Tipps für eine sichere Praxis-IT

Ein Beitrag von Frank Dastych, Vorstandsvorsitzender der KV Hessen

Bevor wir in der nächsten Ausgabe mit Fachartikeln ausgewiesener IT-Experten so richtig in unsere Serie zur Cybersicherheit einsteigen, möchte ich Ihnen heute ganz persönlich und – sozusagen von Arzt zu Arzt – ein paar Empfehlungen mitgeben.

Unsere Praxen sind bedroht:
Es gibt eigentlich keinen Tag, an dem das Thema IT- und Cyber-Sicherheit nicht an Bedeutung gewinnt. Es gibt nun mal kaum noch eine Praxis, die wirklich ohne Online-Anbindung arbeiten kann. Von der Online-Übermittlung der Abrechnung über das PVS-Update bis hin zur nutzlosen TI-Anbindung: Einen Breitbandanschluss braucht faktisch jeder. Fatal ist es, wenn man dann glaubt, in der eigenen Praxis vor dem Thema Cybersicherheit davonlaufen zu können. Man muss sich mit dem Thema beschäftigen und verstehen, welche Gefahren da eigentlich drohen. Und man muss wissen, dass sich die eCrime-Landschaft ständig weiterentwickelt und eine zunehmende Spezialisierung erlebt.

Das vor Augen, ist die Strategie dagegen gar nicht mehr so schwer und aufwendig: Regelmäßige Updates von Betriebssystemen, der Virenschutzsoftware und der Firmware der Router; klare Spielregeln beim Umgang mit dem Internet in der Praxis für alle, also auch für die Praxisinhaber; individuelle Passwörter für alle, Bildschirmschoner mit Sperrfunktion, Trennung der Online-Funktionen, wie E-Mail-Verkehr, vom PVS-System; sichere Backup-Systeme, die einen Schutz vor Verschlüsselungstrojanern und Erpressung bieten, und vielleicht doch eine professionelle Firewall anstelle des Standard-Routers. Mit diesen Maßnahmen erreicht man schon viel.

Zur konkreten Umsetzung in meiner Praxis:
Natürlich haben wir immer die aktuellste Software auf unseren Rechnern und der Hardware. Privates Surfen auf den Praxiscomputern ist ein No-Go. Niemand macht Anhänge von E-Mails auf, niemand antwortet auf E-Mails. Schon gar nicht auf solche, die irgendwelche Passwörter anfordern. Die Datensicherung erfolgt unabhängig vom System, sodass Ransomware dort nicht angreifen kann. Ransomware verschlüsselt die Daten und erpresst dann den Betroffenen, der wieder an seine Daten kommen möchte. Deshalb ist es ratsam, dass das Backup nicht „online" am PC hängt und im Falle eines Angriffs mitverschlüsselt wird.

Wichtig ist: Man sollte seine Mitarbeiterinnen und Mitarbeiter immer wieder daran erinnern, erinnern, erinnern. Dazu kommt noch der Schutz der Sozialdaten, beispielsweise durch blicksichere Bildschirmarbeitsplätze. Bildschirmschoner mit Sperrfunktionen, die nicht erst nach 20 Minuten angehen, sind ein Muss. Wir beziehen Software nur aus vertrauenswürdigen Quellen. Und auf unsere Praxiscomputer

gehört nur das drauf, was drauf muss. Dazu gehören bei uns halt auch regelmäßige Hardware-Investitionen, auch wenn die wehtun. Und wenn man mehrere Standorte hat, dann braucht man auch richtig professionelle Firewalls.

Warum die IT-Infrastruktur einer Praxis nie „fertig" ist:
Das ist wie ein Rennen zwischen Hase und Igel. Die eCrime-Landschaft entwickelt sich ständig weiter und erlebt eine zunehmende Spezialisierung. Das sind keine Script-Kiddies im Kinderzimmer mehr, das sind hochprofessionelle und hochkriminelle Profis. Und wie wir bei diversen Angriffen auf manche Krankenhäuser gesehen haben: Die nehmen auch Tote in Kauf.

Wir sind da leider immer die Igel. Es kommt nur darauf an, dass wir den Abstand nicht zu groß werden lassen und den Hasen stets im Auge behalten.

Man muss sich darüber im Klaren sein: Es geht zum Beispiel gar nicht mal so sehr um die illegale Weiterverwertung Ihrer Daten, also das angebliche Hacken der Praxis. Ihr ganzes Unternehmen steht auf dem Spiel, wenn alle Daten unwiederbringbar verschlüsselt sind. Der Verschlüsselungstrojaner greift da so nebenbei auch noch die Zugangsdaten zum Onlinebanking ab. Super. Und die netten Damen und Herren in Nordkorea oder wo auch immer wissen dann auch gleich, was auf dem Bankkonto ist, um die Lösegeldforderung individuell anzupassen. Wenn Sie überhaupt den Entschlüsselungscode nach Zahlung eines Lösegeldes bekommen.

Zur Telematik-Infrastruktur (TI) und ihren Anwendungen:
Das ist eine ganz eigene Welt. Die ist zwar an sich sicher und kann auch sicher installiert werden. Sie ersetzt aber nicht die sonst benötigte Online-Anbindung der Praxis. Der sichere Internetservice (SIS) in der TI ist keine wirkliche Alternative. Dadurch wird eine sonst unsichere Praxis nicht sicherer. Installiert man die TI-Komponenten, insbesondere den Konnektor, auch noch falsch, kann das womöglich komplett schiefgehen.

Mein Rat: IT-Beratung, aber richtig:
Leider gibt es kein Patentrezept, weil sich jeder in Deutschland IT-Sicherheitsspezialist oder IT-Sicherheitsberater nennen kann, auch wenn er keine wirkliche Ahnung davon hat. Da gibt es absolut nichts, was irgendwo einheitlich geregelt ist. Wobei man das natürlich nicht mit der Welt der Datenschutzbeauftragten verwechseln darf!

Lassen Sie sich also am besten die Referenzen eines solchen Unternehmens zeigen, wenn Sie Hilfe bei der IT-Sicherheit brauchen. Fragen Sie ruhig mal nach, verschaffen Sie sich einen persönlichen Eindruck. Machen Sie sich selber ein bisschen schlau zum Thema ISMS, also Informationssicherheitsmanagementsystem, und den BSI IT-Grundschutzkatalogen, um Dampfplauderern schnell den Wind aus den Segeln zu nehmen. Haben Sie bereits einen (externen) Datenschutzbeauftragten, kann der vielleicht bei der Bewertung eines IT-Sicherheitsdienstleisters helfen.

Sonst sind Sie nicht nur der Igel, sondern werden auch noch die Weihnachtsgans, die man so richtig ausnehmen kann. Und ich selber würde nie ein Unternehmen beauftragen, das nur Arztpraxen betreut. Ob daran auch die kommende Zertifizierung der IT-Dienstleister durch die KBV jemals was ändert? Ich habe da so meine Zweifel. ■

Frank Dastych,
Vorstandsvorsitzender der KV Hessen