Dr. Datenleck

Warum eine komplette Arztpraxis offen im Netz stand

Die Krankenakten zehntausender Patienten einer Celler Arztpraxis waren für jeden übers Internet abrufbar. Als wir dem Fall nachgingen, stießen wir auf eine erhebliche Schwachstelle in Standard-Routern der Telekom.

Von Ronald Eikenberg

Offener Server einer Arztpraxis im Raum Hannover, sämtliche Patientendaten, darunter circa 20.000 Stammdaten, in einer Datenbank offen." Mit diesem Satz beginnt eine beunruhigende Mail, welche die c't-Redaktion im Oktober erreichte. Der IT-Experte Cedric Fischer von der Firma CeFisystems nahm Kontakt mit uns auf, nachdem er im Internet einen frei zugänglichen Windows-Server entdeckt hatte, über den Daten zugänglich waren, die offensichtlich nicht für die Öffentlichkeit bestimmt sind. „Dazu höchst private Daten wie Arbeitsverträge, Kündigungen, Spenden/Schuldnerlisten, BWA etc. über und von dem Inhaber der Praxis", schrieb Fischer.

Wir nahmen umgehend Kontakt mit ihm auf, um der Geschichte auf den Grund zu gehen. Er hatte nicht übertrieben: Anscheinend sind sogar rund 30.000 Patienten betroffen. Sein Fund war offensichtlich echt und die Aktualität der Dateien ließ darauf schließen, dass sie nach wie vor im laufenden Praxisbetrieb mit Patientendaten befüllt wurden. Der Server war ungeschützt, die Zugriffsrechte waren auf „Jeder" gesetzt. Jeder, der die IP-Adresse kannte, konnte also darauf zugreifen. Und diese war kein Geheimnis, sie ließ sich leicht über die frei zugängliche Server-Suchmaschine Shodan herausfinden.

Auf dem Server befand sich alles, was in einer großen Arztpraxis an Daten aufläuft: neben den Stammdaten zehntausender Patienten auch Befunde, Gesprächsnotizen, Arztbriefe und vieles mehr. Die große Menge der Datensätze erklärt sich dadurch, dass es sich um eine Gemeinschaftspraxis mit mehreren Orthopäden handelt und die Daten über viele Jahre zurückreichen.

Wir kontaktierten die Celler Praxis kurz darauf per Mail mit der Bitte, den Zugriff auf die Patientendaten umgehend abzustellen. Daraufhin meldete sich einer der betroffenen Orthopäden bei uns und erklärte, dass er nach dem Eintreffen unserer Mail seinen IT-Dienstleister kontaktiert hatte und das katastrophale Datenleck nun gestopft sei.

Kommissar Zufall

Doch einige Tage später war der Server immer noch offen wie ein Scheunentor. In der Zwischenzeit hatte uns auch ein weiterer Hinweis erreicht, der auf den ersten Blick gar nichts mit dem Fall zu tun hatte: Der IT-Experte Christian Zengel meldete uns ein ungewöhnliches Verhalten eines Telekom-Routers. Legt man bei dem Gerät über das Webinterface eine Port-Weiterleitung für HTTPS-Dienste an, stünden mehr Ports nach außen hin offen, als man erwarten würde. Der Standardport für HTTPS ist 443, laut Zengel gibt der Router bei dieser Auswahl jedoch die Ports 440 bis 449 frei, wenn man den Assistenten der Weboberfläche benutzt. Das wäre ein fatales Fehlverhalten, da sich in diesem Portbereich auch SMB tummelt (Port 445), das Standardprotokoll für Dateifreigaben unter Windows. Bei dem betroffenen Router handelt es sich laut Zengel um die „Digitalisierungsbox Premium", welche die Telekom ihren Businesskunden anbietet.

