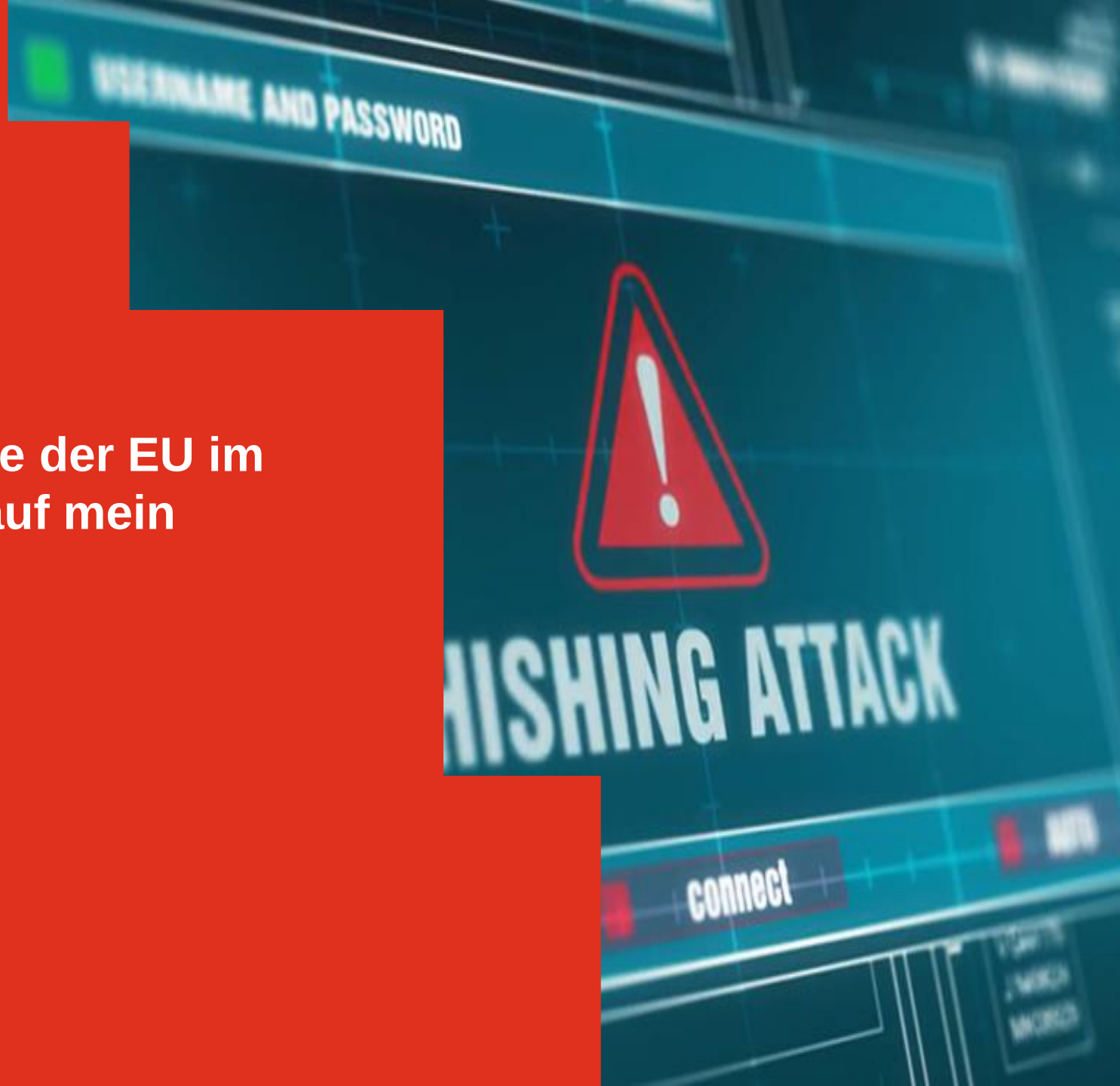
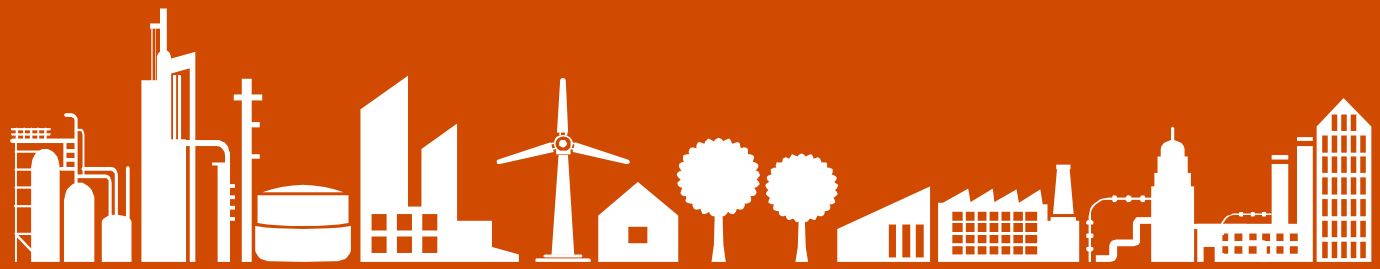
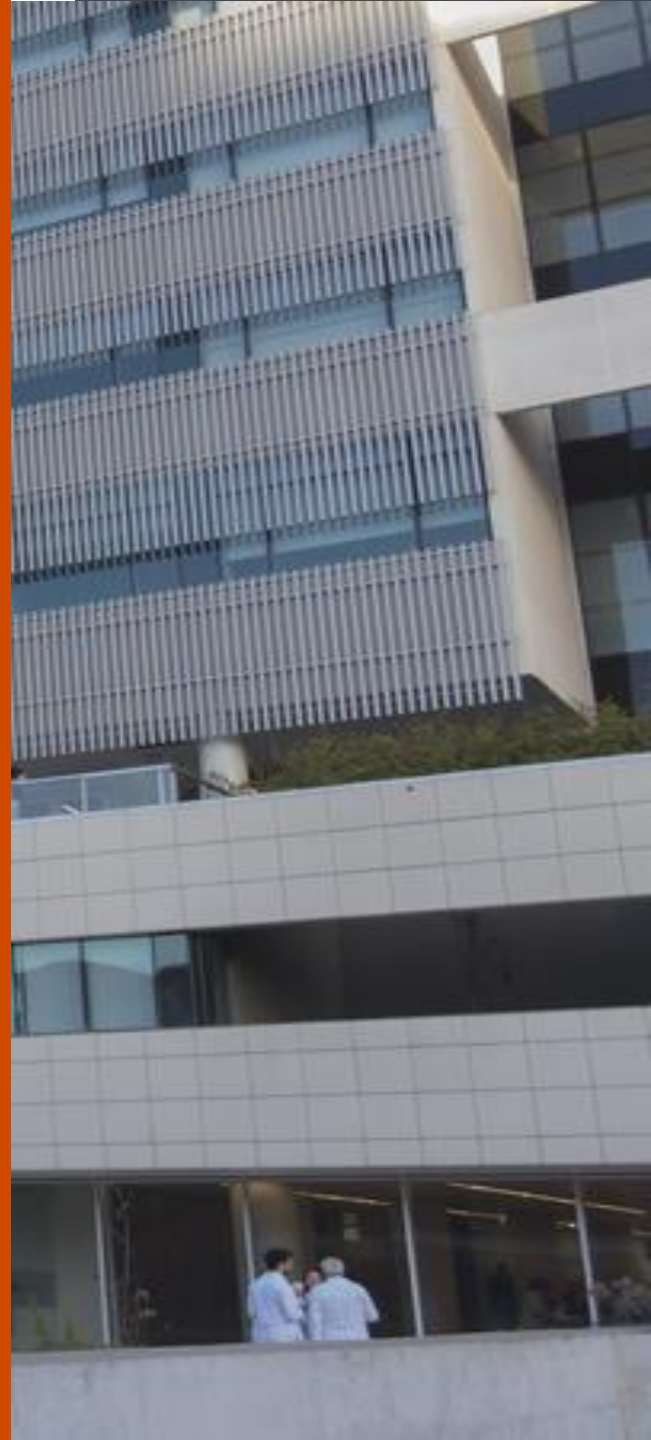
Die neue Cybersecurity-Richtlinie der EU im Überblick: Wie wirkt sich NIS-2 auf mein Unternehmen aus?



