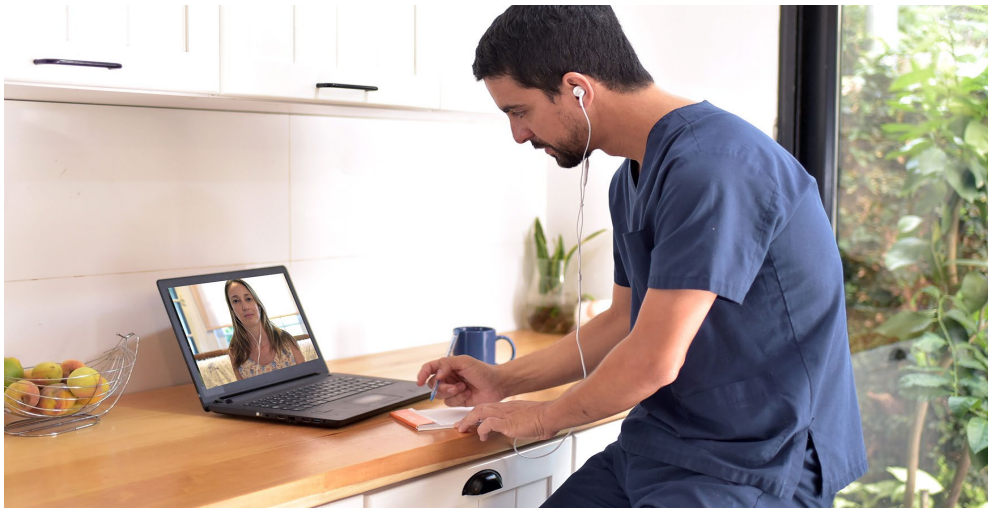
So sichern Sie Ihr IT-Netzwerk im Gesundheitswesen passend ab



In Folge der Telematikpflicht müssen Gesundheitsdienstleister fortan für ein sicheres IT-Netzwerk sorgen und dabei gewissen rechtlichen Anforderungen nachkommen. Um Schutz gegen Cybergefahren wie Diebstahl, Sabotage und Netzausfälle zu gewährleisten, bedarf es eines Höchstmaßes an IT-Sicherheit sowie Digitaler Souveränität. Nur so können eine hohe Datensicherheit und Handlungsfähigkeit aufrechterhalten werden.

Lesen Sie hier, wie Sie für ein sicheres und gesetzeskonformes IT-Netzwerk Sorge tragen.

Beachten Sie die gesetzlichen Vorgaben bei der Anbindung an die Telematik

→ Digital-Gesetz des BMG:

- Verpflichtung zur Umsetzung eines IT-Sicherheitskonzepts, Handlungsaufforderung zur Installation aktueller Sicherheitskomponenten
- Einrichtung der elektronischen Patientenakte (ePA) Anfang des Jahres 2025 für alle gesetzlich Versicherten; Opt-Out-Möglichkeit (Widerspruch, wenn die Patienten die ePA nicht nutzen möchten)
- Digitale Medikationsübersicht: ePA in enger Verknüpfung mit eRezept
- eRezept ab 1. Januar 2024 als verbindlicher Standard in der Arzneimittelversorgung; Vereinfachung der Nutzung per elektronischer Gesundheitskarte und ePA-App
- Digitale Gesundheitsanwendungen werden stärker in die Versorgung integriert und ihr Einsatz transparent gemacht
- Assistierte Telemedizin: niedrigschwelliger Zugang der Versorgung; Aufhebung der 30%-Begrenzung für die Telemedizin

→ § 75 B SGB V **(wird in das Digital-Gesetz transformiert):** Sicherheitsvorgaben für die digitalen Infrastrukturen und Prozesse in Arztpraxen, Zahnarztpraxen und psychotherapeutischen Einrichtungen
- Anforderungen (der Kassenärztlichen Bundesvereinigung) an die sichere Installation und Wartung von Komponenten und Diensten der Telematikinfrastruktur
- Die informationssicheren Systeme sind jährlich an den aktuellen Stand der Technik anzupassen

→ § 75 C SGB V **(wird in das Digital-Gesetz transformiert):** Sicherheitsvorgaben für die digitalen Infrastrukturen und Prozesse in klinischen Einrichtungen
- Verbindliche Richtlinie für alle Krankenhäuser, soweit nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes eingestuft
- Verpflichtung nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele für informationstechnische Systeme, Komponenten oder Prozesse zu treffen
- Die informationssicheren Systeme sind alle zwei Jahre an den aktuellen Stand der Technik anzupassen

→ IT-Sicherheitsgesetz 2.0**:** Erhöhung der Sicherheit informationstechnischer Systeme; stärkt das BSI in folgenden Punkten:
- Verstärkte Kompetenzen bei der Detektion von Sicherheitslücken und der Abwehr von Cyber-Angriffen
- Regelung zur Untersagung des Einsatzes kritischer Komponenten zum Schutz der öffentlichen Ordnung oder Sicherheit in Deutschland; Informationssicherheit in den 5G-Mobilfunknetzen
- Verbraucherschutz (Digitaler Verbraucherschutz (DSV)): Einführung eines einheitlichen IT-Sicherheitskennzeichens
- Nationale Behörde für Cybersicherheitsidentifizierung: BSI laut § 9a Absatz 1 die Nationale Behörde für die Cybersicherheitszertifizierung; Zuständigkeit für die Überwachung und Durchsetzung der Vorschriften im Rahmen der europäischen Schemata für die Cybersicherheitszertifizierung

→ NIS2**:** Europäische Richtlinie für Netzwerk- und Informationssicherheit
- Handlungsanweisung von der Europäischen Kommission, bis Oktober 2024 gewisse Netzwerksicherheitsmaßnahmen in nationales Recht umzusetzen
- Definition von Risiko- und Krisenmanagementbestandteilen
- Verschärfte Meldepflichten zu Sicherheitsvorfällen innerhalb von 24 Stunden inkl. Abschlussbericht
- Härtere Sanktionen bei Rechtsverstößen

→ PDSG**:** Einhaltung des Patientendatenschutzgesetzes
- Schutz sensibler Gesundheitsdaten: Sichere und selbstbestimmte Nutzung von digitalen Angeboten wie ePA (elektronische Patientenakte), eRezept, eVerordnung, eAUB (elektronische Arbeitsunfähigkeitsbescheinigung)

→ **DSGVO-Konformität:** Verarbeitung personenbezogener Daten nach der Datenschutzgrundverordnung

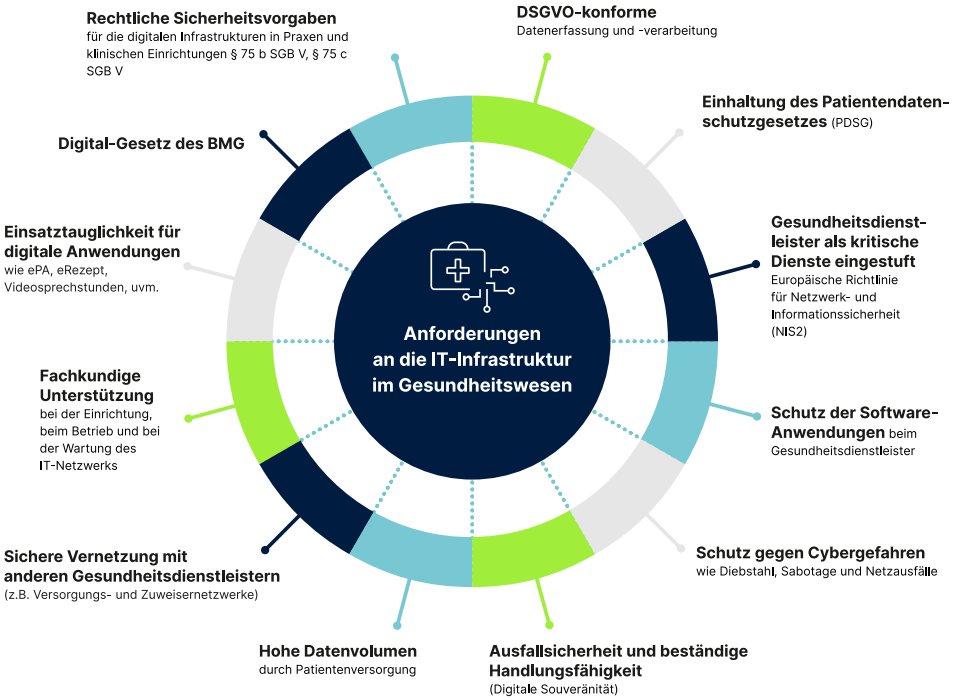
Welche Produkte oder Anwendungen benötigen Sie?

→ Eine Firewall für erhöhte Netzwerksicherheit mit Anwendungskontrolle und -blockierung, Filter- und Verschlüsselungsfunktionen, sowie Angriffserkennung und -prävention
→ Ein oder mehrere Switches für eine hohe Leistungsbereitschaft und Flexibilität beim Aufbau des Netzwerkes
→ Mehrere Access Points zur optimalen WLAN-Abdeckung in Ihrem Arbeitsfeld
→ Cloud-Management Ihrer Netzwerkkomponenten für eine hochsichere, bequeme Fernverwaltung Ihres gesamten Netzwerks sowie übersichtliches 24/7-Monitoring für einen zuverlässigen Betrieb
→ Umfassender Service und Support bei der Einrichtung, beim Betrieb und bei der Pflege Ihres IT-Netzwerkes zur effizienten Auslagerung der IT-Wartung an IT-Spezialisten
→ Eine passende IT-Lösung entsprechend der Größe, Benutzeranzahl und Beschaffenheit Ihres Netzwerks

Finden Sie hier Ihr passendes Healthcare-Paket

Empfehlungen für Ihr IT-Netzwerk im Gesundheitswesen

- → Individuell an Ihre Einrichtung angepasstes Vernetzungskonzept
- → Komplettlösung mit untereinander kompatiblen Komponenten und Services
- → Hohe europäische IT-Sicherheit- und Datenschutzstandards einhalten, wie u. a. Backdoor-Freiheit, DSGVO-Konformität, Digitale Souveränität
- → Vollständige Compliance mit den gesetzlichen Auflagen für den Gesundheitssektor
- → Unterstützung bei Netzwerkeinrichtung & -betreuung
- → Langfristig gepflegte und zukunftsfähige Netzwerk-Software



Sie hätten gerne bei all diesen Schritten professionelle Unterstützung?

Dann kontaktieren Sie uns gerne persönlich und schildern uns Ihre konkrete Situation. Wir freuen uns, wenn wir Ihnen persönlich weiterhelfen können.

LANCOM Systems ist führender europäischer Hersteller von Netzwerk- und Security-Lösungen (WAN, LAN, WLAN, Remote & Mobile Access und Firewalls) für Wirtschaft und Verwaltung mit einem besonderen Augenmerk auf digitale Souveränität, Sicherheit und Zukunftsfähigkeit. Die Soft- und Hardware-Entwicklung sowie Fertigung erfolgen unter höchsten Qualitäts- und Sicherheitsanforderungen hauptsächlich in Deutschland und garantieren eine hundertprozentige Backdoor-Freiheit in allen LANCOM Produkten. Auch die LANCOM Management Cloud steht mit ihren deutschen Host-Servern für europäisches Recht und höchste Datensouveränität ein. Das LANCOM Portfolio umfasst alle benötigten virtuellen und Hardware-Netzwerkkomponenten, Netzwerkmanagement-Tools, Zubehör, Software-Upgrades und einen hauseigenen technischen Hersteller-Support für die klein- bis großflächige Standortvernetzung via Software-defined Networking (SDN).

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de