Schweiz

Patientendaten sind oft leichte Beute

Ein im Auftrag des TA durchgeführter Test zeigt: Die IT-Netzwerke von Arztpraxen weisen zum Teil gravierende Sicherheitslücken auf. Das kann auch für Patienten gefährlich werden.

Simone Rau und Barnaby Skinner

Wie leichtgläubig sind Ärzte? Zumindest Christoph Niederberger reagiert schlagfertig, als er vom «Tages-Anzeiger» gefragt wird, ob man seine Praxis auf Datensicherheit überprüfen dürfe. «Woher weiss ich, dass das nicht schon der Test ist?»

Der Hausarzt hatte an einer Umfrage des TA bei 256 Ärzten teilgenommen. 110 von ihnen, darunter der Allgemeinmediziner aus Wil SG, bekundeten darin ihr Interesse an einer IT-Sicherheitsüberprüfung. Der Check, durchgeführt von der Churer Firma First Security Technology AG, sollte zeigen, wie anfällig Arztpraxen für Cyberangriffe sind, wie gravierend deren Sicherheitslöcher, und wie diese am besten gestopft werden können.

Niederberger hat vorbildlich auf die Anfrage reagiert – weil vorsichtig. Weder kannte er die Journalisten des TA noch die Mitarbeiter der Firma First Security persönlich. Der Kontakt lief anfangs nur über E-Mail. «Dahinter könnte jeder stecken», sagte sich der Arzt.

Tatsächlich beginnen viele Cyberangriffe mit einer E-Mail, deren Absender den Empfängern unbekannt sind. Letztere klicken gedankenlos auf den PDF-Anhang oder das Word-Dokument einer fingierten Rechnung. Schon lädt im Hintergrund ein Programm, das die IT-Sicherheit ausschaltet. In der Branche gilt deshalb: Das grösste Einfallstor in ein IT-Netzwerk ist immer der Mensch, sei das Angriffsziel nun eine kleine Arztpraxis, sei es eine Grossfirma, wie aktuell das Beispiel des Rüstungskonzerns Ruag.

Erst nachdem sich Niederberger von der Identität der Mailabsender überzeugt hatte, willigte er ein, an der IT-Schwachstellenanalyse teilzunehmen; gemeinsam mit zehn weiteren Arztpraxen aus der ganzen Schweiz. Von den total elf testwilligen Ärzten liessen sich nur die Ergebnisse von sieben auswerten. In den restlichen vier Fällen war der Sicherheitstest nicht möglich, weil die Praxen die nötigen Geräte nicht richtig installierten, sie ihre Computer nicht einschalteten oder weil die Internetverbindung zu langsam war.

Auch gespeicherte Röntgenbilder in Patientendossiers sind vor Hackern nicht sicher. Foto: Callista Images (plainpicture)

Keine Updates, keine Firewall

Das Resultat: Alle sieben getesteten Arztpraxen wiesen Sicherheitsprobleme auf. Einer der Ärzte benutzte einen veralteten, ohne Passwort gesicherten WLAN-Router. Mit wenig Aufwand könnte man so den Datenverkehr ausspionieren, um Passwörter oder E-Mails zu stehlen. In einer anderen Praxis war es möglich, von extern die Firewall auszuschalten. So könnten unbemerkt Viren in die Praxis eingeschleust werden.

In zwei der sieben Arztpraxen stiess die Firma First Security auf schwerwiegende Löcher. In beiden Fällen betrafen diese sogenannte NAS. Die Abkürzung steht für Network Attached Storage, auf Deutsch: netzgebundene Speicher. Diese werden eingesetzt, um unterwegs auf Daten zuzugreifen, die im Falle der Ärzte auf dem Computer in der Praxis abgespeichert sind. Sie sind besonders bei Privatnutzern beliebt, um etwa Fotos abzulegen – und sie so jederzeit greifbar zu haben. Weil NAS so günstig und einfach zu handhaben sind, setzen auch immer mehr KMU darauf; wie der Test zeigte, gehören auch Arztpraxen dazu. Diese verwenden diese Art von Speichern aber nicht für Ferienfotos, sondern für sensible Patientendaten.

Beide betroffenen Arztpraxen setzten netzwerkgebundene Speicher der Firma Synology ein. Trotz deren Empfehlung, die regelmässigen Sicherheitsupdates durchzuführen, verzichteten die Ärzte darauf. Die NAS der Praxen waren zudem nicht mit einer Firewall geschützt. Das würde es für Cyberkriminelle noch einfacher machen, an gespeicherte Röntgenaufnahmen, Laborberichte oder Gesundheitschecks zu kommen.

