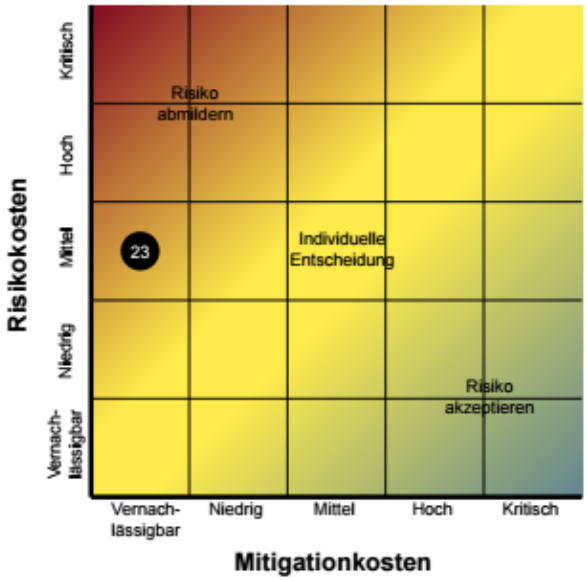
Angriffskomplexität: Kein Angriff

8.23.5 Mögliche abmildernde Maßnahmen

8.23.5.1 Persönliche Konten

Graphische Risikodarstellung





Beschreibung

> Es ist wichtig, dass jede Praxis eine strikte Ein-Benutzer-pro-Konto-Politik einführt, um die Nachvollziehbarkeit zu gewährleisten und im Falle eines Sicherheitsvorfalls gezielte Maßnahmen ergreifen zu können. Dies könnte zwar den Verwaltungsaufwand erhöhen, aber der Zugewinn an Sicherheit und Kontrolle überwiegt deutlich.
> Die Trennung der Konten sorgt für eine individuelle Nachvollziehbarkeit und Nichtabstreitbarkeit von Aktionen. Darüber hinaus können kompromittierte Accounts einfach deaktiviert werden, ohne den Praxisbetrieb dabei komplett lahmzulegen.
>
> Siehe auch: ORP.4.A14 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

> Es entstehen hauptsächlich Kosten durch den Verwaltungsaufwand für die persönlichen Konten.

Verbleibendes Restrisiko

> Es verbleibt ein geringes Restrisiko, das davon abhängig ist, ob ausreichende Maßnahmen implementiert sind (Logging, Monitoring), einen kompromittierten Account erkennen zu können.

8.24 Unverschlüsselte E-Mail-Kommunikation

8.24.1 Beschreibung der Schwachstelle

Patientendaten werden unverschlüsselt per E-Mail versendet. Dadurch sind Vertraulichkeit und Integrietät der Daten gefährdet.

Siehe auch CWE-311 (The MITRE Corporation, 2023)

8.24.2 Herkunft / Nachweise

3 von 16 Praxen (18,75 %) gaben an, Patientendaten per unverschlüsselter E-Mail auszutauschen.

8.24.3 Auswirkung bei Ausnutzung der Schwachstelle

Der Inhalt unverschlüsselter E-Mails könnte mitgelesen werden.

Potenzieller Schaden: Kritisch

8.24.4 Angriffsvektor

Vorbedingungen: Zugriff auf Systeme oder Infrastruktur des Übertragungsweges

Angriffspfad: Abfangen der E-Mail auf dem Übertragungsweg, Auslesen des Inhaltes

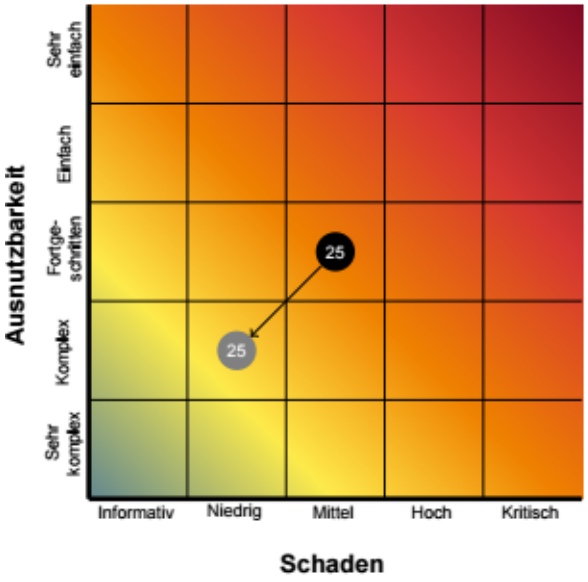
Wahrscheinlichster Angreifer: Gezielte Angreifer

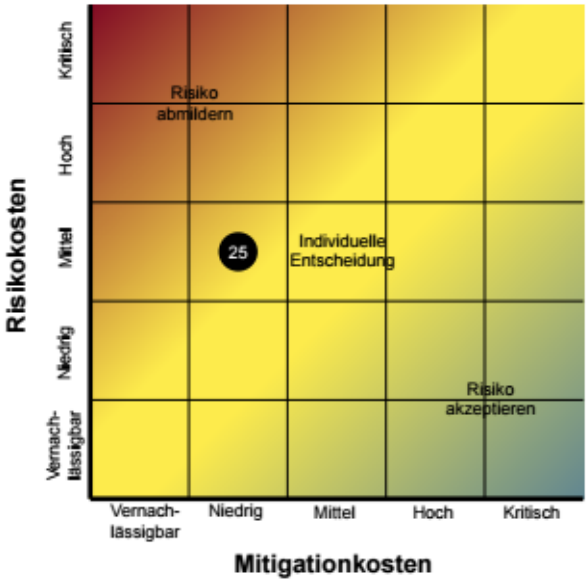
Angriffskomplexität: Komplex

8.24.5 Mögliche abmildernde Maßnahmen

8.24.5.1 Verschlüsselte Übertragung

Graphische Risikodarstellung





Beschreibung

Patientendaten sollten ausschließlich verschlüsselt übertragen werden. Es empfiehlt sich daher, ausgehende E-Mails unter Einsatz geeigneter Zertifikate zu verschlüsseln und zu signieren. Es sollte außerdem darauf geachtet werden, die privaten Schlüssel sicher zu verwalten.

Anstelle von veschlüsselter E-Mails kann auch Kommunikation im Medizinwesen (KIM) verwendet werden, bei dem Daten automatisch verschlüsselt und signiert übertragen werden.

Siehe auch: Art. 32 DSGVO, APP.5.3.A10 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Zertifikate und deren Installation verursachen einen mittleren Kostenaufwand.

Verbleibendes Restrisiko

Bei sachgemäßer Zertifikatsverwaltung ist das verbleibende Restrisiko zu vernachlässigen.

8.25 Fehlende Strukturierung der Informationssicherheit

8.25.1 Beschreibung der Schwachstelle

Security ist ein komplexes Thema mit vielen Facetten. Ohne strukturiertes Vorgehen inklusive einer adäquaten Dokumentation ist eine Umsetzung bzw. eine regelmäßige Prüfung der Informationssicherheit nicht praktikabel.

8.25.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen alle Arztpraxen mitgeteilt, dass sie keinen systematischen Ansatz in Bezug auf die Informationssicherheit verfolgen, wie er etwa durch die Etablierung eines ISMS gegeben wäre.

8.25.3 Auswirkung bei Ausnutzung der Schwachstelle

Ohne eine angemessene Strukturierung der IT-Security-Themen ist die Wahrscheinlichkeit hoch, dass bestimmte Maßnahmen nicht oder nur unzureichend umgesetzt wurden. Die möglichen Schwachstellen sind dabei sehr vielfältig und reichen von fehlenden Prozessen bis hin zu Fehlkonfigurationen.

Potenzieller Schaden: Mittel

8.25.4 Angriffsvektor

Vorbedingungen: Fehlende Strukturierung und Umsetzung der IT-Security-Themen

Angriffspfad: Entsprechend den möglichen Lücken in der Umsetzung

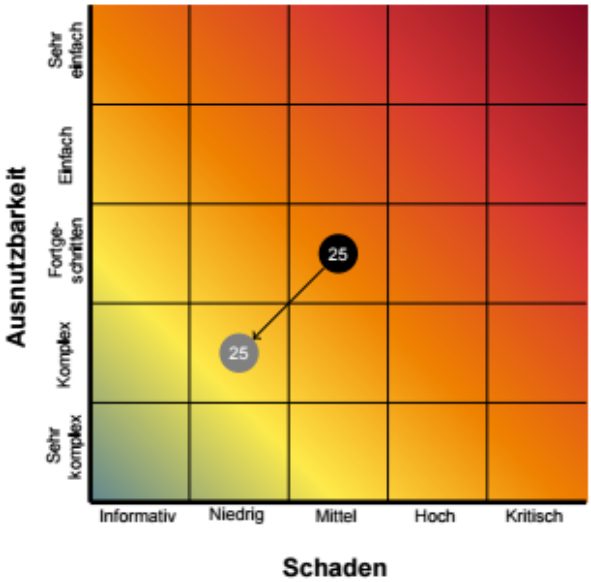
Wahrscheinlichster Angreifer: Gezielte Angreifer

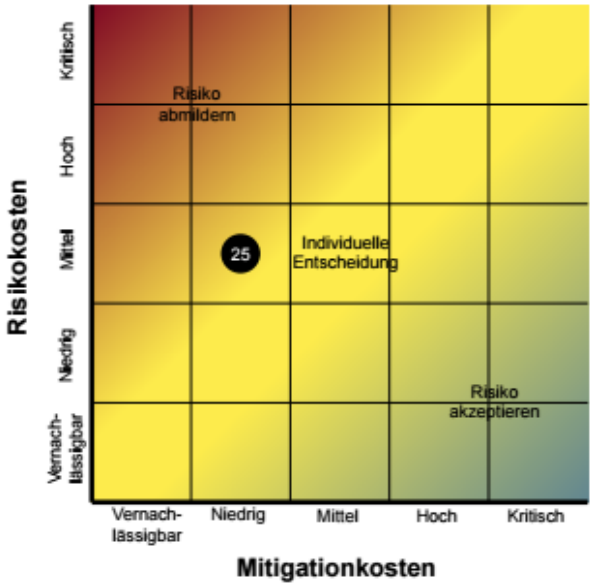
Angriffskomplexität: Fortgeschritten

8.25.5 Mögliche abmildernde Maßnahmen

8.25.5.1 Strukturiertes Vorgehen beim Thema Sicherheit

Graphische Risikodarstellung





Beschreibung

Ein vollständiges ISMS nach BSI-Grundschutz oder ISO 27001 wäre theoretisch eine Option für die Umsetzung der Strukturierungsfrage, allerdings sind die entsprechenden Aufwände vor allem für kleine Praxen kaum verhältnismäßig. Daher sollte anhand von übersichtlichen Hilfestellungen und Beschreibungen eine dem Kontext angepasste Strukturierung angestrebt werden.

Siehe auch: ISMS.1.A1 ff. (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Es entstehen je nach Situation geringe bis mittlere Kosten.

Verbleibendes Restrisiko

Das verbleibende Restrisiko hängt von der Qualität der Strukturierungsmaßnahmen ab.

8.26 Unsichere Netzwerkkonfiguration

8.26.1 Beschreibung der Schwachstelle

Die vorhandenen Sicherheitsmaßnahmen im Netzwerk sind unzureichend. Es ist kein Intrusion Detection System (IDS) bzw. Intrusion Prevention System (IPS) und auch kein dediziertes Firewall-System vorhanden. Das Fehlen dieser Sicherheitsmaßnahmen im Netzwerk kann es einer Angreiferin oder einem Angreifer erleichtern, in das Netzwerk einzudringen und sich unbemerkt auszubreiten.

8.26.2 Herkunft / Nachweise

Zu dieser Schwachstelle haben gemäß dem Fragebogen 11 von 16 (68,75 %) Arztpraxen mitgeteilt, dass sie kein IDS verwenden. 9 der 16 (56,25 %) Arztpraxen gaben an, dass sie kein IPS im Einsatz haben. 4 Praxen, und damit 25 % gaben an, keine Firewall im Einsatz zu haben.

8.26.3 Auswirkung bei Ausnutzung der Schwachstelle

Das Fehlen dieser Sicherheitsmaßnahmen im Netzwerk kann es einer Angreiferin oder einem Angreifer erleichtern, in das Netzwerk einzudringen und sich unbemerkt auszubreiten. Dadurch sind alle Systeme und Daten potenziell gefährdet.

