



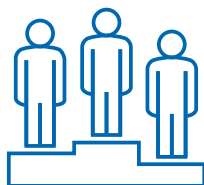
Cybersecurity Regulierung am Beispiel von DORA, NIS 2 und CRA

Regionalgruppe Köln der Gesellschaft für Informatik
Dr. Frank Damm und Niclas Kusenbach

FTI Consulting Cybersecurity

FTI Cybersecurity macht den entscheidenden Unterschied

Jede Cybersecurity-Strategie, jede Vorfallsbearbeitung und jede Untersuchung bringt auch Herausforderungen mit sich, die über die Cybersecurity hinausgehen. Unser Team bietet weltweite Unterstützung in den Bereichen Ermittlungen, forensische Untersuchungen, Datenschutz, Krisenmanagement, strategische Kommunikation und Anti-Geldwäsche.



Interdisziplinäre Erfahrung

Strategischer Ansatz für Herausforderungen der Cybersecurity auf der Basis von Erkenntnissen und Expertenwissen.

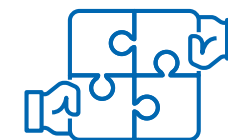
Expertenerfahrung aus Nachrichtendiensten, Strafverfolgungsbehörden und globaler Wirtschaftsunternehmen.



Weltweit

Wir können überall auf der Welt reagieren.

Wir können die größten und komplexesten Aufträge und Untersuchungen bearbeiten.



Integriert und umfassend

Kein anderes Unternehmen in diesem Bereich verfügt über ein Krisenkommunikationsteam.

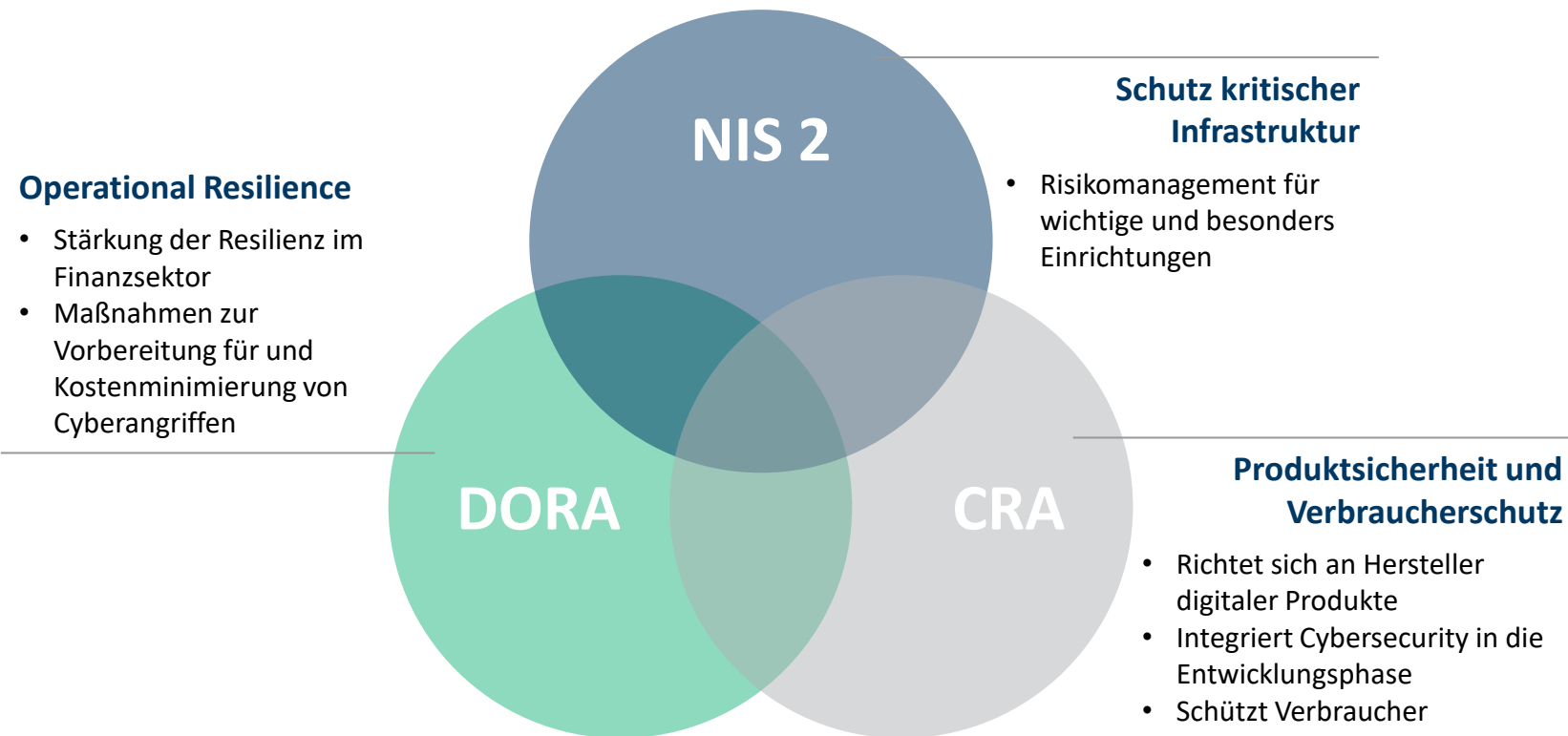
FTI hat verschiedene Expertenteams und diese arbeiten Hand in Hand.

