FMH SERVICES

Cyberattacken im Gesundheitswesen: So handeln Sie richtig

In diesem Beitrag erfahren Sie, wie Sie Ihre Praxis oder Institution vor Cyberattacken schützen und wie Sie sich im Ernstfall richtig verhalten.

Digitale Hilfsmittel erleichtern Gesundheitsfachpersonen die Praxisadministration und verhelfen Prozessen im Arbeitsalltag zu mehr Effizienz. Doch leider bringt die Digitalisierung auch neue Risiken und Bedrohungen mit sich. Denn auch das Gesundheitswesen gerät vermehrt ins Visier von Cyberkriminellen.

Im Rahmen der Digitalisierung nehmen Cyberattacken immer mehr zu. Dass sie jede und jeden treffen können – auch Arztpraxen, Spitäler oder andere Institutionen des Gesundheitswesens –, ist leider eine Tatsache. Denn einerseits ist das Gesundheitswesen mit seinen sensiblen Daten ein attraktives Ziel für Cyberkriminelle, andererseits werden die Opfer dieser Angriffe oft eher zufällig als systematisch ausgewählt.

Verteidigung beginnt vor dem Angriff
Personen und Institutionen, die mit sensiblen Daten zu tun haben, tragen eine Mitverantwortung für die Sicherheit ihrer Systeme und Daten. Deshalb ist es essenziell, präventive Vorkehrungen zu treffen, um das Sicherheitsniveau der IT-Systeme und somit der Daten möglichst hoch zu halten. Zudem gilt: Je schwieriger es für Cyberkriminelle ist, eine Institution anzugreifen, desto weniger attraktiv wird diese als Ziel einer Cyberattacke.

Die wichtigsten Schutzmassnahmen lassen sich in drei Kategorien einteilen:

1. Technische Vorkehrungen
Zu den technischen Vorkehrungen gehört unter anderem der Schutz von Arbeitsgeräten mit einer Firewall und einem Virenscanner. Ausserdem ist es wichtig, Updates von Betriebssystemen, Webbrowsern und Virenschutzprogrammen immer umgehend zu installieren, um mögliche Sicherheitslücken sofort zu schliessen. Die FMH hat dazu ein Dokument [1] herausgegeben, das Praxisärztinnen und -ärzten einen guten Anhaltspunkt für ihre Praxisinformatik gibt. Es beinhaltet Anforderungen, die ein Mindestniveau an Sicherheit für Daten, Informationen und die IT-Infrastruktur sicherstellen.

2. Organisatorische Vorkehrungen
Unter organisatorischen Vorkehrungen versteht man die Implementierung von Prozessen und Weisungen durch den/die Praxisinhaber/in. Beispiele sind das Durchführen regelmässiger Backups oder Weisungen an die Mitarbeitenden bezüglich der Handhabung von Daten und Systemen.

3. Verhaltensbezogene Massnahmen
Selbst eine sichere IT-Infrastruktur kann keinen 100-prozentigen Schutz vor Cyberattacken garantieren. Und schafft es ein Phishing-Mail, die Antivirus-Software zu umgehen und im Postfach der Arztpraxis zu landen, ist es die Person vor dem Computer, die den Unterschied ausmacht: Öffnet sie den virenverseuchten Anhang der Nachricht nicht und kontaktiert stattdessen den IT-Verantwortlichen, kann sie grossen Schaden verhindern. Aus diesem Grund sind regelmässige Schulungen und die Sensibilisierung der Mitarbeitenden für das Thema IT-Sicherheit unerlässlich.

Richtiges Verhalten bei einer Cyberattacke
Eine sichere IT-Infrastruktur und gut geschulte Mitarbeitende machen Cyberkriminellen das Leben schwer und verringern die Wahrscheinlichkeit einer erfolgreichen Cyberattacke auf die entsprechende Institution. Dennoch sollten alle Mitarbeitenden auch wissen, wie sie sich im Falle eines Angriffs verhalten sollen. Denn in einer solchen Situation gilt es effizient und zeitnah zu handeln. Unsere Empfehlung: Stellen Sie Ihren Mitarbeitenden ein Merkblatt mit den wichtigsten Sofortmassnahmen bereit. Dieses sollte auch den Kontakt enthalten, an den sie sich im Ernstfall wenden können.

Zu Ihrer Unterstützung hat HIN eine Checkliste mit Sofortmassnahmen erarbeitet. Einige wichtige Punkte daraus:

- Schnell handeln: Warten Sie beim Verdacht auf einen Angriff nicht ab, sondern handeln Sie sofort.
- Infizierte Geräte vom Netzwerk trennen: Schalten Sie WLAN-Adapter aus und stecken Sie bei Geräten, die mit einem Netzwerkkabel verbunden sind, dieses Kabel aus. Lassen sich die infizierten Geräte nicht eindeutig identifizieren, trennen Sie das gesamte Netzwerk vom Internet.
- Nachricht löschen: Löschen Sie die Nachricht mit dem schädlichen Anhang aus allen E-Mail-Konten, auch aus dem Papierkorb.
- Informieren: Informieren Sie alle an den Arbeitsstationen tätigen Personen. So stellen Sie sicher, dass die Nachricht mit dem schädlichen Anhang auf keinem weiteren Gerät geöffnet wird.
- IT-Partner zu Rate ziehen: Involvieren Sie Ihren IT-Partner oder -Support. Dieser kann das Ausmass des Schadens abwägen und Sie beim weiteren Vorgehen unterstützen.
- Vorfall melden: Wir empfehlen, den Cyberangriff dem Nationalen Zentrum für Cybersicherheit (NCSC) zu melden.

Die gesamte Checkliste finden Sie hier: www.hin.ch/cyberattacke

Lösegeldzahlung: Ja oder nein?
Eine häufige Angriffsmethode ist der Verschlüsslungstrojaner, auch «Ransomware» genannt. Sind Sie von einem Angriff durch Ransomware betroffen, werden die Daten auf Ihrem Arbeitsgerät verschlüsselt und Sie können nicht mehr darauf zugreifen. In diesem Fall werden Sie in der Regel aufgefordert, ein Lösegeld zu bezahlen, damit man Ihnen den Zugang auf die Daten wieder ermöglicht. Dies ist jedoch wenig empfehlenswert, da die Zahlung keine Garantie für den Wiedererhalt Ihrer Daten ist. Ausserdem trägt Ihr Geld dazu bei, dass die Täter ihre Angriffsmethoden weiterentwickeln können und zu weiteren Angriffen animiert werden. Auch in Bezug auf Ransomware gilt: Vorsorge ist die beste Verteidigung. Investieren Sie in eine vollständige Backup-Lösung für Ihre Praxis oder Institution, um im Ernstfall nicht um Ihre Daten fürchten zu müssen.
Optimalerweise besprechen Sie das Backup mit Ihrem IT-Partner oder -Support.

Quellenverzeichnis
[1] «Minimalanforderungen IT-Grundschutz der FMH für Praxisärztinnen und- Praxisärzte», zu finden unter www.fmh.ch /dienstleistungen/e-health/itgrundschutz.cfm

Interessante Artikel
1. https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infosunternehmen/aktuelle-themen/cyberangriffe-gegen-firmen.html
2. https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infosunternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html
3. https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infosunternehmen/vorfall-was-nun/ransomware.html

Zur Person
Uwe Gempp, CSO & IT-Architekt

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