Die Hacker bräuchten dafür nicht einmal besonders gewieft zu sein. Sie könnten via Internet das Passwort der Geräte zurücksetzen lassen und dann das automatisch generierte E-Mail abfangen, indem sie das offene WLAN in den Praxen ausspionieren. Ist das zu aufwendig, gäbe es die Variante Vorschlaghammer. Mit einer kostenlosen Software könnten die Kriminellen automatisch alle Passwortkombinationen prüfen. Das kann je nach Passwortlänge zwar Wochen dauern. Doch irgendwann ist das Passwort geknackt. NAS-Geräte, die wie im Fall der beiden Ärzte ohne Firewall in Betrieb sind, können solche millionenfache Passworteingaben nicht verhindern. Das Perfide: Die Betroffenen merken nicht, dass sie bestohlen werden, weil die Originaldaten auf ihrem Computer noch unbeschädigt vorhanden sind.

Spektakuläre Hackerangriffe

Aber wie hoch ist das Risiko für kleine Privatpraxen überhaupt? Tatsächlich ist es in jüngster Zeit zu spektakulären Fällen gekommen. Im Januar dieses Jahres wurde etwa das Hollywood Presbyterian Medical Center in Los Angeles Opfer von Cyberkriminellen. Die Ärzte des Luxusspitals mussten umgerechnet 3,7 Millionen Franken an Hacker bezahlen, um Zugang zu gestohlenen Patientendaten zurückzuerhalten. Die Kriminellen waren in das Spitalsystem eingedrungen und hatten sensible Daten verschlüsselt. Für die Patienten der Super-GAU. Auf einen Schlag waren ihre Krankenakten von den Ärzten nicht mehr einsehbar. Wenn der Arzt oder die Pflegeperson nicht weiss, wie ein Patient behandelt wurde, welche Medikamente er wie oft braucht, kann das schnell lebensbedrohlich werden. Davon abgesehen, könnten die Hacker die Patientendaten an Unbefugte weiterverkaufen – beispielsweise an Arbeitgeber.

Ähnliches erlebten im Februar zwei Spitäler in Deutschland: Cyber-Gangster nahmen Patientendaten des Neusser Lukaskrankenhauses bei Düsseldorf als Geisel. Dasselbe passierte im Klinikum Arnsberg bei Dortmund. Hier poppten auf Bildschirmen der Klinik Lösegeldforderungen auf, weil die Server gehackt wurden. Auch kleine Arztpraxen rücken ins Visier der Hacker, wie letztes Jahr der Fall eines Arztes aus Freiburg im Breisgau zeigte. Auch in der Schweiz gab es vereinzelte Fälle, wie die FMH auf Anfrage sagt. Details sind nicht bekannt.

Pascal Mittner, Chef von First Security, der den Test für den TA durchführte, sagte: «Es gibt kein Allheilmittel gegen Cyberangriffe, genauso wie es kein Allheilmittel dagegen gibt, zu Hause ausgeraubt zu werden.» Es seien auch bei weitem nicht nur Ärzte, die sorglos mit Speichersystemen umgingen, die am Internet hängen. Bei einem schweizweiten Scan, dessen Ergebnisse seine Firma in ihrem Swiss Vulnerability Report Anfang Juni veröffentlicht und den der TA bereits einsehen konnte, stiess Mittner auf mehrere Tausend NAS-Geräte, die schutzlos im Netz hingen. Unter ihnen befinden sich auch die Datenspeicher von Anwälten und Treuhändern.

Mittner stellt fest, dass Ärzte zu den Berufsgruppen gehörten, die es besonders nötig hätten, ihr Sicherheitsbewusstsein im Internet zu überdenken. Er empfiehlt Daten-Backups an einem sicheren Ort – etwa im internen Netzwerk, einer separaten, gut geschützten Netzwerkzone für Backups oder bei einer auf Backups spezialisierten Firma. Auch die Kontrolle der Firewall-Einstellungen sei wichtig. «Eigentlich sollten die Ärzte ihre Systeme regelmässig überprüfen, um überhaupt zu wissen, wo es Löcher gibt.» Ähnlich wie ein regelmässiger Gesundheitscheck beim Menschen Auskunft über den aktuellen Zustand gebe und auf künftige Probleme hinweisen könne, gebe eine solche Prüfung wichtige Hinweise für Massnahmen in der IT.

> «Eigentlich sollten die Ärzte ihre IT-Systeme regelmässig überprüfen, um Löcher zu finden.»
> Pascal Mittner, CEO First Security

Hausarzt Niederberger erachtet das Resultat der IT-Schwachstellenanalyse als «bedenklich bis erschütternd». Er sei davon ausgegangen, «alle erdenklichen Massnahmen» ergriffen zu haben, um sein IT-System gegen Angriffe von aussen zu schützen. Auch deshalb habe er am Test teilgenommen und auf eine «Top-Note» gehofft. «Wenn wir schon durchfallen, wie steht es dann mit all den Praxen, die sich dieser Prüfung nicht stellten?»

