Rechtzeitig die Daten schützen

Internetviren und was Praxen und Labore dagegen tun können

MICHAEL DALETZKI

Das Szenario

Montag morgen, Sie kommen in die Praxis oder in Ihr Labor, schalten Ihren Rechner ein und stellen ein merkwürdiges Verhalten des PCs fest: Auf dem Bildschirm erscheint ein Totenkopf und der Text auf dem Bildschirm weist darauf hin, dass Sie Geld überweisen sollen. Sie gehen mit einem flauen Gefühl an den nächsten Computer, dieser lässt sich einwandfrei starten. Erleichterung breitet sich aus. Es klingelt das Telefon, eine Praxis ruft an und fragt nach dem Status einer Terminarbeit oder ein Patient nach einem Termin. Sie starten das entsprechende Programm, um den Status zu prüfen. Es kommt eine Fehlermeldung auf den Bildschirm und die Software lässt sich nicht starten. Sie merken nun sehr schnell, dass es sich scheinbar um ein globales Problem in Ihrem Netzwerk handelt. Sie rufen Ihren IT-Administrator an. Dieser verspricht, sich auf Ihrem Computer einzuloggen oder aber zu Ihnen ins Labor oder in die Praxis zu kommen.

Es vergehen zwei bis drei Stunden, bis die Analyse des IT-lers feststeht: Ein Verschlüsselungsvirus – Ransomware (von englisch ransom: Lösegeld) – hat Ihre IT-Struktur befallen. Die Telefone in der Praxis oder im Labor klingeln weiterhin. Praxen oder Patienten möchten mit Ihnen Ihr Anliegen klären, Sie können jedoch keine Auskunft geben, nichts funktioniert mehr. Der Labor- oder Praxisbetrieb kommt schnell zum Stillstand. Nach Rücksprache mit den IT-Spezialisten wird schnell klar, dass die Computer neu installiert werden müssen und der gesamte Datenbestand aus der Datensicherung wiederhergestellt werden muss. Eine Katastrophe bahnt sich an.

Wenn die Praxis oder das Labor gut aufgestellt ist, sollte das IT-Netzwerk in den nächsten 24 Stunden wieder einsatzbereit sein. Zur Erinnerung: Es ist be-

stimmt schon Mittag oder früher Nachmitttag. Dies bedeutet schon zu diesem Zeitpunkt einen Ausfall von fast zwei Tagen. Der IT-ler macht sich an die Arbeit und möchte alle Datenbestände aus der Datensicherung wieder zurückspielen. Plötzlich stellt er fest, dass auch die Datensicherung von der Verschlüsselung betroffen ist. Der Virus ist übergesprungen auf die Datensicherungshardware und auch diese Daten sind nicht mehr verwendbar. An dieser Stelle ist zu hoffen, dass noch mindestens fünf externe Festplatten oder Bänder vorhanden sind, auf denen alle Datenbestände gesichert wurden.

So oder so ähnlich passiert es in Deutschland jeden Tag in vielen Hundert Unternehmen, Laboren und Praxen. Es handelt sich um einen Virus, der häufig mit dem Begriff Ransomware bezeichnet wird und den es in sehr vielen Varianten gibt. Ransomware ist eine Schlüsselbedrohung für die Unternehmenssicherheit.

Indien weist dabei mit 67 Prozent den höchsten Infektionsgrad auf. Es folgen Mexiko (65 Prozent) und die USA (60 Prozent). Deutschland rangiert auf Platz 6 mit 51 Prozent. Japan bildet das Schlusslicht mit 41 Prozent. Unternehmen zahlen einen hohen Preis für die Ransomware-Angriffe: Im Durchschnitt beliefen sich die Schadenskosten auf rund 107.000 Euro pro Ransomware-Befall. Falls die Datensicherung nicht mit der notwendigen Sorgfalt stattgefunden hat, steht die Existenzgrundlage auf dem Spiel.

Daten mehrfach sichern

Es stellt sich also die Frage, wie man seine Datenbestände vor dieser Situation schützen kann. Ein kleiner Hinweis an dieser Stelle: Laut DSGVO besteht die Verpflichtung, die Datenbestände zu schützen, insbesondere wenn es sich um Patientendaten handelt.

