TaylorWessing

DIGITAL LEGAL ACADEMY 2024

Wir denken das Datenrecht der Zukunft – heute.

Cyber Security und Cyber Resilience: Wie sich Europa gegen Hacker wehrt

Manuel Atug, HiSolutions AG, Dr. Paul Voigt und Mareike Christine Gehrmann, Taylor Wessing

14. Mai 2024

Sessions 2024

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

#1	**EU Digital Legal Landscape: Das Big Picture der EU-Digitalstrategie** Prof. Dr. Katharina Kaesling, LL.M. & Thanos Rammos am 16. April 2024
#2	**Data & Data Protection: Startschuss für die Datenrevolution?** Diane Angerhausen, Thomas Kahl & Dajin Lie am 23. April 2024
#3	**Digital Economy & Digital Markets: Fairer Wettbewerb für die Digitalwirtschaft?** Vladimir Yaroshevskiy, Dr. Johanna Götz & Nathalie Koch am 30. April 2024
#4	**Cloud & Digital Infrastructure: Neue Regeln für das Rückgrat der digitalen Wirtschaft** Christoph Endell, Dr. Sabine Kaben & Dr. Carsten Schulz am 7. Mai 2024
#5	**Cyber Security & Cyber Resilience: Wie sich Europa gegen Hacker wehrt** Manuel Atug, Dr. Paul Voigt & Mareike Gehrmann am 14. Mai 2024

Agenda

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

1	**Wie ist IT-Sicherheit reguliert?**
2	Cybersicherheitsarchitektur in Europa
3	**Deep Talk: NIS2-RL**
4	NIS2-RL: Und jetzt? Wie implementiere ich NIS2?
5	**CER/KRITIS-DachG – Umsetzung**
6	Let`s talk…
7	**Exkurs: CRA: Was bedeutet das für die Praxis?**

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

1 Wie ist IT-Sicherheit reguliert?

IT-Bedrohungslage

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Bundesamt für Sicherheit in der Informationstechnik („BSI“):

Bericht „Die Lage der IT-Sicherheit in Deutschland 2023“

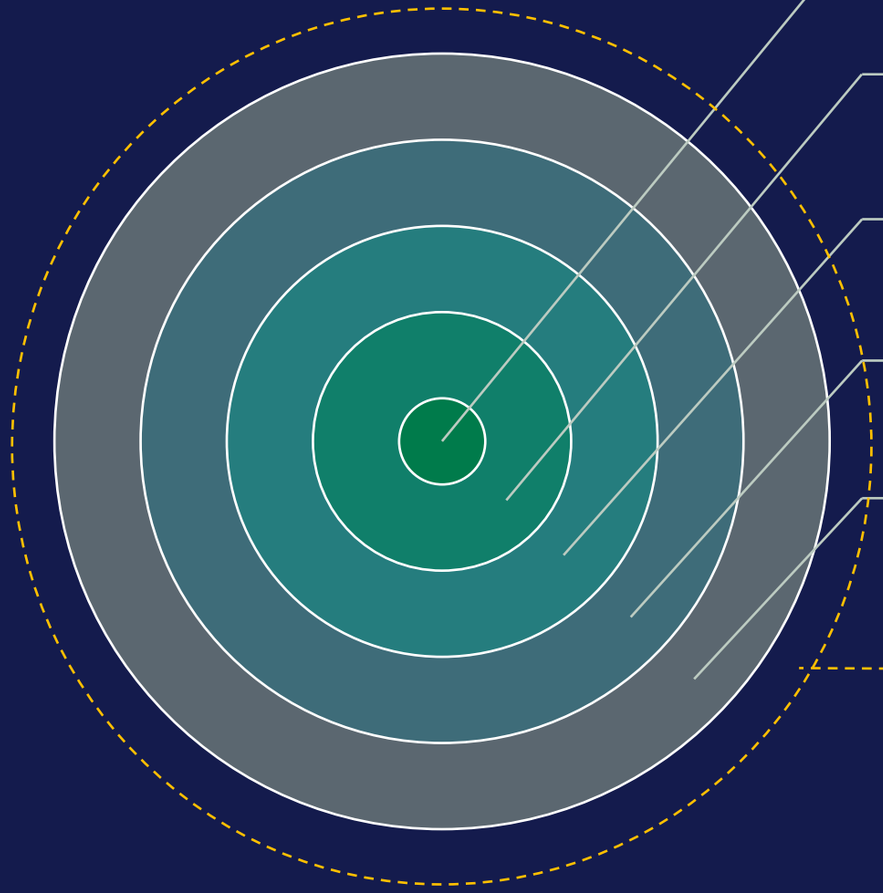
- Wesentliche Ergebnisse:
  - Ransomware bleibt Hauptbedrohung, vor allem für Unternehmen
  - 2023: Schäden iHv 206 Milliarden Euro für die deutsche Wirtschaft
  - BSI hat rund 21.000 infizierte Systeme täglich erkannt
  - Angreifer fangen 750 E-Mails pro Tag ab und sperren 370 Webseiten

