TaylorWessing

IT-Sicherheitsrecht: Neuerungen durch NIS2 – Fokus Energiesektor

Dr. Paul Voigt, Lic. en Derecho, CIPP/E
Rechtsanwalt | Fachanwalt für IT-Recht

25.4.2023

KRITIS-Betreiber

Adressaten: Betreiber Kritischer Infrastrukturen (KRITIS), § 2 Abs. 10 BSIG

*„Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und von hoher Bedeutung (**Qualität**) für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe (**Quantität**) oder Gefährdungen für die öffentliche Sicherheit eintreten würden.“*

KRITIS-Betreiber

Bestimmung der KRITIS-Betreiber gemäß der BSI-KritisV in vier Schritten:

- Dienstleistungen, die wegen ihrer Bedeutung als kritisch anzusehen sind
- z.B.: die Versorgung der Allgemeinheit mit Elektrizität / Gas / Kraftstoff und Heizöl / Fernwärme (§ 2 Abs. 1 KritisV)

- Kategorien von Anlagen oder deren Teile, die für die Erbringung dieser kritischen Dienstleistung erforderlich sind
- z.B.: Stromerzeugungsanlage, Gasförderanlagen und -speicher, Raffinerien, Heiz-kraftwerke und Fernwärme-netze

- Berechnung des relevanten Versorgungsgrades, geht grds. von 500.000 betroffenen Menschen aus
- Quantitativer Ansatz, entgegen der NIS-Richtlinie, die ebenfalls von qualitativen Kriterien ausgeht
- z.B.: Installierte Netto-nennleistung von 104 MW

Generelle Anforderungen an KRITIS-Betreiber

Registrierungspflicht
(§ 8b Abs. 3 BSIG), BSI kann auch selbst Betreiber als KRITIS registrieren

Einrichtung einer Kontaktstelle, über die Kommunikation mit dem BSI erfolgt

TOMs und Nachweiserbringung

Meldepflichten

Einsatz kritischer Komponenten

IT-Sicherheitsanforderungen, § 8a BSIG

- Verpflichtung, angemessene **organisatorische und technische Vorkehrungen** zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme zu treffen, die dem **Stand der Technik** entsprechen
- Ab dem 1. Mai 2023 auch Einsatz von **Systemen zur Angriffserkennung** (§ 8 Abs. 1a BSIG)
- **Branchenspezifische Sicherheitsstandards** (B3S), § 8a Abs. 2 BSIG
  - **Können von KRITIS-Betreibern oder ihren Branchenverbänden erarbeitet werden**
  - **BSI stellt auf Antrag die Eignung der Sicherheitsstandards fest**
    - **B3S besteht u.a. für Aggregatoren und Fernwärmenetze** (gültig bis April 2023)

