Sind die Daten meiner Patienten in meiner Zahnarztpraxis sicher?

Der Missbrauch von vertraulichen Daten jedweder Art durch Unbefugte, ist bei genauerer Betrachtung eine Horrorvorstellung. Doch es gibt noch ein anderes Szenario, das nicht unbedingt weniger erschreckend ist. Stellen Sie sich vor, alle Patientendaten sind von einem Augenblick zum anderen nicht mehr verfügbar. Der Praxisbetrieb käme zum Erliegen.

Weder das Risiko des Datenmissbrauchs noch ein Datenverlust lassen sich zu 100% ausschließen. Auch wenn alle IT-Systeme korrekt installiert, die Mitarbeiter geschult und die geltenden Sicherheitsanforderungen der Kassenärztlichen Vereinigung erfüllt sind, kann es passieren, dass unbeabsichtigt oder durch technische Ausfälle die Praxis zum Erliegen kommt.

Betrachten wir hierfür ein paar Fakten:

- 70% der erfolgreichen Cyberangriffe erfolgen per E-Mail mit vermeintlichen Anhängen oder Links (GDV/2019)
- 5-mal so viele falsche Emails seit Beginn der Corona Krise (https://www.it-daily.net/it-sicherheit/cyber-defence/23792-fuenfmal-mehr-malware-zum-coronavirus)
- Mehr als 50% aller Unternehmen weltweit haben schon Schäden durch digitale Angriffe erlitten
- Hunderte Zahnarztpraxen in den USA lahmgelegt und Lösegelder wurden erpresst (ZM online 03.09.2019)

Doch ist es lohnenswert eine Praxis zu infiltrieren und Patientendaten zu stehlen?

„Wir sind doch viel zu klein und unbekannt, um Hacker anzulocken."

Eine trügerische Annahme. Die meisten Angriffe sind nicht zielgerichtet und beschränken sich selten auf eine einzelne Praxis. Es werden häufig Sicherheitslücken ausgenutzt, die viele betreffen könnten und man schickt die Schadsoftware an möglichst große Verteilergruppe (bspw. per Mail). Arztpraxen stellen aufgrund der Patientendaten ein attraktives Ziel dar, die häufig nur mangelhaft geschützt sind.

Nicht ohne Grund hat die Kassenärztliche Vereinigung Westfalen-Lippe eine Cyber-Versicherung als Schutz in Ihre Ratgeber mit aufgenommen. Die Risiken sind vielseitig und Praxen bieten ein einfaches Angriffsziel.

Was kann man also tun, um sich vor digitalen Risiken zu schützen?

Die hier entstehenden Risiken lassen sich für eine Praxis durch eine Versicherung absichern. Eine sogenannte Cyber-Versicherung kann im Schadensfall nicht nur den finanziellen Schaden kompensieren, sondern bietet häufig eine eigene Schadensabwicklung mit IT-Experten, sodass Ihre Praxis schnell wieder läuft. Dennoch setzt diese voraus, dass der Zustand der IT einschlägige Sicherheitsmaßstäbe berücksichtigt und auch die für eine Praxis geltenden Technischen und Organisatorischen Maßnahmen (TOM) ausreichend gut implementiert sind.

Ansonsten kann sich der Versicherer in vielen Fällen von der Schadenabwicklung zurückziehen, da die Bedingungen nicht eingehalten wurden.

Damit das nicht passiert ist es wichtig, dass die IT einer neutralen Risikoanalyse unterzogen wird, bevor die risikorelevanten Fragen für eine Versicherung beantwortet werden. Ein kleiner Tipp aus der Praxis: Die meisten Unternehmen und Arztpraxen haben Ihre IT-Experten, doch ist es hier interessant einen externen Partner für die Kontrolle zu Rate zu ziehen, da dieser vielleicht auch etwas genauer hinschaut, da es im Zweifel nicht die eigenen Fehler sind die entdeckt werden.

An wen kann man sich wenden und wie sichere ich meine Praxis vernünftig ab?

Zusammen mit dem FVDZ e. V. hat auxmed, der Versicherungskooperationspartner des FVDZ, als Versicherungsmakler ein ganzheitliches Absicherungskonzept entwickelt. Von der Risikoprüfung via IT-Audit, über eine Spezialversicherung mit exklusiven Vorteilen für FVDZ Mitglieder, bis hin zur Integration von bestehenden und auszuarbeitenden Datenschutzmaßnahmen.