IT-Schwachstellenanalyse
Elf Arztpraxen im Test

82 Prozent aller Ärzte in der Schweiz speichern ihre Patientendaten lokal auf ihrem Computer – also praxisintern. Das zeigte kürzlich eine Onlineumfrage des «Tages-Anzeigers», an der 256 Ärzte teilgenommen hatten (TA vom 7. 3.). Elf von ihnen liessen ihre Systeme von der Churer Firma First Security auf Herz und Nieren überprüfen. Sie hängten dafür während 24 Stunden ein kleines Gerät an ihre Computer, das ihnen die Bündner zur Verfügung stellten. Die Box identifizierte Systeme, die im gleichen Netzwerk angeschlossen sind, zum Beispiel WLAN-Router, Handys, Datenspeicher oder medizinische Geräte wie Röntgenscanner. Sodann ermittelte der Test, welche dieser Geräte für Angriffe von aussen Sicherheitslücken aufwiesen und somit teilweise das ganze System in Gefahr bringen. *(bsk)*

Nachrichten

Atomenergie
Probleme in Frankreich könnten Beznau mitbetreffen

Die französische Atomaufsichtsbehörde ASN klärt ab, ob auch das AKW Beznau betroffen ist von den Unregelmässigkeiten bei der Fertigungskontrolle von Reaktordruckbehältern des Atomkonzerns Areva. Die ASN hat das Eidgenössische Nuklearsicherheitsinspektorat (Ensi) darüber informiert. Der 1965 produzierte Reaktordruckbehälter von Block 1 des AKW Beznau weist Materialfehler auf. Ensi-Sprecher David Suchet bestätigte auf Anfrage einen entsprechenden Bericht von «Tribune de Genève» und «24 Heures». Man stehe in ständigem Kontakt mit den europäischen Atomaufsichtsbehörden. Areva hatte Anfang Mai mitgeteilt, es seien Unregelmässigkeiten in den Unterlagen zu AKW-Bauteilen entdeckt worden. *(SDA)*

Ladenöffnungszeiten
Gewerkschaftsbund droht mit Referendum

Sollte das Parlament sich in der Sommersession definitiv für längere Ladenöffnungszeiten aussprechen, will der Schweizerische Gewerkschaftsbund das Referendum ergreifen. Das haben die Delegierten gestern entschieden. Damit zeichnet sich eine Allianz aus SP und Gewerkschaften gegen die Liberalisierung ab. Bereits im Februar hatte die Gewerkschaft Unia ihren Kampf dagegen angekündigt. Auch SP-Präsident Christian Levrat will sich daran beteiligen. *(SDA)*

Parolen für den 5. Juni

Asylgesetzrevision
Die Revision schafft die rechtlichen Voraussetzungen, um die Asylverfahren zu beschleunigen. Dafür bringt der Bund die meisten Asylsuchenden in eigenen Zentren unter. Um die stark verkürzten Beschwerdefristen auszugleichen, erhalten alle Asylsuchenden einen Rechtsvertreter an ihre Seite.

Ja SP, FDP, CVP, Grüne, GLP, BDP, EVP, Economiesuisse, SGB, Travailsuisse, Flüchtlingshilfe, Caritas, Heks
Nein SVP, Hauseigentümerverband

Fortpflanzungsmedizin
Die Gesetzesänderung erlaubt die Präimplantationsdiagnostik (PID). Diese genetische Untersuchung von Embryonen verhindert die Übertragung einer schweren, genetisch bedingten Krankheit von den Eltern auf ihr Kind. Die PID darf gemäss Gesetz bei allen Paaren angewendet werden, die eine künstliche Befruchtung in Anspruch nehmen.

Ja FDP, CVP, GLP, BDP, FMH, Spitalverband
Nein SVP, EVP, Procap, Agile, Insieme, Schweizer Bischöfe
Stimmfreigabe SP, Grüne

Grundeinkommen
Die Volksinitiative für ein bedingungsloses Grundeinkommen will «der ganzen Bevölkerung ein menschenwürdiges Dasein und die Teilnahme am öffentlichen Leben» ermöglichen. Die Ausgestaltung wäre dem Parlament überlassen. Die Initianten schlagen ein Grundeinkommen von 2500 Franken pro erwachsene Person vor.

Ja Grüne
Nein SVP, SP, FDP, CVP, GLP, BDP, EVP, Economiesuisse
Stimmfreigabe Travailsuisse

Milchkuhinitiative
Die Initiative «für eine faire Verkehrsfinanzierung» verlangt, dass die von den Automobilisten entrichtete Mineralölsteuer gänzlich in die Strassenkasse fliesst. Heute kommen davon 50 Prozent, rund 1,5 Milliarden Franken, dem allgemeinen Bundeshaushalt zugute.

Ja SVP, Auto Schweiz, AGVS, ACS, TCS
Nein SP, FDP, CVP, GLP, BDP, EVP, Städteverband, VCS, VÖV

Initiative «Pro Service public»
Der Initiativtext verlangt, dass staatsnahe Betriebe in der Grundversorgung nicht profitorientiert arbeiten. Zudem sollen Topgehälter dieser Betriebe dem Bundesniveau angeglichen werden.

Ja –
Nein SVP, SP, FDP, CVP, Grüne, GLP, BDP, EVP, Economiesuisse, SGV, SGB, Travailsuisse, VPOD, Städteverband, Gemeindeverband