Kranke IT

Sicherheitsforscher haben im Internet über 24 Millionen Datensätze von Patienten mit medizinischen Bilddaten gefunden. Die meisten enthalten nicht nur mehrere Röntgen-, CT- oder MRT-Aufnahmen, sondern auch die Namen der Patienten und der behandelnden Ärzte sowie den Grund der Untersuchung. Das Erschreckende daran: Es handelt sich dabei nicht etwa um ein Archiv, das im Darknet zum Kauf angeboten oder auf einem schlecht gesicherten Cloud-Server deponiert wurde, wie man es aus anderen großen Datenlecks der letzten Zeit kennt.

Vielmehr lassen sich die Daten ohne Authentifizierung oder sonstige Schutzmaßnahmen direkt von Archivservern herunterladen, auf denen Krankenhäuser und Praxen routinemäßig radiologische Bilder archivieren und Ärzten zugänglich machen. Um sie auszulesen, sind keine fortgeschrittenen Hackerfähigkeiten nötig: Die Forscher haben die Server über Shodan und Censys aufgespürt, Suchmaschinen, mit denen jeder Laie spezifische Internetdienste und IoT-Geräte finden kann. Es reicht, dort den richtigen Suchbegriff einzutippen, schon liefert die Suchmaschine eine lange Liste von Archivservern.

Der Zugriff auf die Daten ist dann nicht weniger trivial: Man benötigt lediglich einen DICOM-Viewer (DICOM ist der Standard zur Speicherung und Übertragung medizinischer Bilddaten), der solche PACS-Server (Picture Archiving and Communication System) ansprechen kann. DICOM-Viewer gibt es zum kostenlosen Download im Internet; die wenigen Angaben, die zum Zugriff auf den Server nötig sind, liefert Shodan frei Haus. 590 von 2300 untersuchten Archivservern standen offen wie das buchstäbliche Scheunentor; sechs davon in Deutschland, mit zusammen 15 000 Datensätzen von Patienten.

Gesundheitsdaten gehören zu den persönlichsten Daten überhaupt. Die DSGVO listet sie – neben „rassischer und ethnischer Herkunft“, politischen, religiösen und weltanschaulichen Überzeugungen sowie genetischen und biometrischen Daten – als „besondere Kategorie personenbezogener Daten“. An deren Verarbeitung stellt das Datenschutzgesetz besonders hohe Anforderungen. Dass ein Viertel der DICOM-Server für medizinische Bilddaten völlig ungeschützt ist, lässt einen fassungslos zurück.

Ist den Verantwortlichen gar nicht klar, was sie tun, wenn sie ihr Bilddatenarchiv ans Internet anschließen? Offenbar nicht – auf vielen der Server fanden die Sicherheitsforscher weitere gravierende Schwachstellen, teilweise Jahre alt, auf einigen Servern auch Hinweise auf eine bereits erfolgte Kompromittierung. Dass bereits 2016 ein Artikel im American Journal of Roentgenology auf das Ausmaß des Problems hinwies, sei nur am Rande erwähnt. All das zeigt eine derart geballte IT-Inkompetenz in den Krankenhäusern und Praxen, dass einem angst und bange werden muss.

Dass der DICOM-Standard eine TLS-verschlüsselte Übertragung der Daten zwar ermöglicht, aber nicht vorschreibt und sich zum Thema Client-Authentifzierung ganz ausschweigt, trägt sicher nicht dazu bei, die nötige Aufmerksamkeit bei den Betreibern der Archivserver zu wecken. Hoffen wir, dass das aktuelle Datenleck als Warnruf ausreicht. Viel Hoffnung habe ich allerdings nicht.

Bericht von Greenbone Networks,
Studie von O. Pianykh: ix.de/zmmp

OLIVER DIEDRICH