tenfold

Identity & Access Management im Krankenhausbetrieb

Worauf Gesundheitseinrichtungen im KRITIS-Umfeld achten müssen.

Überblick

- Digitalisierung erfordert Schutzmaßnahmen: Schutz für Kritische Infrastrukturen (KRITIS)
- Branchenspezifische Sicherheitsstandards (B3S) für Krankenhäuser und andere Einrichtungen aus dem Gesundheitsbereich
- Anforderungen an das Identitäts- und Rechtemanagement laut B3S
- Sicherheit für Krankenhausinformationssysteme

Einleitung

Krankenhäuser befinden sich in einer Zwickmühle: Um ihren Patienten die besten Behandlungsmöglichkeiten anbieten zu können, braucht es modernste Technologien. Deren Grundlage ist die fortschreitende Digitalisierung, die neben all ihrer Vorteile auch enorme Gefahrenpotenziale birgt. Gerade im Bereich der IT-Security.

Datendiebstahl und Cybercrime sind heute die beiden am schnellsten wachsenden Formen von Kriminalität. Alleine im Jahr 2019 wurden hier weltweit Schäden in Höhe von 600 Milliarden US-Dollar verzeichnet. Eine Summe, die selbst die jährlichen Ausgaben im gesamten deutschen Gesundheitswesen (rund 400 Milliarden US-Dollar) deutlich übersteigt.

Auch Krankenhäuser und andere medizinische Einrichtungen werden immer wieder zur Zielscheibe von Cyber-Angriffen. So waren etwa Ende 2019 zahlreiche Einrichtungen des Deutschen Roten Kreuzes im Saarland von einer Hacker-Attacke betroffen. Inklusive Erpressungsversuch und Lösegeldforderung.

Somit drängen sich folgende Fragen auf: Wie können sich Krankenhäuser und andere Einrichtungen im Gesundheitswesen bestmöglich schützen? Und wie gelingt der Spagat zwischen dem Wunsch nach technologischem Fortschritt und einer Compliance-gerechten Infrastruktur? Mögliche Antworten liefert der Staat.

Digitalisierung erfordert Schutzmaßnahmen: Schutz für Kritische Infrastrukturen (KRITIS)

Mit der Cyber-Sicherheitsstrategie für Deutschland hat die Bundesregierung im Jahr 2016 einen Fokus auf das Thema IT-Security gelegt: Ein Kernziel ist dabei die Verbesserung der Sicherheit durch den Schutz von IT-Systemen. Das sogenannte IT-Sicherheitsgesetz setzt dort an, wo Betriebsausfälle besonders dramatische Folgen für die Bevölkerung mit sich bringen, bei den IT-Systemen der Kritischen Infrastrukturen (kurz: KRITIS). Zu den so genannten KRITIS zählen unter anderem Einrichtungen und Organisationen aus den Bereichen Gesundheitswesen, Strom- und Wasserversorgung, Finanzwesen oder Telekommunikation. Betreiber kritischer Anlagen müssen demnach ein Mindestniveau an IT-Sicherheit einhalten und erhebliche Störungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden.

Die Branchen selbst können durch das Erarbeiten so genannter branchenspezifischer Sicherheitsstandards (B3S) Maßnahmen zusammenfassen, die für ihren Bereich sinnvoll und notwendig sind und sie dem BSI zur Prüfung vorlegen.

Branchenspezifische Sicherheitsstandards (B3S) für Krankenhäuser und andere Einrichtungen aus dem Gesundheitsbereich

Die Deutsche Krankenhausgesellschaft (DKG) hat für kritische Einrichtungen aus dem Gesundheitsbereich einen branchenspezifischen Sicherheitsstandard (B3S) erarbeitet, nach dem Krankenhäuser ihre IT-Sicherheitsmaßnahmen ausrichten müssen. Dieser gilt für Kliniken ab einer vollstationären Fallzahl von 30.000 pro Jahr. Doch auch für kleinere Einrichtungen sind diese Vorgaben als Richtlinie für mehr Versorgungssicherheit hilfreich. Krankenhäuser, die als kritische Infrastruktur gelten, müssen regelmäßig den Nachweis erbringen, dass sie die von der DKG vorgegebenen branchenspezifischen Anforderungen (B3S) erfüllen. Verantwortlich für den Informationssicherheitsprozess ist der Informationssicherheitsbeauftragte (CISO).

Anforderungen an das Identitäts- und Rechtemanagement laut B3S

Zu den erforderlichen Maßnahmen zählt unter anderem auch die Umsetzung des Identity- und Access Managements. Das klar definierte Ziel: Gesundheitsdaten vor Zugriffen unbefugter Personen zu schützen. Das bedeutet, dass nur jene IT-User den Zugriff zu sensiblen Daten erhalten dürfen, die diesen auch tatsächlich für die Ausübung ihrer Arbeit benötigen.

