

Cyberattacke, Stromausfall, Wasserschaden: Sind Sie vorbereitet?

Was wäre, wenn Sie plötzlich aufgrund einer Cyberattacke nicht mehr auf die Patientendaten Ihrer Praxis zugreifen können? Oder wenn Ihre IT-Systeme unerwartet ausfallen? Unangenehme Fragen. Die man sich trotzdem stellen sollte.

Patientengespräche, Berichte schreiben, Terminkoordination... Für «Was-wäre-wenn»-Fragen bleibt im Alltag von Gesundheitsfachpersonen kaum Zeit. Doch unvorhergesehene Ereignisse können eintreten. Cyberangriffe, der Ausfall von IT-Systemen, der Befall eines Endgerätes mit Schadsoftware, Stromausfälle oder Naturereignisse sind nur einige Beispiele für mögliche Notsituationen. Ist man auf sie nicht vorbereitet, können sie schwerwiegende Konsequenzen haben, den Betrieb stunden- oder tagelang lahmlegen, das Vertrauen der Patienten schädigen oder gar rechtliche Konsequenzen mit erheblichen finanziellen Folgen nach sich ziehen. Dieser Beitrag gibt Inputs, wie Sie sich und Ihre Praxis auf den Ernstfall vorbereiten können.



Notfallplan erstellen

Stellen Sie sich vor, Sie kommen am Morgen in Ihre Praxis und die Patientendaten sind aufgrund eines Ransomware- Angriffs nicht mehr zugänglich. Was tun Sie? Rufen Sie Ihren IT-Partner an? Sagen Sie besser zuerst die ersten Patientenkonsultationen ab? Welche Aufgaben übernimmt Ihre MPA? Um sich all diese Fragen nicht in der Hitze des Gefechts – gestresst und aufgebracht – stellen zu müssen, lohnt es sich, für mögliche Ausnahmesituationen einen Notfallplan bereit zu haben.

So funktioniert es:

- Identifizieren Sie potenzielle Bedrohungen mittels einer Risikoanalyse, die Sie selbst nach bestem Wissen und Gewissen durchführen. Bewerten Sie dabei die Wahrscheinlichkeit und den möglichen Schaden jedes dieser Szenarien.
- Ermitteln Sie auch Schwachstellen in Ihrer Praxis, die zu einem Notfall führen könnten und beheben Sie diese selbst oder mithilfe eines externen ITPartners.
- Basierend auf Ihrer Risikoanalyse entwickeln Sie einen schriftlichen Notfallplan, der Anweisungen für relevante Szenarien enthält. Verschiedene Szenarien mit ähnlichen Konsequenzen können Sie kategorisieren und für jede Kategorie einen Handlungsplan erstellen. Wichtig: Legen Sie die Verantwortlichkeiten klar fest, damit jeder Mitarbeitende seine Zuständigkeiten kennt.
- Regeln Sie auch die Kommunikation in einer Krisensituation: Wie, wann und durch wen werden Teammitglieder, Patienten, IT-Dienstleister und andere Anspruchsgruppen informiert? Beachten Sie, dass die Notfallkommunikationskanäle nicht die gleichen sein sollten, die Sie im Arbeitsalltag nutzen, da diese eventuell ebenfalls nicht mehr funktionieren. Auch ist es wichtig, dass eine stets aktuelle Kontaktliste jederzeit verfügbar ist.

Schulen, überprüfen und anpassen

Je geübter Ihre Mitarbeitenden im Umgang mit Ausnahmesituationen sind, desto sicherer und effizienter können sie im Ernstfall handeln. Regelmässige Notfallübungen schulen Ihr Team und stellen sicher, dass Ihr Notfallplan in der Praxis funktioniert. Ebenfalls ist es wichtig, den Plan regelmässig zu überprüfen: Entspricht er noch den aktuellen Anforderungen und Risiken? Muss er allenfalls an neue Technologien oder Änderungen in der Praxis angepasst werden? Daten absichern Cyberattacken zielen nicht selten darauf ab, betriebsrelevante Daten zu stehlen, und auch Vorfälle wie ein Wasserschaden, ein Brand im Serverraum oder der Konkurs des Cloud-Betreibers können zu vollständigem oder teilweisem Datenverlust führen. Eine zuverlässige Datensicherung ist deshalb elementar, um alle wichtigen Daten im Ernstfall wiederherstellen zu können. Implementieren Sie regelmässige Backups: Ermitteln Sie hierfür zunächst, welche Daten für den täglichen Betrieb in Ihrer Praxis unentbehrlich sind, zum Beispiel Krankengeschichten oder Finanzdaten. Diese haben im Sicherungsplan Vorrang und sollten tagesaktuell gesichert werden. Bei weniger wichtigen oder weniger veränderlichen Daten genügen allenfalls wöchentliche oder monatliche Sicherungszyklen. Stellen Sie sicher, dass Ihre Daten auch an einem sicheren, von den Hauptsystemen getrennten Ort gespeichert werden und testen Sie die Datenwiederherstellung regelmässig.