Inhalt

Nr.	Thema	Seite
1	Übersicht DORA, NIS 2, CRA	5
2	DORA	7
3	NIS 2	10
4	CRA	15
5	Zusammenfassung und Ausblick	19

Überblick über Cybersecurity-Regulierung (EU Cyber Act)

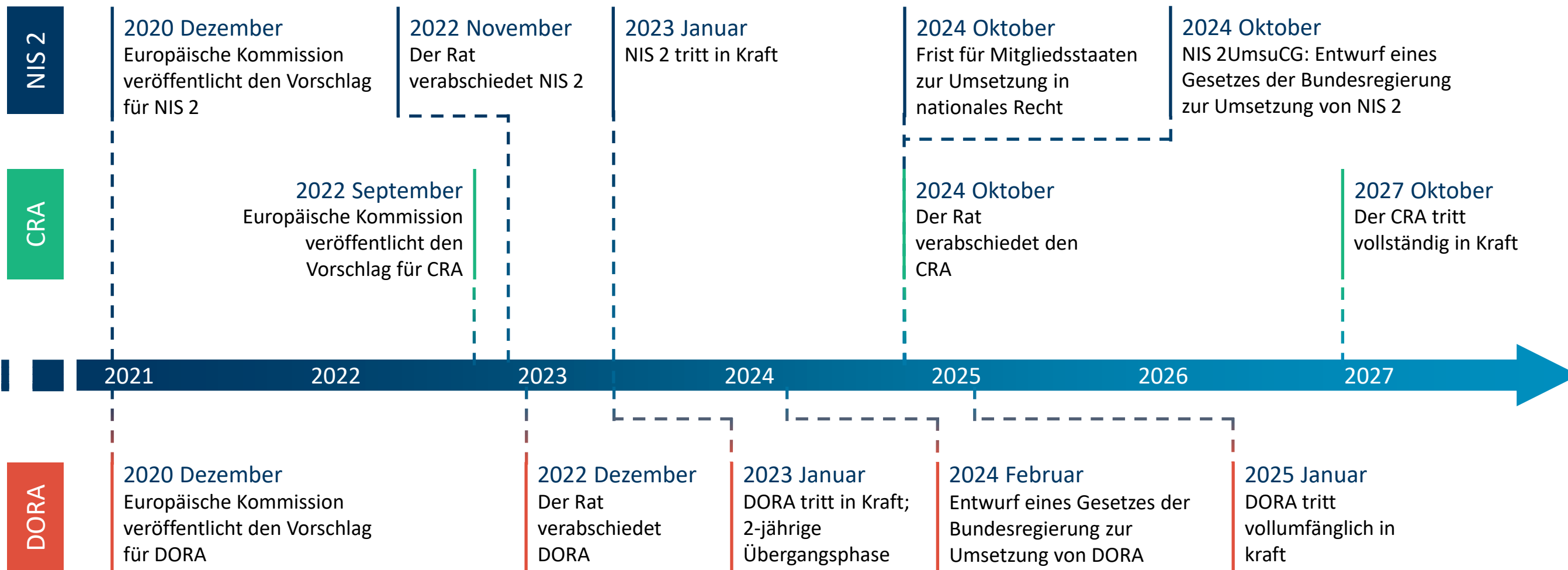
Für robuste Resilienz im Cyberraum



Ziel der Regulierung:

- Europäische Wirtschaft ist resilient bei Cyberbedrohungen
- Einheitliche Standards für Unternehmen
- Höheres Vertrauen in digitale Produkte
- Kostensenkung durch präventive Sicherheitsmaßnahmen

Timeline





DORA

Digital Operational Resilience Act
(EU) 2022/2554¹⁾

Einführung zu DORA

DORA wurde eingeführt, um die Widerstandsfähigkeit des Finanzsektors gegen IT- und Cyberrisiken zu erhöhen, die finanzielle Stabilität zu sichern und die Zusammenarbeit mit Drittanbietern sicherer zu gestalten.

Anforderungen z.B.:

- IKT Risikomanagement und Governance
- Incident response und reporting
- Digital operational resilience testing
- Third-party Risikomanagement

Die Verantwortung für die Umsetzung liegt bei den Vorständen jedes Unternehmens.

Regulatory Technical Standards (RTS): Konkretisieren DORA, z.B. durch Vorgaben für die Meldung schwerwiegender IKT-Vorfälle an die Aufsichtsbehörde

Implementing Technical Standards (ITS): Ergänzen die RTS durch detaillierte Umsetzungsanweisungen und Prozessvorgaben

Von DORA betroffen sind in Europa ca. 22.000 Finanzunternehmen (Banken, Versicherungen, IKT-Dienstleister für Banken).