Agenda

1. Rechtsgeschichtliche Entwicklung
2. NIS2 und NIS2UmsuCG
3. Betroffene Einrichtungen
4. Fallbeispiele
5. Pflichten für betroffene Einrichtungen
6. Meldeverfahren und Befugnisse des BSI
7. Haftungsrisiken und Sanktionen
8. Zusammenfassung





Unsere Experten für die Erfüllung der NIS2 Anforderungen in Ihrem Unternehmen

André Glenzer (DE)
PwC | Partner
Mobile: +49 160 94470376
Email:
andre.glenzer@pwc.com
PwC Cyber Security Services GmbH
Georg-Glock-Straße 22
40474 Düsseldorf

- Seit 2021 bei PwC Cybersecurity Services GmbH
- Über 20 Jahre Cybersicherheit- & Datenschutzerfahrung
- Fokus auf:
  - Aufbau und Auditierung von ISMS nach BSI IT – Grundschutz und ISO 27001
  - Audits im Bereich KRITIS § 8a und eIDAS
- Gestaltet zusammen mit dem BSI relevante Aspekte der oben genannten Rahmenwerke.
- Koordiniert aktuell ein Expertenteam über ganz Deutschland
- Deckt das gesamte Spektrum der Informationssicherheitsdienstleistungen bei PwC ab

Mailin von Knobelsdorff (DE)
PwC | Manager
Mobile: +49 1515 0841576
Email:
mailin.von.Knobelsdorff@pwc.com
PwC WPG GmbH
Kapelle-Ufer
410117 Berlin

- Über fünf Jahre Erfahrung im Risk Consulting
- Fokus auf:
  - BSI IT-Grundschutz und KRITIS Regulatorik
  - Beratung, Implementierung und Audits
- Projekterfahrung von Informationssicherheitsansätzen für öffentlichen Sektor
- § 8a Abs. 3 und 4 BSIG Nachweisprüfung bei KRITIS in unterschiedlichen Sektoren, Großkonzernen
- Zertifizierte ISO 27001 Lead Auditorin

Die **PwC Cyber Security Services GmbH** arbeitet seit vielen Jahren mit Normungsgremien und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen. PwC CSS ist unter anderem **zertifizierter IT-Sicherheitsdienstleister des Bundes**. Die Mitarbeitenden sind hochspezialisierte Experten und Mitautoren **des IT-Grundschutzkompeniums des BSI** sowie langjährige Ausbilder der BSI IT-Grundschutzauditoren und BSI IS-Revisoren. Zudem ist die PwC CSS seit vielen Jahren Inhaber des BSI Rahmenvertrags und konnte den Rahmenvertrag im letzten Jahr erneut gewinnen.

