Hardware-Firewall in der Praxis:

Die fünf größten Missverständnisse

Das Wichtigste vorweg: Als Praxisinhaber sind Sie gesetzlich zum wirksamen Schutz Ihrer Patientendaten verpflichtet. Die Kassenärztliche Bundesvereinigung (KBV) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) haben in der IT-Sicherheitsrichtlinie § 75b SGB V festgelegt, dass jede mit dem Internet verbundene Praxis-IT durch eine Firewall gesichert sein muss. Hierfür wird eine Hardware-Firewall empfohlen, die zwischen Router und Praxisnetzwerk geschaltet wird, um bedrohliche Schadsoftware herauszufiltern.

Dennoch verzichten einige Behandler auf eine Abschirmung ihrer Praxis gegen Cyber-Attacken. Diese Entscheidung beruht meistens auf einem der folgenden, weit verbreiteten Missverständnisse, die wir an dieser Stelle gern aufklären möchten.

1. „Durch den Internet-Router ist meine Praxis-IT ausreichend geschützt."

Gängige Router wie eine Fritzbox bieten in der Regel keine weitreichenden technologischen Möglichkeiten zum Aufspüren von Gefahren. Sie können beispielsweise nicht erkennen, ob es sich um eine harmlose Audiodatei handelt – oder um eine als Audiodatei getarnte Schadsoftware. Im Unterschied dazu verfügen moderne Schutzsysteme wie die UTM-Hardware-Firewall von Epikur über eine eigene Lösung gegen Viren, durch die das auf Ihrem Praxisrechner installierte Anti-Viren-Programm unterstützt wird. Das Sicherheitsniveau wird dadurch deutlich heraufgesetzt.

Zusätzlich verfügt eine UTM-Hardware-Firewall über ein sogenanntes Intrusion Detection System (IDS), durch das ungewöhnliches Verhalten erkannt und Angriffe abgewehrt werden können. Weitere Vorteile gegenüber einem Internet-Router sind eine klare interne Netzwerktrennung, ein URL- und Web-Filter zum Schutz vor Zugriffen auf bekannte bösartige Domains sowie die enthaltene Wartung und Sicherheitsupdates für die gesamte Laufzeit der Hardware-Firewall.

2. „Mir kann nichts passieren, weil ich Apple-Produkte verwende."

Generell gilt: Betriebssysteme von Apple basieren auf Linux und sind daher wie jedes andere Betriebssystem der Welt anfällig gegen spezialisierte Schadsoftware. Diese kann die Betriebssysteme Ihrer Geräte über sogenannte Rootkits infizieren und damit Schutzmaßnahmen umgehen – auch die von Apple-Rechnern. Zudem machen sich Angreifer gern die Schwächen von großen Herstellern wie Microsoft, Apple oder Adobe zu Nutze. Generell gilt: Je mehr ihr Gerät kann, desto angreifbarer ist es. Unsere Hardware-Firewall kann nur eines – das aber richtig gut: Netzwerkschutz. Sie dient als digitaler Türsteher für Ihre Praxis-IT.

3. „Der TI-Konnektor ist genauso gut wie eine Hardware-Firewall."

Obwohl der TI-Konnektor in einer Reihenschaltung Funktionen einer Hardware-Firewall übernehmen kann, machen Sie sich damit abhängig vom SIS-Netzwerk der Telematikinfrastruktur. Dies kann Geschwindigkeitseinbußen und Funktionseinschränkungen zur Folge haben. Ist das SIS-Netzwerk beispielsweise nicht erreichbar, besteht für Ihre Praxis-IT keine sichere Verbindung mehr zum Internet.

Ein weiterer Nachteil: Über den TI-Konnektor lässt sich kein WLAN betreiben. Da das IT-Sicherheitspaket von Epikur über einen WLAN Access Point verfügt, steht Ihnen damit nicht nur ein sicheres Praxis-WLAN zur Verfügung, sondern auch ein vollständig davon getrenntes WLAN für Ihre Patienten. Darüber hinaus haben Sie dank VPN auch dann sicheren Zugriff auf EPIKUR, wenn Sie sich außerhalb Ihrer Praxis aufhalten. Der TI-Konnektor bietet diese Möglichkeit nicht.

4. „Ohne Förderung lohnt sich die Anschaffung einer Hardware-Firewall nicht."

Da Sie in Ihrer Praxis nicht als Privatperson agieren, sind im Fall eines Angriffs nicht nur die persönlichen Urlaubsbilder und Kontodaten in Gefahr, sondern die vertraulichen Daten Ihrer Patienten. Bei aktuellen Attacken geht es oftmals nicht nur um das Ausspähen von Daten, sondern auch darum, die Opfer zu erpressen. Darum sollten Ihr Handeln und Ihr Schutzniveau sich nicht an dem einer Privatperson orientieren, sondern die Professionalität Ihrer Praxis widerspiegeln. Sollten sensible Patientendaten in die falschen Hände geraten oder Sie sich gezwungen sehen, einen Hacker für die Freigabe Ihrer Daten zu bezahlen, kann das schnell teuer werden.

5. „Es besteht derzeit kein Anlass, sich für eine Sicherheitsmaßnahme zu entscheiden."

Gesetzlich sind Sie zum Schutz vertraulicher Patienteninformationen verpflichtet. Und das aus gutem Grund: Laut Lagebericht des Bundeskriminalamts ist die Anzahl an Cyber-Straftaten in den vergangenen Jahren deutlich gestiegen. Zudem gibt sich die Gefahr aus dem Internet oftmals nicht als solche zu erkennen. Viele Kriminelle infiltrieren ungenügend geschützte Computer und spionieren die Nutzer so lange aus, bis sie eine Schwachstelle gefunden haben – wenn es sein muss, über mehrere Monate hinweg.

Um professionelle Kriminelle – also echte Hacker – abzuwehren, benötigen Sie ein Konzept aus mehreren Schutzmaßnahmen. Neben sicheren Passwörtern, einem professionellen Anti-Viren-Programm und regelmäßigen Backups auf separaten Datenträgern stellt die Hardware-Firewall einen wichtigen und äußerst wirkungsvollen Baustein zur Absicherung Ihrer Praxis-IT dar.

Auf unserer Website finden Sie weitere Informationen zum Thema IT-Sicherheit.