Gestaltung einer sicheren digitalen Zukunft für das Gesundheitswesen

Weltweit führen Krankenhäuser und medizinische Einrichtungen neue digitale Technologien wie intelligente medizinische Geräte, Telemedizin und Clouds ein, um Patienten eine bessere Versorgung und individuellere Gesundheitsleistungen zu bieten.

Zugleich ist das Gesundheitswesen ein Bereich, der aggressiv von Cyber-Kriminellen angegriffen wird und bei Datenpannen die höchsten Kosten aufweist.[1] Moderne Gesundheitsleistungen sollten deshalb nach „Secure by Design"-Prinzipien entwickelt werden, die die Sicherheit bereits bei der Entwicklung berücksichtigen – ein Muss, damit das Gesundheitswesen vor dieser täglichen Angriffsflut gut geschützt ist.

„Im Gesundheitswesen entstehen im Durchschnitt weiterhin die höchsten Kosten bei Datenschutzverletzungen."

IBM: „Cost of a Data Breach Report 2020".

Eine sichere digitale Zukunft für Krankenhäuser

Mit dem im Oktober 2020 in Kraft getretenen Krankenhauszukunftsgesetz (KHZG) unterstützt die Bundesregierung die Digitalisierung von Krankenhäusern mit einem umfassenden Investitionsprogramm. Gefördert werden Projekte wie:

1. Entwicklung digitaler Patientenportale
2. Einführung eines digitalen Medikationsmanagements
3. Einrichtung von Systemen zur elektronischen Dokumentation von Pflege- und Behandlungsleistungen
4. Verbesserung der IT-Sicherheit

Erarbeitung von Strategieplänen für die Digitalisierung und Security

Besonders hervorzuheben ist die Stärkung der IT-Sicherheit. Das Gesetz sieht ausdrücklich vor, dass 15 % der Mittel in die Entwicklung einer besseren Cyber-security-Infrastruktur fließen müssen. Der Gesetzgeber hat folglich erkannt, wie wichtig die Integration der Security in die digitale Transformation von Gesund-heitseinrichtungen ist. Denn nur so lässt sich eine sichere digitale Zukunft aufbauen, in der der Schutz von Patientendaten, bei Gesundheitseinrichtungen gespeicherten Informationen und die Widerstandsfähigkeit des Gesundheitswe-sens gegen Angriffe gewährleistet ist.

Resilienz gegen Cyber-Angriffe entwickeln

Seit Beginn der Corona-Pandemie eskalieren die Angriffe auf den Gesund-heitssektor. Im Herbst 2020 verzeichnete die Bundesregierung allein 43 Cyber-Angriffe auf kritische Infrastrukturen (KRITIS) – mehr als doppelt so viele wie im gesamten Vorjahr.[2]

Die Risiken dieser Cyber-Angriffe gehen weit über die Offenlegung von Patientendaten hinaus. Lebensnotwendige Dienstleistungen können unterbrochen und schlimmstenfalls Menschenleben gefährdet werden. Der Anschlag auf ein Universitätsklinikum im Jahr 2020, bei dem eine Patientin wegen eines Cyber-Angriffs starb, ist ein tragischer Beleg dafür.[3]

Die Forderung der Regierung, die Security in jede digitale Initiative zu integrieren, fördert die Einführung sicherer digitaler Dienstleistungen in Krankenhäusern. Von dieser Entwicklung profitieren besonders Patienten und Wissenschaftler, während zugleich die Resilienz gegen Angriffe und die Erfüllung von Datenschutzanforderungen verbessert werden.

Einführung einer sicheren, agilen Plattform für den digitalen Erfolg

Für die Entwicklung und Bereitstellung sicherer digitaler Dienstleistungen muss die IT-Infrastruktur zu einer sicheren, agilen Umgebung werden. Hier bieten Cloud-Plattformen entscheidende Vorteile.

Bei Cloud-Lösungen entfallen z. B. die Bereitstellung, Wartung und Sicherung von Hardware. IT-Teams können sich so ganz auf die Entwicklung von Diensten konzentrieren. Sämtliche Ressourcen sind sofort verfügbar und die Skalierung lässt sich automatisch an den Bedarf anpassen. Die Security wird einfach mit zusätzlichem Code integriert, um Cloud-Ressourcen inhärent und automatisch zu schützen.

Die Cloud erleichtert zudem die Modernisierung lokaler Dienste wie SAP und Archivierung. Auch lassen sich Benutzer, Geräte und Dienste über die Cloud verwalten, überwachen und schützen – ganz gleich, ob diese sich im Standort befinden (On-Premises) oder per Fernzugriff (Remote) verbunden sind. Wichtige Dienste profitieren so von mehr Agilität und Skalierbarkeit, wobei die Sicherheit von Anfang an integriert ist.

Cloud-Initiativen ermöglichen nicht nur die Modernisierung der Infrastruktur, sondern auch fortschrittliche Dienste wie KI und Analysen. Diese lassen sich sicher in digitale Angebote integrieren, damit Krankenhäuser die zukünftige Patientenversorgung besser gestalten können.