Der Kreis der Adressaten der KRITIS-Regulierungen nimmt auf nationaler und europäischer Ebene stetig zu

Entwicklung des IT-Sicherheitsrechts für KRITIS

IT-Sicherheitsgesetz 1.0 = Änderungsgesetz zum BSIG, EnWG, TKG, AtG und TMG

Verpflichtet Betreiber Kritischer Infrastrukturen IT angemessen abzusichern und diese Sicherheit überprüfen zu lassen.

Neue Rechtssetzung durch die EU

NIS 2.0 & RCE (Resilience of Critical Entities) (Umsetzung bis 17. Oktober 2024)

- Referentenentwurf (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG)
- Erweiterter Anwendungsbereich: neue Sektoren und „size-cap rule“
- Erweiterungen der Pflichten:
  - Konkretisierung der Maßnahmen, Meldepflichten u.s.w.
  - Governance und Organhaftung

DORA (Digital Operational Resilience Act) VO (Anwendung bis 17.1.2025)

- Betriebsstabilität digitaler Systeme des Finanzsektors

2015 | 2016 | 2017 | 2021 | 2022/2023 | Zukunft

BSI-Kritisverordnung

Definition Sektoren

Schwellenwerte (Bedeutung des Versorgungsgrads)

Umsetzungsgesetz NIS 1

Neu: Regelungen für Anbieter Digitaler Dienste

IT-Sicherheitsgesetz 2.0

Einsatz von **Systemen zur Angriffserkennung** (§ 8a Abs. 1a)

Neuer Sektor: **Siedlungsabfallentsorgung**

Selbsterklärung zur IT-Sicherheit: **Unternehmen im besonderen öffentlichen Interesse** (§ 8f)

KRITIS-Dachgesetz

- Umsetzung der RCE Richtlinie
- Kohärente Regelungslogik

(IT Sicherheitsgesetz 3.0)/ NIS2UmsuCG

Inkrafttreten DORA

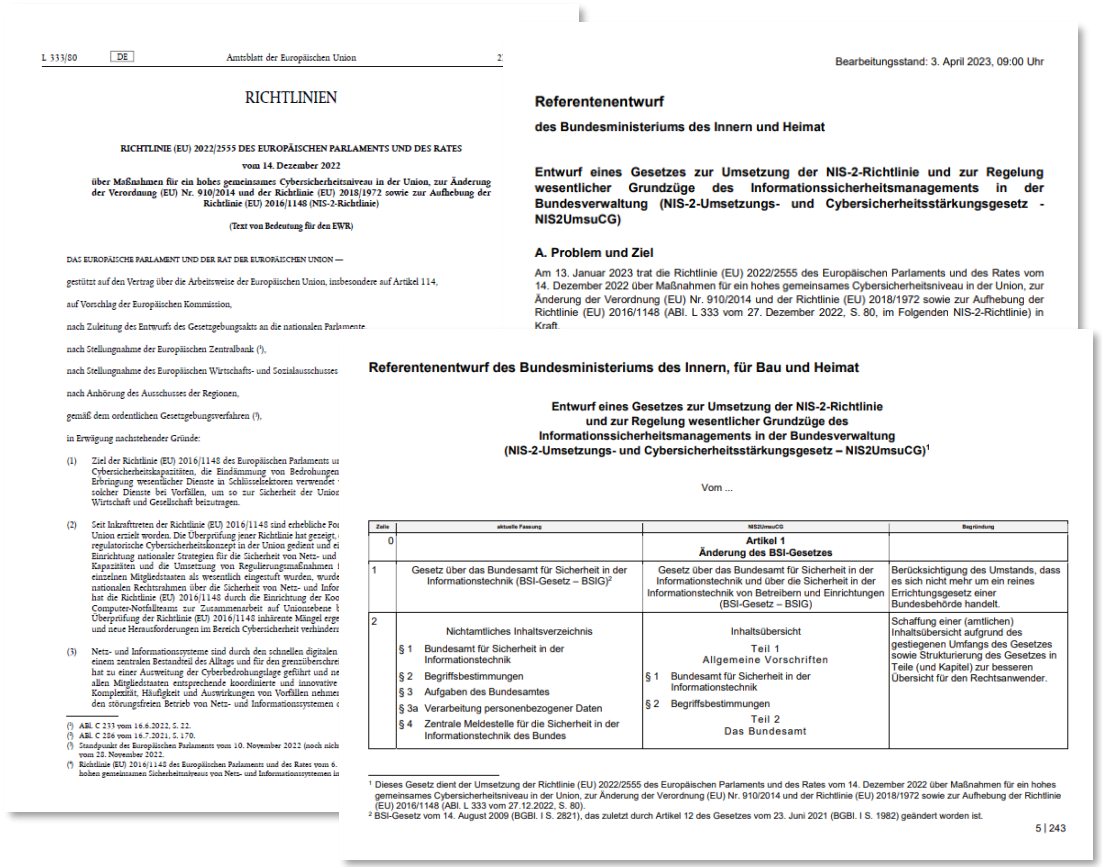
PwC

Quelle: Referentenentwurf des NIS2UmsuCG ist eine inoffizielle Veröffentlichung.

