Deutsche Stiftung für Recht und Informatik

Cybersicherheit im Krankenhaus

Ein neuer Strauß an Vorgaben durch Digi-G, NIS2UmsuCG und KRITIS-DachG

Tilmann Dittrich, LL.M. (Medizinrecht)
Heinrich-Heine-Universität Düsseldorf

„Fahrplan des Vortrags“

1. Einleitung: Cyberangriff auf das Uniklinikum Frankfurt und der „Crowdstrike-Blackout“
2. Vorgaben für Kritis-Krankenhäuser
   a) Aktuelle Vorgaben nach dem BSIG
   b) Künftige Vorgaben durch das NIS2UmsuCG
   c) Künftige Vorgaben durch das KRITIS-DachG
   d) Compliance-Regelungen – Vorstandshaftung
   e) Besondere Haftungsfragen für Krankenhäuser
3. Gesetzliche Neuerungen durch das Digitalgesetz
   a) Security-Awareness in Krankenhäusern
   b) Änderungspotential bei § 391 SGB V
4. Fazit

Uniklinik Frankfurt bekämpft weiter Folgen des Hackerangriffs

Die Uniklinik Frankfurt vermeldet erste Erfolge im Kampf mit den Folgen eines Hackerangriffs. Nach über drei Monaten sind die akuten Probleme beseitigt. Für die zukünftige IT-Sicherheit steht die Arbeit aber noch an.

Veröffentlicht am 17.01.24 um 09:55 Uhr

Die Gefährdungslage für Krankenhäuser

Quelle Foto: https://www.hessenschau.de/panorama/uniklinik-frankfurt-bekaempft-weiter-folgen-des-hackerangriffs-v1,uniklinik-bekaempft-weiter-hackerangriff-100.html

