Moritz Eckert
Hausarzt in Herzberg

Daniel Köhler
IT-Dienstleister aus Sarstedt

Rauchende Köpfe

Hinter den *Rauchenden Köpfen* stecken vier Praxiserfahrene, die sich unermüdlich dafür einsetzen, die Bürokratie im Praxisalltag zu minimieren: Dr. Christoph Claus, Moritz Eckert, Dr. Sabine Frohnes und Timo Schumacher.
Aus ihrer Feder stammen etwa die bekannten EBM- und GOÄ-Spicker. Tipps zu Abrechnung und Regressschutz publizieren sie in jeder Ausgabe von *Hausärztliche Praxis*.

Porträts: Eckert (o.), Köhler (u.), Foto: iStock.com/RollingCamera

Waches Team schützt vor IT-Knock-out am besten

Die IT-Sicherheitsrichtlinie bringt für Praxen teils Vorgaben mit sich, die eher in Firmen Standard sind – doch diese haben dafür eine eigene IT-Abteilung. Wie gerade kleine und mittlere Praxen die Richtlinie praktikabel umsetzen können, haben die Rauchenden Köpfe und IT-Experte Daniel Köhler überlegt. Fest steht: Ein geschultes Praxisteam ist das beste Schutzschild gegen IT-Angriffe.

Johanna Dielmann-von Berg

Seit 1. Oktober greift die geänderte IT-Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung (KBV) für Praxen (S. 16). Deren Vorgaben sind zwar umsetzbar – vieles davon ist etwa in größeren Büros oder Firmen längst Standard, diese werden in der Regel aber von größeren IT-Dienstleistern oder eigenen IT-Abteilungen unterstützt. Gerade für kleinere und mittlere Praxen können die Vorgaben teils so ambitioniert sein, dass sie sich dadurch künftig noch stärker an IT-Dienstleister binden müssen (etwa mit Blick auf Software-Updates/Patchmanagement oder Server- und E-Mail-Sicherheit).

Merke: Wichtig ist, dass alle Praxen das Einmaleins eines soliden Basisschutzes umsetzen. Der Grundschutz unterscheidet sich von Praxis zu Praxis nämlich sehr stark, weiß IT-Experte Daniel Köhler aus seiner Erfahrung. Sofern aber der Grundschutz gewährleistet ist – und an Firewall oder Fritzbox nicht „rumgepfuscht" wurde, sei eine Arztpraxis „von außen" ziemlich sicher.

Wichtig: Die besten Abwehrschilde gegen IT-Angriffe sind die Mitarbeitenden. Es gilt die einfache Grundregel: Wird keine Schadsoftware angeklickt, kann sie in der Praxis-IT auch keinen Schaden anrichten. Daher legt auch die IT-Sicherheitsrichtlinie jetzt zurecht so großen Wert auf die regelmäßige Schulung des Praxisteams.

Diesen Schutz braucht jeder

Zum Einmaleins der Schutzausrüstung besonders für kleine und mittlere Praxen zählen Moritz Eckert von den *Rauchenden Köpfen* und Daniel Köhler zunächst vier Punkte, die jede Praxis einrichten sollte (für Großpraxen gelten höhere Standards!):

1. Einrichtung eines Routers und einer Firewall, die aktuell gehalten werden. Legt man die IT-Sicherheitsrichtlinie wörtlich aus, reicht laut Köhler aber auch eine Fritzbox als Firewall.

Merke: Alle Ports von außen sollten geschlossen sein.

2. Das WLAN für die Praxiskommunikation sollte, wenn überhaupt, **getrennt** von einem WLAN für Mitarbeitende oder Patientinnen und Patienten eingerichtet sein. Dabei sollte der Zugang zum Router immer für die Öffentlichkeit unzugänglich sein, sodass beispielsweise Patienten gar nicht auf die Idee kommen können, sich im Wartezimmer über den Schlüssel auf dem Router ins Netz einzuwählen.

