

Kleine IT-Sicherheitstipps für KMU und Arztpraxen



- Klare dienstliche Vereinbarung zur Nutzung des Internets bzw. der Computer
- Legen sie einen Verantwortlichen fest (oder Outsourcing), welcher die Systeme aktuell hält (Updates, Upgrades, Patch- Management)
- Wer kümmert sich um Backup's (Festlegung)?
Wichtig, physikalische Trennung der Sicherung (Offline- Backup), regelmäßige Überprüfung, ob einspielbar und konsistent, u.U. Lagerung außerhalb der Firma/ Praxis (Brandfall, Hochwasser u.a.)
- WLAN-Nutzung, wenn ja, getrennte Netze für Firma/ Praxis und Privatnutzung (Gast- WLAN), Zeitschaltung: nach Feierabend/ Wochenende autom. Abschalten
- Rechnersperre bzw. Bildschirmschoner mit Passwort setzen, unbefugte Nutzung verhindern
- Anschließen von USB- Sticks, mobilen Festplatten, Handys nur unter starken Sicherheitsauflagen, besser möglichst vermeiden
(Ausnahme: mobile Festplatte zur Datensicherung/ Backup)
- Regelmäßige Schulung der Mitarbeiter zum Umgang mit Computern, Internet, E-Mail u.a.
- Praxen sollten regelmäßig die Sicherheit des Kartenlesers überprüfen (Plombe, Etiketten)
- Hinweise zum sicheren Umgang mit E-Mails, Dateianlagen, Links usw.,
Nutzen sie eine E-Mailverschlüsselung und Signierung!
Sind eigene Mailadressen und Maildomains mit SPF, DKIM und/ oder DMARC abgesichert?
SPF = Sender Policy Framework - Absenderadress-Fälschungen vermeiden
DKIM = DomainKeys Identified Mail - Sender-Authentifizierung
DMARC = Domain-based Message Authentication, Reporting and Conformance) -
Kontrollsystem, Regelwerk
- In dem Zusammenhang ist es wichtig ein gutes und aktuelles Antiviren Programm zu haben, eine Firewall (auch vom Betriebssystem oder dem Antiviren Programm) sollte sowohl global als auch pro Computer lokal aktiv sein
- Proaktive Auswertung von Firewall- oder Access- Logs, um rechtzeitig Angriffe und Schwachstellen zu identifizieren
- Existiert ein Netzwerkplan? (sehr wichtig, fehlt häufig !!!)
- Gibt es Regelungen (Notfallplan für IT-Sicherheitsvorfälle, auch andere Vorfälle), Alarmierungsplan, Kontakt- Verzeichnisse
Informationspflichten?

- Im Hinblick auf CEO- und BEC- Fraud (Geschäftsführerschwindel) sollten klare und transparente Regelungen bezüglich Geld- Überweisungen getroffen werden
- Feste Ansprechpartner bei externen Dienstleistern (insbesondere auch für die eigene technische Betreuung)
- Positionierung der Monitore, Bildschirmfilter damit Kunden bzw. Patienten nicht die Möglichkeit haben Login- Daten auszuspähen
- Gibt es die Möglichkeit der 2FA Authentifizierung, sollte diese möglichst genutzt werden, Passwort nicht unter Tastatur kleben o.ä.
- Wartungszugänge (VPN, RDP, Team-Viewer u.a.) sollten überwacht und bei Nichtnutzung deaktiviert werden, auch hier möglichst 2FA oder aber lange, komplexe Passwörter verwenden
- Informieren sie sich auf einschlägigen IT- Portalen (BSI, heise.de, golem.de u.a.) oder Ärzteportale über aktuelle Schwachstellen und Bedrohungen, damit sie schnell reagieren können
- Physikalische Absicherung des Zugangs zur Firma/ Praxis (feste Tür, Türschloss, Fensterabsicherung), ggf. Einbruchmeldeanlage
- Haben sie einen Webauftritt?
Wer kümmert sich darum (inhaltlich, technisch)?
Absicherung des Webauftritt's, Einhaltung der DSGVO, Updates + Sicherheits- Patches, sichere Zugangsdaten usw.
- Datenbanken gehören nicht ins Internet bzw. sollten darüber nicht erreichbar sein (nötige Ausnahmen entsprechend absichern)
- Für den Fall das nichts mehr geht, muss
ein separater Internetanschluss kurzfristig nutzbar,
ein Telefonanschluss für die Kommunikation (ggf. Handy) und
ein separater Rechner (Laptop) mit eigener separater Mailadresse
verfügbar sein