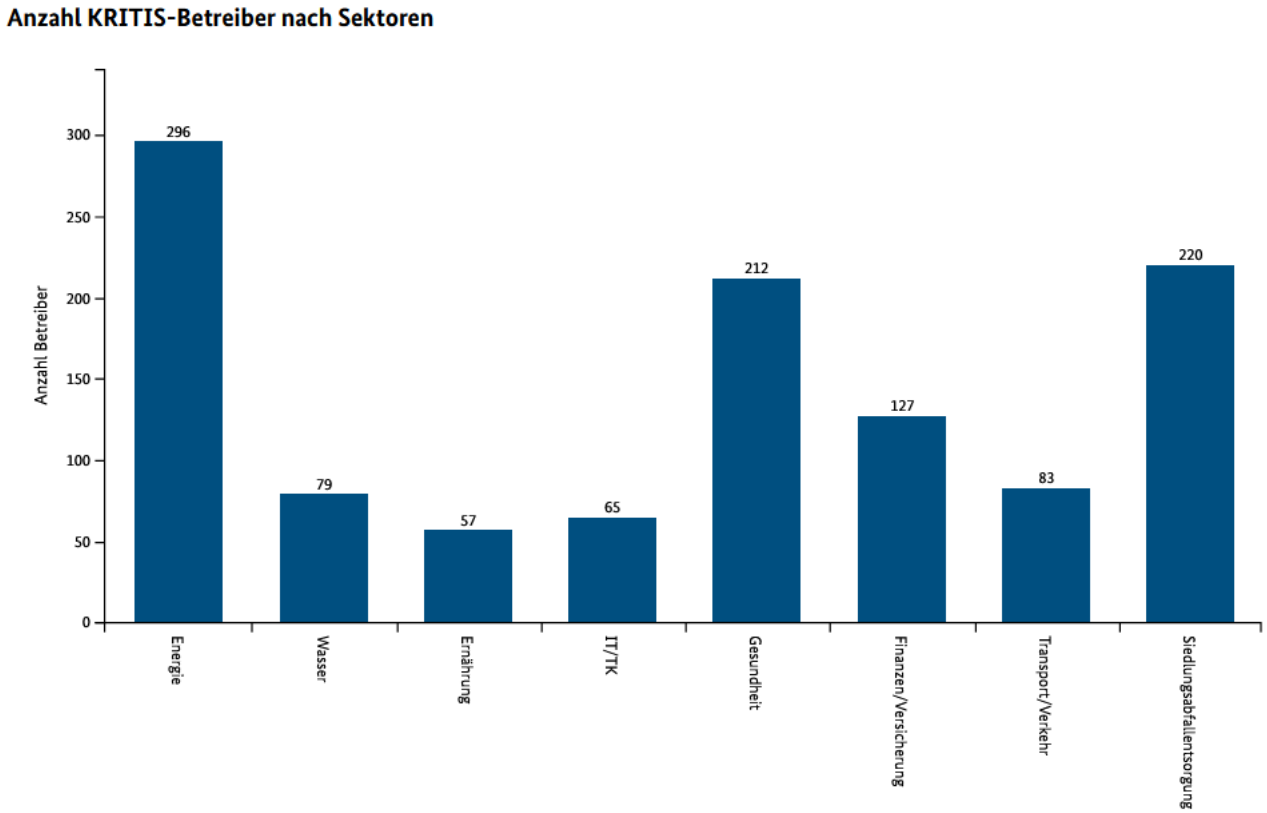
Die Gefährdungslage für Krankenhäuser

- Gefahr auch in der digitalen Lieferkette – Crowdstrike-Vorfall
- Jährliche Schäden von Cybercrime für deutsche Wirtschaft über 200 Milliarden Euro
- Riesiger Bewältigungsaufwand für Krankenhäuser
- Besondere Bedeutung der Business Continuity wegen Gesundheitsgefahren
- Gesetzgeber reagiert engmaschig
  - Zusätzlich zur Datensicherheit (Art. 5, 32 DSGVO) zunehmend leges speciales für die Cybersicherheit

Aktuelle Vorgaben nach dem BSIG

- Kritische Infrastruktur: Plankrankenhäuser ab 30.000 vollstationären Behandlungsfällen/Jahr
- 5-10 Prozent aller Krankenhäuser in Deutschland (Schätzung der DKG von 2017)
- Pflichtenkanon aus §§ 8a, 8b BSIG:
  - Organisatorische und technische Vorkehrungen (OTV) inkl. System zur Angriffserkennung
  - Nachweispflicht über OTV im 2-Jahres-Turnus
  - Mitwirkungspflichten bei Überprüfung durch BSI
  - Registrierung der Einrichtung/Benennung einer Kontaktstelle
  - Meldepflicht bei Störungen an das BSI
- Gesetzliche Vermutung für OTV bei Umsetzung des Branchenspezifischen Sicherheitsstandards (B3S)
- Hilfsangebote des BSI (u.a. Entsendung eines Mobile Incident Response Team – MIRT)

Aktuelle Vorgaben nach dem BSIG



Quelle Bild: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html#doc1106676bodyText1

Aktuelle Vorgaben nach dem BSIG

Umsetzung der Risikomanagement-Vorgaben in Reifegraden

Reifegrad	ISMS	BCMS
1	1,5 %	8 %
2	36,5 %	49 %
3	32 %	24 %
4	19 %	12 %
5	11 %	7 %

Aktuelle Vorgaben nach dem BSIG

Weitere Fakten zum Kritis-Sektor „Gesundheit“:

- Umsetzungsgrad 2 (von 5) dominiert bei Angriffserkennungssystemen (in meisten Sektoren schon Grad 3)
- 40 gemeldete Störungen Q2/2024
  - Nur „Transport und Verkehr“ mit 53 mehr, danach mit 39 „Energie“
- Hohe Meldebereitschaft im Lagebericht 2023 hervorgehoben

#NIS2KNOW – Künftige Vorgaben durch das NIS2UmsuCG

Compliance & Recht

Meinung

Bei der NIS2-Umsetzung droht Chaos

17.04.2024 Von Bernhard Kretschmer (Autor) FOLGEN

Bernhard Kretschmer, Vice President Services und Cybersecurity bei NTT, ist überzeugt davon, dass die Umsetzung von NIS2 im Chaos endet.

Quelle Screenshot:
https://www.computerwoche.de/a/bei-der-nis2-umsetzung-droht-chaos,3698631

Künftige Vorgaben durch das NIS2UmsuCG

- 2020: Europäische Cybersicherheitsstrategie
- 2022: NIS-2-RL und RCE-RL
  - NIS-2-RL löst NIS-RL ab (Netzwerkinformationssicherheits-RL)
  - RCE-RL neu: Physische Resilienz von wichtigen Einrichtungen
  - All-Gefahren-Ansatz: NIS-2-RL und RCE-RL gehen Hand in Hand
- Oktober 2024: Umsetzungsfrist Mitgliedstaaten
  - Dezember 2023: Referentenentwurf KRITIS-DachG
  - Juli 2024: Kabinettsentwurf NIS2UmsuCG
- Für NIS2UmsuCG Umsetzung im Frühjahr 2025 realistisch, für KRITIS-DachG derzeit nicht abzusehen

