IT-Sicherheit in der Praxis selbst anpacken

IT-Sicherheit Hehre Ziele gibt es viele. Manche sollte man nicht nur mit guten Vorsätzen angehen, sondern mit einem handfesten Plan. Zu diesen gehört die IT-Sicherheit. Wir zeigen Ihnen, wie Sie diese in Ihrer Praxis schrittweise und pragmatisch selbst optimieren können, angefangen mit einem IT-Inventar und einem Sicherungsplan.

Uwe Gempp, Philipp Senn

Ein Cyberangriff ist für eine Arztpraxis ein existenzbedrohendes Szenario. Zum einen, weil Tage oder Wochen vergehen können, bis der Betrieb wieder normal funktioniert. Zum andern, weil das Vertrauen der Patientinnen und Patienten nachhaltig geschädigt wird, wenn diese ihre Krankengeschichte im Internet wiederfinden. Wie ist es bei Ihnen, wären Sie auf ein solches Ereignis vorbereitet? Verlassen Sie sich als Ärztin, Praxisinhaber, Unternehmerin eher auf Ihr Glück oder helfen Sie diesem mit Planung und System auf die Sprünge?

Als Ärztin oder Arzt schultern Sie die Verantwortung für die sensiblen Daten Ihrer Patientinnen und Patienten. Möchten Sie zu deren Schutz die IT-Sicherheit Ihrer Praxis verbessern, sind aber nicht sicher, wo Sie beginnen sollen? Als erster Schritt zu einem Ihrer Praxis angemessenen Schutzkonzept [1] sollten Sie sich einen Überblick verschaffen. Sie legen die Basis mit einem aussagekräftigen IT-Inventar. Dieses lässt sich auch gleich für eine erste Anwendung nutzen: den Aufbau einer Backup-Strategie.

Transparenz herstellen: Am Anfang war das Inventar

Eine der grössten Herausforderungen für die Datensicherheit in Arztpraxen ist die mangelnde Transparenz der IT-Landschaft. Ohne einen Überblick über die eingesetzten Geräte, Daten und Systeme ist es unmöglich, ein wirksames Schutzkonzept umzusetzen. Die Lösung für dieses Problem ist ein umfassendes IT-Inventar, welches die Hardware- und Software-Ressourcen der Praxis verzeichnet.

Für das IT-Inventar werden zunächst alle Geräte erfasst, beginnend mit den Computern, ebenso Datenträger wie USB-Sticks oder externe Festplatten, Labor- und andere medizinische Geräte. Dazu können Sie unsere Excel-Vorlage [2] verwenden, die Sie am Ende dieses Artikels verlinkt finden. Für jedes Gerät werden Angaben wie Verwendungszweck, Standort, verantwortliche Benutzer, enthaltene Daten und eingesetzte Software-Versionen (Betriebssystem, Antivirus, Anwendungen) festgehalten.

Die Angaben im Inventar sollten mindestens jährlich überprüft und aktualisiert werden [3]. Neue Geräte werden umgehend ins Inventar aufgenommen, nicht mehr verwendete aus dem Inventar entfernt (oder mit einem Hinweis «nicht mehr in Betrieb» versehen). Bei Geräten, die ausser Betrieb genommen wurden, muss sichergestellt werden, dass sämtliche Daten vollständig und unwiderruflich gelöscht wurden, bevor sie entsorgt werden. Wir raten davon ab, nicht mehr benötigte Geräte weiterzugeben oder zu verkaufen [4].

Backup mit der 3-2-1-Regel

Als Goldstandard für eine Backup-Strategie hat sich die 3-2-1-Regel bewährt [7]. Auch Sie können diese in Ihrem Sicherungsplan umsetzen:

- 3 Kopien aller wichtigen Daten aufbewahren (1 Original und 2 Backups)
- 2 unterschiedliche Backup-Medien verwenden (z.B. 1 externe Festplatte und 1 sicherer Cloudspeicher)
- 1 Datensicherung an einem räumlich von der Praxis getrennten Standort lagern (z.B. im privaten Safe)

Mit der 3-2-1-Regel erhöhen Sie die Ausfallsicherheit Ihrer Backups um ein Vielfaches. Auch wenn ein Brand die Praxis verwüstet oder der Cloudbetreiber Konkurs geht, bleiben die Daten intakt und zugänglich. Erfunden wurde die Regel übrigens nicht von einem IT-Spezialisten, sondern von einem selbst von Datenverlust betroffenen Anwender.