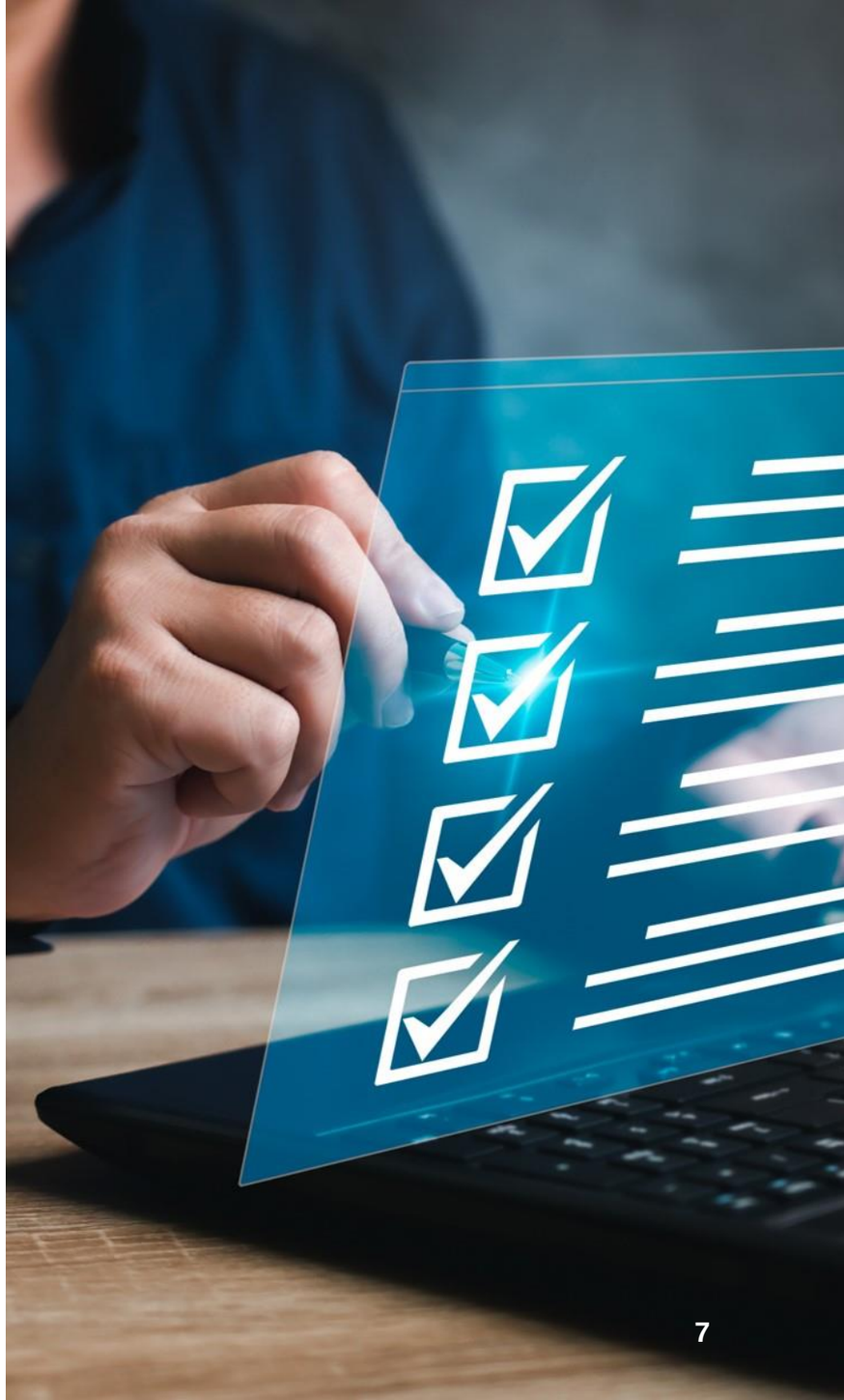
Auditierungspflicht nach § 8a BSIG

Auditierungspflicht, § 8a Abs. 3 BSIG

- Erfüllung der Sicherheitsstandards müssen von KRITIS-Betreibern alle zwei Jahre durch geeignete Audits, Prüfungen oder Zertifizierung nachgewiesen werden