3. Installation eines aktuellen Virenscanners. Praxen, die Windows nutzen, können hier auch den von Windows mitgelieferten Microsoft Defender einsetzen. Dieser hat in der Regel ein ausreichendes Schutzniveau für Praxen und wird von Windows auf die neuesten Schadprogramme aktualisiert. Er schneidet auch immer wieder in unabhängigen Tests sehr gut ab.

4. Regelmäßige Schulung des Praxispersonals. Je besser die Mitarbeitenden für IT-Gefahren und deren Verhinderung sensibilisiert sind, desto besser ist eine Praxis geschützt. Oder vereinfacht gesagt: Wenn etwa niemand in der Praxis auf etwas Falsches in einer E-Mail/KIM-Nachricht klickt, kann der Praxis nichts passieren.

Zudem sollte jede Praxis einen Plan des eigenen Netzwerks besitzen, dies kann etwa helfen, die Folgen in einem IT-Notfall schneller abzuschätzen. Dies schreibt auch die IT-Sicherheitsrichtlinie vor. Die KBV gibt dazu ein Beispiel an die Hand. Dieses ist jedoch nur ein Beispiel, wie so etwas aussehen kann.

Wichtig: Ein Netzplan muss immer individuell auf eine Praxis angepasst sein und deren genaue Konfiguration aufzeigen. Das ist für Praxen in der Regel nur mithilfe ihres IT-Dienstleisters machbar.

Rechte und E-Mail-Sicherheit

Gerade weil das Personal gleichzeitig das beste Schutzschild und der beste Angriffspunkt ist, sollte sich jede Praxis über Nutzerprofile mit unterschiedlichen Rechten Gedanken machen. So sollten essenzielle Funktionen Chefsache sein – also eine Fernwartung der Praxis-PC sollten nur Sie als Chefin oder Chef freigeben dürfen!

Merke: Große Unternehmen wie Microsoft,

Foto: x, y

Apple oder Google werden nie von sich aus bei Ihnen anrufen und Zugriff auf Ihren Rechner verlangen.

Die größte Bedeutung kommt dem Praxispersonal im Umgang mit E-Mails/KIM-Nachrichten zu. Denn hier ist ein höheres technisches Sicherheitslevel für Praxen bislang nur aufwändig zu realisieren. Das Problem: Es gibt für die E-Mail-Sicherheit sehr gute Lösungen, die an Microsoft oder andere Softwareanbieter andocken. Diese können bei Praxen aber nicht eingerichtet werden, weil Praxisdaten potenziell gesundheitssensible Informationen enthalten können und diese nicht in der Cloud dieser Anbieter landen dürfen.

Schutzstufe je nach Sicherheitsbedürfnis

Aufsetzend auf diesem Einmaleins des IT-Schutzes hängt es vom jeweiligen Sicherheitsbedürfnis (oder für größere Praxen auch Vorgaben der Richtlinie) ab, welche Schutzstufe Praxen für sich einrichten. Köhler unterscheidet in seinem Konzept dabei drei bis vier Schutzstufen.

Wichtig: Für die Wahl der Schutzstufe ist auch die Sensibilität und Kompetenz des Personals ausschlaggebend! Je geringer der „physische" oder technische Schutz, desto mehr Sicherheitsverantwortung verlagert sich aufs Team.

Stufe 1: Basisschutz

Wer diese Stufe wählt, setzt vor allem auf sein Praxisteam bei der IT-Sicherheit. Hier werden die Maßnahmen des Einmaleins dahingehend verfeinert, dass die Funktionalität des Virenscanners maximal erhöht wird. Dieser sollte sich immer noch einmal zwischenschalten, wenn Links oder Dokumente aus E-Mails geöffnet werden. Zudem können bei manchen Virenscannern auch Filter für Webseiten hinterlegt werden, um den Virenschutz zu steigern. Ansonsten werden in dieser Stufe bei Router oder Firewall keine besonderen Konfigurationen („über das Normale hinaus") veranlasst, vereinfacht gesagt: Alles ist frei. Es kann auf jegliche Webseiten etc. zugegriffen werden – hier findet keine Blockade oder Vorfilterung statt.

