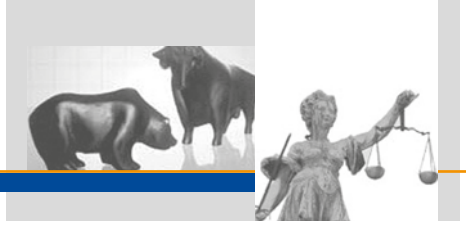


Cyberkriminalität –

IT Sicherheit & Angewandter Datenschutz

Sprechen Sie „Cybercrime"? Phishing, Hoaxes, Social Engineering, CEO Fraud, Ransomware, Scams, Skimming, DDOS-Attacken … wenn Ihnen diese Begriffe nichts sagen, wird es Zeit sich auf den aktuellen Stand möglicher Angriffszenarien zu bringen! IT-Sicherheit und Schutz gegen die gut getarnten Angriffe von Cyberkriminellen sind nicht nur Aufgabe Ihres IT Dienstleisters. Ihr Praxis-Team muss auf die Bedrohungen vorbereitet sein – der Faktor Mensch ist der größte Risikofaktor, der sich allein durch technische Maßnahmen nicht ausgleichen lässt! Doch was tun?

Mag. (FH) Simone Uecker

Simone Uecker

/// Daten – Angriffsziel & Wirtschaftsfaktor

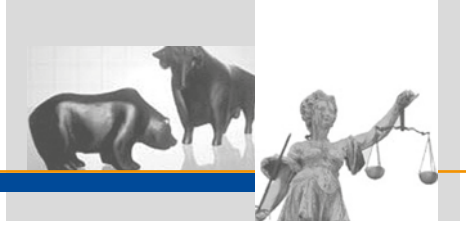
In Zeiten der papierlosen Praxis, der digitalen Patientenakte und der zunehmenden Digitalisierung aller behandlungsrelevanten Daten (z.B. digitales Röntgen, digitale Abformung, 3D-Modelldruck) sind Daten das zentrale Wirtschaftsgut einer Praxis – ohne Daten, Server, PC geht nichts mehr. Können Sie sich einen Behandlungstag mit Komplettausfall Ihrer IT vorstellen? „Oh nein!" wird hier vielfach der erste Gedanke sein, „Hoffentlich muss ich das nie erleben!" ist schnell der nächste Gedanke. Wie soll ein Röntgenbild angefertigt werden woher wissen wir über Allergien oder Risikofaktoren der Patientin Bescheid, wie sollen wir neue Termine vergeben ohne Einsicht ins Terminbuch, wie soll die Cerec-Krone angefertigt werden, und läuft der Steri überhaupt ohne Freigabe am PC? Nahezu alle unterstützenden Prozesse und vielfach sogar einzelne Behandlungsschritte laufen ohne funktionierende IT nicht mehr – der Super-GAU: die Praxis steht still!

Zugleich steigen die Kriminalitätsraten rund um Wirtschaftsspionage, Sabotage und Datendiebstahl auf neue Höchstwerte. So wurden laut aktuellen Studien bereits mehr als die Hälfte der Unternehmen in Deutschland in den letzten zwei Jahren zum Opfer dieser Straftaten rund um Cyberkriminalität – und die Dunkelziffer ist hoch! Viele Praxisinhaber kennen Kollegen, die zum Opfer von Lösegelderpressung durch Datenverschlüsselung (sog. Ransomware) geworden sind. Datenverlust oder der Praxis-Stillstand durch lahmgelegte IT sind nicht nur ferne Horrorszenarien, sondern werden leider schnell traurige Realität – verbunden mit hohen Kosten durch Ausfall, Wiederherstellung der Daten und der Infrastruktur und im Extremfall möglicherweise sogar Strafen der Datenschutz-Aufsichtsbehörden.

/// Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten – Die Kunst des Krieges, Sun Tsu

Unter Cyberkriminalität werden alle Straftaten zusammengefasst, die sich gegen IT Systeme oder deren Daten richten oder die durch diese informationstechnischen Systeme begangen werden. Die Ausprägungen an Bedrohungen, Straftaten und Angriffen sind vielfältig, doch wer seinen Feind nicht kennt, kann sich auch nicht effektiv schützen. Praxisinhaber, Praxismanagement und Teams sind also gefordert sich ständig sich auf dem neuesten Stand zu halten, welche Angriffsformen aktuell verbreitet sind und welche Maßnahmen Schutz bieten. Die zunehmend professionelleren Angriffe sind die Schattenseite des schnellen technischen Fortschritts mit all seinen Vorteilen an Komfort und Informationszugang. So sollte es zur Pflichtübung werden, nicht nur den neuesten technischen Trends zu folgen, sondern auch zumindest jährlich das Team im Umgang mit aktuellen Bedrohungen zu schulen und die eigene IT auf mögliche Angriffspunkte zu prüfen.

