Cybersecurity Regulierung am Beispiel von DORA, NIS 2 und CRA

Fachgruppe Sicherheitsmanagement der Gesellschaft für Informatik

Dr. Frank Damm und Niclas Kusenbach

FTI CONSULTING™

8. November 2024

FTI Consulting Cybersecurity

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

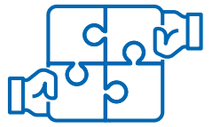
Strategischer Ansatz für Herausforderungen der Cybersecurity auf der Basis von Erkenntnissen und Expertenwissen.

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

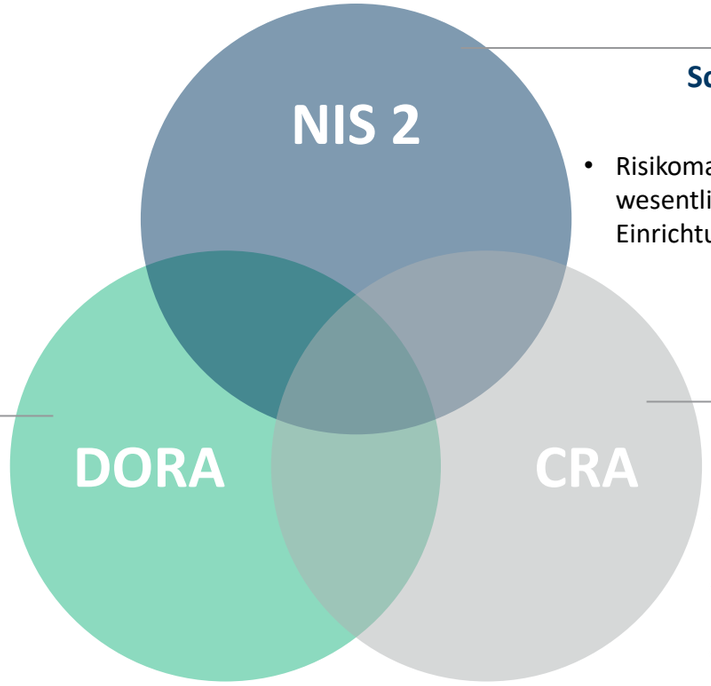
Nr.	Thema	Seite
1	Übersicht DORA, NIS 2, CRA	3
2	DORA	5
3	NIS 2	9
4	CRA	17
5	Zusammenfassung und Ausblick	21

Überblick über Cybersecurity-Regulierung (EU Cyber Act)

Für robuste Resilienz im Cyberraum

Operational Resilience

- Stärkung der Resilienz im Finanzsektor
- Maßnahmen zur Vorbereitung für und Kostenminimierung von Cyberangriffen



Schutz kritischer Infrastruktur

- Risikomanagement für wesentliche und wichtige Einrichtungen

Produktsicherheit und Verbraucherschutz

- Richtet sich an Hersteller digitaler Produkte
- Integriert Cybersecurity in die Entwicklungsphase
- Schützt Verbraucher

Ziel der Regulierung:

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

Timeline


NIS 2
2020 Dezember
Europäische Kommission veröffentlicht den Vorschlag für NIS 2
2022 November
Der Rat verabschiedet NIS 2
2023 Januar
NIS 2 tritt in Kraft
2024 Oktober
Frist für Mitgliedsstaaten zur Umsetzung in nationales Recht
2024 Oktober
NIS 2UmsuCG: Entwurf eines Gesetzes der Bundesregierung zur Umsetzung von NIS 2
CRA
2022 September
Europäische Kommission veröffentlicht den Vorschlag für CRA
2024 Oktober
Der Rat verabschiedet den CRA
2027 Oktober
Der CRA tritt vollständig in Kraft
2021
2022
2023
2024
2025
2026
2027
DORA
2020 Dezember
Europäische Kommission veröffentlicht den Vorschlag für DORA
2022 Dezember
Der Rat verabschiedet DORA
2023 Januar
DORA tritt in Kraft; 2-jährige Übergangsphase
2024 Februar
Entwurf eines Gesetzes der Bundesregierung zur Umsetzung von DORA
2025 Januar
DORA tritt vollumfänglich in kraft

DORA

Digital Operational Resilience Act (EU) 2022/2554[1)]

FTI CONSULTING

1) https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2554

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

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

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

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

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 BCP und 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

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

Unser Gesamtansatz zur Einhaltung von DORA/NIS 2/CRA

Stufe 1 Diagnose

Die Diagnose erfasst den Reifegrad Ihrer Organisation in Bezug auf die Einhaltung der Vorschriften und vorhandene Lücken. Es werden Maßnahmen erarbeitet und eine Roadmap mit Prioritäten zur Umsetzung der Maßnahmen.

Zentrale Aktivitäten

- Festlegung von Schwerpunktbereichen, Sammlung von Informationen und Durchführung einer Gap Analyse
- Überprüfung der digitalen und operativen Resilienz und Erstellung eines Maßnahmenplans

Stufe 2 Design

Beim Design unterstützen wir Sie bei der Konzeption, Entwicklung und Vorbereitung des neuen Zielbetriebsmodells.

Zentrale Aktivitäten

- Entwicklung einer Ausfallsicherheitsstrategie, eines Risikomanagements und eines Rahmens für die Reaktion auf Vorfälle
- Konzeption von Tests und Erstellung von IKT-Anbieterverzeichnissen und Vertragsklauseln

Stufe 3 Implementierung

Hier werden die Governance, Prozesse, Strategien und Verfahren eingeführt und die erforderlichen Kontrollen eingeführt.

