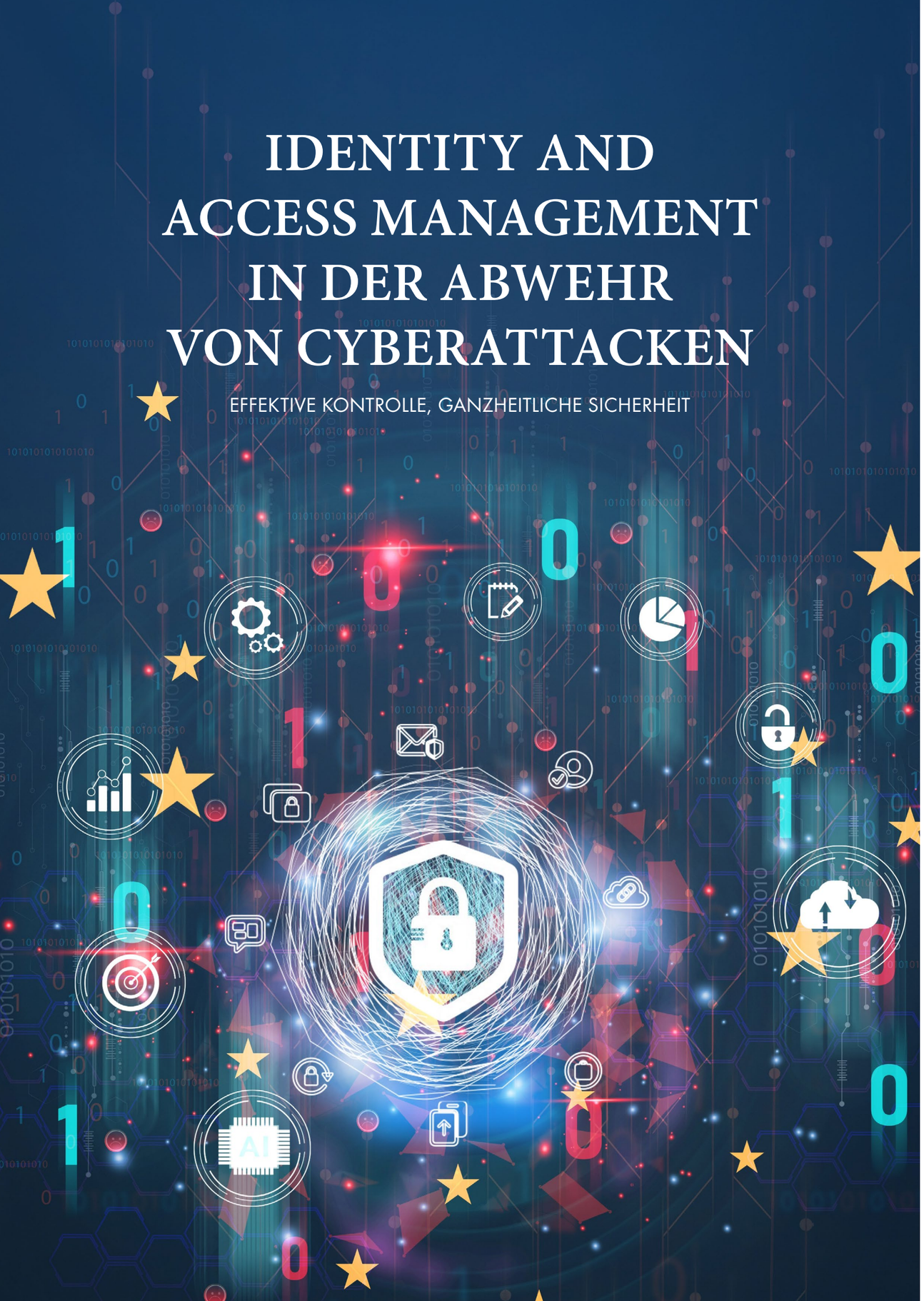
IDENTITY AND ACCESS MANAGEMENT IN DER ABWEHR VON CYBERATTACKEN

EFFEKTIVE KONTROLLE, GANZHEITLICHE SICHERHEIT



Die Digitalisierung ist längst ein unverzichtbarer Bestandteil des Gesundheitswesens. Systeme wie elektronische Patientenakten, digitale Bildgebung und automatisierte Verwaltungsprozesse haben die Effizienz und Qualität der Patientenversorgung deutlich verbessert – daran gibt es keinen Zweifel. Doch mit den Chancen kommen auch Risiken. Gesundheitseinrichtungen gehören ganz klar zu den bevorzugten Zielen von Cyberkriminellen.

Kritische Infrastrukturen (KRITIS) sind in besonderem Maße auf eine funktionierende IT angewiesen. Erfolgreiche Angriffe auf KRITIS-Betreiber können nicht nur zu volkswirtschaftlichen Schäden führen, sondern im Falle von Krankenhäusern auch gefährliche Auswirkungen auf die Patientenversorgung haben. Die Bedrohungslage bleibt jedoch angespannt, die Zahl der Cybervorfälle steigt. 2024 gingen beim Bundesamt für Sicherheit in der Informationstechnik (BSI) 726 Meldungen zu Vorfällen ein. 2023 waren es 490.

Ransomware-Angriffe sind besonders häufig. Dabei verschlüsseln Angreifer die Systeme und fordern Lösegeld. Die durchschnittliche Ausfalldauer nach einer Ransomware-Attacke in Deutschland variiert, je nach Art des Angriffs, Größe der Organisation und Maßnahmen zur Wiederherstellung. Die durchschnittliche Dauer zur Wiederherstellung der Betriebsfähigkeit nach einem Angriff dauert in vielen Fällen 1–3 Wochen, wenn keine Lösegeldzahlung erfolgt und Organisationen auf Backups zurückgreifen. Unternehmen, die Lösegeld zahlen, benötigen oft länger, da die Wiederherstellung komplex ist und mehrere Methoden kombiniert werden müssen.