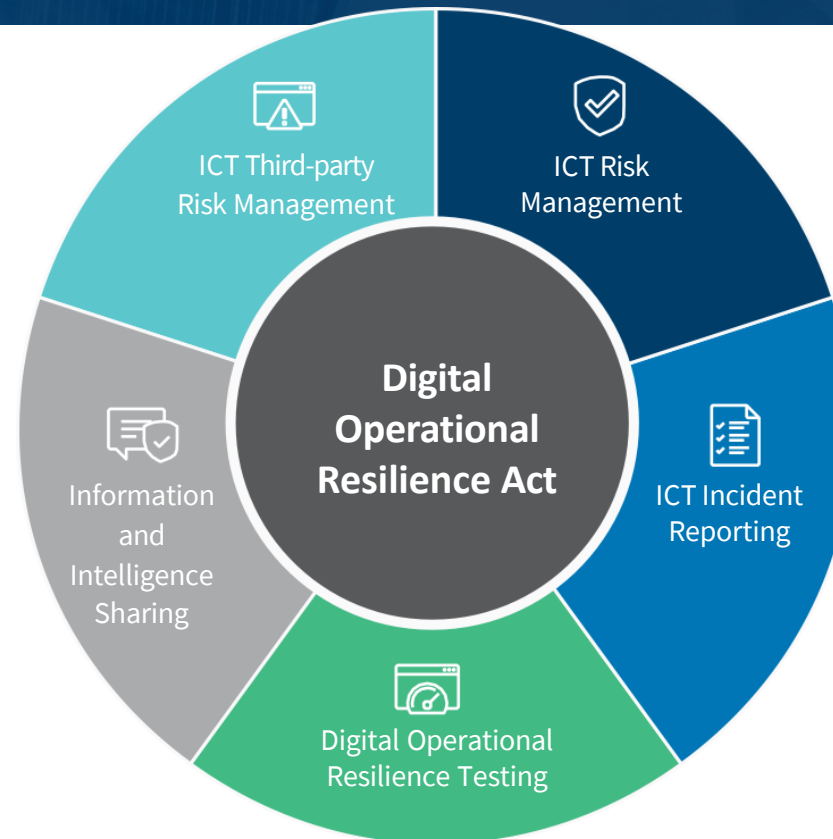
DORA Hauptanforderungen

ICT Third-party Risk Management (TPRM)

- Risikoorientierte Festlegung der Cybersicherheitsanforderungen für den Vertrag mit dem Drittanbieter
- Austausch von Cyber Vorfallsberichten und Beteiligung der Drittanbieter bei der Reaktion
- Kontrolle und Prüfung

Information Sharing

- Entwicklung eines Verfahrens und eines Betriebsmodells für den Informationsaustausch zu Cyber Vorfällen, um diese zu vermeiden und den Schaden zu vermindern



Digital Operational Resilience

- Erstellung eines Plans für operational testing in Übereinstimmung mit TIBER-DE mit Umfang, Ansatz und Methoden (einschließlich Schwachstellenbewertung, Penetrationstests, Red Teaming, Quellcode-Audit, Konfigurationsprüfung), Zeitplan, Zuständigkeiten, Korrekturmaßnahmen
- Umsetzung des Testplans

ICT Risk Management

- Festlegung einer angemessenen Governance
- Entwicklung eines effizienten Rahmens für das Risikomanagement und Unterstützung seiner Umsetzung
- Risikobewertung durchführen
- Bereitstellung von Fachwissen für die Entwicklung cybersicherer IKT-Systeme
- Konzeption, Einführung und Betrieb eines umfassenden Systems zur Erkennung, Analyse und Reaktion auf Cyberangriffe
- Entwurf und Test von Business Continuity Planning (BCP) und Disaster Recovery (DR)

ICT Incident Reporting

- Festlegung, Umsetzung, Prüfung und Aktualisierung eines umfassenden Plans zur Reaktion auf Zwischenfälle
- Vorschlag eines Rahmens und eines Betriebsmodells für die Meldung von IKT-bezogenen Cyber Vorfällen

