MYRA

WHITEPAPER

IT-Sicherheit schafft die Vertrauensbasis für E-Health Lösungen

IT-Sicherheit schafft die Vertrauensbasis für E-Health

Patientinnen und Patienten in Deutschland erleben einen grundlegenden Wandel im Gesundheitswesen. Neue Digitallösungen wie die elektronische Patientenakte (ePA), das E-Rezept, die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) oder der jüngst beschlossene digitale Impfpass ersetzen zunehmend ihre analogen Pendants.

Detaillierte Informationen zu Untersuchungen, Diagnosen, Therapiemaßnahmen, Behandlungsberichten, Impfungen oder Medikationsplänen werden elektronisch angelegt, archiviert und kommuniziert. Das Smartphone entwickelt sich zum zentralen Gesundheits-Hub als Schnittstelle zu Arztpraxen, Krankenkassen und Kliniken. Diese weitreichende Transformation ermöglicht immense Effizienzsteigerungen. Kritische Gesundheitsdaten liegen jederzeit vor, überflüssige Mehrfachdiagnosen und Untersuchungen bei einem Wechsel der Arztpraxis erübrigen sich.

> *Nur wenn wir die Chancen der Digitalisierung nutzen, können wir die Patientenversorgung besser machen.*
>
> Ex-Bundesgesundheitsminister Jens Spahn zur Bedeutung digitaler Prozesse im Gesundheitswesen – WiWo 12.4.2019

Damit die Vorzüge der Digitalisierung in die Praxis einfließen können, müssen die Lösungen von den Patient:innen angenommen werden. Dafür bedarf es konkreter Mehrwerte und vor allem Vertrauen in die Technologie. Letztere will das Bundesgesundheitsministerium (BMG) durch strikte Datenschutzvorgaben aufbauen.

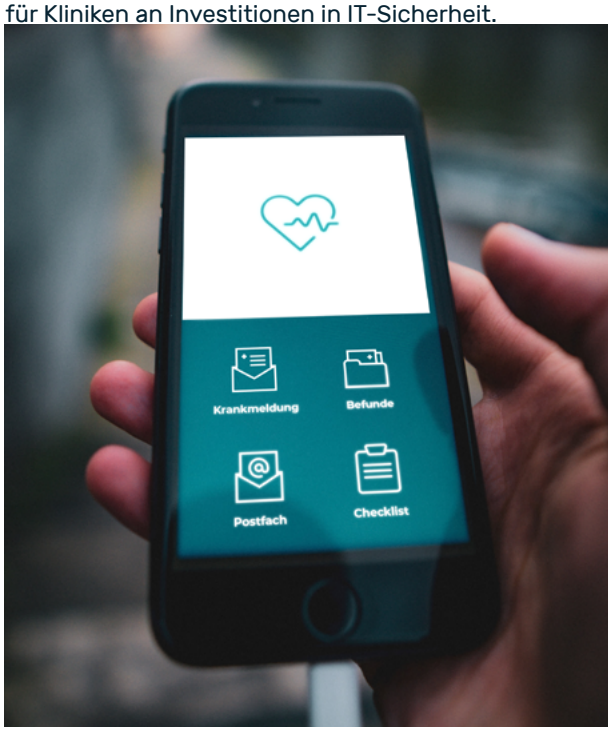
Der Schutz kritischer Patientendaten zählt zu den obersten Prinzipien aller medizinischen Digitallösungen. Das wiederum erfordert IT-Sicherheit auf höchstem Niveau. Aus diesem Grund koppelt das Krankenhaus-Zukunftsgesetz (KHZG) die Fördermittel für Kliniken an Investitionen in IT-Sicherheit.

E-Health: die kritische Bedeutung von Webportalen

Die Nutzung von Online-Services gehört für einen Großteil der Bevölkerung zum Alltag. Webdienste wie etwa für Mailing, Office oder Media Streaming haben sich in den vergangenen Jahren enorm weiterentwickelt und stehen klassischen Programmen und Apps auf PC, Tablet oder Smartphones in nichts nach.

Diese Leistungsfähigkeit und Stabilität erwarten Patient:innen auch von neuen Gesundheitsportalen im Netz. Kommt es hier zu performancebedingten Verzögerungen oder Ausfällen, wirft das ein schlechtes Bild auf die zugrunde liegende Technologie. Selbst wenn sensible Daten per se nicht gefährdet sind, genügt bereits ein stotternder Webauftritt, um das Vertrauen in eine E-Health-Lösung entscheidend zu schwächen.

