

Minimierung von Sicherheitsrisiken beim vernetzten Arbeiten im Gesundheitswesen

Minimierung von Sicherheitsrisiken beim vernetzten Arbeiten im Gesundheitswesen

Felix Gerdes, Cisco Systems GmbH

Schließen Sie bei Auslandsreisen Ihren Reisepass vom Verlassen des Hotels weg? Oder lassen Sie ihn auf dem Nachttisch liegen? Sicherlich führen Sie dieses nur mit erheblichem Aufwand zu ersetzende Dokument mit sich oder es wird – trotz des beschränkten möglichen Zutritts zum Hotelzimmer – zusätzlich unter Verschluss gebracht. So mache ich es jedenfalls – angepasst an den Risikograd. In manchen Situationen erscheint ein abgeschlossener Koffer als Aufbewahrungsort als ausreichend sicher. In einem Land hatte ich jedoch auch bei der Aufbewahrung im Hoteltresor kein sehr gutes Gefühl. Wir passen fast immer unsere eigenen Sicherheitsmaßnahmen intuitiv den gegebenen Situationen an.

Patientenakten, sofern sie noch in Papierform existieren, werden ebenso spätestens am Ende des Tages unter Verschluss gebracht. So hofft man zumindest. Tagsüber werden Akten, die gerade gebraucht werden, nicht völlig unbeaufsichtigt offen liegen gelassen. Ärzte, Schwestern und Arzthelfer verringern das Risiko der Einsicht durch Unbefugte oder den Diebstahl der Akte durch ihr Handeln. Sie passen ihr Handeln am Arbeitsplatz, sei es in der Praxis oder in der Klinik, der Risikoeinschätzung an. Die Anweisungen zum sicheren Umgang mit Patientendaten, die die Mitarbeiter erhalten, beruhen auf formal oder weniger formal und intuitiv durchgeführten Bedrohungsanalysen: „Liegt diese Akte hier sicher? Merken ich oder meine Mitarbeiter es, falls die Akte verschwindet? Ist der Zugang von Patienten in diesem Bereich eingeschränkt und kontrolliert?“

Nun werden bald, dank der elektronischen Gesundheitskarte, Patientendaten elektronisch kommuniziert. Die Einführung des elektronischen Rezepts bedeutet für eine Praxis oder Apotheke ein Wechsel von Papier auf elektronische Versandmedien. Der Zugang zum Gesundheitsnetzwerk erfordert daher eine neue Risikoeinschätzung. Das neue, vernetzte Arbeiten im Gesundheitswesen, von dem wir uns alle Qualitätssprünge und Kosteneinsparungen erhoffen, verlangt, dass jeder, der einen Heilberuf ausübt und jedes Krankenhaus, jede Krankenversicherung, jede Apotheke und jedes zuliefernde Rechenzentrum sich zu Beginn der Einführung der elektronischen Gesundheitskarte Gedanken über die Risiken dieser neuen Arbeitsweise macht.

Vernetztes Arbeiten ist nicht per se risikoreicher als das Arbeiten ohne Netzzugang. Es wird generell sogar davon ausgegangen, dass trotz des vernetzten Arbeitens, Patientendaten noch sicherer bearbeitet, versendet und gespeichert werden. Um diesen Sicherheitsgrad zu erreichen, bedarf es jedoch, dass Teilnehmer am Gesundheitsnetzwerk ihre Arbeitsweise – bestimmte Abläufe und organisatorische Aspekte des möglichen Handelns – den neuen Medien anpassen.

Neue Technologien haben schon immer eine Anpassung unseres Handelns erforderlich gemacht

Genau wie der Computer mehr ist als eine Schreibmaschine, so ist das Gesundheitsnetzwerk viel mehr als ein Ersatz für Faxverkehr oder den Transfer von Daten per Diskette. Es wäre also ein Trugschluss zu glauben, man müsste seine Abläufe in der Praxis, der Apotheke oder in der Klinik kaum anpassen. Die Adoption von neuen Technologien (beispielsweise das Automobil, EC-Karten oder das Mobiltelefon) erfordert immer ein gewisses Umdenken und das Anpassen des eigenen Handelns in Zusammenhang mit der Technologie. Bei dieser Adoption einer neuen Technologie passen wir uns unbewusst oder bewusst und systematisch den neuen Gegebenheiten an. Die hohe Bedeutung, die dem Schutz von vertraulichen Patientendaten beigemessen wird, spricht dafür, dass Teilnehmer am Gesundheitsnetzwerk sich ebenfalls bewusst und systematisch auf die neue Arbeitsweise vorbereiten. Die notwendigen Vorkehrungen müssen weder verhältnismäßig teuer noch mit persönlichen Nachteilen verbunden sein. Konsequenterweise durchgeführte bieten sie einen umfassenden Schutz vor Verlust von Patientendaten sowie unbefugtem Zugang zum Gesundheitsnetzwerk.

Die zu treffenden Sicherheitsmaßnahmen sollten aktuellen Risiken angemessen sein. Gleichzeitig sollten die Komplexität sowie der Aufwand dieser Maßnahmen handhabbar bleiben. Sowohl Großkliniken als auch kleinere Arztpraxen und Apotheken haben es mit Risiken durch Bedrohungen, Diebstahl, Verlust und Betriebsausfälle zu tun.

Vor einigen Jahren hatte ein Systemadministrator noch Wochen oder Tage Zeit, um Gegenmaßnahmen gegen Netzwerkbedrohungen einzuleiten. Das Zeitfenster für solche Maßnahmen hat sich heute auf Minuten oder Sekunden verringert. Der Internet-Wurm –Sapphire– hatte im Januar 2003 nur 11 Minuten gebraucht, um sich weltweit zu verbreiten und einen immensen Schaden anzurichten. Das Herunterladen von Virenschutz-Updates kann daher nicht mehr die einzige Schutzmaßnahme für Netzwerke und Endgeräte sein. ...

Dokumentinformationen zum Volltext-Download

Ä

Titel:

Minimierung von Sicherheitsrisiken beim vernetzten Arbeiten im Gesundheitswesen Artikel ist erschienen in:
Telemedizinführer Deutschland, Ausgabe 2006

Kontakt/Autor(en): Felix Gerdes, Cisco Systems GmbH Seitenzahl:

3,5

Sonstiges:

keine Abb.

Dateityp/ -größe:

PDF / 499 kB

Click&Buy-Preis in Euro: 0,00

Ä Rechtlicher Hinweis:

Ein Herunterladen des Dokuments ist ausschließlich zum persönlichen Gebrauch erlaubt. Jede Art der Weiterverbreitung oder Weiterverarbeitung ist untersagt.

Hier gehts zum freien PDF Download...