Die vertrauensvolle und sichere Versorgung von Patienten ist eine wichtige Pflicht

Kritische Infrastrukturen: Kennen Sie Ihre hauseigenen Schwachstellen?

Die Informations- und Kommunikationstechnologie ist DIE Schlüsseltechnologie des 21. Jahrhunderts. Sie gewinnt auch im Gesundheitswesen an Bedeutung. Zum Beispiel erleichtern Mitarbeiter-Apps die interne Kommunikation. Allerdings bedarf es gerade hier besonders sicherer Tools. Denn IT-Landschaften im Gesundheitswesen werden von höchster Stelle als so genannte «Kritische Infrastrukturen (KRITIS)» eingeordnet. Was dahinter steckt und was zu beachten ist.

Im Gesundheitswesen geniesst die sichere Versorgung von Patienten höchste Priorität. Hapert es in der IT-Landschaft von Gesundheitszentren und Spitälern jedoch an einer ausreichenden Datensicherheit, kann dies gravierende Auswirkungen für alle Beteiligten haben. Zum Beispiel können Patientendaten leicht ausgespäht werden. Das geschieht oft mit dem Ziel, die Informationen für teures Geld weiter zu verkaufen. Interessant sind die Daten nicht nur für Pharmafirmen oder Versicherungen. Auch mancher Arbeitgeber langt zu, um den Gesundheitszustand seiner Arbeitnehmenden auszuspionieren.

Wichtig: höchste Datenschutzstandards im Gesundheitswesen

Im Gesundheitswesen sind daher höchste Datenschutzstandards unerlässlich, um den Missbrauch sensibler Patienteninformationen zu verhindern. Für jedes Spital, jede Pflegeeinrichtung und jede Arztpraxis. Das sieht auch der deutsche Gesetzgeber so. Das Bundesamt für Sicherheit und Informationstechnik (BSI) stuft die elektronische Kommunikationslandschaft im Healthcare-Sektor nämlich als so genannte Kritische Infrastruktur (KRITIS) ein. Darunter fallen IT-Infrastrukturen, die eine zentrale Bedeutung für das Gemeinwesen haben.

Der Schweizer Bundesrat sieht's genauso und hat wie Landesnachbar Deutschland per Gesetz eine nationale Strategie zum Schutz kritischer Infrastrukturen verabschiedet. Ebenfalls mit dem Ziel, diese bestmöglich zu schützen. In Deutschland legt das Gesetz den Betreibern besondere Auflagen auf. Unter anderem müssen sie einen IT-Sicherheitsbeauftragten benennen und einen zertifizierten Mindestschutz an IT-Sicherheit nachweisen.

Schlupflöcher im hauseigenen Datenschutz

Was viele Arbeitgeber in diesem Zusammenhang allerdings oftmals nicht im Blick haben: Viele der Informationen, die im Gesundheitswesen entstehen, werden nicht nur in der hauseigenen IT-Infrastruktur vorgehalten. Sie kursieren auch über andere Kanäle. Messengerdienste wie WhatsApp haben sich zum Beispiel als praktischer Kanal in der internen Kommunikation entpuppt.

Zum Beispiel, weil sich viele Kollegen ständig im Haus bewegen und nicht konstant über einen stationären PC zu erreichen sind. Auch deren Erreichbarkeit per Telefon ist begrenzt. Befinden sich Pfleger oder Ärzte gerade in einer Behandlung, gehen sie nicht ran. Später vergessen sie unter Umständen zurückzurufen. So kann es dauern, bis man sich über einen kritischen Befund ausgetauscht hat. Per Instant Messenger lässt sich die Kommunikation komfortabler steuern. Die Kollegen antworten dann, wenn sie Zeit haben und nichts gerät in Vergessenheit.

Gefährlich: Ärzte, Pfleger und Fachangestellte teilen Informationen mit WhatsApp

98 Prozent der Klinikärzte gebrauchen aus diesen Gründen WhatsApp und Co. täglich im Job. Sie schicken Bilder von Befunden hin und her, tauschen sich über den Krankheitsverlauf von Patienten aus und stellen im Chat gemeinsame Diagnosen. Das ergab eine Studie des Deutschen Datenschutz-Instituts (DDI).

Was aus Sicht der Mediziner die Arbeit erleichtert, ist in punkto Datenschutz höchst riskant. Dann jedenfalls, wenn die Kommunikation über frei verfügbare Instant Messenger wie Whats-

App gesteuert wird, denn diese entsprechen in keiner Weise den strengen Anforderungen, die die Gesetzgeber an eine Kritische Infrastruktur stellen.

