Cyberkriminalität macht auch vor Gesundheitseinrichtungen nicht Halt

Patientendaten sind lukrative «Geiseln»

Schneller Austausch von Patientendaten birgt grosse Vorteile – und Gefahren: Elektronische Patientendossiers erleichtern die Kommunikation zwischen Institutionen, sind aber anfällig für Internetangriffe. Experten erklären, welche Gefahren lauern und wie man damit umgeht.

Von Claudia Weiss

Lahmgelegte Operationscomputer, Infusionssysteme, die verrückt spielen, oder elektronische Patientendossiers, die als «Geiseln» genommen werden, um Lösegeld zu erpressen: Was wie Science-Fiction anmutet, passiert bereits in der Realität. Solche Szenarien werden sich für Sicherheitsexperten in den nächsten Jahren noch als harte Knacknüsse erweisen: Die Strategie des Bundesrats, sämtliche Patientendossiers elektronisch zu vernetzen und bei einem Notfall auch vom Ausland darauf zugreifen zu können, ist bestechend und soll möglichst rasch realisiert werden. Zuerst aber muss die Sicherheit für die hochsensiblen Patientendaten gewährleistet sein.

Zwar beruhigt eHealth Suisse, das «Koordinationsorgan Bund Kantone», und ordnet die Gefahren als nicht sehr gross ein: «Schon heute sind viele Gesundheitsdaten elektronisch gespeichert», heisst es im Online-Dokument zum Thema Sicherheit. «Sie sind zwar sehr persönlich, aber lassen sich – anders als etwa Bankdaten – kaum in Geld umwandeln. Deshalb sind sie für Hacker weniger interessant.» Das klingt einleuchtend. Und beruhigend. Wären da nicht auch anderslautende Berichte. «Pandasecurity» beispielsweise, eine Firma, die Sicherheitssoftware herstellt, hat unlängst ein ganzes Dossier zum Thema «The Cyber Pandemic» veröffentlicht. Und dort zeigt sich eine andere Realität: Gemäss ihrem Bericht werden ausgerechnet Spitäler, Kliniken oder Labors «immer häufiger Opfer von Cyberattacken»: 2015 seien 253 Sicherheitslücken im Gesundheitssektor aufgetaucht, mehr als 500 Personen seien betroffen gewesen und 112 Millionen Daten gestohlen worden. «Medizinische Daten sind sehr kostbar und hochsensitiv, und wer immer diese Daten kontrolliert, kann daraus enormen Profit schlagen», heisst es im Dossier. Das widerspricht den Ansichten von eHealth Suisse. Was jetzt – sind Gesundheitsdaten gefährdet oder nicht?

In den letzten Jahren wurden Spitäler im Vergleich zu anderen Branchen intensiver angegriffen.

Bedrohung hat 2015 um fast zwei Drittel zugenommen

Die beunruhigende Antwort von Experten: Fakt ist, dass Spitäler in den letzten Jahren vergleichsweise intensiver angegriffen wurden als andere Branchen. Martin Leuthold, Leiter Geschäftsbereich Sicherheit der Stiftung Switch, sagt: «Der Gesundheitssektor zeigt das zweithöchste Wachstum an Vorfällen.» Das grösste Angriffsziel nach Regierungsorganisationen ist laut neusten Berichten das Gesundheitswesen, noch vor Banken und Industrie. Auch Peter E. Fischer, Leiter für Informationssicherheit und Datenschutz im Gesundheitswesen an der Hochschule Luzern und Präsident von Swiss Internet Security Alliance (SISA), sieht eine wachsende Gefahr: «Laut dem neusten ‹IBM Cyber Security Intelligence›-Index haben die Bedrohungen im Jahr 2015 gegenüber 2014 um fast zwei Drittel zugenommen.»

