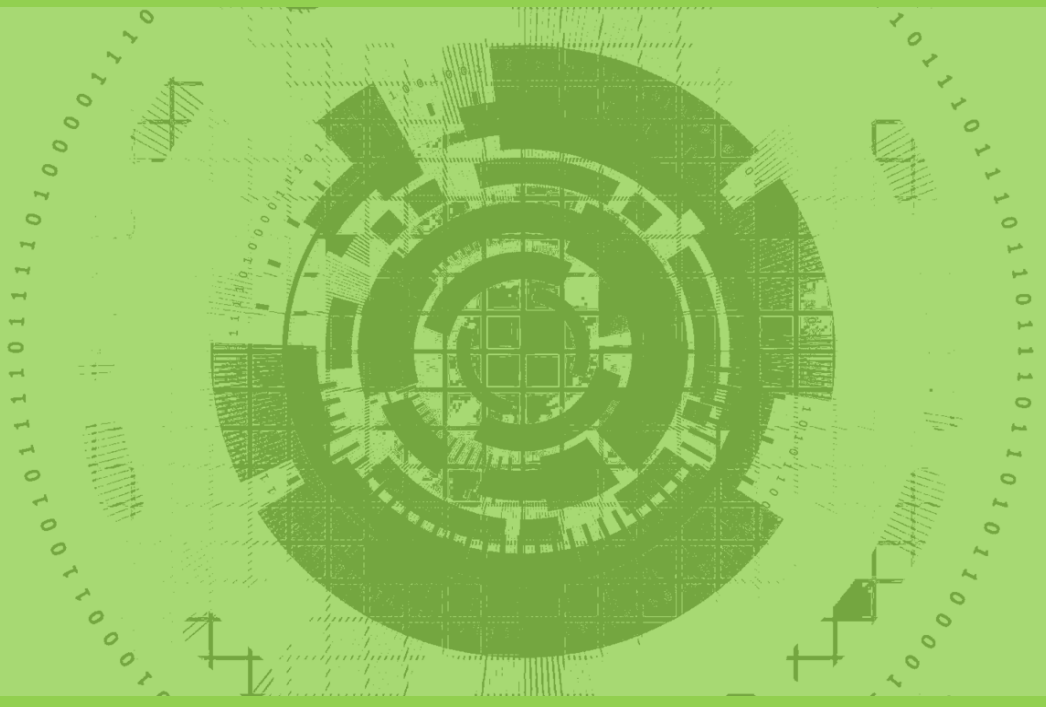
www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

6 Basics Cybersicherheit



Krankenhäuser

Wie schütze ich mein Krankenhaus?

Die technische Entwicklung im IT-Sektor in den letzten 25 Jahren ist enorm und hat auch im Gesundheitswesen zu völlig neuen Möglichkeiten geführt. Dies schließt die Bereiche Diagnostik und Pflege aber auch den Bereich der Verwaltung in den Krankenhäusern mit ein. Das ist eine erfreuliche Entwicklung, da durch den technischen Fortschritt die Effizienz und Qualität der zentralen Geschäftsprozesse eines Krankenhauses erheblich verbessert werden konnten. Es gibt jedoch auch eine dunkle Seite, die sich in den letzten Monaten zum Teil dramatisch manifestierte: Krankenhäuser wurden Opfer von Cyberangriffen.

Der Fortschritt im IT-Bereich erstreckt sich leider auch auf die Fähigkeiten von Angreifern und das technische Niveau von Schadcode. Dies ist insbesondere bei den negativen „Erfolgen“ von sogenannter Ransomware deutlich geworden: Über kriminelle Geschäftsmodelle wird die Weiterentwicklung der Angriffssoftware ständig verbessert. Das Zahlen von Lösegeld für verschlüsselte Dateien finanziert so möglicherweise den nächsten Angriff auf höherem technischem Niveau.

Sicherheitsmaßnahmen müssen in einem Wettlauf mit der Weiterentwicklung der Fähigkeiten von Angreifern und dem technischen Fortschritt stetig angepasst werden. Informationssicherheit muss daher als Prozess verstanden werden, der kontinuierliche Aufmerksamkeit und Fortschreibung erfordert. Die Komplexität und die Anzahl der unterschiedlichen IT-Systeme, die von einer IT-Abteilung in einem Krankenhaus betreut werden müssen, haben sich in den vergangenen Jahrzehnten deutlich erhöht. Medizintechnische Systeme, die früher als technische Insellösungen ihren Dienst verrichteten, müssen heute an die medizinischen Netzwerke der Krankenhäuser angebunden werden, um das geforderte Effizienzniveau zu erreichen.

