„Cyberkriminalität bleibt eine Dauerbedrohung“

Die Digitalisierung des Gesundheitswesens macht die beteiligten Systeme auch anfälliger für Cyberkriminalität. Wie die Angreifer vorgehen, was im Falle eines Angriffs zu tun ist und welche Präventionsmöglichkeiten es gibt, erklärt Lars Huwald, Cybercrime-Ermittler im Landeskriminalamt Berlin, in einem Interview mit praxisnah.

Foto: Lars Huwald, privat

Herr Huwald, in Ihrem Vortrag zum SpiFa-Tag 2022 war Ihre Aussage deutlich: Die Frage ist nicht, ob, sondern wann Sie angegriffen werden. – Wie oft sind Arzt- und Zahnarztpraxen seither von Cyberattacken betroffen?

Lars Huwald: Eigentlich ständig. Arzt- und Zahnarztpraxen oder Kliniken betreiben IT-Systeme und verwenden technische Schnittstellen. Damit sind sie per se angreifbar. Die Täter greifen ungezielt über Sicherheitslücken und Schadsoftware an. Sie schießen mit der großen Schrotflinte quer durchs Internet und schauen dann, wen sie getroffen haben. Das heißt, Arztpraxen sind nicht sicherer oder unsicherer als andere.

Wer sind die Angreifer?

Die Hauptangreifer, die uns am meisten beschäftigen, sind professionelle Akteure mit Angestellten. Die sitzen nicht mehr in einer Garage, sondern in richtigen Firmengebäuden. Ihr Ziel ist es, Geld zu verdienen, Lösegeld für die Daten, die verschlüsselt wurden.

Daneben gibt es noch ein paar Anfänger, die versuchen, sich auf dem Markt zu etablieren. Eine dritte Gruppe ist ein sehr spezielles Level von staatlichen Akteuren, die auf Sabotage aus sind. Hier entstehen eher Kollateralschäden – wenn zum Beispiel eine Klinik ausfällt – aber das ist sehr selten.

Hat sich in den vergangenen Jahren bei den Angriffen etwas geändert?

Ja, jetzt werden immer mehr Daten heruntergeladen und ins Internet gestellt – sensible Daten aller Art. Die Täter wollen zeigen, was sie können und sie erpressen damit gleich doppelt: Sie fordern Lösegeld für die Entschlüsselung von Daten und drohen, die Daten weiterzuverkaufen. Und: Mit den veröffentlichten Daten kommt noch ein weiterer Schaden, nämlich der Verstoß gegen den Datenschutz, hinzu.

Wie gehen die Angreifer vor?

Die Angriffe finden auf zwei verschiedene Arten statt:

Eher selten, aber sehr kritisch, ist der sogenannte Supply-Chain-Angriff – oder auch Angriff auf die Wertschöpfungskette. Wenn es ein Täter schafft, eine Software-Firma oder deren Produkte anzugreifen, dann haben die Kunden, also die Praxen, den Angriff schon mit eingekauft. Um das zu verhindern, müssen die Systeme immer aktuell gehalten werden, auch wenn es manchmal lästig wird, ein System für zwei Stunden mehrmals herunterzufahren.

Die weitaus häufigere Art ist das Versenden von E-Mails mit einem Anhang oder einem Link. Im Bereich der professionellen Täter sind diese sehr gut gestaltet. Sie scheinen sich nahtlos in eine bestehende Kommunikation einzubinden oder tarnen sich als Newsletter von einer beruflich relevanten Vereinigung.

Die E-Mails sind so gut gemacht, dass man auch wirklich draufklicken kann. Das passiert gerade im hektischen Praxisalltag. In der Folge wird eine Schadsoftware aktiv, die sich herunterlädt, sich installiert, in der Regel alles unbemerkt, und die anfängt zu wirken.

Die Betroffenen merken also gar nichts?

Sie könnten merken, dass etwas nicht wie erwartet funktioniert. Etwa eine Rechnung, die sich nicht öffnet, oder ein Newsletter, der zu einer unbekannten Website führt, die dann wieder verschwindet. Das wären Hinweise, die auch ein Bauchgefühl sein könnten.