Er bestätigt zwar die Aussage von eHealth Suisse, dass ein Diebstahl von Gesundheitsdaten oder Manipulation von medizinischen Geräten keine sofortige Bereicherung ermögliche. Aber: «Die Daten und die Geräte sind so sensibel, dass der Schaden ungleich höher sein kann als durch das unberechtigte Abheben von Geldbeträgen von einem Konto.» Werde eine Krankengeschichte veröffentlicht, könne das zur Folge haben, dass jemand >>

keine Stelle mehr finde oder gesellschaftlich geächtet werde. Grosse Auswirkungen, die letztlich die Betroffenen doch dazu bringen könnten, tief in die Taschen zu greifen, um die Daten wieder herauszulösen und damit geheimzuhalten. Deshalb sind Erpressungen mit sogenannter «Ransomware» in letzter Zeit zur häufigsten und gefährlichsten Bedrohung geworden. Mit Hilfe solcher Schadprogramme gelingt es, in Computer einzudringen und den Zugriff auf Daten zu verhindern. «Das Schweizer Gesundheitswesen wäre schlecht beraten, die Bedrohungen zu verharmlosen», findet deshalb Martin Leuthold von Switch.

Die neuen Richtlinien von eHealth Suisse legen fest, wer wo für die Sicherheit der Daten sorgen muss.

eHealth Suisse erarbeitet neue Richtlinien

Tatsächlich ist sich eHealth Suisse der Risiken bewusst. «Die Bedrohungen und die Bedeutung der Datensicherheit haben in den letzten Jahren zweifellos zugenommen», räumt Adrian Schmid, Leiter der Geschäftsstelle, ein. Allerdings seien im Schweizer Gesundheitswesen bisher kaum konkrete Fälle von digitalem Datendiebstahl bekannt. Ausserdem seien es in den meisten publik gewordenen Beispielen zugriffsberechtigte Personen gewesen, die Informationen gestohlen hätten – zum Beispiel bei der Krankenakte des Formel-1-Fahrers Michael Schumacher. «Im Alltag sind missbräuchliche Zugriffe von Berechtigten ohnehin das grössere Problem als der technische Angriff von aussen», sagt Schmid. «Vor diesem Hintergrund ist auch unsere Aussage zu sehen, die allerdings nicht mehr ganz aktuell ist.» Die Aussage im Faktenblatt werde überarbeitet und demnächst im Zusammenhang mit den Vorgaben zum ePatientendossier neu formuliert. Denn: «Der Entwurf der Ausführungsbestimmungen des Bundes zum ePatientendossier macht sehr weitgehende Vorgaben zur Datensicherheit», betont Schmid. Darin wird detailliert aufgeführt, wer wo für Datenschutz und Datensicherheit zuständig ist. Zum Beispiel Punkt 4.15.1: «Gemeinschaften müssen den Datenschutz und die Datensicherheit über den

Die Eingabe von Patientendaten in Computersysteme erleichtert den Austausch unter verschiedenen Abteilungen oder sogar verschiedenen Institutionen. Aber was elektronisch vernetzt ist, muss besonders gut geschützt werden. Foto: Martin Glauser

gesamten Lebenszyklus der Systeme des elektronischen Patientendossiers sicherstellen. Dazu müssen formale Prozesse definiert, eingeführt und eingehalten werden für die Dokumentation, die Spezifikation, das Testen, die Qualitätskontrolle und die kontrollierte Umsetzung bei der Einführung oder der Entwicklung neuer Systeme; bei grösseren Änderungen oder Entwicklungen an bestehenden Systemen; bei dem Wechsel der Betriebsplattformen.»

Exakte Vorgaben, welche die IT-Verantwortlichen von Einrichtungen im Gesundheitsbereich noch vor grosse Herausforderungen stellen werden. Denn die Fälle, die Pandasecurity aus den USA zusammengetragen hat, klingen drastisch: «Universitätsspitäler und -kliniken von Utah – Daten von 2,2 Millionen Patienten gestohlen»; «Anthem Versicherungsgesellschaft – Zugang zu 80 Millionen Kundenakten»; «Hollywoods Presbyterianisches Medizinzentrum – 3,7 Millionen Dollar Lösegeld gefordert». Pandasecurity spricht vor allem von «ransom attacks», bei denen die Daten mit einer Software quasi gefangengenommen und gegen Lösegeld wieder freigegeben werden. Auch in Deutschland ist Cyber-Erpressung schon vorgekommen, beispielsweise beim Lukashospital in Neuss und beim Klinikum Arnsberg.