IT-Inventar nutzbar machen: der Sicherungsplan

Das IT-Inventar um seiner selbst willen zu pflegen, ist nicht unser Ziel. Vielmehr wollen wir es gleich ein erstes Mal produktiv einsetzen – und entwickeln eine Backup-Strategie. Diese ist eine Schlüsselkomponente unseres Schutzkonzepts [5]. Sie stellt sicher, dass wichtige Daten bei einem Sicherheitsvorfall – sei es ein Ransomware-Angriff, Brand, Wasserschaden oder Diebstahl – wiederhergestellt werden können. Indem festgelegt wird, welche Daten und Geräte gesichert werden müssen, auf welches Speichermedium und in welchen Abständen, kann die Praxis das Risiko eines Datenverlusts minimieren und dazu beitragen, dass der Betrieb nach dem Vorfall rasch wieder aufgenommen werden kann.

Ermitteln Sie zunächst, welche Daten für den Praxisbetrieb am wichtigsten sind und daher im Sicherungsplan Vorrang haben sollen. Dazu können Krankengeschichten, Finanzdaten und alle anderen Informationen gehören, die für den täglichen Betrieb der Praxis unentbehrlich sind. Diese sollten somit auch tagesaktuell gesichert werden. Bei weniger wichtigen oder weniger veränderlichen Daten genügen allenfalls wöchentliche oder monatliche Sicherungszyklen. Ist diese Frage geklärt, lässt sich daraus Ihr Speicherbedarf und der geeignete Zeitplan ableiten. Als Ort für das Backup empfehlen wir externe Festplatten. Diese sollten möglichst ausserhalb der Praxisräumlichkeiten und gut verschlossen aufbewahrt werden (siehe Box). Eine Sicherung in der Cloud ist ebenfalls möglich, unterliegt jedoch strengen Vorschriften, die sich aus dem Datenschutzgesetz und der beruflichen Geheimhaltungspflicht ergeben [6].

Da Sie nun Ihren Sicherungsplan erstellt haben, ist es an der Zeit, ihn umzusetzen. Automatische Backups lassen sich mithilfe von Software-Tools einrichten. Nehmen Sie hier im Zweifel die Unterstützung einer Fachperson in Anspruch. Ihre Backups sollten Sie regelmässig testen (lassen) – mindestens jährlich. Denn nichts ist nutzloser, als eine Sicherung, aus der sich die Daten im Fall der Fälle nicht wiederherstellen lassen.

Zusammenfassung: IT-Inventar und Backup-Strategie

- Listen Sie Ihre Geräte auf – angefangen mit Ihren Computern – mithilfe der Excel-Vorlage.
- Erfassen Sie die Angaben zu den Geräten sowie die Daten, die auf jedem Gerät gespeichert sind.
- Erstellen Sie anhand der Informationen aus dem IT-Inventar einen Sicherungsplan. Dieser enthält mindestens den Datenbestand, das Speichermedium und die Backup-Zyklen.
- Implementieren Sie den Sicherungsplan mittels Konfiguration der Speichermedien und Einrichtung automatischer Backups.
- Spielen Sie einmal im Jahr die Daten aus Ihren Backups testweise wieder zurück, um sicherzustellen, dass diese ordnungsgemäss funktionieren.

Mit dieser Bestandsaufnahme und der neuen Backup-Strategie haben Sie nicht nur das grundlegende Problem der Transparenz Ihrer IT-Landschaft gelöst, sondern auch den Grundstein gelegt für ein solides IT-Schutzkonzept. Durch die Erstellung eines Inventars von Geräten und Daten und die Verwendung dieser Informationen für die Umsetzung eines Sicherungsplans schützen Sie Ihre Praxis vor den Risiken eines Datenverlusts und stellen ihren Weiterbetrieb im Krisenfall sicher. Auf support.hin.ch sind weitere Anleitungen, Checklisten und Antworten auf häufige Fragen zum Thema IT-Sicherheit abrufbar, die zur Erweiterung des Schutzkonzepts herangezogen werden können.

© Kmitu / Dreamstime

Schlüsselelemente eines IT-Schutzkonzepts sind Inventar und Backup.

Korrespondenz
philipp.senn[at]hin.ch

Literatur
Vollständige Literaturliste unter www.saez.ch oder via QR-Code

Uwe Gempp
ist Chief Security Officer (CSO) und IT-Architekt bei Health Info Net AG (HIN).

Philipp Senn
ist Projektleiter Communication und IT Security / Awareness Referent bei Health Info Net AG (HIN).