IT-Sicherheitsgesetz

Worum geht es?

- Ziel des Gesetzes ist die Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland.
- Krankenhäuser mit mind. 30 Tsd. stationären Fällen pro Jahr fallen gemäß der ergänzenden am 30.06.2017 in Kraft getretenen 1. Verordnung zur Änderung der BSI-Kritisverordnung (auch 2. Korb der BSI-KritisV genannt) unter KRITIS (Kritische Infrastruktur).
- KRITIS-Häuser haben eine Kontaktstelle einzurichten und eine Meldepflicht für IT-Sicherheitsvorkommnisse gemäß § 8b (3) BISG.
- KRITIS-Häuser bekommen über die Kontaktstelle regelmäßig wertvolle Informationen zur IT-Sicherheit.
- TIPP: Nicht unter KRITIS fallende Häuser erhalten vergleichbare Informationen über eine freiwillige Anmeldung im UPKRITIS (s. u.).
- KRITIS-Häuser haben in regelmäßige Prüfungen (audits) die Einhaltung von branchenspezifischen Mindestsicherheitsniveaus sicherstellen gemäß § 8a (3) BSIG.
- Pflichtverletzungen können mit einem Bußgeld bis 100 Tsd. € geahndet werden.

Hintergrundinformation

- Das Gesetz führt die Cybersicherheitsstrategie und die Allianz für Cybersicherheit fort
- Das Gesetz adressiert die Betreiber Kritischer Infrastrukturen
- Zu den Kritischen Infrastrukturen zählt das Gesetz die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen
- Für die Umsetzung werden zahlreiche zusätzliche Stellen geschaffen, u.a. bei BSI, Verfassungsschutz, Bundesnetzagentur, BND und Bundesumweltministerium
- Betreibern kritischer Infrastrukturen entsteht Aufwand für das
  - Betreiben einer Kontaktstelle
  - Einrichten eines Meldesystems für IT-Sicherheitsvorfälle
  - Einhalten eines angemessenen Sicherheitsniveaus
  - Durchführen von Audits
- Die Anzahl der Betreiber kritischer Infrastrukturen über alle Sektoren wird im Gesetz auf max. 2000 geschätzt, nach den ergänzenden Kriterien der BSI-KritisV 2. Korb fallen voraussichtlich 110 Krankenhäuser unter das IT-Sicherheitsgesetz
- Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards (B3S) zur Gewährleistung der

Anforderungen vorschlagen. Für die Krankenhäuser arbeitet der „Branchenarbeitskreis Medizinische Versorgung" an diesem Thema.

- Der vom BAK Medizinische Versorgung erarbeitete B3S muß vom BSI auf Eignung geprüft werden.

Was bedeutet es für ein Krankenhaus, das zur kritischen Infrastruktur zählt?

- Es muß bis zum 30.12.2017 eine Kontaktstelle eingerichtet werden.
- Es muß bis zum 30.06.2019 der Prüfnachweis gemäß § 8a (§) erbracht werden.
- Es müssen frühzeitig organisatorische und technische Maßnahmen eingeleitet werden, um das geforderte Sicherheitsniveau zu erreichen und notwendige Strukturen und Prozesse zu etablieren wie z. B. ein ISMS
- Alle zwei Jahre ist zukünftig eine Sicherheitsüberprüfung (Audit) durchzuführen

Wie engagiert sich der KH-IT in dieser Sache?

- Initiierung eines Arbeitskreises KRITIS, aus dem sich der Branchenarbeitskreis (BAK) "Medizinische Versorgung" entwickelt hat.
- Zahlreiche Mitglieder des BAK "Medizinische Versorgung " sind im KH-IT organisiert u.a. der Leiter (Forchheim), stellvert. Leiter (Gruetz) und stellvertr. Sprecher (Schütz)
- Themenslot auf verschiedenen KH-IT Tagungen und Informationen an die Mitglieder

Letzte Meldung!!!

- Die DKG hat auf ihrer Website den beim BSI zur Eignungsprüfung eingereichten B3S veröffentlicht. Kliniken bietet sich damit eine gute Grundlage für die umzusetzenden Anforderungen.
  ==> bit.ly/B3S_eingereicht

Wo ich finde ich weitergehende Informationen?

- IT-Sicherheitsgesetz bit.ly/ITSG_Gesetz
- BSI-KritisV Korb 2 bit.ly/BSI-KritisV2
- Handlungsempfehlung des BAK bit.ly/BAK-Handlungsempfehlung
- FAQ zum IT-Sicherheitsgesetz bit.ly/ITSG_FAQ
- Webseite des UP KRITIS bit.ly/UPKRITIS_Zusammenarbeit
- Antragsformulare zur Mitgliedschaft im UP KRITIS bit.ly/UPKRITIS_Anmeldung

Thorsten Schütz, Vorstand KH-IT, stellvertr. Sprecher des BAK Medizinische Versorgung