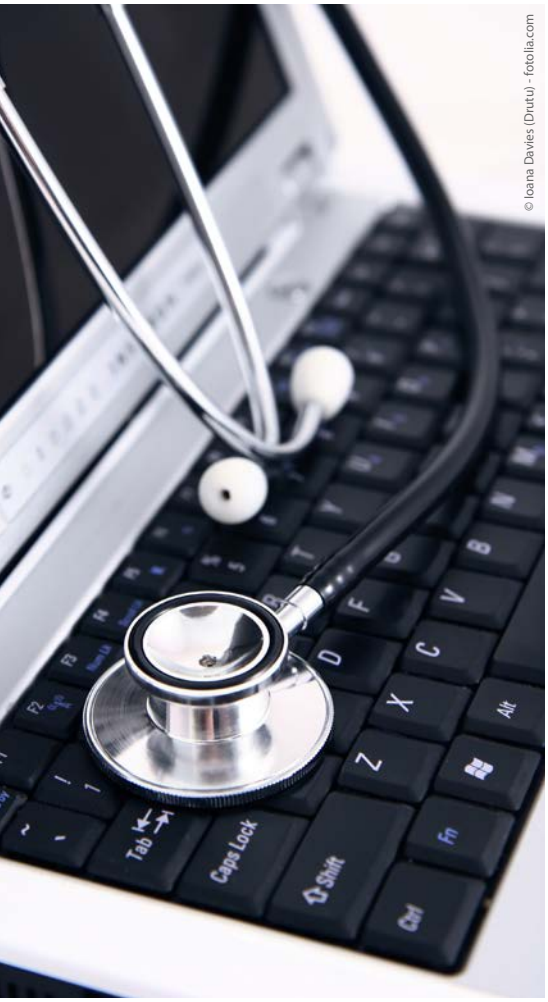
Serie **Praxisorganisation und -führung**

Schutz vor Cyberkriminalität: Tipps für den Praxisalltag

...weil Qualität in der Praxis führt.

Tagtäglich kursieren im Internet betrügerische E-Mails mit gefährlichen Anhängen oder Links. Präparierte Internetseiten können Schadsoftware (Malware) übertragen oder sensible Daten abgreifen (Phishing). Durch unachtsames Öffnen eines E-Mail-Anhanges oder eines Internet-Links können Ihre Daten zerstört bzw. gestohlen und Ihr Praxis-Netzwerk vollständig stillgelegt werden.



© Ioana Davies (Drutu) - fotolia.com

Einfache Maßnahmen und eine erhöhte Aufmerksamkeit können vor derartigen Gefahren – nicht nur Ihren Praxis-Computer – schützen.

Hier einige Hinweise:

- Sensibilisieren Sie Ihre Mitarbeiter für das Thema: Greifen Sie das Thema in Ihrer Teambesprechung auf. Aufmerksamkeit schaffen bspw. kostenlose Info-Grafiken der Allianz für Cyber-Sicherheit oder die Broschüre „Sicheres Surfen im Internet – so schützen Sie sich!“ der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.
- ! Vorsicht bei E-Mails mit Anhängen und Links:
  Gehen Sie vor dem Öffnen der E-Mail auf Nummer sicher: Prüfen Sie u. a. den Absender (z. B. bekannte/unbekannte oder kryptische E-Mail-Adresse?). **Im Zweifelsfall E-Mail löschen bzw. den Absender kontaktieren.** Ein Video des Bundesinstitutes für Sicherheit in der Informationstechnik (BSI) gibt praktische Tipps für den schnellen Check: „Drei Sekunden für mehr E-Mail-Sicherheit“
- Prüfen Sie genau, ob Sie sich auf der richtigen Website befinden, bevor Anmeldedaten eingegeben werden.
- Aktualisieren Sie regelmäßig das Betriebssystem, den Browser und sämtliche genutzte Software. Das BSI hat wesentliche Maßnahmen zusammengestellt: „Leitfaden für sicheres Patch-Management“.
- Nutzen Sie eine aktuelle Antiviren-Software und Firewall.
- Ein Konzept zur regelmäßigen Datensicherung (Backup) hilft im Ernstfall. Die Wiederherstellung der Daten sollte ebenfalls regelmäßig getestet werden.
- ! Lassen Sie sich bei der Installation einer Antiviren-Software, der richtigen Konfiguration einer Firewall oder der Implementierung eines Datensicherungskonzeptes unterstützen, bspw. durch Ihren Systembetreuer.
- Führen Sie E-Mail-Kommunikation und Internet-Recherchen nach Möglichkeit nicht aus dem Praxis-Netzwerk aus, sondern nutzen Sie dafür einen separaten Zugang.
- Weitere Infos: Technische Anlage zu „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ und „PraxisCheck Informationssicherheit der KBV“ (www.kbv.de/html/mein_praxischeck.php)
- Überprüfen Sie Ihren Versicherungsschutz (z. B. Berufshaftpflicht) und schließen bei Bedarf eine Zusatzversicherung gegen Cyberkriminalität ab.

► Die Qualitätsmanagement-Richtlinie definiert „Informationssicherheit und Datenschutz“ in § 3 als ein Grundelement des Qualitätsmanagements.

Quelle: QEP-Newsletter (30) der Kassenärztlichen Bundesvereinigung: www.kbv.de >> Service >> Service für die Praxis >> QEP >> QEP – Qualität und Entwicklung in Praxen >> QEP-Newsletter

Sie haben Fragen oder wünschen weitere Informationen? Gern können Sie sich an Christin Richter telefonisch unter 0391 627-6446 oder per Mail an christin.richter@kvsa.de wenden.