Dr. Datenleck, Teil 2

Nachholbedarf bei der IT-Sicherheit deutscher Arztpraxen

Der Daten-GAU in der Celler Arztpraxis wirft kein gutes Licht auf die IT-Sicherheit in deutschen Praxen. Vorgeschriebene Kontrollen gibt es offenbar nicht. Unterdessen ist die Telekom bemüht, die gefährliche Router-Lücke zu schließen, die zu dem Datenleck beigetragen hat.

Von Ronald Eikenberg

Unser Artikel „Dr. Datenleck – Warum eine komplette Arztpraxis offen im Netz stand“ aus der vergangenen c't hat für viel Wirbel gesorgt. Wir haben darin aufgedeckt, dass unter anderem die sensiblen Gesundheitsdaten von rund 30.000 Patienten einer Celler Gemeinschaftspraxis für Orthopädie für jeden über das Internet abrufbar waren. Zu der Datenschutz-Katastrophe hatte eine Verkettung mehrerer Fehler geführt: Zum ersten war der Dateiserver im Praxisnetz unzureichend geschützt. Offenbar konnte jeder im internen Netz darauf zugreifen.

Der GAU trat jedoch erst durch eine Schwachstelle in einem Telekom-Router ein: Die Telekom Digitalisierungsbox machte nämlich mehr Ports von außen zugänglich, als auf den ersten Blick ersichtlich war. Nutzte man den Einrichtungsassistenten des Routers, um eine Port-Weiterleitung für Port 80 oder 443 einzurichten, hat der Assistent eigenmächtig die Ports 80 bis 89 oder 440 bis 449 nach außen geöffnet. So war der Dateiserver mit den Patientendaten auf Port 445 plötzlich für Gott und die Welt erreichbar – ohne Passwort und über das Internet. Falls Sie unseren Artikel verpasst haben, können Sie ihn gratis unter ct.de/y1m7 lesen.

Nach der Veröffentlichung der Geschichte haben unsere Leser das Thema intensiv diskutiert. Allein im Artikelforum auf ct.de zählten wir innerhalb weniger Tage über 1000 Leserkommentare, weitere Zuschriften gingen per Mail ein. Von Spott bis Mitgefühl ist alles dabei, Kern der Diskussionen ist jedoch oftmals der Versuch, die Schuldfrage zu klären. Doch diese ist kaum zu beantworten. Denn trotz der Router-Lücke ist die Praxis vermutlich nicht aus der Verantwortung zu ziehen.

Eine Praxis ist grundsätzlich für die Sicherheit der Patientendaten zuständig, wie die Kassenärztliche Bundesvereinigung (KBV) gegenüber c't erklärte: „Ärztinnen und Ärzte unterliegen der Schweigepflicht, sie sind für die besonders sensiblen Patientendaten in ihrer Praxis verantwortlich.“

Hinweise missachtet

Offensichtlich waren die Patientendaten in der Celler Praxis nicht nach dem Stand der Technik geschützt. Und der mangelnde Zugriffsschutz ist nur eines der Probleme. Die KBV hat mit der Bundesärztekammer „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ erarbeitet (siehe ct.de/y1m7). Das Dokument richtet sich direkt an Ärzte und ist so formuliert, dass die Maßnahmen „auch für den technischen Laien verständlich“ sind.

Darin geht es unter anderem um den „Schutz von Patientendaten vor Zugriffen aus dem Internet“. Dort heißt es: „Rechner mit Patientendaten sollten niemals direkt mit dem Internet verbunden sein. Sobald ein direkter Zugriff aus dem Internet auf einen Rechner mit Patientendaten gelingt und diese Daten in unverschlüsselter Form abgelegt wurden, lassen sich diese auslesen.“ Selbst eine Verschlüsselung der Daten hilft in diesem Fall nicht, „da die Daten für die reguläre Nutzung jeweils entschlüsselt werden müssen und damit ein Zugriff wieder möglich wäre.“


Quelle: Telekom

Nicht nur die Digitalisierungsbox Premium ist von dem fatalen Bug betroffen, sondern auch die Schwestermodelle „Standard“ und „Smart“.

