Ransomware – so gefährlich ist sie für Krankenhäuser

In die IT eindringen, die Daten verschlüsseln, das System lahmlegen und für die Wiederherstellung Lösegeld verlangen. Mit diesen Methoden sind Hacker unterwegs – und erpressen leider viel Geld.

Arno Laxy, München

Was sagen aktuelle Studien zur Lage im Gesundheitswesen und was empfiehlt das Bundesamt für Sicherheit in der IT (BSI) als Schutzmaßnahmen?

In der Nacht auf den 20. Juni attackierten Hacker die Spitäler der Schweiz, offenbar ohne Geldforderungen und glücklicher Weise, ohne größeren Schaden anzurichten: Krankenhaus- bzw. Patientendaten wurden nicht kompromittiert. Das AMEOS Klinikum St. Elisabeth in Neuburg an der Donau wurde am 25. Juli angegriffen, die sofort eingeleiteten Sicherheitsmaßnahmen konnten aber offenbar Schaden abwenden. Diese zwei Meldungen aus der jüngsten Zeit zeigen, wie allgegenwärtig die Gefahr durch Hackerangriffe auf Krankenhäuser und Kliniken ist – und, dass die Gefährdung durch erpresserische Software, Ransomware, immer mit im Blick ist.

Letzteres ist nicht allzu verwunderlich, denn nur zu oft sind in den letzten Jahren Kliniken und Krankenhäuser Opfer von Cyber-Attacken geworden. Besonders tragisch war das der Fall in Düsseldorf. Eine Patientin gelangte nicht in die gesperrte Notaufnahme des Universitätsklinikums – wegen der lahmgelegten IT – und starb auf dem Weg in eine andere Notaufnahme.

Das BSI vermerkte in seinem noch aktuellen Bericht zur Lage der IT-Sicherheit 2021 einen deutlichen Anstieg cyber-krimineller Erpressungsmethoden über Ransomware. Der Verband der IT-Wirtschaft Deutschlands, bitkom pflichtete bei und ergänzte, dass „die Schäden durch Erpressung, verbunden mit dem Ausfall von Systemen oder der Störung von Betriebsabläufen, seit 2019 um 358 % gestiegen“ seien. Cyberangriffe hätten bei sage und schreibe 86 % aller Unternehmen in Deutschland zuletzt einen Schaden verursacht. Ransomware-Angriffe würden mit großer Wucht die deutsche Wirtschaft erschüttern, und zwar Betriebe aller Größen und Branchen. Die aktuellen Meldungen aus Neuburg und der Schweiz zeigen aber auch, dass sich das Gesundheitswesen im deutschsprachigen Raum wirkungsvoller gegen Ransomware und andere Cyberattacken wappnet. Diese These vertritt auch der im Juni erschienene Sonderbericht für das Gesundheitswesen der jährlich erscheinenden weltweiten Studie „The State of Ransomware 2022“ des Sicherheitssoftware-Anbieters Sophos.

Demnach seien im Gesundheitswesen Krankenhäuser, Kliniken und Co. besser auf Cyberangriffe vorbereitet. Zunächst einmal würden sich die meisten Organisationen im Gesundheitswesen dafür entscheiden, das mit solchen Attacken verbundene finanzielle Risiko durch den Abschluss einer Cyberversicherung zu verringern.

Allerdings würde es, so die Autoren des Berichts, für das Gesundheitswesen immer schwieriger, Versicherungsschutz zu erhalten, was wahrscheinlich auf die hohe Anzahl von Ransomware-Vorfällen in diesem Sektor zurückzuführen sei. Daraus resultierte eine Versicherungslücke – der Versicherungsschutz in der Branche läge bei nur 78 % verglichen mit 83 % im Durchschnitt alle Branchen. Im Ergebnis müssten viele Organisationen des Gesundheitswesens für die vollen Kosten eines Angriffs aufkommen, was die Gesamtkosten für die Beseitigung von Ransomware erhöhe.

Das Gesundheitswesen würde deswegen seine Cyberabwehr verstärken. Nicht um ohne Versicherung gegen Attacken zu bestehen, sondern, um doch noch Versicherungsschutz zu erhalten. Aber auch bei bereits versicherten Krankenhäusern und Kliniken würde die Cyberversicherung bessere Abwehrmaßnahmen gegen Hacker vorantreiben. Der Studie zufolge haben 97 % der Gesundheitsorganisationen mit Cyberversicherung ihre Abwehrmaßnahmen verbessert, um ihre Cyber-Versicherungsposition zu verbessern.