Zuletzt: Ransomware Angriff in den USA

- Angriff auf US-Konzern United Health.
  Der unmittelbare Schaden: $872 Millionen

Schlüsselelement der Digital Decade

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing



Standards (z.B. ISO, Grundschutz)

Guidelines der Aufsichtsbehörden (z.B. ENISA)

Produkt-spezifisch (z.B. CRA)

Sektor-spezifisch (NIS-2 / BSIG)

Regulierung (u.a. DORA)

Datenschutz (DS-GVO / BDSG)

Allgemeine zivil- und gesellschaftsrechtliche Vorgaben (Risikomanagement)

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

2 Cybersicherheitsarchitektur in Europa

Meilensteine der Cybersicherheitsstrategie

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

IT-SiG 1.0:
Erster umfassender Rechtsrahmen für Cyber Security

NIS-Umsetzungsgesetz:
Anpassung der deutschen Regelungen an die NIS-RL

IT-SiG 2.0:
Gesetzgebungsprozess über mehrere Jahre, Änderungen u.a. an BSIG

NIS-RL 2.0:
Erhöhung der Anforderungen an die Cyber-sicherheit, löst NIS-RL ab

Juni 2015 | Juli 2016 | Juni 2017 | Juni 2019 | April 2021 | seit 2021 | Januar 2023

NIS-RL:
1. Rechtsrahmen für IT-Sicherheitsstandards auf EU-Ebene

Cybersecurity Act (CSA):
Permanentes Mandat für ENISA; Zertifizierung für IKT-Produkte, -Dienste und Prozesse

seit 2021 stetig angepasst

BSI-KritisV: Wird an das IT-SiG 2.0 angepasst

in Kraft seit Januar 2023
Umsetzungsfrist 17. Oktober 2024

Meilensteine der Cybersicherheitsstrategie

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Digital Operational Resilience Act (DORA): Stärkung der Betriebsstabilität im Finanzsektor

in Kraft seit 16. Januar 2023, gilt ab 17. Januar 2025

Januar 2023

Januar 2023

in Kraft seit 16. Januar 2023, gilt ab 17. Oktober 2024

Critical Entities Resilience (CER-RL): Richtlinie über die Resilienz kritischer Infrastruktur

seit Juli 2023

KRITIS-Dachgesetz: Resilienz und physische Sicherheit Kritischer Infrastrukturen, Umsetzung CER-RL

März 2024

Annahme EP 12. März 2024

Cyber Resilience Act (CRA): Verordnung über die Resilienz von Produkten mit digitalen Elementen

April 2024

Cyber Solidarity Act: Geplanter Rechtsakt zur Erkennung von und Reaktion auf Cyberangriffe

Annahme EP 24. April 2024

Mai 2024

Referentenentwurf 7. Mai 2024

NISUmsuCG: 5. Referentenentwurf, soll zum 1. Oktober 2024 in Kraft treten

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

3 Deep Talk: NIS2-RL

NIS2-RL und was nun?

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Süddeutsche Zeitung

Neue EU-Richtlinie für Cybersicherheit setzt Geschäftsführer unter Druck

Geschäftsführungen haben tagtäglich die unters
Herausforderungen zu stemmen. Mit der neuen NIS2-R
kommt nun noch die Dimension der Rechtssic
Sie wie Unternehmen den neuen Anforderu
hen Geldstrafen schützen können.