Effiziente und effektive Geschäftsprozesse sind erforderlich, die sich zwangsläufig auch über die IT-Abteilungen der Krankenhäuser erstrecken müssen. Bei der Gestaltung dieser Geschäftsprozesse müssen die Ressourcen der Krankenhäuser individuell berücksichtigt werden. Sicherheitsprozesse müssen so gestaltet werden, dass sie eine kontinuierliche Fortentwicklung, auch unter Berücksichtigung der daraus resultierenden Kosten, fokussieren. Kurzfristige bzw. einmalige Investitionen in IT-Sicherheitslösungen werden nicht ausreichen, um dem technischen Fortschritt auch auf der Seite von Angreifern und Schadcode auf Dauer standzuhalten.

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

Es existieren viele branchenspezifische Umsetzungshinweise, Orientierungshilfen und Handlungsempfehlungen, z.B.

- Handlungsempfehlungen zur Verbesserung der Informationssicherheit an Kliniken vom 31. Mai 2017
- Krankenhäuser als kritische Infrastrukturen - Umsetzungshinweise der Deutschen Krankenhausgesellschaft (DKG) vom 19. Dezember 2017
- IT-Sicherheit: Allgemeine Grundsätze und Empfehlungen zum Informationssicherheitsmanagement von Universitätsklinika (VUD)
- Orientierungshilfe IT-Sicherheit in Kliniken des Bayerischen Landesamtes für Sicherheit in der Informationstechnik vom Oktober 2020
- Branchenspezifischer Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus der Deutschen Krankenhausgesellschaft (DKG) vom Oktober 2019
- Maßnahmenkatalog zur Verbesserung der IT-Sicherheit in Bayerischen Krankenhäusern des Forschungsprojektes Smart Hospitals der Universität der Bundeswehr München (Ausgabe 2020/2021 vom Juli 2021)

Darüber hinaus existiert (branchenübergreifend) das IT-Grundschutzkompendium des BSI, die ISO/IEC 27000er Normenreihe und nicht zuletzt der VdS 10000 Standard sowie CISIS12.
Wenn man nun alle diese z.T. sehr umfangreichen Umsetzungshinweise, Orientierungshilfen, Handlungsempfehlungen sowie die anerkannten Standards und Regelwerke auf sechs wesentliche Punkte reduziert, die den größtmöglichen Nutzen und Schutz gegen Cyberattacken bietet, dann sind dies erfahrungsgemäß nachstehende sechs Basics. Die große Mehrheit der Cyber-Angriffe kann durch diese Schritte verhindert oder deren Auswirkungen deutlich reduziert werden.

In diesem Leitfaden, der kontinuierlich gemäß der aktuellen technologischen Entwicklungen und neuster Erkenntnisse angepasst wird, stellt Ihnen der Cyber-Sicherheitsrat Deutschland e.V., mit freundlicher Unterstützung unseres Mitglieds AuraSec GmbH, die wichtigsten Maßnahmen vor.

Mit freundlichen Grüßen

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

Jan C. Arfwedson
Vorsitzender eHealth-Hub
Cyber-Sicherheitsrat Deutschland e.V.

1. Netzwerksegmentierung

In Krankenhäusern werden zahlreiche und völlig unterschiedliche IT-Systeme betrieben. Systeme der Medizintechnik, die früher noch allein und isoliert ihren Dienst verrichteten, müssen heute an die medizinischen Netzwerke angebunden werden, um den Anforderungen an Effizienz und Qualität im Bereich der Diagnostik und Pflege genügen zu können.

Der Lebenszyklus von vernetzten medizinischen Systemen ist zum Teil deutlich länger als der technische Innovationszyklus im Bereich der IT. In den Krankenhäusern ist teilweise noch Medizintechnik mit Betriebssystemen an Netzwerke angeschlossen, die in anderen Bereichen der IT schon längst zum „alten Eisen“ gehören. Solche Systeme können daher mit gefährlichen Schwachstellen behaftet sein, über die Angreifer oder Schadcode in das Netzwerk eindringen können. Der Betrieb von solchen Systemen in großen homogenen Netzwerken, gegebenenfalls „neben“ Systemen der Verwaltung, stellt ein erhebliches Risiko dar. Falls ein Schadcode auf einem System zur Ausführung gelangt, kann er sich über ungesicherte IT-Netzwerke möglicherweise weitläufig ausbreiten und weitere Systeme infizieren. Falls dazu auch medizintechnische Systeme gehören, kann auch die Sicherheit von Patienten und damit Leib und Leben gefährdet sein.