Gezielte Angriffe auf die Praxis im Sinne von Wirtschaftskriminalität oder Wirtschaftsspionage mit dem Ziel die Praxis gezielt zu schädigen oder Daten gezielt zu stehlen und beispielsweise als „Leak" (also als Geheimnisverrat oder unautorisierte Veröffentlichung) zugänglich zu machen sind selten. Vielmehr sind es allgemeine Schadsoftware oder Täuschungen, die im Internet und via E-Mail kursieren und jeden – somit auch die Praxis – treffen können und wollen. Als Nutzer müssen Sie in der Lage sein, Phishing, Hoaxes, Social Engineering, CEO Fraud Versuche, Tarnungsmethoden von Schadsoftware, Ransomware-Angriffe, Scams, Skimming, DDOS-Attacken und mehr



/// Tatort Praxis - Machen Sie den Selbst-Check

Wer seine Praxis in Hinblick auf Datenschutz und Datensicherheit vorbereiten will, sollte mit einem kritischen Blick auf die möglichen Angriffspunkte starten: schwarze Kleidung an und Maske auf (à la Datendieb) und schleichen Sie mal durch die Praxis. Nehmen Sie Ihre Praxis als potentiellen Tatort von Angreifern unter die Lupe und identifizieren Sie Ihre Schwachstellen!

Am Eingang und Empfang geht's los:

- Sind die Bildschirme einsehbar oder durch Sichtschutzfolien geschützt?
- Ist der Laptop Ihrer Abrechnungskraft mit einem Sicherheitsschloss gegen Diebstahl gesichert?
- Liegen USB-Sticks, SD-Karten rum? Wissen Sie welche Daten darauf gespeichert sind und ob ein Verschlüsselungsverfahren die Daten schützt?
- Liegen lose Ausdrucke im Drucker und Karteikarten auf dem Schreibtisch während die Rezeption unbesetzt ist?

Weiter geht's im Behandlungszimmer … sie glauben gar nicht, wie neugierig Ihre Patienten sind, während sie auf Sie warten!

- Werden die Bildschirme konsequent (oder besser automatisiert) gesperrt?
- Sind die USB-Anschlüsse des PCs im Behandlungszimmer gesperrt?
- Ist die Linse der Bildschirmkamera verdeckt? Auch beim iPad zur Patientenaufklärung?
- Werden Passwörter nach aktuellen Sicherheitsstandards verwendet oder können wir uns mit einfachsten Passwörtern Zugriff verschaffen? „praxis" oder „behandlung" entsprechen nicht den Standards der Datensicherheit, die Sie sich wünschen!
- Wer stellt sicher, dass Ihr Virenschutz regelmäßig aktualisiert wird? Finden die Updates wirklich automatisch statt?

Angekommen bei Ihrem Server ist IT Fachwissen gefragt:

- Ist eine Firewall aufgesetzt und sind Sie sicher, dass diese auch ausreichend konfiguriert ist (z.B. nicht der FTP Port pauschal freigegeben wird, weil irgendeine Software diesen Weg für ihre Updates nutzt)?
- Wer stellt sicher, dass bei Ihren – durch VPN gesicherten? – Fernzugriffen auch Virenschutz installiert ist und regelmäßig aktualisiert wird?
- Ist eine Systemtrennung zwischen Praxis-Netzwerk und Internet-/E-Mail-/Recherche-PC etabliert, wie sie auch von Datenschutz-Behörden empfohlen wird?
- Werden Log-Files erstellt und wird kontrolliert, dass das tägliche Backup auch erfolgreich durchgeführt wurde?
- Haben Sie schon einmal eine „Feuerwehrübung" einer Datenwiederherstellung von Backups oder eines Angriffs auf Ihre Datensicherheit durchgeführt?

Vergessen Sie den „Faktor Mensch" nicht! Trotz bester technischer Vorkehrungen ist der Mensch vor der Maschine vielfach die größte verbleibende Schwachstelle.

- Achten Ihre Mitarbeiter wirklich darauf, jede (wirklich jede, auch .pdf) externe Datei vor dem Öffnen mit dem Virenschutz zu prüfen?
- Wird die Anweisung zum Sperren der PCs wirklich befolgt?
- Wissen Sie und Ihre Mitarbeiter um die Gefahren, die von gefälschten Telefonhotlines ausgehen, die kostenpflichtige Software oder gar Schadsoftware über (von Ihren Mitarbeitern autorisierten) Fernzugriff installieren?
- Wird nicht gelegentlich doch der automatisierte Virenscan aus Bequemlichkeit oder Unwissenheit abgebrochen anstatt im Hintergrund die Arbeit zu verrichten?

Einen umfangreicheren Selbst-Check finden Sie unter: www.4med-consult.de/datensicherheit

zu erkennen. Wenn für Sie diese Begriffe wie Fremdworte einer unbekannten Sprache klingen, wird es Zeit Ihr Wissen auf den neuesten Stand zu bringen!