NIS-2 und das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz bilden den Kern der neuen KRITIS- Cybersicherheitsregulierung

Was ist NIS-2?

- NIS-2 ist eine Richtlinie der EU, mit dem Ziel ein hohes gemeinsames Cybersicherheitsniveau sicherzustellen
- Umsetzungspflicht der Mitgliedstaaten bis zum 17. Oktober 2024
- In Deutschland: Referentenentwurf des BMI (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG) / Verabschiedung des Gesetztes wird in DE bis Ende 2023 erwartet



L 333/80 DE Amtsblatt der Europäischen Union 27.12.2022

RICHTLINIEN

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

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)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank (1),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses (2),

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren (3),

in Erwägung nachstehender Gründe:

(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments u... Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen... Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet... solcher Dienste bei Vorfällen, um so zur Sicherheit der Union... Wirtschaft und Gesellschaft beizutragen.

(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fo... Union erzielt worden. Die Überprüfung jener Richtlinie hat gezeigt,... regulatorische Cybersicherheitskonzept in der Union gedient und ei... Einrichtung nationaler Strategien für die Sicherheit von Netz- und... Kapazitäten und die Umsetzung von Regulierungsmaßnahmen... einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde... nationalen Rechtsrahmen über die Sicherheit von Netz- und Infor... hat die Richtlinie (EU) 2016/1148 durch die Einrichtung der Koo... Computer-Notfallteams zur Zusammenarbeit auf Unionsebene... Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel erge... und neue Herausforderungen im Bereich Cybersicherheit verhinder...

(3) Netz- und Informationssysteme sind durch den schnellen digitalen... einem zentralen Bestandteil des Alltags und für den grenzüberschre... hat zu einer Ausweitung der Cyberbedrohungslage geführt und ne... allen Mitgliedstaaten entsprechende koordinierte und innovative... Komplexität, Häufigkeit und Auswirkungen von Vorfällen nehmen... den störungsfreien Betrieb von Netz- und Informationssystemen...

(1) ABl. C 233 vom 16.6.2022, S. 22.
(2) ABl. C 286 vom 16.7.2021, S. 170.
(3) Standpunkt des Europäischen Parlaments vom 10. November 2022 (noch nicht... vom 28. November 2022.
(4) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6... hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in...

Bearbeitungsstand: 3. April 2023, 09:00 Uhr

Referentenentwurf

des Bundesministeriums des Innern und Heimat

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG)

A. Problem und Ziel

Am 13. Januar 2023 trat die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 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 (ABl. L 333 vom 27. Dezember 2022, S. 80, im Folgenden NIS-2-Richtlinie) in Kraft.

Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)[1]

Vom ...

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
0		**Artikel 1 Änderung des BSI-Gesetzes**	
1	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)[2]	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Betreibern und Einrichtungen (BSI-Gesetz – BSIG)	Berücksichtigung des Umstands, dass es sich nicht mehr um ein reines Errichtungsgesetz einer Bundesbehörde handelt.
2	Nichtamtliches Inhaltsverzeichnis § 1 Bundesamt für Sicherheit in der Informationstechnik § 2 Begriffsbestimmungen § 3 Aufgaben des Bundesamtes § 3a Verarbeitung personenbezogener Daten § 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes	Inhaltsübersicht Teil 1 Allgemeine Vorschriften § 1 Bundesamt für Sicherheit in der Informationstechnik § 2 Begriffsbestimmungen Teil 2 Das Bundesamt	Schaffung einer (amtlichen) Inhaltsübersicht aufgrund des gestiegenen Umfangs des Gesetzes sowie Strukturierung des Gesetzes in Teile (und Kapitel) zur besseren Übersicht für den Rechtsanwender.

[1] Dieses Gesetz dient der Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 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 (ABl. L 333 vom 27.12.2022, S. 80).
[2] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist.

5 | 243

Quelle: Referentenentwurf des NIS2UmsuCG ist eine inoffizielle Veröffentlichung.

Diese zentralen Neuerungen bringen NIS-2 und das NIS2UmsuCG für Unternehmen und die Bundesverwaltung in Deutschland mit sich

Ausweitung des Anwendungsbereichs

- Schwellenwerte werden um Size Cap Rule erweitert
- Neue Sektoren
- Einbeziehung der Bundesverwaltung

Konkretisierung und Ausweitung der Pflichten

- Pflicht organisatorische wirksame Maßnahmen zu ergreifen, um Risiken für die Sicherheit zu beherrschen
- Erstmals Konkretisierung dieser Maßnahmen in Art. 21 (2) der Richtlinie bzw. in § 30 (4) des Referentenentwurfs
- Melde-, Registrierungs-, Nachweis und Unterrichtungspflichten

Governance und Organhaftung

- Neue Obergrenze für Bußgelder: bis zu 2 % des globalen Jahresumsatzes
- Persönliches Überwachungs- und Umsetzungspflicht bei den Leitungsorganen
- Zwingende Organhaftung auch in Bezug auf die Bußgelder

Quelle: Referentenentwurf des NIS2UmsuCG ist eine inoffizielle Veröffentlichung.