Aus diesem Grund müssen Leistungsfähigkeit und Stabilität speziell dort sichergestellt sein, wo die Patient:innen mit der Lösung interagieren. Dasselbe Maß an technischer Ausgereiftheit erwarten auch Ärzteschaft und Klinikpersonal. Die Technologie soll den beruflichen Alltag erleichtern und nicht für zusätzliche Komplexität sorgen.



Diagnosen, Therapiemaßnahmen, Medikationspläne und vieles mehr lässt sich mit der ePA mobil per Smartphone-App verwalten. Damit die E-Health-Lösung zum Erfolg wird, müssen Sicherheit, Datenschutz und Performance überzeugen.

Auslastung und externe Angriffe: Herausforderungen für die digitale Infrastruktur

Umfassende E-Health-Lösungen wie die ePA oder der digitale Impfpass sind für die Nutzung durch Millionen von Bürgerinnen und Bürgern konzipiert. Online-Portale und Schnittstellen zu diesen Diensten müssen daher in der Lage sein, selbst bei unvorhersehbaren Traffic-Spitzen fehlerfrei zu arbeiten.

Die Corona-Pandemie hat gezeigt, wie stark kritische Dienste auf flexible und schnelle Skalierbarkeit angewiesen sind. Besonders zu Beginn der Pandemie mussten die offiziellen Informationsportale der Gesundheitsbehörden bis zu 100-mal mehr Last stemmen als zu regulären Zeiten. Dienste ohne ausreichende Server-Kapazitäten oder Überlastungsschutz gehen in solchen Szenarien zwangsläufig in die Knie.

Mögliche Folgen von Cyberattacken auf E-Health-Lösungen und Telematik:

- Verzögerte Übertragung kritischer Notfalldaten
- Erschwerte Medikation in Notfallsituationen
- Überflüssige Mehrfachuntersuchungen
- Verzögerte Behandlung
- Kein Zugriff der Patient:innen auf ihre eigenen Gesundheitsdaten
- Strafzahlungen bei Datenschutzverletzungen & Datenabfluss

Stark beanspruchte Infrastrukturen sind außerdem ein bevorzugtes Ziel für externe Angriffe. Wenn Systeme ohnehin an der Belastungsgrenze arbeiten, genügen bereits geringe negative Einflüsse von außen, um maximale Wirkung zu erzielen. Cyberkriminelle schonen damit die eigenen Ressourcen und provozieren mit ihren Attacken dennoch schwerwiegende Ausfälle. Cybervorfälle werden daher von der Allianz aktuell als das größte Risiko für das Gesundheitswesen gelistet (Allianz Risk Barometer – Results Appendix 2024).

Aber auch IT-Infrastrukturen mit ausreichend Reserven sind zunehmend durch externe Angriffe gefährdet. Seit Beginn der Corona-Pandemie stehen das Gesundheitswesen sowie andere kritische Sektoren vermehrt unter Beschuss. Cyberkriminelle greifen aus finanzieller oder politischer Motivation gezielt existenzielle Dienste an. Das zeigen sowohl die Mitigationsdaten von Myra als auch Untersuchungen von Interpol, dem Bundes-kriminalamt (BKA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

Datenschutzhürden bei der Dienstleisterwahl

Gesundheitsdaten gelten laut Art. 9 Datenschutz-Grundverordnung (DSGVO) als besonders sensibel und erfordern daher entsprechend hohe Schutzmaßnahmen - dazu gehören auch Informationen zu Impfungen und Impfterminen. Die hohen Anforderungen an IT-Sicherheit für E-Health-Lösungen spiegeln sich ebenfalls in den regulatorischen Vorgaben des BMG und der gematik wider, die zunehmend anspruchsvoller ausfallen. Dieser Trend wird sich fortsetzen – insbesondere im Zusammenhang mit kritischen Infrastrukturen. E-Health-Betreiber, Kliniken und Ärzteschaft werden sich daher intensiver mit der internen Datenarchitektur sowie mit Compliance-relevanten Themen befassen müssen. Unterstützende Informationen zur Umsetzung finden sich etwa im branchenspezifischen B3S-Standard.

