IT-Sicherheit im Gesundheitswesen

Modernisierung des Sektors
mit smarter Cyber Defense

Inhalt

Einleitung

Wie verändert die Digitalisierung, die im Zuge der Pandemie immer mehr Fahrt aufgenommen hat, die Gesundheitsbranche? Welches Wachstum sehen wir bei Konzepten wie der Telemedizin? Wie sieht es mit den Ausgaben für digitale Technologien in Deutschland im Vergleich zum Rest Europas aus und welchen Beitrag leisten staatliche Initiativen?

Welche Auswirkungen hat die zunehmende Verbreitung von Technologien auf die Cyber-Sicherheit? Ist der Gesundheitssektor im Zeitalter zunehmender Bedrohungen und Cyberangriffe ausreichend geschützt? Müssen Gesundheitsdienstleister zusätzliche Maßnahmen ergreifen, um ihre wichtige IT-Infrastruktur und sensible Patientendaten zu schützen?

Wir untersuchen, welche Rolle fortschrittliche Cyber-Defense spielen kann und wie Sie Ihre Cyber-Reife bestimmen. Wir helfen Ihnen, zwei entscheidende Fragen zu beantworten: Wodurch zeichnet sich eine Cyber-Defense-Strategie aus? Wie wägen Sie die Vorteile interner Cyber-Sicherheit gegenüber Managed Services ab?

1. Der zunehmende Einsatz von Technologie im Gesundheitswesen

Die Digitalisierung des Gesundheitswesens läuft bereits seit einiger Zeit, aber die Corona-Pandemie hat sie weiter beschleunigt. Aufgrund von Lockdowns und Social-Distancing-Regeln stieg die Nutzung digitaler Services wie Telemedizin, Telekonsultation und Fernüberwachung von Patienten. Entscheidend dafür sind vernetzte Geräte sowie sichere Cloud-Plattformen und -Anwendungen.

So ist beispielsweise die Telemedizin – die Versorgung mit klinischen und nicht-klinischen Dienstleistungen aus der Ferne – während der Pandemie geradezu explodiert. Patienten wollten Fahrten mit Bus und Bahn und das Risiko einer Virusinfektion vermeiden und benötigten eine sichere Möglichkeit, um medizinische Dienstleister zu erreichen. Die Telemedizin erwies sich dafür als ideal.

Telemedizin umfasst unter anderem Teletherapie, Telekonsultation und Patientenüberwachung und ist einer der wichtigsten Trends im Gesundheitswesen: 2021 betrug das Marktvolumen etwa 12,5 Milliarden US-Dollar, und bis 2027 dürfte es 41,5 Milliarden US-Dollar erreichen.[1]

Mit Telekonsultations-Apps können Patienten ganz einfach Ärzte konsultieren und Diagnosen und Rezepte erhalten – ganz bequem von zu Hause aus. Allerdings ist das Konzept kein völlig neuer Trend, sondern existiert schon seit einiger Zeit.

Bereits 2019 nutzte ein chinesisches Krankenhaus die 5G-Technologie, um aus der Ferne eine Gehirnoperation durchzuführen. Der Patient litt an Parkinson und erhielt mithilfe chirurgischer Instrumente, die von Ärzten in 3000 km Entfernung bedient wurden, ein Implantat.[2] In Zukunft könnten erfahrene Experten durch Fernchirurgie in der Lage sein, komplexe Eingriffe direkt an Patienten in abgelegenen Gebieten durchzuführen, was einen bedeutenden Fortschritt für die Telemedizin darstellen würde.

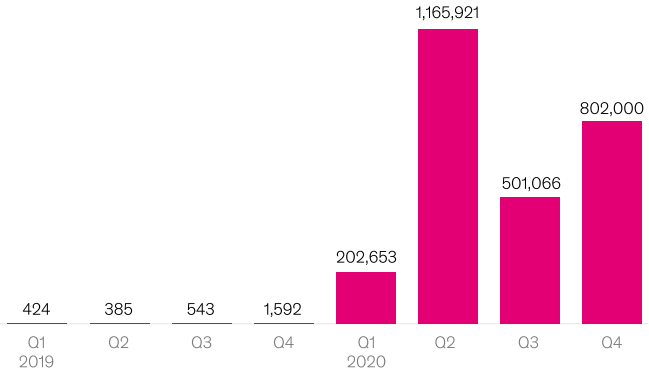
Diese digitalen Trends helfen Fachleuten im Gesundheitswesen, Zeit und Kosten zu sparen. Telematik bietet darüber hinaus noch weitere Vorteile. Aus Sicht der Patienten ermöglicht die Beschleunigung von Diagnosen eine Verbesserung ihrer Lebensqualität. In einigen Fällen hat die Technologie sich sogar als lebensrettend erwiesen – im wahrsten Sinne des Wortes.

2. Die Situation in Europa in einem Wort: Hyper-Wachstum

In Ländern wie Deutschland gab es in den letzten vier Jahren einen massiven Ausbau der digitalen Infrastruktur. McKinsey berichtet, dass über 90 % der Allgemeinarztpraxen in Deutschland an die Telematikinfrastruktur angeschlossen sind.[3]

Vor der Pandemie nutzten weniger als 3.000 Patienten Telekonsultationen. Mit der Ausbreitung des Virus stiegen die Zahlen jedoch stark an: 2020 lag die Zahl der Patienten, die eine Telekonsultation in Anspruch nehmen, bereits bei 2,7 Millionen, was einem atemberaubenden Wachstum auf das 900-Fache entspricht. Im selben Jahr wurden außerdem 685 Millionen Rezepte remote ausgestellt.

