FMH SERVICES

So schützen Sie Ihre Praxis vor Cyberattacken

Im Rahmen der Digitalisierung nehmen Cyberattacken immer mehr zu. Dass sie jede und jeden treffen können – auch Arztpraxen und Institutionen des Gesundheitswesens –, ist leider eine Tatsache. Doch wer sich der Gefahr bewusst ist und sich entsprechend vorbereitet, ist Cyberkriminellen keinesfalls schutzlos ausgeliefert.

Im Jahr 2023 nahm die Zahl der in der Schweiz verübten Cyberattacken erneut zu. Das Gesundheitswesen mit seinen sensiblen, besonders schützenswerten Daten ist für Cyberkriminelle durchaus ein attraktives Ziel. Und da die Opfer dieser Angriffe oft eher zufällig als systematisch ausgewählt werden, kann es jede und jeden treffen.

Ransomware: Wenn Daten im Darknet auftauchen
Vielleicht können Sie sich an den 2023 immer wieder in den Medien thematisierten Namen «Play» erinnern. Es handelt sich dabei um eine kriminelle Gruppe, die zahlreiche sogenannte Ransomware-Angriffe auf Schweizer Unternehmen verübt hat. Bei einer solchen Attacke beschaffen sich Cyberkriminelle Zugang zu sensiblen Daten, verschlüsseln diese und fordern in der Folge Lösegeld für die Entschlüsselung. Oft drohen sie zudem mit der Publikation der Daten, sollte das Lösegeld nicht gezahlt werden.

Zu den Opfern von «Play» gehörten unter anderem der Behörden-Software-Anbieter Xplain und die Berner IT-Dienstleiterin Unico Data AG. Bei beiden Angriffen wurden Daten von Kunden der Unternehmen entwendet und teilweise gar im Darknet publiziert – darunter Daten des Bundesamts für Polizei (Fedpol), der SBB, des Kantons Aargau, der Kinokette Pathé sowie der Siloah-Gruppe, einer Versorgerin in der Altersmedizin in der Region Bern. Im selben Halbjahr angegriffen wurden die Medienunternehmen NZZ und CH Media, was im Juni 2023 auch zum Diebstahl von Adressdaten von FMH-Mitgliedern führte.

Denial of Service: Böswillige Überlastung von Websites
Ein anderes Ziel verfolgen sogenannte Denial-of-Service- Attacken, kurz DDoS. Dabei versuchen Hacker, Server durch künstlich erhöhte Nachfragen zu überlasten. Die attackierten Websites sind dann nicht mehr oder nur eingeschränkt erreichbar. Ein Beispiel hierfür war der Angriff auf die Website der eidgenössischen Räte www.parlament.ch im Juni 2023, welcher dazu führte, dass diese zeitweise nicht mehr erreichbar war.

Schützen Sie Ihre Praxis
Je besser Sie die IT-Infrastruktur Ihrer Praxis oder Institution schützen, desto schwerer machen Sie es Cyberkriminellen – und desto geringer ist das Risiko, dass diese mit ihren Machenschaften bei Ihnen Schaden anrichten. Nachfolgend geben wir Tipps, die Sie selbst oder gemeinsam mit Ihrem IT-Partner umsetzen können.

Halten Sie Ihre Infrastruktur aktuell
Veraltete Betriebssysteme und Programme sind ein beliebtes Einfallstor für Cyberkriminelle, denn Updates und Aktualisierungen schliessen häufig bekannte Sicherheitslücken. Um Ihre Praxis oder Institution bestmöglich zu schützen, gilt es deshalb sicherzustellen, dass Ihre IT-Infrastruktur auf dem neuesten Stand ist – und zwar jedes einzelne Arbeitsgerät.

