RICHTIGE VERSICHERUNG KANN GROSSEN ÄRGER SPAREN

Apotheken können sich strafbar machen, wenn sie gehackt werden

APOTHEKE ADHOC, 26.07.2021 15:10 Uhr

-  Foto: shuterrstock.com/sitthiphong

Immer mehr Großhacks: Die Gefahr, Opfer von Cyberangriffen zu werden, steigt für Apotheken rasant.

***Berlin* - Der Ausfall des DAV-Portals hat den Apotheken einmal die Bedeutung digitaler Sicherheitsarchitektur vor Augen geführt. Doch es muss gar kein so grundlegender Konstruktionsfehler sein: Allein in den vergangenen Wochen gab es weltweit mehrere schwere Cyberangriffe, die nicht nur Behörden und Konzerne getroffen haben, sondern auch massenhaft Einzelhändler und Endnutzer. Ein Hack muss nicht die einzelne Apotheke vor Ort ins Visier nehmen, um dort massiven Schaden anzurichten. Es ist allerhöchste Zeit, dass sich Apotheken dagegen wappnen, fordern die Apotheken-Absicherungsexperten Christian Ring, Dresden und Michael Jeinsen aus Berlin.**

Eine bislang unbekannte Gruppe namens „REvil“ hackt den US-amerikanischen IT-Dienstleister Kaseya, um 70 Millionen US-Dollar Lösegeld zu erbeuten – und in Schweden bleiben hunderte Supermärkte der Kette Coop geschlossen. Denn die Supermarktkette arbeite mit Software von Dienstleistern, der wiederum Kaseya-Kunde ist – deren Abrechnungssysteme hatten die Hacker gekapert und verschlüsselt, die Coop-Märkte konnten deshalb ihre Kassensysteme nicht mehr benutzen. Den Namen Kaseya hatte von den Supermarktbediensteten wohl kaum jemand schon mal gehört. Doch von dem Hack mit Domino-Effekt ist nicht nur Schweden betroffen, auch in Deutschland sind nach Angaben Bundesamts für Sicherheit in der Informationstechnik (BSI) mehrere tausend Firmencomputer infiziert worden. Bis jetzt sind die Probleme nicht vollständig gelöst – über drei Wochen nach dem Hack.

Die Liste ließe sich lange fortsetzen: Schlagzeilen machte zuletzt auch der Landkreis Bitterfeld in Sachsen-Anhalt. Durch eine Sicherheitslücke in der Drucker-Software drangen die Hacker am 6. Juli in das Amts-Netz ein und legten alles lahm. Zeitweise ging gar nichts mehr, Sozialleistungen konnten nicht ausgezahlt, Bürgeramtsangelegenheiten nicht erledigt und Fahrzeuge nicht angemeldet werden. Mit Behelfsmaßnahmen wird derzeit ein Minimalbetrieb aufrechterhalten, zur normalen Arbeit ist das Amt aber auch drei Wochen nach dem Hack nicht zurückgekehrt. Die Liste der Beispiele allein aus der jüngsten Vergangenheit ließe sich lange fortsetzen: Im September 2020 legte ein Hack die Düsseldorfer Uniklinik lahm, Anfang des Jahres die Urologische Klinik Planegg, im März traf es die Evangelische Klinik Lippstadt. Ebenfalls im März traf es den französischen Hersteller Pierre Fabre und es wurde bekannt, dass die chinesische Hackergruppe Hafnium eine Sicherheitslücke bei Exchange-Servern von Microsoft, um 57.000 Server zu infizieren – allein in Deutschland.

Jüngstes Opfer wurde die Haftpflichtkasse VVaG aus Darmstadt, bei der nach aktuellen Erkenntnissen auch in größerem Maße Daten abgeflossen sind. Der Schaden- und Unfallversicherer betreut laut Wirtschaftswoche deutschlandweit rund zwei Millionen Versicherungsverträge mit einem Beitragsvolumen von rund 200 Millionen Euro. Die Liste der Beispiele ließe sich noch lang fortsetzen und illustriert bereits eine grundlegende Erkenntnis der vergangenen Monate: Die Gefahr von Cyberangriffen war noch nie so groß wie im Moment, und sie wird steigen. „Wenn Gesundheitsdaten immer wertvoller werden, wird kein moderner Einbrecher mehr das Brecheisen ansetzen. Er wird sie mit seinem Computer gefahrenfrei von zu Hause absaugen und im Darknet zu Geld machen“, erklärt Christian Ring das absehbare Zukunftsszenario. Einer aktuellen Untersuchung des IT-Sicherheitsunternehmens Deep Instinct zufolge hat sich die Zahl von Ransomware-Angriffen wie dem auf Kaseya – bei denen Daten verschlüsselt werden, um dann für deren Freigabe ein Lösegeld zu verlangen – in den vergangenen zwei Jahren verachtfacht. Allein im ersten Halbjahr gab es demnach einen Anstieg von 244 Prozent.