Anzahl der von den gesetzlichen Krankenkassen erstatteten Online-Konsultationen



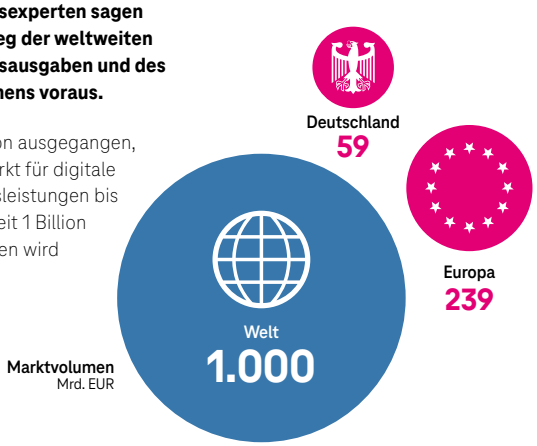
Bildquelle: McKinsey Company

Es ist nicht überraschend, dass auch andere digitale Gesundheitsdienste im Trend liegen. Die Popularität von E-Health-Apps ist ebenfalls stark angestiegen. Die Top 40 der deutschen E-Health-Apps wurden rund 2,4 Millionen Mal heruntergeladen. Eine der häufigsten Kategorien von E-Health-Apps ist die Terminbuchung. Andere Kategorien sind Diagnose-Apps, Krankenversicherungsportale, krankheitsspezifische Apps und elektronische Patientenakten.

Insgesamt werden die Ausgaben für die Digitalisierung in der Gesundheitsbranche voraussichtlich weiter steigen. Nach Angaben der Unternehmensberatung Roland Berger werden die Ausgaben für digitale medizinische Services bis 2026 weltweit 1 Billion Euro betragen. Europas Beitrag dazu wird sich auf etwa 239 Milliarden Euro belaufen, wobei der Anteil Deutschlands auf 59 Milliarden Euro geschätzt wird.[4]

Gesundheitsexperten sagen einen Anstieg der weltweiten Gesundheitsausgaben und des Marktvolumens voraus.

Es wird davon ausgegangen, dass der Markt für digitale Gesundheitsleistungen bis 2026 weltweit 1 Billion Euro erreichen wird



Bildquelle: Roland Berger

Die aktive Rolle der Regierung

Kommt Deutschland mit der Digitalisierung des Gesundheitswesens zurecht? Das Land hat den größten europäischen Markt für häusliche Krankenpflege mit einer wachsenden Zahl pflegebedürftiger Menschen. Da es jedoch Lücken in der digitalen Infrastruktur des Gesundheitswesens gibt, hat die Bundesregierung Maßnahmen eingeleitet, um diese zu schließen und die Digitalisierung zu beschleunigen. 2020 hat die Regierung Finanzierungsmittel vorgesehen, um öffentliche Krankenhäuser beim Ausbau ihrer digitalen Gesundheitsinfrastruktur zu unterstützen. Im Rahmen des Krankenhauszukunftsgesetzes (KHZG) hat der Bundestag 3 Milliarden Euro für Krankenhäuser zur Modernisierung ihrer Infrastruktur bereitgestellt. Die Kostenträger im Gesundheitswesen finanzieren weitere 1,3 Milliarden Euro.[5]

Die im Rahmen des Gesetzes bereitgestellten Mittel sollten von den öffentlichen Krankenhäusern für verschiedene Initiativen wie Patientenportale, E-Dokumentation, digitale Medikamentenverwaltung, Telemedizin, Robotik und IT-Sicherheit verwendet werden. Krankenhäuser müssen 15 % der Fördergelder für die IT-Sicherheit verwenden, um die Bedrohungen durch Cyberkriminelle einzudämmen.[6] Bis Februar 2022 wurden fast 6.000 Anträge eingereicht.[7]

3. Hohes Tempo bei der Modernisierung – aber wie steht es um die Sicherheit?

Cloud, Big Data, das Internet der Dinge (IoT), tragbare Geräte und 5G-Konnektivität bilden die Grundlage der digitalen Trends in der Branche. Die meisten Anwendungen und Portale im Gesundheitswesen werden auf Hyperscaler-Plattformen wie Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) usw. aufgebaut.

Der Sektor stellt außerdem rasch auf elektronische Gesundheitsakten (EGA) um und digitalisiert damit immer größere Datenmengen. Gesundheitsdienstleister greifen über verschiedene Anwendungen auf die digitalen Patientenakten zu und erhalten so einen sofortigen Überblick über die Krankengeschichte, die Medikamente und die Behandlung der Patienten. Mobile und Webtechnologien bilden das Rückgrat dieser Anwendungen. Bei diesen Anwendungen haben die Einhaltung der DSGVO und der Schutz von Patientendaten höchste Priorität, da sie für die Integrität und Vertraulichkeit der medizinischen Informationen unerlässlich sind. Darüber hinaus setzen Anbieter fortschrittliche Technologien wie künstliche Intelligenz (KI), maschinelles Lernen (ML) und Deep Learning (DL) ein.

- Machine Learning bezieht sich auf ein Verfahren, bei dem Computer-Algorithmen auf Basis von Daten lernen und automatisch verbessert werden, ohne explizit programmiert zu werden.
- Deep Learning ist eine spezielle Form des ML, bei der künstliche neuronale Netze eingesetzt werden, um komplexe Muster in großen Datensätzen zu erkennen und zu analysieren.
- DL ist ein Unterbereich des ML, der auf der Verwendung von neuronalen Netzen mit vielen Schichten basiert, während ML verschiedene Techniken wie Entscheidungsbäume, Random Forests und Support-Vector-Maschinen umfasst.

Einsatz hochmoderner Technologien zur Datenspeicherung und Datenanalyse

Die Digitalisierung erzeugt riesige Datenmengen in der Cloud, die strukturiert und organisiert werden müssen, um verwertbare Erkenntnisse zu gewinnen. Fortschrittliche Datenanalysetools wie KI, ML und DL helfen bei der Ableitung von Bedeutungen und beschleunigen die Datenanalyse.

Durch die Anwendung von ML-Modellen auf Patientendatensätze lassen sich Muster identifizieren und KI-basierte Tools verarbeiten Bilder, um Krankheiten zu erkennen und Frühdiagnosen zu stellen. Einige Akteure im Gesundheitswesen evaluieren auch aktiv DL-Plattformen, um ihre IT-Abläufe zu sichern. Darauf möchten wir im Folgenden näher eingehen.

