slis

Lexikon IT-Sicherheit

Vielen ist „IT“ und „Datensicherheit“ ein Begriff, doch was genau es damit auf sich hat, ist vielleicht unklar. Besonders beim Umgang mit sensiblen Gesundheitsdaten ist eine sichere Praxis-IT unverzichtbar. Um verständlicher zu machen, was eine sichere Praxis-IT alles umfasst, haben wir die wichtigsten Begriffe zum Thema IT-Sicherheit in einem Lexikon zusammengefasst. Sie können das Lexikon auch ganz einfach abspeichern oder ausdrucken, um es im Arbeitsalltag immer zur Hand zu haben.

Datensicherung/Backups

Mithilfe einer automatisierten Datensicherung stellen Arztpraxen sicher, dass wichtige Gesundheitsdaten ihrer Patient:innen für den Fall von Cyberattacken oder technischen Störungen auf einem zweiten Speicherträger gesichert sind. Da Backups auf USB-Sticks oder externen Festplatten anfällig für Verlust, Diebstahl oder fehlerhafter Datenspeicherung sind, gibt die „KBV/KZBV IT-Sicherheitsrichtlinie“ vor, für alle Endgeräte in der Praxis regelmäßig Datensicherungen durchzuführen. Wir unterstützen Praxen mit einer automatisierten, verschlüsselten und zukunftsorientierten Datensicherung im Rechenzentrum sowie aktivem „Monitoring“ So sind Praxis-Backups inklusive sensibler Gesundheitsdaten optimal vor Hackerangriffen, Diebstahl und Datenverlust geschützt.

Cyberversicherung

Eine Cyberversicherung ist eine Zusatzversicherung für Unternehmen, um sich gegen finanzielle Schäden durch Hackerangriffe und Cyberkriminalität zu schützen. Besonders für Praxen ist die zusätzliche Absicherung durch eine Cyberversicherung wichtig, um sich beispielsweise gegen den Diebstahl von sensiblen Gesundheitsdaten abzusichern. Auch für den Fall, dass die Praxis-IT durch einen Virus lahmgelegt wird, sodass ein geregelter Praxisablauf nicht mehr möglich ist, ist eine Cyberversicherung hilfreich. Alles Wichtige rund um den Nutzen, die Leistungen und die Haftung einer Cyberversicherung erfahren Sie in unserem FAQ – Cyberversicherung.

Firewall

Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Mit unserem Angebot Sichere Praxis-IT erhalten Praxen und medizinische Einrichtungen eine zukunftsfähige Next Generation (UTM)-Firewall. Diese besitzt neben dem Hauptzweck, das Netzwerk von Nutzer:innen zu schützen, zusätzlich intelligente Analyse- und Filtermechanismen. Inklusive „Monitoring“ ermöglichen unsere Services eine frühzeitige Erkennung von Störungen.

slis

Managed Service Provider

Ein Managed Service Provider stellt seinen Kundinnen und Kunden langfristig wiederkehrende IT-Dienstleistungen oder Services zur Verfügung und sorgt für deren Betrieb, Verwaltung und Wartung. Die Verantwortung für die Serviceleistung geht somit auf den Managed Service Anbieter über. Auf diese Weise erhalten Leistungserbringer alle Services aus einer Hand und werden bei IT-Themen spürbar entlastet.

KBV/KZBV IT-Sicherheitsrichtlinie

Die KBV/KZBV IT-Sicherheitsrichtlinie ist ein Leitfaden für den Datenschutz und die IT-Sicherheit in Arztpraxen. Sie wird von der Kassenärztlichen Bundesvereinigung (KBV) und der Kassenzahnärztlichen Bundesvereinigung (KZBV) bereitgestellt. Neben klaren Vorgaben enthält sie auch Empfehlungen zur Umsetzung. Ziel der IT-Sicherheitsrichtlinie ist es, die IT-Systeme und sensiblen Daten der Arztpraxen besser zu schützen.

Monitoring

In der IT-Branche beschreibt Monitoring die kontinuierliche Überwachung von Prozessen und Abläufen. Es dient der frühzeitigen Erkennung und Behebung von Störungen in der Praxis-IT. Mithilfe von Monitoring erkennen Managed Service Provider auftretende Störungen in Echtzeit und beheben sie umgehend. So müssen Praxen Störungen in der Regel gar nicht erst melden und können sich voll und ganz dem Praxisalltag widmen.

Ransomware

Ransomware oder ein sogenannter Verschlüsselungstrojaner ist ein Schadprogramm, das Daten auf Computern und Servern verschlüsselt und so den Zugriff und die Nutzung der Daten verhindert. Betroffene Einrichtungen im Gesundheitswesen können dann nicht mehr auf die Patientendaten zugreifen und müssen den Praxisbetrieb vorübergehend einstellen. Häufig erhalten die Betroffenen von den Hackern Lösegeldforderungen, um die verschlüsselten Daten wieder freizugeben. Es ist möglich, dass die Hacker dabei sensible Daten abfangen und kopieren. Praxisinhaber:innen sind gesetzlich dazu verpflichtet, ihre Patient:innen über den möglichen Datendiebstahl zu informieren. Da dies für eine Praxis existenzbedrohend sein kann, ist eine sichere Praxis-IT unerlässlich. Erfahren Sie mehr über IT-Gefahren im Praxisalltag.