Dabei gilt es Branchenunterschiede zu beachten, dass kritische Infrastrukturen wie das Gesundheitswesen häufig länger benötigen, da Systeme redundant und komplexer sind, was die Wiederaufnahme des Betriebs erschwert. Für Einrichtungen, in denen jede Sekunde zählt, ist dies eine gefährliche Zeitspanne, die nicht nur die Effizienz, sondern auch die Patientensicherheit gefährdet und nicht hinnehmbar ist.

Drei zentrale Probleme kennzeichnen die aktuelle Sicherheitslage im Gesundheitswesen. Erstens fehlt es häufig an einer klaren Kontrolle über Zugänge. Ohne standardisierte Prozesse zur Verwaltung von Benutzerkonten und Berechtigungen entstehen zwangsläufig Sicherheitslücken. Das Teilen von Passwörtern oder die Weiterverwendung veralteter Zugriffsrechte sind nur zwei Beispiele dafür. Zweitens nutzen viele Einrichtungen IT-Infrastrukturen, die nicht mehr auf dem neuesten Stand der Technik sind. Veraltete Systeme sind anfällig für moderne Bedrohungen, da ihnen die notwendigen Sicherheitsupdates fehlen. Drittens sind Gesundheitsdaten ein besonders attraktives Ziel für Cyberkriminelle, da sie nicht nur für Identitätsdiebstahl und Erpressung genutzt werden können, und daher im Darknet hohe Preise erzielen. Das Gesundheitswesen muss sich dieser Tatsache stellen und nachhaltige sowie effiziente Lösungen finden, um die Sicherheitslage zu verbessern, ohne den Betrieb zu stören.

Lösungsansätze

Die Implementierung eines Identity and Access Managements (IAM) ist der richtige Weg, um die Sicherheitslage zu verbessern. Dieses Sicherheitssystem stellt sicher, dass der Zugriff auf Unternehmensdaten streng kontrolliert und geschützt ist. IAM-Lösungen setzen auf verschiedene Schlüsseltechnologien, um Sicherheit und Effizienz zu maximieren.