Ein typisches Beispiel: DL-Plattformen zur Sicherung der IT

Mit herkömmlichen Lösungen zum Endgeräteschutz können Ransomware- und Malware-Angriffe unentdeckt bleiben. Deshalb ist ein erweiterter Bedrohungsschutz erforderlich. Gesundheitsdienstleister setzen daher auf fortschrittliche Technologien wie DL und KI, um Cyberangriffe zu erkennen, vorherzusagen und zu verhindern. Eine DL-basierte Plattform – Deep Instinct – hilft ihnen dabei, ihre IT-Infrastruktur zu sichern und Cyberangriffe zu verhindern.

Wie Telekom Security das Universitätsklinikum Bonn unterstützt

Das renommierte Lehrkrankenhaus hat 1.300 Betten und 8.300 Mitarbeiter. Jedes Jahr behandelt es 350.000 ambulante und 50.000 stationäre Patienten und bewältigt 40.000 Notfälle. Aufgrund von über 10.000 an das Netzwerk angeschlossenen Geräten sah sich das Klinikum mit einer täglichen Zunahme der Bedrohungen konfrontiert. Telekom Security, Teil des Magenta Security Portfolios der Deutschen Telekom, hilft dem Krankenhaus, seine kritische Infrastruktur vor fortschrittlichen Bedrohungen zu schützen. Mit Deep Instinct, einer DL-basierten Plattform, kann das Krankenhaus nun Zero-Day-Angriffe verhindern und profitiert von höherer Genauigkeit bei der Bedrohungserkennung und -abwehr. Die Plattform ermöglicht es dem Klinikum, Bedrohungen in Echtzeit und mit sehr geringer Fehlerquote zu entschärfen.

Über Deep Instinct

Deep Instinct ist ein Cyber-Sicherheitsunternehmen, das DL-Technologie auf die Sicherheit anwendet, damit Unternehmen Malware erkennen und unschädlich machen können.

Das größte Risiko für unseren Betrieb ist Ransomware. Bedrohungen und Cyber-Vorfälle sind im Vergleich zum Vorjahr um 20 % gestiegen, und unsere alte Lösung konnte damit nicht umgehen. Mit den Cybersecurity-Funktionen von Telekom Security und Deep Instinct können wir heute über 10.000 Endpunkte schützen. Insgesamt haben wir festgestellt, dass die Zeit bis zur Bedrohungserkennung um etwa 35 % gesunken ist.

Außerdem wurden die IT-Ausfallzeiten reduziert, was unserem Unternehmen über 35 % finanzielle Verluste erspart hat.

Dieter Padberg – CIO, Universitätsklinikum Bonn

Der Einfluss von Technologien im Gesundheitswesen wächst, wobei sensible Patientendaten im Mittelpunkt der Prozesse stehen. Die Anbieter digitalisieren ihren Betrieb immer weiter, aber sind die Daten auch sicher? Aufgrund der größeren Angriffsfläche wird die Cyber-Sicherheit in Unternehmen des Gesundheitswesens in Zukunft noch wichtiger.

4. Der Stand der Sicherheit in der Gesundheitsbranche

Das Risiko von Cyber Attacken und der Variantenreichtum dieser Angriffe nehmen exponentiell zu. Der Healthcare Breach Report 2021 (H2) berichtet, dass 2021 etwa 45 Millionen Menschen von Cyberangriffen und Datenschutzverletzungen im Gesundheitswesen betroffen waren. 2020 lag diese Zahl bei 34 Millionen und 2018 bei etwa 14 Millionen. Somit hat sie sich in nur drei Jahren verdreifacht.[8]

Datenschutzverletzungen haben unweigerlich auch finanzielle Auswirkungen. In Bezug auf Verluste gehört das Gesundheitswesen zu den am stärksten betroffenen Branchen. Forbes berichtet, dass die durchschnittlichen Kosten einer einzelnen Sicherheitsverletzung 2021 bei 9,2 Millionen Dollar lagen, 2 Millionen Dollar mehr als 2020.[9] Die finanziellen Auswirkungen geben zwar Grund zur Sorge, doch vor allem ist die Tatsache besorgniserregend, dass Angriffe auf Organisationen des Gesundheitswesens den täglichen Betrieb und die Behandlungsqualität erheblich beeinträchtigen können – mit allen denkbaren Folgen.

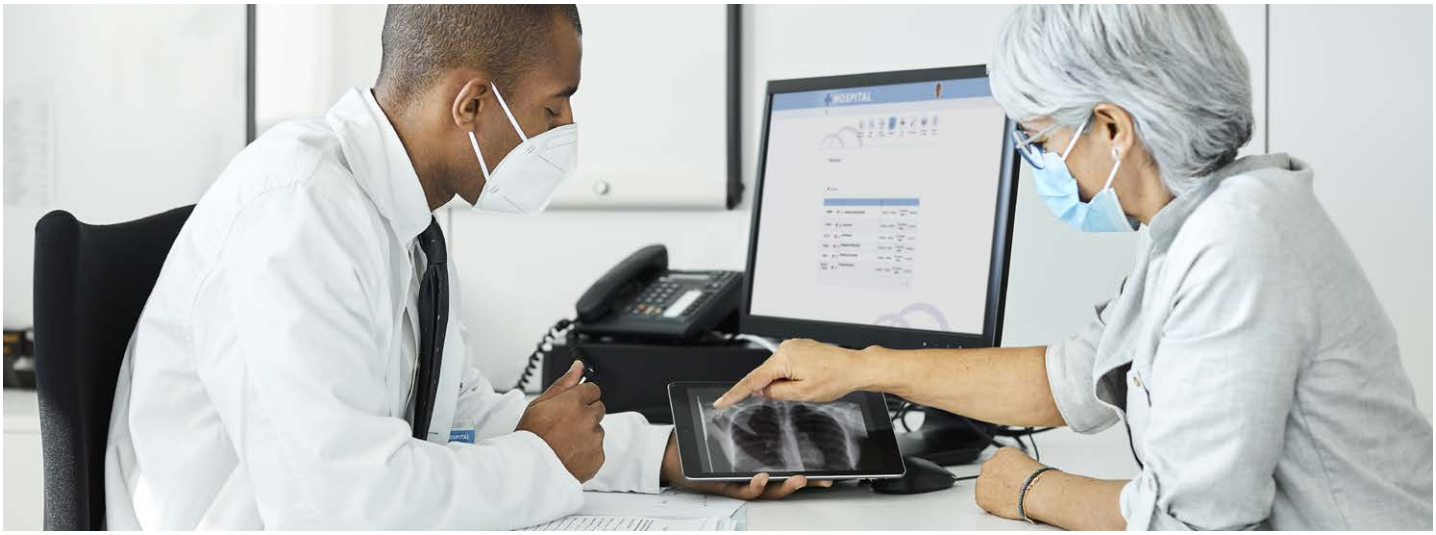
2021 veröffentlichte die Cybersecurity and Infrastructure Security Agency (CISA) eine Studie, die einen direkten Zusammenhang zwischen Cyberangriffen und Sterblichkeit zeigt. Wenn zum Beispiel ein Krankenhaus von einem Cyberangriff betroffen ist, kann dies zu einem Ausfall des IT-Netzwerks führen. Netzwerkausfälle wirken sich auf die Fähigkeit des Krankenhauses aus, Diagnosetechnologie anzubieten und auf elektronische Gesundheitsakten zuzugreifen – und damit auf die Qualität der Pflege. The Verge, eine amerikanische Website für Technologie-Nachrichten, berichtete, dass in etwa 70 % der von Ransomware-Angriffen betroffenen Gesundheitsorganisationen der Betrieb unterbrochen und die Patientenversorgung verzögert worden sei.[10]