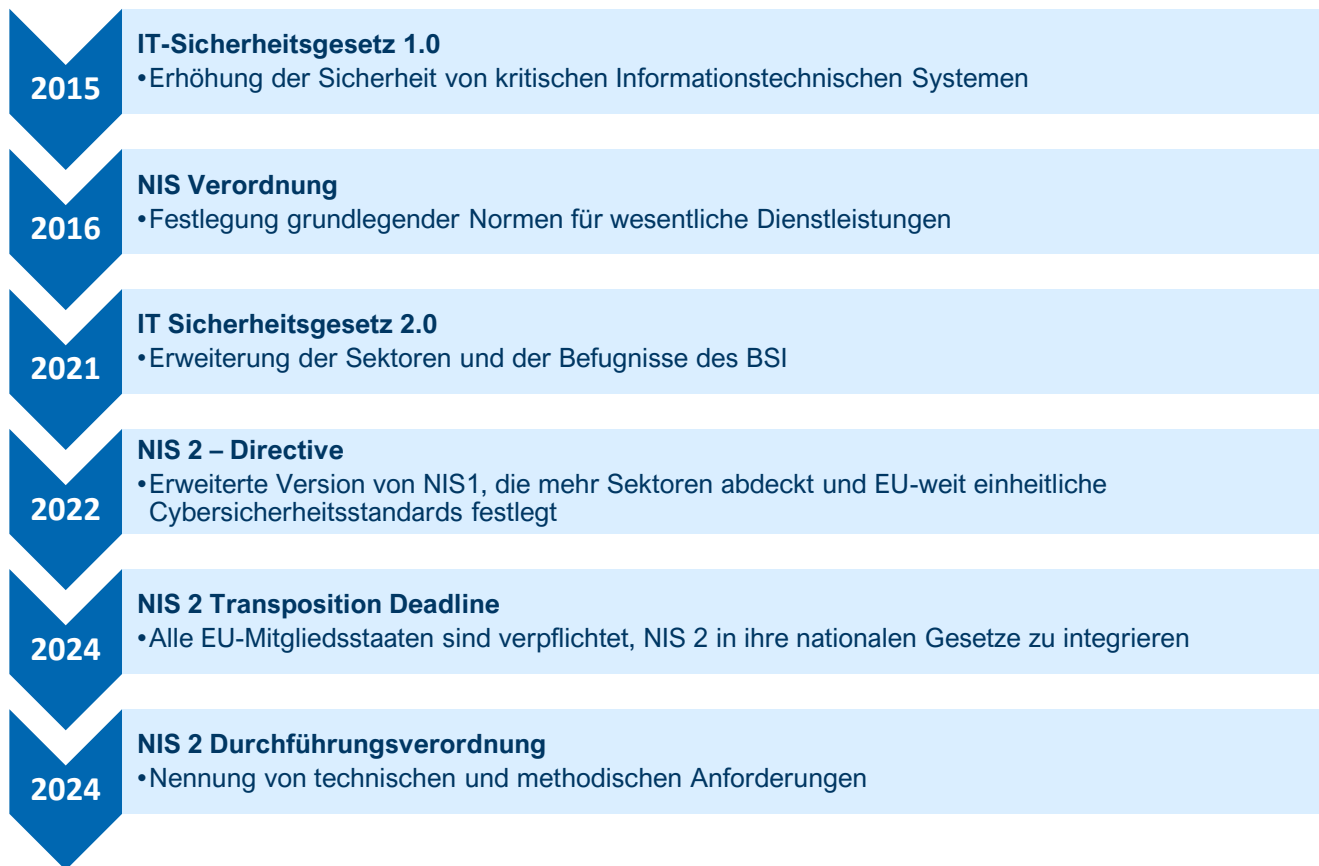


NIS 2

Network and Information Security Directive 2
(EU) 2022/2555¹⁾

Einführung in NIS 2

NIS 2 vereinheitlicht die EU-weite Resilienz kritischer Infrastrukturen gegen Cyber-Bedrohungen, unterstützt die grenzüberschreitende Zusammenarbeit und gewährleistet eine sichere Digitalisierung im Binnenmarkt.



Betroffen sind in DE ca. 30.000 Unternehmen, die eine wichtige oder besonders wichtige Einrichtung nach NIS 2 sein werden.

Die Verantwortung für die Umsetzung liegt bei der Geschäftsleitung **jedes einzelnen Unternehmens.**

Anforderungen:

- Netzwerk- und Informationssicherheit
- Risikomanagement
- Incident Management
- Sicherheit der Lieferkette

NIS 2-Anforderungen auf einen Blick

Wichtige und besonders wichtige Einrichtungen müssen sich auf die folgenden Anforderungen vorbereiten:

Kontinuierliche Verbesserung & Compliance-Überwachung

- Kontinuierliche Überprüfung und Aktualisierung der technischen und organisatorischen Maßnahmen
- Neue Bedrohungen und Schwachstellen angehen
- Audits, Prüfungen und Zertifizierungen durch zuständige Behörden managen

Dokumentation

- Dokumentation von technischen und organisatorischen Maßnahmen und deren Wirkung
- Meldungen zu Sicherheitsvorfällen