Eine solche Technologie ist die Multi-Faktor-Authentifizierung (MFA). Sie ergänzt das traditionelle Passwort durch eine zusätzliche Sicherheitsebene. Das kann beispielsweise ein temporärer Code sein, der an ein Mobilgerät gesendet wird, oder auch biometrische Daten wie Fingerabdrücke. Diese Methode macht es Angreifern extrem schwer, unberechtigt auf Systeme zuzugreifen.

Ein weiteres wichtiges Element von IAM ist Single Sign-On (SSO). Mitarbeitende müssen sich nicht mehr für jedes System separat einloggen. Sie können sich einmal authentifizieren und erhalten dann sicheren Zugriff auf alle benötigten Anwendungen. Die Organisation kann in Verbindung mit bspw. MFA und weiteren Richtlinien das Sicherheitsniveau ganzheitlich verbessern. Das spart Zeit, verringert die Komplexität

IAM-LÖSUNGEN GEHEN TIEF IN DIE SICHERHEITSARCHITEKTUR HINEIN. SIE BIETEN NICHT NUR SCHUTZ VOR EXTERNEN ANGRIFFEN, SONDERN AUCH EINE EFFEKTIVE KONTROLLE ÜBER INTERNE ZUGRIFFE UND GEWÄHRLEISTEN SO EINE GANZHEITLICHE SICHERHEIT.

Dirk Wahlefeld
Principal Solutions Architect
Imprivata
www.imprivata.com/de

und erhöht die Benutzerfreundlichkeit – und ist damit ein entscheidender Faktor in stressigen Arbeitsumgebungen wie Krankenhäusern.

Eine automatisierte Berechtigungsverwaltung stellt zudem sicher, dass die Zugriffsrechte von Mitarbeitenden regelmäßig überprüft und bei Bedarf angepasst werden. So wird verhindert, dass ehemalige Mitarbeitende oder Mitarbeitende mit geänderten Aufgabenbereichen weiterhin Zugriff auf sensible Daten erhalten.

Es gibt auch andere Schutzstrategien, die zur Verbesserung der Cybersicherheit eingesetzt werden können. Eine Möglichkeit sind netzwerkbasierte Schutzmaßnahmen wie Firewalls und Intrusion Detection Systems (IDS). Diese Technologien schützen vor externen Bedrohungen. Allerdings können sie keine umfassende Kontrolle über den internen Zugriff auf Daten gewährleisten.

Eine weitere Möglichkeit sind Lösungen zur Sicherung von Endgeräten, die Sie unbedingt in Betracht ziehen sollten. Diese Endpoint-Protection-Dienste bieten Schutz für die Geräte selbst – aber sie können nicht sicherstellen, dass die Zugriffsrechte der Benutzer korrekt verwaltet werden.

Diese Alternativen sind nützliche Ergänzungen, keine Frage. Aber IAM-Lösungen wie die von Imprivata gehen tiefer in die Sicherheitsarchitektur hinein. Sie bieten nicht nur Schutz vor externen Angriffen, sondern auch eine effektive Kontrolle über interne Zugriffe und gewährleisten so eine ganzheitliche Sicherheit – und das alles aus einer Hand.

Die Vorteile von IAM im Gesundheitswesen

IAM-Lösungen bieten eine ganze Reihe von Vorteilen. Die deutlich verbesserte Sicherheit ist zweifelsohne einer der größten Pluspunkte. Maßnahmen wie MFA und SSO reduzieren Angriffsflächen erheblich. Selbst wenn Angreifern ein Passwort bekannt wird, bleibt der Zugang durch die zweite Authentifizierungsstufe geschützt.

IAM steigert zudem die Effizienz von Arbeitsabläufen. SSO macht es überflüssig, sich mehrfach in verschiedene Systeme einzuloggen. Das ist ein entscheidender Vorteil, insbesondere in Notaufnahmen, wo Sekunden über Leben und Tod entscheiden können.

