CYBERSICHERHEIT DEUTSCHER KRANKENHÄUSER

ANOFRDERUNGEN AN DIE CYBERSICHERHEIT



REGULATORISCHE ANFORDERUNGEN

BSI-Gesetz §8 Vorgaben d. Bundesamtes, §8a-f
IT - SIG 2.0 Erhöhung d. Sicherheit IT Systeme
§75c SGB V IT-Sicherheit in Krankenhäusern
DSGVO Art. 32 Sicherheit der Verarbeitung
NIS-2 Richtlinie (noch kein nationales Recht)

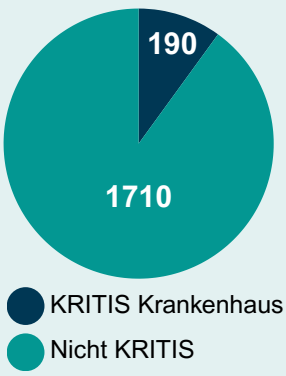
MÖGLICHE UMSETZUNG

ISO/IEC 27001
Branchenspez. Sicherheitsstandard (**B3S**) für Krankenhäuser

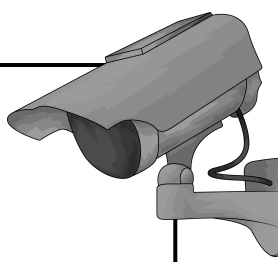


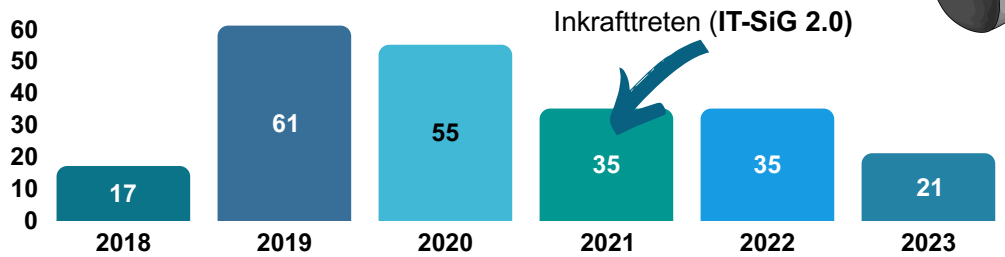
Krankenhäuser mit **mehr als 30.000 stationären Fällen pro Jahr** zählen zur Kritischen Infrastruktur (**KRITIS**) und **müssen Cyber-Incidents melden**. Kleinere Krankenhäuser zukünftig auch auf Basis der **NIS-2 Richtlinie.**

Datenschutzverstöße müssen gem. **Art. 33 DSGVO** auch durch kleinere Einrichtungen an Aufsichtsbehörde gemeldet werden.



CYBER-INCIDENTS BEI KRITIS-KRANKENHÄUSERN

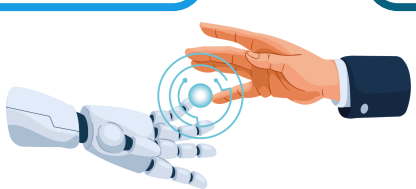




IT-SICHERHEITSRELEVANTE HERAUSFORDERUNGEN

Ungleichmäßig entwickelte IT-Infrastruktur

Aufbau IT-Risikomanagement



Begrenzte Ressourcen

IT-Sicherheitskultur

BEISPIELE FÜR ZWISCHENFÄLLE 2024

01/2024 Bezirkskliniken Mittelfranken
Daten durch Ransomware verschlüsselt

02/2024 Uniklinik Brandenburg an d. Havel
Phishing Attacke auf E-Mail Server

02/2024 Klinikverbund Soest
Patientendaten verschlüsselt und gestohlen

09/2024 Bobingen Wertachkliniken
Ransomware Attacke legt Systeme lahm

10/2024 Johannesstift Diakonie Berlin
Daten durch Ransomware verschlüsselt

Autor: Grigori Rogge

ATLAS DIGITALE GESUNDHEITSWIRTSCHAFT