Potenzieller Schaden: Hoch

8.26.4 Angriffsvektor

Vorbedingungen: Vorhandenes Einfallstor für Angreifer

Angriffspfad: Eindringen in das Netzwerk, Lateral Movement

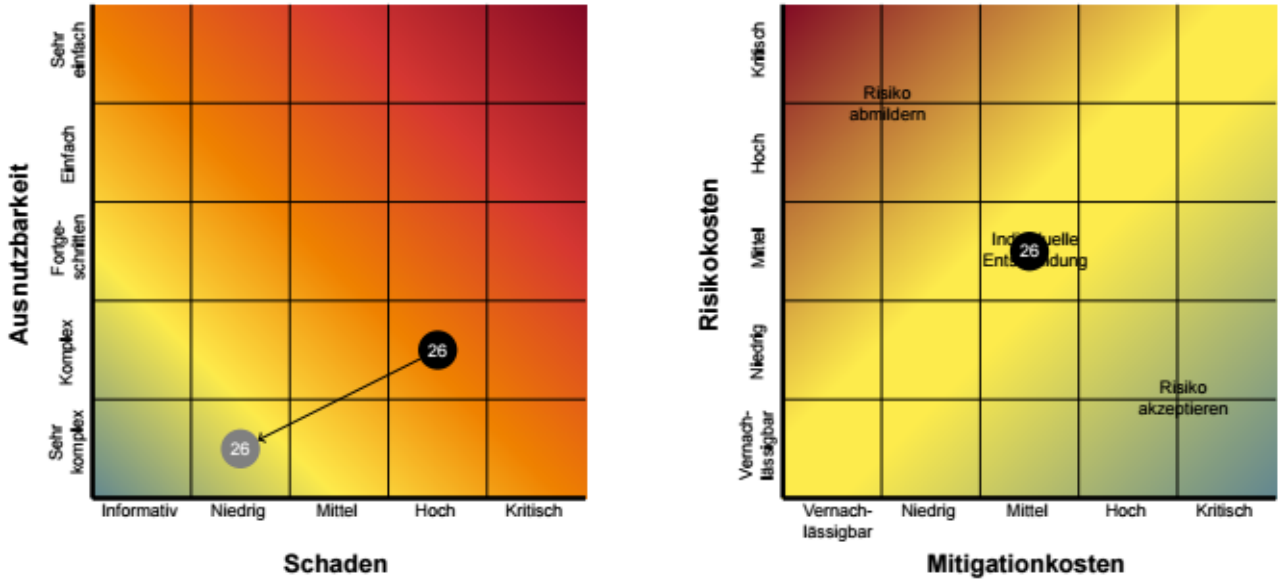
Wahrscheinlichster Angreifer: Gezielte Angreifer

Angriffskomplexität: Bewertung: Komplex

8.26.5 Mögliche abmildernde Maßnahmen

8.26.5.1 IDS/IPS und dedizierte Firewall

Graphische Risikodarstellung



Beschreibung

Um das Eindringen in ein Netzwerk zu erschweren und rechtzeitig auf Angriffe reagieren zu können, sollte eine IDS/IPS-Lösung implementiert werden. Zudem wird die Implementierung einer dedizierten Firewall empfohlen. Hierbei sollte spezielle Sorgfalt auf eine sichere Konfiguration gelegt werden.

Siehe auch: NET.3.2.A4 (Bundesamt für Sicherheit in der Informationstechnik, 2023)

Kostenabschätzung

Je nach aktuellem Zustand können mittlere bis hohe Kosten für die Anschaffung und Konfiguration der Geräte sowie gegebenenfalls Änderungen an der Netzwerkstruktur anfallen.

Verbleibendes Restrisiko

Das Restrisiko ist vernachlässigbar.

9 Mögliche Schwachstellen

Neben den über die Antworten in den Fragebögen abgesicherten Schwachstellen sind die folgenden möglichen Schwachstellen erwähnenswert. Eine genaue Betrachtung wird, da diese nicht im Fokus der Befragung stand, nicht durchgeführt.

Aufgrund der festgelegten Herangehensweise in diesem Projekt können per Definition auch technische Schwachstellen kaum oder nur durch die Antwort der jeweiligen Dienstleister erkannt oder belegt werden. Eine ergänzende technische Analyse in Form von Penetrationstests oder Konfigurationsprüfungen wäre eine mögliche Maßnahme, um hier bessere Einblicke zu erhalten.

9.1 Unzureichende Sicherung öffentlich erreichbarer Ports

Laut Aussagen in den Fragebögen sind jeweils nur die Ports für HTTPS[5] (Port 443), bzw. für VPN-Verbindungen (keine Port-Angaben) geöffnet.

Die Absicherung der nach außen geöffneten Ports wurde jedoch nicht im Detail geprüft. Auch aufgrund der Beispiele von erfolgreichen Remote-Angriffen auf Praxen ist jedoch zu erwarten, dass nicht alle notwendigen Maßnahmen in den Firewalls umgesetzt sind bzw. Fehler in der Konfiguration zu möglichen Schwachstellen führen.

9.2 Unzureichendes Logging- und Monitoring-Konzept

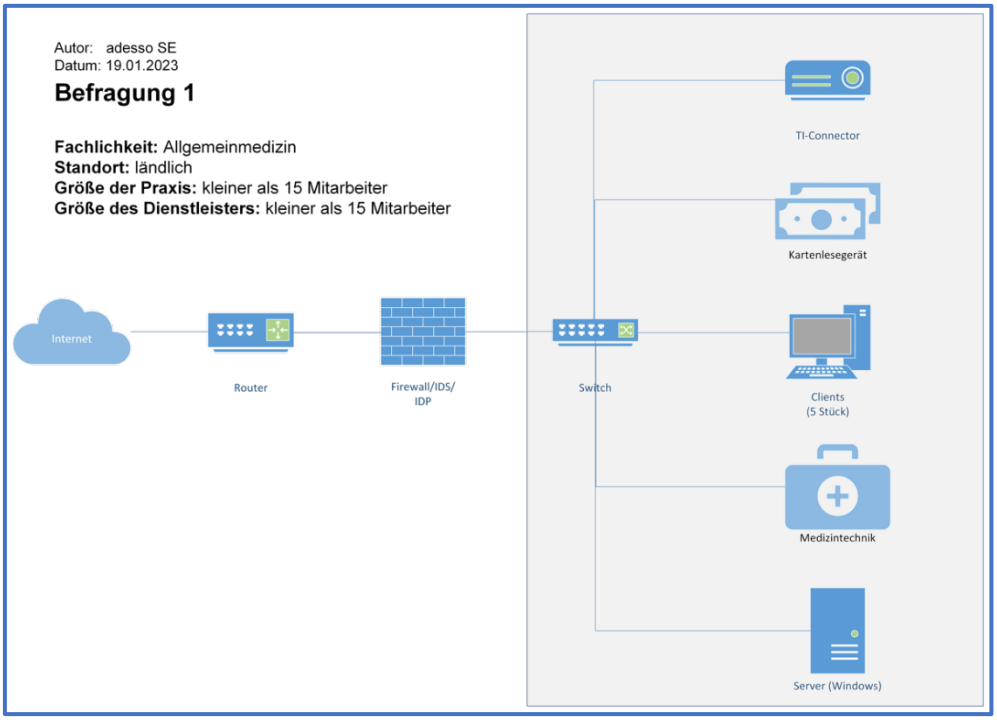
Logging und Monitoring war ebenfalls kein dediziertes Thema für den Fragebogen, jedoch liegt anhand von Gesprächen die Vermutung nahe, dass eine strukturierte Sammlung und Auswertung von Protokolldaten kaum erfolgt. Eine vollständige Überwachung mittels Security Information and Event Management (SIEM) und auswertenden Use-Cases wäre vermutlich ein zu großer Schritt und zu kostenintensiv, jedoch könnte – auch durch Auswertungen in den Praxisverwaltungsprogrammen – durchaus die Möglichkeit zur Erkennung von z. B. Betrugsversuchen weiterentwickelt werden. Dies wäre eine Aufgabe der Hersteller.

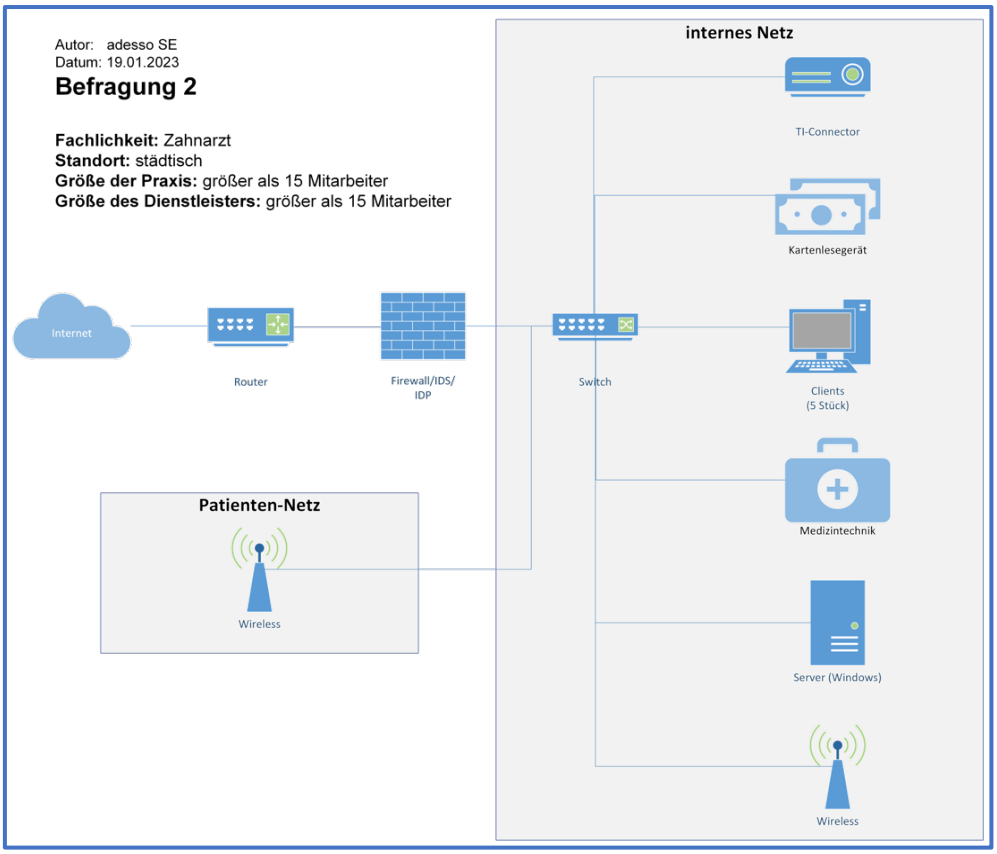
9.3 Unsichere Praxisverwaltungs-Software

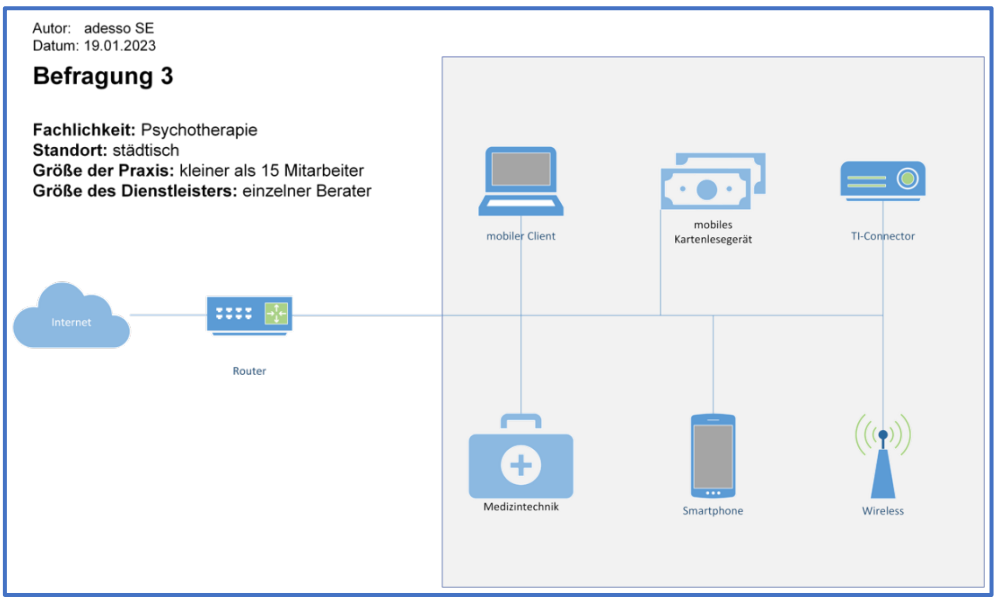
Wie bereits in Kapitel 4.1 angedeutet, ist durchaus erwartbar, wenn auch nicht dediziert überprüft, dass in der sehr heterogenen Software-Landschaft (jede Praxis der Stichprobe verwendet die Software eines anderen Herstellers) Produkte zu finden sind, die ebenfalls ein deutliches Verbesserungspotenzial bezüglich technischer Sicherheit aufweisen. Ein Indiz für diese Annahme ist das Patch-Management bzw. die teilweise nicht vorhandenen Patches für Software-Produkte.