Als effiziente Alternative zum aufwendigen Inhouse-Betrieb bietet sich das Outsourcing der IT-Sicherheit an. Managed Service Provider übernehmen Implementierung, Wartung und Betrieb von erforderlichen Sicherheitslösungen und machen dadurch wertvolle Ressourcen für das Kerngeschäft frei. Unternehmen vermeiden mit dieser Strategie zusätzliche Aufwendungen für Software, Hardware und Personal. Angesichts eines umkämpften Arbeitsmarktes sind hochqualifizierte IT-Fachkräfte ohnehin nur schwer zu finden. Laut Bitkom sind in Deutschland 149.000 IT-Stellen quer durch alle Branchen unbesetzt (Stand Dez. 2023). Im Schnitt dauert es fast acht Monate, bis geeignete Fachleute für offene Stellen gefunden sind.

Allerdings muss der Service Provider gut ausgesucht sein. Zwar besteht mit dem EU-US Data Privacy Framework ein neues Abkommen zum interkontinentalen Transfer von Daten. Allerdings haben die Erfahrungen mit den Vorgängern „Safe Harbor“ und „Privacy Shield“ gezeigt, wie schnell die Rechtslage kippen kann. Aufgrund der konträren Positionierung von europäischer DSGVO und US-Recht bleiben Datenschutzbestimmungen nur schwer umsetzbar. Durch die Wahl lokaler Anbieter, die derselben Rechtsprechung unterliegen und höchste Datenschutzanforderungen erfüllen, lassen sich solche Hürden umgehen.

Das macht Myra zum richtigen Partner für E-Health

- DSGVO-konformer Spezialanbieter mit Branchenexpertise
- Leistungserbringung in deutschen Rechenzentren
- Myra erfüllt alle 37 Leistungsmerkmale des BSI für qualifizierte DDoS-Mitigation-Dienstleister
- Security Operations Center: 24/7 Full-Service-Betreuung durch unsere IT-Fachleute
- ISO 27001 auf Basis von IT-Grundschutz: RZ-Standorte & Institution zertifiziert
- BSI-KRITIS-qualifiziert, PCI-DSS-zertifiziert, Trusted-Cloud-zertifiziert, BSI C5

Myra ist der Spezialanbieter für das Gesundheitswesen

Myra Security entwickelt und betreibt hochzertifizierte Schutzlösungen zur Absicherung digitaler Geschäftsprozesse. Als Spezialanbieter für sensible und kritische Infrastrukturen haben wir langjährige Erfahrung im Schutz von Unternehmen und Organisationen im Gesundheitswesen, in der Finanz- und Versicherungsindustrie sowie in den Sektoren KRITIS und der öffentlichen Verwaltung. Kunden in diesen hochregulierten Bereichen profitieren von zertifizierter Sicherheit und Konformität mit DSGVO, NIS-2, DORA, IT-SiG, BSI-KRITIS und branchenspezifischen Standards.

Myra stellt sicher, dass Online-Portale von Bundesbehörden wie Infektionsschutz.de der Bundeszentrale für gesundheitliche Aufklärung (BZgA) sowie das Webportal des BMG für Millionen von Bürgerinnen und Bürgern jederzeit erreichbar sind.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSI KRITIS-qualifiziert | EU-DSGVO konform | BSI C5 Testat | Trusted Cloud | IDW PS 951 ISAE 3402

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard | KRITIS-qualifiziert nach §3 BSI-Gesetz | Konform mit der (EU) 2016/679 Datenschutz-Grundverordnung | BSI-C5-Testat | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister |

Myra Security ist der neue Maßstab für globale IT-Sicherheit

Die Myra-Technologie überwacht, analysiert und filtert schädlichen Internet-Traffic bevor virtuelle Angriffe einen realen Schaden anrichten. Unsere zertifizierte Security-as-a-Service-Plattform schützt Ihre digitalen Geschäftsprozesse vor vielfältigen Risiken wie DDoS-Angriffen, Bot-Netzwerken und Angriffen auf Datenbanken.

Bundesministerium für Gesundheit | ITSG | msc Munich Security Conference | Barmenia EINFACH. MENSCHLICH.

BZgA Bundeszentrale für gesundheitliche Aufklärung | BIOSCIENTIA MEDIZIN. LABOR. SERVICE. | Smartifyit! | STADT REGENSBURG