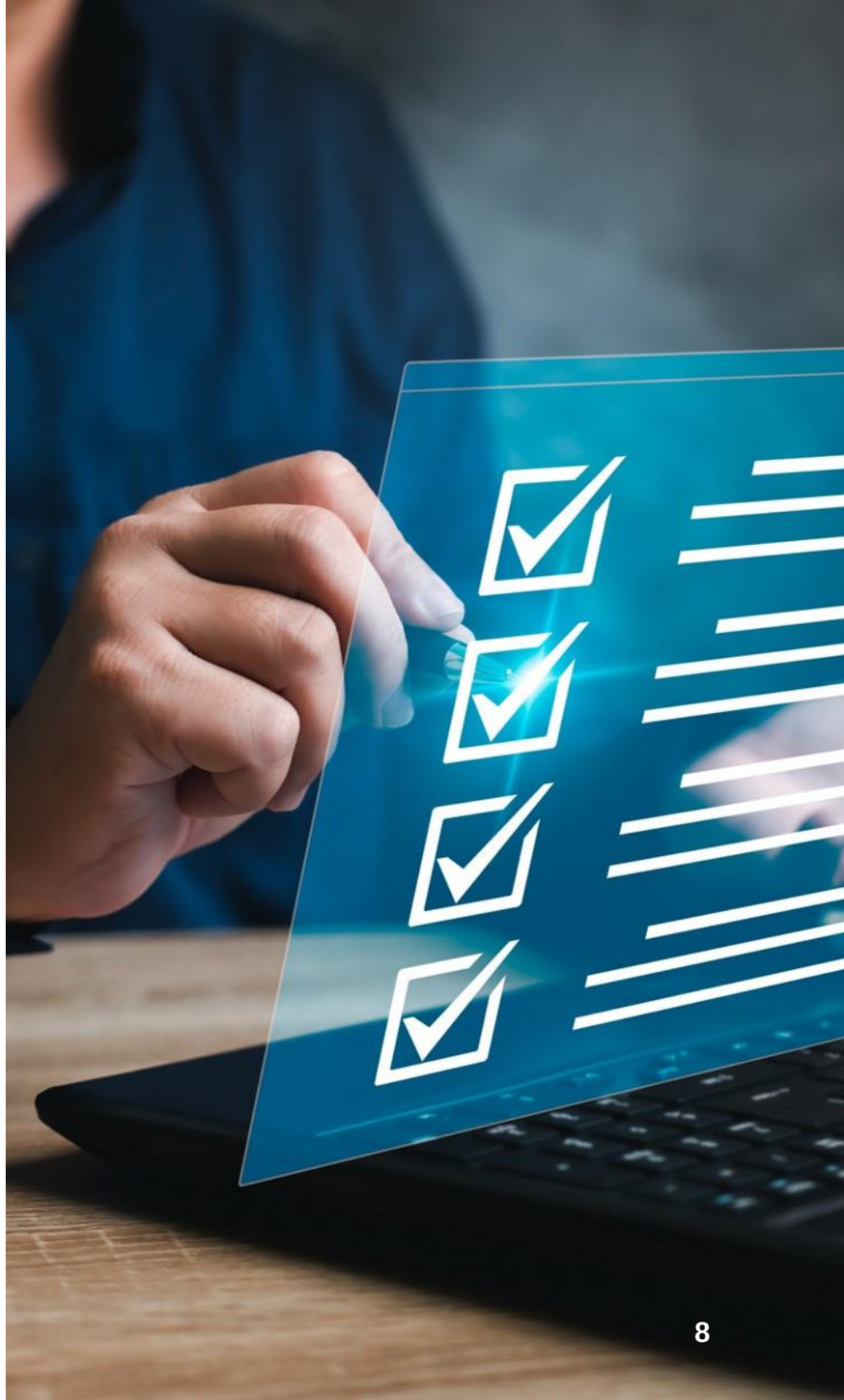
Meldepflichten, § 8b BSIG

- **Störungen** von IT- Systemen, Komponenten oder Prozessen, die zu Ausfällen oder Beeinträchtigungen der Funktionsfähigkeit der KRITIS geführt haben **und**
- **Erhebliche Störungen** die zu Ausfällen oder Beeinträchtigungen der Funktionsfähigkeit der KRITIS führen können, müssen an das BSI gemeldet werden
- **Störung** = Funktionsfähigkeit der erbrachten kritischen Dienstleistung muss bedroht sein
- **Erheblich:**
  - Störungen, die **nicht automatisiert** oder **mit wenig Aufwand** mithilfe der Schutzmaßnahmen, sondern nur mit deutlich **erhöhtem Ressourcenaufwand** gemäß § 8a BSIG **abgewehrt werden können**



Meldepflichten, § 8b BSIG

- Nennung der technischen Rahmenbedingungen, der möglichen grenzübergreifenden Auswirkungen und der erbrachten kritische Dienstleistung sowie die Auswirkungen der Störung auf diese Dienstleistung
- Möglichkeit der **stufenweisen Meldung:**
  1. **Informationen, die ohne erheblichen Rechercheaufwand ermittelbar sind**
  2. **Ergänzung der Informationen**
- **Anonyme Meldung** möglich, sofern kein Ausfall oder Beeinträchtigung (folgt aus § 8b Abs. 4 S. 3 BSIG)



Einsatz Kritischer Komponenten und Sanktionen

- Meldepflichten für den Einsatz Kritischer Komponenten:
  - Anzeigepflicht beim erstmaligen Einsatz eines IT-Produkts der gleichen Art, das gesetzlich als KRITIS-Komponente festgelegt ist (§ 9b Abs. 1 BSIG)
- Sanktionen: Bußgelder bis 20 Mio. EUR bei Unternehmen möglich