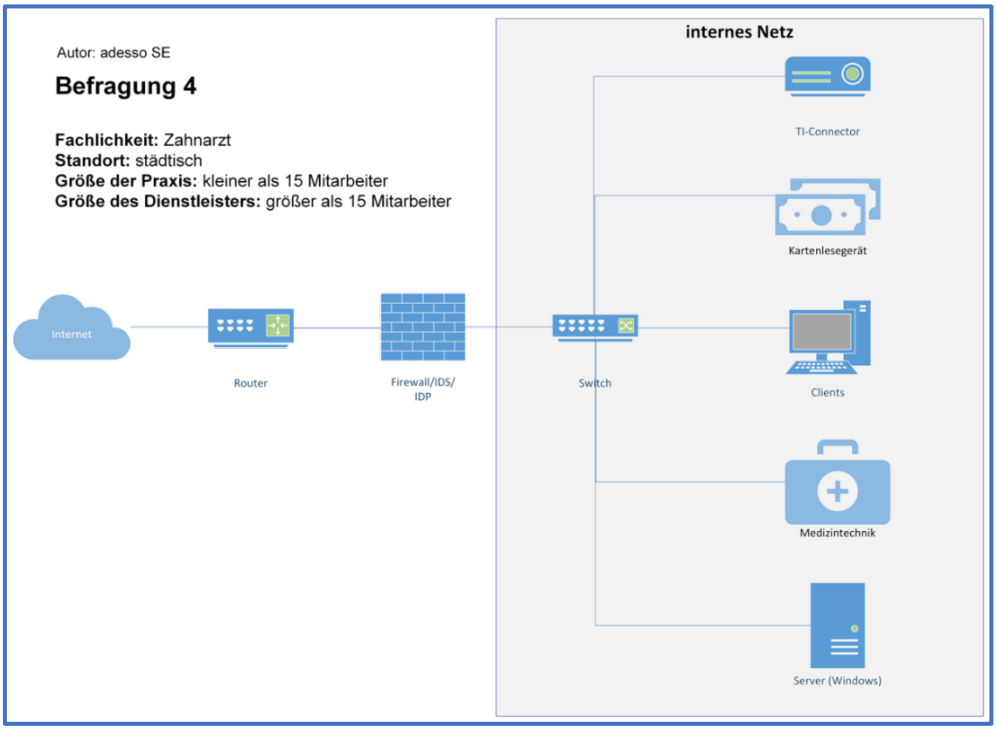
[5] HTTPS bzw. Port 443 wird benötigt, üm eine Website mit TLS Verschlüsselung erreichbar zu machen, wenn eine Praxis die Website im eigenen Netzwerk betreibt.