Der SMB-Dateiserver mit den Daten zehntausender Patienten (Port 445) lief offenbar auf dem gleichen System wie ein VPN-Dienst (Port 443), welcher für den Zugriff aus dem Internet freigegeben war. Hätte die Praxis also Grundregeln der IT-Sicherheit befolgt und den VPN-Dienst auf einem separaten System betrieben, wäre es nicht zu dem fatalen Datenleck gekommen. Auch ein effektiver Zugriffsschutz beim Dateiserver hätte das Leck verhindert – Router-Lücke hin oder her.

Unkontrolliert

Während Arztpraxen auf stichprobenartige Hygienekontrollen der Gesundheitsämter gefasst sein müssen, interessiert sich von offizieller Seite anscheinend niemand ernsthaft dafür, ob und wie effektiv ein Arzt die intimen Daten seiner Patienten schützt. Die Kassenärztliche Bundesvereinigung ließ uns hierzu wissen: „Die Praxisinhaber haften für die Sicherheit der Patientendaten. Vorgeschriebene Kontrollen gibt es nicht, wir empfehlen Praxen, sich bei IT-Fragen grundsätzlich Unterstützung von Experten zu holen.“

Doch gute Experten sind schwer zu finden – ein unabhängiges Prüfsiegel für IT-Dienstleister im Gesundheitswesen, anhand derer Ärzte die Qualifikation erkennen können, ist c't nicht bekannt. Ab einer Größe von 20 Mitarbeitern muss eine Praxis zwar „einen Datenschutzbeauftragten benennen, der die Einhaltung des Datenschutzes und der Datensicherheit in der Praxis kontrolliert“. Einen solchen gibt es in der Celler Praxis, offenbar konnte auch er den Daten-GAU nicht verhindern.

Angesichts dieser Situation muss man davon ausgehen, dass Celle kein Einzelfall ist und Hacker auch in anderen Arztpraxen leichtes Spiel haben. Nach Angaben der KBV gibt es in Deutschland 101.932 Praxen – wenn auch nur ein Prozent davon bei der IT-Sicherheit patzt, wären das schon über 1000. Der Fall Celle beschäftigt inzwischen auch die zuständige Landesbeauftragte für den Datenschutz Niedersachsen, Barbara Thiel. Gegenüber der Celleschen Zeitung, die über unseren Artikel berichtete, erklärte sie: „Dieser [Fall] hätte meiner Behörde bereits im Oktober gemeldet werden müssen. Es ist jetzt an der Zeit, die Dinge aufzuklären."

Inzwischen habe es dazu eine Gesprächsanfrage gegeben, schriftlich würde der Sachverhalt jedoch noch nicht vorliegen. Offenbar hat die Praxis die in der DSGVO angegebene Meldefrist von 72 Stunden um Wochen überzogen. Das verschärft die Situation für die Praxis deutlich, denn wer die Mitteilungspflichten nicht befolgt, den erwartet ein Bußgeld von bis zu 10 Millionen Euro oder zwei Prozent des Jahresumsatzes. Hinzu kommen eventuelle Schadenersatzforderungen der betroffenen Patienten (siehe dazu die Artikel „Die Bomben ticken" auf Seite 166 sowie „Höchst sensibel" auf Seite 172).

Telekom reagiert

Aber zurück zur Telekom. Diese hatte gegenüber c't eingeräumt, bereits seit Mai 2019 von der Router-Schwäche beim Port-Forwarding zu wissen. Informiert wurden die betroffenen Kunden jedoch erst, nachdem wir unseren Artikel veröffentlicht hatten. Vielleicht hätte der Daten-GAU in Celle verhindert werden können, hätte man die Praxis frühzeitig über das Sicherheitsproblem informiert.

Auch das Firmware-Update ist erst nach unserem Artikel erschienen. Die neue Firmware barg eine Überraschung: Sie ist nämlich nicht nur für die Digitalisierungsbox Premium erschienen, die in der Celler Arztpraxis zum Einsatz kam, sondern auch für die beiden Schwestermodelle „Standard" und „Smart".

Die neue Firmware trägt die Versionsnummer 11.01.02.100, Sie finden die Update-Dateien über ct.de/y1m7 zum Download. Wer eine der betroffenen Digitalboxen betreibt oder administriert, sollte das wichtige Update umgehend installieren. Die Telekom hatte schon mit einem vorherigen Update einen Versuch unternommen, die Situation zu entschärfen. Diese Änderung dürfte jedoch die meisten bestehenden Router nicht erreicht haben, da sie erst nach einem Werksreset wirksam wurde. *(rei@ct.de)* c't

Teil 1 und Router-Update: ***ct.de/y1m7***