# E-Mail-Verschlüsselung: so selbstverständlich wie die Händedesinfektion im Krankenhaus

Jeder Arzt desinfiziert sich täglich mehrmals die Hände. Ein standardisierter und selbstverständlicher Prozess im Krankenhaus, bei dem Jedem klar ist warum: Die Übertragung von Viren und Bakterien soll vermieden werden. So ähnlich verhält es sich mit der E-Mail-Verschlüsselung. Sie ist notwendig, um das Krankenhaus als Organisation vor Datenmanipulation und Cyberangriffen zu schützen, doch bisher wird die E-Mail-Verschlüsselung im Krankenhaus stiefmütterlich behandelt.

## Warum unverschlüsselte E-Mails ein Sicherheitsrisiko darstellen

Im Krankenhaus ist die E-Mail, wie in anderen Unternehmen auch, eines der zentralen digitalen Kommunikationsmittel. Die E-Mail genießt hohes Ansehen und Vertrauen. Sie ist schnell versendet und die Information landet innerhalb weniger Sekunden im E-Mail-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 der E-Mail verschaffen.

Das kann insbesondere für ein Krankenhaus ein erhebliches Sicherheitsrisiko darstellen. Auch wenn es für Krankenhäuser für den Austausch von Abrechnungsdaten ein gesetzlich vorgeschriebenes Verfahren gibt und der Versand medizinischer Patientendaten innerhalb der Telematikinfrastruktur mit KIM – Kommunikation im Medizinwesen – sicher und standardisiert erfolgt, dürfen nicht-medizinische Daten wie personenbezogene Mitarbeiterdaten, Finanzdaten oder die Verbandskommunikation nicht außer Acht gelassen werden. Für diese nicht-medizinischen Daten stehen Krankenhäuser selbst in der Verantwortung, entsprechende Sicherheitsvorkehrungen für den sicheren E-Mail-Versand zu treffen.

Man stelle sich vor, wenn Dritte Zugang zu nicht-medizinischen aber vertraulichen Informationen wie Mitarbeiterdaten, Dienstplänen oder Verträgen mit Banken erhalten. Industriespionage und Big Data-Auswertungen sind dabei die relevanten Stichwörter. Ein Krankenhaus übernimmt mit der Erfüllung eines medizinischen Versorgungsaustrages eine besondere, verantwortungsvolle Rolle und muss daher den Anforderungen schützenswerter, kritischer Infrastrukturen umfänglich gerecht werden. Das schreibt auch § 75c SGB V vor, der alle Krankenhäuser verpflichtet, Vorkehrungen zur Vermeidung von sicherheitsrelevanten Vorfällen zu treffen. 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, wird die E-Mail-Sicherheit auch in Krankenhäusern oftmals stiefmütterlich behandelt.

## Wie Krankenhäuser nicht-medizinische Daten sicher versenden können

Das mögliche Abfangen und Manipulieren von E-Mails kann im Krankenhaus durch einfache Maßnahmen verhindert werden: Das Verschlüsseln von E-Mails 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 der E-Mail kennt den öffentlichen Schlüssel zum Beispiel aus Schlüsselverzeichnissen. Ist der öffentliche Schlüssel von einem TrustCenter verifiziert, kann der Absender der E-Mail sicher sein, dass seine E-Mail nur von dem gewünschten Empfänger geöffnet werden kann. Der Empfänger der E-Mail wiederrum verfügt allein über einen privaten Schlüssel, mit dem er die ihm zugesendete E-Mail entschlüsseln kann.

Durch dieses Verfahren ergeben sich mehrere Vorteile für Krankenhäuser: Bei S/MIME 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. So wird verhindert, dass unbefugte Dritte Inhalte von E-Mails im Krankenhaus mitlesen können. Der Inhalt der E-Mail bleibt vollständig und unverändert - es ist nicht möglich, ihn zu manipulieren. Zudem können sich Krankenhäuser gegenüber dem Empfänger einer E-Mail zweifelsfrei als Absender der Nachricht ausweisen.

## Weitere Informationen

Damit in Krankenhäusern die E-Mail-Verschlüsselung so selbstverständlich wie das Händedesinfizieren wird, können sich Interessierte unter www.mein-sicheres-krankenhaus.de umfassend zur E-Mail-Verschlüsselung im Krankenhaus informieren. Die DKTIG 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 Erfordernissen des Krankenhauses entwickelt werden.

*René Schubert, Geschäftsführer DKTIG* ■