Im September 2020 störte ein Ransomware-Angriff die Notfallversorgung im Universitätsklinikum Düsseldorf, sodass kritische medizinische Maßnahmen teilweise nicht mehr möglich waren.[11]

Es kommt immer wieder zu solchen Ereignissen, bei denen Cyberattacken schwerwiegende Folgen für Gesundheitsdienstleister haben und die ein erhebliches Risiko für die optimale Behandlung der Patienten mit sich bringen können.

Mit der fortschreitenden Digitalisierung werden auch Umfang, Tiefe und Häufigkeit der Cyberangriffe zunehmen. Noch dazu werden sie immer ausgereifter. Im Durchschnitt dauert es etwa 212 Tage, um einen Angriff zu entdecken und weitere 75 Tage, um ihn einzudämmen.[12] Aufgrund der Commoditisierung intelligenter Hacking-Tools wie Malware-as-a-Service (MaaS), Distributed Denial of Service (DDoS) und Botnets wird es insgesamt einfacher, Angriffe auf Gesundheitsorganisationen zu starten.

Angesichts der sprunghaften Zunahme von Angriffen raten die Behörden Gesundheitseinrichtungen dringend, robuste Cyber-Sicherheitsmaßnahmen zu implementieren, um Bedrohungen zu erkennen und darauf zu reagieren. Sind sie ausreichend vorbereitet, um die Herausforderungen zu meistern? Schwache IT-Systeme machen es Hackern noch leichter. Deshalb müssen Gesundheitsorganisationen ihre IT modernisieren und fortschrittliche Cyber-Sicherheit integrieren. Besonders zu nennen ist dabei der B3S IT-Sicherheitsstandard. Dies ist ein Regelwerk, das von deutschen Krankenhäusern und anderen kritischen Infrastrukturen zu erfüllen ist, um ein angemessenes Maß an IT-Sicherheit und Datenschutz zu gewährleisten.



5. Cyber-Defense: Sicherheit braucht einen Richtungswechsel

Malware kann jeden treffen und DDoS-Angriffe können jede Organisation lahmlegen – nicht nur Betreiber kritischer Infrastrukturen (KRITIS). Cyberkriminelle haben es zunehmend auf kleine und mittelständische Unternehmen abgesehen, die sie oft als leichtes Ziel betrachten. Aus diesem Grund muss Cyber-Sicherheit als zentrale Managementaufgabe betrachtet werden, um das Risiko von Datendiebstahl, IT-Ausfällen und Erpressung zu verringern. Grundsätzlich muss die Cyber-Sicherheit mit der digitalen Innovation und Transformation Schritt halten: Wenn alles vernetzt ist, muss alles abgesichert sein. Mit anderen Worten: Alles, was vernetzt ist, erfordert Cyber-Sicherheit und Cyber-Defense – insbesondere weil nicht nur die Zahl der Angriffe zunimmt, sondern sie auch immer ausgereifter werden. Laut dem ehemaligen BSI-Präsidenten Arne Schönbohm haben die heutigen Angreifer wenig mit dem stereotypen Hacker in einem dunklen Keller gemein.

> Managed Cyber Defense ist vergleichbar mit professionellem Brandschutz. Zur Vorbeugung platzieren wir virtuelle „Rauchmelder“ im gesamten Internet. Sobald irgendwo eine Rauchwolke auftaucht, schlagen sie Alarm und wir können reagieren und virtuelle Brände löschen – also die Cyber-Attacken unterbinden. Das Team unseres Security Operations Centre (SOC) arbeitet rund um die Uhr, um dies zu ermöglichen.
>
> **Rüdiger Peusquens – Head of Cyber Defense & Security Testing, Telekom Security**

Gesundheitsorganisationen müssen sich auch gegen hochspezialisierte Banden wappnen. Obwohl sich dieses Whitepaper auf das Gesundheitswesen konzentriert, gelten einige Grundregeln für die IT-Sicherheit analog auch für andere Sektoren. Und das ist erst der Anfang: Viele Bereiche sind noch nicht digitalisiert, werden aber bald in die Cloud verlagert – und benötigen dann erweiterten Schutz. Mit anderen Worten: Unternehmen brauchen einen anderen Ansatz für die Sicherheit – einen virtuellen Sicherheitsgurt, der auch im kontinuierlichen Änderungsmodus der Cloud-Transformation zuverlässig schützt. Umfassende Cyber-Defense kombiniert Vorhersage, Prävention, Erkennung, Reaktion und Wiederherstellung. Sie betrachtet die gesamte IT-Infrastruktur von Unternehmen, vom Netzwerk über Server bis hin zu Diensten und Endgeräten.

