KURZDARSTELLUNG

Cybersicherheit im Gesundheitswesen: große Veränderungen und komplexe Herausforderungen

Vier kritische Cybersecurity-Probleme, die das Gesundheitswesen heute belasten.

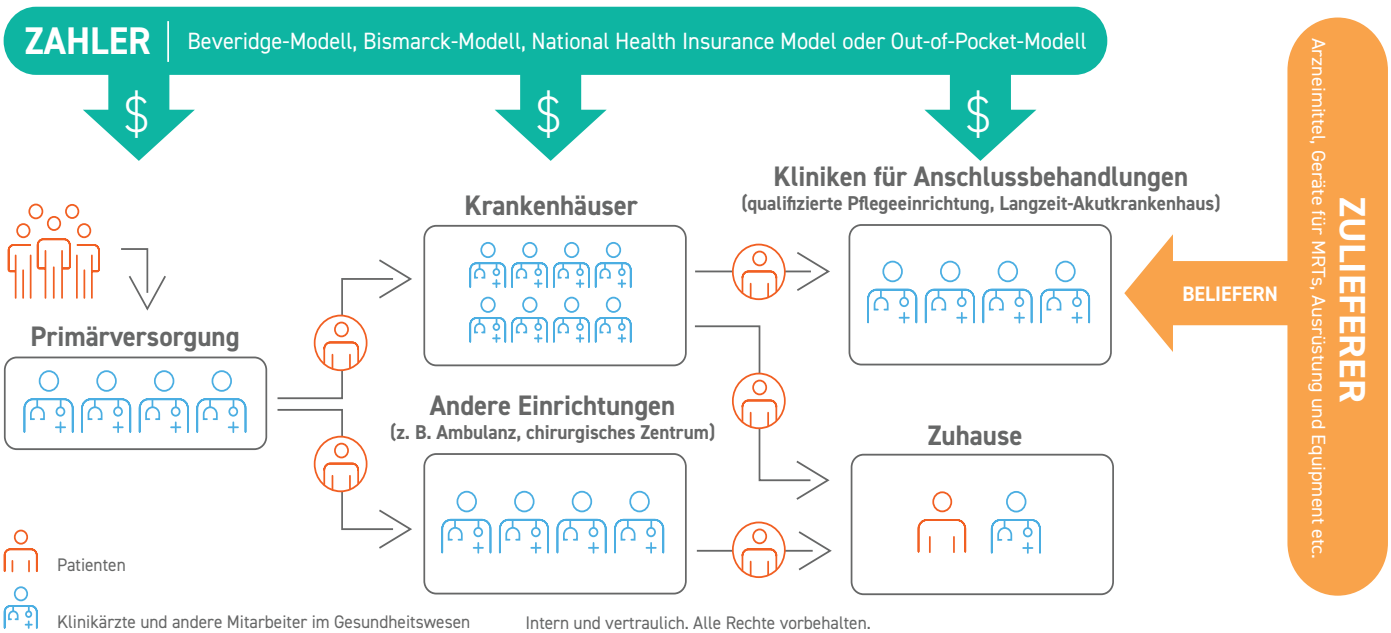
Zusammenfassung

Mit Beginn der COVID-19-Pandemie stieg der Bedarf an telemedizinischen Leistungen, Fachkräften für die Fernpflege, cloudbasierten Datenmanagement- und Geschäftsprozessen sowie vernetzten Geräten für die Remote-Überwachung von Patienten. Um das alles zu meistern, haben viele Healthcare-Organisationen ihre Prozesse angepasst und ihre digitale Präsenz erweitert. Auf diese Weise konnten Fachkräfte ihre Patienten von überall aus persönlich, virtuell oder zu Hause betreuen. Diese Entwicklung hat allerdings auch eine Reihe von Cybersecurity-Herausforderungen hervorgebracht bzw. weiter verschärft.
In dieser Kurzdarstellung beschäftigen wir uns mit den neuen Herausforderungen und komplexen Veränderungen in der Cybersicherheit, die das weltweite Gesundheitswesen betreffen.

