Der gläserne Kranke

Am 25.09.2019 habe ich bei GMX-News den folgenden Text gefunden. Und weil Berichte solchen Inhalts nach meinen Erfahrungen (seit Beginn der HATSCHI-Kolumne) relativ schnell wieder „von der Bildfläche verschwinden“ (ein Schelm, wer Böses dabei denkt …) möchte ich diesen hier für die Nachwelt erhalten, indem ich ihn in die HATSCHI-Kolumne aufnehme. Einen herzlichen Dank an den Bayerischen Rundfunk!

BR24 17.09.2019, 07:02 Uhr

Millionenfach Patientendaten ungeschützt im Netz

Hochsensible medizinische Daten, unter anderem von Patienten aus Deutschland und den USA, sind nach Recherchen des BR und der US-Investigativplattform ProPublica auf ungesicherten Internetservern gelandet. Jeder hätte darauf zugreifen können.

Brustkrebsscreenings, Wirbelsäulenbilder, Röntgenaufnahmen eines Brustkorbs, der Herzschrittmacher ist gut erkennbar. Es sind intimste Bilder, die über Jahre hinweg frei verfügbar im Netz zu finden gewesen sind. Diese Datensätze von weltweit mehreren Millionen Patienten liegen auf Servern, die nicht geschützt sind. Auch Tausende Patienten aus Deutschland lassen sich in diesem Datenleck finden. Das hat eine gemeinsame Auswertung des Bayerischen Rundfunks und des US-amerikanischen Rechercheportals ProPublica ergeben.

Die Bilder sind hochauflösend und gespickt mit zahlreichen Informationen. Fast alle davon sind personenbezogen: Geburtsdatum, Vor- und Nachname, Termin der Untersuchung und Informationen über den behandelnden Arzt oder die Behandlung selbst.

Röntgenbilder von bayerischen Patienten im Netz

In Deutschland sind laut BR-Recherchen mehr als 13.000 Datensätze von Patienten betroffen, in mehr als der Hälfte sind Bilder enthalten: Sie waren noch bis vergangene Woche zugänglich und stammen von mindestens fünf verschiedenen Standorten. Der größte Teil der Datensätze entfällt auf Patienten aus dem Raum Ingolstadt und aus Kempen in Nordrhein-Westfalen.

Weltweit ist die Dimension deutlich größer, Server auf der ganzen Welt sind ungeschützt: In rund 50 Ländern von Brasilien über die Türkei bis Indien sollen 16 Millionen Datensätze offen im Netz sein. Besonders betroffen sind Patienten aus den USA. Allein bei einem einzelnen Anbieter für radiologische Untersuchungen lagen nach einer Auswertung von ProPublica mehr als eine Million Datensätze von Patienten vor.

Patientendaten einfach zu finden

Wenn Patienten in einer MRT-Röhre untersucht werden, entstehen zwei- und dreidimensionale Bilder vom Körperinneren. Diese Bilder werden von den Geräten auf einen speziellen Server geschickt, der für die Bildarchivierung verwendet wird, ein sogenanntes "Picture Archiving and Communication System" (PACS). Auch Röntgenaufnahmen und Bilder aus der Computertomographie landen auf diesen Servern.

Sind die Server nicht ausreichend gesichert, ist es trivial, an die Daten heranzukommen, erklärt der Experte für Informationssicherheit Dirk Schrader. Er kontaktierte die Investigativ- und

Datenjournalisten des Bayerischen Rundfunks, nachdem er weltweit mehr als 2.300 Rechner gefunden hatte, auf denen diese Datensätze lagen. Die Server waren ungeschützt.

Keine Passwörter, kein Datenschutz

Schrader spricht von einem "near realtime-access". Ein Zugriff, beinahe in Echtzeit also. "Bei den Systemen, die ich überprüft habe, hatte ich den Eindruck, dass ich im Zweifelsfall sogar in der Lage wäre, früher als der Arzt auf das Bild zuzugreifen", sagt er.

Journalisten von BR Recherche/BR Data haben das Vorgehen von Schrader nachvollzogen. Es wurden auch stichprobenartig Betroffene kontaktiert und so die Echtheit der Daten bestätigt.

Datenschutzbeauftragter Kelber: "Das geht niemanden irgendetwas an"

Der Bundesbeauftragte für Datenschutz, Ulrich Kelber, spricht von einem "verheerenden ersten Eindruck", als ihm die Reporter einen Patientendatensatz in anonymisierter Form zeigen. Er warnt vor möglichen Folgen: "Sie möchten nicht, dass ein Arbeitgeber, ein Versicherungskonzern, eine Bank diese Daten kennt, und ihnen keinen Vertrag oder keinen Kredit gibt." Diese Daten würden unsere digitale Identität ausmachen, "sie gehören nicht in die Hände Dritter."