Diese Sicherheitslücke passte ziemlich gut zu dem Fall der offen zugänglichen Patientendaten. Die IP-Adresse der Praxis stammt nämlich aus dem Adressbereich der Telekom-Geschäftskunden. Außerdem handelte es sich bei dem Server um einen Windows-Dateiserver, der über Port 445 erreichbar war. Und anders war es zu diesem Zeitpunkt kaum zu erklären, dass die Patientendaten immer noch ungeschützt über das Internet abrufbar waren. Wir nahmen erneut Kontakt mit der Celler Praxis auf und berichteten von unserem Verdacht, dass eine Router-Lücke in Zusammenhang mit dem Fall stehen könnte.

Kurz darauf rief der verantwortliche IT-Dienstleister an. Tatsächlich war eine Digitalisierungsbox Premium der Telekom im Einsatz. Dem Techniker war bei

seinem Einsatz aufgefallen, dass mehr Ports als gedacht freigegeben waren. Obwohl nur 443 zugänglich sein sollte, war der gesamte Bereich von 440 und 449 eingestellt. Offensichtlich gab es einen Zusammenhang zu der Router-Lücke.

Der Techniker erklärte, dass er die Konfiguration nach unserer ersten Kontaktaufnahme korrigiert und einen Portscan von außen durchgeführt habe, um zu verifizieren, dass die Ports des Servers nicht länger über das Internet erreichbar sind. Danach habe er die Firmware der Digitalisierungsbox noch auf den aktuellen Stand gebracht. Aber warum war der Dateiserver mit den Patientendaten weiterhin im Internet?

Gefährliche Router-Lücke

Wir kauften einen betroffenen Router, um uns selbst ein Bild von der Situation zu machen. Tatsächlich gab der Router mehr Ports frei, als man erwarten würde. Der Router ordnet „HTTPS“ den Ports 440 bis 449 und „HTTP“ den Ports 80 bis 89 zu. Bei unseren Untersuchungen drängte sich außerdem eine Theorie auf, warum der Praxisrouter weiterhin die Zugriffe aus dem Internet auf den Dateiserver durchleitete, obwohl die Konfiguration angeblich korrigiert worden war.

Es gibt im Webinterface mehrere Speicherknöpfe mit unterschiedlichen Funktionen. Ein einfaches Speichern übernimmt die geänderte Konfiguration umgehend. Dann gibt es noch die Möglichkeit, die geänderten Einstellungen als Boot-Konfiguration zu speichern. Macht man das nicht, sind nach einem Neustart des Routers wieder die vorherigen Einstellungen aktiv. Der Dienstleister der Praxis hatte nach der Korrektur der Port-Weiterleitung eigenen Angaben zufolge ein Firmware-Update durchgeführt – und das endet immer mit einem Router-Neustart. Mutmaßlich hatte der Techniker die neue Konfiguration also nicht als Boot-Konfiguration hinterlegt.

Weitere Versuche mit der Digitalisierungsbox zeigten, dass die fehlerhafte Umleitung anscheinend in der aktuellen Firmware korrigiert wurde, zumindest ein bisschen. Startet man mit einer frischen Konfiguration, etwa nach einem Werksreset, ordnet der Router die Ports für HTTP und HTTPS korrekt zu. Beginnt man allerdings mit einer älteren Firmware und bringt diese auf den aktuellen Stand, übernimmt der Router die fehlerhafte Zuordnung von der alten Version. Selbst wer die Firmware immer zeitnah auf den aktuellen Stand gebracht hat, war also von der Sicherheitslücke betroffen, sofern nicht gerade ein Werksreset durchgeführt wurde.

Gibt man bei dem Business-Router der Telekom den Dienst „HTTPS“ nach außen frei, öffnet er gleich zehn Ports für Zugriffe aus dem Internet.