Als Goldstandard für eine Backup-Strategie hat sich die 3-2-1-Regel bewährt:

- 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)

Für eine zuverlässige Datensicherung lohnt es sich, eine externe IT-Fachperson zu Rate zu ziehen.

Externe Unterstützung sicherstellen

Im Notfall bleibt keine Zeit zu warten... Stellen Sie deshalb sicher, dass Ihnen im Fall des Falles externe IT- Unterstützung schnell und zuverlässig zur Verfügung steht. Es lohnt sich, mit Ihren IT-Dienstleistern Service- Level-Agreements (SLAs) abzuschliessen, welche etwa die zugesicherten Leistungen und die Reaktionszeiten definieren.

Unangenehme Fragen, die zu stellen sich lohnt

Die Vorbereitung auf mögliche Krisenszenarien braucht Zeit und vor allem Kopfarbeit. Doch auch wenn die meisten dieser Szenarien (hoffentlich!) niemals eintreffen werden: Im Fall des Falles liefert eine sorgfältige Vorbereitung Antworten auf die schwierigen Fragen. Hilfreiche Antworten, die dazu beitragen, den Betrieb sicherzustellen und die Sicherheit sensibler Patientendaten zu gewährleisten.

Externe IT-Partner: Darauf gilt es zu achten

Die Unterstützung durch externe IT-Dienstleister ist für eine effiziente und datenschutzkonforme IT-Infrastruktur fast unumgänglich. Der gewählte Partner muss die Anforderungen des neuen Datenschutzgesetzes (nDSG) erfüllen und die Sicherheit und den Schutz der Patientendaten gewährleisten. Deshalb sollte er...

- ... nachweisen können, dass er alle relevanten Datenschutzanforderungen einhält, insbesondere im Hinblick auf die Sicherheit der Verarbeitung personenbezogener Daten. Dies erkennen Sie am einfachsten an seinen Sicherheitszertifizierungen, z.B. ISO /IEC 27001 (Informationssicherheitsmanagement) oder Label CyberSeal der Allianz Digitale Sicherheit Schweiz.
- ... dokumentierte technische und organisatorische Massnahmen (TOM) vorweisen können, welche die Sicherheit der Datenverarbeitung gewährleisten, z.B. Nutzung von Verschlüsselung, Zugriffssteuerungen, regelmässige Sicherheitsüberprüfungen.
- ... Erfahrung in der Arbeit mit sensiblen Daten im Gesundheitswesen haben.
- ... Ihrer Praxis das Recht einräumen, regelmässige Audits und Überprüfungen durchzuführen.
- ... seine Mitarbeitenden regelmässig in Bezug auf Datenschutz und IT-Sicherheit schulen.
- ... definierte Reaktionszeiten und ein dokumentiertes Notfallmanagement vorweisen können.
- ... eine Datenschutz-Folgenabschätzung durchführen oder unterstützen können.

Diese Vereinbarungen sollten Sie mit Ihrem IT-Partner treffen:

- Vertraulichkeitsvereinbarung (Non-Disclosure Agreement, NDA): Diese stellt sicher, dass alle Mitarbeitenden, die Zugang zu Patientendaten haben, zur Verschwiegenheit verpflichtet sind.
- Auftragsdatenverarbeitungsvereinbarung (ADV): Diese regelt, wie der IT-Dienstleister die Daten verarbeiten darf und schützen muss.
- Vorlagen für beide Vereinbarungen stellt die FMH zur Verfügung.

Daniel Huser

Bereichsleiter Projektmanagement & IT-Architektur

Health Info Net AG
Seidenstrasse 4
8304 Wallisellen
Telefon 0848 830 740
daniel.huser@hin.ch
www.hin.ch