- Halten Sie Ihr System auf dem neuesten Stand. Dazu zählen die Betriebssysteme der Arbeitsgeräte ebenso wie Browser, E-Mail-Programme, Virenschutzprogramme und andere genutzte Programme auf den Geräten.
- Installieren Sie Updates umgehend, insbesondere wenn es sich um Sicherheits-Updates handelt.
- Erstellen Sie regelmässig Backups von Ihren Systemen.

Schützen Sie jedes Arbeitsgerät
Schon ein einziger Computer oder Laptop oder ein einziges Smartphone ohne genügenden Schutz bietet Cyberkriminellen eine Möglichkeit, Ihre Institution anzugreifen. Es kann helfen, ein Inventar aller genutzter Arbeitsgeräte zu erstellen, um den Überblick über die darauf getroffenen Schutzmassnahmen zu behalten.

- Installieren Sie auf jedem Arbeitsgerät in Ihrer Institution einen aktuellen Virenschutz und aktivieren Sie die Sicherheitsfunktionen Ihres Betriebssystems. Dies gilt für Windows- ebenso wie für Mac-Geräte.
- Schützen Sie alle Geräte (Computer, Laptop, Router, Handy etc.) durch sichere Passwörter. Acht bis zehn Stellen inklusive Zahlen und Sonderzeichen sind das Minimum.
- Setzen Sie limitierende Benutzerberechtigungen und arbeiten Sie nicht mit dem Administrator-Account.

Jederzeit aufmerksam sein
Die beste technische Infrastruktur ist nicht sicher genug, wenn ihre Nutzer sich nicht korrekt verhalten. Denn ein einziger falscher Klick kann im schlimmsten Fall grossen Schaden anrichten. Deshalb ist es wichtig, sich im Arbeitsalltag der Relevanz der IT-Sicherheit jederzeit bewusst zu sein. Das gilt für jeden einzelnen Mitarbei- tenden, von der MPA bis zum Chefarzt.

- Seien Sie vorsichtig bei verdächtigen E-Mails, selbst wenn diese von Ihnen bekannten Absendern zu stammen scheinen. Leider können Absenderadressen einfach gefälscht werden.
- Löschen Sie verdächtige Nachrichten umgehend, ohne angefügte Dateien im Anhang zu öffnen. Löschen Sie die Nachricht auch im Papierkorb Ihrer E-Mail-Ablage.
- Klicken Sie nie auf Links in verdächtigen E-Mails und öffnen Sie keine von deren Anhängen.
- Setzen Sie sichere Passwörter für Ihre Benutzer- accounts
- Vorsicht beim Surfen! Laden Sie keine unbekannten Programme herunter. Achten Sie bei der Angabe von Informationen auf eine genügende Verschlüsselung. Diese erkennen Sie an dem Schloss-Symbol oben links bei der Anzeige der URL einer Website.
- Übermitteln Sie sensible Daten nur verschlüsselt an sicher identifizierte Empfänger.

Eine lohnenswerte Investition
Eine Cyberattacke kann grossen Schaden anrichten: ein mehrere Stunden oder gar Tage andauernder Unterbruch des normalen Praxisbetriebs, Kosten für die Wiederherstellung der Daten, viel Aufwand und nervliche Belastung Ihrerseits, ganz zu schweigen von dem Vertrauensverlust bei Patientinnen und Patienten, wenn diese darum bangen müssen, ob ihre Gesundheitsdaten im Darknet publiziert werden könnten. Ja, eine sorgfältig gepflegte IT-Infrastruktur, eine funktionierende Backup-Lösung und wenn möglich gar eine Schulung aller Mitarbeitenden erfordern einiges an Planung und Aufwand. Doch sie können auch viel bewirken und Ihnen viele Probleme ersparen!

Zur Person
Daniel Huser, Bereichsleiter Projektmanagement & IT-Architektur
Mitglied der erweiterten Geschäftsleitung

Health Info Net AG
Seidenstrasse 4
8304 Wallisellen
Telefon 0848 830 740
daniel.huser@hin.ch
www.hin.ch