Energiewirtschaftsgesetz

Anwendungsbereich

- Alle Betreiber von Energieversorgungsnetzen und Betreiber von solchen Energieanlagen, die gem. § 10 Abs. 1 BSIG als Kritische Infrastruktur bestimmt wurden

Allgemeine Anforderungen

- **Kontaktstelle beim BSI registrieren**

IT-Sicherheitspflichten

- **Gewährleistung eines angemessenen Schutzes gegen Bedrohungen für TK- und EDV-Systeme, § 11 Abs. 1a, b EnWG**
- **Einhaltung des Sicherheitskatalogs von BNetzA u. BSI mit entsprechender Dokumentation**
- **Einsatz von Systemen zur Angriffserkennung, Frist: 1. Mai 2023 (§ 11 Abs. 1e EnWG)**

Energiewirtschaftsgesetz

Meldepflichten an BSI

- **Bei IT-Störungen gem. § 11 Abs. 1c EnWG:**
  - (erhebliche) Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse,
  - die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben (bzw. führen können)

Energiewirtschaftsgesetz

Nachweispflicht

- Dass eine Kontaktstelle beim BSI registriert wurde,
- erstmalig zum 1. Mai 2023,
- dann alle zwei Jahre.

Kritische Komponenten

- Bis 22. Mai 2023 erstellen BNetzA und BSI eine Katalog mit **Kritischen Komponenten**
  - Einhaltung der Vorgaben spätestens 6 Monate nach dessen Inkrafttreten verpflichtend

Ausblick:
Reform der europäischen Richtlinie – NIS 2.0

- **Am 16.01.2023 in Kraft getreten:**
  - *Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)*
    - Löst die 2016 in Kraft getretene NIS-Richtlinie ab und entwickelt sie weiter

- **Änderungen im Anwendungsbereich:**
  - Differenzierung zw. Betreibern wesentlicher Dienste und Anbieter digitaler Dienste aufgehoben → Unterscheidung anhand des Grads der Kritikalität des Sektors nach **„wesentlich“** u. **„wichtig“**

- Genaue Schwellenwerte für wesentliche u. wichtige Dienste werden direkt durch Richtlinie bestimmt
  - Erforderlich ist – unbeschadet einiger Ausnahmen – die **Beschäftigung von mindestens 50 Personen** oder ein **Jahresumsatz von mehr als 10 Mio. Euro**

NIS 2: Anwendungsbereich

- **Erweiterung der Sektoren**
  - **Wesentliche Einrichtungen**
    - Neu: Abwasser, Verwaltung von IKT-Diensten, Öffentliche Verwaltung, Weltraum
    - Ergänzungen: Energie, Gesundheit, Digitale Infrastruktur
- NIS 2 findet Anwendung bei Energieunternehmen in den Teilsektoren
- Elektrizität,
  - **Neue Einrichtungen: Elektrizitätserzeuger, nominierte Strommarktbetreiber, Anbieter von Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdiensten, Betreiber von (Endnutzer-)Ladepunkten**
- Fernwärme und –kälte (neu)
- Erdöl,
  - **Neue Einrichtung: zentrale Bevorratungsstellen**
- Erdgas und
- Wasserstoff (neu).

NIS 2: TOOMs

- **Umfangreiche Maßnahmen für Betreiber wesentlicher und wichtiger Dienste**
  - **Angemessene TOOMs sind zu ergreifen (risikobasiert nach Größe, Risiken, Ausmaß der Gefährdung, etc.)**
  - **Stand der Technik**
  - **Maßnahmenkatalog ist umzusetzen:**
    - Risikoanalyse- und Sicherheitskonzepte
    - Prävention von Sicherheitsvorfällen
    - Lieferkettensicherheit
    - Betriebskontinuität
    - HR Security
    - Verschlüsselungsstrategien
    - Klares Krisenmanagement
    - Etc.
  - **EU Kommission kann Pflichten konkretisieren**
  - **Ggf. zukünftig Pflicht zur Nutzung zertifizierter Produkte**