Ein weiterer Vorteil ist, dass es die Einhaltung gesetzlicher Vorgaben erheblich erleichtert. Datenschutzgesetze wie die DSGVO oder HIPAA verlangen eine lückenlose Dokumentation und Kontrolle von Zugriffen – und IAM-Systeme erfüllen diese Anforderungen. IAM-Systeme bieten integrierte Tools, die diese Anforderungen automatisch erfüllen und so Compliance-Prozesse erheblich erleichtern.

Schließlich überzeugen IAM-Lösungen durch hohe Flexibilität und Skalierbarkeit. Sie lassen sich exakt an die spezifischen Anforderungen und die Größe jeder Organisation anpassen – von kleinen Kliniken bis hin zu großen Krankenhausketten.

Herausforderungen und Risiken

Es gibt Herausforderungen und Risiken bei der Implementierung von IAM-Systemen, das sollte man nicht leugnen. Die Kosten für die Anschaffung und Integration mögen anfangs hoch sein, doch sie rechnen sich. Diese Investition zahlt sich schnell aus! Denn sie verhindert Sicherheitsvorfälle und senkt langfristig die Betriebskosten.

Die technische Komplexität der Systeme stellt eine weitere Hürde dar. Die Integration erfordert Fachwissen. Doch keine Sorge: Anbieter wie Imprivata bieten umfangreiche Unterstützung, um diesen Prozess so reibungslos wie möglich zu gestalten.

Schließlich besteht eine Abhängigkeit vom Anbieter, was für einige Organisationen ein Nachteil sein könnte. Eine sorgfältige Auswahl und transparente Vertragsmodelle minimieren dieses Risiko jedoch auf ein absolutes Minimum und sorgen für langfristige Planungssicherheit.

Kosten und Nutzen

Die Einführung eines IAM-Systems ist eine wichtige Investition, die sich auszahlt. Die Hauptkosten entstehen durch die Anschaffungs- und Lizenzgebühren sowie die Schulung der Mitarbeitenden. Doch der Nutzen ist enorm: Ein Krankenhaus mit 1.000 Mitarbeitenden hat durch die Implementierung von SSO jeden Monat rund 200 Arbeitsstunden eingespart. Auch die Anzahl der Sicherheitsvorfälle sank in Einrichtungen mit IAM-Systemen um bis zu 70 %. Das zeigen Erfahrungsberichte von Imprivata.

Die Einführung eines IAM-Systems erfolgt in mehreren Schritten. Als erstes wird die aktuelle IT-Sicherheitslage analysiert, um Schwachstellen und Anforderungen zu identifizieren. Im nächsten Schritt wird ein geeigneter Anbieter ausgewählt. Dabei sind Faktoren wie Benutzerfreundlichkeit und Skalierbarkeit entscheidend. In einer Pilotphase testen wir das System in einer Abteilung, um sicherzustellen, dass es auch in der Praxis funktioniert.

Im Anschluss werden die Mitarbeitenden geschult, damit sie das System korrekt nutzen können. Die Einführung erfolgt schrittweise, um den laufenden Betrieb nicht zu stören. Schließlich optimieren wir das System kontinuierlich, um auf neue Bedrohungen und Anforderungen zu reagieren.

Fazit: Ein Sicherheitsnetz für die digitale Zukunft

Cyberangriffe auf Gesundheitseinrichtungen sind eine ernsthafte Bedrohung. Sie gefährden nicht nur IT-Systeme, sondern auch Patienten und ihr Vertrauen in das Gesundheitssystem. Moderne IAM-Lösungen von Imprivata sind die Antwort auf diese Risiken. IAM ist mehr als eine Sicherheitsmaßnahme – es ist eine strategische Investition in eine sichere und effiziente digitale Zukunft.

Dirk Wahlefeld

PLUS

Besuchen Sie unsere **Website**, nehmen Sie an unserem **Einführungswebinar** teil oder **kontaktieren Sie uns** direkt für eine individuelle Beratung.