Um einen adäquaten Schutz der eigenen Infrastruktur zu ermöglichen, ist die Segmentierung des eigenen Netzes daher unabdinglich. Dazu ist es erforderlich, die Netzwerke zu segmentieren und über eine Firewall mit entsprechendem Regelwerk voneinander zu trennen. Nur legitime Daten dürfen von einem Netzwerk in das andere gelangen. Angreifern und Schadcode muss die Möglichkeit genommen werden, sich in weitere Netzwerke auszubreiten. Dabei ist die Schutzwirkung dieser Segmentierung umso größer, je kleiner die Segmente konzipiert werden. Gleichzeitig steigt damit jedoch auch der administrative Aufwand, der von Seiten der IT-Abteilung oder der beauftragten Dienstleister zu bewältigen sein wird. Dementsprechend ist ein angemessenes Verhältnis zwischen laufenden Kosten und Schutzwirkung durch die Segmentierung zu finden. Zwangsläufig erhöhen sich durch die Segmentierung der Netzwerke die Kosten für ein Krankenhaus. Diese Kosten erstrecken sich nicht allein auf eine einmalige Investition in eine Firewall-Infrastruktur. Die fortlaufende Aktualisierung der Firewall-Systeme sowie die Fortschreibung und kontinuierliche Anpassung des Regelwerks müssen ebenfalls berücksichtigt werden.

- ✓ **Trennung von medizintechnischen und Verwaltungsnetzwerken**
- ✓ **Anwendung von Firewalls**

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.

2. Zugangsmanagement

Im Bereich der Diagnostik und Pflege in einem Krankenhaus sind Effizienz und Geschwindigkeit kein rein betriebswirtschaftliches Ziel. Vielmehr geht es häufig auch darum, über Effizienz und Geschwindigkeit Leben zu retten. Dies betrifft insbesondere die Intensivmedizin oder die Notaufnahme.
Gleichzeitig muss sichergestellt werden, dass hochsensible medizinische Daten, nicht gegenüber Unbefugten offengelegt werden.
Dazu ist eine angemessene und effiziente Zugangskontrolle zu IT-Systemen erforderlich. Zwar können längere und komplexere Passwörter das Sicherheitsniveau deutlich verbessern, jedoch nimmt die Eingabe solcher Passworte auch mehr Zeit in Anspruch, wodurch sich gegebenenfalls die Behandlung von Patienten verzögert bzw. die Effizienz der Mitarbeitenden im medizinischen Bereich über einen längeren Zeitraum betrachtet sinkt.
Zugangssysteme sind erforderlich, die beidem gleichermaßen Rechnung tragen: Sicherheit und Effizienz.

- ✓ **Angemessene Zugangskontrollen**
- ✓ **Trennung von Admin- und Nutzerrollen**
- ✓ **Berechtigungskonzepte auch für Admins**
- ✓ **Network Access Control (NAC)**

3. Schwachstellen-Management und Penetrationtesting

Das Schwachstellen-Management muss im Rahmen des Vorfallmanagements geeignete Prozesse ermöglichen, um mit auftretenden oder bekannten Schwachstellen umzugehen – das Wissen um die Schwächen der eigenen Infrastruktur und der eingesetzten Systeme macht hier den Unterschied.

Dabei stellen die vernetzten Systeme der Medizintechnik eine besondere Herausforderung dar. Die Hersteller der Medizintechnik müssen über den gesamten Lebenszyklus eines vernetzten Medizinprodukts einbezogen werden. Es muss sichergestellt werden, dass die Hersteller von vernetzten Medizingeräten Schwachstellen in ihren Systemen erkennen und zeitnah Sicherheitsupdates bereitstellen.

Eine besondere Herausforderung ist ferner, dass es sich bei IT-Systemen in einem Krankenhaus, gerade auch im Bereich der Medizintechnik, um hochspezifische und allein für diesen Sektor entwickelte Produkte handelt. Zwar können Erkenntnisse über Schwachstellen von Standard-IT-Systemen oder Betriebssystemen aus typischen Datenbeständen dafür verwendet werden, Standardsysteme abzusichern, sie lassen sich bisweilen jedoch nur sehr begrenzt auf die hochspezifischen Systeme in einem Krankenhaus übertragen. Umso mehr ist es die Aufgabe der Hersteller, kontinuierlich zu überprüfen, ob die von ihnen entwickelten Systeme Schwachstellen aufweisen. Ein rein reaktives Vorgehen, das sich gegebenenfalls darauf beschränkt, eine Schwachstelle, die gegebenenfalls von Angreifern oder Schadcode bereits ausgenutzt wurde, zu schließen, kann in einem Krankenhaus nicht als ausreichend angesehen werden.

