IT-Sicherheitsgesetz 2.0

Worum geht es?

- Am 28.05.2021 tritt das “Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme” (IT-Sicherheitsgesetz 2.0, IT-SiG 2.0) in Kraft.
- Es bringt eine Reihe von Neuerungen und Verschärfungen gegenüber dem bisherigen "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme in Deutschland" aus 2015
- Die Rolle des BSI wird mit dem IT-SiG 2.0 weiter gestärkt.
- Es werden Regelungen zum Einsatz kritischer Komponenten definiert und eine IT-Sicherheitskennzeichen für Produkte eingeführt
- Es werden "Unternehmen im besonderen öffentlichen Interesse" definiert
- Es gilt weiterhin für Betreiber Kritischer Infrastrukturen eine Meldepflicht zu IT-Sicherheitsvorkommnissen und das Durchführen 2-jährlicher Audits/Prüfnachweise.
- 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.).
- Bußgelder von bisher max. 100 Tsd. € werden mit dem IT-SiG auf bis zu 20 Mio. EUR erhöht in Angleichung an die EU Datenschutzgrundverordnung (EU-DSGVO)
- 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).
- Ergänzend zum IT-Sig 2.0 wird zum Beginn 2022 eine Aktualisierung der bisher für Krankenhäuser geltenden BSI-KritisV erwartet.

Hintergrundinformation

- Das Gesetz ist eine Fortführung der Cybersicherheitsstrategie und der Allianz für Cybersicherheit
- Das Gesetz adressiert die Betreiber Kritischer Infrastrukturen
- Zu den Kritischen Infrastrukturen zählen die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen

- Die Anzahl der Betreiber kritischer Infrastrukturen über alle Sektoren wird 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.
- Die für Krankenhäuser aktuell gültige Version eines B3S liegt in der Version 1.1 vor, welche gemäß Feststellungsbescheid vom 22.10.2019 zur Gewährleistung der Anforderungen nach § 8a Abs. 1 BSIG geeignet ist.

Was bedeutet das für mich als IT-Leiter?

- Betreibern kritischer Infrastrukturen entsteht Aufwand für das
  - Betreiben einer Kontaktstelle
  - Einrichten eines Meldesystems für IT-Sicherheitsvorfälle
  - Einhalten eines angemessenen Sicherheitsniveaus
  - Durchführen von Audits

Wo ich finde ich weitergehende Informationen?

- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)
  https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1632338583765
- Branchenspezifischer Sicherheitsstandard (B3S)
  https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf
- Antworten zum § 8a Prüfnachweis des BSI
  https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-zu-Par-8a-BSI-allgemein/faq-zu-par-8a-bsi-allgemein_node.html
- Teilnahme im UP KRITIS
  https://www.kritis.bund.de/SubSites/Kritis/DE/Aktivitaeten/Nationales/UPK/Kontakt/UPK_Kontakt.html

Wie engagiert sich der KH-IT in dieser Sache?

- Initiierung des Arbeitskreises KRITIS, aus dem inzwischen der aktuelle Branchenarbeitskreis (BAK) "Gesundheitsversorgung" hervorgegangen ist.
- Stellen von Mitgliedern im BAK "Medizinische Versorgung ", u.a. den Leiter (Forchheim), stellvert. Leiter (Gruetz) und stellvertr. Sprecher (Schütz)
- Themenslot auf verschiedenen KH-IT Tagungen und Information an die Mitglieder

Autor:
Thorsten Schütz, Vorstand KH-IT, Stellvertr. Sprecher des BAK Medizinische Versorgung