IT-Security

IT-Sicherheit im Krankenhaus: Hack bringt Krankenhäuser zum Stillstand

9. Oktober 2019 • IT-Security • von Bianca Wellbrock

★★★★★ 5 (1)

Dass die IT-Sicherheit im Krankenhaus eine ernst zu nehmende Angelegenheit ist, zeigte sich im Juli, als durch einen Cyberangriff ein ganzer Verbund an Krankenhäusern sowie Altenpflegeheimen vom DRK in Rheinland-Pfalz und dem Saarland stillgelegt wurde. Das Netzwerk und die IT-Infrastruktur wurden durch eine Ransomware infiziert. Zwar war der Betrieb noch möglich, durch das Verschlüsseln von Server und Datenbanken jedoch nur sehr eingeschränkt: Man musste mit Stift und Papier arbeiten.

Ransomware bedroht Gesundheitssektor

Am Morgen des 14. Juli 2019 gegen 6:30 Uhr wollten die Küchenmitarbeiter des Krankenhauses in Saarlouis das System hochfahren – erfolglos. Sie informierten den Leiter der IT, der feststellen musste, dass das komplette Netzwerk der DRK Trägergesellschaft Süd-West

© celiafoto - Fotolia.com

von einer Schadsoftware befallen war. Server und die Datenbanken des kompletten Verbunds waren verschlüsselt.

Telefon und Fax funktionierten zwar noch, jedoch hatten die Kliniken und Einrichtungen keinen Internetzugang, waren also nicht per E-Mail erreichbar. Eine konkrete Lösegeldforderung sei nicht eingegangen. Allerdings ging eine E-Mail mit einer Textdatei ein, die noch ungeöffnet ans BKA weitergeleitet wurde. Noch am selben Nachmittag des 14. Julis konnte man die kryptische Verschlüsselung der Server und Datenbanken stoppen.

Schadsoftware befällt zentralen Server

Die IT-Sicherheit im Krankenhaus war empfindlich gestört, denn die Angreifer zielten auf einen zentralen Server (Domain Controller) ab, an dem sich sämtliche Benutzer und Rechner des DRK-Netzwerks authentifizieren. Damit waren alle elf Krankenhäuser und die vier Altenpflegeeinrichtungen, die unter dem Dach dieser Trägergesellschaft organisiert sind, von dem Angriff betroffen.

Aus Sicherheitsgründen nahm man am folgenden Sonntagnachmittag die Server vom Netz – insgesamt 480 Server. Man wollte nicht nur den Befall überprüfen, sondern auch verhindern, dass sich die Schadsoftware noch weiter ausbreitet.

Arbeit ohne IT-Infrastruktur

Arbeit ohne IT-Infrastruktur

Bernd Decker, Geschäftsführer der Trägergesellschaft, erklärte die Misere, die aus dem Sicherheitsvorfall entstand: Die Patientenaufnahme, aber auch die Befunderhebung von beispielsweise Laboruntersuchungen mussten in der Zeit des IT-Stillstands mit Bleistift, Kugelschreiber und Papier vorgenommen werden. „So wie das früher mal war“, so Decker.

Nicht betroffen seien glücklicherweise medizinische Geräte. Decker erklärte außerdem, es gäbe keinerlei Hinweise darauf, dass Unbefugte Einsicht in vertrauliche Patientendaten genommen hätten. Die Patientenversorgung war durchgehend gewährleistet.

Dennoch: Die Arbeit war deutlich aufwendiger – und muss zudem doppelt gemacht werden. Laufen die Systeme wieder, müssen die Daten in die Datenbanken eingescannt oder eingegeben werden.

Sicherheitslücke identifiziert

Unklar blieb anfangs, wie die Schadsoftware auf den Server gelangen konnte. Hinweise darauf, dass Patientendaten abgegriffen wurden, existieren glücklicherweise nicht. Die zuständige Trägergesellschaft DRK Süd-West erstattete Anzeige und schaltete das Landeskriminalamt (LKA) ein. Nach wie vor ist keine Lösegeldforderung bekannt. Die E-Mail mit der verschlüsselten Textdatei wurde ungeöffnet an die Behörden übergeben.