Künftige Vorgaben durch das NIS2UmsuCG

- Einrichtungskategorien:
  - Betreiber kritischer Anlagen (Nachfolger Kritische Infrastruktur)
    - Nationale Besonderheit: weiterhin Bestimmung anhand von Schwellenwerten
  - Neu: wichtige und besonders wichtige Einrichtungen
    - Bestimmen sich nach KMU-Kriterien der EU (Mitarbeiterzahl + Umsatz/Bilanz)
  - Von 5.000 auf ~30.000 betroffene Unternehmen + öff. Einrichtungen
    - Zusätzlich noch mittelbare Betroffenheit in der Lieferkette

- Sektor Gesundheit: u.a. „**Gesundheitsdienstleister**“ -> jedenfalls Krankenhäuser, uU auch große MVZ-Ketten
  - Zudem noch Arznei- und Medizinprodukthersteller sowie EU-Referenzlaboratorien

Künftige Vorgaben durch das NIS2UmsuCG

Dreh- und Angelpunkt: Risikomanagement für IT-Gefahren (§ 30)

- Kritische Anlagen: auch Angriffserkennungssysteme (§ 31 Abs. 2)
- Scope BSIG alt: OTV für Prozesse, die für Dienstleistung **maßgeblich** sind
- Scope NIS2UmsuCG: für alle IT-Prozesse der Einrichtung
- Katalog an Sicherheitsmaßnahmen: u.a. Business-Continuity-Management (§ 30 Abs. 2 Nr. 3)

Künftige Vorgaben durch das NIS2UmsuCG

3-Stufige Meldepflicht bei Störungen an eine gemeinsame Meldestelle von BSI und BBK (§ 32)

- Frühe Erstmeldung (unverzüglich, spätestens 24 h nach Kenntniserlangung)
- Meldung (unverzüglich, spätestens 72h nach Kenntniserlangung)
- Abschlussmeldung (spätestens 1 Monat nach Meldung)
- Ggf. Zwischenmeldungen

Künftige Vorgaben durch das NIS2UmsucG

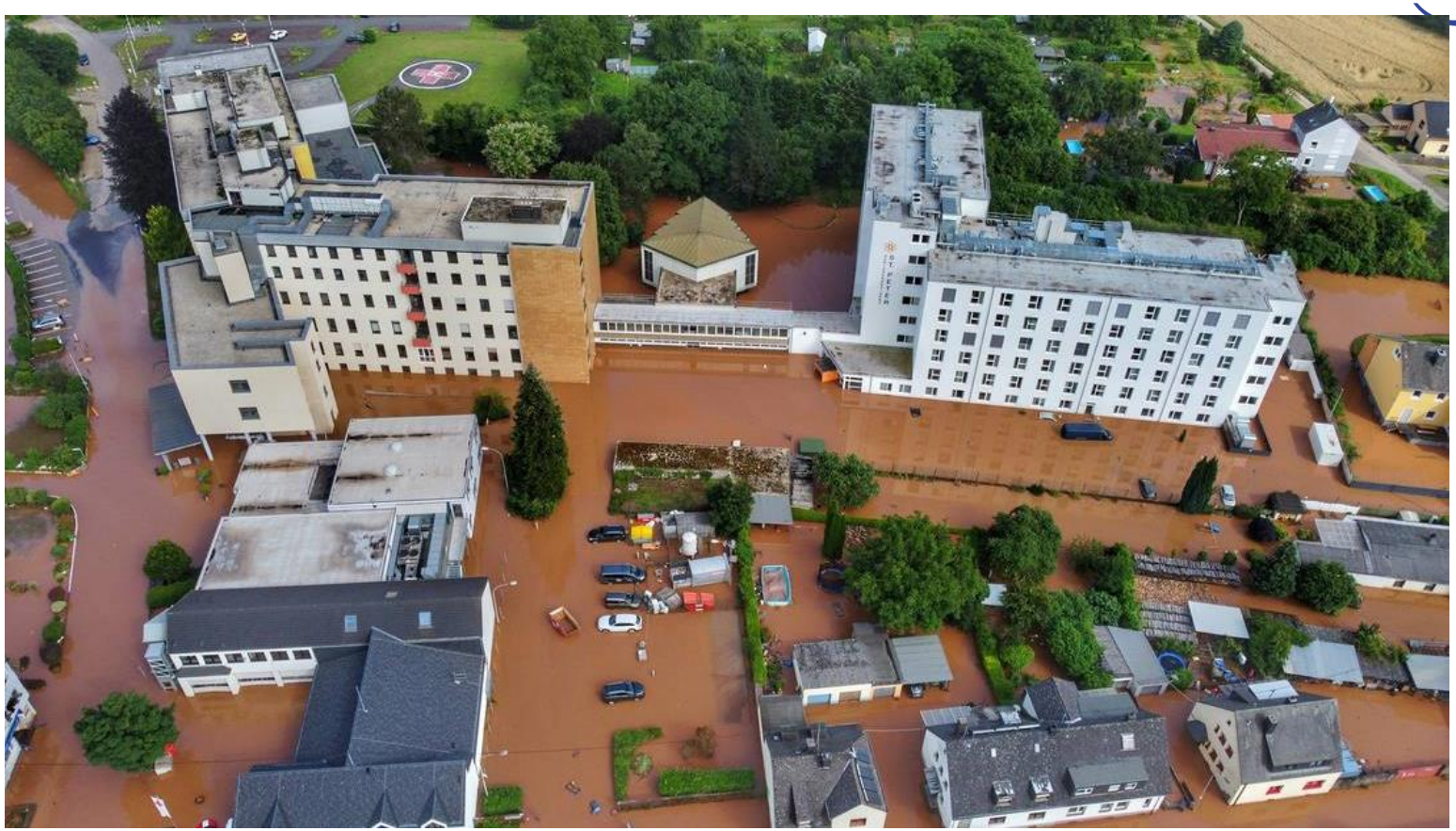
- Registrierungspflicht für alle Einrichtungen (§ 33)

