IT-Sicherheit im Krankenhaus

E-Mails sicher und geschützt versenden

Von René Schubert

Die Digitalisierung im deutschen Gesundheitswesen hat in den vergangenen Jahren immer stärker an Bedeutung gewonnen. Damit einher geht ein zunehmender elektronischer Versand von sensiblen medizinischen sowie nicht-medizinischen Daten im Krankenhaus. Um das Krankenhaus als Organisation vor Datenmanipulation und Cyberangriffen zu schützen, muss die E-Mail-Kommunikation im Sinne des Risikomanagements und der Sorgfaltspflicht ganzheitlich und sicher umgesetzt werden.

Keywords: *Datenschutz, IT, Strategie*

Täglich versendet und empfängt ein Krankenhaus eine Vielzahl von personenbezogenen, medizinischen, statistischen oder allgemein betriebsinternen Daten. Für diese Datenarten gibt es unterschiedliche Wege der Absicherung. Für den Versand von medizinischen Daten wie beispielsweise Diagnosen, Untersuchungsergebnissen, Therapieempfehlungen oder elektronischen Arztbriefen wird derzeit in Krankenhäusern über die Anbindung an die Telematikinfrastruktur der Standard KIM, Kommunikation im Medizinwesen, etabliert. Über KIM können Krankenhäuser medizinische Daten sicher und authentifiziert mit registrierten Nutzern der Telematikinfrastruktur austauschen. Mit dem § 301 SGB V ist für die Übermittlung von Abrechnungsdaten der Krankenhausbehandlung von Krankenhäusern an Krankenkassen seit 1996 ein gesetzlicher Rahmen definiert. Über diesen elektronischen Weg werden Daten verschlüsselt übertragen. Das Krankenhaus erhält die Sicherheit, dass die Daten nur der vorgesehene Empfänger entschlüsseln kann. Der Empfänger wiederum erhält die Sicherheit, dass Daten tatsächlich vom angegebenen Absender stammen.

Darüber hinaus versendet ein Krankenhaus eine Reihe von nicht-medizinischen Daten, die dennoch dem Datenschutz unterliegen. Das können personenbezogene Mitarbeiterdaten, interne Informationen wie Rechnungen, Dienst- und Finanzpläne, E-Mails vom Chefarztsekretariat oder die Kommunikation mit Verbänden und Behörden sein. Wie ein Krankenhaus diese sensiblen Daten versendet, ist nicht über ein standardisiertes Verfahren oder per Gesetz geregelt. Krankenhäuser stehen selbst in der Verantwortung, entsprechende Vorkehrungen für den sicheren Datenversand zu treffen.

Warum unverschlüsselte E-Mails ein Sicherheitsrisiko darstellen

Bisher wird der sichere Versand von nicht-medizinischen Daten im Krankenhaus recht stiefmütterlich behandelt. Und das, obwohl im Krankenhaus die E-Mail, wie auch in anderen Unternehmen, eines der zentralen digitalen Kommunikationsmittel ist.

Die E-Mail genießt hohes Ansehen und Vertrauen. Sie ist schnell versendet und die Information landet innerhalb weniger Sekunden im Postfach des Empfängers. Dabei legt eine E-Mail im Internet mehrere Stationen zurück und passiert verschiedene Server und Netzwerke weltweit. Wird eine E-Mail unverschlüsselt versendet, so wie es bisher bei einer Vielzahl von Einrichtungen im Gesundheitswesen der Fall ist, können sich potenzielle Angreifer leicht Zugang zu den Inhalten verschaffen. Beim unverschlüsselten Versand werden betriebsinterne Daten ganz ungeschützt, für jeden einsehbar, wie beim Versand einer Postkarte, im Klartext über das Internet übertragen. ▶

Weitere Informationen

Unter *www.mein-sicheres-krankenhaus.de* können sich Interessierte umfassend zur E-Mail-Verschlüsselung im Krankenhaus informieren. Die DKTIG, getragen von der Deutschen Krankenhausgesellschaft sowie den 16 Landeskrankenhausgesellschaften, sensibilisiert unter dem Schlagwort MEIN SICHERES KRANKENHAUS insbesondere zur Absicherung von Datenkommunikation im Krankenhaus. Neben dem Problembewusstsein soll die themenbezogene Webseite auch Lösungsvorschläge unterbreiten, die dann krankenhausindividuell an den jeweiligen Erfordernissen entwickelt werden.

Auf jedem Server, auf dem die E-Mails zwischengespeichert werden, kann die Nachricht mitgelesen werden. Ein leichtes Spiel für Angreifer, die Daten ausspähen, Identitäten stehlen oder Cyberangriffe vorbereiten wollen. Mit 80 Prozent sind E-Mails das gefährlichste Einfallstor neben gefälschten Websites, gekaperten Identitäten und Server-Angriffen.

„Man stelle sich vor, wenn Dritte Zugang zu vertraulichen Informationen wie Mitarbeiterdaten, Dienstplänen oder Verträgen mit Banken erhalten. Industriespionage und Big Data-Auswertungen sind dabei die relevanten Stichwörter."

Man stelle sich vor, wenn Dritte Zugang zu vertraulichen Informationen wie Mitarbeiterdaten, Dienstplänen oder Verträgen mit Banken erhalten. Industriespionage und Big Data-Auswertungen sind dabei die relevanten Stichwörter. Mit Big Data-Analysen können Cyberkriminelle Themen, die sie interessieren, filtern und entsprechende Nutzerprofile erstellen oder diese gesammelten Daten weiterverkaufen. Da Angriffe über diesen Weg des Datendiebstahls in der Regel nicht sichtbar oder nachweisbar sind, halten Krankenhäuser noch nicht im geforderten Umfang Maßnahmen zum Schutz der E-Mail-Sicherheit vor.