Tatsächlich war Lösegeld offenbar das Ziel der Attacke, auch wenn man anfänglich keine Lösegeldforderung fand. Bernd Decker erklärte später zusammen mit dem IT-Leiter der DRK-Trägergesellschaft Hans-Peter Blug: „In jedem Verzeichnis, das verschlüsselt war, gab es immer eine Textdatei, die die Lösegeldforderung beinhaltete“.

Fünf Tage nach der Entdeckung konnte die Schwachstelle, über die die Angreifer eingedrungen sind, identifiziert werden, sodass das Problem – hoffentlich nachhaltig – gelöst werden konnte. Nach und nach gingen die betroffenen Einrichtungen wieder online.

BSI fordert mehr Anti-Cybercrime-Auflagen

Dass ein solcher Angriff nicht folgenlos bleiben kann, versteht sich von selbst. In den vergangenen Jahren gab es zwar immer mal wieder Hackerangriffe auf Krankenhäuser, jedoch waren hier nur einzelne Krankenhäuser betroffen, nie ein Verbund.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnte bereits im April 2019 vor gezielten Ransomware-Angriffen auf Unternehmen. Im aktuell vorliegenden Fall lobte Isabel Münch, Fachbereichsleiterin Präventive Cyber-Sicherheit und Kritische Infrastrukturen (KRITIS) beim BSI, das bedachte Vorgehen der DRK-Trägergesellschaft: Zügig seien Aufsichtsbehörden, das LKA sowie die Datenschutzbeauftragten informiert worden. Dank dem „Mobile Incident Response Team“ (MIRT) des BSI – einer Eingreiftruppe, die bei Cyberangriffen zügig unterstützt – konnte das BSI helfen, die verschlüsselten Dateien zurückzuholen. Für kritische Infrastrukturen, zu denen auch Krankenhäuser zählen, ist dieser BSI-Service kostenfrei.

Für Münch ist dieser aktuelle Anlass jedoch auch eine Gelegenheit, höhere Sicherheitsanforderungen im Gesundheitswesen durchzusetzen. Geplant ist eine Novelle des im Juli 2015 in Kraft getretenen „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz). Auch Klinikverbünde sollen demnach nachweislich den deutlich höheren Sicherheitsanforderungen nach der BSI-KRITIS-Verordnung genügen. Die BSI-KRITIS-Verordnung trat Ende Juni 2019 verbindlich für zahlreiche deutsche Krankenhäuser und Kliniken in Kraft. Betroffene Krankenhäuser sind verpflichtet, ihre IT-Infrastruktur so zu schützen, dass Angriffe auf Einzelsysteme keine Auswirkungen auf das gesamte Netzwerk haben.

Münch rät Klinik- und Praxischefs, sich professionelle Unterstützung zum Abwehren von Cyberrisiken zu suchen.

Meist gelesene Artikel

Erfolgreicher SHA-1-Angriff: jetzt Zertifikat tauschen & mit SHA-2 sicher sein

Frühjahrsputz für Mac OS Yosemite: Mac OS X 10.10 säubern, optimieren und sichern

Frühjahrsputz Apple iOS: iPhone & iPad aufräumen & absichern

---

0 Kommentar(e)

Schreibe einen Kommentar

Hinterlassen Sie uns einen Kommentar...

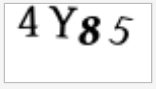
* Die DSGVO-Checkbox ist ein Pflichtfeld

* Dieses Formular speichert Name, E-Mail und Inhalt, damit wir den Überblick über auf dieser Webseite veröffentlichte Kommentare behalten. Für detaillierte Informationen, wo, wie und warum wir deine Daten speichern, wirf bitte einen Blick in unsere Datenschutzerklärung.

Ich stimme zu

E-Mail-Adresse

Name



CAPTCHA-Code

KOMMENTIEREN

NACH OBEN