Daher ist die regelmäßige Schulung (und ggf. auch Prüfung der Mitarbeitenden) bei diesem Vorgehen extrem relevant. Besonders der richtige Umgang mit Spam und Phishing bei E-Mails sollte sitzen – langfristig ist laut Köhler davon auszugehen, dass auch bei KIM ähnliche Fake-Nachrichten wie per E-Mail erkannt werden müssen.

Köhler erklärt: „Viele glauben, dass bereits mit dem Öffnen einer E-Mail etwas passiert. Das ist aber nicht so. Man kann im Postfach jede Nachricht anklicken und lesen, sofern aktuelle E-Mail-Programme eingesetzt und sicher konfiguriert sind. Wenn einem dann daran etwas komisch vorkommt, sollte man sie direkt löschen."

Wichtig: Keinesfalls sollten aber Links oder angehängte Dateien ohne Prüfung geöffnet werden. Laden Sie nie Dateien einfach herunter und installieren sie diese, erinnert Köhler. Die KBV-Schulung sei ein Anfang, sollte aber ausgebaut werden. So enthalte sie wenig Training zum Umgang mit Spam/Phishing, etwa woran man dies erkennt.

Zwischenstufe: getrennte Netze

Zwischen Stufe 1 und 2 ist eine weitere Variante denkbar, die für die meisten Praxen aber im Alltag wenig praktikabel sein dürfte, schätzt Eckert. Hier würde die Praxis vom Netz getrennt und das Surfen wäre nur über einen separaten PC oder Tablet möglich. Alternativ könnte man eine „Sandbox" aufbauen, also eine isolierte, virtuelle Umgebung, in der etwa Dateien geöffnet werden, ohne dass sie dem Hauptsystem schaden können. Laut Köhler ist es in den meisten Praxen aber unrealistisch, für das Öffnen von E-Mails und dem restlichen Praxisbetrieb ständig zwischen normaler und Sandbox-Umgebung zu wechseln.

Stufe 2: Ausgang durch Filter

Soll das Team technisch etwas mehr unterstützt werden als in Stufe 1, kann auch die Möglichkeit der Praxis zum Surfen im Netz begrenzt werden. Das heißt, bei der Firewall sind von außen alle Ports geschlossen. Wenn von innerhalb der Praxis nach draußen kommuniziert wird, durchläuft dieses erstmal einen Contentfilter. Der Virenscanner kann in seiner Standardkonfiguration bleiben oder maximiert (Stufe 1) werden.

In der Firewall würde also ein Contentfilter eingerichtet, der ständig auf Neuerungen aktualisiert wird. Hier hat in der Regel jede Firewall eigene Filterlisten, die meist lizenziert werden müssen. „Wenn jemand im Internet surft oder E-Mails bearbeitet, geht es immer durch diesen Filter", so Köhler.

Wichtig: Lassen Sie sich vom IT-Dienstleister in die Handhabung einweisen. Der Nachteil: Ein guter Contentfilter kostet.

Stufe 3: Fort Knox

Alle Internetzugänge zur Praxis über die Firewall sind von außen wie von innen erstmal dicht. Gesurft werden kann zum Beispiel dann nur auf Webseiten, die Praxischefin oder -chef freigegeben haben. Diese Webseiten werden aktiv in der Firewall freigegeben. Der Virenscanner behält die Standardkonfiguration.

Theoretisch ist es laut Köhler möglich, dass alle E-Mails zuerst an die Firewall gehen und nur im E-Mail-Programm auftauchen, wenn diese „sauber" sind. „Das ist aber nur praxisindividuell und sehr aufwändig – und damit entsprechend teuer – einzurichten."

Der Nachteil liegt für Eckert auf der Hand: Im Praxisalltag wird manch Banales wie Adresssuchen viel umständlicher. ●

Ihre Fragen

Haben Sie Fragen zur Abrechnung oder Praxisführung?

Mailen Sie der Redaktion: **info@medizinundmedien.eu**