Ransomware-Angriffe fast verdoppelt

Ransomware-Angriffe auf das Gesundheitswesen haben sich, so die Studie, fast verdoppelt – 66 % der befragten Organisationen des Gesundheitswesens waren 2021 von Ransomware betroffen, gegenüber 34 % im Jahr 2020.

Ähnliche Werte zur Zahl der von Ransomware betroffenen Unternehmen nennt der Ransomware Trends Report 2020 des Speichersoftware-Anbieters Veeam. Demnach sind Unternehmen sehr oft im Hintertreffen, wenn es darum geht, sich gegen Ransomware-Angriffe zu verteidigen. 72 % der Unternehmen waren teilweise oder vollständig von Angriffen auf ihre Datensicherungsträger betroffen, was die Möglichkeit der Datenwiederherstellung ohne Zahlung des Lösegelds drastisch beeinträchtigt.

80 % der erfolgreichen Angriffe zielten auf bekannte Schwachstellen ab. Fast alle Angreifer (94 %) versuchten, die Datensicherungen unbrauchbar zu machen, um das Opfer daran zu hindern, die Daten ohne Zahlung des Lösegelds wiederherzustellen.

Schutzmaßnahmen ergreifen, Kombination von Maßnahmen

Die Brisanz der Gefahren von Ransomware-Angriffen hat das BSI im Februar 2022 dazu veranlasst, einen Maßnahmenkatalog mit den unbedingt erforderlichen präventiven Grundlagen zur Vorbereitung auf einen Ransomware-Angriff zu veröffentlichen. Adressat sind in erster Linie Unternehmen und Behörden, die sich bis jetzt noch nicht oder nur wenig mit dem Thema beschäftigt haben. Diesen präsentiert das BSI eine Übersicht ineinandergreifender Schutzmaßnahmen, die aber auf keinen Fall den IT-Grundschutz ersetzen. Als wichtigste Adhoc-Maßnahme, die sich besonders rasch realisieren lässt, nennt es die Verwendung von Backups. Die gesicherten Daten sollen nicht am Standort der Organisation vorgehalten werden, sondern außerhalb und physisch vom Netzwerk getrennt. Nur so kann gewährleistet werden, dass die Hacker die Datensicherung deaktivieren.

Gleichzeitig betont das BSI, dass nicht eine Maßnahme helfe, sondern eben die Kombination von Maßnahmen an unterschiedlichen Stellen in der IT. Zwischen der erfolgreichen Attacke auf ein IT-System und der Verschlüsselung, die erst die Erpressung ermöglicht, können Wochen bis Monate vergehen. Genügend Zeit zum Aufspüren und Stoppen der Infektion also. Das zeigen auch die eingangs genannten Beispiele der Kliniken in Neuburg an der Donau und in der Schweiz.