/// „Klicken Sie auf die Schaltfläche Aktualisieren, um die neueste Software zum Schutz Ihrer Dateien zu installieren" – und schon sind Sie den Angreifern ins Netz gegangen

Das Internet und E-Mail sind sicherlich das Eintrittstor für den Großteil der Gefahren durch Cyberkriminalität. Ein laxer, unbedarfter Umgang oder das schnelle Surfen nach dem neuesten Klatsch und Tratsch in einer kurzen Pause und schon ist es passiert: „Ihr Windows ist beschädigt, Ihre gesamten Systemdaten werden in 211 (Countdown) Sekunden gelöscht. Klicken Sie auf die Schaltfläche Aktualisieren, um die neueste Software zum Schutz Ihrer Dateien vor dem Löschen zu installieren." – wer hier klickt und den seriös wirkenden Aufforderungen am Bildschirm folgt (mit der besten Intention Schlimmes zu verhindern), ist bereits im Netz der Kriminellen gefangen. Hier kann der gut geschulte Nutzer schnell enttarnen, dass trickreiche Betrüger am Werk sind und die richtigen Maßnahmen ergreifen, um die Praxis keinem Risiko auszusetzen.

/// Was tun?

Die technischen Maßnahmen zum Schutz gegen Cyberkriminelle sind vielfältig und müssen in Abstimmung mit Ihrem IT-Dienstleister regelmäßig aktualisiert werden. Ein aktueller Virenschutz, der auch tatsächlich automatisch seine Arbeit verrichtet und ein durchdachtes Backup-Konzept sind Ihr bester Schutz – nicht nur gegen Cyberkriminelle. Auch die beste Cyberversicherung kann nicht helfen, wenn Ihre Daten unwiederbringlich verloren sind!

Doch auch das beste Backup-Konzept ist nicht ausreichend, wenn die Backups nicht diszipliniert erstellt werden, die Medien an geeigneter Stelle aufbewahrt werden und der Backup-Erfolg auch kontrolliert wird – dafür ist Ihr IT-Dienstleister nämlich nicht verantwortlich! Hier ist eine klare Aufgabenverteilung an zuverlässige Mitarbeiter gefragt und eine regelmäßige Kontrolle im besten Interesse der Praxis. Auch sogenannte „Feuerwehr-Übungen" können im Rahmen des Notfallkonzepts durchgeführt werden: hier wird ein kompletter Datenverlust simuliert und ein Backup zur Wiederherstellung des Systems getestet, wie es z.B. bei einem Verschlüsselungs- und Erpressungsangriff erforderlich wäre. So wissen Sie, dass Ihr Backup auch im Fall des Totalverlusts ausreichend ist, ihr IT-Dienstleister auf den Ernstfall vorbereitet ist und Sie testen, wie lange die Wiederherstellung im Notfall dauern würde und welchen Praxis-Ausfall Sie im schlimmsten Fall in Kauf nehmen müssten. Vielleicht stellen Sie auch fest, dass es in Ihrem Backupprozess erhebliche Lücken gibt und eine Wiederherstellung gar nicht möglich ist? Doch lieber erfahren Sie das im sicheren Rahmen einer Übung (während Ihre Daten noch alle vorhanden sind) als im Ernstfall mit tatsächlichem Datenverlust.

Der „Tatort Praxis" bietet vielfältige Angriffspunkte – machen Sie jetzt den Selbst-Check und beurteilen Sie selbst, wie gefährdet Ihre Praxis und Ihr Team wirklich ist!

/// FAZIT: Machen Sie Ihr Praxis-Team zur „Human Firewall"

Die ständig neuen Bedrohungen und die ständige Weiterentwicklung unserer Technologien (Stichwort: Telematikinfrastruktur, 3D, Cloud Dienste, Telemedizin) erfordern am Ball zu bleiben. Wer die Bedrohungen nicht kennt, kann sich nicht effektiv dagegen schützen! Zumindest die jährliche Schulung des Praxis-Teams auf die wichtigsten Verhaltensweisen sollte zur Selbstverständlichkeit werden. Damit kann die verpflichtende Unterweisung zu Schweigepflicht und Datenschutz endlich zum Leben erweckt werden!

Machen Sie Ihr Team zur „Human Firewall", dem menschliche Schutzschild gegen Cyberkriminalität in Ihrer Praxis! Hier können Sie auch auf externe Fortbildungsangebote setzen, wie z.B. **Cyberkriminalität – Wie schütze ich meine Praxis?** GERL Dental München & 4MED Consult– Anmeldung & Termine unter **www.gerl-dental.de/akademie**

AUTORIN
Mag. (FH) Simone Uecker

KONTAKT

4MED Consult
Amselweg 8
82194 Gröbenzell
E-Mail: simone.uecker@4med-consult.de
Internet: www.4med-consult.de