Anforderungen an das Identitäts- und Rechtemanagement laut B3S

Zu den erforderlichen Maßnahmen zählt unter anderem auch die Umsetzung des Identity- und Access Managements. Das klar definierte Ziel: Gesundheitsdaten vor Zugriffen unbefugter Personen zu schützen. Das bedeutet, dass nur jene IT-User den Zugriff zu sensiblen Daten erhalten dürfen, die diesen auch tatsächlich für die Ausübung ihrer Arbeit benötigen.

Sicherheit für Krankenhausinformationssysteme

Das Krankenhausinformationssystem (KIS) ist das zentrale Steuerungs- und Dokumentationssystem für die stationäre und medizinische Versorgung. Störungen an zentralen KIS-Infrastrukturkomponenten oder an angebundene IT-, Medizintechnik- oder Abteilungssubsystemen können schnell dazu führen, dass der medizinische Behandlungsprozess gestört wird. Dementsprechend kommt der Absicherung des KIS im Krankenhaus eine besonders wichtige Bedeutung zu. Die darin gespeicherten Daten müssen gemäß dem Sicherheitsstandard einerseits jederzeit verfügbar sein und andererseits vor unbefugten Zugriffen geschützt werden. Um das Risiko von Datenmissbrauch auf ein Mindestmaß reduzieren zu können, braucht es ein geregeltes Berechtigungsmanagement.

In Verbindung mit den Maßnahmenempfehlungen des B3S für die Gesundheitsversorgung im Krankenhaus bedeutet dies für die Absicherung des KIS unter anderem:

- Die Prozesse zur Benutzeranlage, Änderung und Deaktivierung müssen festgelegt, dokumentiert und eingehalten werden. Umfangreiche Automatisierung minimiert dabei die Fehlerquote zum Teil massiv. Für die Automatisierung sind technische Schnittstellen in die betroffenen Systeme notwendig.

- Benutzerdaten sollten stets aus einer zentralen Identity-Quelle kommen, aus welcher auch andere IT-Systeme, wie zum Beispiel Active Directory, gespeist werden können.

- Anträge und die Vergabe von Zugriffsrechten müssen klar geregelt sein. Empfehlenswert ist es, die Verantwortlichen aus den Fachbereichen in die Prozesse aktiv miteinzubeziehen. Auch wenn die administrative Durchführung durch die IT angestoßen wird, so sollten die tatsächlichen Verantwortlichen (sogenannte „Data Owner“) die Anträge zuvor prüfen und mit einer entsprechenden Begründung entweder freigeben oder ablehnen müssen.

- Die Zuordnung von Zugriffsrechten muss nachvollziehbar dokumentiert sein. Dazu zählen zumindest: Antragsteller, Datum und Uhrzeit der Beantragung, beantragte Berechtigungen, Freigabeprozess und Durchführungsnachweis. Dabei ist zu beachten, dass die Dokumentation nur nachvollziehbar ist, wenn sie lückenlos extrahiert werden kann. E-Mails in einem Sammelpostfach oder Tickets in einem Helpdesk-System erfüllen diese Anforderung nicht vollumfänglich, da die notwendigen Datenstrukturen für ein brauchbares Reporting fehlen.

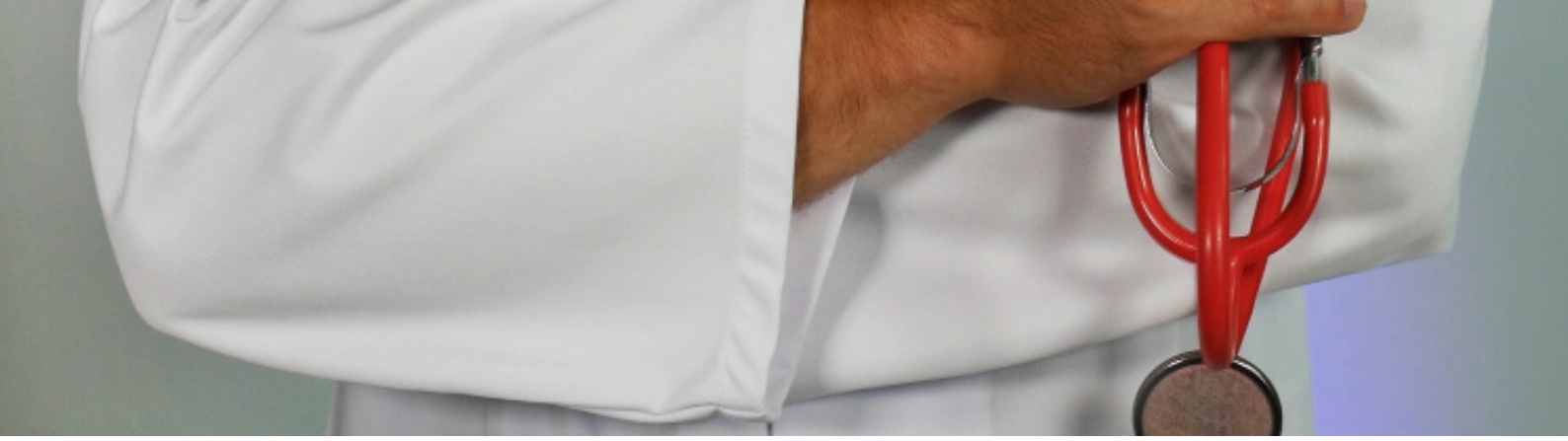
- Die Zugriffsrechte müssen einem regelmäßigen Rezertifizierungsprozess unterzogen werden. Dabei sollten von den jeweiligen Verantwortlichen die Zuordnungen der Berechtigungen regelmäßig auf den aktuellen Bedarf hin überprüft und korrigiert werden. Diesen Prozess manuell umzusetzen, ist von der Erhebung der aktuellen Zugriffsrechte über die Vorlage bei den Verantwortlichen bis zur Durchführung der gewünschten Änderungen durch die IT-Abteilung, sehr aufwändig und fehleranfällig. So weichen zum Beispiel die tatsächlichen Zugriffsrechte binnen kurzer Zeit häufig von dem zur Überprüfung vorgelegten Stand ab.