Diese Einrichtungen sind zukünftig laut Referentenentwurf (Stand Juli 2023) von NIS2UmsuCG betroffen

Besonders wichtige Einrichtung *(in NIS2 "wesentliche")*

Großunternehmen:

- Unternehmen oder rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft
- **Mindestens 250 Mitarbeitende ODER mindestens 50 Mio. EUR** Jahresumsatz mit einer Jahresbilanzsumme von **mindestens 43 Mio. EUR**
- **Sektoren** Energie, Verkehr und Transport, Finanz- und Versicherungswesen, Gesundheitswesen, Trinkwasser, Abwasser, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten (B2B) oder Weltraum

Mittlere Unternehmen:

- Unternehmen oderrechtlich unselbstständige Organisationseinheit einer Körperschaft
- **50 bis 249 Mitarbeitende** und einem Jahresumsatz von weniger als **50 Mio. EUR oder** einer Jahresbilanzsumme **von weniger als 43 Mio. EUR** ODER
- **weniger als 50 Mitarbeitende und einen** Jahresumsatz zwischen 10-50 MIO EUR und Jahresbilanzsumme zwischen 10 und 43 MIO EUR
- **Sektoren:** Anbieter von TK-Diensten oder öffentlich zugänglichen TK-Netzen

Jedes Unternehmen (Größenunabhängig) der Sektoren:

Qualifizierte Vertrauensdiensteanbieter, Top-Level-Domain-Name Registries oder DNS-Diensteanbieter

Öffentlicher Sektor

Einrichtungen der „Zentralregierungen" bspw. Bundesministerien, Bundeskanzleramt

Kritische Anlagen[1]

Hohe Bedeutung für das Funktionieren des Gemeinwesens (Ausfall oder Beeinträchtigung führen zu erheblichen Versorgungsengpässen oder Gefährdungen der öffentliche Sicherheit)

Sektoren:

- Energie
- Verkehr und Transport
- Finanz- und Versicherungswesen
- Gesundheitswesen
- Trinkwasser und Abwasser
- Ernährung
- Informationstechnik und Telekommunikation
- Weltraum
- Siedlungsabfallentsorgung

Anlagen werden in KRITIS-V definiert

[1] eine natürliche oder juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine Kritische Anlage ausübt

Wichtige Einrichtung

Unternehmen, die *keine Kritischen Anlagen betreiben*

Mittlere Unternehmen der Sektoren:

- Energie
- Transport und Verkehr
- Finanz und Versicherungswesen
- Gesundheitswesen
- Trinkwasser und Abwasser
- Informationstechnik und Telekommunikation
- Verwaltung von IKT-Diensten (B2B)
- Weltraum

Mittlere Unternehmen und Großunternehmen der Sektoren:

- Logistik
- Siedlungsabfallentsorgung
- Produktion
- Chemie
- Ernährung
- verarbeitendes Gewerbe
- Anbieter digitaler Dienste
- Forschung

Größenunabhängig:
Vertrauensdiensteanbieter,
Hersteller von Rüstungswaren und Produktion mit VS NfD IT-Sicherheitsfunktion, Störfallverpflichete

Bundes-verwaltung

Stellen des Bundes, Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen auf Bundesebene, sowie öffentliche Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen. **NICHT** Bundes-wehr und MAD

Quelle: Referentenentwurf des NIS2UmsuCG ist eine inoffizielle Veröffentlichung.

Fallbeispiele: Können Sie bereits zwischen besonders wichtigen Einrichtungen, wichtigen Einrichtungen und Kritischen Anlagen unterscheiden?

Stadtwerke Musterstadt

Die Stadtwerke Musterstadt ist ein großes städtisches Versorgungsunternehmen mit 78 Mitarbeitende und einem Jahresumsatz von 30 Millionen Euro. Ihr Strom beliefert 700.000 Haushalte.

Besonders wichtige Einrichtung

Kritische Anlage

LAB AG

Die Laborgruppe “LAB AG" ist ein großes Unternehmen mit 400 Mitarbeitende und einem Jahresumsatz von 80 Millionen Euro. Die Jahresbilanzsumme liegt bei 68 Millionen Euro.

Besonders wichtige Einrichtung (Großunternehmen)

ForschungPlus

Das Forschungsstart-up "ForschungPlus" ist ein kleineres Unternehmen im Forschungssektor mit 25 Mitarbeitende und einem Jahresumsatz von 3 Millionen Euro.

Voraussetzungen werden NICHT erfüllt

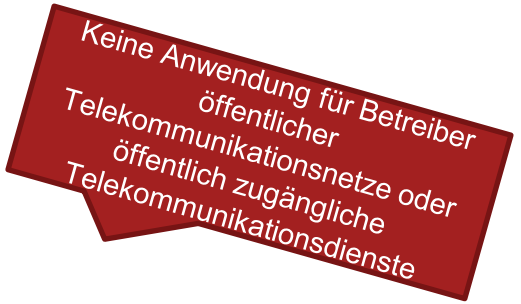
TrustSign

"TrustSign“ ist ein Anbieter qualifizierter Vertrauensdienste, hat 35 Mitarbeitende und einen Jahresumsatz von 5 Millionen Euro.