Krankenhäuser können ihrerseits einen Beitrag leisten, indem sie regelmäßig Penetrationstests über die von ihnen betriebenen Systeme durchführen lassen. Dabei muss idealerweise von den Penetrationstestern auch nach neuen noch unbekannten Schwachstellen gesucht werden.

- ✓ **Regelmäßige Schwachstellenscans**
- ✓ **Schwachstellenmanagement bei Herstellern von Medizintechnik**
- ✓ **Regelmäßige Penetrationstests**

4. Patchmanagement und Systemhärtung

Um Sicherheiten gewährleisten zu können muss die eigene Infrastruktur stets auf dem aktuellen Stand der Technik gehalten werden; dazu zählen sowohl Geräte als auch Software. Ältere Konfigurationen oder Softwareversionen werden (teilweise) nicht mehr unterstützt oder es können Sicherheitslücken auftreten. Besonders bei älteren Versionen von Software sind diese Schwachstellen oftmals direkt im Internet zu finden, mitsamt Leitfäden zur Ausnutzung.

Dies stellt ein besonderes Risiko für vernetzte Medizinprodukte dar. Falls auf der Basis von Standard-Softwareprodukten die hochspezifischen Funktionen der Medizinprodukte realisiert werden, besteht das Risiko, dass Medizinprodukte gleiche o.ä. Schwachstellen wie die verwendete Standardsoftware aufweisen. Durch die höhere Produktlebenszeit im Bereich der medizinischen Systeme kann eine Schwachstelle so gegebenenfalls die kürzeren Produktlebenszeiten der verwendeten Standardlösungen überschreiten.

Die Systeme in einem Krankenhaus müssen so ausgelegt sein, dass sie dem jeweiligen Anspruch an ihre Verfügbarkeit genügen können. In aller Regel erfordert eine Aktualisierung der Software die vorübergehende Außerbetriebnahme der jeweiligen Systeme. Die regelmäßige Aktualisierung der Software muss bereits bei der Systemkonzeption aber auch im Rahmen der Betriebskonzepte auf der Seite der Krankenhäuser berücksichtigt werden. Die Anwender müssen in der Lage sein, Wartungsfenster überbrücken zu können. Häufig wird von Seiten der Ärzteschaft für wichtige Systeme gefordert: „Das System muss immer verfügbar sein.“ Falls diesem Anspruch von Seiten einer IT-Abteilung in einem Krankenhaus Rechnung getragen wird, indem unsachgemäß auf regelmäßige erforderliche Systemaktualisierung verzichtet wird, resultiert gerade daraus das Risiko, dass solche Systeme bei einem Angriff kompromittiert werden, da Schwachstellen nicht rechtzeitig beseitigt wurden.

Ein sachgemäßes und verantwortungsvolles Patchmanagement, das auch die Ansprüche der Anwender - gerade im medizinischen Bereich – berücksichtigt, stellt eine wichtige Sicherheitsmaßnahme im Kampf gegen Cyberattacken dar.

- ✓ **Anschaffung aktueller Hard- und Software**
- ✓ **Härtung von Systemen**
- ✓ **Etablierung von Wartungsfenstern**

5. Mitarbeiterschulung und Sensibilisierung

Die Sensibilisierung der Mitarbeitenden, auch außerhalb von Response-Teams, ist ein wichtiger Grundstein um die eigene Infrastruktur und Organisation zu schützen. Mitarbeitende müssen, angepasst an das eigene Berechtigungskonzept, in der jeweiligen Infrastruktur ihren Tätigkeiten nachgehen können und bieten so Angriffsfläche.
Der Personalmangel in einem Krankenhaus im Bereich der Pflege kann dazu führen, dass Mitarbeitende ggf. nicht regelmäßig für die Teilnahme an Schulungs- und Sensibilisierungsmaßnahmen zur Informationssicherheit freigestellt werden können. Der zusätzliche Druck durch die Corona-Pandemie ist dabei ein verstärkender Faktor.
Phishing stellt jedoch eine Gefahr für die Organisation dar, welcher mit generellen Handlungsempfehlungen entgegengewirkt werden kann. Mailfilter und Whitelists können einen Großteil böswilliger E-Mails, Dateianhänge und Links herausfiltern, jedoch können trotzdem Fehler passieren – und diese Fehler passieren oftmals unbewusst und ohne böswillige Absicht. Regelmäßige Aufklärungen sowie (geregelte) Pen- oder Phishing-Tests mit, an oder bei der eigenen Belegschaft bieten Möglichkeiten zu praxisnahen Erfahrungen für Mitarbeitende und stärken das Bewusstsein gegenüber diesen Themen.

