IT-Sicherheitsgesetz

Worum geht es?

- Ziel des Gesetzes ist die Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland.
- Für Betreiber Kritischer Infrastrukturen wird eine Meldepflicht zu IT-Sicherheitsvorkommnissen definiert.
- Regelmäßige Prüfungen (audits) sollen die Einhaltung von branchenspezifischen Mindestsicherheitsniveaus sicherstellen.
- Pflichtverletzungen können mit einem Bußgeld bis 100 Tsd. € geahndet werden.
- Mit der am 30.06.2017 in Kraft getretenen 1. Verordnung zur Änderung der BSI-Kritisverordnung (auch 2. Korb der BSI-KritisV genannt) wurden Kriterien definiert, wonach sich entscheidet, welches Krankenhaus als kritische Infrastruktur zu betrachten ist.

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.

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

- Es muß bis zum 30.12.2017 eine Kontaktstelle eingerichtet 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 (Audits) 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 (Gruetz), stellvert. Leiter (Forchheim) und stellvertr. Sprecher (Schütz)
- Themenslot auf verschiedenen KH-IT Tagungen und Informationen an die Mitglieder

Letzte Meldungen

- 25.07.15 Das IT-Sicherheitsgesetz tritt offiziell in Kraft
- 03.05.16 BSI-KritisV Korb 1 tritt in Kraft
  (Sektoren Energie, Informationstechnik u. Telekommunikation, Wasser u. Ernährung)
- 30.06.2017 BSI-Kritis Verordnung Korb 2 tritt in Kraft
  (u.a. mit Festlegungen zum Sektor Gesundheit)
- 27.07.2017 Der UPKRITIS BAK Medizinische Versorgung veröffentlicht "Handlungsempfehlungen zur Verbesserung der Informationssicherheit an Kliniken" in Version 1.2

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