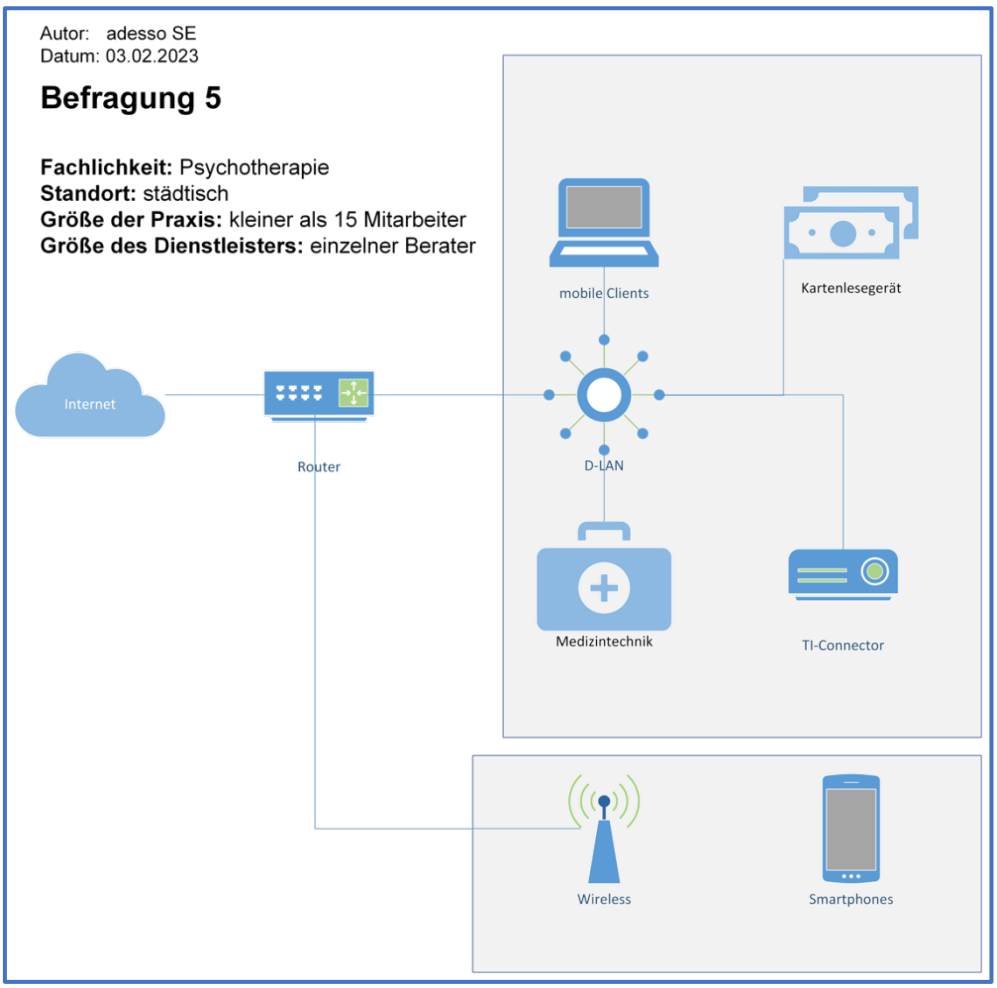
10 Anhang: Netzpläne

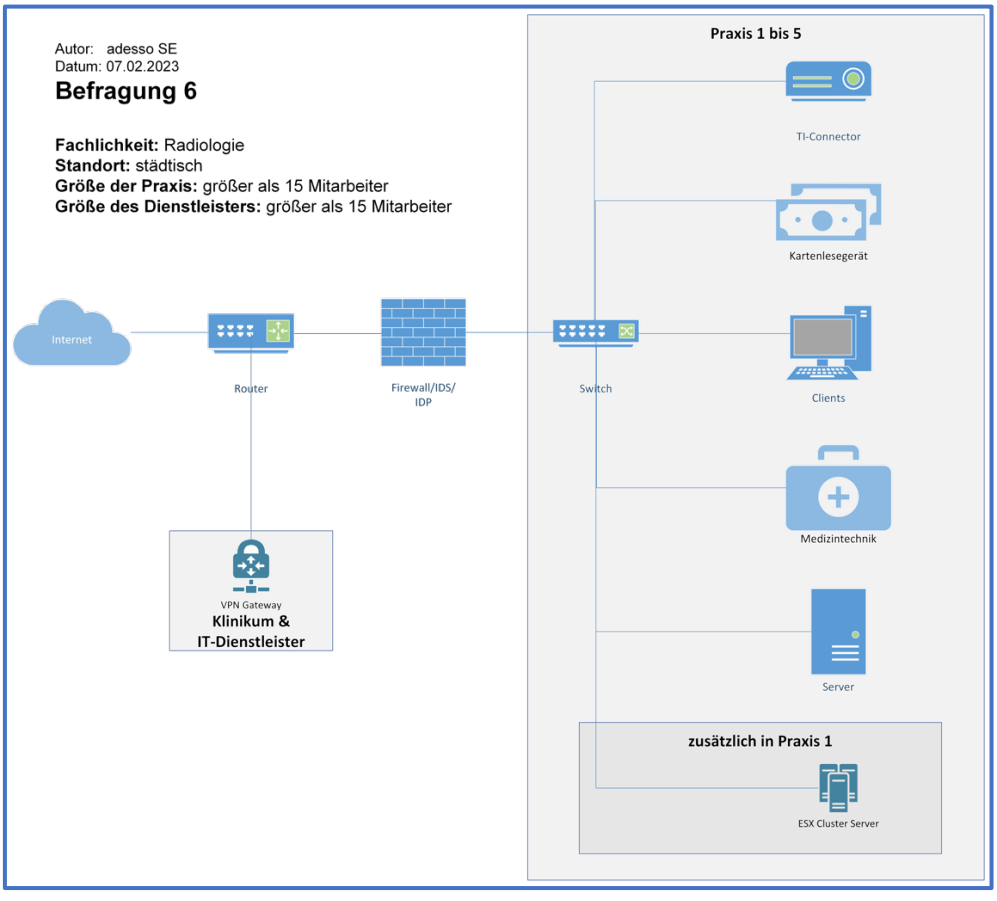


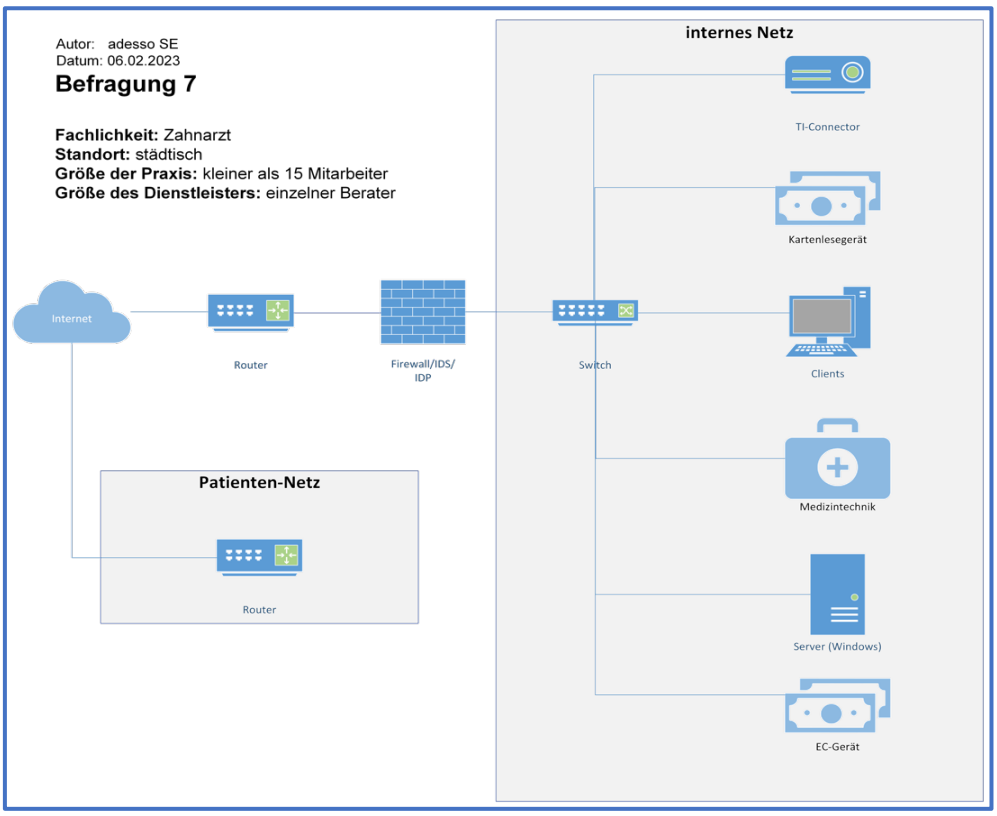


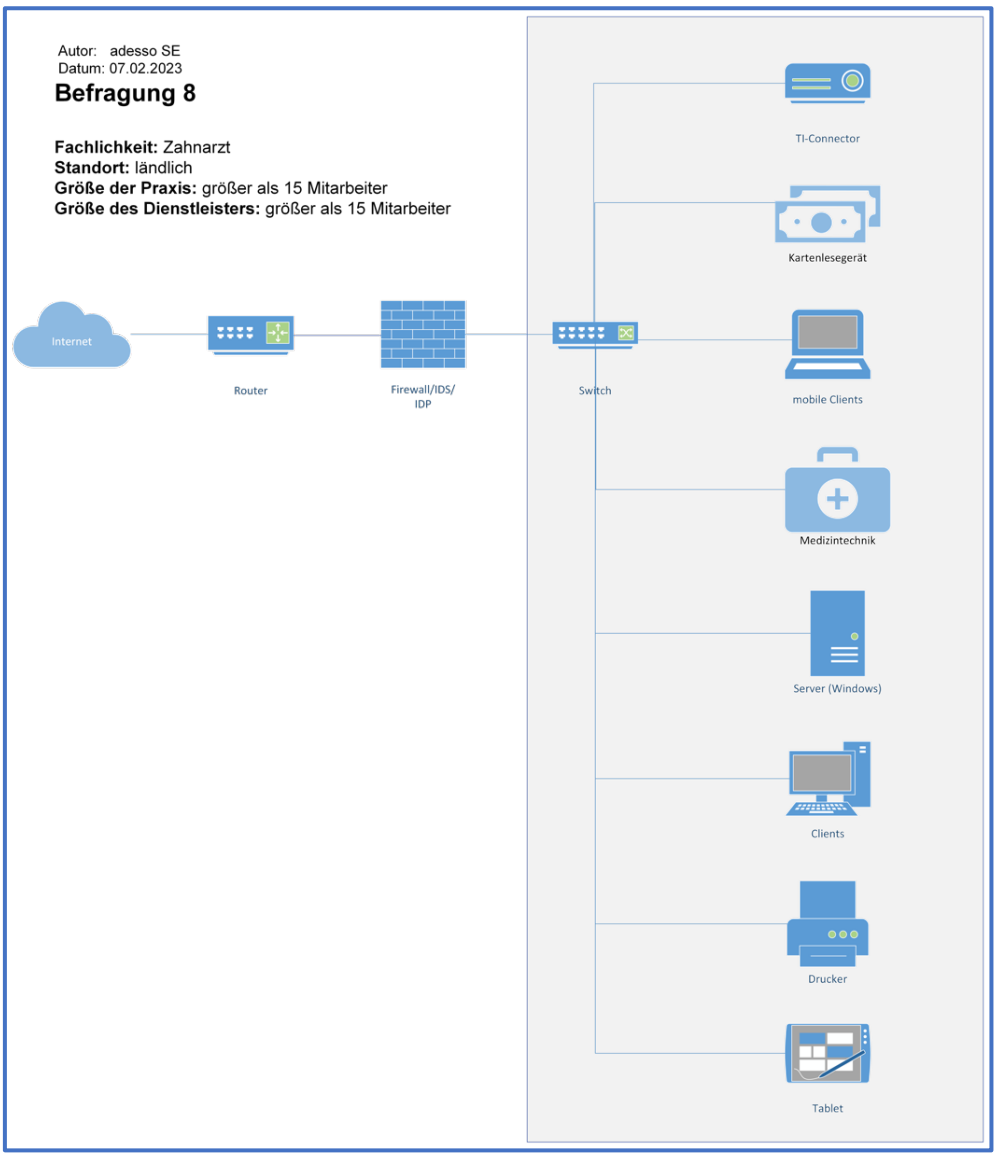

Autor: adesso SE
Datum: 19.01.2023
Befragung 3
Fachlichkeit: Psychotherapie
Standort: städtisch
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: einzelner Berater
mobiler Client
mobiles Kartenlesegerät
TI-Connector
Internet
Router
Medizintechnik
Smartphone
Wireless

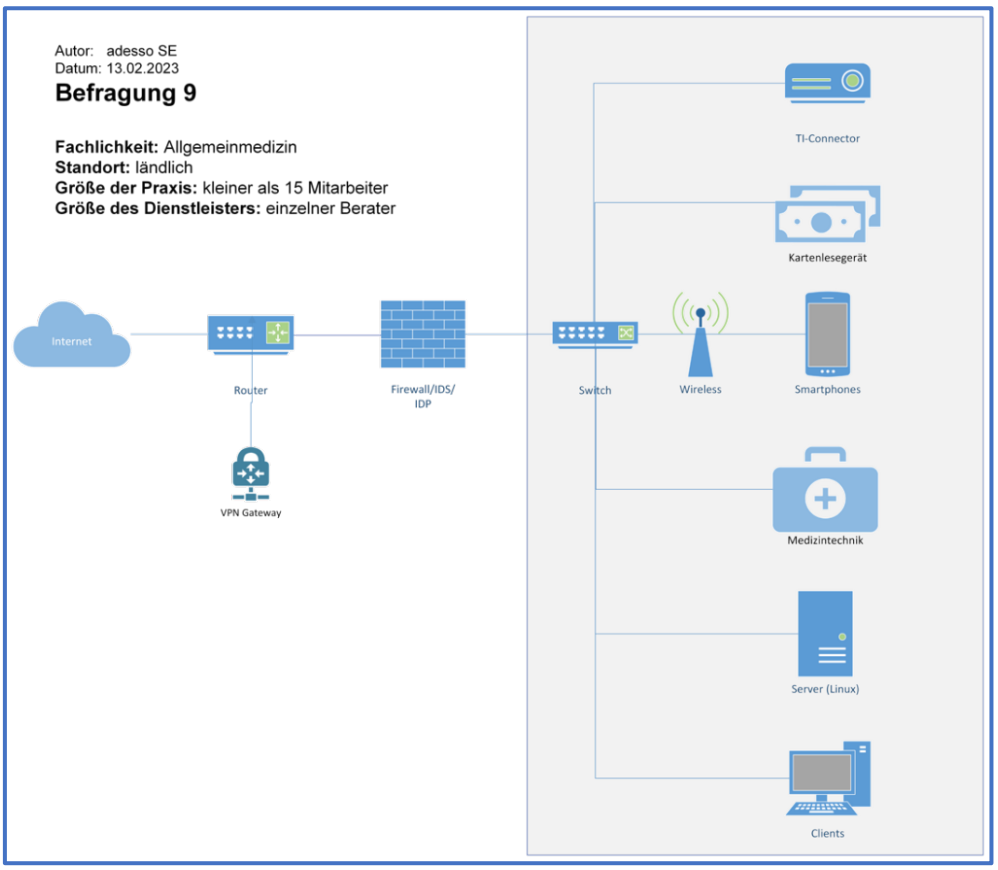

Autor: adesso SE
Befragung 4
Fachlichkeit: Zahnarzt
Standort: städtisch
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: größer als 15 Mitarbeiter
internes Netz
TI-Connector
Kartenlesegerät
Internet
Router
Firewall/IDS/ IDP
Switch
Clients
Medizintechnik
Server (Windows)

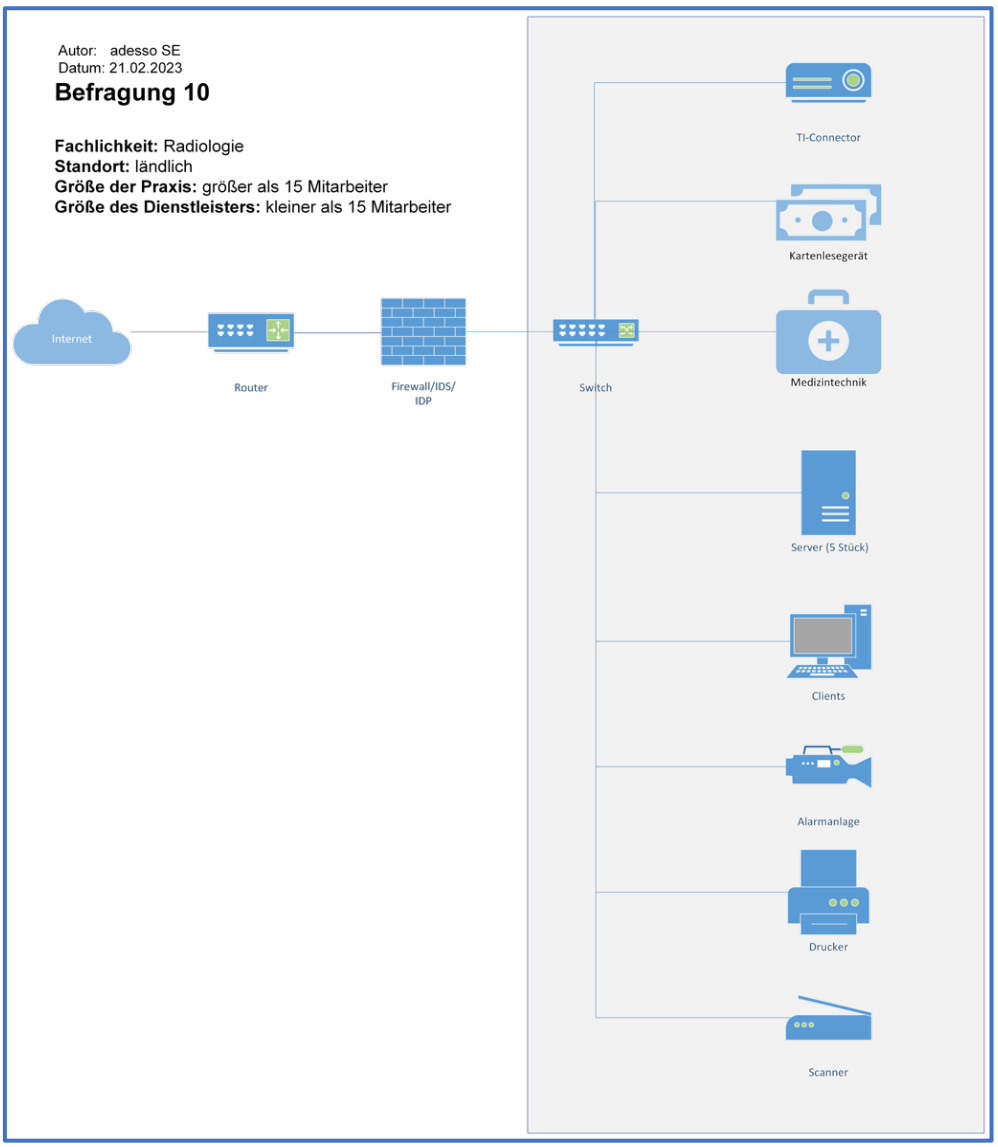

Autor: adesso SE
Datum: 03.02.2023
Befragung 5
Fachlichkeit: Psychotherapie
Standort: städtisch
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: einzelner Berater
mobile Clients
Kartenlesegerät
Internet
Router
D-LAN
Medizintechnik
TI-Connector
Wireless
Smartphones

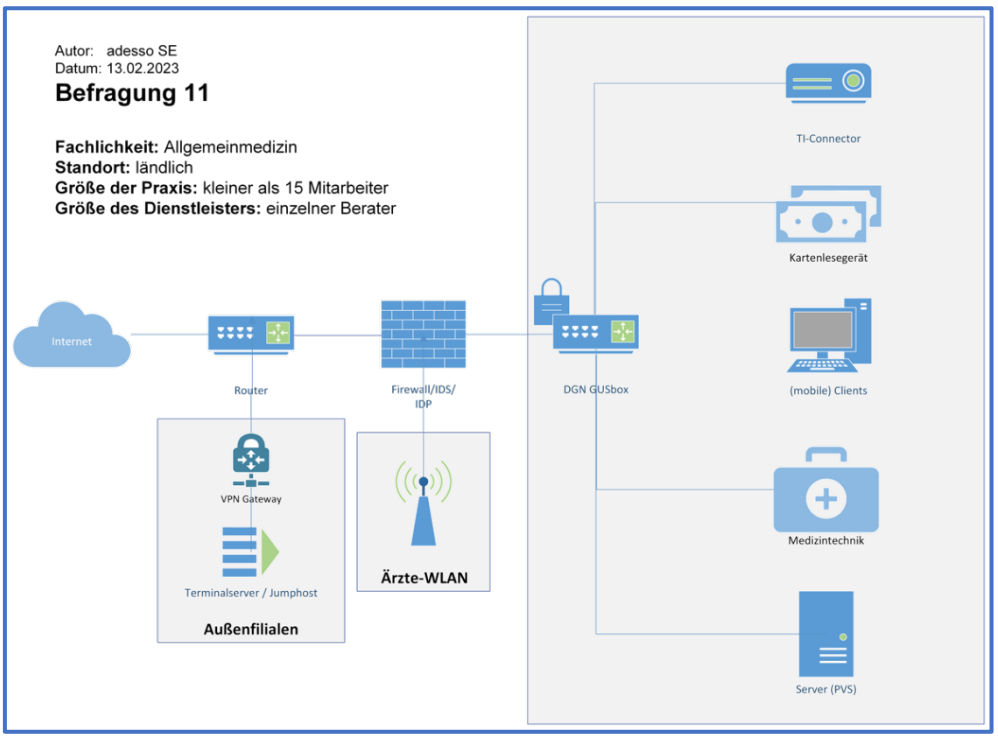

Autor: adesso SE
Datum: 07.02.2023
Befragung 6
Fachlichkeit: Radiologie
Standort: städtisch
Größe der Praxis: größer als 15 Mitarbeiter
Größe des Dienstleisters: größer als 15 Mitarbeiter
Praxis 1 bis 5
TI-Connector
Kartenlesegerät
Internet
Router
Firewall/IDS/
IDP
Switch
Clients
Medizintechnik
VPN Gateway
Klinikum &
IT-Dienstleister
Server
zusätzlich in Praxis 1
ESX Cluster Server