Cyber-Defense: Intern oder als Managed Service?

Eintrittspunkte blockieren, Angreifer aufspüren und Eindringlinge abwehren: Organisationen im Gesundheitswesen benötigen Rundumschutz für ihre digitalen Daten. Talentierte Sicherheitsfachkräfte sind sehr gefragt verlangen hohe Gehälter. Viele Unternehmen müssen sich daher überlegen, ob sie Cyber-Defense intern einrichten oder ihre Sicherheit an Managed Service Provider auslagern sollen. Wer vor dieser Entscheidung steht, sollte prüfen, ob sein Unternehmen über ausreichende Maßnahmen zur Prognose, Prävention und Erkennung von Angriffen sowie zur angemessenen Reaktion und Wiederherstellung verfügt. Da die IT-Infrastruktur immer komplexer wird, ändern Cyberkriminelle ständig ihre Angriffsvektoren. Der Kampf gegen kriminelle Banden erfordert hochqualifizierte Sicherheitsspezialisten, die rund um die Uhr arbeiten – denn schließlich schlafen Hacker nie.

6. Häufig vernachlässigte Aspekte der Cyber-Sicherheit: Erkennung und Reaktion

Wer wirksame Schutzmechanismen aufbauen will, sollte die Bedrohungen von Anfang an verstehen und sie systematisch reduzieren. Alle Maßnahmen müssen in Einklang mit den Prioritäten und der Risikobereitschaft seines Unternehmens stehen. Viele Unternehmen müssen ihre Sicherheitsprozesse überdenken und benötigen einen vollständigen Überblick über die Bedrohungslandschaft, um die Korrelation zwischen den beiden Variablen zu ermitteln und besser reagieren zu können. Sie sollten Cyber-Sicherheit als fortlaufenden Prozess betrachten und nicht als einmalige Investition oder ein Programm, bei dem eine jährliche Überprüfung ausreicht.

Da Hacker immer gerissener und ihre Methoden immer ausgereifter werden, sollten wir uns ansehen, wie Angreifer typischerweise Vorgehen, um die Verteidigungsmaßnahmen von Unternehmen zu durchbrechen.

Cyber Kill Chain: Hacker sind geduldig

Angreifer bewegen sich oft 200 Tage lang in einem Unternehmensnetzwerk, bevor sie zuschlagen oder entdeckt werden. Sie unterteilen ihren Angriff in mehrere Phasen – die so genannte Cyber Kill Chain.

- **Erkundung**
  Im ersten Schritt sammelt der Angreifer Informationen über das Ziel.
- **Durchführung des Angriffs**
  Der Hacker versucht, Malware in das Unternehmen einzuschleusen – oft über einen E-Mail-Anhang.
- **Exploit und Installation**
  Ein Mitarbeiter startet und installiert die Malware unwissentlich, indem er auf die infizierte Datei klickt.
- **Command and Control**
  Wenn niemand im Unternehmen die Installation bemerkt, kann der Hacker die Malware über einen Server von außen steuern.
- **Lokale Kompromittierung**
  Der Cyberkriminelle erforscht das interne Netzwerk, spioniert Zugangsdaten aus oder installiert weitere Malware.
- **Interne Erkundung**
  Der Angreifer kundschaftet die interne IT des Unternehmens aus.
- **Laterale Bewegung**
  Der Eindringling infiziert und kompromittiert weitere Systeme. Mit diesen lateralen Bewegungen bringt er mehr und mehr Systeme unter seine Kontrolle.
- **Aktionen und Exfiltration**
  Jetzt hat der Hacker sein Ziel erreicht: Er kann Geschäftsdaten ausspionieren und Systeme verschlüsseln oder zerstören.

Wer eine robuste IT-Umgebung aufbauen will, muss für jede Phase die richtigen Cyber-Defense-Werkzeuge bereithalten. Telekom Security (Teil der Deutschen Telekom) zeigt, wie das in der Realität aussieht: Unsere Sicherheitsspezialisten haben eine Anwendungsfall-Bibliothek entwickelt. Die umfangreiche Datenbank enthält Playbooks, die spezifische Szenarien für jede Angriffsphase beschreiben.

Ein Beispielszenario sind bösartige Websites oder IP-Adressen, die mit den Computern eines Unternehmens kommunizieren.

Die Protokollquellen sind hier Firewalls und die Kommunikationsschnittstellen der Netzwerke (Proxy). Wenn der Anwendungsfall Passwortspionage und Angriffe auf Passwörter beinhaltet, sind Active Directory und User Directory als Protokollquellen erforderlich. Da sich Angriffsvektoren ändern und neue Bedrohungen auftauchen, passt Telekom Security die Bibliothek kontinuierlich an. Dabei stützen wir uns auf Erkenntnisse aus der eigenen Infrastruktur sowie aus den Sicherheits-Services, die wir für unsere Kunden zur Verfügung stellen.

7. Ein leistungsstarkes Trio: SOC, SOAR und SIEM

Wer ist dafür verantwortlich, dass Unternehmen Angriffe erkennen und früh genug abwehren können, um erheblichen Schaden zu verhindern? Diese Aufgaben werden von einem Security Operations Center (SOC) mithilfe von Softwarefunktionen für Security Orchestration, Automation and Response (SOAR) sowie Security Information and Event Management (SIEM) übernommen. SOCs überwachen und analysieren die Aktivitäten in der gesamten IT-Landschaft eines Unternehmens. Sie suchen nach anomalen Aktivitäten in Netzwerken, Servern, mobilen und stationären Clients, Datenbanken, Anwendungen, Webservern und anderen Systemen und können so Sicherheitsvorfälle erkennen. SOCs können außerdem Betriebstechnologien in industriellen Netzwerken schützen. Das Lagebild im SIEM ist eine Gesamtübersicht über die Sicherheitslage in einem IT-System, die durch die Zusammenführung und Korrelation von Informationen aus verschiedenen Quellen erstellt wird. Die Korrelationsbildung von Einzelevents ist ein wichtiger Teil des SIEM-Systems, der es ermöglicht, komplexe Angriffsmuster zu erkennen und darauf schnell zu reagieren.

