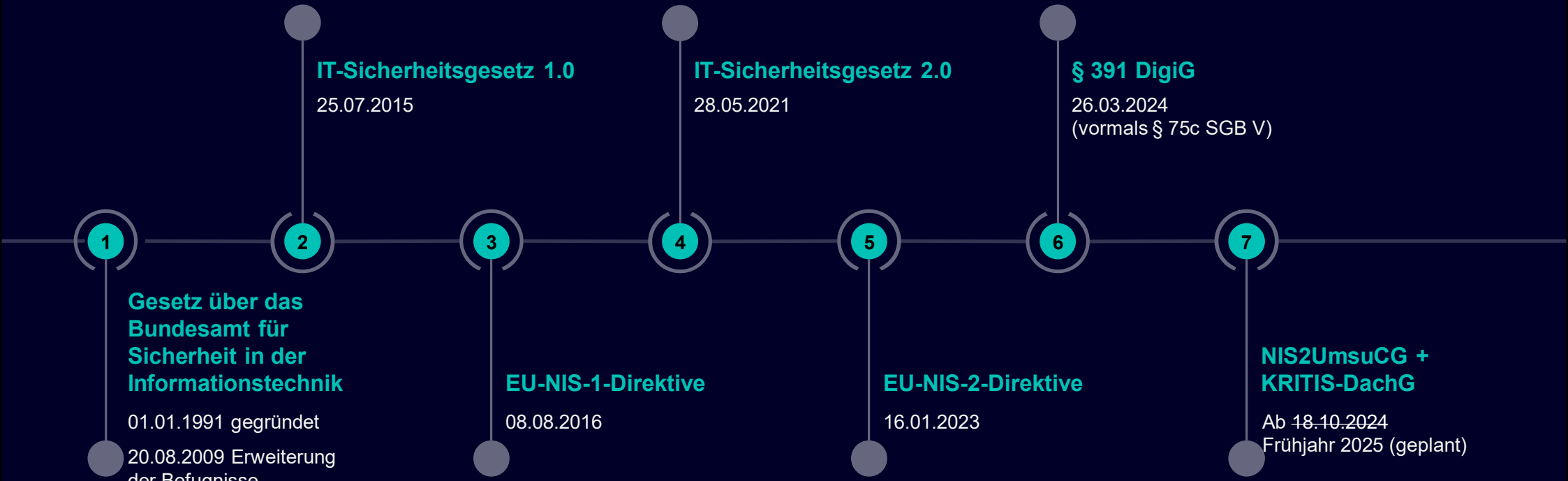
Smart Hospitals

B3S, NIS 2 & Cybersecurity Services

Vorbehaltlich der noch kommenden Änderungen.
Stand November 2024

SIEMENS

Die Gesetzesentwicklung für die IT-Sicherheit in der medizinischen Versorgung



SIEMENS

Überblick der verschiedenen Gesetze mit dem einheitlichen Ziel, die medizinische Versorgung sicherzustellen

§ 75c SGB V

Überführt in
§ 391 DigiG

Ziel
IT-Sicherheit in Krankenhäusern

EU-NIS-2-Direktive

Überführung in
Länderrecht

Ziel
IT-Sicherheit

EU-RCE/CER-Direktive

Überführung in
Länderrecht

Ziel
Resilienz und Krisen

SIEMENS

Ein Überblick der Regularien inklusive Schwellenwerte

§ 391 DigiG

- Verpflichtung zur IT-Sicherheit gemäß „Stand der Technik“
- Verankerung des B3S für die *medizinische Versorgung*, im Gesetzestext als geeignete Umsetzungsform empfohlen

Für alle Krankenhäuser verpflichtend umzusetzen

NIS2UmsuCG

- ≥ 50 Mitarbeitende **oder** ≥ 10 Mio. € Umsatz und ≥ 10 Mio. € Bilanz → **wichtige Einrichtung**
- ≥ 250 Mitarbeitende **oder** ≥ 50 Mio. € Umsatz und ≥ 43 Mio. € Bilanz **oder** Betreiber kritischer Anlagen (KRITIS-Betreiber) → **besonders wichtige Einrichtung**

KRITIS-DachG

- Krankenhäuser, wenn diese 500 Tsd. Personen (hier: Patienten) versorgen
- Registrierung durch staatliche Behörden möglich, u.a. als Folge von Risikoanalysen

SIEMENS

Was ist
§ 391 DigiG?

Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens. (DigiG) § 391 regelt die **IT-Sicherheit in Krankenhäusern.**

SIEMENS

§ 391 DigiG – Überblick

Eckpunkte

Ziel

Absicherung aller relevanten Prozesse und Systeme im Betrieb sowie der IT-Sicherheit in Krankenhäusern

Fokus

IT-Sicherheit in Krankenhäusern, optional Branchenspezifischer Sicherheitsstandard (B3S) als vollumfängliche Umsetzungsempfehlung

Adressat

Alle Krankenhäuser

Gültigkeit

01.01.2022 (SGB V § 75c)
→ § 391 DigiG seit 26.03.2024

Frist

B3S wird spätestens zum 01.01.2025 aktualisiert

SIEMENS

§ 391 DigiG – Maßnahmen

Mitarbeiter der Führungsebene

Die Geschäftsführung trägt die **Gesamtverantwortung** für die Umsetzung der erforderlichen Maßnahmen (für den B3S).

- IT-Sicherheit (TOMs) nach „Stand der Technik“
- Vermeidung von Störungen der **Verfügbarkeit, Integrität und Vertraulichkeit**
- Betriebliches Kontinuitätsmanagement
- Robuste/resiliente Architektur
- Informationssicherheits-managementsystem (ISMS)
- Absicherung aller relevanten Prozesse und Systeme für den Betrieb
- Security Awareness des Personals
- Vorfallerkennung und Behandlung
- Asset-Management
- **B3S** erfüllt die Anforderungen

SIEMENS

Was ist **NIS2UmsuCG?**

Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz ist ein deutscher Gesetzentwurf, der die EU-Richtlinie NIS 2 in nationales Recht umsetzen soll.

NIS 2
Betroffene Industriesektoren

Sonstige kritische Sektoren

Smart Hospitals

Sektoren mit hoher Kritikalität

SIEMENS

NIS2UmsuCG – Überblick

Eckpunkte

Ziel

Erreichung eines hohen Grundlevels in der Cyber-security innerhalb der EU

Revision der NIS 1 (erste europaweite Cybersecurity-Richtlinie)

Fokus

Security-Richtlinien für Netzwerke und Informationssysteme, Meldepflichten an das BSI, Risikomanagement, IT-Sicherheit in der Lieferkette

Adressat

18 Sektoren: Krankenhäuser mit den folgenden Schwellenwerten:

≥ 50 Mitarbeiter **oder** ≥ 10 Mio. € Umsatz und ≥ 10 Mio. € Bilanz
→ **wichtige Einrichtungen**

≥ 250 Mitarbeiter **oder** ≥ 50 Mio. € Umsatz und ≥ 43 Mio. € Bilanz
→ **besonders wichtige Einrichtungen**

Gültigkeit

Umsetzung der NIS 2 in nationales Recht und Anwendung dieses Gesetzes ab Frühjahr 2025

NIS 2 hat die NIS 1 seit 16.01.2023 ersetzt

Frist

Umsetzungspflicht erfolgt unmittelbar mit Verabschiedung des Gesetzes

NIS2UmsuCG – Maßnahmen

Mitarbeitende der Führungsebene

- können **persönlich** für Schäden **haftbar** gemacht werden
- können sogar von ihren **Funktionen entbunden** werden!

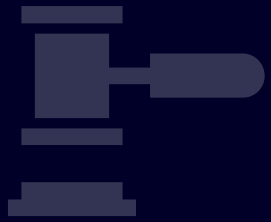
- Richtlinien zur Risikoanalyse und Risikomanagement
- Incident Handling
- Business Continuity
- Sicherheit in der Lieferkette
- Erfassung von Informationssystemen und Umgang mit Schwachstellen
- Konzepte und Verfahren
- Cybersicherheitsschulungen
- Kryptographie und Verschlüsselung
- Zugriffskontrollrichtlinien und Asset-Management
- Multi-Faktor-Authentifizierung

SIEMENS

Meldepflicht

Was? Bis wann?

- Erstmeldung innerhalb von 24 h an das BSI, nachdem der Vorfall bekannt wurde
- Nach 72 h Folgemeldung mit Details zu Schweregrad und Auswirkungen
- Weitere Zwischenmeldungen auf Nachfrage durch das BSI
- Fortschritts- oder Abschlussmeldung spätestens einen Monat, nachdem der Vorfall gemeldet und behandelt wurde, dann jedoch mit Beschreibung, Ursachen, Maßnahmen etc.



