Tatort Praxis |

Selbst-Check zu angewandtem Datenschutz & Datensicherheit in der Praxis

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? Achtung falls die Bildschirme auch zur Befundung eingesetzt werden (abnehmbare Sichtschutzfolie)!
- 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?
- Gibt es eine Markierung und Inventarisierung der genutzten mobilen Datenträger, um fremde Datenträger schnell zu erkennen?
- Liegen lose Ausdrucke im Drucker und Karteikarten auf dem Schreibtisch während die Rezeption unbesetzt ist?
- Ist der Karteikarten-/Aktenschrank absperrbar und wird auch wirklich versperrt, wenn die Rezeption unbesetzt ist?
- Gibt es eine „Clean Desk" Regelung, damit in Pausen und Abends keine offenen Ausdrucke, Karteikarten, etc. unversperrt rumliegen?
- Ist die Internetnutzung (geschäftlich und privat) für Ihre Mitarbeiter freigegeben?

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 oder nur die Praxis-Software oder werde nur – mehr Alibi als echte Sicherheit – die Programme in der Taskleiste abgelegt sodass nur der Desktop zu sehen ist?
- 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 rund um Ihren **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?
- Wie ist das WLAN für Praxis und Patienten gesichert, um Zugriffe auf Ihre Praxis-Daten zu verhindern?
- Werden Log-Files erstellt und 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?
- Ist Ihr Backup wirklich ausreichend, um kurzfristig eine vollständige Wiederherstellung Ihrer Daten zu ermöglichen? Wie viel Ausfallzeit müssen Sie überbrücken, bis Ihre Praxis mit dem Backup wieder funktionsfähig ist?

Vergessen Sie nicht den Faktor Mensch! Weiter zum **Mitarbeiter-Check** >>>

Sprechen Sie uns an für weitere Informationen und individuelle Angebote: info@4med-consult.de | www.4med-consult.de

Sind Ihre Mitarbeiter Ihre „Human Firewall"?

Vergessen Sie den „Faktor Mensch" nicht! Trotz bester technischer Vorkehrungen ist der Mensch vor der Maschine ein kritischer Faktor, um die ausgefeilten Angriffe abzuwehren und die Sicherheit Ihrer Praxis und Ihrer Daten zu gewährleisten.

- Wann wurden Ihre Mitarbeiter zuletzt auf Cybercrime-Bedrohungen, Datenschutz und Datensicherheit geschult? Ist Ihr Wissen auf dem aktuellen Stand?
- Gibt es ungeschulte Mitarbeiter, z.B. auf Grund von Neueinstellungen, Auszubildende?
- Kennen Sie und Ihre Mitarbeiter die aktuellen Cybercrime-Bedrohungen?
    - Phishing (E-Mail, Telefon)
    - Identitätsdiebstahl & Social Engineering
    - Schadprogramme (Viren, Trojaner, AdWare etc.)
    - Spam E-Mails und ihre Erkennungsmerkmale
    - Hoaxes, vorgetäuschte Fehlermeldungen
    - Ransomware
    - DDOS-Angriffe
- 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?
- Gibt es eine Arbeitsanweisung zum Umgang mit Fernzugriff-Anfragen, um sicherzustellen, dass nur berechtigte Unternehmen den Fernzugriff zu Supportzwecken nutzen?
- Ist die Zuständigkeit für die Prüfung/Aktualisierung des Virenschutzes klar festgelegt? Werden auch die über Fernzugriff (VPN) verfügbaren Computer geprüft?
- Wird nicht gelegentlich doch der automatisierte Virenscan aus Bequemlichkeit oder Unwissen abgebrochen anstatt im Hintergrund die Arbeit zu verrichten?

Eine kleine Unachtsamkeit … und Ihre Praxis steht still!

Mit dem Selbst-Check können Sie mögliche Schwachstellen Ihrer Praxis definieren, doch was nun?

1 Sprechen Sie mit Ihrem IT-Dienstleister!

Ein umfassendes Sicherheitskonzept ist eine komplexe Aufgabe – Ihr IT Dienstleister ist Ihr kompetenter Partner gegen Cyberkriminelle. Planen Sie regelmäßige, kleinere Investitionen in Ihre IT Infrastruktur, um auf dem Stand der Technik zu bleiben.

2 Schulen Sie Ihr Team!

Nutzen Sie externe Angebote zur Schulung und besprechen Sie sicherheitsrelevante Themen in Teambesprechungen, um Ihr Praxis-Team regelmäßig zu sensibilisieren. Machen Sie Ihr Team mit einer internen Schulung – spannend, praxisnah und kurzweilig – zu Ihrer „Human Firewall"!

3 Ein externer Audit schafft Klarheit!

Ihr Fokus ist der Patient und seine Behandlung! Sie kennen jede Ecke Ihrer Praxis! So wird man schnell „betriebsblind". Nutzen Sie das geschulte Auge eines Experten von außen, um mögliche Schwachstellen und Verbesserungspotentiale sichtbar zu machen. Wenn die Praxis wächst, auf digitales Röntgen umgestellt wird oder Komponenten ausgetauscht werden, sollte auch Ihr Sicherheitskonzept überprüft werden – ein externer Audit öffnet die „betriebsblinden" Augen!

Sprechen Sie uns an für weitere Informationen und individuelle Angebote: info@4med-consult.de | www.4med-consult.de