1

Threat-Intelligence sorgt für Transparenz in Bedrohungslagen

Um die Sicherheitslage zu überwachen, verwenden SOC-Spezialisten Ereignisdaten aus den IT-Systemen und Sensoren eines Unternehmens und kombinieren sie mit kontextbezogenen Informationen aus externen Quellen. Zunächst analysieren sie Informationen von Antiviren-Systemen oder Firewalls sowie Protokolldaten von Anwendungen und Server-Betriebssystemen. Um jedoch beurteilen zu können, ob es sich um einen ernsthaften Sicherheitsvorfall oder einen Fehlalarm handelt, müssen sie die Ergebnisse mit Kontextinformationen anreichern – mit anderen Worten: mit Daten eines Threat-Intelligence-Service.

Threat-Intelligence hilft Unternehmen, Bedrohungen schnell zu erkennen und ihre IT zu schützen, indem es Indikatoren für die Gefährdung (Indicators of Compromise, IoC) zusammen mit einer Vielzahl anderer aktueller Informationen über die Bedrohungslage zur automatischen Auswertung bündelt und strukturiert. IoC sind alle Merkmale und Daten, die darauf hinweisen, dass ein Computersystem oder Netzwerk kompromittiert wurde.

Das Threat-Intelligence-Ökosystem von Anbietern wie Telekom Security umfasst Sicherheitsdienstleister, Forschungsinstitute und Behörden wie das BSI, die ihre Erkenntnisse teilen, um die Effizienz zu steigern. SOC-Experten sind jedoch auch in Internetforen und sozialen Medien aktiv, wo Hacker Informationen über neue Sicherheitslücken und Angriffsmethoden austauschen.

Solche Threat-Intelligence-Services bestehen aus mehreren Modulen. Ein Vulnerability Advisory Service beispielsweise informiert Kunden über neu entdeckte Schwachstellen in Hard- und Software und gibt Empfehlungen, wie sie diese beheben können. Credential Leakage Monitoring gibt Informationen über gestohlene Zugangsdaten weiter, wenn diese im Internet auftauchen. So können Unternehmen die entsprechenden Konten deaktivieren. Fraudulent Domain Monitoring, also das Überwachen von betrügerischen Domains, die arglose Nutzer täuschen sollen, macht Kunden auf aktuelle Phishing-Szenarien aufmerksam.

2

SIEM + SOAR: Datenanalyse, Alarmklassifizierung, automatisierte Reaktion

SIEM analysiert und korreliert Daten in Echtzeit. Solche Systeme bieten Unternehmen einen umfassenden Überblick über ihre IT-Sicherheit. Sie sammeln kontinuierlich Protokolldaten von Endpunkten wie PCs oder Servern, Routern, Switches, Anwendungen, Firewalls und anderen Systemen und werten diese automatisch aus. Dazu verwenden sie Methoden des maschinellen Lernens. Das SIEM schlägt zuverlässig Alarm, sobald es Anomalien feststellt. Da jeder Anwendungsfall in der Cyber-Kill-Chain mit einer bestimmten Korrelationsregel verknüpft ist, wird das SIEM-System hellhörig, wenn ein Benutzer beispielsweise wiederholt die falschen Anmeldeinformationen verwendet, um innerhalb von weniger als einer Minute mehrfach auf denselben Client zuzugreifen.

Es könnte aber auch ein Mitarbeiter sein, der sein Passwort vergessen hat. Nicht jeder Alarm ist ein echter Sicherheitsvorfall. Analysten auf Stufe 1 filtern zunächst Fehlalarme heraus. Doch wenn es sich tatsächlich um einen Angriff handelt, reagieren sie sofort. Wenn sie sich den Vorfall nicht erklären können, leiten sie ihn an Experten der Stufe 2 oder 3 weiter, die weitere Untersuchungen einleiten.

SOAR hilft Sicherheitsteams darüber hinaus bei der Verwaltung und Analyse von sowie der Reaktion auf Bedrohungen und Warnungen. Da die Teams nicht jede Bedrohung manuell untersuchen können, bleiben manche unbeachtet, was zu schwerwiegenden Vorfällen führen kann. Wenn die Systeme nicht ausreichend integriert sind, müssen die Teams außerdem Daten aus verschiedenen Quellen untersuchen.

Dies ist zeitaufwändig und fehleranfällig, und das Übersehen bestimmter Bedrohungen kann verheerende Folgen haben. Genau hier hilft SOAR. Eine SOAR-Plattform bietet eine vollständige Ansicht der Daten auf einer einzigen Konsole – Analysten müssen keine unterschiedlichen Systeme überprüfen. Da Erkennung, Untersuchung und Behebung automatisiert sind, verbessern sich Erkennung und Reaktion erheblich. SOAR übernimmt sich wiederholende Aufgaben und automatisiert manuelle Prozesse, sodass Sicherheitsanalysten mehr Zeit haben, sich auf wichtige Aufgaben zu konzentrieren. So lassen sich Produktivität und Effizienz steigern.

3

Verteidigung: Reaktion auf Vorfälle und Forensik

Wenn es sich um einen Cyberangriff handelt, werden Experten für die Reaktion auf Vorfälle hinzugezogen. Sie dämmen Angriffe ein, eliminieren den Eindringling und stellen ausgefallene IT-Systeme in der Regel wieder her. In besonders schwierigen oder kritischen Fällen ziehen sie einen IT-Forensiker zur Unterstützung hinzu, der zu ermitteln versucht, wie der Hacker vorgegangen ist und der versucht, Indizien zu sammeln. Letzteres ist von entscheidender Bedeutung, wenn die Organisation einen Versicherungsanspruch für etwaige Schäden oder Verluste geltend machen möchte.

SOC: Intern oder als Managed Service?