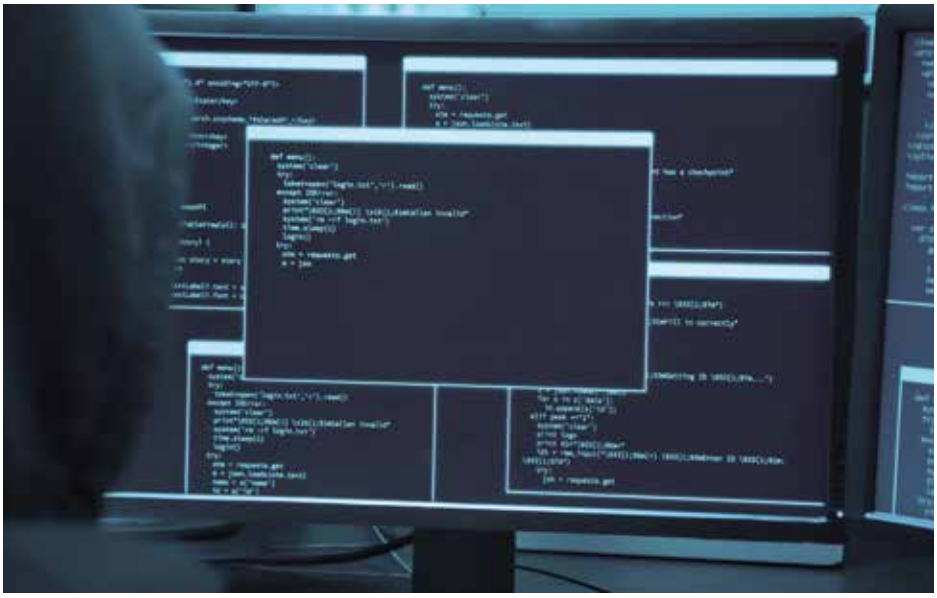
Nehmen wir an: Ich merke schnell, es funktioniert nicht, wie erwartet. Was ist dann zu tun?

Sofort den IT-Dienstleister einschalten. Der kann prüfen, ob es wirklich ein Angriff war. Er kann die Systeme offline schalten, neu aufsetzen und es ist in kurzer Zeit erledigt.

Unser Tipp lautet allerdings: Gehen Sie schon präventiv mit dem IT-Dienstleister in medias res. Besprechen Sie, wie schnell er im Falle eines Angriffs reagieren würde und was er dafür braucht.

Es hat sich bezahlt gemacht, wenn der Dienstleister in der Lage ist, auch nur bei einer Verdachtsmeldung prompt zu prüfen, ohne ein großes Ticket aufzumachen.

Bei Arztpraxen ist die gematik-Infrastruktur eine besondere Thematik. Ob der



Dienstleister an diese Blackbox rangeht, ist nicht geklärt. Er muss aber auf jeden Fall möglichst unbürokratisch loslegen können.

Also eher einmal zu viel Alarm schlagen?

Vor allem, ohne dass die Mitarbeiter Angst vor Konsequenzen haben, wenn sie etwas melden. Etwa, weil das mit Kosten verbunden ist oder weil der Chef davor warnt. Die MFA sitzen an der Front und wenn die Angst haben, es zu melden, dann melden sie es nicht.

Sie sollten eher ermutigt werden, Alarm zu schlagen – wenn der Rechner laut wird, der Lüfter sich schnell dreht, wenn die Rechnung nicht aufgeht oder ähnliches. Dass sie einen Verdacht bzw. Vorfall gemeldet haben, muss ein wunderbarer Prozess sein, wo sich alle bedanken. Lieber zehn Fehlmeldungen am Tag als dass ein Angriff durchschlägt.

Was passiert, wenn ein Angriff erfolgreich ist?