Einführung

Dass im Gesundheitsbereich viel auf dem Spiel steht, sollte niemanden überraschen. Am laufenden Band erscheinen neue medizinische Technologien und Anwendungen, um das Wohlbefinden und die Sicherheit von Patienten während der gesamten Behandlung zu fördern.

Jedoch können erfolgreiche Cyberangriffe auf kritische Healthcare-Infrastrukturen und elektronische Patientenakten einen regelrechten Kaskadeneffekt verursachen und die Patientenversorgung auf erschreckende Weise beeinträchtigen:



- Patienten erhalten nicht die nötige Versorgung, wenn Healthcare-Provider aufgrund von Ransomware- oder DDoS-Attacken nicht auf ihr Netzwerk zugreifen können.
- Chirurgen müssen lebensrettende Operationen verschieben, weil sie nicht auf die benötigten Informationen zugreifen können.
- Störungen in der Diagnose und bei Labortests verzögern die medizinische Behandlung.
- Wenn Notaufnahmen nicht verfügbar sind, müssen Rettungswagen Gesundheitseinrichtungen ansteuern, die um Kilometer weiter entfernt liegen. Dies kann negative und manchmal auch irreversible Folgen haben.

Geschützte Gesundheitsdaten sind im Darknet heiß begehrt

Krankenhäuser und andere Healthcare-Organisationen sind nach wie vor extrem beliebte Ziele externer und interner Cyberangriffe, da geschützte Gesundheitsdaten (Protected Health Information, PHI) im Darknet sehr gefragt sind. Oft bringen diese Daten mehr Geld als andere personenbezogene Informationen.

Kreditkarten beispielsweise können gesperrt und ersetzt werden, wenn verdächtige Transaktionen bemerkt werden, was ihren Marktwert verringert. Im Gegensatz dazu werden medizinische Akten höher gehandelt, weil es sich um unveränderbare Datensätze handelt, die sich nicht einfach modifizieren oder löschen lassen. Cyberkriminelle können folglich über einen langen Zeitraum von solchen Daten profitieren, während die betroffenen Patienten finanziell und emotional belastet werden und oft viel Zeit brauchen, um die Schäden solcher betrügerischer Aktivitäten zu beheben. Beispiele sind etwa der Kauf von verschreibungspflichtigen Medikamenten, die Inanspruchnahme von Behandlungen, die Einreichung gefälschter medizinischer Anträge oder der Erhalt privater Darlehen bzw. die Ausstellung von Kreditkarten mithilfe gestohlener Patientenakten.

Ransomware nach wie vor ein Problem

Bedrohungsakteure finden immer neue Wege, Schwachstellen auszunutzen. Oft kommen Security-Operations-Center (SOCs) im Gesundheitsbereich nicht dazu, diese Sicherheitslücken zu schließen. Nicht selten bleiben sie unbemerkt, weil ihre Investitionen in die Cybersicherheit nicht ausreichen, um mit den fortschrittlichen Hacking-Methoden Schritt zu halten. So nutzen Cyberkriminelle aktiv ungepatchte Schwachstellen wie Log4j aus; diese dienen als primäre Angriffsvektoren für Ransomware-Attacken. Es kommt also nicht von ungefähr, dass Ransomware als größte Bedrohung im Gesundheitswesen betrachtet wird.

Dieser Trend wird sich wahrscheinlich auch 2022 fortsetzen, da 42 %[1] der Healthcare-Organisationen in den letzten zwei Jahren von Ransomware-Angriffen betroffen waren. 36 %[2] dieser Vorfälle ereigneten sich außerdem über Dritte, wie etwa die aufsehenerregenden Supply-Chain-Angriffe auf anfällige kritische Infrastrukturmanagement-Software.