Das bedeutet, dass Sie im Nachgang auch noch mit Strafen rechnen müssen, falls die Sorgfaltspflicht im Umgang mit Datenbeständen verletzt wurde. Es wird viel Prophylaxe im Bereich Feuer betrieben, mit Feuermeldern und einer Feuerversicherung, viele Praxen und Labore sind auch gegen Einbruch versichert. Die Kosten belaufen sich jährlich auf viele Hundert Euro. Die Fragestellung lautet aber an dieser Stelle: Was wird gegen Datenverlust unternommen? Die Gegenmaßnahmen hierfür sind der Brandschutz des 21sten Jahrhunderts.

Leider gibt es, ums dies vorwegzunehmen, keinen 100-prozentigen Schutz gegen die Bedrohung aus dem Internet.

Der Schutz, den es aufzubauen gilt, besteht aus mehreren Teilen. An der ersten Stelle steht die Datensicherung. Eine Datensicherung, die fachmännisch aufgesetzt ist, versetzt den Netzwerkbetreiber (Praxisinhaber bzw. Laborinhaber) in die Lage, innerhalb von maximal 24 Stunden wieder voll arbeitsfähig zu sein. Leider sind die aktuellen Viren inzwischen so intelligent, dass auch Datensicherungsbestände mit verschlüsselt werden, sofern im Netzwerk online, wie z. B. auf einem NAS System. Die Zeiten sind definitiv vorbei, in denen einfach nur die Daten auf einen anderen Datenspeicher kopiert wurden. Die Datensicherung muss so ausgeführt werden, dass sie mehrfach vorhanden ist. Gesichert wird mit einer speziellen Sicherungssoftware, die Daten in der Nacht als Vollsicherung auf einen Datenspeicher im Netzwerk speichert und dann am Tag auf einen externen Datenträger, der jeden Tag ausgetauscht wird. Es sollten mindestens fünf Tagesdatenträger vorhanden sein, außerdem vier Wochensicherungen, die zyklisch getauscht werden. Gespeichert wird verschlüsselt. Die Datensicherung sollte jeden Tag eine Mail zusenden, die auch kontrolliert wird. In dieser Mail steht, ob die Datensicherung funktioniert hat oder nicht. Die externen Datenträger gehören definitiv außer Haus, neben Ihrem Serversystem nutzen sie beispielsweise bei einem Brand nichts mehr. Einmal im Quartal spielt man testweise einigen Daten zurück, um die Restore(Wiederherstellungs)-Funktion sicherzustellen. Das kostet Ihren Systemadministrator vielleicht 30 Minuten Aufwand, der Netzwerkbetreiber hat dafür ein sicheres Gefühl und kann ruhig schlafen.

Wie Rechner geschützt werden

Rechner werden häufig über E-Mails mit Ransomware infiziert. Der gefährliche Inhalt ist ihnen nicht anzusehen, oft sind es hervorragend angefertigte Bewerbungsmails. Auch Datenbestände vom Arbeitsamt werden mit einbezogen, um die Bewerbungsmails an den richtigen Empfänger zu bringen.

Bevor eine E-Mail im Labor oder der Praxis ankommen darf, sollte sie mit dem Verfahren der zwei „Türsteher" auf Spam und Viren geprüft werden. Der erste Türsteher prüft, ob die E-Mail Spam ist. Wenn diese Hürde genommen wurde, prüft der zweite Türsteher, ob in der E-Mail ein Virus enthalten ist. Es sollte vermieden werden, dass Mails sofort in das Netzwerk gelangen und dann erst auf schadhafte Software geprüft werden. Besser ist, vorab zu untersuchen, ob alles sauber ist, so bleibt die „Pest" im Internet und erreicht nicht den Labor- oder Praxiscomputer. Postfächer mit E-Mails können mit wenigen Handgriffen z. B. auf ein Hosted Exchange Postfach umgewandelt werden. Das ist allerdings nicht kostenlos, sondern die Dienstleister berechnen ab fünf Euro pro Monat. Gut investiertes Geld.

Ein weiterer Schwachpunkt in vielen Netzwerken ist das Intenet-Gateway, der Router. Oft gibt es bei der Hardware, z. B. Fritzbox oder Telekom-Geräten, bei Vertragsabschluss ein Speedport als Router mit dazu. Die Geräte verfügen über keine ausreichende Schutzfunktion. Wenn eine Fritzbox oder ein Speed Port in Betrieb genommen wird, können alle angeschlossenen PCs ins Internet, weil es keine Beschränkung dafür gibt.

Moderne Firewall-Systeme stellen die Verbindung zum Internet her, aber es kommt noch niemand aus dem Netzwerk in das Internet. Der Zugriff muss explizit erlauben werden. Nur dadurch erhält man den Überblick, was in dem jeweiligen Netzwerk passiert. Mit solchen Systemen kann auch bestimmt werden, welche Internetseiten verfügbar sein sollen. Ein Beispiel hierfür wäre, dass niemand auf die Seite von Amazon und Zalando zugreifen kann, außer der PC des Geschäftsführers.

Firewall-Systeme prüfen zusätzlich den gesamten Datenverkehr und schalten im Notfall bei fragwürdigem Verhalten der Rechner im Netzwerk die Zugriffe automatisiert ab. Die Kosten einer solchen Firewall sind natürlich höher als die einer Fritzbox.

Auf einen Virenscanner sollte ebenfalls nicht verzichtet werden. In einem Netzwerk muss ein Virenscanner installiert sein, der von einem Server verwaltet wird. Es handelt sich um Businesslösungen und nicht um freie Produkte, die vielleicht auch noch in bestimmten Intervallen Werbung einblenden. Gute Virenscanner haben ein Deep Learning System, ein selbst lernendes System, um neue Angriffe aus dem Internet abzuwehren. Ein Reporting und eine E-Mail-Benachrichtigung ist hierbei selbstverständlich.

Es ist enorm wichtig, dass die Rechnersysteme aktuell sind. Windows XP-Rechner und bald auch Windows 7-Systeme (Support läuft im Januar 2020 aus) gehören nicht mehr in ein Netzwerk, in dem Patientendaten verarbeitet werden. Es sollten alle Updates von Microsoft eingelesen werden, um dadurch wichtige Sicherheitslücken zu schließen. Zusatzsoftware, wie z. B. Java und Adobe Reader-Produkte müssen ebenfalls auf dem aktuellen Stand gehalten werden.

Eine sehr große Schwachstelle in jedem Netzwerk, egal ob nur ein PC oder 20 PCs, ist der Mensch. Viele Mitarbeiter in einem Labor oder in einer Praxis wissen nicht, worauf sie achten müssen, damit keine Viren in das Netzwerk einfallen. Eine Schulung der Mitarbeiter vor Ort ist eine hervorragende Prävention gegen ungewollten Virenbefall. Sie kann mit einer Datenschutzschulung kombiniert werden und nimmt ca. vier Stunden in Anspruch.

Da die Gefahr, die von den Internetviren ausgeht, groß ist, sind neue Versicherungsformen stark im Kommen. Cyber Security Policen werden inzwischen von vielen Gesellschaften angeboten. Die Beiträge der Versicherer richten sich natürlich nach dem bestehenden Risiko. Wenn also die oben genannten Punkte beachtet worden sind, wird der Beitrag sicher geringer ausfallen als wenn ein Netzwerk versichert werden muss, das nicht ausreichend geschützt ist. Einen sehr guten Ansatz für die Unternehmenssicherheit bietet die VDS 10000.

Fazit

IT-Sicherheit besteht aus vielen Bausteinen, die ineinander greifen. Verschlüsselungsviren können die Existenzgrundlage gefährden, wenn nicht ausreichend Prävention betrieben wird. IT-Sicherheit gehört in fachmännische Hände und kann nicht nebenbei erledigt werden. Einen 100-prozentigen Schutz gibt es jedoch leider nicht.

Michael Daletzki
medianetX GmbH
Spreckenburgstraße 10
32760 Detmold
E-Mail: m.daletzki@medianetx.de