Minimierung von Sicherheitsrisiken beim vernetzten Arbeiten im Gesundheitswesen

Felix Gerdes, Cisco Systems GmbH

Schließen Sie bei Auslandsreisen Ihren Reisepass vorm 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 beschränkt 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 täglichen 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. Konsequent durchgeführt 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.

Autor: Felix Gerdes
Titel: Minimierung von Sicherheitsrisiken beim vernetzten Arbeiten im Gesundheitswesen
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2006
Seite: 320-323

Kap_3_7_TMF_06 320 13.10.2005, 11:35:43 Uhr

Netzwerkattacken können in Form von Viren, Würmern, trojanischen Pferden oder, seit Neuestem, raffinierten gemischten Bedrohungen durch die Kombination mehrerer Arten von Attacken entstehen.

Die neue, vernetzte Arbeitsweise erfordert also nicht nur den Schutz von Patientendaten, sondern auch das Vorbeugen gegen Risiken durch Störung oder gar den Stillstand des Praxis- oder Krankenhausbetriebs. Risiken, die eine Störung der Versorgungsabläufe bedeuten, können sowohl für Patienten aber auch für die direkt von einer Attacke betroffenen Arztpraxis, einem Krankenhaus oder einer Apotheke empfindliche Folgen wie Produktivitäts- und Umsatzausfälle haben. Die Versorgungsqualität wird in Zukunft in hohem Maße indirekt oder gar direkt von der Qualität der Sicherheitsmaßnahmen abhängen. Teilnehmer am Gesundheitsnetzwerk, bei denen sich wiederholt grobe Sicherheitslücken feststellen lassen, werden – zum Schutz der Allgemeinheit und Förderung der gewünschten Kollaboration über die sektoralen Grenzen des Gesundheitswesens hinweg – mit Sanktionen rechnen müssen. Diese Risiken gilt es also auf ein absolutes Minimum zu reduzieren. Zum Zeitpunkt der Verfassung dieses Artikels (Juni 2005) arbeiten viele Industrieteilnehmer eng zusammen mit der gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte gGmbH) daran, effektive und praktikable Sicherheitskonzepte zu entwickeln.

Um wirklich effektiv zu sein, müssen solche Sicherheitskonzepte auf einen ganzheitlichen Ansatz aufgebaut sein. Sicherheit kann nicht nachträglich als Zubehör montiert werden, da diese Vorgehensweise die Komplexität unverhältnismäßig erhöht, letztendlich teurer wird, viele Sicherheitslücken offen lässt und nicht zuverlässig ist.

Die für das Gesundheitsnetzwerk angestrebte integrierte Sicherheit muss Teil der „DNA“ des Netzwerks und der Arbeitsweise der Institutionen und Unternehmen werden. Wenn es jedem Autofahrer überlassen wäre, Airbags und ABS-Bremssysteme nach seiner Wahl auszusuchen und selber einbauen zu lassen, hätten wir heute längst nicht die Sicherheit auf unseren Straßen, die in den letzten Jahrzehnten durch zentrale Vorgaben und Maßnahmen der Industrie realisiert wurden. Bei einer integrierten Sicherheit können sich alle Teilnehmer wirklich darauf konzentrieren, die Vorteile des vernetzten Arbeitens im Gesundheitsnetzwerk auszuschöpfen, anstelle sich damit auseinanderzusetzen, welche Sicherheitsmaßnahmen eingeführt werden sollen und wie die einzelnen Komponenten zusammenpassen.

Sicherheitstechnologien im Netzwerk unterstützen sicherheitsbewusstes Handeln

Ein modernes Netzwerk ist in der Lage, sich selbst zu verteidigen (Self-Defending Network) und weist folgende Eigenschaften auf: Es...

- beruht auf einem integrierten Sicherheitskonzept,
- kann einem veränderten Sicherheitsbedarf angepasst werden,
- kann der Organisationskultur angepasst werden,
- sichert hohe Netzwerkverfügbarkeit zu,
- sieht schnelle, genaue und angemessene Reaktionen vor,
- ist wirtschaftlich in der Anschaffung und im Betrieb,
- belastet die Gemeinkosten nur in geringem Umfang und
- wird auf der vorhandenen Netzwerkinfrastruktur errichtet.