Besonders wichtige Einrichtung

Quelle: Referentenentwurf des NIS2UmsuCG ist eine inoffizielle Veröffentlichung.

Pflichten für betroffene Einrichtungen und Anlagen, die unter die NIS2 Regelungen fallen im Einzelnen



Risikomanagement

Geeignete, verhältnismäßige und *wirksame* technische und organisatorische Maßnahmen ergreifen, um Störungen der IT-Sicherheitsziele zu vermeiden. Maßnahmen entsprechend dem Stand der Technik

Kritische Anlagen haben erhöhte Anforderungen

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- BCM: Back-up-Management, Wiederherstellung, Krisenmanagement
- Sicherheit der Lieferkette (einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern)
- Sicherheitsmaßnahmen für Erwerb, Entwicklung und Wartung informationstechnische Systeme, Komponenten und Prozesse einschließlich Schwachstellen Management
- Bewertung von Risikomanagementmaßnahmen
- Cyberhygiene und Schulungen
- Kryptografie und Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle, und Management von Anlagen
- Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung,
- gesicherte Sprach-, Video- und Textkommunikation sowie ggf. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung
- Weitergehende EU Anforderungen für 2024 angekündigt: DNS-Diensteanbieter, Top Level Domain Name Registries, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter

Pflichten für betroffene Einrichtungen und Anlagen, die unter die NIS2 Regelungen fallen im Einzelnen

Registrierungs-pflicht

- **Für besonders wichtige und wichtige Einrichtung Top-Level-Domain-Name Registries** drei Monate nach Betroffenheitssbeginn; Betreiber Kritischer Anlagen sofort
- BSI kann die Registrierung eigenständig vornehmen
- Bußgeld bei unterbliebener Registrierung
- Besondere Registrierungspflicht für bestimmte Einrichtungen

Nachweispflichten

- **Für besonders wichtige Einrichtungen:** Nach Registrierung festgelegter Zeitpunkt (spätestens vier Jahre nach Inkrafttretung des Gesetzes) und folgend im zwei-Jahres Turnus
- Nachweis erfolgt in geeigneter Weise: Sicherheitsaudits, Zertifizierungen oder Prüfungen (mit Übermittlung der Sicherheitsmangel)
- Neu: BSI kann die Nachweisverfahren konkretisierend festlegen

Meldepflichten, Rückmeldungen

- **Für kritische, wichtige und besonders wichtige Einrichtungen:** 4-Stufiges Modell über Meldezeitpunkte
- Meldungen bei Sicherheitsvorfällen an BSI und BBK
- Keine Anwendung für Betreiber öffentlicher Telekommunikationsnetze oder öffentlich zugängliche Telekommunikationsdienste

Unterrichtungspflichten

- **Besonders wichtige und wichtige Einrichtungen:** Pflicht bei erheblichem Sicherheitsvorfall : Empfänger der Dienste muss unterrichtet werden.
- Evl. Informierung der Öffentlichkeit
- Einrichtungen aus den Sektoren Finanz- und Versicherungswesen Informationstechnik und Telekomunikation, Verwaltung von IKT-Diensten und Digitale Dienste**, müssen Maßnahmen oder Abhilfemaßnahmen BSI und Diensteempfänger mitteilen**

Quelle: Referentenentwurf des NIS2UmsuCG ist eine inoffizielle Veröffentlichung.

Mehrstufiges Meldeverfahren bei Sicherheitsvorfällen für Kritische Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen

Stufe 1 – frühe Erstmeldung

- Unverzüglich, spätestens innerhalb von 24 Stunden
- Bei Verdacht auf:
  - Erheblichen Sicherheitsvorfall
  - Rechtswidrige oder böswillige Handlungen
  - Grenzüberschreitende Auswirkung

Stufe 2 – bestätigende Erstmeldung

- Unverzüglich, spätestens innerhalb von 72 Stunden
- Bei erheblichem Sicherheitsvorfall Meldung abgeben
- Informationen aus Stufe 1 bestätigen oder aktualisieren
- Erste Bewertung abgeben
- Schweregrad, Auswirkung ggf. Kompromittierungsindikatoren angeben

Stufe 3 - Zwischenmeldung

Auf Ersuchen des BSI muss eine Zwischenmeldung über relevante Statusaktualisierungen getätigt werden

Stufe 3a - Fortschrittsmeldung

- Wenn Sicherheitsvorfall noch nach Stufe 2 andauert, wird eine Fortschrittsmeldung statt einer Abschlussmeldung vorgelegt
- Abschlussmeldung folgt innerhalb eines Monats nach Bearbeitung des Sicherheitsvorfalls

Stufe 4 - Abschlussmeldung

- Spätestens ein Monat nach Meldung gemäß Stufe 2
- Abschlussmeldung enthält folgendes:
  - Ausführliche Beschreibung
  - Schweregrad und Auswirkung
  - Art der Bedrohung bzw. Ursachen
  - Abhilfemaßnahmen ggf. grenzüberschreitende Auswirkungen

Zusätzliche Meldung für Betreiber kritischer Anlagen: Art der betroffenen Anlage, der kritischen Anlage bzw Dienstleistung und die Auswirkungen

Pflichten, die sich für die Unternehmensleitung aus den neuen NIS2 Anforderungen ergeben