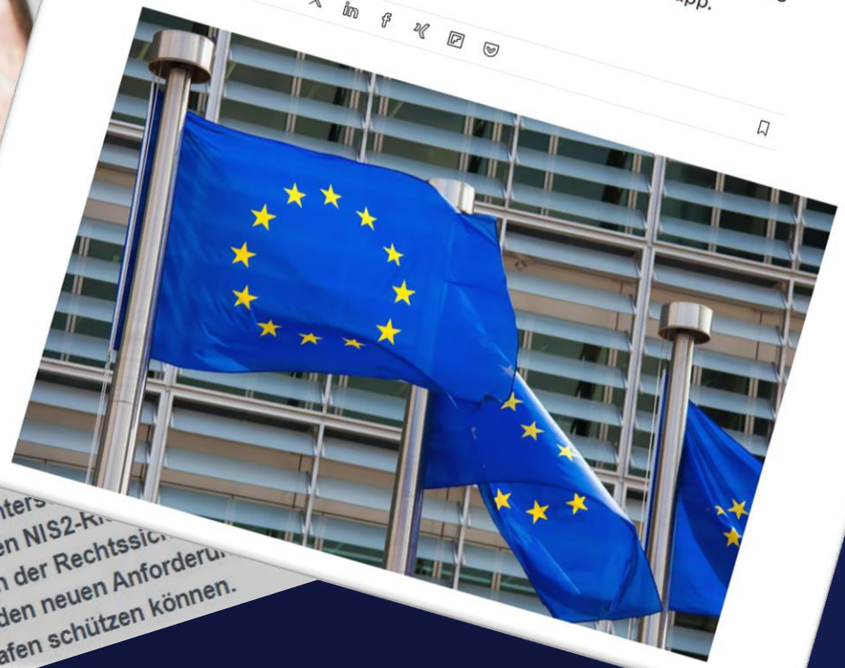
Handelsblatt

IT-Sicherheit

„Kaum zu bewältigen“: Neue EU-Richtlinie für Cybersicherheit setzt Unternehmen unter Zeitdruck

Ob Energieversorger, Onlinemarktplätze, Konzerne oder Mittelständler: Unternehmen müssen auf Geheiß der EU mehr für Cybersicherheit tun. Die Frist ist knapp.

Christof Kerkmann
16.01.2023 - 16:19 Uhr



Quelle:
https://www.handelsblatt.com/technik/it-internet/it-sicherheit-kaum-zu-bewaeltigen-neue-eu-richtlinie-fuer-cybersicherheit-setzt-unternehmen-unter-zeitdruck/28925008.html

Quelle:
https://www.sueddeutsche.de/advertorial/sophos/neue-eu-richtlinie-fuer-cybersicherheit/

NIS2-RL

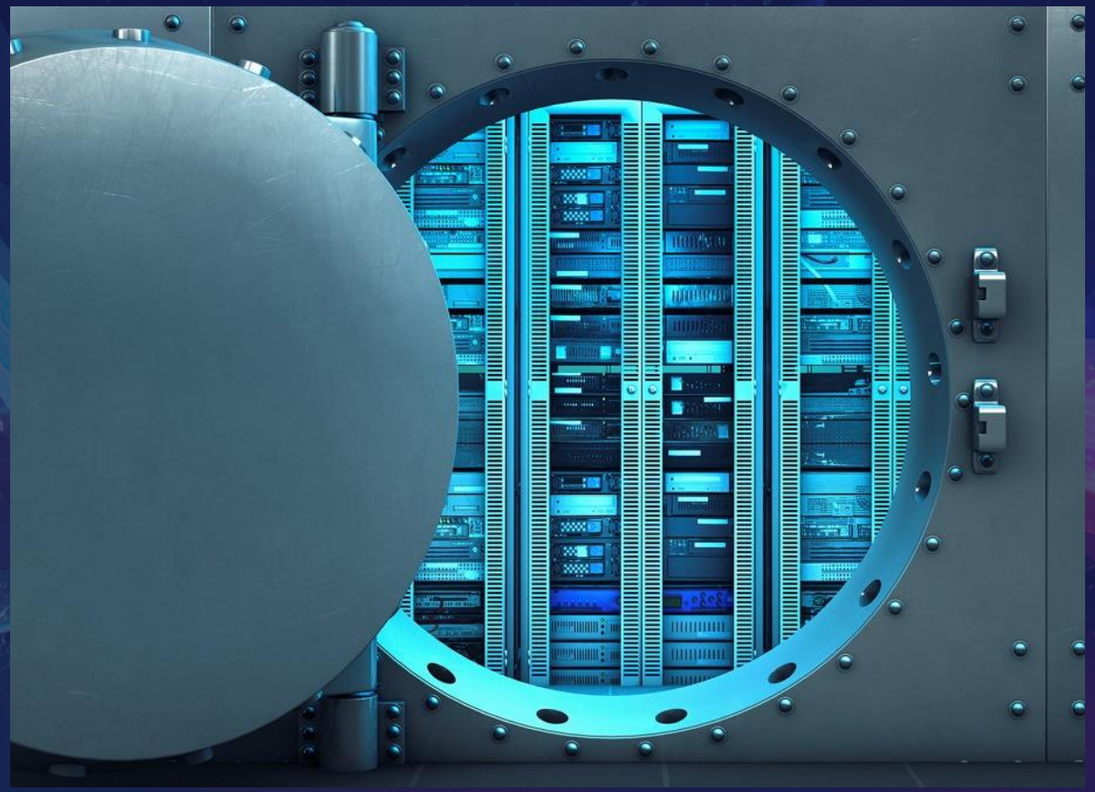
DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (Link)