- Nachweispflicht (§ 39 und § 61)
  - Immer für Betreiber kritischer Anlagen, 3-Jahres-Turnus
  - Auf Verlangen auch besonders wichtige Einrichtungen
    - Besonderheit: für Plankrankenhäuser nach § 108 SGB V 5-Jahres-Turnus, der durch RVO verkürzt werden kann
    - Sinn?
      - Verkürzung ist Reaktionsmöglichkeit auf Veränderung der Bedrohungslage
      - Langer Turnus: aufgrund öffentlicher Finanzierung ggf. „Verschonung“, aber das betrifft eigentlich auch viele andere Sektoren

Künftige Vorgaben durch das NIS2UmsuCG

Bußgeldregelungen „á la DSGVO“ (§ 65)

- Umfangreicher Bußgeldkatalog
- Für wichtige und besonders wichtige Einrichtungen weltweiter Konzernumsatz für Bemessung relevant
- aber: Bußgeldvorschriften des BSIG bislang völlig irrelevant (Stand 2023: 1 eingeleitetes OWi-Verfahren wegen fehlerhaftem Nachweis über OTV); aufgrund Vielzahl neu betroffener Einrichtungen ggf. kurzfristig „Verschonung“



Künftige Vorgaben durch das Kritis-DachG

Klinik Ehrang nach der Hochwasser-Katastrophe an der Ahr (dauerhaft geschlossen)

(Quelle Bild: https://www.volksfreund.de/region/trier-trierer-land/am-limit-was-das-ende-der-klinik-ehrang-fuer-die-notfallversorgung-bedeutet_aid-79416695)

Künftige Vorgaben nach dem KRITIS-DachG

- Adressiert die physische Sicherheit
  - Brände, Sabotage, Terror, Strahlungsunfälle, Störungen durch Bauarbeiten, Klimaereignisse
  - Schnittmenge mit Krankenhausalarm- und –einsatzplanung (KAEP) -> Synergien!

- Umsetzung der RCE-RL in eigenem KRITIS-DachG
  - „Dach“ unglücklich gewählt, impliziert „Obergesetz“ zu sein, steht aber auf gleicher Stufe mit BSIG, dessen Anwendungsbereich deutlich größer ist
  - BBK wird Aufsichtsbehörde, erhält dadurch deutliches Kompetenz-Upgrade

Künftige Vorgaben durch das KRITIS-DachG

Anwendungsbereich:

- Nur Betreiber Kritischer Anlagen (§ 4); ggf. dann später wichtige und besonders wichtige Einrichtungen
- Bestimmung über Schwellenwerte in Rechtsverordnung (gemeinsam mit NIS2UmsuCG)
- Sektor Gesundheit: u.a. Gesundheitsdienstleister

Künftige Vorgaben durch das KRITIS-DachG

Dreh- und Angelpunkt: Risikomanagement für physische Gefahren (§ 10)

- Grundlage: staatliche und unternehmenseigene Risikoanalysen (§ § 8, 9)
- Mindestmaßnahmen-Katalog des BBK
- Branchenspezifische Resilienz-Standards (durch Branchenverbände erarbeitet; parallel zu B3S in BSIG)

Künftige Vorgaben durch das KRITIS-DachG

Weitere Pflichten und Regelungen:

- Keine eigene Nachweispflicht, aber Einsichtsrecht BBK in KRITIS-Nachweise des BSIG (passt dogmatisch nicht) (§ 11)
- 3-stufige Meldepflicht bei Sicherheitsvorfällen an gemeinsame Meldestelle des BBK und BSI (§ 12)
  - In bisherigen Entwürfen leider keine 1:1-Entsprechung der Melderegelungen
- Bußgeldvorschriften mit Konzernregelung, vermutlich erst späteres Inkrafttreten

Compliance-Regelungen in NIS2/KRITIS-DachG

- Beide Gesetze mit eigenen Compliance-Vorschriften, die Geschäftsleitung in Pflicht nehmen (§ 38 BSIG-E/ § 14 KRITIS-DachG-E)
- Überwachung der Umsetzung des Risikomanagements
- Letztverantwortung -> keine vollständige Delegation von Compliance-Pflichten
- Persönliche Haftung der Geschäftsleitung für Verstöße
  - Hauptstreitpunkt im gesetzlichen Verfahren; von Verzichtsverbot auf Regresse Abstand genommen; jetzt Gleichlauf mit AktG/GmbHG
- „Schulbank-Pflicht“: Geschäftsleitungen müssen regelmäßig Schulungen wahrnehmen, um überhaupt Überwachungspflicht einhalten zu können (Fachkenntnisse erwerben)

Besondere Haftungsfragen für Krankenhäuser

- Immanentes Risiko von Gesundheitsschäden durch Cybervorfälle
- Bei Angriff auf Uniklinikum Düsseldorf 2020 titelte Presse „Erster Cybertoter“, konnte nicht nachgewiesen werden
- Zivilrecht: Einbettung Cybergefahren in Arzthaftungsregularien (§ § 630a ff. BGB)
  - Bislang kaum diskutiert in Literatur
  - Wohl kein vollbeherrschbares Risiko mit Beweislastumkehr, aber Risikobereich, der zur „Sekundären-Darlegungslast“-Rspr. passt
  - Nachweis effektiver Sicherheitsmaßnahmen über B3S
- Strafrecht: v.a. Fahrlässigkeitsdelikte (§ § 222, 229 StGB)
  - Verantwortliche im Klinikum können Täter sein
  - Sorgfaltsmaßstab: wiederum über B3S
- Zeigt herausragende Rolle des B3S sowie der peniblen Dokumentation über dessen Einhaltung

Gesetzliche Neuerungen durch das DigiG

- Mai 2024 in Kraft getreten
- V.a. Änderungen für elektronische Patientenakte (ePA) und TI
- Neustrukturierung und Erweiterung der Cybersicherheitsvorschriften im SGB V
  - Strukturierung in den § § 390 ff. SGB V
  - Ehemaliger § 75c nun § 391 SGB V: IT-Sicherheit in Krankenhäusern
  - Cloud-Computing in § 393 SGB V: Voraussetzung von C5-Testaten

Gesetzliche Neuerungen durch das DigiG

Änderungen für Krankenhäuser

- § 391 SGB V ist Auffangvorschrift für die IT-Sicherheit von allen Krankenhäusern, die nicht schon BSIG unterfallen
- Orientierung an BSIG, aber „Light-Variante“: Einhaltung von OTV, aber weder Melde- noch Nachweispflicht, auch keine Sanktionen
- Neu: OTV müssen auch „**Sicherheits-Awareness**“ umfassen
  - Klarstellungswirkung: auch bislang umfassten OTV schon Awareness; B3S orientiert sich an ISO 27001 (ISMS), selbstverständlich auch Abschnitt zu Awareness
- Vorschläge des Gesetzgebers für Awareness-Maßnahmen: von Informationsmaterialien über Schulungen bis zu simulierten Angriffen

Optimierungsbedarf im SGB V

- Problem: Keine Kenntnisse über Gefährdungslage (BSIG: über Meldungen) und Reifegrade von Management-Prozessen (BSIG: über Nachweise) bei „kleineren“ Krankenhäusern
  - BReg auf kleine Anfrage (BT-Drs. 20/10907): nur Kenntnisse über Kritis-Krankenhäuser

- Balance zwischen Schutz der Bevölkerung und Überbürokratisierung: zumindest Einführung einer Meldepflicht bei Störungen
  - Ohnehin im Regelfall auch Meldung nach Art. 33 DSGVO
  - Ähnliche Informationen zu sammeln, ggf. mit anderer Zielrichtung auszuwerten
  - Keine Überforderung bei strukturiertem Meldeprozess im Krankenhaus

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen zur Cybersicherheit in allen Bereichen des Gesundheitswesens: