„Das was ich durchgemacht habe, wünsche ich niemandem!“

Dr. Michael Kann

Ich bin niedergelassener Zahnarzt in Wiesbaden. Ende vergangenen Jahres ist mir der Super-GAU passiert: Mein Praxiscomputer wurde gehackt, alle Patienten- und Abrechnungsdaten waren mit einem Mal weg. Ich wurde erpresst.

Foto: OPTI-Zahnarztberatung

„Es war ein Alptraum: Meine Praxis lag brach, ich konnte nicht arbeiten, hatte Verdienstausfälle und Kosten in noch unbekannter Höhe und wurde erpresst.“

Im Juli 2017 habe ich im Stadtteil Biebrich eine Praxis übernommen, die seit 1977 existiert. Das zahnärztliche Team besteht aus vier Behandlern, darunter ein Fachzahnarzt für Oralchirurgie und ein Spezialist für Endodontie. Wir haben 1.000 Scheine im Quartal und decken das gesamte Spektrum der Zahnheilkunde ab.

Die Praxis-Software ist gekapert!

Als ich Anfang November eines Morgens in meine Praxis kam, liefen meine Mitarbeiterinnen aufgeregt auf mich zu: „Die Praxis-Software ist weg!“ Die Software kann ja nicht einfach verschwunden sein, denkt man sich, doch in der Tat entpuppten sich sämtliche Verknüpfungen als weiße Dateien, mit der Endung „.arena“ – sinnlose Dateien im Grunde. Was für ein Schock!

Ein Blick auf den Praxisserver bestätigte die Befürchtung: Restlos alle Dateien endeten auf .arena. Darüber hinaus fand ich aber auch zusätzliche, lesbare Textdateien, die es vorher nicht gab. Darin stand, dass alle meine Daten verschlüsselt worden seien und dass ich eine E-Mail an eine bestimmte Adresse schreiben müsse, um die Lösegeldforderung entgegenzunehmen.

Was tun? Am Ende habe ich diese E-Mail geschrieben. Via Google fand ich später heraus, dass es sich um eine Ransomware

Foto: arrow - Fotolia.com

handelt, die den Praxis-Computer infiziert hatte. Der Verschlüsselungscode dieser Schadsoftware ist auf militärischem Sicherheitsniveau angesiedelt, was bedeutet, dass keinerlei Sicherheitsmängel bekannt sind. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigte auf Nachfrage diese Information: Es gibt keine bekannten Schwächen. Das heißt, ohne aktuelles Back-up kann man die Daten nur mit dem Schlüssel wiederherstellen – und den hat nur der Hacker.

Es stellte sich heraus, dass diese Angriffsvariante vornehmlich über den Fernzugang des Servers erfolgt. Die Attacke ist demnach über einen langen Zeitraum gelaufen: Über Monate hatten die Hacker Benutzernamen und Passwörter ausprobiert, bis sie irgendwann die richtige Kombination herausgefunden haben. Was für ein Wahnsinn. Diese Angriffe tauchen zwar in den Serverprotokollen auf, aber mal ehrlich: Schauen Sie da regelmäßig rein?

Das Erste, was ich tat, war: den Fernzugang zu schließen. Außerdem schaltete ich das BSI ein und rief die Kriminalpolizei an – Datendiebstahl ist ja ein Fall von Wirtschaftskriminalität. Dabei wird man von den Beamten durchaus mit Hinweisen und Tipps unterstützt, aber letzten Endes wird eben – auch für die Versicherung – nur eine Strafanzeige gegen Unbekannt gestellt.

Der kurze Weg vom Opfer zum Täter

Meine Praxis lag brach, ich konnte nicht arbeiten, hatte Verdienstausfälle und Kosten in noch unbekannter Höhe und wurde erpresst. Ich war der Geschädigte, sollte man meinen. Doch weit gefehlt. Denn es geht um Patientendaten. Und die Frage ist: Hatte ich alles getan, um diese sensiblen Daten sorgfältig und gewissenhaft zu sichern? Glauben Sie mir: Vom Opfer wird man sehr schnell zum Täter. Das gilt auch dann, wenn man aus Unkenntnis versäumt, die entsprechenden Behörden zu informieren und alle Patienten wie auch betroffene Dritte über die Vorfälle zu unterrichten.

Das BSI zeigte sich übrigens sehr interessiert, denn je nachdem, um was für eine Variante es sich bei der Ransomware handelt, gibt es durchaus Möglichkeiten, die Daten wieder zu entschlüsseln. Die Erpressungssoftware auf meinem Rechner war, als das passierte, allerdings noch keine zwei Monate auf dem Markt und damit recht neu.

Keine Chance also.

Die nächste Sofortmaßnahme war extrem wichtig: das Internet trennen. Ich zog den Server vom Internet ab, fuhr ihn komplett herunter und schaltete ihn nicht mehr an.

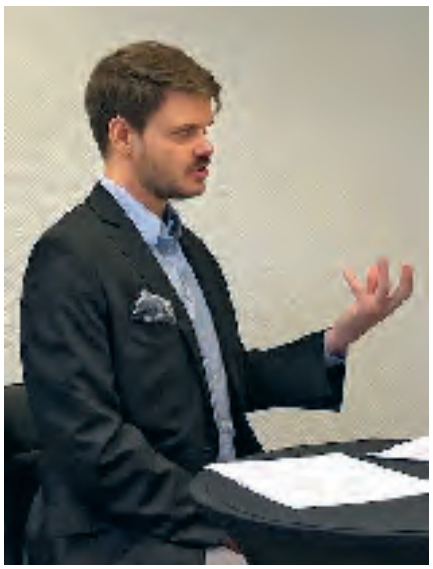

Foto: OPTI-Zahnarztberatung

„Die Frage ist: Hatte ich alles getan, um diese sensiblen Daten sorgfältig und gewissenhaft zu sichern? Glauben Sie mir: Vom Opfer wird man sehr schnell zum Täter."