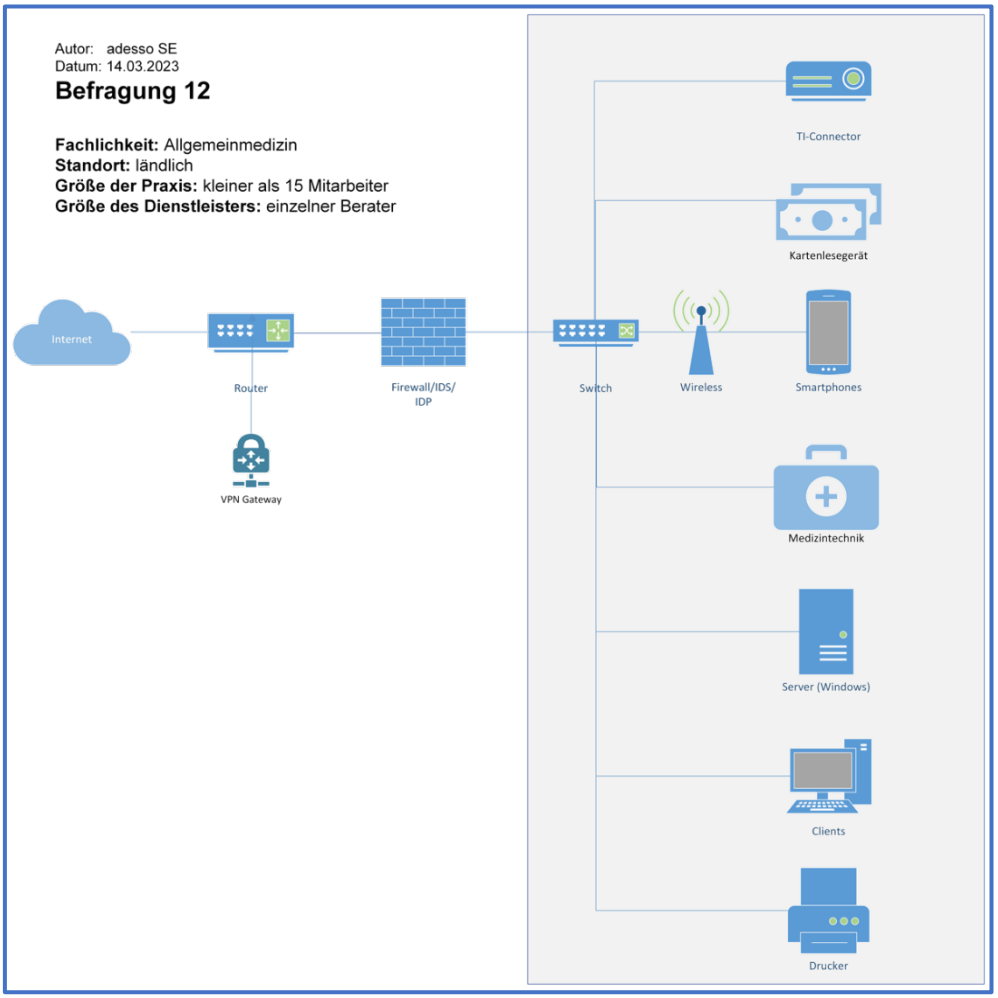

Autor: adesso SE
Datum: 06.02.2023
Befragung 7
Fachlichkeit: Zahnarzt
Standort: städtisch
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: einzelner Berater
internes Netz
TI-Connector
Kartenlesegerät
Internet
Router
Firewall/IDS/
IDP
Switch
Clients
Medizintechnik
Patienten-Netz
Router
Server (Windows)
EC-Gerät

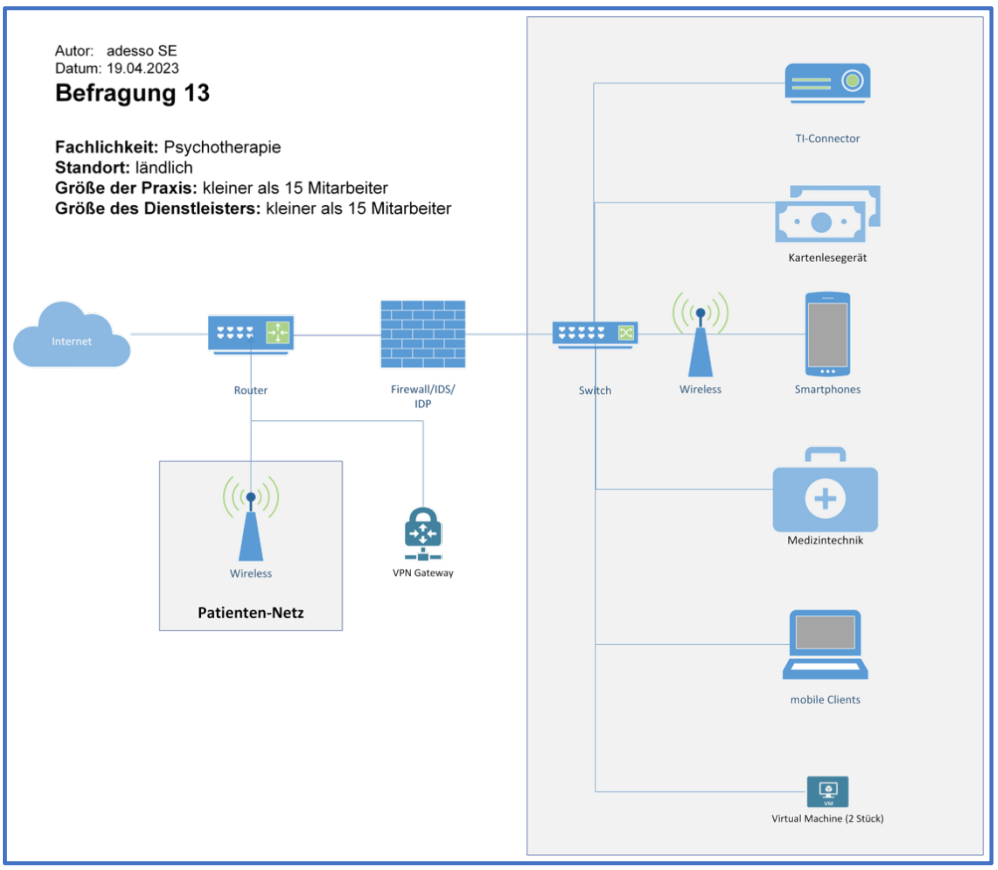

Autor: adesso SE
Datum: 07.02.2023
Befragung 8
Fachlichkeit: Zahnarzt
Standort: ländlich
Größe der Praxis: größer als 15 Mitarbeiter
Größe des Dienstleisters: größer als 15 Mitarbeiter
Internet
Router
Firewall/IDS/
IDP
Switch
TI-Connector
Kartenlesegerät
mobile Clients
Medizintechnik
Server (Windows)
Clients
Drucker
Tablet

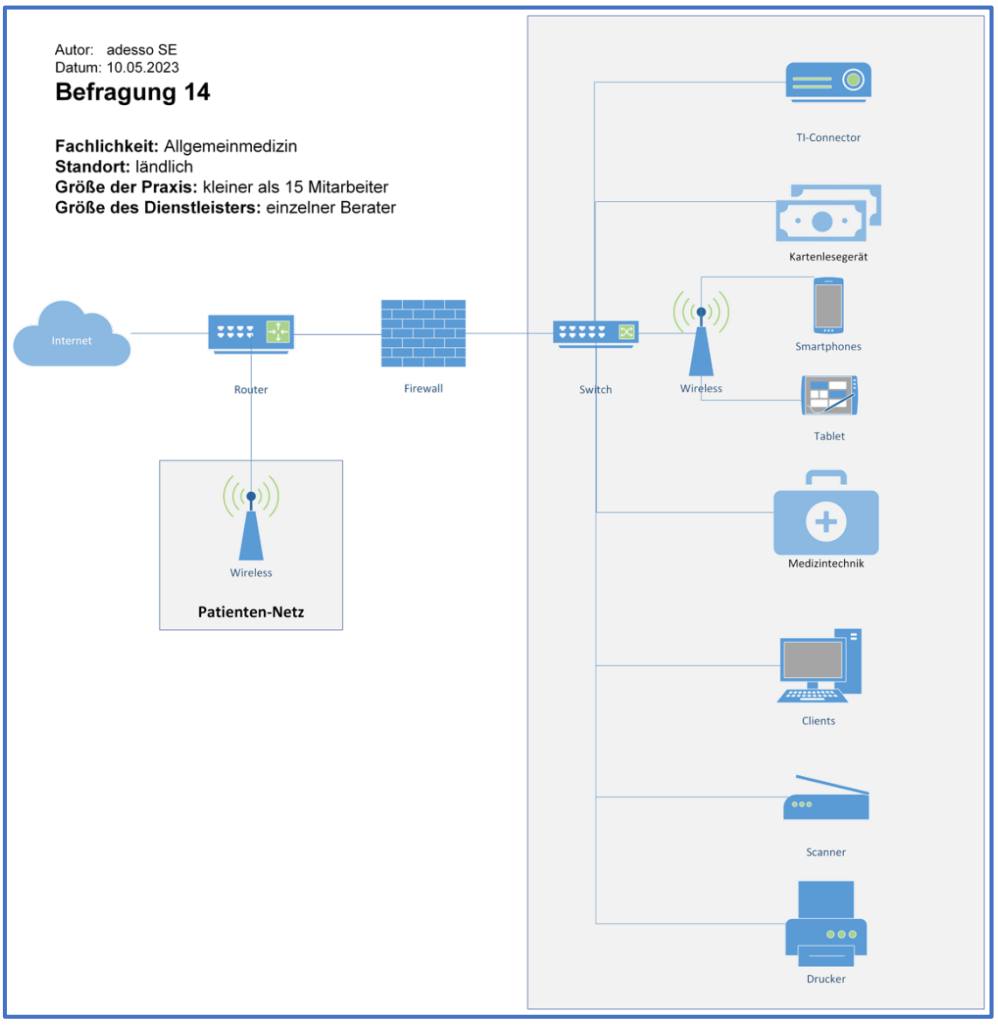

Autor: adesso SE
Datum: 13.02.2023
Befragung 9
Fachlichkeit: Allgemeinmedizin
Standort: ländlich
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: einzelner Berater
Internet
Router
VPN Gateway
Firewall/IDS/
IDP
Switch
Wireless
TI-Connector
Kartenlesegerät
Smartphones
Medizintechnik
Server (Linux)
Clients

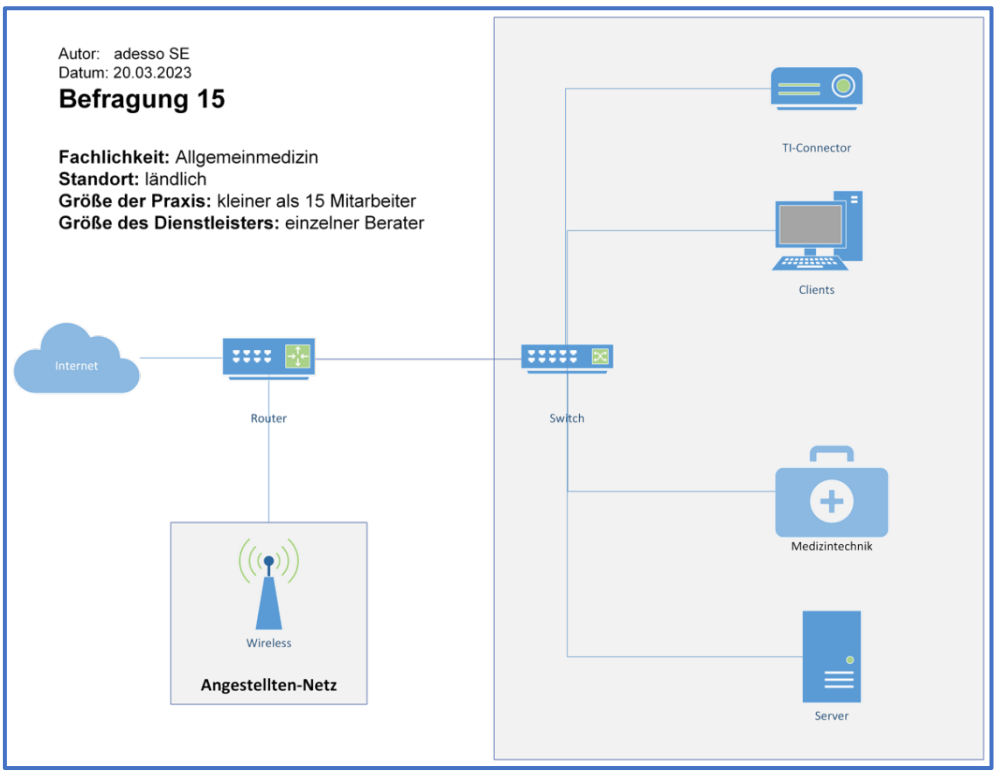

Autor: adesso SE
Datum: 21.02.2023
Befragung 10
Fachlichkeit: Radiologie
Standort: ländlich
Größe der Praxis: größer als 15 Mitarbeiter
Größe des Dienstleisters: kleiner als 15 Mitarbeiter
Internet
Router
Firewall/IDS/ IDP
Switch
TI-Connector
Kartenlesegerät
Medizintechnik
Server (5 Stück)
Clients
Alarmanlage
Drucker
Scanner