Die meisten Sicherheitsvorfälle sind auf Schwachstellen in Netzwerkservern zurückzuführen

2021 war für die Branche ein Rekordjahr in Sachen Sicherheitsvorfälle: Geschützte Patientendaten wurden infolge etlicher Datenlecks offengelegt. Das U.S. Office for Civil Rights (OCR), das dem Department of Health and Human Services (HSS) untersteht, berichtete etwa, dass mehr als 700 Einrichtungen betroffen waren (Abbildung 1) und in diesem Zusammenhang über 42 Millionen geschützte Gesundheitsdaten gestohlen wurden, verloren gingen oder an die Öffentlichkeit gelangten (Abbildung 2). Bei den kürzlich gemeldeten Vorfällen[3] traten Datenlecks auf und die Zahl der Schwachstellen war bereits Anfang 2022 besorgniserregend hoch (Abbildung 3).

Die Top Ten der 2021 gemeldeten Sicherheitsvorfälle im Gesundheitswesen waren alle auf erfolgreiches Hacking zurückzuführen. Die Schwere dieser Vorfälle wurde dabei anhand der Zahl der Betroffenen gemessen. 90 % davon ereigneten sich auf den Netzwerkservern der Provider (Abbildung 4). Netzwerkserver und E-Mails machten zusammen 80 % der Angriffsvektoren aus, was sich negativ auf akute Behandlungen und Ergebnisse auswirkte.

Abbildung 1
Sicherheitsvorfälle im Gesundheitswesen, bei denen 500 oder mehr Datensätze betroffen waren

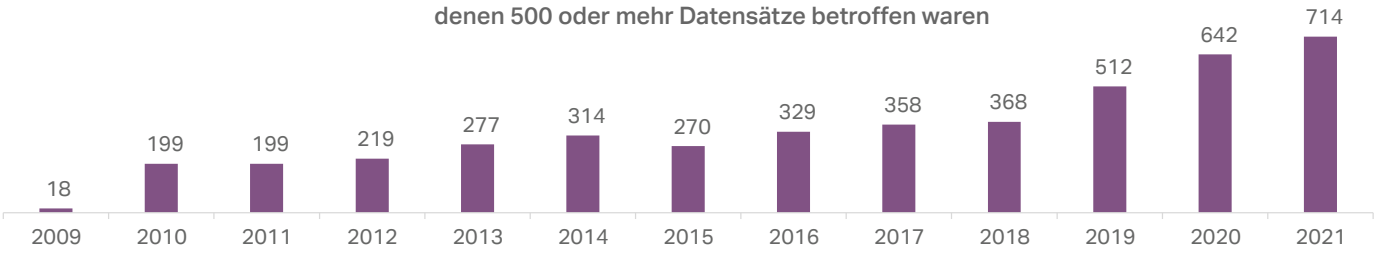
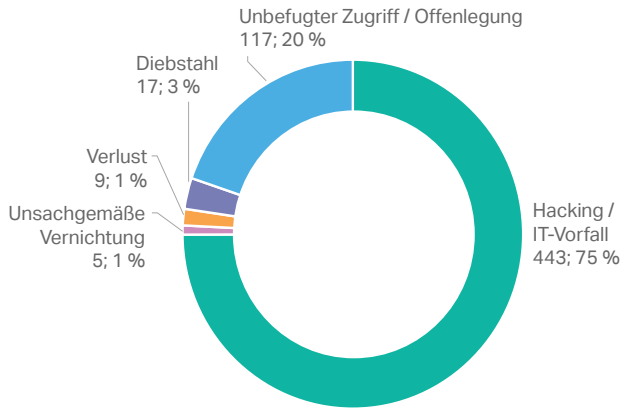


Abbildung 2

U.S. Department of Health and Human Services, Office for Civil Rights, gemeldete Sicherheitsvorfälle im Jahr 2021
Gesamt: 5



U.S. Department of Health and Human Services, Office for Civil Rights, Zahl der Betroffenen im Jahr 2021