Kooperation mit zuständigen Behörden

- Untersuchungen erleichtern und Abhilfemaßnahmen auf Anforderung der Behörden umsetzen
- Angebote von den Behörden zur Unterstützung bei einem Sicherheitsvorfall



Registrierung

- Betreiber registrieren sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI)

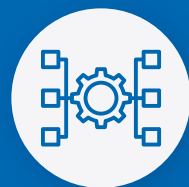
Risikomanagementmaßnahmen

- Angemessene und wirksame technische und organisatorische Maßnahmen umsetzen
- Widerstandsfähigkeit von IT-Netzwerken und Informationssystemen sicherstellen
- Risikobewertungen durchführen und Cybersicherheitsmaßnahmen ergreifen
- Geschäftsleitungen nehmen regelmäßig an Schulungen zur Cybersicherheit teil
- und setzen Risikomanagement-Maßnahmen um und überwachen deren Umsetzung

Meldepflichten

- Erhebliche Sicherheitsvorfälle müssen innerhalb von 24 Stunden an die zuständigen Behörden gemeldet werden (Erstmeldung)
- Meldung nach 72 Stunden
- Abschlussmeldung nach 4 Wochen
- Behörden können die Unterrichtung der Kunden und der Öffentlichkeit verlangen

Technische und organisatorische Maßnahmen nach § 30 NIS 2UmsuCG



Geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen



Stand der Technik einhalten, einschlägige europäische und internationale Normen berücksichtigen, mindestens 10 Detailthemen umsetzen



Vermeidung und Minderung der Auswirkungen von Cybervorfällen

Geschäftsleitung: Risikomanagementmaßnahmen umsetzen und ihre Umsetzung überwachen

Umsetzung und Einhaltung von Maßnahmen angemessen dokumentieren

Detaillierte Anforderungen aus der EU-Richtlinie ¹⁾

Detaillierte Beschreibungen sind im Anhang der Durchführungsverordnung (EU) 2024/2690²⁾

§30.2.1

Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik

§30.2.2

Bewältigung von Sicherheitsvorfällen

§30.2.3

Backup-Management und Wiederherstellung, Krisenmanagement

§30.2.4

Sicherheit der Lieferkette

§30.2.5

Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen

§30.2.6

Bewertung der Wirksamkeit von Risikomanagementmaßnahmen

§30.2.7

Cyberhygiene und Schulungen

§30.2.8

Konzepte und Verfahren für den Einsatz von Kryptografie

§30.2.9

Sicherheit des Personals, Konzepte für Zugriffskontrollen und Management von Anlagen

§30.2.10

Multi-Faktor-Authentifizierung & gesicherte Kommunikation

1) Directive (EU) 2022/2555

2) http://data.europa.eu/eli/reg_impl/2024/2690/oj



CRA

Cyber Resilience Act

(COM(2022) 454 final)¹⁾

Was ist der Cyber Resilience Act (CRA)?

Jährliche Kosten der Cyberkriminalität

5.5 Billionen EUR (2021)

1. Mangel an Cybersicherheit bei Produkten:

Aktuelle Produkte, insbesondere solche ohne embedded systems, weisen oft keine robusten Sicherheitsmaßnahmen auf, was zu weitverbreiteten Schwachstellen führt.

2. Unzureichendes Nutzerbewusstsein:

Nutzer haben ein unzureichendes (Sach-)verständnis, wodurch sie daran gehindert werden, Produkte mit angemessenen Cybersicherheitsmerkmalen auszuwählen.

Der CRA ist ein Vorschlag für eine EU-weite Verordnung zur Cybersicherheit von digitalen Produkten. Er wird eingeführt, um die wachsenden Risiken und Kosten von Cyberangriffen zu bewältigen.