NIS2:
Leitungsorgane und Meldepflichten

- Verantwortlichkeit der **Leitungsorgane** – Überwachungspflicht und Haftung, sowie regelmäßige Weiterbildungspflicht (Art. 20)
- Genau Vorgaben über Ablauf, Inhalt und Zeitrahmen der Meldung eines Sicherheitsvorfalls (Art. 23)
  - „Frühwarnung“ grundsätzlich innerhalb von 24 Stunden nach Kenntnisnahme (rechtswidriger Angriff? Grenzüberschreitende Auswirkungen?)
  - Spätestens 72 Stunden nach Kenntnisnahme ausführliche Meldung des Sicherheitsvorfalls (Bewertung Schwere und Auswirkungen des Vorfalls)
  - Spätestens einen Monat nach der Sicherheitsvorfallsmeldung muss ein Abschlussbericht eingereicht werden, welcher mindestens Folgendes enthält: Eine detaillierte Beschreibung des Vorfalls, dessen Ernsthaftigkeit und Auswirkung, dessen (wahrscheinlicher) Ursprung, unternommene und laufende Minderungsmaßnahmen
  - Ggf. auch Meldung über „Beinahe-Vorfälle“, Art. 13 Abs. 3, Art. 30
  - Ggf. auch Benachrichtigung an Empfänger der Dienstleistungen wenn Beeinträchtigung für diese, sowie u.U. der Öffentlichkeit (Art. 23 Abs. 1, 7)

NIS2:
Wie geht es weiter?

Umsetzung in nationales Recht bis **Oktober 2024**

Konkrete **Umsetzung** durch den deutschen Gesetzgeber erforderlich; entsprechende „Schärfung“ der Pflichten

Bußgelder: bis zu 10 Mio EUR / 2% des weltweiten Jahresumsatzes

Herzlichen Dank für Ihre Aufmerksamkeit!

Ihre Fragen

Ihr Ansprechpartner

Paul Voigt ist spezialisiert auf IT- und Datenschutzrecht. Er begleitet Mandanten in nationalen und internationalen Datenschutzprojekten und verfügt über eine ausgewiesene Expertise im IT-Vertrags- und IT-Sicherheitsrecht sowie im E-Commerce.

Er berät in vier Sprachen – Deutsch, Englisch, Französisch, Spanisch – Unternehmen verschiedenster Art: vom frisch gegründeten Start-up über mittelständische Unternehmen bis hin zu Global Playern. Daneben vertritt er Online-Glücksspielanbieter in zivil- und verwaltungsrechtlichen Verfahren bis zum Bundesverwaltungsgericht. Außerdem betreut er regelmäßig Mandanten aus Übersee bei ihrem Markteintritt in Europa.

Zahlreiche Veröffentlichungen und Empfehlungen weisen die Fachkompetenz von Paul Voigt aus.

Sprachen

- Deutsch, Englisch, Spanisch, Französisch

Name der nächsten Generation - Informationstechnologie: Datenschutz, The Legal 500 Deutschland 2019 – 2021

Führender Name als Aufsteiger in der Informationstechnologie; Empfohlen für Datenschutz- und IT-Recht:
„super und schneller Jurist“, „umfangreiche Kompetenz“, „Rising Star“, „gut bei Themen mit IT-sicherheitsrechtlichen Bezügen“, JUVE Handbuch, 2020/2021

„Paul Voigt verbindet ein nahezu unerschöpfliches Fachwissen mit einem ebenso großen wirtschaftlichen Verständnis“, The Legal 500 Deutschland, 2020

Ausgezeichnet als „Anwalt des Jahres“ für Datenschutzrecht, Best Lawyers in Deutschland, Handelsblatt, 2020

TOP Anwalt für Datenschutzrecht, WirtschaftsWoche 2020 und 2019

Hervorgehoben als Best Lawyer für Datenschutzrecht, Best Lawyers in Germany, Handelsblatt 2020 und 2019

Dr. Paul Voigt, Lic. en Derecho, CIPP/E

Partner
Berlin

+49 30 885636-410
p.voigt@taylorwessing.com

Beratungsschwerpunkte

- Informationstechnologie/ Telekommunikation
- Urheber- & Medienrecht
- Litigation & Dispute Resolution
- Technology, Media & Communications

Europa > Mittlerer Osten > Asien

taylorwessing.com