Compliance

- Gewährleistung unternehmerischer IT-Sicherheit ist Aufgabe der Geschäftsleitung
- Geschäftsleitung sind diejenigen natürlichen Personen, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer Einrichtung berufen sind bspw. Vorstand einer AG, Geschäftsführer der GmBH, Vorstände, Behördenleitung

Billigungs- und Überwachungspflichten

- Geschäftsleitung besonders wichtiger Einrichtungen und wichtiger Einrichtungen muss ergriffenen Risikomanagementmaßnahmen billigen und ihre Umsetzung überwachen
- Eine Beauftragung Dritter ist NICHT zulässig

Schulungen und Fachkenntnisse

- **Für besonders wichtige und wichtige Einrichtungen:** Regelmäßige Schulungen für Geschäftsleiter und Mitarbeitende
- **Für Betreiber Kritische Anlagen:** Verpflichtung zur Schulung zum Einsatz von Angriffserkennungssystemen
- Registrierung einer geeigneten Kontaktstelle beim BSI (Sicherstellung der fachlichen Geeignetheit)

Betreiber Kritischer Anlagen

- Einsatz von Systemen zur Angriffserkennung
- Identifizierung von Bedrohungen im laufenden Betrieb
- Einsatz geeigneter Beseitigungsmaßnahmen
- Zusätzlicher Teil der Nachweisanforderung(siehe S. 10)
- Ad hoc Prüfungen möglich
- Anzeige gegenüber dem BMI beim erstmaligen Einsatz einer **kritischen Komponente**. BSI kann Einsatz untersagen (Gefahr der Spionage, Terrorismus)

Quelle: Referentenentwurf des NIS2UmsuCG ist eine inoffizielle Veröffentlichung.

Aufsichts- und Durchsetzungsbefugnisse des BSI durch das Wirksamwerden der NIS2-Richtlinien

Besonders wichtige Einrichtungen

- BSI kann ohne Verdachtsmomente die Einhaltung der Anforderungen überprüfen
- BSI kann Anweisungen erteilen u.a. Verstöße öffentlich bekannt zu geben
- Benennung eines Überwachungsbeauftragten durch das BSI iSe Compliance-Monitorships
- Aufhebung von Zertifizierungen bis hin zu Untersagung der Tätigkeit (jur. Person) oder Aufgabenwahrnehmung (natürliche Person)

Wichtige Einrichtungen

- Bei Kenntniserlangung der Nichteinhaltung: Überprüfung der Einhaltung der Anforderungen und verbindliche Anweisung zur Umsetzung
- BSI kann Anweisungen erteilen u.a. Verstöße öffentlich bekannt zu geben

Quelle: Referentenentwurf des NIS2UmsuCG ist eine inoffizielle Veröffentlichung.

Haftungsrisiken der Geschäftsleitung und Sanktionsvorschriften bei Verstößen gegen die Richtlinien

Sanktionsvorschriften

- Stufenkonzept für Bußgeldtatbestände bis zu 20 Millionen EUR
- Fahrlässiges und vorsätzliches Verschulden
- Bußgeldrahmen für wichtige Einrichtungen bis zu 7 Mio. EUR oder ein Höchstbetrag von mindestens 1,4% des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens
- Bei besonders wichtigen Einrichtungen bis zu 10 Mio. EUR oder ein Höchstbetrag von mindestens 2% des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens
- Keine Differenzierung zwischen besonders wichtigen Einrichtungen und Kritischen Anlagen

Haftungsrisiko für Geschäftsleitung

- Beispiel: Cyberangriff mit betriebseinschränkenden Auswirkungen aufgrund mangelhaft überwachten Risikomanagementprozesses in besonders wichtigen Einrichtung
- Folgen:

  Kostenpositionen z.B.

  - Lösegeldzahlungen
  - Kosten für externe Dienstleister
  - Bußgelder infolge von DS-GVO- oder BSIG-Verstößen

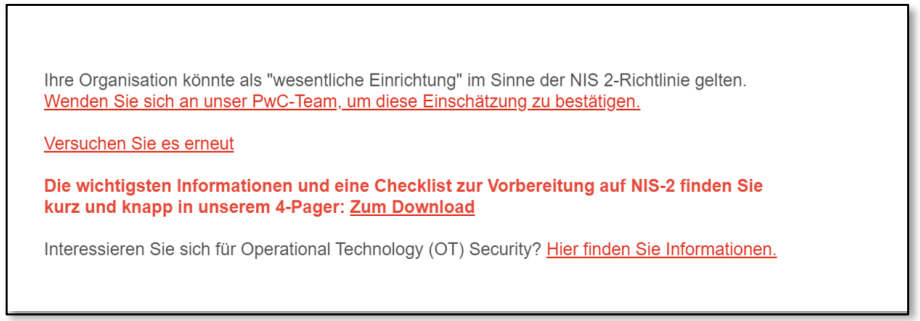
Haftung des Geschäftsleiters

- Bei Verletzung der Überwachungspflichten haftet ein Geschäftsleiter für die entstandenen Schäden (Ausnahme Sektor Zentralregierung)
- Besonderheit: Verzicht der Einrichtung auf Ersatzansprüche gegen die Geschäftsleitung oder ein Vergleich der Einrichtung über diese Ansprüche ist **unwirksam**
- Ausnahme: Bei Zahlungsunfähigkeit der Leitungsperson kann ein Vergleich mit ihren Gläubigern erfolgen oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird

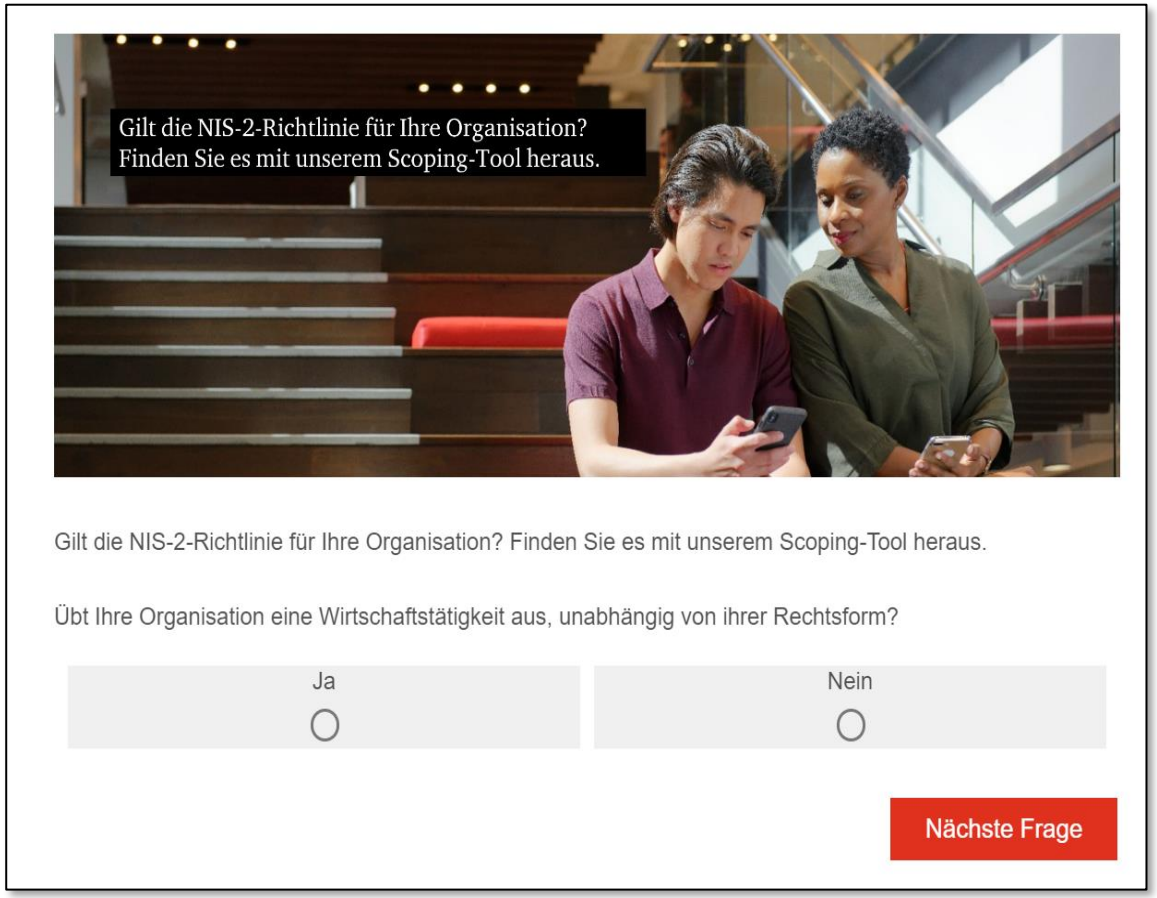
Aufgrund des erweiterten Anwendungsbereichs der NIS2-Richtlinie sind im Vergleich zur NIS1-Richtlinie deutlich mehr Unternehmen betroffen

Das PwC-Tool zur Analyse der Auswirkungen unterstützt Unternehmen bei der Ermittlung ihrer Betroffenheit

- Unternehmen können unser fragebogenbasiertes Tool nutzen, um festzustellen, wie und ob sie von NIS2 betroffen sind.
- In dem Fragebogen werden Fragen zu den folgenden Bereichen gestellt: Unternehmensgröße (Anzahl der Mitarbeitenden), Jahresumsatz, Bilanzsumme, Standort des Unternehmens, Art des Unternehmens und Branchenaktivitäten.
- Ergebnisse: "Wichtiges Unternehmen", "Wesentliches Unternehmen" oder "Nicht betroffen“.
- Das Ergebnis ist nur eine erste Einschätzung. Danach können Sie das PwC-Team direkt per E-Mail kontaktieren.



Jetzt durchführen!



Zusammenfassung und Ausblick

- Das NIS2UmsuCG kommt voraussichtlich Ende 2023 und ist das bislang komplexeste Rahmenwerk des nationalen IT Sicherheitsrechts
- Gesetzlich ergeben sich zahlreiche Änderungen im Anwendungsbereich, der in erheblichem Maße erweitert wird und längst nicht mehr nur KRITIS betrifft
- Insgesamt werden die Vorgaben zur Cybersecurity-Compliance deutlich verschärft und können mit erheblichen Bußgeldern belegt werden

Vielen Dank für Ihre Aufmerksamkeit.

pwc.de