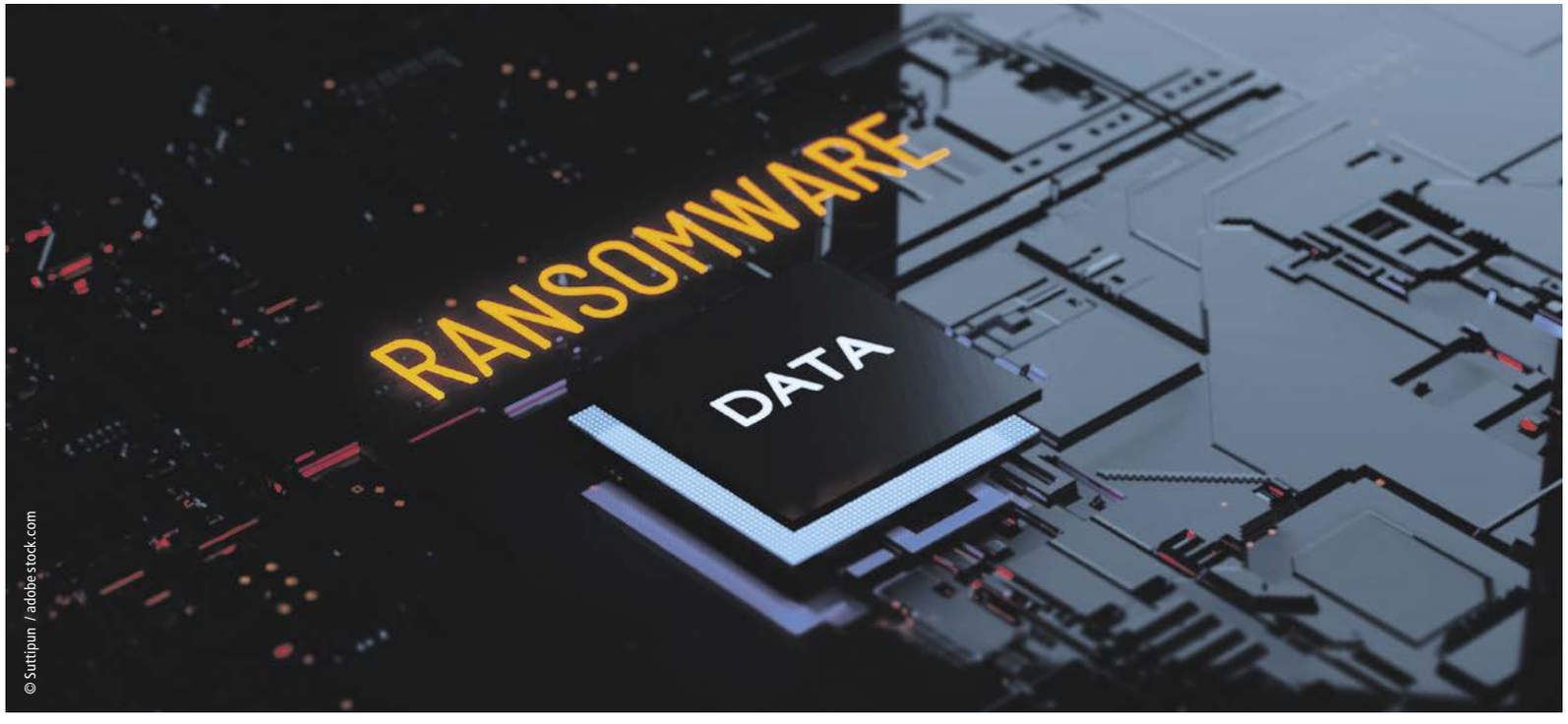
Wichtig ist ein systematisches Vorgehen, angefangen bei den schützenswerten Ressourcen, deren Identifikation und anschließender Überprüfung. Erster Anlaufpunkt sind die Einstellungen von Servern, der sichere Umgang mit E-Mails sowie der Aufbau eines aktiven Schwachstellenmanagements. Dieses regelt, dass nur notwendige Dienste und Ports freigegeben werden, Fernzugriffe nur abgesichert erfolgen können, Netzwerke segmentiert und Anwendungen auf ungewöhnliche Aktivitäten hin kontrolliert werden.

Am Arbeitsplatzrechner empfehlen die BSI-Experten u.a. regelmäßige und rasche Software-Updates, lassen sich doch so Sicherheitslücken effektiv und ohne viel Aufwand schließen. Zu den weiteren Maßnahmen gehören Klassiker wie Virenschutz, Deaktivieren von Makros und Scriptings sowie die richtige Handhabung von E-Mails. Die Anleitung fußt auf den praktischen Erfahrungen der BSI-Mitarbeiter, was auch die Tabelle am Ende des Maßnahmenkatalogs zeigt. Sie bewertet die Maßnahmen nach deren Nutzen-Aufwand-Verhältnis und weist mit der Kategorie „Quick-Wins“ auf kurzfristig besonders hilfreiche Aktionen hin. Damit leistet der Katalog genau das, was leider immer noch viel zu oft benötigt wird: schnell umsetzbare Praxistipps zum Schutz von Ransomware bereitstellen.

Ganzheitliches Sicherheitskonzept

Diese Schutzmaßnahmen sind, und das soll hier nochmals betont werden, nur ein Teil eines ganzheitlichen Sicherheitskonzepts für Krankenhäuser. Dessen Kern ist die Informationssicherheit wie es das IT-Sicherheitsgesetz 2.0 verpflichtend für alle Krankenhäuser verlangt. Mit nach dem Stand der Technik angemessenen organisatorischen und technischen Vorkehrungen der IT-Sicherheit sollen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit verhindert werden.

Patientensicherheit und Behandlungseffektivität stehen dabei genauso im Fokus wie informationstechnische Systeme, Komponenten oder Prozesse. Zusammen haben sie eine zentrale Bedeutung für den ordnungsgemäßen Betrieb des Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen. ■



© Suttipun / adobe stock.com