- Verlässt ein Mitarbeiter die Einrichtung, so muss sein Konto im KIS-System deaktiviert werden. Zur zuverlässigen Umsetzung dieser Anforderung gehört die Anbindung an die Software des Personalwesens. Damit können Eintritte, Abteilungs- oder Standortwechsel, sowie das Ausscheiden von Mitarbeitern automatisch abgebildet werden.

Über die Maßnahmenempfehlungen hinaus ist es empfehlenswert, die Zugriffsberechtigungen im KIS über ein globales Rollenmanagement abzubilden. Damit kann nicht nur das Ausscheiden von Mitarbeitern aus der Einrichtung abgebildet werden, sondern auch der – wesentliche komplexere – Fall eines Abteilungs- oder Positionswechsels. Das Rollenmanagement sorgt dann automatisch dafür, dass nicht mehr benötigte Berechtigungen entzogen, und für die neue Position zusätzlich erforderliche Zugriffsrechte zugeordnet werden.

Fazit

Die Digitalisierung im Gesundheitsbereich bietet enorme Chancen und schreitet mit hohem Tempo voran. Doch wo sich Gelegenheiten bieten, lauern auch immer Gefahren. Um auf diese möglichst gut vorbereitet zu sein, beinhaltet der B3S für die Gesundheitsversorgung im Krankenhaus Maßnahmenempfehlungen zur Umsetzung der IT-Sicherheit. Mit dem Abschnitt „Identitäts- und Rechtemanagement“ werden Vorgaben für die Behandlung von Benutzerkonten und Zugriffsrechten gesetzt. Da zahlreiche Maßnahmen und Werkzeuge in der IT-Sicherheit auf der Identität des Benutzers aufbauen, gilt es diese Daten besonders zu schützen, um die IT-Sicherheit als Ganzes nicht zu gefährden.



Über tenfold

tenfold ist ein Berechtigungsmanagement-System zur zentralen und einfachen Verwaltung von IT-Benutzern und deren Zugriffsrechten auf verschiedenen Systemen.

Es bestehen unter anderem technische Schnittstellen zu wichtigen Serversystemen wie Active Directory und Groupware-Lösungen. Ebenso kann tenfold an Anwendungen von Drittanbietern wie SAP angeschlossen werden. Das Portfolio wird ergänzt durch die Integration von kritischen, branchenspezifischen Anwendungssystemen wie dem Krankenhausinformationssystem ORBIS.

tenfold bietet Schutz vor Datendiebstahl und befreit IT-Personal von zeitintensiven, manuellen Aufgaben in der Berechtigungsverwaltung. Gleichzeitig wird die Einhaltung von Compliance-Bestimmungen sichergestellt und die Einrichtung vor den negativen Folgen einer Regelverletzung geschützt.

Über ORBIS

ORBIS ist die einzigartige Lösung für Arbeitsabläufe in der Medizin, der Administration und im Management von Einrichtungen im Gesundheitswesen. Als ganzheitliches Krankenhaus-Informationssystem sorgt ORBIS für eine 360 Grad Sicht auf die Patientenbehandlung. ORBIS ermöglicht es, die Abläufe in Ihrer Klinik effizient und umfassend zu gestalten. Dadurch werden Aufwendungen für administrative Aufgaben, Dokumentation und Koordination reduziert. Dies führt zu erheblichen Kosteneinsparungen und hilft, Erlöse zu steigern. Durch seine Flexibilität besitzt ORBIS ein einzigartiges Leistungsspektrum und passt sich perfekt an die Abläufe jeder Einrichtung an.

info@tenfold-security.com
www.tenfold-security.com