- In Kraft: 16. Januar 2023
- Umsetzungsfrist: 17. Oktober 2024
- Ziel: Schutz von KRITIS vor Cyberbedrohungen, hohes EU-weites Sicherheitsniveau

Adressaten

- Betreiber wesentlicher Einrichtungen und Betreiber wichtiger Einrichtungen
- Erforderlich ist – unbeschadet einiger Ausnahmen – die Beschäftigung von mindestens 50 Personen oder ein Jahresumsatz bzw. eine Jahresbilanzsumme von mehr als 10 Mio. Euro



NIS2-RL

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Erweiterung der Sektoren

- Wesentliche Einrichtungen
  - Neu: Abwasser, Verwaltung von IKT-Diensten, Öffentliche Verwaltung, Weltraum
  - Ergänzungen: Energie, Gesundheitswesen, Digitale Infrastruktur
- Wichtige Einrichtungen
  - Post- und Kurierdienste, Abfallwirtschaft, Hersteller und Händler chemischer Stoffe und Gemische, digitale Dienste, Forschungseinrichtungen

Droht ein Bußgeld/Sanktionen?

- Wesentliche Einrichtungen: Bis zu 10 Mio. Euro / 2 % des weltweiten Jahresumsatzes der Unternehmensgruppe gegen Art. 21 oder 23 (Cyber Security Maßnahmen und Meldungen)
- Wichtige Einrichtungen: Bis zu 7 Mio. Euro oder 1,4 % des gesamten weltweiten Jahresumsatzes der Unternehmen bei Verstößen gegen Art. 21 oder 23

Pflichten für betroffene Einrichtungen, u. a.:

- Angemessene **TOMs** sind zu ergreifen (risikobasiert nach Größe, Risiken, Ausmaß der Gefährdung etc.)
- **Maßnahmenkatalog** ist umzusetzen, u.a.
  - Konzepte in Bezug auf Risikoanalyse und Sicherheit für Informationssysteme
  - Bewältigung von Sicherheitsvorfällen
  - Lieferkettensicherheit
  - Betriebskontinuität
  - HR Security
  - Verschlüsselungsstrategien
  - Krisenmanagement
- EU Kommission kann Pflichten konkretisieren
- ggf. zukünftig Pflicht zur Nutzung zertifizierter Produkte
- **Meldepflichten** bei Sicherheitsvorfällen (Frühwarnung, Zwischenbericht, Abschlussbericht
- Registrierung

NIS2-RL

Wenn nicht selbst vom Anwendungsspektrum umfasst, ist branchenunabhängige vertragliche Verpflichtung im Rahmen der Lieferkette möglich:

Andere Unternehmen, die unter NIS2-Richtlinie fallen, sind dazu verpflichtet, Risikomanagement Maßnahmen im Bereich der Cybersicherheit in die vertraglichen Vereinbarungen mit ihren direkten Lieferanten einzubeziehen

Überblick NIS2-Umsetzungsgesetz (Entwurf)