- ✓ **Regelmäßige und anlassbezogene Schulungs- und Sensibilisierungsmaßnahmen**
- ✓ **Pen- und Phishing-Tests zur Überprüfung der Mitarbeiter-Resilienz**

6. Krisenmanagement

Krankenhäuser sind verpflichtet, einen Alarm- und Einsatzplan zur Bewältigung von übergreifenden Notfallsituationen zu erstellen und aktuell zu halten. Häufig erstreckt sich dieser Plan jedoch nicht bis in alle relevanten Bereiche des Krankenhauses hinein. Spezifische Szenarien, wie zum Beispiel ein Ausfall von zentralen IT-Systemen durch einen Angriff oder Schadcode, werden oftmals nicht angemessen abgedeckt.

Dabei müssen zwei Ebenen berücksichtigt werden: Zum einen müssen Anwender dieser Systeme in der Lage sein, einen Ausfall zu überbrücken und zum anderen müssen die technischen Abteilungen die Verfügbarkeit der kompromittierten Systeme in einem angemessenen Zeitraum wiederherstellen können. Konkret bedeutet dies, dass das medizinische Personal über einen begrenzten Zeitraum auch ohne die Systeme zurechtkommen muss. Die Erfahrung zeigt ferner, dass die erstellten Notfallpläne auch für die spezifischen Szenarien geübt und aktualisiert werden müssen. Ein überalterter oder fehlerhafter Notfallplan stellt ansonsten leicht eine Anleitung zum Scheitern dar.

Für das Erstellen, Aktualisieren und Erproben der Notfallpläne müssen die erforderlichen Ressourcen bereitgestellt werden, was eine zusätzliche Herausforderung für die Krankenhäuser darstellt. Um die Notfallplanung angemessen und effizient umsetzen zu können sollte auch hier ein ganzheitlicher Ansatz gewählt werden: Von den jeweiligen Verfügbarkeitsbedarfen der zentralen Geschäftsprozesse ausgehend, müssen Risiken bewertet werden. Es muss ermittelt werden, welche Ausfallzeiten für welche Systeme noch kompensiert werden können. Auf der Basis dieser Ausfallzeiten müssen reaktive Notfallpläne zur Wiederherstellung der Systeme und Notfallpläne zur Überbrückung der Ausfälle auf der Seite der Anwender konzipiert werden.

Präventive Maßnahmen sind erforderlich, um die Eintrittswahrscheinlichkeit und gegebenenfalls die Schadenshöhe eines Ausfalls zu begrenzen. Alle Maßnahmen und Pläne müssen regelmäßig überprüft und aktualisiert werden. Die Mitarbeitenden müssen auf die Szenarien durch regelmäßige und angemessene Übungen vorbereitet werden. All dies ist effizient und effektiv über ein Managementsystem zur Geschäftsfortführung (Business Continuity Management System, BCMS) zu leisten.

- ✓ **Ergänzung des Alarmplans um IT-Komponenten**
- ✓ **Übung und Optimierung des Notfallplans**
- ✓ **Business Impact Analyse**

Cybersicherheit
auf einen Blick

1 Netzwerk-segmentierung

- ✓ Trennung von medizintechnischen und Verwaltungsnetzwerken
- ✓ Anwendung von Firewalls

2 Zugangsmanagement

- ✓ Angemessene Zugangskontrollen
- ✓ Trennung von Admin- und Nutzerrollen
- ✓ Berechtigungskonzepte auch für Admins
- ✓ Network Access Control (NAC)

3 Schwachstellen-management und Penetrationtesting

- ✓ Regelmäßige Schwachstellenscans
- ✓ Schwachstellenmanagement bei Herstellern von Medizintechnik
- ✓ Regelmäßige Penetrationstests

4 Patchmanagement und Systemhärtung

- ✓ Anschaffung aktueller Hard- und Software
- ✓ Härtung von Systemen
- ✓ Etablierung von Wartungsfenstern

5 Mitarbeiterschulung und Sensibilisierung

- ✓ Regelmäßige und anlassbezogene Sensibilisierungsmaßnahmen
- ✓ Pen- und Phishing-Tests zur Überprüfung der Mitarbeiter-Resilienz

6 Krisenmanagement

- ✓ Ergänzung des Alarmplans um IT-Komponenten
- ✓ Übung und Optimierung des Notfallplans
- ✓ Business Impact Analyse

Ganzheitlich denken:
Zugang beschränken, Daten sichern, Systeme schützen!

www.cybersicherheitsrat.de

Cyber-Sicherheitsrat Deutschland e.V.