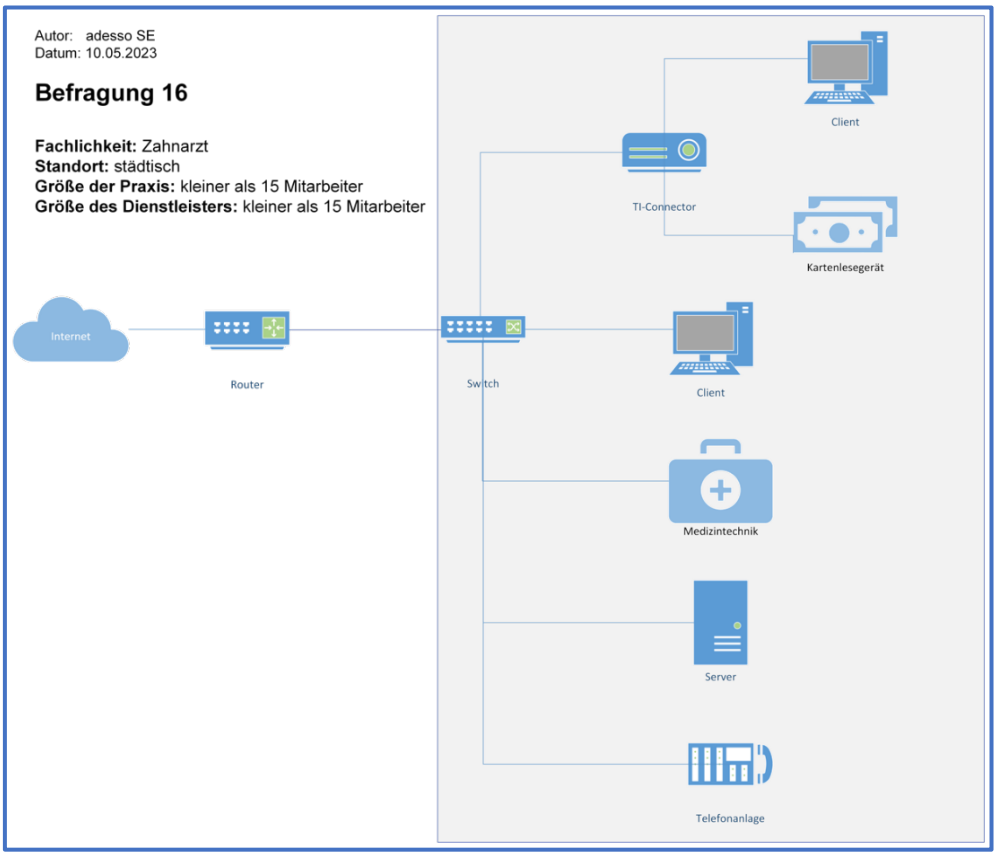

Autor: adesso SE
Datum: 13.02.2023
Befragung 11
Fachlichkeit: Allgemeinmedizin
Standort: ländlich
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: einzelner Berater
Internet
Router
Firewall/IDS/ IDP
DGN GUSbox
TI-Connector
Kartenlesegerät
(mobile) Clients
Medizintechnik
Server (PVS)
VPN Gateway
Terminalserver / Jumphost
Außenfilialen
Ärzte-WLAN


Autor: adesso SE
Datum: 14.03.2023
Befragung 12
Fachlichkeit: Allgemeinmedizin
Standort: ländlich
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: einzelner Berater
Internet
Router
Firewall/IDS/ IDP
Switch
Wireless
TI-Connector
Kartenlesegerät
Smartphones
Medizintechnik
Server (Windows)
Clients
Drucker
VPN Gateway


Autor: adesso SE
Datum: 19.04.2023
Befragung 13
Fachlichkeit: Psychotherapie
Standort: ländlich
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: kleiner als 15 Mitarbeiter
Internet
Router
Firewall/IDS/ IDP
Switch
Wireless
Smartphones
TI-Connector
Kartenlesegerät
Medizintechnik
mobile Clients
Virtual Machine (2 Stück)
Wireless
Patienten-Netz
VPN Gateway


Autor: adesso SE
Datum: 10.05.2023
Befragung 14
Fachlichkeit: Allgemeinmedizin
Standort: ländlich
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: einzelner Berater
Internet
Router
Firewall
Switch
Wireless
TI-Connector
Kartenlesegerät
Smartphones
Tablet
Medizintechnik
Clients
Scanner
Drucker
Wireless
Patienten-Netz


Autor: adesso SE
Datum: 20.03.2023
Befragung 15
Fachlichkeit: Allgemeinmedizin
Standort: ländlich
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: einzelner Berater
TI-Connector
Clients
Internet
Router
Switch
Medizintechnik
Wireless
Angestellten-Netz
Server


Autor: adesso SE
Datum: 10.05.2023
Befragung 16
Fachlichkeit: Zahnarzt
Standort: städtisch
Größe der Praxis: kleiner als 15 Mitarbeiter
Größe des Dienstleisters: kleiner als 15 Mitarbeiter
Client
TI-Connector
Kartenlesegerät
Internet
Router
Switch
Client
Medizintechnik
Server
Telefonanlage

11 Anhang: Fragebogen

Fragebogen zur Cybersicherheit in Arztpraxen

Ihre Praxis

Wie viele Beschäftigte hat Ihre Praxis (inkl. Ärzte)? 0

Wie viele Ärzte sind in Ihrer Praxis tätig? 0

Wie viele Beschäftigte arbeiten regelmäßig mit EDV-Systemen? 0

Wie viele Patienten behandeln Sie ca. pro Jahr? 0

Wie groß ist ihr Patientenstamm? 0

Wie lautet die PLZ ihrer Praxis? 0

Würden Sie Ihre Praxis als städtische oder ländliche Praxis bezeichnen?
☐ Städtisch
☐ Ländlich

Ist Ihre Praxis über mehrere Standorte verteilt?
☐ Nein
☐ Ja, über 0 Standort(e)

In welchem Fachbereich ist Ihre Praxis tätig?
☐ Hausarztpraxis ☐ Zahnarztpraxis ☐ Psychotherapeutische Praxis ☐ Radiologische Praxis

Wer ist für die IT in Ihrer Praxis zuständig? (Z.B. interner Mitarbeiter, Dienstleister, Bekannter)

Ist die IT-Verantwortliche Person / der IT-Dienstleister speziell ausgebildet bzw. der IT-Dienstleister besonders zertifiziert (z.B. ISO 27001, Herstellerzertifizierung), wenn ja, wie?

Gibt es Dienstleister/Externe IT-Verantwortliche mit (temporären) Zugriffsmöglichkeiten auf Patientendaten?
☐ Ja
☐ Nein

Wenn ja, wie viele? 0

Fragebogen zur Cybersicherheit in Arztpraxen

Dienstleister 1

Wie viele Angestellte hat ihr IT-Dienstleister ca.? 0

Wodurch hat ihr IT-Dienstleister die Kompetenz für die Administration der Systeme in Arztpraxen (Schulungen, Zertifizierungen, private Erfahrungen, Schule, Projekte in X Arztpraxen (x= 5, 10, 100, 500, 1000))?

Wie viele Praxen betreut der Dienstleister?

Hat Ihre Praxis mit diesen Dienstleistern bzw. externen IT-Verantwortlichen Verträge zur Auftragsdatenverarbeitung?
- ☐ Ja
- ☐ Nein
- ☐ Teilweise
- ☐ Unbekannt

Werden Patientendaten an Dienstleister/Externe IT-Verantwortliche übermittelt? (Z.B. für Backups, Fehlersuche oder die Weiterverarbeitung)
- ☐ Ja
- ☐ Nein

Wenn ja, gibt es eine Rechtsgrundlage für die Übermittlung der Daten?
- ☐ Ja
- ☐ Nein
- ☐ Nicht bekannt

War die Gewährleistung der Informationssicherheit ein Kriterium bei der Auswahl des IT-Dienstleisters?
- ☐ Ja
- ☐ Nein

Verfügt der Dienstleister oder externe IT-Verantwortliche über definierte technische und organisatorische Maßnahmen (TOMs), die einen geeignetes Schutzniveau der Daten erwarten lassen?
- ☐ Ja
- ☐ Nein
- ☐ Nicht bekannt

Haben Dienstleister oder externe IT-Verantwortliche Remote-Zugriff auf die Systeme der Praxis?
- ☐ Ja
- ☐ Nein
- ☐ Unbekannt

Fragebogen zur Cybersicherheit in Arztpraxen

Wenn ja, wie ist der Remote-Zugriff realisiert?

Dienstleister 2 (sofern vorhanden)

Wie viele Angestellte hat ihr IT-Dienstleister ca.? 0

Wodurch hat ihr IT-Dienstleister die Kompetenz für die Administration der Systeme in Arztpraxen (Schulungen, Zertifizierungen, private Erfahrungen, Schule, Projekte in X Arztpraxen (x= 5, 10, 100, 500, 1000))?

Wie viele Praxen betreut der Dienstleister?

Hat Ihre Praxis mit diesen Dienstleistern bzw. externen IT-Verantwortlichen Verträge zur Auftragsdatenverarbeitung?
- ☐ Ja
- ☐ Nein
- ☐ Teilweise
- ☐ Unbekannt

Werden Patientendaten an Dienstleister/Externe IT-Verantwortliche übermittelt? (Z.B. für Backups, Fehlersuche oder die Weiterverarbeitung)
- ☐ Ja
- ☐ Nein

Wenn ja, gibt es eine Rechtsgrundlage für die Übermittlung der Daten?
- ☐ Ja
- ☐ Nein
- ☐ Nicht bekannt

War die Gewährleistung der Informationssicherheit ein Kriterium bei der Auswahl des IT-Dienstleisters?
- ☐ Ja
- ☐ Nein

Verfügt der Dienstleister oder externe IT-Verantwortliche über definierte technische und organisatorische Maßnahmen (TOMs), die einen geeignetes Schutzniveau der
- ☐ Ja
- ☐ Nein
- ☐ Nicht bekannt

Fragebogen zur Cybersicherheit in Arztpraxen

Daten erwarten lassen?

Haben Dienstleister oder externe IT-Verantwortliche Remote-Zugriff auf die Systeme der Praxis?

- ☐ Ja
- ☐ Nein
- ☐ Unbekannt

Wenn ja, wie ist der Remote-Zugriff realisiert?

Praxisspezifische Systeme

Welches Praxisverwaltungssystem (PVS) setzen Sie ein?

Wie ist die Architektur des Praxisverwaltungssystems (zentraler Server im lokalen Netzwerk, Cloud, Einzelplatzinstallation, Tablets)?

Kann es vorkommen, dass ein Patient Zugang zu einem ungesperrten PC hat?

Bitte beschreiben Sie den Arbeitsablauf, der beginnt, wenn der Patient in den Behandlungsraum geführt wird. Insbesondere soll beschrieben werden, wann der Patient sich allein im Raum aufhält und wann Patientendaten aus dem PVS aufgerufen werden.

Fragebogen zur Cybersicherheit in Arztpraxen

Falls ein zentraler Server eingesetzt wird: Wie ist der Zugriff auf den PVS-Dienst freigegeben und wie ist die Authentisierung realisiert? (z.B. SMB, Dateifreigabe mit Vollzugriff für „Jeder“)

Setzen Sie weitere Software mit Verarbeitung von Patientendaten ein? Wenn ja, welche Art von Software (z.B. für Studien, digitale Anamnesebögen, Archivsysteme)?

Setzen Sie ein Terminvergabesystem (CGM life eServices, doctolib, Samedi, m.Doc, Formular auf Webseite) ein? Wenn ja, wie ist dieses an Ihre Praxis angebunden? (Anfragen per E-Mail, Schnittstelle zum PVS, Dateidownload z.B. FTP). Wie ist diese Anbindung abgesichert?

Ist jedem Nutzer ein eigenes Benutzerkonto im Terminvergabesystem zugeordnet?
Wenn ja, wer verwaltet die Benutzer?
Wenn nein, wie viele Personen kennen die Anmeldedaten des Nutzers?
Gibt es ehemalige Angestellte, die immer noch Zugriff auf das Terminvergabesystem haben?

Setzen Sie Systeme für Onlinerezepte oder Befundanfrage (CGM life eServices, doctolib, Samedi, m.Doc, Formular auf Webseite) ein? Wenn ja, wie ist dieses an Ihrer Praxis angebunden? (Anfragen per E-Mail, Schnittstelle zum PVS, Dateidownload z.B. FTP)

Fragebogen zur Cybersicherheit in Arztpraxen

Ist jedem Nutzer ein eigenes Benutzerkonto im System für Onlinerezepte oder Befundanfrage zugeordnet? Wenn ja, wer verwaltet die Benutzer?