DIGITAL LEGAL ACADEMY 2024 by TaylorWessing

Gesetzgebungsverfahren

- „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ (**NIS2UmsuCG**)
- Überschießende Umsetzung der NIS2
- 7. Mai 2024: 5. Referentenentwurf
- In Kraft treten: geplant 1. Oktober 2024
- Neustrukturierung des BSIG

Erhöhter Bußgelderrahmen

- Erweiterung um neue Bußgeldtatbestände
- Bestehende Bußgelder teils deutlich erhöht
- Aktuell: Bußgeldhöhe bis zu 10 Mio. Euro (wenn Umsatz > 500 Mio. Euro, dann 2 % des weltweiten Vorjahresumsatzes

Leitungsorgane, § 38

- Letztverantwortung: Risikomanagement Maßnahmen für Cybersecurity sind zu „billigen“, Umsetzung zu überwachen, regelmäßige Schulungen sind wahrzunehmen
- Binnenhaftung: Ersatzansprüche des Unternehmens gegen das verantwortliche Leitungspersonal bei Verletzung; diese sind durchzusetzen (grds. kein Verzicht, Vergleich in Grenzen möglich, D&O Versicherung möglich)

Bestimmung Adressaten

- Besonders wichtige Einrichtungen, wichtige Einrichtungen und Betreiber kritischer Anlagen
- NIS2UmsuCG regelt zweigleisig: Unternehmensgröße überschritten (Art. 2 Abs. 2 NIS2-RL) oder „Kritische Anlage“, die Schwellenwerte überschreitet (Art. 2 Abs. 3 NIS2-RL)

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

4 NIS2-RL: Und jetzt? Wie implementiere ich NIS2?

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden **Risikomanagement-maßnahmen** im Bereich der **Cybersicherheit** zu **billigen und ihre Umsetzung zu überwachen**

Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risiko-managementpraktiken im Bereich der Sicherheit in der Informationstechnik und die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste zu erwerben

Risikomanagement

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

- **ISMS:** Konzepte in Bezug auf Risikoanalyse, Sicherheit für Informationssysteme, Bewertung der Wirksamkeit von Maßnahmen, Kryptografie, Identitäts- und Berechtigungsmanagement
- **BCM und Krisenmanagement:** Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement, gesicherte Notfallkommunikation
- **Lifecycle Management:** Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informations-technischen Systemen, Komponenten und Prozessen (…)

- **Bewältigung von Sicherheitsvorfällen**
- **Awareness:** grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit, Clean Desk
- **Sicherheit des Personals**
- **Sichere Authentifizierung:** Verwendung von Lösungen zu MFA oder kontinuierlichen Authentifizierung
- **Sichere Kommunikation:** gesicherte Sprach-, Video- und Textkommunikation
- **Dienstleistersteuerung:** Sicherheit der Lieferkette (…)
- **Krypographie und Verschlüsselung**

Zusätzliche Anforderungen an Betreiber kritischer Anlagen (KRITIS)

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

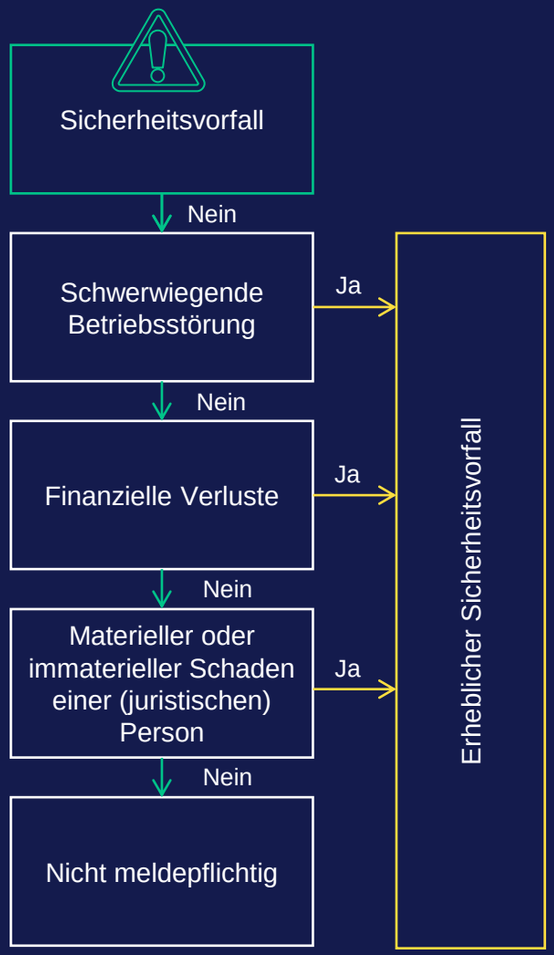
Systeme zur Angriffserkennung (SzA):