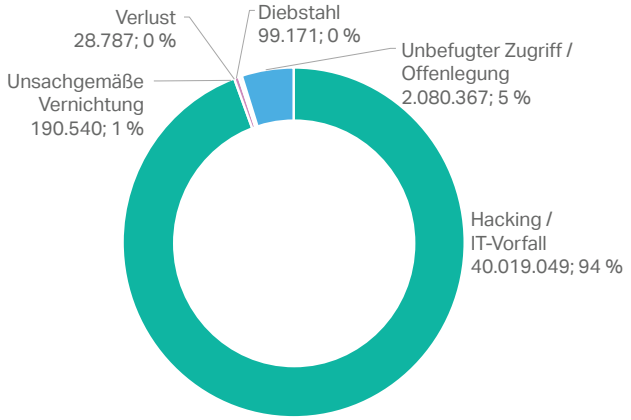
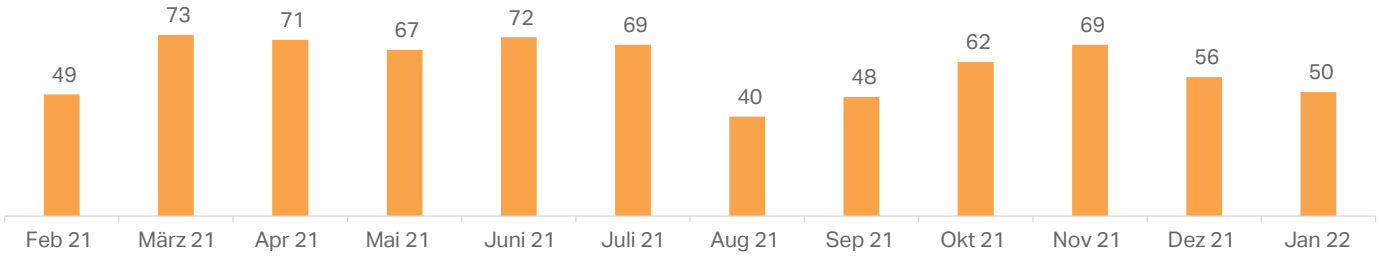


Abbildung 3
Sicherheitsvorfälle im US-amerikanischen Gesundheitswesen in den letzten 12 Monaten

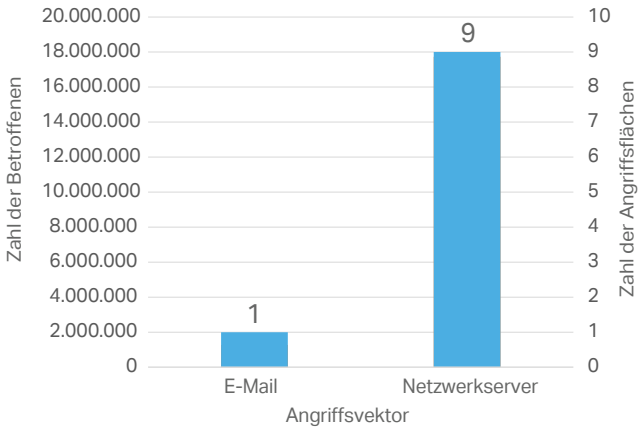


Vier kritische Cybersicherheitsrisiken im Gesundheitsbereich

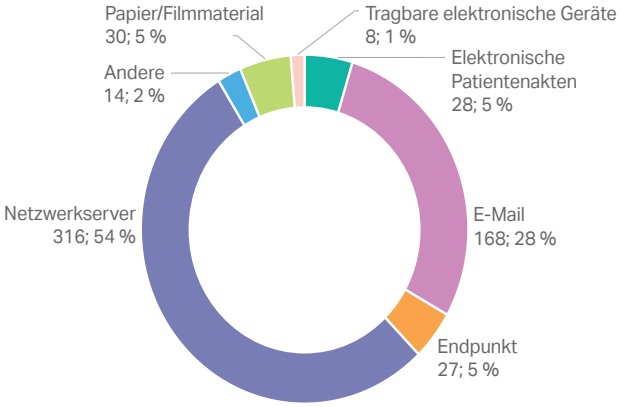
Neben den vielen Vorteilen moderner Technologien im Gesundheitswesen sind neue medizinische Geräte sowie die Vernetzung verschiedener Healthcare-Systeme mit vielen Risiken verbunden. Der gesamte Healthcare-Bereich hat mit vier großen Cybersecurity-Herausforderungen zu kämpfen:

Abbildung 4

Top Ten der 2021 gemeldeten Sicherheitsvorfälle im US-amerikanischen Gesundheitswesen



U.S. Department of Health and Human Services, Office for Civil Rights, Angriffsfläche im Jahr 2021



1. Kritische Infrastruktur erhalten und kontinuierlich verfügbar machen
2. Patientendaten vor internen Risiken schützen
3. Die Integrität medizinischer Daten bewahren
4. Sicherheitsvorfälle infolge von Ransomware- und Phishing-Angriffen vermeiden

Wer seine kritische Infrastruktur ausbaut, ohne in die Infrastruktursicherheit zu investieren, geht ein immenses Risiko ein. Healthcare-Organisationen, die nicht genug in Bereiche wie Patch- und Konfigurationsmanagement, Zugriffskontrolle, Datenverschlüsselung und Patientenportalsicherheit investieren, können ihren Patienten weder eine hohe Qualität und zeitnahe Betreuung bieten noch den Schutz ihrer Daten gewährleisten. Ein unzureichender Schutz von Gesundheitsdaten, der nicht den geltenden Datenschutzgesetzen und -richtlinien entspricht, kann schwerwiegende Folgen nach sich ziehen, wie etwa Datenlecks, eine lückenhafte Pflege, schlechte Behandlungsergebnisse, Störungen im Rechnungsprozess, finanzielle Schäden, Ausgaben für die Problembehebung, Gerichtskosten und Vergleichszahlungen, hohe Geldstrafen, Vertrauensverlust und Imageschäden.

Fazit

Nach über zwei Jahren Pandemie sind Healthcare-Organisationen immer noch überlastet und unterbesetzt. Auch die kontinuierliche technologische und digitale Transformation, die eigentlich dazu dient, die Betreuung der Patienten zu verbessern, kann das Personal überfordern. Die SonicWall-Cybersicherheitslösungen für das Gesundheitswesen erleichtern den Wandel und helfen Organisationen, die Infrastruktursicherheit zu stärken sowie die Patientenversorgung effizienter, resilienter und sicherer zu gestalten. Mit diesem integrierten, zentral verwalteten Sicherheitsstack aus Edge-, Datencenter-, Zugriffs-, Wireless-, E-Mail- und Endpoint-Lösungen können Healthcare-Organisationen die Behandlungsergebnisse ihrer Patienten während der gesamten Betreuung verbessern.

Lesen Sie unser Whitepaper „Grenzenlose Cybersicherheit für das Gesundheitswesen“ und erfahren Sie, wie Sie mit den SonicWall-Produkten für den Healthcare-Bereich die Verfügbarkeit kritischer Infrastrukturen, die Integrität elektronischer Gesundheitsdaten und die Vertraulichkeit und Sicherheit persönlicher Gesundheitsinformationen gewährleisten.

1 Quelle: The Impact of Ransomware on Healthcare During COVID-19 and Beyond (Auswirkungen von Ransomware auf das Gesundheitswesen während der COVID-19-Pandemie und darüber hinaus), Ponemon Institute.

2 Quelle: The Impact of Ransomware on Healthcare During COVID-19 and Beyond (Auswirkungen von Ransomware auf das Gesundheitswesen während der COVID-19-Pandemie und darüber hinaus), Ponemon Institute.

3 Quelle: HIPAA Journal, Januar 2022, Healthcare Data Breach Report (Bericht über die Sicherheitsvorfälle im Gesundheitswesen), https://www.hipaajournal.com/january-2022-healthcare-data-breach-report/

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Erkennung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall Krankenhäusern, Kliniken und Gesundheitsdienstleistern weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.com/healthcare.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

SONICWALL

ExecBrief-HealthcareCybersecurity-A4-JK-6455