Setzen Sie Systeme für Online Video-Sprechstunden (Sprechstunde.Online, Doccura, Elvi) ein? Wenn ja, tauschen Sie dabei auch Dateien aus?

Nutzen Sie darüber hinaus Dienste bzw. Mittel zur Patientensteuerung in Ihrer Praxis? Bspw. intelligente Telefonanlage, zentraler Terminkalender? Wenn ja, welche?

Architektur Ihres Netzwerks

Welche Geräte sind in Ihr Netzwerk eingebunden?
(Z.B. Desktops, Smartphones, Tablets, Gebäudetechnik in Form von Alarmanlagen, Türöffnern, Heizthermostaten, Medizintechnik, Smart Speaker wie Alexa etc., EC-Kartenlesegeräte, Server, TI-Konnektor)

Sind private Geräte Ihrer Mitarbeiter ins Netzwerk eingebunden (Bring Your Own Device)? Wenn ja, wie?

Fragebogen zur Cybersicherheit in Arztpraxen

Ist das Netzwerk in verschiedene Netze aufgeteilt? Wenn ja, in welche?
(z.B. Patienten W-LAN, Server-Netz, Med.-Geräte Netz)

Ist im Netzwerk eine Netzwerkzugangskontrolle (NAC) implementiert? (z.B. MAC-Filter, Authentisierung per Zertifikat)

Gibt es Geräte, die Sie außerhalb der Arztpraxis (räumlich definiert) nutzen und die mit den Systemen innerhalb der Praxis verbunden sind (Laptops, Tablets, Mobiltelefone etc.)? Wenn ja, welche?

Wenn „Ja“: Können Sie beschreiben, wie und ob die Kommunikation dieser Geräte geschützt ist? (Z.B. VPN, PVS, unbekannt)

Gibt es Dienste/offene Ports, die Sie ins Internet freigeben? Wenn ja, welche? (Z.B. VPN, SIP & VoIP, PVS, RDS, File-Share)

Fragebogen zur Cybersicherheit in Arztpraxen

Ist Ihre Praxis mit anderen Netzen, z.B. per VPN, verbunden? (Z.B. VPN, Wartungsverbindungen zu Hersteller, TI, PVS)

Arbeiten Sie oder Ihre Mitarbeiter aus dem Homeoffice oder mobil? Wenn ja, wie greifen jene auf Daten aus dem Praxisnetzwerk zu?

Wie sind die Praxisgeräte ans Internet angebunden? (Z.B. über Proxy, TI, direkt über lokalen Router)

Gibt es ein W-LAN für Patienten? ☐ Ja. ☐ Nein

Sind Sie an die Telematikinfrastruktur angebunden? ☐ Ja. ☐ Nein

Sind Sie an andere Dienste wie KV-Safenet angebunden? ☐ Ja. ☐ Nein

Welche Geräte sind über den TI-Konnektor und die Telematikinfrastruktur ans Internet angebunden?

Gibt es Geräte, die über einen lokalen Router, parallel zum TI-Konnektor, ans Internet angebunden sind? Wenn ja, welche?

Fragebogen zur Cybersicherheit in Arztpraxen

Sicherheitsvorkehrungen im Netzwerk

Welche Sicherheitssysteme sind in Ihrem Netzwerk installiert?

- ☐ Firewall, Hersteller _____
- ☐ Intrusion Detection System (IDS)
- ☐ Intrusion Prevention System (IPS)

Falls Firewall/IDS/IPS vorhanden, wie werden Alarme ausgewertet?

Endgerätesicherheit

Wie viel Prozent ihrer Endgeräte sind durch die folgende Maßnahme geschützt?

Zentral Verwaltete Antivirensoftware	0 %
Standard-Antivirensoftware	0 %
Zentrale Verwaltung (Z.B. MDM, Lokales Active Directory)	0 %
Cloudbasierte Verwaltung (Z.B. Intune, Azure AD)	0 %
GPO-Richtlinien / technisch durchgesetzte Policies	0 %
Festplattenverschlüsselung	0 %
Patch- und Updatemanagement	0 %

Wie wird das Patch- und Updatemanagement umgesetzt?

Fragebogen zur Cybersicherheit in Arztpraxen

Ihre weiteren Maßnahmen zur Endgerätesicherheit:

Sicherheit Medizinischer Geräte

Wie viel Prozent Ihrer medizinischen IT-Geräte sind durch die folgende Maßnahme geschützt?

Antivirensoftware	0 %
Zentrale Verwaltung (Z.B. MDM, Active Directory)	0 %
GPO-Richtlinien / technisch durchgesetzte Policies	0 %
Festplattenverschlüsselung	0 %
Weitere: _____	0 %
Patch- und Updatemanagement	0 %

Gibt es Geräte, die nicht aktualisiert werden? Wenn ja, welche und weshalb?

Fragebogen zur Cybersicherheit in Arztpraxen

Physische Sicherheit

Gibt es einen dedizierten Server? Wenn nein, auf welchem System läuft der PVS-Server?

Befinden sich Server in abgeschlossenen Schränken/Räumen?

Sind IT-Systeme in Räumen, in denen sich Patienten aufhalten, besonders vor physischer Manipulation geschützt? Wenn ja, wie? (Z.B. USB-Schnittstellen deaktiviert, Rechner verschlossen)

Befinden sich Netzwerkanschlüsse in Räumen, in denen Patienten sich ohne das Praxispersonal aufhalten dürfen? Wenn ja, sind diese in einem separaten Netzwerk, mit geringerem Zugriff?

Haben außer Ihren Mitarbeitern weitere Personen außerhalb der Dienstzeit Zutritt zu den Räumlichkeiten der Praxis? (Z.B. Gebäudeverwalter, Reinigungskraft, Dienstleister) Wenn ja, wie ist die Zutrittskontrolle geregelt?

Fragebogen zur Cybersicherheit in Arztpraxen

Wie sind Clients außerhalb der Dienstzeit geschützt? (z.B. Bildschirm sperren, Herunterfahren)

Organisatorische Sicherheit

Gibt es jemanden in Ihrer Praxis, der sich mit den Vorgaben zum Datenschutz beschäftigt?

☐ Ja
☐ Nein

Gibt es jemanden in Ihrer Praxis, der sich mit den Vorgaben zur Informationssicherheit beschäftigt?

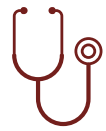
☐ Ja
☐ Nein

Gibt es eine Dokumentation der Geräte Ihrer Praxis, inklusive ihrer Konfiguration, ihrer Position im Netzwerk und ihren Kommunikationsbeziehungen?

☐ Ja
☐ Nein
☐ Teilweise

Wer ist für Informationssicherheit/Datenschutz zuständig? Sind beide Aufgaben in einer Person gebündelt oder verteilt auf mehrere? Wie sind die zuständigen Personen für ihre Aufgabe geschult?
(Z.B. Leistungserbringer, MFA, weitere Angestellte, Dienstleister)

Kennen Sie die Rechtgrundlage für die Erhebung bzw. Verarbeitung der Patientendaten und damit nötige Schutzanforderungen?



Fragebogen zur Cybersicherheit in Arztpraxen

Betreiben Sie ein ISMS (Information Security Management System)?

Bieten Sie Awareness-Schulungen für Ihre Mitarbeiter an? Wenn ja, sind diese verpflichtend?

Haben Sie eine Passwort-Richtlinie? Wenn ja, wie sieht diese aus? Wird sie technisch durchgesetzt?
Haben Sie sich mit sicheren Passwörtern auseinandergesetzt?

Haben Sie eine Backup-Strategie? Wenn ja, wie sieht diese aus?

Testen Sie regelmäßig die Funktionsfähigkeit Ihrer Backups? Wenn ja, wie oft?

Fragebogen zur Cybersicherheit in Arztpraxen

Woher beziehen Sie Ihre Programme/Anwendungen/Apps? (Z.B. offizielle AppStores (Apple/Google/Microsoft); offizielle Programmherstellerseiten; weitere vertrauensvolle Quellen)

Wie tauschen Sie Patientendaten mit anderen Institutionen oder Patienten aus? (Fax, E-Mail, KIM, Webportal, Portale von KH, Radiologieverbund)

Werden die Daten verschlüsselt? Wenn ja, wie übertragen Sie das Geheimnis für die Verschlüsselung?

Schließen Sie Geräte oder Medien Ihrer Patienten an Ihre Systeme an? Z.B. USB-Sticks, CDs, Röntgenbilder, Speicherkarten, Medizingeräte?

Wie empfangen Sie Laborergebnisse oder Röntgenbilder von Dritten?

Fragebogen zur Cybersicherheit in Arztpraxen

Benutzer und Berechtigungen

Ist jedem EDV-Mitarbeiter eine persönliche Benutzerkennung im PVS zugeordnet? (Auch Auszubildenden, MFA, Ärzten) Wenn nein, weshalb nicht?

Halten Sie es für sinnvoll, wenn es unterschiedliche Rechte für Ärzte und Mitarbeiter in Praxisverwaltungssystemen gibt?

Ist jedem EDV-Mitarbeiter eine persönliche Benutzerkennung in den Praxis-Computern zugeordnet?

Arbeitet in der Praxis jeder Mitarbeiter ausschließlich unter seiner eigenen Kennung?

Wie authentisieren sich die Nutzer an den IT-Systemen? (Alle zutreffenden ankreuzen)

☐ Nutzername/Passwort ☐ Token ☐ Biometrie ☐ Andere: _____

Fragebogen zur Cybersicherheit in Arztpraxen

Nutzen Sie eine Multi-Faktor-Authentisierung? [ ] Ja [ ] Nein

Sind den Mitarbeitern Rollen zugeordnet, die keine weiteren Befugnisse haben, als die sie für Ihre Tätigkeitsausübung benötigen?

Weitere Anmerkungen:

12 Anhang: Matrix – Schwachstellen/Praxis

Die Verteilung der Schwachstellen über alle Praxen ist in der folgenden Tabelle dargestellt:

Nr.	Feststellung	Praxis 1	Praxis 2	Praxis 3	Praxis 4	Praxis 5	Praxis 6	Praxis 7	Praxis 8	Praxis 9	Praxis 10	Praxis 11	Praxis 12	Praxis 13	Praxis 14	Praxis 15	Praxis 16
1	PC mit angemeldetem Account						x			x	x			x	x		x
2	Sensible Daten auf externen Geräten		x	x		x			x	x				x	x		
3	Unzureichende Betrachtung der DSGVO-Anforderungen			x		x						x			x		x
4	Fehlende Funktionstests der Backups		x		x		x	x	x	x		x	x	x	x	x	x
5	Unzureichende Awareness Schulungen	x	x	x	x	x		x		x		x	x		x	x	x
6	Unsichere Entsorgung von IT-Geräten	x															
7	Unzureichender Virenschutz	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
8	Unzureichende Verschlüsselung	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
9	Unverschlüsselte Backups					x											x
10	Ungesicherte Netzwerkdosen öffentlich zugänglich		x				x					x	x	x	x		
11	Verwendung fremder Datenträger						x	x	x		x	x			x		x
12	Unzureichendes Berechtigungsmanagement			x	x	x			x						x	x	
13	Unsichere Anwendungen													x			
14	Unzureichendes IT-Know-how					x								x	x	x	
15	Ungesicherte Medizintechnik		x		x	x		x		x	x	x	x	x	x	x	x
16	Unzureichendes Patch- und Updatemanagement		x		x	x	x	x	x	x	x	x	x	x	x	x	
17	Keine zentrale Verwaltung für IT-Systeme		x	x	x	x	x	x	x				x		x	x	x
18	Unzureichende Dokumentation der Infrastruktur	x		x		x		x			x	x	x	x	x	x	x
19	Potenziell unsichere Passwörter			x	x	x		x	x	x		x	x		x	x	
20	Privatgeräte im Netzwerk			x	x	x		x		x					x		
21	Fehlende Segmentierung	x					x		x	x			x				x
22	Parallelbetrieb TI-Konnektor	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	X
22	Gemeinsam benutzte User-Konten	x			x							x			x	x	
23	Unverschlüsselte E-Mail-Kommunikation											x		x	x		
24	Fehlende Strukturierung der Informationssicherheit	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
25	Unsichere Netzwerkkonfiguration			x	x	x		x		x	x	x	x	x	x	x	x

13 Anhang: Checkliste für Arztpraxen

1. Benutzerkonten- und Zugriffsmanagement:

- Implementieren Sie automatische Bildschirmsperren nach einer bestimmten Zeit (3–5 Minuten) der Inaktivität auf allen PCs.
- Ermutigen Sie die Benutzer, ihre PCs zu sperren, wenn sie ihren Arbeitsplatz verlassen.
- Implementieren Sie eine strikte Ein-Benutzer-pro-Konto-Richtlinie, um die Nachvollziehbarkeit zu gewährleisten und im Falle eines Sicherheitsvorfalls gezielte Maßnahmen ergreifen zu können.
- Implementieren Sie ein Rollen- und Berechtigungskonzept, das auf dem Prinzip der minimal notwendigen Berechtigungen basiert, bei dem jedem Benutzer nur die für seine Arbeit unbedingt erforderlichen Rechte gewährt werden.
- Führen Sie regelmäßig Sicherheitsschulungen für das Personal durch, um das Bewusstsein für die Risiken und die Bedeutung der Datensicherheit zu erhöhen.
- Implementieren Sie eine Richtlinie für das Homeoffice, die das Speichern sensibler Daten auf persönlichen Geräten verbietet.
- Implementieren Sie strenge Passwortrichtlinien, die eine ausreichende Länge und Komplexität erfordern. Vermeiden Sie Standardpasswörter und setzen Sie eine Mindestlänge von 20–25 Zeichen für Wortfolgen und 8–12 Zeichen für Passwörter mit erweiterten Zeichenarten durch. Erhöhen Sie die Kontosicherheit durch die Verwendung einer Zwei-Faktor-Authentisierung.

2. Sicherheit von IT-Systemen und Netzwerken:

- Die Einrichtung und Konfiguration der IT-Systeme sollten durch einen professionellen, zertifizierten Dienstleister durchgeführt werden.
- Bei der Inbetriebnahme von Geräten sollten Standardpasswörter umgehend geändert werden, um einen verbesserten Schutz gegen unbefugten Zugriff zu gewährleisten.
- Es ist notwendig, medizintechnische Geräte in ein eigenständiges Netzwerksegment zu übertragen, welches mit spezifischen Schutzmechanismen und Firewall-Regeln ausgestattet ist. Private Geräte müssen von diesem Netzwerksegment ferngehalten werden und dürfen lediglich in separaten Netzwerken zugelassen sein.
- Eine zentralisierte Virenschutzlösung, die eine kontinuierliche Überwachung der Systeme ermöglicht und die Aktualität der Konfigurationsdateien sicherstellt, sollte implementiert werden.
- Um Daten zu schützen, selbst wenn der physische Datenträger gestohlen oder kompromittiert wird, sollte eine vollständige Festplattenverschlüsselung auf allen IT-Systemen durchgeführt werden.
- Ein regelmäßiges und strukturiertes Patch- und Update-Management sollte implementiert werden, um alle Systeme, einschließlich medizintechnischer Geräte, auf dem neuesten Stand zu halten und bekannte Sicherheitslücken zu schließen.
- Der Netzwerkzugriff sollte über Intrusion Detection Systeme (IDS) oder Intrusion Prevention Systeme (IPS) sowie dedizierte Firewalls kontrolliert werden.
- Der Zugriff auf öffentliche Ports sollte zusätzlich über eine dedizierte Firewall abgesichert werden. Dabei ist eine korrekte Konfiguration sehr entscheidend.
- Insbesondere für größere Praxen sollte eine zentrale Verwaltung der IT-Systeme implementiert werden.

- Um Schwachstellen besser einschätzen zu können, sollte die Infrastruktur ausreichend dokumentiert werden.
- Es wird dringend empfohlen, dass Sie qualifizierte IT-Fachleute beauftragen, um bestehende Lösungen für die Speicherung und Verarbeitung von Patientendaten zu evaluieren und zu implementieren. Dies minimiert das Sicherheitsrisiko und stellt sicher, dass die Verfahren korrekt durchgeführt werden.

3. Datenschutz und Compliance:

- Löschen Sie alle Datenträger vollständig und unwiederbringlich mit zertifizierten Datenlöschverfahren, bevor Sie ein Altgerät ausmustern.
- Ziehen Sie die physische Vernichtung von Datenträgern in Betracht, um einen zusätzlichen Schutz gegen Datenmissbrauch zu bieten. Nutzen Sie dazu gegebenenfalls einen professionellen Dienstleister.
- Führen Sie spezialisierte Schulungen zu Datenschutzthemen und DSGVO-Vorschriften für alle Mitarbeiter durch.
- Prüfen Sie alle Verträge mit Dienstleistern sorgfältig und fügen Sie entsprechende Klauseln zur Auftragsdatenverarbeitung hinzu, um die Einhaltung der DSGVO sicherzustellen.

4. IT-Kenntnisse und Bewusstsein:

- Stellen Sie sicher, dass nur qualifizierte IT-Fachleute für die Einrichtung und Konfiguration der Systeme verantwortlich sind.
- Stellen Sie sicher, dass regelmäßige Fortbildungen und Schulungen durchgeführt werden, um das technische Wissen der Mitarbeiter aktuell zu halten, diese über die neuesten Sicherheitsvorschriften zu informieren und ein Bewusstsein für IT-Sicherheitsthemen zu schaffen.

5. E-Mail- und Kommunikationssicherheit:

- Senden Sie Patientendaten immer verschlüsselt per E-Mail. Die privaten Schlüssel für die Verschlüsselung sollten sicher verwaltet werden.

6. Zusätzliche Sicherheitsmaßnahmen:

- Implementieren Sie einen strukturierten Ansatz für Informationssicherheitsthemen.
- Verwenden Sie ein Logging- und Monitoring-Konzept, um Angriffe besser erkennen und nachverfolgen zu können.

13.1 Onepager

1. Benutzerkonten- und Zugriffsmanagement:

- ☐ Bildschirmsperren bei Inaktivität auf allen PCs aktiviert.
- ☐ Benutzer aufgefordert, den PC beim Verlassen zu sperren.
- ☐ Ein-Benutzer-pro-Konto-Richtlinie umgesetzt.
- ☐ Rollen- und Berechtigungskonzept, mit minimal notwendigen Berechtigungen, umgesetzt.
- ☐ Sicherheitsschulungen für das Personal durchgeführt.
- ☐ Homeoffice-Richtlinie umgesetzt.
- ☐ Ausreichende Passwortrichtlinie definiert und erzwungen.

2. Sicherheit von IT-Systemen und Netzwerken:

- ☐ Professionelle Prüfung der Konfiguration der IT-Systeme durchgeführt.
- ☐ Standardkennwörter geändert.
- ☐ Eigenes Netzwerk mit Firewall-Regeln für Medizintechnik umgesetzt.
- ☐ Zentralisierte Virenschutzlösung implementiert.
- ☐ Alle Festplatten sind verschlüsselt.
- ☐ Patch- und Update-Management geplant und umgesetzt.
- ☐ IDS und IPS sind im Einsatz und konfiguriert.
- ☐ Öffentliche Ports sind über eine dedizierte Firewall abgesichert.
- ☐ Zentrale Verwaltung der IT-Systeme implementiert.
- ☐ Dokumentation der Infrastruktur vollständig.
- ☐ Lösungen zur Speicherung und Verarbeitung von Patientendaten evaluiert und implementiert.

3. Datenschutz und Compliance:

- ☐ Prozess zur unwiederbringlichen Löschung von Datenträgern bei Ausmusterung besteht.
- ☐ Notwendigkeit der Vernichtung von Datenträgern geprüft.
- ☐ Spezialisierte Schulungen zu Datenschutzthemen und DSGVO-Vorschriften durchgeführt.
- ☐ Alle Verträge auf DSGVO-Konformität geprüft und ggf. ergänzt.

4. IT-Kenntnisse und Bewusstsein:

- ☐ Verantwortung für IT-Systeme an qualifizierte IT-Fachleute übergeben.
- ☐ Fortbildungs- und Schulungsplan für Mitarbeiter definiert.

5. E-Mail- und Kommunikationssicherheit:

- ☐ Sichere E-Mail-Verschlüsselung umgesetzt.

6. Zusätzliche Sicherheitsmaßnahmen:

- ☐ Strukturierter Ansatz für Informationssicherheitsthemen implementiert.
- ☐ Logging- und Monitoring-Konzept evaluiert und umgesetzt.

CyberPraxMed – Cyber-Sicherheit in Arztpraxen

Bundesamt für Sicherheit in der Informationstechnik

adesso business. people. technology.

DATATREE

14 Verweise

Bundesamt für Sicherheit in der Informationstechnik. (2023). *APP.5.3 Allgemeiner E-Mail-Client und -Server*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_5_3_Allgemeiner_E-Mail_Client_und_Server_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *APP.6 Allgemeine Software*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_6_Allgemeine_Software_Edition_2023.pdf?__blob=publicationFile&v=3#download=1 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *CON.1 Kryptokonzept*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_1_Kryptokonzept_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *CON.2 Datenschutz*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_2_Datenschutz_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *CON.3 Datensicherungskonzept*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *CON.6 Löschen und Vernichten*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *INF.8 Häuslicher Arbeitsplatz*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_8_Haeuslicher_Arbeitsplatz_Edition_2023.pdf?__blob=publicationFile&v=3#download=1 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *ISMS.1 Sicherheitsmanagement*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/01_ISMS_Sicherheitsmanagement/ISMS_1_Sicherheitsmanagement_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *NET.1.1 Netzarchitektur und -design*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_1_1_Netzarchitektur_und_design_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *NET.3.2 Firewall*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2023.pdf?__blob=publicationFile&v=4 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *NET.3.4 Network Access Control*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_3_4_Network_Access_Control_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *OPS.1.1.3 Patch- und Änderungsmanagement*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_1_1_3_Patch_und_Aenderungsmanagement_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *OPS.1.1.4 Schutz vor Schadprogrammen*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_1_1_4_Schutz_vor_Schadprogrammen_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *OPS.1.1.7 Systemmanagement*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_1_1_7_Systemmanagement_Edition_2023.pdf?__blob=publicationFile&v=4 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *ORP.3 Sensibilisierung und Schulung zur Informationssicherheit*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/02_ORP_Organisation_und_Personal/ORP_3_Sensibilisierung_und_Schulung_Editon_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *ORP.4 Identitäts- und Berechtigungsmanagement*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *SYS.1.1 Allgemeiner Server*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/07_SYS_IT_Systeme/SYS_1_1_Allgemeiner_Server_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *SYS.2.1 Allgemeiner Client*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/07_SYS_IT_Systeme/SYS_2_1_Allgemeiner_Client_Edition_2023.pdf abgerufen

Bundesamt für Sicherheit in der Informationstechnik. (2023). *SYS.4.5 Wechseldatenträger*. Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/07_SYS_IT_Systeme/SYS_4_5_Wechseldatentraeger_Edition_2023.pdf?__blob=publicationFile&v=3 abgerufen

Bundeskriminalamt, C. (2021). *Cybercrime: Bundeslagebild 2021*. Von https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf abgerufen

The MITRE Corporation. (2023). *CWE-1059: Insufficient Technical Documentation*. Von https://cwe.mitre.org/data/definitions/1059.html abgerufen

The MITRE Corporation. (2023). *CWE-1277: Firmware Not Updateable*. Von https://cwe.mitre.org/data/definitions/1277.html abgerufen

The MITRE Corporation. (2023). *CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer*. Von https://cwe.mitre.org/data/definitions/212.html abgerufen

The MITRE Corporation. (2023). *CWE-284: Improper Access Control*. Von https://cwe.mitre.org/data/definitions/284.html abgerufen

The MITRE Corporation. (2023). *CWE-306: Missing Authentication for Critical Function*. Von https://cwe.mitre.org/data/definitions/306.html abgerufen

The MITRE Corporation. (2023). *CWE-311: Missing Encryption of Sensitive Data*. Von https://cwe.mitre.org/data/definitions/311.html abgerufen

The MITRE Corporation. (2023). *CWE-358: Improperly Implemented Security Check for Standard*. Von https://cwe.mitre.org/data/definitions/358.html abgerufen

The MITRE Corporation. (2023). *CWE-521: Weak Password Requirements*. Von https://cwe.mitre.org/data/definitions/521.html abgerufen

The MITRE Corporation. (2023). *CWE-653: Improper Isolation or Compartmentalization*. Von https://cwe.mitre.org/data/definitions/653.html abgerufen

The MITRE Corporation. (2023). *CWE-657: Violation of Secure Design Principles*. Von https://cwe.mitre.org/data/definitions/657.html abgerufen

The MITRE Corporation. (2023). *CWE-693: Protection Mechanism Failure*. Von https://cwe.mitre.org/data/definitions/693.html abgerufen

The MITRE Corporation. (2023). *CWE-732: Incorrect Permission Assignment for Critical Resource*. Von https://cwe.mitre.org/data/definitions/732.html abgerufen

The MITRE Corporation. (2023). *CWE-841: Improper Enforcement of Behavioral Workflow*. Von https://cwe.mitre.org/data/definitions/841.html abgerufen