Sicherheit und Agilität mit der Cloud

Planung der Integration von Clouds und Security

Das Erstellen und Schützen dieser neuen Umgebungen mag wie eine gewaltige Aufgabe erscheinen. Sie werden damit aber nicht alleingelassen: Fortinet als führender Cybersecurity-Anbieter und AWS-Technologiepartner kann Ihnen zusammen mit AWS dabei helfen, Ihre Digitalisierung zu planen und erfolgreich umzusetzen.

Gemeinsam können wir Ihre Entwickler und Security-Teams auf die AWS-Cloud-Plattform vorbereiten – vom Modell der gemeinsamen Verantwortung (AWS Shared Responsibility Model) und Sicherheitsaspekten bis hin zu Best Practices für die Entwicklung. Diese Schulungen verkürzen auch Projektzeiten, weil Ihre Teams dann darauf vertrauen können, von Grund auf sichere Cloud-Dienste zu entwickeln.

Fortinet bietet mit der Fortinet Security Fabric für AWS ein breites, integriertes Portfolio an Cloud-Sicherheitslösungen, die agile Cloud-Dienste durch agile Cloud-Security schützen. Einrichtungen im Gesundheitswesen können so besser ihrer Verantwortung für den Schutz von Daten, Cloud-Anwendungen und den Zugang zur Cloud nachkommen. Die Bereitstellung und Sicherheit der zugrunde liegenden Infrastruktur übernimmt dagegen AWS.

aws partner network
Advanced
Technology
Partner
Security Competency
Networking Competency
Marketplace Seller
Public Sector Partner

Dieses Zusammenspiel wird durch integrierte Funktionen vereinfacht, die den erweiterten Schutz dynamisch bereitgestellter, umfassenderer Cloud-Workloads automatisieren. Ein weiterer Vorteil: Verwenden Automatisierungsfunktionen die AWS-Dienste, kann das die Bedrohungserkennung und -reaktion verkürzen sowie Risiken und mögliche Beeinträchtigungen von Diensten minimieren.

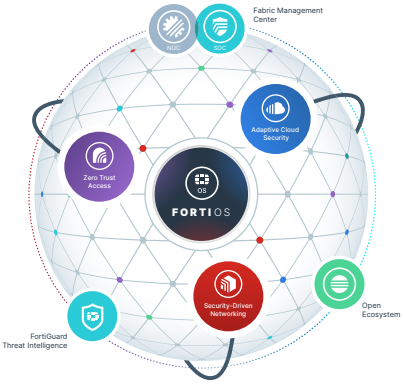
Eine sichere, skalierbare und ausfallsichere Konnektivität ermöglicht die Schaffung eines integrierten Ökosystems, das Cloud-, Remote- und lokale Dienste sowie externe Partnerschaften umfasst. Diese optimierte Bereitstellung sorgt dafür, dass Dienste die Anforderungen hinsichtlich Verfügbarkeit, Reaktionsfähigkeit und Sicherheit zuverlässig erfüllen.

Planen Sie Ihre sichere digitale Zukunft mit Fortinet und AWS

Entscheidend für eine sichere Digitalisierung und Cloud-Nutzung ist die Zusammenarbeit aller Beteiligten. Fortinet und AWS kooperieren weltweit mit Gesundheitseinrichtungen, um eine erfolgreiche digitale Transformation zu gewährleisten. Gemeinsam können wir Sie bei der Planung eines Digitalisierungsprozesses unterstützen, der die Cloud und die Sicherheit bereits integriert. Das erleichtert auch die Definition sicherer, digitaler Dienste, für die Sie eventuell Fördergelder beantragen möchten. Mögliche Projekte wären zum Beispiel:

- Schaffung eines sicheren, selbstheilenden und vernetzten Gesundheitsökosystem
- Entwicklung von Anwendungen und Dienste, die von Grund auf agil und sicher sind
- Schutz von Krankenhaus- und Patientendaten mit einem Zero-Trust-Ansatz
- Verbesserung der Sicherheit mit einer automatisierten Bedrohungsabwehr
- Steigerung der Agilität und Senkung der laufenden Kosten mit über die Cloud bereitgestellten Diensten

Lassen Sie uns besprechen, wie wir gemeinsam eine sichere digitale Zukunft im Gesundheitswesen gestalten können.



Fortinet Security Fabric für AWS

1. IBM: „Cost of a Data Breach Report 2020“.
2. Antwort auf die Kleine Anfrage der Abgeordneten Dr. Jürgen Martens, Stephan Thomae, Grigorios Aggelidis, eines weiteren Abgeordneten und der FDP-Fraktion (Drucksache 19/23851)
3. https://www.swisscybersecurity.net/cybersecurity/2020-09-18/frau-stirbt-nach-cyberangriff-in-deutschem-krankenhaus

www.fortinet.com/de

13. August 2021, 8: 26 Uhr

1222752-0-0-DE