Telekom wusste Bescheid

Der IT-Dienstleister der Arztpraxis hat nach unserer zweiten Kontaktaufnahme erneut reagiert – dieses Mal war das Datenleck endlich dauerhaft geschlossen. Eine Shodan-Recherche im IP-Bereich der Telekom-Businesssparte deutete darauf hin, dass es noch weitere Fälle wie den der Celler Arztpraxis gibt. Wir informierten die Telekom über das Sicherheitsproblem der Digitalisierungsbox. Ein Sprecher des Unternehmens bestätigte es und erklärte, dass „diese Schwäche beim Port-Forwarding seit Mai 2019 bekannt“ sei.

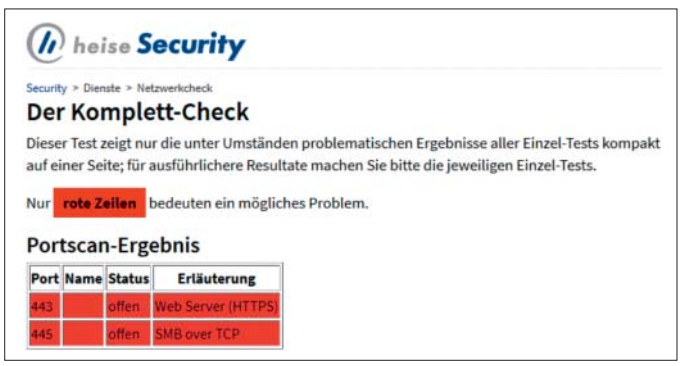
Ein Patch soll nun für Abhilfe sorgen, auch ohne Werksreset. Er fügte hinzu: „Wenn Sie mich fragen, warum es von Mai bis heute gedauert hat, einen solchen Patch anzubieten, so kann ich Ihnen darauf keine Antwort geben. Das ist eindeutig ein Fehler von uns, hier hätten wir schneller gemeinsam mit dem Hersteller Bintec Elmeg agieren müssen.“ Die Telekom gab an, sich nun um die Freigabe des Firmware-Updates zu kümmern und seinen Kunden empfehlen zu wollen, es einzuspielen.

Offen bleibt die Frage, wer für Schäden haftet, die durch die oben beschriebene Situation entstanden sind. Diese Frage dürfte derzeit die Celler Arztpraxis beschäftigen, denn es handelt sich nach Datenschutzgrundverordnung (DSGVO) um einen meldepflichtigen Vorfall, der laut Art. 33 unverzüglich und möglichst innerhalb von 72 Stunden nach Bekanntwerden der zuständigen Datenschutzaufsichtsbehörde zu melden ist.

Da es sich um hochsensible Patientendaten handelt und Unbefugten ein detaillierter Einblick in die Krankheitsgeschichte zehntausender Patienten möglich war, hätten außerdem die vom Datenleck betroffenen Personen unverzüglich informiert werden müssen, so wie es Art. 34 DSGVO vorsieht. Wer diese Mitteilungspflichten nicht befolgt, hat mit einem Bußgeld von bis zu 10 Millionen Euro oder 2 Prozent des weltweit erzielten Jahresumsatzes zu rechnen. Wir haben der Gemeinschaftpraxis vor der Veröffentlichung Gelegenheit gegeben, Stellung zu dem Fall zu beziehen. Eine unserer Fragen war, ob und wann der Vorfall gemeldet wurde. Auch mehr als eine Woche nach Ablauf unserer Frist blieben unsere Fragen unbeantwortet.

Wer auf Nummer sicher gehen möchte, dass keine Dienste im internen Netz unerwartet von außen erreichbar sind, kann einen externen Portscan auf die eigene Internet-IP-Adresse durchführen. Dazu können Sie zum Beispiel den Netzwerkcheck von heise Security nutzen. Dieser überprüft, ob unter Ihrer IP offene Ports erreichbar sind und teilt Ihnen das Ergebnis sofort mit. *(rei@ct.de)* c't

***Netzwerkcheck:* ct.de/yjkh**



Der Netzwerkcheck von heise Security spürt Dienste im internen Netz auf, die übers Internet erreichbar sind – in diesem Fall durch einen fehlkonfigurierten Telekom-Router.