IT-Sicherheit für alle Krankenhäuser

Die Digitalisierung bietet viele Chancen, Patientenversorgung zu verbessern, birgt aber auch Gefahren, die mit der wachsenden Durchdringung der Abläufe und Prozesse mit Informationstechnik einhergehen. Ein Krankenhaus übernimmt mit der Erfüllung eines medizinischen Versorgungsauftrages eine besondere, verantwortungsvolle Rolle und muss daher den Anforderungen schützenswerter, kritischer Infrastrukturen umfänglich gerecht werden. Denn Datenschutz bedeutet auch Patientenschutz.

Der Gesetzgeber hat in den letzten Jahren viele Regelungen zur Erhöhung der IT-Sicherheit eingeführt. Dazu gehören beispielsweise die Datenschutz-Grundverordnung, das IT-Sicherheitsgesetz aus 2015 oder das Patientendaten-Schutz-Gesetz (PDSG) aus dem Jahr 2020. Mit dem PDSG wurde der § 75c in das Sozialgesetzbuch (SGB) V eingefügt. Demnach sind seit dem 1. Januar 2022 alle Krankenhäuser in Deutschland verpflichtet, Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme zu treffen.

„Die Erfüllung von Schutzzielen der Cyber- und Informationssicherheit im Krankenhaus kann nur gelingen, wenn alle Aspekte der spezifischen Sicherheitsgefährdungen berücksichtigt werden."

Für diejenigen Krankenhäuser, die mit mehr als 30.000 vollstationären Fällen jährlich zu den kritischen Infrastrukturen zählen, wurden zur Verbesserung der IT-Sicherheit branchenspezifische Maßnahmen definiert. Für die Branche „Medizinische Versorgung" hat die Deutsche Krankenhausgesellschaft (DKG) gemeinsam mit Fachexperten den „Branchenspezifischen Sicherheitsstandard" (B3S) für Krankenhäuser entwickelt, der konkrete Anforderungen für die im Krankenhaus eingesetzten Systeme, Prozesse und organisatorische Hinweise für die Umsetzung von IT-Sicherheit enthält.

Für Krankenhäuser, die nicht unter die gesetzlichen Regelungen des Bundesamtes für Sicherheit in der Informationstechnik fallen, jedoch Maßnahmen für IT-Sicherheit nach § 75c SGB V umsetzen müssen, hat die DKG Hinweise und Musterkonzepte im Rahmen eines Dokumentenpaketes erstellt, welches Krankenhäuser bei der konkreten Planung und Umsetzung dieser Maßnahmen unterstützt.

Ganzheitlicher Ansatz gefordert

Die Erfüllung von Schutzzielen der Cyber- und Informationssicherheit im Krankenhaus kann nur gelingen, wenn alle Aspekte der spezifischen Sicherheitsgefährdungen berücksichtigt werden. Bei diesen Vorkehrungen insbesondere in Bezug auf § 75c SGB V darf die sichere E-Mail-Kommunikation nicht außer Acht gelassen werden, denn ohne sie gibt es keinen zeitgemäßen Datenschutz im Krankenhaus.

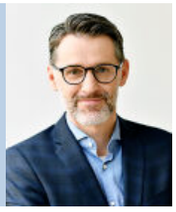
Das mögliche Abfangen und Manipulieren von Mails kann im Krankenhaus durch einfache Maßnahmen verhindert werden: Das Verschlüsseln mittels Zertifikat beispielsweise über das Verfahren S/MIME (Secure / Multipurpose Internet Mail Extensions).

Bei dem Verfahren werden Daten in einer E-Mail mit einem öffentlichen sowie einem privaten Schlüssel versehen. Der Absender kennt den öffentlichen Schlüssel zum Beispiel aus Schlüsselverzeichnissen. Ist der öffentliche Schlüssel von einem TrustCenter verifiziert, kann der Absender sicher sein, dass seine Nachricht nur von dem gewünschten Empfänger geöffnet werden kann. Der Empfänger der E-Mail wiederum verfügt allein über einen privaten Schlüssel, mit dem er sie entschlüsseln kann. Mit diesem Verfahren werden die Daten Ende-zu-Ende verschlüsselt. Das heißt, sie gelangen geschützt bis zum Empfänger innerhalb einer Organisation und enden nicht an der „Haustür“ wie bei anderen Verfahren, beispielsweise TLS, Transport Layer Security.

Weitere Vorteile bringt zudem die Nutzung eines E-Mail-Gateways, über das Krankenhäuser mehrere Zertifikate managen und automatisiert verwalten können. Dieses Gateway bündelt den gesamten Mail-Verkehr wie eine virtuelle Poststelle und verschlüsselt und signiert ausgehende Nachrichten. Eingehende Nachrichten werden ebenso entschlüsselt, die Signaturen überprüft und das Prüfungsergebnis an den Empfänger übermittelt. Die Bearbeitung erfolgt automatisiert nach einem flexibel anpassbaren Regelwerk, die zentral über eine webbasierte Administrationsoberfläche passend zu den jeweiligen Anforderungen angelegt werden können.

Die DKTIG spricht sich dafür aus, dass die E-Mail-Sicherheit in eine ganzheitliche Sicherheitsarchitektur im Krankenhaus einbezogen wird und zu einem standardisierten sowie selbstverständlichen Prozess wird. Dies ist notwendig, um das Krankenhaus als Organisation vor Datenmanipulation und Cyberangriffen zu schützen und muss so selbstverständlich werden wie die Händedesinfektion. ■

René Schubert
Geschäftsführer
DKTIG
Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH
Humboldtstr. 9
04105 Leipzig



René Schubert