In den USA forderten Erpresser Millionen von Dollar für die gestohlenen Patientendaten.

Schweizer Spitäler sind nicht gefeit vor Attacken

In der Schweiz, so heisst es bei der Sicherheitsabteilung der Stiftung Switch, sind die Spitäler ebenfalls nicht gefeit: «Aus unserer Sicht müssen auch Organisationen aus dem Gesundheitswesen in der Schweiz damit rechnen, vermehrt angegriffen zu werden», warnt Sicherheitsexperte Leuthold. Und Peter Fischer von der Hochschule Luzern sagt: «Auch in Schweizer Spitälern sind Fälle von versuchtem Hacking bekannt geworden. Die Beispiele zeigen, dass Gesundheitseinrichtungen besonders gefährdet sind und daher noch viel besser geschützt werden müssen.» Laut Fischer drohen diverse Gefahren: Eine totale Blockade von Daten oder ein Weiterverkauf von Daten sind ebenso möglich wie die Lösegeldforderung für eine Datenfreigabe oder Attacken auf elektronisch gesteuerte Instrumente wie Insulinpumpen, Überwachungsmonitore oder Herzschrittmacher. «Das sind alles reale, potenzielle Gefahren», fasst er zusammen.

>>

Medizinaltechnologie ist schwierig zu sichern

Fischer erklärt auch, warum das Gesundheitssystem zunehmend verletzlich für Hackerangriffe wird: «Zwar haben bereits heute viele Ärzte und Spitäler zahlreiche Patientendaten elektronisch gespeichert.» Nur: «Diese Daten sind meist lokal gespeichert, also innerhalb eines Spitalnetzes.» Das elektronische Patientendossier hingegen, das auf einer Cloud gespeichert sei und bei entsprechender Zugangsberechtigung von überall her eingesehen werden könne, biete weit mehr Angriffsfläche. Erschwerend komme hinzu, dass im Gesundheitswesen die Informationstechnik keine Kernkompetenz sei, «und Informationssicherheit erst recht nicht».

Auch bei Switch können die Sicherheitsfachleute ziemlich genau orten, wo das Problem liegt: Medizinaltechnologie werde intern immer stärker vernetzt, sei aber aus Sicherheitssicht nicht für die im Internet herrschende Bedrohungslage gewappnet. «Dies primär, weil Medizinalsysteme auf eine viel längere Lebensdauer ausgelegt sind, ursprünglich nicht für eine vernetzte Welt mit entsprechendem Bedrohungsbild entwickelt wurden und sich nach wenigen Jahren nur noch schwer gegen die sich schnell weiterentwickelnde Bedrohungslage schützen lassen», erklärt Martin Leuthold. Dazu komme, dass die Spitäler sehr komplexe Informationssysteme betreiben und sehr hohe Datenmengen verarbeiten und speichern. All dies mache IT-Systeme von Spitälern verletzlich. Und wenn es nicht am System liege, bleibe immer noch der Weg über «die grösste Schwachstelle im System – den Menschen»: Mitarbeiter, die irrtümlich ein Phishing-Mail («Angeln nach Passwörtern») und damit die Lücken von innen öffnen.

Die grösste Schwachstelle ist der Mensch, der irrtümlich ein schädliches Phishing-Mail öffnet.

