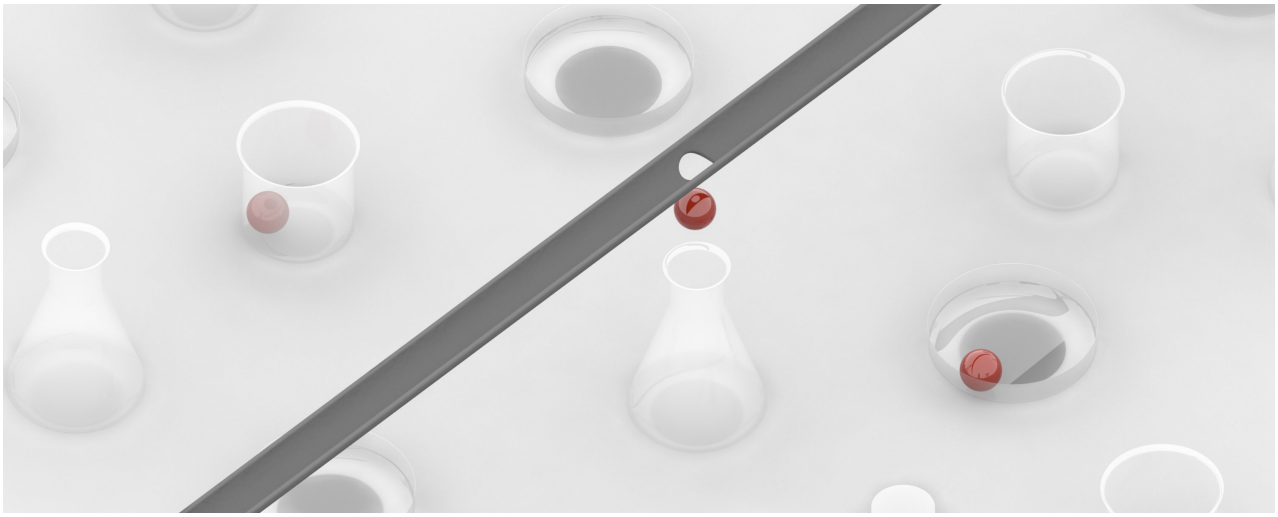

IT/TK IM GESUNDHEITSWESEN

Umsetzung des IT□Sicherheitsgesetzes in Kliniken – wie die Pflicht zur Kür wird

Seit dem 30. Juni 2017 gilt die erste Ergänzungsverordnung zur BSI-KRITIS-Gesetzgebung, mit der im Gesundheitswesen die Kliniken mit mehr als 30.000 vollstationären Patienten pro Jahr in die Kategorie „Kritische Infrastrukturen" KRITIS eingruppiert werden.

Damit fallen diese Kliniken wie zuvor schon viele Unternehmen aus den Sektoren Energie, Versorgung, Transport und Verkehr, IT und Telekommunikation, Finanz- und Versicherungswesen sowie Ernährung in den Gültigkeitsbereich des IT-Sicherheitsgesetzes.

Das Gesetz von 2015 verfolgt vorrangig das Ziel, die informationstechnischen Systeme besser zu schützen und die Informationssicherheit durchgängig zu erhöhen.

Bis zum 30. Juni 2019 haben die Kliniken nun Zeit, die vom Branchenarbeitskreis „Medizinische Versorgung" im Umsetzungs-Plan UP KRITIS definierten Maßnahmen zu realisieren. Der bemessene Zeitraum ist insofern herausfordernd, als die geforderten Aktivitäten, beispielsweise die Einführung eines Information Security Management Systems ISMS, bei der Umsetzung als zeitintensiv gelten.

Der Aspekt von angedrohten Sanktionen spielt erwartungsgemäß eine

gewichtige Rolle. Jedoch sollte sich jede KRITIS-Klinik einmal vor Augen führen, welche nachhaltigen Vorteile für die Institution aus der Umsetzung des IT-Sicherheitsgesetzes resultieren:

- Sicherheitsniveau erhöhen – Sicherheitsrisiken verringern
- Steigerung der Reputation als Institution durch hohe Informationssicherheit
- Abwenden von Angriffen und dadurch Sicherstellen der Handlungsfähigkeit
- Vermeiden von hohen Aufwänden nach Schaden durch Präventionsmaßnahmen
- Verringern des Haftungs-Risikos für das Krankenhaus-Management
- Profilierung gegenüber mündiger werdenden Patienten
- Sensibilisierung der gesamten Belegschaft („Awareness") für den zeitgemäßen Umgang mit der modernen IT und den damit verbundenen Risiken
- Aufdeckung ineffizienter Prozesse und Beseitigung von Medienbrüchen
- Gesteigerte Transparenz bei der Risikokommunikation an das Management
- Generieren einer soliden Basis für die Personalplanung in puncto Informationssicherheit

Diese beeindruckende Liste ließe sich sicherlich noch um den einen oder anderen Punkt ergänzen. Die Einführung eines Information Security Management Systems basiert auf prozess-, organisations- und technikrelevanten Maßnahmen, die die gesamte Organisation des Krankenhauses einbeziehen und deshalb vom Management aktiv unterstützt werden muss.

Die Umsetzung wird idealerweise durch fachkompetente externe Berater begleitet, die über eine Kombination von zertifizierter Expertise im Bereich Informationssicherheit, umfassendem technischen und organisatorischem Know-how und vor allem einschlägiger Klinikerfahrung verfügen.

Hierzu bietet die Adiccon GmbH ein interessantes KRITIS-Klinik-Beratungspaket an. Wenn Sie Fragen haben oder weitere Informationen wünschen, sind wir gerne für Sie da. Nehmen Sie Kontakt zu uns auf – wir freuen uns auf Sie!

Diese Pressemitteilung wurde auf PRESSEBOX veröffentlicht

Veröffentlicht am Donnerstag, 30.11.2017

AUTOR
Karsten Hellinger

Vielen Dank für Ihr Interesse.
Weitere Blog Beiträge finden Sie unter adiccon.de