IT-Sicherheit in der Praxis

Wann haben Sie das letzte Mal das Passwort ausgetauscht?

Auf Server und PC-Arbeitsplätzen in der Praxis liegen sensible Daten, auf die auch Cyber-Kriminelle gern Zugriff hätten. Ihnen können Praxischefs bereits mit einfachen Mitteln Paroli bieten. Entscheidend dafür ist das richtige Sicherheitskonzept.

© Jürgen Fälsche / Fotolia

Etwa 80 % der Angriffe von Cyber-Kriminellen zielen auf kleine und mittlere Unternehmen, zu denen auch Arztpraxen zählen, so Dr. Oliver Grün, Präsident des Bundesverbandes IT-Mittelstand. Große Unternehmen betrieben heute einen hohen Aufwand, um wertvolle Informationen auf ihren Festplatten zu schützen. „Kleine Arztpraxen können das nicht in dem Umfang leisten, bieten Angreifern aber durchaus lukrative Geheimnisse, wie personenbezogene medizinische Daten“, meint Grün. Dabei können sich Ärzte auch ohne einen Systemadministrator in der Praxis mit den richtigen Kniffen gut schützen.

„IT-Sicherheit in der Praxis sollte immer Chefsache sein“, betont Grün nachdrücklich. Der Arzt müsse dafür nicht viel Zeit mit der eigentlichen Technik verbringen – hiermit könne auch ein IT-Dienstleister beauftragt werden. Wesentlich dabei sei, die wichtigsten Angriffspunkte in der Praxis zu kennen, um ein gutes Sicherheitskonzept entwickeln zu können. Ein erster Schritt in die richtige Richtung sei, das Bewusstsein für Sicherheit im Praxisteam zu erhöhen. Dazu gehöre zum Beispiel, dass Praxisrechner gesperrt werden, wenn etwa MFA ihren Arbeitsplatz für eine Pause verlassen. Anhänge in einer E-Mail sollten nur geöffnet werden, wenn klar ist, wer der Absender ist. Solche Verhaltensweisen für mehr Sicherheit im Alltag könnten gemeinsam in den Teamsitzungen festgelegt werden.

Routinemäßiger Passwortaustausch

Ein anderer zentraler Punkt sei das Zugriffsmanagement. „Zirka 60 bis 70 Prozent der Angriffe kommen von innen“, sagt Grün. Das können etwa Mitarbeiter

und Kollegen sein, die nun in einer anderen Praxis tätig sind, aber noch Einblick in Daten des ehemaligen Arbeitgebers haben. Ein Beispiel dafür sei der Terminkalender der Praxis – so dieser online ist. Das passiere dann, wenn Passwörter nicht routinemäßig ausgetauscht würden. Wichtige Zugangsdaten sollten in regelmäßigen Intervallen erneuert werden: „Etwa alle drei Monate empfiehlt sich hier als Faustregel“, erklärt Grün.

Gefahren drohen den Praxisdaten aber auch von außerhalb, wobei diese nicht immer menschlicher Natur sind. Sogenannte Bots – kleine Schadprogramme – durchkämmen systematisch das Internet auf der Suche nach Sicherheitslücken. Ein mögliches Ziel ist der Praxisserver, also der Computer, der dauerhaft mit dem Internet verbunden ist. „Im Schnitt wird ein Server hunderte Male am Tag angegriffen“, berichtet Sicherheitsexperte Grün. Das funktioniere beispielsweise so: Bietet die Internetseite der Praxis einen Service für Patienten, um Termine zu buchen – und damit ein Onlineformular – werde der Bot aktiv. Automatisiert trage er Schadcodes (z. B. HTML-Befehle) etwa in das Textfeld für die Terminbuchung ein. Ist der Server mit der Praxiswebsite davor nicht gefeit, werde er vom Bot „geentert“. „Der Server verschickt dann unbemerkt Spam oder wird ausgehorcht“, sagt Grün. Gegen solche Zugriffe helfen Firewall und Antivirenprogramme.

Damit keine Einfallstore für Cyber-Kriminelle in der Praxis bestehen, müssen die Sicherheitsprogramme stets aktuell gehalten werden. Dabei ist es laut dem Experten bereits riskant, die Programme länger als eine Woche nicht zu aktualisieren. Auch Betriebssystem, Internetbrow-

ser und andere täglich benutzte Anwendung benötigen regelmäßige Pflege, erklärt Grün. Das betreffe alle mit dem Internet verbundenen Rechner in der Praxis.

Auch mobile Geräte der Praxis verschlüsseln

Auch mobile Geräte können Sicherheitsrisiken bergen: „Werden USB-Sticks in der Praxis verwendet, sollten diese verschlüsselt sein“, betont Grün. Solche Speicher mit Hardwareverschlüsselung seien in der Regel teurer als die ohne Verschlüsselung. Bei Verlust können Dritte die gespeicherten Informationen aber nicht auslesen. Auf einigen Modellen befindet sich zudem ein eigener Virenschutz. Das ist auch bei anderen Geräten in der Praxis wichtig: Tablet-PC oder Laptops, die Ärzte beispielsweise auf Kongressen nutzen, sollten ebenfalls eine Festplattenverschlüsselung aktiviert haben.

Ein weiterer wesentlicher Punkt für Ärzte ist die Datensicherung: „IT-Sicherheit bedeutet nicht nur Vertraulichkeit, sondern auch Verfügbarkeit.“ Damit meint Grün, dass Ärzte regelmäßige Datensicherungen durchführen und anlegen, auf die sie zurückgreifen können, falls Geräte defekt oder mit Viren befallen sind. Dabei mahnt Grün vor den immer beliebter werdenden Cloud-Lösungen, bei denen sich Daten auf externen Servern speichern und überall auf der Welt abrufen lassen. Wer bei Microsoft OneDrive, Google Drive, Dropbox oder anderen Anbietern Daten ablege, müsse diese verschlüsseln. Dafür können, so Grün, Programme wie „Boxcryptor“ verwendet werden. „Wird die Cloud gehackt, finden Angreifer darin dann nur ungenießbaren Datensalat.“

Marco Hübner