Ein SOC macht aktuelle Sicherheitsbedrohungen transparent, verbessert die Erkennungsrate möglicher Cyberangriffe und verkürzt Reaktionszeiten. Es trägt dazu bei, wirtschaftliche Risiken aufgrund von IT-Ausfällen zu vermeiden, und erleichtert die Umsetzung von gesetzlichen Vorschriften und Unternehmensrichtlinien. Wer vor der Entscheidung steht, ein SOC intern zu betreiben oder als Managed Service zu erwerben, sollte sich die folgenden Fragen stellen:

Verfügt meine Organisation über die notwendigen Kenntnisse und Ressourcen?

Hacker kennen keinen Feierabend. Deshalb muss Ihr SOC rund um die Uhr besetzt sein, um Bedrohungen und Sicherheitsvorfälle sofort analysieren und darauf reagieren zu können. Haben Sie genügend Fachkräfte? Tauschen sie kontinuierlich Informationen mit anderen innerhalb eines Sicherheits-Ökosystems aus? Denken Sie auch daran, dass Sicherheitsexperten äußerst gefragt und teuer sind.

Verfügen wir über die notwendige Infrastruktur?

SOCs stellen hohe Anforderungen an Infrastruktur und technische Ausstattung. Sie benötigen effektive Erkennungs- und Analysetools und technische und organisatorische Sicherheitsmaßnahmen wie biometrische Zugangskontrollsysteme.

Welche Datenquellen können wir nutzen?

Effektive Cyber-Defense nutzt verschiedene Arten von Daten: relevante Ereignisdaten aus den IT-Systemen und Sensoren des Unternehmens sowie kontextbezogene Informationen aus externen Quellen. Prüfen Sie, ob Ihre Spezialisten über ausreichende Kapazitäten zur Verarbeitung von sehr großen Datenmengen verfügen. Ebenso wichtig ist die Frage, ob Sie Ihre Teams kontinuierlich schulen können, damit sie mit den Fähigkeiten und Kenntnissen krimineller Cyber-Banden Schritt halten.

Wissensweitergabe: Geteilte Sicherheit ist Doppelte Sicherheit

Im SOC eines Anbieters wie Telekom Security analysieren Sicherheitsexperten nicht nur Angriffe auf die Infrastruktur Ihres Unternehmens, sondern auch auf die zahlreicher anderer Kunden. Sie sichten und bewerten täglich mehrere Milliarden sicherheitsrelevante Datensätze aus Tausenden von Quellen – fast vollständig automatisiert. Und sie teilen ihre Erkenntnisse und Erfahrungen mit ihren Kunden.

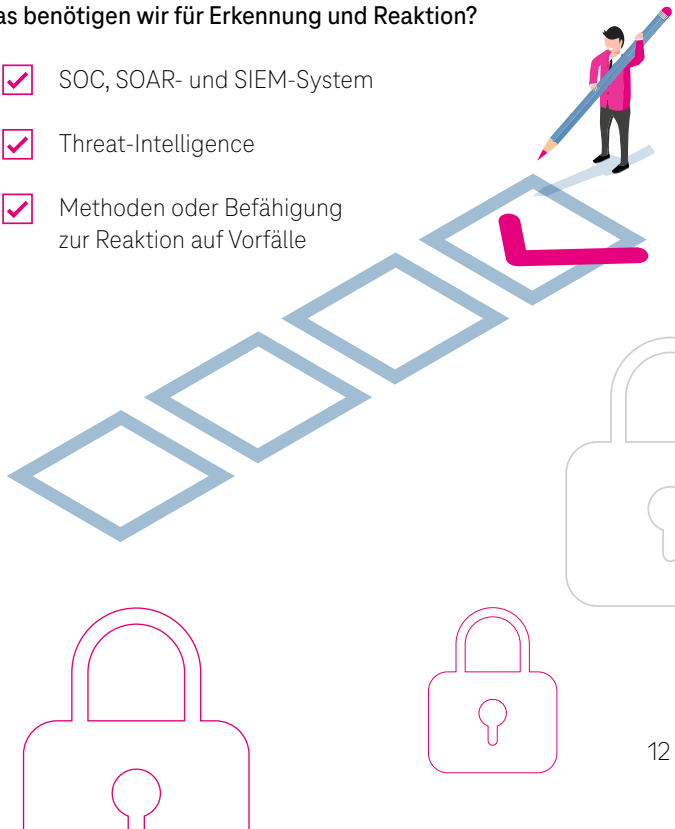
Für kleine und mittelständische Unternehmen (KMU) sind Einrichtung und Betrieb von SOCs oft zu kompliziert und zu teuer. Viele große Unternehmen aus dem Finanz- oder Automobilsektor und Betreiber kritischer Infrastrukturen haben dagegen ihre eigenen Cyber-Defense-Zentren eingerichtet. Obwohl sie im Gegensatz zu KMUs über genügend verwertbare Daten verfügen, nutzen sie allerdings oft keine automatisierte Datenanalyse. Außerdem fehlt ihnen oft das Personal, um im Falle eines Alarms sofort zu reagieren. Die Alternative: Unternehmen beauftragen SOC-Services als Managed Cyber Defense-Lösung.

Ein verwaltetes SOC kann viele Kunden gleichzeitig bedienen. Bei Anbietern wie Telekom Security bleiben die Kundendaten aus Compliance-Gründen streng getrennt. Unabhängig von der Größe und den vereinbarten Service-Level-Agreements (SLAs) profitieren jedoch alle Kunden gleichermaßen von der stetig wachsenden Erfahrung der SOC-Analysten und ihrem Wissen über die verschiedenen Angriffsvektoren.

Checkliste

Was benötigen wir für Erkennung und Reaktion?

- ☑ SOC, SOAR- und SIEM-System
- ☑ Threat-Intelligence
- ☑ Methoden oder Befähigung zur Reaktion auf Vorfälle



8. Cyber-Bedrohungen: Wie gut ist Ihre Abwehr?

Können Sie Ihre Cyber-Defense-Strategie schnell anpassen, um auf die wachsende Zahl von Bedrohungen aus dem Internet zu reagieren? Sollten Sie mehr in Erkennung, Reaktion, und Prävention investieren? Sie können die Robustheit Ihrer Verteidigung einschätzen, indem Sie folgende Fragen beantworten:

- Welche Maßnahmen ergreifen wir, um unsere Infrastruktur zu schützen?
- Kennen wir unsere wichtigsten Assets und die größten Risiken?
- Können wir abschätzen, wie viel Schaden ein unentdeckter Angriff und gestohlene Daten für unser Unternehmen bedeuten würden?
- Sind wir sicher, dass wir Hacker schnell erkennen und Angriffe abwehren können?