Es gibt Schadsoftware, die innerhalb von 25 Minuten ganze IT-Systeme verschlüsselt, es gibt andere, die zwei, drei Wochen bis Monate braucht. Zuerst kommt die Schadsoftware auf einen Rechner, der hauptsächlich für E-Mails verwendet wird. Die Software will aber kritische Daten angreifen, die in der Regel nicht auf diesem PC sind, sondern in einem geschützteren System. Die Software muss sich durch die IT-Landschaft durchhangeln. Dafür hat sie ein Repertoire, mit dem sie kreativ arbeiten kann. Deshalb ist der Zeitraum auch hochgradig variabel – je nachdem, wie gut und wie automatisiert die Software ist. Sie verschafft sich nach und nach mehr Rechte. Das nennen wir „Privilege Eskalation". Außerdem geht sie quer durch die ganze IT-Landschaft, bis sie die kritischen Sachen erreicht, die für die Täter relevant sein können. Während sich die Software verbreitet, werden die Daten heruntergeladen und dann – am Ende der täterseitigen Aktivitäten auf den IT-Systemen – verschlüsselt. Sie sehen dann nur noch die Lösegeldforderung.

Und was ist dann zu tun?

Dann ist das Kind im Brunnen. Sie müssen aber trotzdem sofort den IT-Dienstleister informieren, damit der schauen kann, welche Systeme betroffen sind und prüfen, ob noch eine Datensicherung existiert, sodass das System neu aufgebaut werden kann. Der Dienstleister muss zudem prüfen, ob die Datensicherung auch betroffen ist.

Der zweite Schritt wäre, uns – die ZAC – ins Boot zu holen. Wir nutzen unser Wissen über die Täter und haben manchmal die Möglichkeit der Entschlüsselung. Vor allem aber sind wir der kühle Kopf. Wir helfen unbürokratisch, ohne eigene finanzielle Interessen und nicht mit Blaulicht. Wenn wir angerufen werden, können wir gut einschätzen, ob es sich um einen Angriff handelt, und eine Anzeige in die Wege leiten.

Wir haben auch so wichtige Tipps wie, den Datenschutzbeauftragten des Landes zu informieren. Denn wenn personenbezogene Daten betroffen sein könnten, haben Sie für die Erstmeldung nach Bekanntwerden eines mutmaßlichen Hackerangriffs und der Kompromittierung personenbezogener Daten exakt 72 Stunden Zeit. Danach sind die Bußgelder drakonisch. Solche vermeintlichen Kleinigkeiten können schnell untergehen.

Oft kommt der Gedanke, dass es betriebswirtschaftlich günstiger sei, den Täter zu bezahlen, als alles wieder teuer aufzubauen. Davon raten wir grundsätzlich ab. Denn erstens unterstützen wir als Polizei die Täter nicht. Und zweitens: Es ist niemals eine schnelle Lösung. Das Lösegeld muss in einer kuriosen Kryptowährung bezahlt werden, die in der Regel nicht vorgehalten wird. Und: Die Täter liefern die Daten nicht auf einem Silbertablett, sondern eine Software, mit der die Betroffenen die Daten selbst entschlüsseln müssen. Das kann sich über Wochen hinziehen.

Kurz: Die Täter zu bezahlen ist möglich, wenn es die Ultima Ratio ist. Es ist nicht strafbar. Aber ist ein sehr aufwendiger Weg.

Wie können sich Praxen vor solchen Angriffen schützen und welche Rolle spielt die Telematik-Infrastruktur der gematik?

Hier haben wir eine schwierige Gemengelage: Die Praxen haben die eigenen IT-Systeme, die in der Regel der Dienstleister betreibt. Und dann gibt es den Konnektor, den die gematik betreibt bzw. bereitstellt. Auf diese Teile haben die Praxen keinen Einfluss. Das heißt, bei einem Verdacht auf einen Angriff, muss dieser auch der gematik gemeldet werden.

ZAC

- ZAC sind die Zentrale Ansprechstellen Cybercrime der Polizei für Unternehmen, Behörden und sonstige Institutionen
- Sie gibt es in jedem Bundesland
- Kontakt: https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html

Angriffspunkt Nr. 1 bleibt jedoch der Faktor Mensch. Wir empfehlen deshalb zum einen eine Kultur, in der das Personal keine Angst hat, einen Fehler oder einen falschen Klick zu melden, und zum anderen einen Meldeweg, der funktioniert.

