online ist. Das passiert 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 hundert Male am Tag angegriffen“, berichtet Sicherheitsexperte Grün. Das funktioniert 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, Internetbrowser 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 Model-

len 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

Cyber-Kriminalität: Jedem Zweiten fehlt das Notfallkonzept

Eine aktuelle Studie bringt verheerende Lücken im Notfallmanagement kleiner Betriebe ans Licht. Das gilt auch für Arztpraxen.

Gut die Hälfte aller Unternehmen in Deutschland ist in den vergangenen zwei Jahren Opfer von digitaler Spionage, Sabotage oder Datendiebstahl geworden. Dabei rangiert das Gesundheitswesen auf Platz vier der Top 5 der am stärksten betroffenen Branchen (58 %), die Versicherungen auf Rang drei (60 %). Häufigstes Angriffsziel und damit Haupteinfallstor sind die IT-Systeme und die Kommunikationsinfrastruktur der Betriebe. Das zeigen die Ergebnisse einer repräsentativen Umfrage des Hightech-Verbands BITKOM, für die Geschäftsführer und Sicherheitsverantwortliche von 1.074 Unternehmen interviewt wurden. Demnach sind mittelständische Unternehmen – zu denen

auch Praxen zählen – mit 61 % am stärksten von Spionage- oder Sabotageakten betroffen.

Problematisch ist vor allem, dass die Unternehmen keine ausreichenden Notfallkonzepte vorhalten. Alle befragten Unternehmen verfügten zwar über einen Grundschutz, bestehend aus Virenscannern, Firewalls und regelmäßigen Updates aller Programme. Dies sollte laut BITKOM aber durch spezielle Angriffserkennungs- und Verschlüsselungssysteme ergänzt werden. Ein Notfallmanagement für den tatsächlichen Krisenfall konnten nur 49 % vorweisen – und das, obwohl schnelles Handeln im Krisenfall unbedingt notwendig ist. Zu den Zielen des Notfallmanagements ge-

höre es etwa, einen Datenabfluss zu stoppen oder beim Ausfall wichtiger Systeme die Arbeitsfähigkeit des Betriebs so schnell wie möglich wieder herzustellen, so der BITKOM. „Die Maßnahmen zur Vorbereitung eines Notfallmanagements reichen vom Erstellen einer Kontaktliste mit den wichtigsten Ansprechpartnern bis zu mehrtägigen Übungen, bei denen verschiedene Szenarien durchgespielt werden“, sagt BITKOM-Hauptgeschäftsführer Dr. Bernhard Rohleder.

Noch zu wenig wird laut Verband auch getan, um die Mitarbeiter für Risiken aus dem Web zu sensibilisieren. Nur 52 % der Befragten führten Schulungen der Mitarbeiter durch – das betreffe auch Bereiche wie die richtige Verwendung von Zugangsdaten oder den korrekten Umgang mit externen Datenträgern.

Rebekka Höhl

Weitere Infos zum IT-Notfallmanagement und einen Selbsttest für Betriebe finden Sie im IT-Sicherheitsblog für den Mittelstand: www.dsin-blog.de/