1. Schritt: Status-Quo ermitteln

Zuallererst sollte der aktuelle Status-Quo der eigenen Praxis IT festgestellt werden und hieraus das individuelle Risiko abgeleitet werden. Dies kann in Zusammenarbeit mit Ihrem IT-Dienstleister oder externen Experten geschehen.

Ein IT-Audit bringt die benötigte Klarheit in risikorelevante Fragestellungen und spricht anhand einer Gefahrenpotentialanalyse Handlungsempfehlungen aus.

2. Schritt: Risikoprüfung der Versicherung

Anhand von Risikofragen wird das individuelle Risiko bemessen und für Ihre Praxis eine auf Zahnärzte zugeschnittene und spezialisierte Versicherung ausgewählt. Hier wurde zusammen mit dem Assekuradeur Viktor ein Produkt entwickelt, dass sich vor allem an Zahnärzte orientiert und mit besonderen Leistungen erweitert wurde. Für Verbandsmitglieder wird der Selbstbehalt um 50% reduziert und eine dreijährige Prämiengarantie festgelegt. Zudem erhält jedes Mitglied Zugriff auf einen 24 Stunden Support im Ernstfall, hinter dem direkt IT-Spezialisten, bis hin zu IT-Forensikern sitzen, die sich um Ihre potentielle Gefahrensituation zu kümmern.

3. Schritt: Absicherungsmodell implementieren

Abschließend ist das erarbeitete Absicherungsmodell in das Qualitätsmanagement und Datenschutzkonzept der Praxis zu implementieren. Hier ist wichtig, dass bspw. die Überprüfung der technischen und organisatorischen Maßnahmen in die Ergebnisse des IT-Audits mit aufgenommen werden, um als Resultat ein ganzheitliches Präventionsmodell zu stricken.

Wie gehen Kriminelle eigentlich genau vor? Ein Beispiel anhand von Ransomware:

Jemand aus Ihrer Praxis erhält eine Mail mit einem vermeintlichen harmlosen Anhang. Das perfide an dieser Stelle ist, dass auch vertrauenswürdige Absender unfreiwillig zum Wirt werden können. Schadsoftware verbreitet sich häufig über die Kontaktadressen bereits kompromittierter Rechner.

Auch wenn nicht direkt etwas passieren muss, wenn der Anhang geöffnet wurde, wird ein Programm im Hintergrund geöffnet, dass Ihre Daten und die der im Netzwerk befindlichen Rechner verschlüsselt. Häufig wird dieses Verfahren erst aufgedeckt bzw. entdeckt, wenn auch von Seiten der Kriminellen, davon auszugehen ist, dass auch Back-ups durch die Ransomware unlesbar wurden. Andernfalls hätte man die Möglichkeit ein Backup aufzuspielen und das System innerhalb weniger Stunden wieder komplett funktionstüchtig zu betreiben. Hacker lernen auch hier dazu und verstecken ihre Software manchmal monatelang im Hintergrund.

Abbildung 1: Die Abbildung zeigt den Bildschirm eines von der Ransomware WannaCry kompromittierten Systems.

Wie einleitend kurz beschrieben ist der Stillstand der Praxis zwar ein großes übel, dass auch eklatante monetäre Folgen haben kann, doch sollte einem bewusst sein, dass eine Software, die sich über längere Zeit in Ihrem System befindet eine Backdoor zum Datenabfluss öffnen kann und so hoch sensible Patientendaten in kriminelle Hände fallen könnten.

Eine Ransomware ist so programmiert, dass dem Betroffenen Fristen zur Datenwiederherstellung zugesprochen werden, sofern eine Summe in bspw. Bitcoin überwiesen wird. Die Software „verspricht“, dass man im Anschluss alle Daten wiederbekommt.

Ob und welche Daten man wirklich wiederherstellen kann, sei dahingestellt. Die Zahlung der geforderten Beträge gibt einem keine Garantie, dass man Daten wieder zurückerhält. Vor allem diejenigen, die auf die erste Erpressungsforderung eingegangen sind, sind häufig auch bereit eine zweite oder dritte Zahlung zu leisten.

Autoren: Dipl.-Ing. Elmar Niebling & Jan Siol

Jan Siol

Geschäftsführer der auxmed GmbH
www.auxmed.de

M.A. Management
Financial Planner&Consultant
Finanzfachwirt (FH)