Womöglich ließen sich aus den Resten noch Dateien retten. Und umgekehrt galt: Je länger ich den Server noch benutze, desto mehr laufe ich Gefahr, diese Daten auch noch zu verlieren. Letztlich kann eine professionelle Firma zur Datenrettung umso mehr Daten wiederherstellen, je schneller man den Server außer Betrieb setzt.
Zu dem Zeitpunkt war ich mir aber gar nicht sicher, ob die Daten überhaupt zurückgewonnen werden können – sprich: ob meine Back-ups funktionieren.

Die Lösegeldforderung trifft ein

Dann erhielt ich eine Lösegeldforderung: Ich sollte einen halben Bitcoin zahlen, ein halber Bitcoin war damals zwischen 4.200 und 4.300 Euro wert.
Das erste Problem, wenn man mit Bitcoins bezahlen will: Man hat üblicherweise kein Bitcoin-Konto, auf dem zufälligerweise gerade auch noch ein halber Bitcoin liegt. Die Einrichtuung eines derartigen Kontos inklusive Überweisung der entsprechenden Summe kann bis zu einer Woche dauern. Ich hatte eine Frist von 48 Stunden ... Ansonsten würde sich die Summe auf einen ganzen Bitcoin erhöhen. Was man in dieser Situation durchmacht, wünsche ich niemandem.
Am Ende hatte ich Glück. Über zig Ecken konnte ich Bekannte auftun, die ein Bitcoin-Konto besaßen. Innerhalb von zwölf Stunden war das Geld schließlich überwiesen.

Der drohende Schaden wäre eine Katastrophe gewesen

Der drohende Umsatzschaden, der hier im Raum stand – immerhin fehlten zu diesem Zeitpunkt nicht abgerechnete Daten aus anderthalb Monaten –, wäre eine absolute Katastrophe für mich gewesen. Wie hätte ich diese Daten – 1.000 Scheine pro Quartal – wieder rekonstruieren können? Also zahlt man erstmal. Und wartet auf die Rückmeldung.
In meinem Fall erhielt ich, nachdem der halbe Bitcoin eingegangen war, wieder per E-Mail ein kleines Programm. Da es ja gut möglich war, dass dieses Programm auch wieder einen Virus enthält, habe ich mir für die Sichtung Hilfe gesucht: Profis arbeiten in diesen Fällen mit virtuellen Maschinen, die man sich wie abgesicherte Sandkisten vorstellen muss, in denen man die Programme öffnet und ein damit eventuell freigesetzter Virus gefangen bleibt. In dieser Umgebung befand sich quasi ein virtuelles Abbild meines Servers. Das Programm hat nun dieses Abbild gescannt und daraus die Schlüssel erzeugt, die ich per E-Mail an den Hacker zurückschicken sollte, der aus diesen Daten wiederum den Entschlüsselungsschlüssel errechnet. Genau das hat mein Erpresser aber nicht getan. Stattdessen teilte er mir mit, er habe anhand dieser Schlüssel erkannt, dass ich noch weitere Rechner besitze und verlange darum noch ein weiteres halbes Bitcoin. Sowohl die Kripo als auch das BSI rieten mir dringend davon ab, dieser Forderung nachzukommen. Und zwar, um die Nachahmung möglichst unattraktiv zu gestalten.

Foto: OPTI-Zahnarztberatung

„Am Ende hatte ich Glück, denn man konnte aus den vorhandenen Back-ups alle Daten wiederherstellen."

Diese Programme scannen das gesamte Internet

Dabei muss man wissen: Die Programme, die den Weg in interne Netze öffnen, laufen vollautomatisch. Sie scannen das gesamte Internet nach offenen Fernzugangsports und wenn sie eine solche Adresse gefunden haben, werden diese Angriffe ebenfalls vollautomatisch durchgeführt.
Man darf sich das keinesfalls so vorstellen, dass hier jemand schräg gegenüber in einer Wohnung gesessen und überlegt hat: „Knacke ich jetzt diese Praxis?" Nein, dass ich und meine Praxis Opfer eines solchen Angriffs wurden, ist purer Zufall. Es hätte auch die Unternehmerin XY oder die Firma YZ treffen können. Das sind keine Hacker mit nerdigen Computerkenntnissen! Im Gegenteil, im Grunde kann jeder Teenager mit seinem PC derartige Angriffe starten, die entsprechende Software besorgen sich die Hacker im Darknet. Früher hat man Daten gestohlen und die Besitzer erpresst. Das war für den Verbrecher mit einem hohen Risiko verbunden, weil er sich für solche Erpressungen ja sichtbar machen musste. Heute dagegen ist es so, dass der Inhalt der Beute den Hacker gar nicht interessiert. Er verschlüsselt einfach nur die Daten ohne sie je gesehen zu haben. Die Methode funktioniert, weil die Daten für den Besitzer einen Wert haben. Diese Geschichte hat mich unendlich viel Nerven gekostet. Glücklicherweise konnte man aus den vorhandenen Back-ups alle Daten wiederherstellen. Die Nachforderung habe ich nämlich nicht mehr beglichen. ■