Wichtig ist bewusstes Verhalten

Das heisst, der Mensch ist das grösste Risiko. Das ist einerseits ungünstig, weil Irren immer menschlich bleiben wird. Andererseits bedeutet es auch, dass Organisationen den Hackerangriffen nicht machtlos gegenüberstehen – denn Menschen sind lernfähig. Sicherheitsexperte Fischer von der Hochschule Luzern sagt: «Es braucht vor allem das Bewusstsein und das richtige Handeln aller Personen, die mit diesen Daten und Geräten zu tun haben. Dort ist die grösste Lücke, damit die grösste Gefahr und deshalb auch der bedeutendste Handlungsbedarf.»

Die wichtigsten Tipps im Umgang mit Internetsicherheit hat Switch zusammengefasst (siehe Kasten). Tatsächlich seien sich die Spitäler ihrer Verantwortung sehr wohl bewusst, sagt Leuthold, sie betrieben vielfach Informationssicherheitsmanagement und IT-Security nach heutiger «Good Practice». Nur: «Das organisierte Verbrechen im Internet (Cybercrime) entwickelt sich so schnell, dass diese Massnahmen heute allein nicht ausreichen, sondern die Abwehr verstärkt werden muss.» Zentral werde dabei unter anderen die Fähigkeit zur schnellen Erkennung erfolgreicher Angriffe und jene zur schnellen Abwehr erkannter Angriffe sein. «Wir von Switch fokussieren uns seit Jahren auf diese Themen», sagt der Sicherheitsexperte. «Es gibt aber keine Möglichkeiten, alle vorhandenen technischen Lücken zu beheben, erst recht in der Medizinaltechnologie, in der oft veraltete Systeme eingesetzt werden und Aktualisierungen aufgrund rechtlicher Vorgaben sehr aufwendig sind.» Um trotzdem einen weitgehend sicheren Schutz aufbauen zu können, werde nicht jedes Spital für sich arbeiten können; vielmehr werde eine «Bündelung der Mittel in gemeinsamen Kompetenzzentren» nötig.

Ein Trost: «Die beiden von Switch betriebenen ‹Top Level Domains› .ch und .li sind nachweislich die sichersten ihrer Art weltweit», sagt Martin Leuthold. Grund sei eine enge Zusammenarbeit zwischen dem Bundesamt für Kommunikation, Switch als Betreiber, dem Schweizer Regierungscomputer Emergency Response Team (Melani) und den Strafverfolgungsbehörden (Kobik). Diese Zusammenarbeit erlaube, für Phishing- und Malware missbrauchte Domains innerhalb 24 Stunden zu sperren, wenn der Domainhalter die Probleme nicht beseitigt.

Schutz vor Internet-Verbrechen

Eine oft benutzte Methode des Cyberverbrechens geschieht mittels Ransomware: Immer häufiger sperren Cyberkriminelle den Zugriff auf Daten und fordern Lösegeld für die Freigabe. Inzwischen haben sie für solche Fälle sogar professionelle Helpdesks eingerichtet, die Auskunft geben. Switch hat eine Zusammenstellung gemacht, mit welchen Massnahmen man sich dagegen schützen kann (www.switch.ch):

Backup
Machen Sie regelmässig ein Backup Ihrer Daten, zum Beispiel auf einer externen Festplatte oder bei einem Clouddienst.

Virenscanner
Richten Sie ein Virenschutzprogramm ein – am besten so, dass es automatische Updates der Virenliste macht.

Firewall
Installieren Sie eine Firewall. Sie alarmiert sie bei Problemen im Internet.

Updates
Laden Sie regelmässig Updates für Ihre Programme, Plugins sowie Apps herunter und installieren Sie immer die aktuellsten Versionen. Sie enthalten Patches für bekannte Schwachstellen.

Gute, neue Passwörter
Ändern Sie öfter die Passwörter zu Ihren Bank- und E-Mail-Konti sowie allem, was Sie online abwickeln. Benutzen Sie schwer zu knackende Abfolgen von Buchstaben, Zahlen und Zeichen. Notieren Sie sich diese nirgends, sondern verwenden Sie solche, die Sie sich merken können.

Vorsicht
Seien Sie zurückhaltend mit der Heraus- beziehungsweise Eingabe Ihrer Daten. Klicken Sie auch nicht auf jeden Link oder Anhang in E-Mails oder Facebook-Nachrichten.