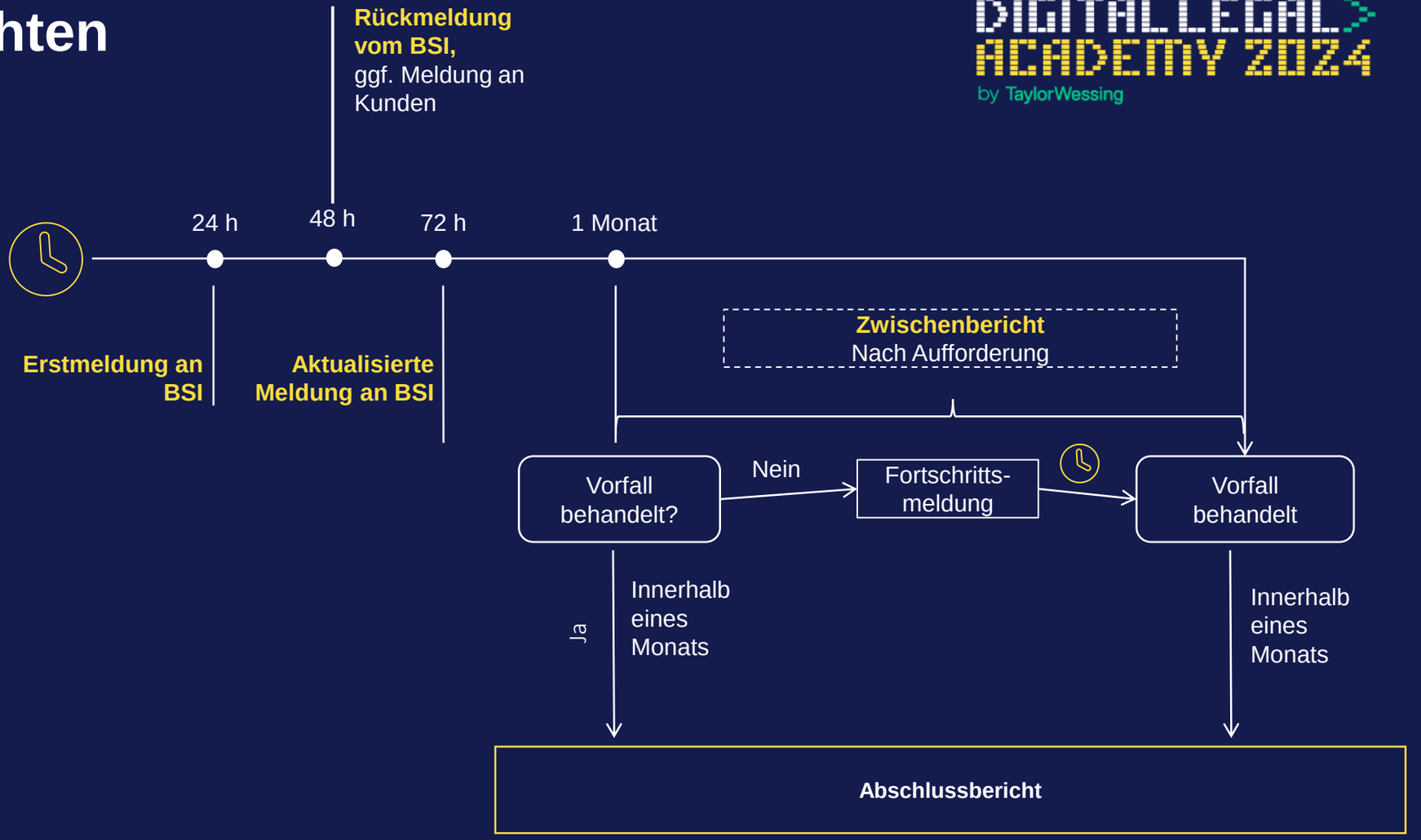
BSI Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung für KRITIS Betreiber nach § 8a BSIG bereits vorhanden, Umsetzung seit 1. Mai 2023 verpflichtend