Können Sie die folgenden Fragen mit „Ja“ beantworten?

- Werden wir täglich über Cyber-Bedrohungen informiert?
- Überwachen wir regelmäßig, ob unsere Server und Clients Kontakt mit bekannten Trojaner-Command-and-Control-Servern haben?
- Verwenden wir SIEM-Tools, um sicherheitsrelevante Ereignisse in unserer IT zu erkennen, zusammenzuführen und zu bewerten?
- Erhalten wir aktuelle Informationen über die neuesten Sicherheitslücken in unserer Infrastruktur?
- Kümmern wir uns rechtzeitig um Schwachstellen?
- Erkennen wir Vorbereitungen für Phishing-Angriffe, bevor sie gestartet werden?
- Überprüfen wir, ob gefälschte Websites unsere Unternehmensseite simulieren?
- Wurden die Passwörter unserer Mitarbeiter jemals kompromittiert?
- Haben wir Notfallpläne für verschiedene Arten von Angriffen?

Was Sie vielleicht brauchen:

Als Organisation des Gesundheitswesens haben Sie vielleicht nicht auf jede Frage eine Antwort. In jedem Fall ist es unerlässlich, dass Sie sich über Ihren aktuellen Cyber-Sicherheits-Reifegrad im Klaren sind.

Sobald Sie Ihr Sicherheitsniveau kennen, können Sie damit beginnen, die Lücken in Ihrer Sicherheitsarchitektur zu schließen.

Telekom Security kann Ihnen dabei helfen, den Reifegrad Ihrer Cyber-Sicherheit zu bewerten, eine Roadmap zu erstellen und alle notwendigen Verbesserungen zu priorisieren und umzusetzen.

9. Immer auf der sicheren Seite: Managed Cyber Defense von Telekom Security

Unsere Kunden haben sehr unterschiedliche Anforderungen an einen Managed Cyber Defense-Service, die von der Unternehmensgröße oder ihrer Branche abhängen. Telekom Security unterstützt Organisationen des Gesundheitswesens bei der Entwicklung einer auf sie zugeschnittenen Cyber-Defense-Strategie. Für kleinere Kunden kann dies bei der Endpunktsicherheit beginnen, während sich große Unternehmen für die SOC-as-a-Service-Variante entscheiden können. Sicher ist jedoch: Jeder Kunde profitiert von unserer Threat-Intelligence-Kompetenz und erhält automatisch und unverzüglich alle neuen Erkenntnisse über Angriffsarten.

Wir haben jahrelange Erfahrung in der Bekämpfung von Cyberangriffen und verfügen über die notwendigen Tools, Technologien und Fachkräfte. Telekom Security betreibt in Bonn Europas größtes und modernstes Cyber Defense Center und unterhält ein globales Netzwerk von SOCs in Asien, Nord- und Südamerika, Afrika sowie an mehreren europäischen Standorten. Allein in Bonn überwachen 240 Experten rund um die Uhr die Sicherheit der Systeme der Telekom und unserer Kunden.

Täglich analysiert das Zentrum rund 2,5 Milliarden Hinweise auf mögliche Sicherheitsvorfälle, um die Telekom und ihre Kunden nachhaltig vor Schäden zu schützen und Prognosen über zukünftige Angriffsmuster zu erstellen. Unsere Spezialistenteams haben bereits mehr als 20 Millionen verschiedene Angriffsmuster gesammelt und profitieren von unseren vielfältigen Kontakten zu Regierungsstellen, Forschungseinrichtungen und anderen Netzbetreibern.

Im ISG Provider Lens™-Bericht „Cyber Security Services and Solutions 2022“ für Deutschland wird Telekom Security in drei Kategorien als führend genannt:

- Strategic Security Services
- Managed Security Services
- Technical Security Services

Möchten Sie mehr über unsere Managed Cyber Defense erfahren?

Unser Expertenteam berät Sie gerne, wie Sie Cyberangriffe erkennen und abwehren können. Es kann dazu beitragen, Ihr Unternehmen vor Erpressung, Datenverlust und IT-Ausfällen zu schützen. Und sie können Ihnen zeigen, wie unser Managed Cyber Defense-Service die Sicherheit Ihres Unternehmens sofort verbessert.

Quellen

1. PR Newswire
2. https://news.cgtn.com/news/3d3d774d7945444e33457a6333566d54/index.html
3. https://www.mckinsey.com/industries/life-sciences/our-insights/germanys-ehealth-transformation-makes-good-but-uneven-progress#:~:text=Telemedicine%20consultations%20have%20increased%20significantly,of%202020%20(Exhibit%201).
4. https://www.mynewsdesk.com/rolandberger/pressreleases/digital-and-physical-innovations-stimulate-the-healthcare-sector-3130832
5. https://www.healthcareitnews.com/news/emea/german-hospitals-receive-digital-health-boost
6. https://www.healthcareitnews.com/news/emea/german-hospitals-get-3-billion-funding-boost-digitalisation
7. https://www.marketopportunities.fi/home/2022/german-hospital-future-fund-hospitals-are-starting-the-implementation-of-digitalization-projects?type=business-opportunity&industry=health-and-wellbeing
8. https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people
9. https://www.forbes.com/sites/forbestechcouncil/2022/05/03/data-security-must-be-prioritized-in-the-healthcare-industry/?sh=1b1b4d581cd3
10. https://www.theverge.com/2021/9/27/22696097/hospital-ransomware-cyberattack-death-rates-patients
11. https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/
12. https://venturebeat.com/2022/05/25/report-average-time-to-detect-and-contain-a-breach-is-287-days/

KONTAKT
security@telekom.de

HERAUSGEBER
Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn
Deutschland