Sanktionen

Bußgelder bei Nichteinhaltung der vorgegebenen Maßnahmen und/oder Meldepflichten:

- Wichtige Einrichtungen Min. 7 Mio. € oder 1,4% des weltweiten Jahresumsatzes
- Besonders wichtige Einrichtungen Min. 10 Mio. € oder 2,0% des weltweiten Jahresumsatzes
- Basierend auf Grad des Verstoßes und Größe des Unternehmens

Was ist **KRITIS-DachG?**

Das KRITIS-Dachgesetz ist ein deutscher Gesetzentwurf, der die Resilienz und physische Sicherheit kritischer Infrastrukturen regelt. Es setzt die EU-Richtlinie EU RCE in Deutschland um und legt zusätzliche Pflichten für Betreiber kritischer Anlagen fest.

KRITIS-DachG – Überblick

Eckpunkte

Ziel

Erweitert den Schutz kritischer Infrastrukturen über die IT-Sicherheit hinaus durch Erhöhung der Resilienz gegenüber physischen Bedrohungen, Pandemien und dergl.

Fokus

Meldepflichten, physische Sicherheit, Personal und Krisenmanagement

Aufsicht: KRITIS-Aufsicht wird um das BBK erweitert, gemeinsam mit dem BSI und teilweiser Einbindung von Landesbehörden

Adressat

- Krankenhäuser, wenn diese 500 Tsd. Personen (hier: Patienten) versorgen
- Registrierung durch staatliche Behörden möglich, u.a. als Folge von Risikoanalysen

Gültigkeit

Das Dachgesetz tritt voraussichtlich im Frühjahr 2025 in Kraft

Frist

Registrierung innerhalb von drei Monaten nach Identifizierung

Risikoanalyse neun Monate nach Registrierung, dann alle vier Jahre

Umsetzung Resilienzmaß-nahmen neun bis zehn Monate nach Registrierung

KRITIS-DachG – Maßnahmen

Mitarbeitende der Führungsebene

- Geschäftsleitende **müssen** die **Maßnahmen für Resilienz** und deren **Umsetzung garantieren**
- Es herrscht eine allgemeine Dokumentationspflicht im Rahmen des Resilienzplans und des Risikomanagements. Deren **Nachweise** sind auf **Nachfrage vorzulegen**

Krisenmanagement

Resilienzplan

Business Continuity Management

Reaktion auf und Abwehr von Vorfällen sowie Begrenzung negativer Folgen

Angemessener physischer Schutz der Liegenschaften und kritischen Anlagen

Richtlinien und Verfahren

Schulungen, Übungen, Sensibilisierung des Personals

Risikoanalysen und Registrierungspflicht bei Betreibern

Sicherheitsmanagement für eigenes und externes Personal

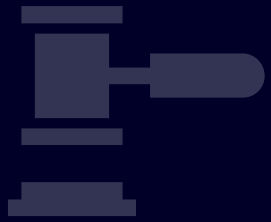
Wiederherstellung der kritischen Dienstleistung nach Vorfällen

SIEMENS

Meldepflicht

Was? Bis wann?

- Meldung innerhalb von 24 h nachdem ein Vorfall bekannt wurde, an die gemeinsame Meldestelle von BSI und BBK
- Ausführlicher Bericht spätestens einen Monat nach Meldung des Vorfalls
- Parallel dazu Meldung an das BSI über NIS-2-relevante Vorfälle



Sanktionen

Bußgelder bei Nichteinhaltung der vorgegebenen Maßnahmen und/oder Meldepflichten:

- Keine Unterlagen vorlegen, ob eine Anlage kritisch ist, trotz Anordnung: bis 500 Tsd. EUR
- Nicht übermitteln von (Audit-)Ergebnissen: bis 200 Tsd. EUR
- Keine Unterlagen zum Nachweis der Umsetzung von KRITIS-DG Anforderungen vorlegen, trotz Anordnung: bis 100 Tsd. EUR
- Unvollständige oder unrichtige Angaben bei der Registrierung: bis 50 Tsd. EUR

Vielen Dank!

Kontakt

Herausgeber: Siemens AG

Nathalie Lazar

Siemens AG
Siemens Deutschland
Vertical Sales
RC-DE SI B ASM A9 S V
Gateway Gardens
De-Saint-Exupéry-Str. 5

Mobil +49 (173) 5904654

E-Mail nathalie.lazar@siemens.com

SIEMENS