Nachweispflicht:

Alle 3 Jahre, durch Prüfung nachzuweisen

Die Meldepflichten





Die Unterrichtungspflichten

Einrichtungen aus Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Verwaltung von IKT-Diensten und Digitale Dienste

Erhebliche Cyberbedrohung

BSI

BSI über Bedrohung und alle möglichen Abhilfemaßnahmen informieren

Besonders wichtige Einrichtungen*, wichtige Einrichtungen

Erheblicher Sicherheitsvorfall

Betroffene Kunden per Veröffentlichung informieren

Partizipationspflicht** für besonders wichtige Einrichtungen und Betreiber kritischer Anlagen im **Onlineportal des BSI

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

5 CER / KRITIS-DachG - Umsetzung

KRITIS-DachG – physische Sicherheit

Alle 4 Jahre: Risikoanalysen und -bewertungen!

„Wirtschafsstabilität beeinträchtigenden, naturbedingten, klimatischen und vom Menschen verursachten Risiken berücksichtigen, darunter solche sektorübergreifender oder grenzüberschreitender Art, Unfälle, Naturkatastrophen, gesundheitliche Notlagen, sowie hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten“ sowie „Wirtschafsstabilität beeinträchtigenden, Risiken berücksichtigen, die sich aus dem Ausmaß der Abhängigkeiten anderer Sektoren von der kritischen Dienstleistung, die von der kritischen Anlage – auch in benachbarten Mitgliedstaaten und Drittstaaten – erbracht wird“

Alle 2 Jahre: Resilienzplan nachweisen!

Die Aufgaben

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Prävention

Verhindern von Sicherheitsvorfällen, unter gebührender Berücksichtigung von Katastrophenvorsorge und Maßnahmen zur Anpassung an den Klimawandel

Physischer Schutz

Physischer Schutz von Räumlichkeiten und kritischen Infrastrukturen gewährleisten zum Beispiel durch Aufstellen von Zäunen und Sperren, Instrumenten und Verfahren für die Überwachung der Umgebung, Detektionsgeräten und Zugangskontrollen

Vorfalls- und Krisenmanagement

Kapazitäten zur Reaktion, Abwehr und Folgeeinschränkung bei Vorfällen, unter gebührender Berücksichtigung der Umsetzung von Risiko- und Krisenmanagementverfahren und -protokollen und vorgegebener Abläufe im Alarmfall

Wiederanlauf

Gewährleistung von Wiederherstellung, unter gebührender Berücksichtigung von Maßnahmen zur Aufrechterhaltung des Betriebs und der Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen

Sicherheitsmanagement

Berücksichtigung von Maßnahmen wie Festlegung von Personalkategorien, Zugangsrechten zu Räumlichkeiten, kritischen Infrastrukturen und zu sensiblen Informationen und der Einführung von Verfahren für Zuverlässigkeits-überprüfungen, Festlegung von Schulungsanforderungen und Qualifikationen

Sensibilisierung von Personal

Personal für die unter den Maßnahmen unter gebührender Berücksichtigung von Schulungen, Informationsmaterial und Übungen zu sensibilisieren

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

6 Just talk …

Speaker

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Manuel Atug

Principal, HiSolutions AG

Mareike Christine Gehrmann

Partnerin, Taylor Wessing

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

Partner, Taylor Wessing

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

7 Exkurs: CRA? Was ist geplant?

Cyber Resilience Act

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Gesetzgebungsverfahren:

- 15. September 2022: EU Kommission veröffentlicht Entwurf der Verordnung über grundlegende Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen
- 12. März 2024: Annahme des Entwurfs durch das EU Parlament
- Umsetzungsfrist: 36 Monate nach Inkrafttreten

Ziele:

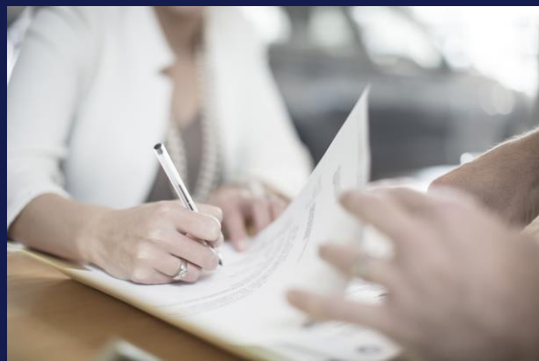
- Sicherheit von Produkten mit digitalen Elementen soll bei der Konzeption, Erstellung und über den gesamten Lebenszyklus sichergestellt werden
- Transparenz der Sicherheits-eigenschaften von Produkten mit digitalen Elementen soll erhöht werden

