

Agenda

- Was ist die KBV-IT-Sicherheitsrichtlinie?
- Welche gesetzlichen Anforderungen sind umzusetzen?

Live

- Vorstellen unserer Themenseite
- Unsere IT-Sicherheits-Starterseminare
- Unsere Awareness-Trainings
- KBV-Informationen

- Ziele
 - Entwicklung einer Standard-Vorgabe zum Schutz sensibler Daten in den Praxen
 - Risikominimierung Datenverlust und Betriebsausfallzeiten
- Vorgabe durch die KBV, geprüft durch das BSI – Grundlage ist das DVG
- Unterscheidung zwischen Vorgaben, welche umgesetzt werden müssen und Empfehlungen
- Anforderungen können je nach Praxisgröße variieren.

Mit Einführung weiß jede Praxis, welche Anforderungen umzusetzen sind um im Falle eines IT-Sicherheitsvorfalls rechtlich „auf der sicheren Seite“ zu sein!

- Schwer, alles in der kurze der hier vorhanden Zeit unterzubringen.
- Die wichtigsten Anforderungen
 - professioneller Virenschutz
 - Browser-Einstellungen – es dürfen keine vertraulichen Daten gespeichert werden
 - Wenn an Endgeräten nicht gearbeitet wird sind diese zu sperren (Windows + L)
 - Das Praxisnetzwerk ist anhand eines Netzwerkplans zu dokumentieren
 - Zum 01.01.2022 ist eine hardwarebasierte Firewall einzusetzen
 - Wechseldatenträger (z.B. die täglichen Sicherungsfestplatten) müssen vor jeder Benutzung auf Viren überprüft werden

- Vorstellen unserer Themenseite (https://www.cgm.com/deu_de/lp/it-sicherheit-msh.html)
- Unsere IT-Sicherheits-Starterseminare (https://www.cgm.com/deu_de/lp/it-sicherheit-msh.html)
- Unsere Awareness-Trainings (https://www.cgm.com/deu_de/lp/it-sicherheit-msh.html)
- KBV-Informationen (<https://www.kbv.de/html/it-sicherheit.php>)

- Formulieren Sie jetzt ihre Fragen im F&A-Bereich dieser Veranstaltung
- Unsere Empfehlungen:
 - Besuchen Sie unser kostenloses Startseminar zum Thema IT-Sicherheit
 - Lassen Sie den „IST-Zustand“ ihrer IT in Sachen IT-Sicherheit professionell durch einen zertifizierten Dienstleister überprüfen
 - **Links und Dokumente zum Thema finden Sie heute am Messestand des CGM MEDISTAR SYSTEMHAUSES hier auf der MEDISTAR Hautnah Online**
 - **Dort oder in der „Network-Lounge“ stehen wir Ihnen gerne für Gespräche zur Verfügung**

- September 2020: IT-Sicherheitsvorfall am Universitätsklinikum Düsseldorf#
 - Hacker haben sich Zutritt zur Heinrich-Heine-Universität verschafft
 - UKD dort an die Systeme angeschlossen und deswegen betroffen
 - Konsequenz: UKD tagelang von der Notfallversorgung abgetrennt.
 - Hacker haben eine „alte“ Sicherheitslücke genutzt – ein einfaches Softwareupdate hätte schlimmstes verhindert

- Oktober 2020: vertrauliche Psychotherapiedaten in Finnland gehackt und teilweise veröffentlicht
 - Besonderheit: Mit den Daten wurden nicht die Behandler konfrontiert, sondern es wurde versucht die Patienten mit ihren sensiblen Daten zu erpressen.