

•🕸• SECUREPOINT

KBV-SICHERHEITSRICHTLINIEN EINFACH ERFÜLLEN

IT-SECURITY FÜR GESUNDHEIT UND PFLEGE



ES GEHT UM MEHR ALS DATENSCHUTZ

Digitale Dienste sicher nutzen, Gesundheitsdaten schützen und vernetzte Geräte zuverlässig absichern

IT-Sicherheit ist essenziell für reibungslose Abläufe im Gesundheitssektor. Sie unterstützt die Betriebsfähigkeit medizinischer Einrichtungen, indem sie Angriffen auf die Infrastrukturen vorbeugt. Sie ermöglicht vertrauliche Kommunikation zwischen Patienten und Leistungserbringenden, indem sie vor Datenabfluss schützt. Sie kann Geschäftsführende vor den juristischen oder finanziellen Folgen eines Sicherheits-Vorfalles schützen.

Mit der zunehmenden Digitalisierung sind auch die konkreten Anforderungen an IT-Security gewachsen. Die europäische und nationale Gesetzgebung für den Schutz kritischer Infrastrukturen (KRITIS) schlägt sich im Gesundheitsbereich vor allem in Form der KBV-Richtlinien zur IT-Sicherheit nieder.

Securepoint bietet mit dem neuen Security-Bundle „Fortress“ eine Lösung an, mit der ein Großteil der Anforderungen an medizinische Praxen abgedeckt sind.



FORTRESS

Network & Human Security

UTM Firewall	✓
Awareness Next	✓
Unified Security Report	✓

Endpoint Security

Windows VPN (Cloud Managed)	✓
Cloud Shield (Windows)	✓
Antivirus Pro	✓
Darkweb Scan	✓

Mobile Security

Mobile Device Management	✓
VPN (Mobile Devices)	✓
Cloud Shield (Mobile Devices)	✓



UTM-Firewall mit VPN und Cloud Shield

Nr.	Anforderung der KBV	Quelle	Relevanz
1	Einsatz einer Firewall	Anlage 1, Punkt 1	verpflichtend
2	Schutz vor Viren und Spam	Anlage 1, Punkt 40	verpflichtend
3	Verschlüsselung der Datenübertragung	Anlage 2, Punkt 2	verpflichtend ab 6 Mitarbeitenden
4	Individuelle Definition von Zugriffsrechten auf Daten	Anlage 2, Punkt 2	verpflichtend ab 6 Mitarbeitenden
5	Netzwerk-Segmentierung	Anlage 3, Punkt 2	verpflichtend ab 20 Mitarbeitenden



Awareness-Training

Nr.	Anforderung der KBV	Quelle	Relevanz
1	Schulung der Praxisleitung	Anlage 1, Punkt 8	verpflichtend
2	Schulung von Mitarbeitenden	Anlage 1, Punkt 10	verpflichtend
3	Kompetenter Umgang mit Spam	Anlage 1, Punkt 10	verpflichtend



Mobile Device Management

Nr.	Anforderung der KBV	Quelle	Relevanz
1	Zwingender Einsatz von PIN oder Code	Anlage 1, Punkt 32	verpflichtend
2	App-Zugriffsrechte beschränken	Anlage 1, Punkt 33	verpflichtend
3	Fern-Sperrung von Geräten bei Verlust	Anlage 1, Punkt 34	verpflichtend
4	Durchsetzen einer verbindlichen Richtlinie für die Nutzung mobiler Geräte	Anlage 2, Punkt 2	verpflichtend ab 6 Mitarbeitenden
5	Einsatz eines Mobile Device Management	Anlage 3, Punkt 7	verpflichtend ab 20 Mitarbeitenden
6	Zentrale Verwaltung von Zertifikaten für Mobilgeräte	Anlage 3, Punkt 9	verpflichtend ab 20 Mitarbeitenden



Antivirus Pro

Nr.	Anforderung der KBV	Quelle	Relevanz
1	Aktueller Virenschutz auf Endgeräten	Anlage 1, Punkt 20	verpflichtend



Update-Management

Nr.	Anforderung der KBV	Quelle	Relevanz
1	Zwingender Einsatz von PIN oder Code	Anlage 1, Punkt 32	verpflichtend
2	App-Zugriffsrechte beschränken	Anlage 1, Punkt 33	verpflichtend
1	Zwingender Einsatz von PIN oder Code	Anlage 1, Punkt 32	verpflichtend

UNSERE LÖSUNG FÜR MEHR IT-SICHERHEIT

Das IT-Sicherheitspaket „Fortress“ von Securepoint bietet umfassenden, mehrschichtigen Schutz für Arztpraxen und medizinische Einrichtungen. Es schützt Netzwerke, Endgeräte und den sicheren Fernzugriff und hilft dabei, sensible Patientendaten zuverlässig abzusichern.

Mit Fortress wird IT-Sicherheit planbar und verständlich: Eine leistungsstarke Kombination zentraler Sicherheitslösungen schützt Ihre Praxis im laufenden Betrieb und lässt sich flexibel an Ihre Anforderungen anpassen.



Securepoint GmbH

Bleckeder Landstraße 28
21337 Lüneburg

Tel.: +49 (0)4131 / 24010
info@securepoint.de
www.securepoint.de

•O• SECUREPOINT

Überreicht durch Ihren Securepoint-Partner