Adressaten:

- Hersteller, Bevollmächtigte, Importeure, Händler

Rechtsfolge bei Zuwiderhandlungen:

- Bußgelder von bis zu **15 Millionen Euro** oder **2,5 Prozent des weltweiten Jahresumsatzes**



Cyber Resilience Act

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Anknüpfungspunkt:

- **Kritikalität der Produkte mit digitalen Elementen**
  - Nicht kritische Produkte mit digitalen Elementen (z.B. PC-Spiele, smarte Alltagsgeräte)
  - Kritische Produkte mit digitalen Elementen Klasse I (z.B. Browser, Passwort-Manager) und Klasse II (z.B. Router, Chipkarten/-leser, Firewalls für den industriellen Einsatz)
  - Hochkritische Produkte mit digitalen Elementen – darunter fallen noch keine Produkte
  - Konformitätsbewertung durch den Hersteller (Klasse I) oder durch einen unabhängigen Dritten (Klasse II)
- Ausnahmen bspw. für gewisse medizinische Produkte oder Produkte für militärische Zwecke
- Free und Open-Source Software nur bei gewerblicher Nutzung erfasst
- Hard- und Softwareprodukte sowie dessen zugehörige Datenverarbeitungslösungen in der Cloud, Geräte, die (auch) drahtlos kommunizieren; keine SaaS (NIS2-RL)

Pflichten der Hersteller:

- Besondere **Vorgaben** an Design, Entwicklung und Produktion
- Cybersecurity Risk Assessment
- Beifügen von **Produktinformationen** sowie **Gebrauchsanweisungen**
- **Konformitätsprüfungsverfahren**
  - CE-Zertifizierung
  - EU-Konformitätserklärung
- **Due Diligence bei Integration von Drittanbieter-komponenten** (Dokumentationspflichten vor Inverkehrbringen)
- **Meldepflichten,** u.a. an ENISA unverzüglich, spätestens innerhalb von 24h, nach Entdecken von Schwachstellen

Cyber Resilience Act

DIGITAL LEGAL ACADEMY 2024
by TaylorWessing

Pflichten der Händler:

- Händler müssen mit der **gebotenen Sorgfalt** bezüglich der Sicherheitsanforderungen des CRA handeln
- **Sicherstellen**, dass
  - Produkt die CE-Zertifizierung trägt,
  - Hersteller alle relevanten Informationen sowie die Gebrauchsanweisung beigefügt hat,
  - Importeur seinen Namen sowie eine Kontaktadresse am Produkt / an der Verpackung angebracht hat
- **Meldepflicht an die Marktaufsichtsbehörde** sowie – soweit möglich – an die Nutzer des Produkts, wenn dem Händler bekannt wird, dass der Hersteller das Produkt nicht in Einklang mit den Vorschriften des CRA bringen kann

Pflichten der Importeure:

- **Sicherstellen**, dass
  - Hersteller Konformitätsprüfungsverfahren durchlaufen hat
  - Hersteller die relevanten Informationen und Gebrauchsanweisungen beigefügt hat
  - Produkt die CE-Zertifizierung trägt
- Dürfen **nur Produkte auf den Markt bringen**, die den essenziellen Sicherheitsanforderungen des CRA entsprechen
- Anbringen von Name sowie Kontaktadresse an Produkt / Produktverpackung
- Behalten einer **Kopie der EU-Konformitätserklärung für 10 Jahre**, nachdem das Produkt auf den Markt gebracht wurde
- **Meldepflicht an die Marktaufsichtsbehörde** sowie – soweit möglich – an die Nutzer des Produkts, wenn dem Importeur bekannt wird, dass der Hersteller das Produkt nicht in Einklang mit den Vorschriften des CRA bringen kann

TaylorWessing

DIGITAL LEGAL ACADEMY 2024

Wir denken das Datenrecht der Zukunft – heute.

taylorwessing.com