Zum integrierten Schutz gehören zunächst praktikable, physische Sicherheitsmaßnahmen, die konsequent im Unternehmen eingeführt werden müssen. In erster Linie geht es hier um organisatorische Maßnahmen die zu ergreifen sind und nachstehend (ohne einen Anspruch auf Vollständigkeit erheben zu wollen) beschrieben werden.

Eine Erweiterung oder Verschärfung der bereits praktizierten Zugangskontrollen gehört zu den ersten Maßnahmen für alle, die am Gesundheitsnetzwerk arbeiten wollen. Unbewachte Bildschirmarbeitsplätze, auf dem Monitor aufgeklebte Passwortzettel und „Gruppenpasswörter“ sind spätestens ab heute tabu.

Der Zugang zur IT-Infrastruktur eines Krankenhauses muss ebenso eingeschränkt werden wie der Zugang zu den Netzwerkperipheriegeräten (NTBA und Modem oder Router) in einer Apotheke oder Arztpraxis. NTBA, Modem und Router sollten mindestens in einem geeigneten Schrank abgeschlossen werden.

Dass der elektronische Heilberufsausweis nicht unbeaufsichtigt im Kartenlesegerät stecken darf, ist selbstverständlich. Nicht ganz selbstverständlich dagegen ist das regelmäßige Ändern von Passwörtern – eine sehr effektive Präventivmaßnahme. Mit der Verfügbarkeit von billigen drahtlosen Netzzugangsgeräten (WLAN (WiFi)-Zugangsgeräten) besteht die Möglichkeit für ihre Mitarbeiter, sich eigene, ungesicherte Netzzugänge einzurichten. Die Sicherheitsregularien müssen also effektive Kontrollen und Sanktionen gegen unautorisierte drahtlose Netzzugangspunkte vorsehen.

Das Netzwerk ist überall. Die organisatorischen Maßnahmen sind notwendig, um sicherzustellen, dass der Zugang zum Netzwerk nicht überall stattfinden kann.

Beim Aufbau der Verbindung mit dem Gesundheitsnetzwerk greifen technische Maßnahmen, die das Unternehmen oder der Systemlieferant gewählt haben, um einen schnellen und gleichzeitig sicheren Versand von Daten zu ermöglichen.

Das Sicherheitskonzept für das Gesundheitsnetzwerk wird vorsehen, dass ein Zugang nur über eine verschlüsselte VPN-Verbindung (Virtual Private Network) möglich sein wird. Einfach für den Anwender zu bedienen, sorgt spezielle Software auf dem Rechner und im Router (auch Konnektor genannt) dafür, dass die Verbindung zum Netz aufgebaut wird. Beim Aufbau der Verbindung führen zentrale Rechner eine Authentifizierung und Sicherheitsüberprüfung des Teilnehmers durch und entscheiden, ob eine Verbindung zum Netzwerk etabliert wird. Durch die Einführung solcher Netzzugangskontrollen, sog. Network Admission Control (NAC), wird zusätzlich das Risiko des Zugangs zum Netz durch unsichere und nicht autorisierte Geräte eliminiert. Heute gehört NAC, eine Initiative von Cisco Systems und weiteren Herstellern, zu einem wichtigen Kernelement des vernetzten Arbeitens. Inzwischen beteiligen sich mehr als 60 Hersteller an diesem Programm.

(Referenz: http://www.cisco.com/en/US/partners/pr46/nac/partners.html)

Kap_3_7_TMF_06 321 13.10.2005, 11:35:46 Uhr

Moderne Einwahlknotenpunkte (VPN-Konzentratoren) wählen nach dem Aufbau der Verbindung die effizienteste Route zum benötigten System. Eine im Router integrierte Firewall sorgt dafür, dass nur die Datenpakete, die vom entsprechenden Rechner angefordert und erwartet werden, auch durchgelassen werden – dies ohne, dass der Anwender es mitbekommt oder gar selbst eingreifen müsste. Modernste Router im Kern des Gesundheitsnetzwerks oder im Kern der Netzwerke von größeren Teilnehmern wie Krankenhäuser oder Krankenversicherungen werden in der Lage sein, nicht nur den Datenverkehr so zu lenken, dass Wartezeiten minimiert werden, sie werden ebenfalls Datenpakete (Packets = die vielen Bruchstücke einer Datei während des Versands im Netzwerk) inspizieren und prüfen, dass sie frei von Viren, Würmern und trojanischen Pferden sind. Weiterhin wird sogar auf Anwendungsebene geprüft, ob „Packets" von der Software autorisierter Teilnehmer angefordert wurden und für autorisierte Teilnehmer bestimmt sind. Vertrauliche Informationen könnten also im Gesundheitsnetzwerk auf drei Ebenen geprüft und nur an vertraute Personen, Rechner und Softwareapplikationen geschickt werden. Integrierte Abwehrtechniken könnten dafür sorgen, dass die Verbreitung von Viren, Würmern und trojanischen Pferden verhindert wird.