Ein weiteres Thema sind die Rechte- und Rollen-Konzepte. Wenn jeder Rechner im Netzwerk mit allen anderen verbunden ist, dann ist das der perfekte Weg für die Schadsoftware.

Wenn ein Rechner aber nur für E-Mails und vielleicht das Terminmanagement zuständig ist und nicht auf die Patientendaten zugreifen kann, dann haben Sie eine gute Abschottung. Das wirkt archaisch und das Segmentieren geht mit weniger Komfort einher, aber es macht die Daten sicherer. Genauso gilt es, Benutzerkonten und Zugriffsrechte zu definieren. Das geschieht in Absprache mit dem IT-Dienstleister.

Das Gleiche gilt für die Datensicherung. Vollautomatische Systeme sind auch vollautomatisiert angreifbar. Die Schadsoftware schlägt dann los, wenn die Datensicherung beginnt. Wenn man dagegen händisch jeden Freitag eine Festplatte anschließt und über ein kleines Skript die Daten sichert, die Festplatte mit nach Hause nimmt und in der nächsten Woche eine andere nutzt, die jemand anders mit nach Hause nimmt, dann ist das sehr sicher – auch im Brandfalle. In der Praxis ist eine Mischung aus häufigen Sicherungen (der täglich veränderten Daten) und selteneren Komplettsicherungen ein guter Ansatz.

IT-Dienstleister spielen eine wichtige Rolle. Aber wer ist gut?

Das werden wir auch des Öfteren gefragt. Wir dürfen aber keine Empfehlung geben und wir wissen es auch nicht. Es gibt keinen Standard, den man nachlesen kann. Man kann als Kunde aber einen Krisenfall durchsprechen und fragen: Wie schnell und wie reagieren Sie? Wir haben schon kleine IT-Teams erlebt, die in einer Klinik unfassbar gut reagiert haben, besser als große.

Welche Tipps geben Sie den Praxisteams?

Gemeinsam mit dem Dienstleister muss der Praxisinhaber oder die Praxisinhaberin den Meldeweg abklären: Wie ist bei einem Sicherheitsvorfall zu reagieren und wie schnell sind die IT-Experten erreichbar? Die Vorgehensweise muss den MFA bekannt sein und in Teambesprechungen thematisiert werden.

Es ist schwer, die Sensibilisierung immer aufrechtzuerhalten. Aber Cyberkriminalität bleibt eine Dauerbedrohung. Sie können sich nicht freikaufen, indem Sie eine dicke Software kaufen und dann sicher sind. Die Angreifer finden immer wieder neue Maschen. Es gehört einfach zur technischen Welt, dass IT-Systeme angreifbar sind und dass da keiner schuld ist.

Zu wissen, wenn etwas passiert, dann haben wir einen Meldeweg, der nichts extra kostet, der nicht aufwendig ist – das ist die allerwichtigste Maßnahme. Durch schnelle und gute Reaktion können Angriffe am besten abgewehrt werden.

Foto: NINENII – stock.adobe.com

Gesetzgeber nimmt Security-Awareness in den Fokus

Der Gesetzgeber hat die Kassen(zahn)ärztlichen Bundesvereinigungen verpflichtet, in einer Richtlinie die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung festzulegen.

Diese Richtlinie soll „auch Anforderungen an die sichere Installation und Wartung von Komponenten und Diensten der Telematikinfrastruktur, die in der vertragsärztlichen und vertragszahnärztlichen Versorgung genutzt werden“ umfassen.

Mit dem Gesetz zur Beschleunigung der Digitalisierung im Gesundheitswesen vom 26. März 2024 wurden diese Anforderungen in § 390 SGB V (früher § 75b) verschoben.

➤ Ergänzt wurde unter anderem, dass die Richtlinie auch „Maßnahmen zur Sensibilisierung von Mitarbeiterinnen und Mitarbeitern zur Informationssicherheit (Steigerung der Security-Awareness)“ enthalten soll.