Darüber hinaus illustrieren die Beispiele vor allem zwei Erkenntnisse, die für jede Vor-Ort-Apotheke relevant sind: Erstens kommen ihr die Ziele der Hacker-Angriffe immer näher – zweitens müssen sie sich nicht um einzelne Opfer bemühen, um eine erhebliche Anzahl von Apotheken in Deutschland lahmzulegen. Denn in einer immer engmaschiger vernetzten, globalen Gesundheits-Infrastruktur reicht es, die richtigen Datentransfer-Knotenpunkte zu infizieren, von denen Schadsoftware dann nach unten durchsickert – in letzter Instanz zu einzelnen Betrieben wie Apotheken.

„Die meisten Apotheken sagen – und ich betone: zu Recht – ‚Wer hat denn schon Interesse an meinen Daten?' Dieser Gedanke ist aber falsch, denn: bei Ihnen selbst muss gar nichts passieren", sagt Jeinsen. „Hacker greifen keine einzelnen Apotheken an, sondern große Unternehmen wie Versicherungen, Rechenzentren oder Softwarehäuser. Über diese Institutionen kann dann jede mit ihnen verbundene Apotheke infiziert werden. Als Hacker würde ich eine Krankenversicherung oder Rezeptsammelstelle hacken, weil auch dort heute noch nicht die höchsten Sicherheitsstandards vorgehalten werden. Bildlich gesprochen leben wir heute noch im Zeitalter der offenen-IT-Tür: Selbst amerikanische IT-Unternehmen, das Pentagon oder der Bundestag sind schon erfolgreich gehackt worden."

Dabei hätten die Apotheken besondere Schwachstellen, berichtet Ring: So wie die Hacker den Landkreis Bitterfeld kapern konnten, indem sie über den Drucker ins Netzwerk kamen, gebe es auch in Apotheken Gerätschaften, die beispielsweise über das WLAN angebunden sind und gefährliche Sicherheitslücken aufweisen können. „Neben den Datenschnittstellen zu den Rechenzentren, haben wir auch bei den Nahinfrarot-Spektrometern in konkreten Fällen festgestellt, dass diese Geräte beste Einfallstore für Datenmissbrauch sind. Hacker sind tatsächlich schon über Spektrometer in Apotheken eingedrungen. Neue Anwendungen wie Nachbestellfunktionen in Kommissionierern werden diese Gefahren noch vergrößern – je mehr Geräte angebunden sind, desto mehr Einfallstore gibt es", so der Cyberversicherungs-Experte. Sein Tipp: NIR-Spektrometer gerne nutzen – aber nur als Stand-Alone-Gerät, niemals in Apotheken-Netze eingebunden.

Speziell Apotheken liegen dabei gleich an mehreren für Hacker besonders lukrativen Schnittstellen zwischen Leistungserbringern und Kostenträgern im Gesundheitswesen, durch ihre EDV laufen besonders sensible – und damit wertvolle – Daten. „Für den Datensatz eines Krebspatienten werden im Darknet mit rund 800 Dollar bezahlt. Wenn man 500 Datensätze abgreift, kann man schon reich werden", erklärt Jeinsen. Aber nicht der finanzielle Wert, sondern die rechtliche Bewertung der in Apotheken verarbeiteten Daten macht das Thema für Apotheken besonders heikel: Denn abgesehen von der Gefahr, dass die eigene EDV und damit der Betrieb lahmgelegt wird, bringt die besondere Schützenswürdigkeit der in ihnen verarbeiteten Daten Apotheken in besonderen Zugzwang. „Wie bei der Diskretion am HV auch, liegt die Datensicherheit auch bei Datenrechtsverstößen gemäß DSGVO bei den Apotheken. Sie sind in der Pflicht, in einem solchen Schaden, genau und exakt festzustellen, was vorgefallen ist und das den jeweiligen Aufsichtsbehörden ordnungsgemäß zu melden", erklärt Jeinsen. „Zudem sind alle potenziell betroffenen Kunden innerhalb von 72 Stunden rechtsverbindlich dokumentiert zu informieren – das heißt, der Apotheker hat nach Erkennen des Schadens nur 72 Stunden Zeit, einen Datenrechtsanwalt und einen IT-Forensiker finden, die ihm die Schadenquellen untersuchen, Kundendaten sichern, eine vollständige Meldung absetzen und auch noch alle potenziell betroffenen Kunden schriftlich zu informieren."

„Das Datenschutzrisiko liegt im Falle eines Hacks deshalb bei den Apotheken. Sie sind in der Pflicht, in einem solchen Schaden, genau und exakt festzustellen, was vorgefallen ist und das den Aufsichtsbehörden ordnungsgemäß zu melden", erklärt Jeinsen. „Dabei sind alle potenziell betroffenen Kunden innerhalb von 72 Stunden rechtsverbindlich dokumentiert zu informieren – das heißt, der Apotheker kann 72 Stunden nicht richtig arbeiten, muss einen Datenforensiker und einen Datenschutz-anwalt finden, der ihm das auswertet und aufschlüsselt."

Und dazu gebe es speziell wegen der Natur der Daten keine Alternative: „Nach den 72 Stunden wird laut DSGVO aus einer Ordnungswidrigkeit ein Straftatbestand, weil es sich um die drei besonders schützenswerten Datengruppen handelt: persönliche Daten, Finanzdaten und Gesundheitsdaten", so Jeinsen. „Apotheken begehen deshalb nicht wie jede Drogerie oder Tankstelle eine Ordnungswidrigkeit, wenn sie geklaute Daten nicht unverzüglich melden, sondern es droht sofort die Pflichtangabe an die Staatsanwaltschaft."

Genau hier müssten Versicherungspolicen greifen, fordert Ring. „Das eigentliche Problem ist die 72-Stunden-Klausel", sagt er. „Das Entscheidende ist nämlich nicht, dass die Kosten für Anwalt und IT-Forensiker getragen werden, sondern dass man die Garantie hat, innerhalb der Frist solche Experten zu bekommen, die das Problem wirklich lösen können." Denn, gerade das zeichnet große Cyberangriffe ja aus: Durch den Befall zentraler Knotenpunkte werden Betriebe zu hunderten, wenn nicht tausenden gleichzeitig angegriffen. Der Kaseya-Hack habe genau gezeigt, was dann passiert: „In Schweden haben die meisten Märkte keine Anwälte mehr gekriegt, weil sich die ersten alle gekrallt hatten. Der Engpass sind genau diese Spezialisten. Und ein solcher Hack würde niemals einzelne Apotheken betreffen."

Entscheidend sei deshalb, eine Police zu zeichnen, die eine Rund-um-die-Uhr-Abdeckung samt Kontakt zu Fachanwälten und IT-Forensikern garantiert, die im Notfall sofort tätig werden und durch die Aussendung an Datenschutzbeauftragte und andere Dienststellen nicht nur die Einhaltung der 72-Stunden gewährleisten, sondern mit ihrer Arbeit im Zweifelsfall auch die Aufrechterhaltung des Betriebs ermöglichen.

Das sollte seiner Ansicht nach vor allem schnell geschehen, denn Experten seien sich einig, dass es nur noch eine Frage der Zeit sei, bis auch die Apotheken von einem Großangriff à la Kaseya getroffen werden. „Die Versicherung ist so lange noch billig, wie es keine größeren Schäden gibt. Nach dem ersten Großhack werden die Kosten aber explodieren und die Apotheken, die sich erst danach versichern, werden dann nicht mehr 500, sondern eher 1000 Euro im Jahr dafür zahlen müssen“, so Jeinsen. „Und so ein Ereignis wird es garantiert geben, spätestens mit dem E-Rezept. Es gibt niemanden in der Versicherungsbranche, der das anders sieht. Cyberrisk-Policen werden damit zur normativen Pflicht in Apotheken, das wird die Feuerversicherung des 21. Jahrhunderts.“