Für größere Netzbetreiber bieten moderne, vollintegrierte Netzwerksicherheits-Management und -Antwortsysteme skalierbare Lösungen zur webbasierten Implementation von Sicherheitsstandards auf wirtschaftliche Art und Weise. Durch die Zusammenarbeit von Routern, Switches, Firewall-Geräten und so genannten Sicherheitsagenten auf den Rechnern sämtlicher angeschlossener Arbeitsplätze können Sicherheit bedrohende Ereignisse auf Ebene von Nachrichten, Geschehnissen und Arbeitssitzungen (Sessions) in der Netzwerktopologie aufgespürt und in koordinierter Art und Weise bekämpft werden.

Neben dem Transport von Patientendaten über verschlüsselte Leitungen werden die zu versendenden Daten selber als zusätzliche Schutzmaßnahme von der Softwareanwendung verschlüsselt.

Für Großkliniken gilt genauso wie für kleinere Apotheken und Arztpraxen die Maßgabe, die Komplexität ihrer Systeme (und Sicherheitsvorkehrungen) zu reduzieren und dadurch die Kosten auf ein Minimum zu senken. Entscheidend bei der Wahl von Netzwerkkomponenten sind die unkomplizierte Wartbarkeit und die schnelle Behebung von Fehlern. Groß- wie Kleinunternehmen sind daher gut beraten, sich für einen einzigen Ansprechpartner für den Aufbau und das Management ihrer Netzwerksysteme zu entscheiden. Eine Recherche der Firma Sage hat im Jahr 2003 ergeben, dass alleine die Wahl eines einzigen Lieferanten zu Kostenersparnissen in Höhe von rund 29 Prozent führt. Die US-Börse NASDAQ konnte bei der Implementierung von Netzwerksicherheitsmaßnahmen sogar zwischen 30 und 40 Prozent sparen, weil sie sich für die voll integrierte Lösung eines einzigen Lieferanten entschieden hatte.

Die Sicherheitstechnologie hat sich in den letzten Jahren in drei Stufen weiterentwickelt. Die ersten Einzelprodukte im Bereich der Netzwerksicherheit haben zu einem hohen Integrationsbedarf geführt. In dieser ersten Phase lag die Herausforderung bei der Integration von Einzelprodukten. In der zweiten Stufe wurde die Fähigkeit der Zusammenarbeit zwischen Produkten verschiedener Hersteller wie z. B. IBM, Trend Micro, McAfee und Symantec unterstützt. Heute befinden wir uns in der dritten Phase, in der es notwendig ist, nicht nur reaktiv, sondern proaktiv mit adaptierfähigen Mitteln den Sicherheitsschutz zu gewährleisten. Daher spricht man heute von adaptierfähigem Bedrohungsschutz.

Die Elemente des adaptierfähigen Bedrohungsschutzes sind:

- Die Firewall, die für grundlegende Zugangskontrolle und Packet-Inspektion sorgt
- Dedizierte Störungsschutzsysteme (wie das IPS von Cisco) und Network-Antivirus-Dienstleistungen können noch genauer in Datenpaketen nach Bedrohungen und Viren schauen
- Netzwerkintelligenz – das Zusammenspielen von sämtlichen sicherheitsrelevanten Komponenten mit der Aufteilung von LANs in separate VLANS, Quality of Service (QoS), um die Anwendung von Netzwerkbandbreiten zu kontrollieren und zu überwachen, das Routing in Abhängigkeit von der Netzwerktopologie sowie Information über Netzverkehrsströmen und -lasten

Die Kombination der genannten Elemente ermöglicht eine neue Klasse von Netzdienstleistungen, die ins gesamte Netzwerk eingewoben werden können:

Diese Dienstleistungen umfassen:

- Anwendungsschutz (Application Security), eingehende Inspektion über die Firewall und im Bedrohungsschutzsystem (Intrusion Protection System), um Sicherheitsregeln durchzusetzen, z. B. Verbot von Instant Messenger
- Anti-X-Verteidigung, um einen breit angelegten Schutzwall vor Bedrohungen am Rande des Netzwerks zu gewährleisten. Hier geht es u. a. um Anti-Wurm- und, Anti-Virus-Maßnahmen sowie E-Mail-Sicherheit (Anti-Spam, Anti-Phishing). Diese Technologien werden in den äußersten Randbereichen des Netzwerks eingesetzt, um die Auswirkungen von Attacken gegen den Kern oder die Verteilerknoten des Netzwerks zu minimieren und eine Ausbreitung der Störung zu erreichen
- Netzwerkabwehr und -kontrollmaßnahmen: Netzwerkintelligenz und die Virtualisierung von Sicherheitstechnologien erlauben die schichtweise Anordnung von Prüf-, Kontroll-, und Wechselbeziehungsfähigkeiten, um jedes Element eines Netzwerkes zu schützen. Durch die Aggregation von Informationen über Bedrohungen sowie die Analyse von Wechselbeziehungen sind proaktive Schutzmaßnahmen möglich

Ein Netzwerk, das in der Lage ist, sich gegen Störungen selber zu verteidigen (Self-Defending Network), entsteht durch den integrierten Einsatz sämtlicher o. g. Technologiekomponenten. Es ist davon auszugehen, dass die Betreiber des zukünftigen Gesundheitsnetzwerks diese hier beschriebenen integrierten Schichten von proaktiven Schutzmaßnahmen einführen werden, letztendlich um die Vertraulichkeit von Versicherten- und Patientendaten zu gewähren.

Kap_3_7_TMF_06 322 13.10.2005, 11:35:47 Uhr

Moderne Netzwerksicherheitslösungen bieten damit einen voll integrierten Schutz vom Kern des Netzwerks bis hinein in die Peripherie eines jeden Teilnehmers. Dabei sollten die Teilnehmer, besonders Netzbetreiber wie Krankenhäuser oder Krankenversicherer, auch auf den Schutz ihrer Investition achten. Sicherheitstechnologie, die eventuell günstiger in der Anschaffung, aber nach zwei Jahren obsolet ist und durch teuere Neubeschaffungen ersetzt werden muss, wird sicherlich nicht zu einer Reduktion der Kosten im Gesundheitswesen führen.

Fazit

Das vernetzte Arbeiten im Gesundheitswesen, ermöglicht und intensiviert durch die Einführung der elektronischen Gesundheitskarte, bringt für Versicherte und Patienten, aber auch für Ärzte, Zahnärzte, Apotheker und Krankenhausbetreiber viele Chancen, positive Veränderungen in der Versorgungsqualität und in der Kostenstruktur herbeizuführen. Das vernetze Arbeiten vieler Teilnehmer im Gesundheitswesen mittels neuer Kommunikationsverfahren erfordert ein Umdenken und eine Anpassung der eigenen Organisation und ihrer Prozesse. Der Schutz von Patientendaten kann ohne teuere und nachteilige Maßnahmen realisiert werden. Die Einführung von Sicherheitsmaßnahmen ist sogar eine lohnende Investition, bedenkt man die fatalen Folgen einer Betriebsunterbrechung. Die Realisierung organisatorischer und prozessualer Veränderungen, zusammen mit den technischen und eher unsichtbaren Sicherheitsmaßnahmen wie VPN, Firewall, Virusscanning, usw., führen zu einer integrierten Sicherheit. Integrierte Sicherheitsmaßnahmen bieten einen effektiven Schutz vor Bedrohungen auf mehreren Ebenen, sind einfach zu verwalten und, besonders wenn sie von einem einzigen Hersteller geliefert werden, viel wirtschaftlicher zu betreiben.

Kontakt
Felix Gerdes
Business Development Manager
Healthcare – Gesundheitskarte
Cisco Systems GmbH
Neuer Wall 77
20354 Hamburg
Tel. 0 40/37 67-44 04
Fax 0 40/37 67-44 44
fgerdes@cisco.com.

Kap_3_7_TMF_06 323 13.10.2005, 11:35:48 Uhr