Sisa-Check
Führen Sie monatlich den Sisa-Check durch (Swiss Internet Security Alliance, www.swiss-isa.ch)

Adblocker
Installieren Sie einen Adblocker.

«Das führt dazu, dass es für Internetkriminelle weniger interessant ist, .ch- und .li-Domains zu missbrauchen.»

Allen Gefahren zum Trotz: eHealth macht Sinn

Angesichts solcher Gefahren stellt sich dennoch die Frage, wie sinnvoll denn ein elektronischer Austausch von Patientendaten insgesamt wirklich ist? Für Experten ist das keine Frage: «Die Rückkehr zu papierbasierten Patientendossiers, wie es einige Spitäler in den USA propagieren, kann nicht die richtige Marschrichtung sein», sagt Peter Fischer von der Hochschule Luzern. «Sind Patientendaten für Leistungserbringer elektronisch verfügbar, hat das klare, unverzichtbare Vorteile.» Ohne Zugriff auf Patientendaten, betont er, hätten wir heute schon ein allgegenwärtiges Problem: Untersuchungen müssen unnötigerweise wiederholt werden, Patienten machen aus der Erinnerung falsche Angaben, und sogenannte Medienbrüche – das Wechseln des Mediums während der Übertragung, also zum Beispiel von Papier auf Mail oder umgekehrt – generieren häufig Fehler. Auch das Erkennen von Alarmsignalen bleibe dem Zufall überlassen, wenn medizinische Geräte nicht vernetzt seien und damit nicht aus der Ferne überwacht werden können. «Bei den aktuellen Personalengpässen ist es allerdings undenkbar, die Geräte vor Ort zu überwachen, von der Wirtschaftlichkeit ganz zu schweigen», sagt Fischer klar. «Die Frage lautet also nicht, ob wir es elektronisch machen, sondern wie.»

«Die Frage ist nicht, ob wir elektronische Patientendaten austauschen wollen, sondern wie.»

Auch Leuthold von Switch sagt: «Hundertprozentige Sicherheit ist nicht zu erreichen. Es ist aber ausreichend, wenn Organisationen das Sicherheitsniveau so deutlich erhöht haben, dass ‹faule› Angreifer lieber die schlechter geschützten Organisationen angreifen.» Das Kunststück, fasst Peter Fischer zusammen, sei nun, «bestmögliche Sicherheit, gute Handhabbarkeit und wirtschaftliche Verträglichkeit» unter einen Hut zu bekommen. Eine absolute Sicherheit, da ist auch er realistisch, gibt es in der eTechnologie nicht. «Die gab es nirgends und wird es auch nirgendwo geben. Das gilt für die Informationssicherheit gleich wie für den Strassenverkehr», sagt er. Trotzdem stelle sich niemand die Frage, ob man den Strassenverkehr einstellen solle. Vielmehr seien sowohl im Strassenverkehr wie beim elektronischen Patientendossier neben den technologischen Voraussetzungen auch die menschlichen Komponenten «Bewusstsein» und «Handlungskompetenz» notwendig.

Ziel sei, das Restrisiko so weit zu minimieren, dass die vielfältigen Vorteile bei weitem überwiegen. «Wichtig ist, dass alle Beteiligten wie Ärzte, Pflegefachpersonen, Lösungsanbieter und auch wir als Hochschule zusammenspannen, damit wir eine gute Lösung und dadurch das Vertrauen der Patientinnen und Patienten bekommen.» Denn nur dann werden sich viele Patienten entscheiden, für sich ein elektronisches Patientendossier anlegen zu lassen. Und nur so kann eHealth Suisse der Erfolg werden, den sich der Bundesrat vorstellt: «Der Schweizer Bevölkerung den Zugang zu einem bezüglich Qualität, Effizienz und Sicherheit hochstehenden und kostengünstigen Gesundheitswesen zu gewährleisten.» ●