Begutachtung der hauseigenen IT-Infrastruktur

Kritisch wird es beispielsweise, weil die Voreinstellung von WhatsApp vorsieht, dass übermittelte Fotos automatisch auf der Festplatte des Empfängertelefons gespeichert werden. Von dort gelangen sie leicht in die Cloud. Handelt es sich um ein privates Gerät, das für die interne Kommunikation benutzt wird, bekommen unter Umständen unberechtigte Dritte automatisch Zugriff auf die Daten.

Nicht immer werden Mitarbeitende ausserdem aus Chatgruppen entfernt, wenn sie sich einer neuen beruflichen Herausforderung zuwenden. Auf diese Weise sehen sie sensible Patienten-Daten ein, für die sie keine Autorisierung mehr haben.

Beides sind grob fahrlässige Verstösse gegen den Datenschutz. Daher sollten Arbeitgeber im Gesundheitswesen bei der Begutachtung ihrer IT-Infrastruktur nicht nur den hauseigenen Server und die direkt angeschlossenen Systeme unter die Lupe nehmen. Sie sollten auch hinterfragen, wie ihre Angestellten kommunizieren.

Kommunikation über den Messenger: Ist ein Verbot angeraten?

Das heisst aber nicht, dass Verantwortliche in Spitälern und andern Gesundheitsinstitutionen ihren Mitarbeitenden die Kommunikation über den Messenger verbieten müssen. Dazu bietet die orts- und zeitunabhängige Kommunikation einfach zu viele Vorteile:

- Die Zusammenarbeit und das Zusammengehörigkeitsgefühl verbessern sich, weil man immer einen direkten Draht zu den Kollegen hat.
- Die Qualität der Patientenbetreuung steigt nachweislich aufgrund des zuverlässigeren Austauschs.

Die Lösung besteht im Implementieren einer professionellen Mitarbeiter-App zur internen Kommunikation. Mit ihr lassen sich zum Beispiel Röntgenbilder oder Patientendossiers völlig unbedenklich austauschen.

Die Vorteile einer professionellen Mitarbeiter-App

Claudio Badertscher, Business Development Manager Healthcare DACH der Connect Solutions AG, meint dazu: «Wer innerhalb kritischer Infrastrukturen (KRITIS) Daten und Informationen austauscht, darf das auf keinen Fall über frei zugängliche Messengersysteme tun. Wer vom Gesetzgeber so eingestuft wird, für den gelten besonders strenge Datenschutz-Regeln, die die Apps nicht erfüllen. Die Alternative zu WhatsApp und Co sind sichere und zertifizierte Mitarbeiter-Apps, mit denen sich die interne Kommunikation komfortabel und vor allem sicher steuern lässt.»

Aus den folgenden Gründen sollten sich Mitarbeitende innerhalb kritischer Infrastrukturen nur über Mitarbeiter-Apps austauschen:

- Die Daten werden nicht wie bei WhatsApp auf amerikanischen Servern gespeichert.
- Stattdessen werden sie lokal oder on-premise nach dem weltweit erprobten ISO-Standard 27001 gehostet.
- Dieses Zertifikat steht für maximale Sicherheit von Informationen, Daten und Systemen und ist konform mit den deutschen und schweizerischen IT-Sicherheitsgesetzen.
- Eigentümer der übertragenen Daten bleibt immer das Unternehmen, das die Mitarbeiter-App einsetzt. Unberechtigtes Teilen, Ablegen oder Duplizieren der Daten wird so verhindert.
- Die Zugriffsberechtigungen zu der Unternehmens-App werden an zentraler Stelle verwaltet und stets aktualisiert.
- Scheidet ein Mitarbeiter aus, erlischt sein Account automatisch.

Fazit: Mit einer Mitarbeiter-App schlagen Arbeitgeber im Gesundheitswesen zwar nicht wie im Märchen sieben Fliegen mit einer Klappe, aber doch immerhin drei!

1. Sie kommen den Kommunikationsvorlieben ihrer Mitarbeitenden nach und stärken deren Bindung.
2. Sie gewährleisten den Schutz der Privatsphäre ihrer Patienten.
3. Sie können sich auf einen Partner verlassen, der Sicherheit auf höchstem Niveau garantiert. Denn die App wird regelmässig von externen Experten überprüft.

So wischen Arbeitnehmende alle Sorgen in Sachen Datenschutz mit einem Streich vom Tisch. Wenn das nicht märchenhaft ist…

Autorin

Sonja Dietz

Weitere Informationen

Connect Solutions AG
Telefon +41 44 500 22 15
www.qnnect.com