Integration von Cybersicherheit **durch den Hersteller** über den gesamten Produktlebenszyklus

Entwurfsphase → **Bereitstellung**

Produkte mit **digitalen Elementen** sind anfällig für Cyberangriffe, die Benutzer und Organisationen schweren Risiken aussetzen, einschließlich Datenschutzverletzungen, Datenmanipulationen und Beeinträchtigungen der Verfügbarkeit von Diensten

Digitale Elemente

Software oder Hardware Produkt und dessen Lösungen zur Datenübertragung, einschließlich Teilen, die separat verkauft werden sollen



Produkte mit digitalen Elementen sollten mit der CE-Kennzeichnung versehen sein, aus der die Konformität mit CRA hervorgeht.

Hauptanforderungen

Sicherheitsanforderungen

Sicherheit durch Design

Hersteller müssen sicherstellen, dass Produkte **ohne bekannte ausnutzbare Schwachstellen** auf den Markt gebracht werden und sichere Default-Konfigurationen bieten

Risikobasierter Ansatz

Produkte müssen **risikobasiert entwickelt** werden und Schutzmaßnahmen wie Verschlüsselung, Zugriffskontrollen und Schutz vor Datenmanipulation umfassen

Lebenszyklus-Sicherheit

Sicherheitsunterstützung und **Schwachstellenmanagement** müssen während des gesamten Produktlebenszyklus gewährleistet sein, einschließlich **regelmäßiger Updates** und Patches

Transparenz

Hersteller müssen klare Informationen über die Sicherheitsmerkmale ihrer Produkte bereitstellen

Nutzer sollen fundierte Sicherheitsentscheidungen treffen können

Konformitätsbewertung

Klasse I

Kein bis niedriges Risiko...

...für kritische Infrastrukturen, sensible Daten, lebenswichtige Funktionen

IoT-Geräte, Standardsoftware für Endanwender
Keine Konformitätsbewertung durch Dritte notwendig, Selbstbewertung

Klasse II

Moderates bis hohes Risiko...

Betriebssysteme, Netzwerksicherheitssysteme (Firewalls, VPNs), Software in Industrieanlagen
Konformitätsbewertung durch Dritte benötigt

Auswirkungen, Vorteile und Sanktionen

24^h Zeit bis zum Melden einer Schwachstelle

Verbraucher & Partnerunternehmen

- Höheres Vertrauen in digitale Produkte und Systeme sowie besserer Schutz von persönlichen Daten und der Privatsphäre
- Vereinfachtes Risikomanagement für Unternehmen, die zertifizierte sichere Produkte verwenden

Hersteller

- Müssen die Sicherheitsprinzipien während der Entwicklung und des gesamten Lebenszyklus eines Produkts einhalten und Konformitätsbewertungen durchführen lassen
- Müssen vor Markteintritt eine technische Dokumentation anfertigen und Cybersicherheitsrisiken bewerten
- Der CRA erleichtert den Markteintritt in die gesamte EU und reduziert die Fragmentierung durch unterschiedliche nationale Vorschriften

Für Verstöße gegen Cybersicherheitsanforderungen

Bis zu **15** Mio. EUR oder **2.5** % des weltweiten Umsatzes

Für andere Verstöße

Bis zu **10** Mio. EUR oder **2** % des weltweiten Umsatzes

Für Falschangaben an Behörden

Bis zu **5** Mio. EUR



Zusammenfassung und Ausblick

Zusammenfassung und Ausblick

Trotz der

Verlagerung von Daten und menschlicher Interaktion in den Cyberraum

und zunehmender Cyberbedrohungen

funktionieren

unser Geld

unsere Infrastruktur

unsere Alltagsprodukte

Für weitere Informationen kontaktieren Sie bitte:

Hans-Peter Fischer

Senior Managing Director,
Head of Cybersecurity Germany

+49.69.9203 7019

hpf@fticonsulting.com

Dr. Frank Damm

Managing Director,
Cybersecurity Consulting

+49.211.3029 7966

frank.damm@fticonsulting.com

EXPERTS WITH IMPACT™

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

©2023 FTI Consulting, Inc. All rights reserved. www.fticonsulting.com