Auch Sebastian Schinzel, Professor für IT-Sicherheit an der FH Münster, spricht von einem "handfesten Skandal". Er arbeitet derzeit in einem Projekt des Bundeslandes Nordrhein-Westfalen daran, die Cybersicherheit für die Gesundheitswirtschaft zu verbessern: "Diese Daten sind hochsensibel, und ich möchte natürlich auf keinen Fall, dass das im Internet steht, ohne Passwort-Authentifizierung. Ich finde das katastrophal."

Behörde für IT-Sicherheit informiert 46 Länder

Dirk Schrader, der den BR auf das Problem aufmerksam gemacht hatte, kontaktierte auch das für IT-Sicherheit zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI). Auf Anfrage teilte ein Sprecher mit, dass man 17 Fällen nachgehe und "drei betroffene Einrichtungen direkt über den Sachverhalt" informiert habe.

Das BSI darf aus rechtlichen Gründen nicht selbst auf die Daten zugreifen. In den restlichen 14 Fällen, in denen die IP-Adresse alleine nicht ausreichte, um das Leck zu identifizieren, habe man die Internetprovider kontaktiert. Diese seien nun angehalten, die betroffenen Einrichtungen zu informieren. Außerdem habe man Behörden in 46 Ländern kontaktiert.

Mehrere Server mit sensiblen Patientendaten waren nach BR-Informationen bis vergangene Woche erreichbar, darunter ein Server mit 7.000 Untersuchungsdaten von Patienten in Bayern. Das Bayerische Landesamt für Datenschutzaufsicht steht mit dem Betreiber des Servers in Kontakt, wie ein Sprecher auf Anfrage schriftlich mitteilt. Nun würden nächste Schritte geprüft: "Dies kann von aufsichtlichen Maßnahmen wie einer verbesserten IT-Sicherheit bis hin zur Einleitung eines Bußgeldverfahrens gehen." Der BR hat ihm bekannte Standorte kontaktiert. Mittlerweile sind die Server vom Netz.

Datenleck lange nicht ernst genommen

Bereits im Jahr 2016 veröffentlichte Oleg Pianykh, Professor für Radiologie an der Harvard Medical School, eine Studie zu ungeschützten PACS-Servern. Er hatte damals mehr als 2.700 offene Systeme ausfindig machen können: "Wir haben ein Riesenproblem mit medizinischen Geräten, die komplett ungesichert und ungeschützt sind. Und irgendjemand, ein x-beliebiger Hacker, kann sich mit diesen Geräten verbinden und die Patientendatensätze kompromittieren", sagt Pianykh im Interview mit BR und ProPublica.

In Fachkreisen nahm man die Studie von Pianykh zwar zur Kenntnis, doch offenbar sah niemand Grund zum Handeln. Schließlich habe der US-Forscher nicht überprüft, ob sich echte Daten auf den Servern befanden, heißt es aus der Branche. So sind viele Datensätze von Patienten bis heute ungesichert im Netz.

Die Recherche ist eine Kooperation des Bayerischen Rundfunks mit dem US-amerikanischen Recherchebüro ProPublica.
Team: Pia Dangelmayer, Arne Meyer-Fünffinger, Ulrich Hagmann, Uli Köppen, Steffen Kühne, Verena Nierle, Oliver Schnuck, Josef Streule, Hakan Tanriverdi, Tatjana Thamerus, Maximilian Zierer sowie Jack Gillum, Jeff Kao und Jeff Larson von ProPublica.

So weit der Bericht des Bayerischen Rundfunks. Und nun meine Bitte an alle Menschen, die bis hierhin dem Text gefolgt sind:

Sie beherrschen glücklicherweise noch die allmählich aussterbende Kulturtechnik des Sinn entnehmenden Lesens. Ermöglichen Sie es doch bitte ganz vielen Menschen in Ihrem Freundes- und Bekanntenkreis, diese vom Bayerischen Rundfunk publizierte Recherche zur Kenntnis zu nehmen, und machen Sie sich die kleine Mühe, diesen Text weiterzuleiten!

Ganz herzlichen Dank im Interesse einer zukünftigen, re-humanisierten Gesundheitsversorgung.

Reinhard F. Spieß