Zentrale Aktivitäten

- Durchführung einer Cyber-Risikobewertung und Implementierung neuer Kontrollen und Prozesse
- Implementierung von Systemänderungen, Schulungen und Testprogrammen

Stufe 4 Einführung in den Betrieb

Während der Einführung werden die in den vorangegangenen Stufen durchgeführten Änderungen durch Maßnahmen wie Schulungen und Kontrollvalidierung in der Organisation verankert.

Zentrale Aktivitäten

- Überprüfung der Wirksamkeit der Kontrollen und Durchführung von Workshops zur Schulung des Personals
- Durchführung von Tabletop-Übungen und Übergabe der endgültigen Ergebnisse

NIS 2

Network and Information Security Directive 2
(EU) 2022/2555[1)]

FTI CONSULTING

1) https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:3A32022L2555

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.

2015
IT-Sicherheitsgesetz 1.0
- Erhöhung der Sicherheit von kritischen Informationstechnischen Systemen

2016
NIS Verordnung
- Festlegung grundlegender Normen für wesentliche Dienstleistungen

2021
IT Sicherheitsgesetz 2.0
- Erweiterung der Sektoren und der Befugnisse des BSI

2022
NIS 2 – Directive
- Erweiterte Version von NIS1, die mehr Sektoren abdeckt und EU-weit einheitliche Cybersicherheitsstandards festlegt

2024
NIS 2 Transposition Deadline
- Alle EU-Mitgliedsstaaten sind verpflichtet, NIS 2 in ihre nationalen Gesetze zu integrieren

2024
NIS 2 Durchführungsverordnung
- Nennung von technischen und methodischen Anforderungen

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

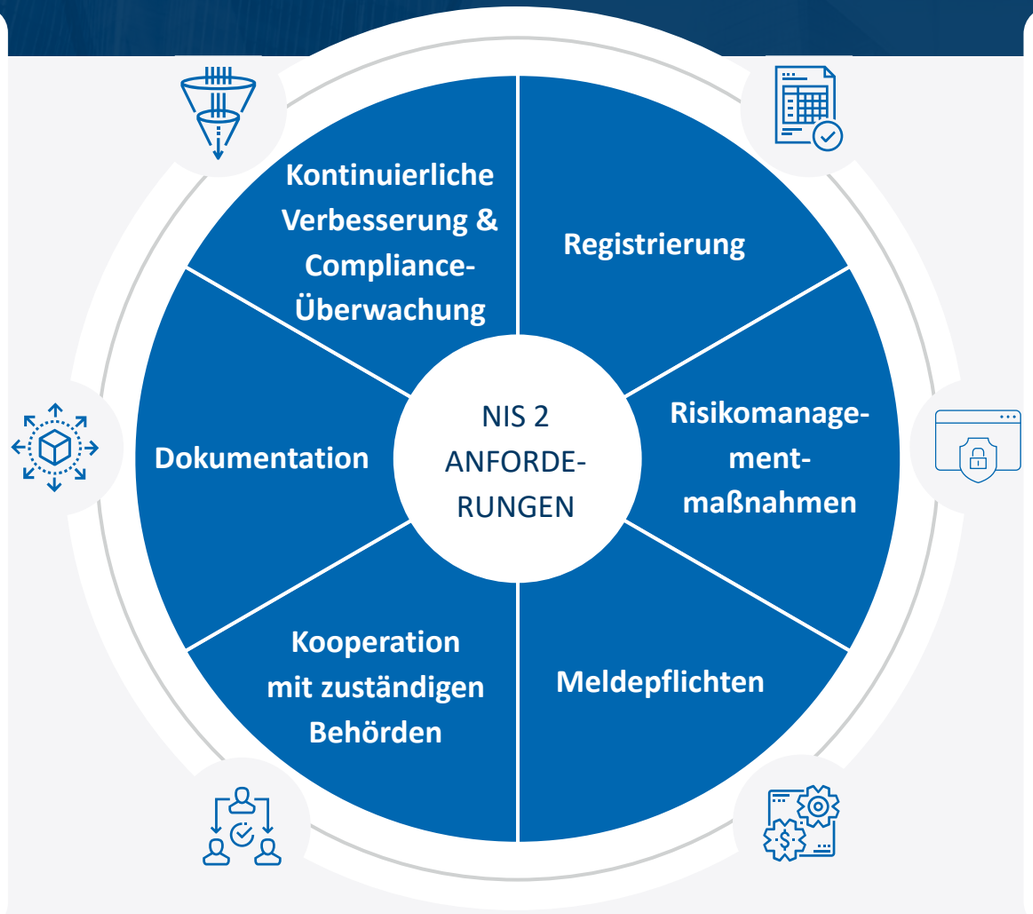
- Kontinuierliche Überprüfung und Aktualisierung der technischen und organisatorischen Maßnahmen
- Neue Bedrohungen und Schwachstellen angehen
- Audits, Prüfungen und Zertifizierungen durch zuständige Behörden managen

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) 2024/2690[2)]

§30.2.1

Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informations-technik

§30.2.2

Bewältigung von Sicherheitsvorfällen

§30.2.3

Backup-Management und Wiederherstellung, Krisenmanagement

§30.2.4

Sicherheit der Lieferkette

§30.2.5

Sicherheitsmaßnah-men bei Erwerb, Entwicklung und Wartung von informationstechni-schen Systemen

§30.2.6

Bewertung der Wirksamkeit von Risikomanagement-maßnahmen

§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

Effektive Umsetzung durch systematisches Vorgehen und durch Außensicht

ISO27000

NIST CSF

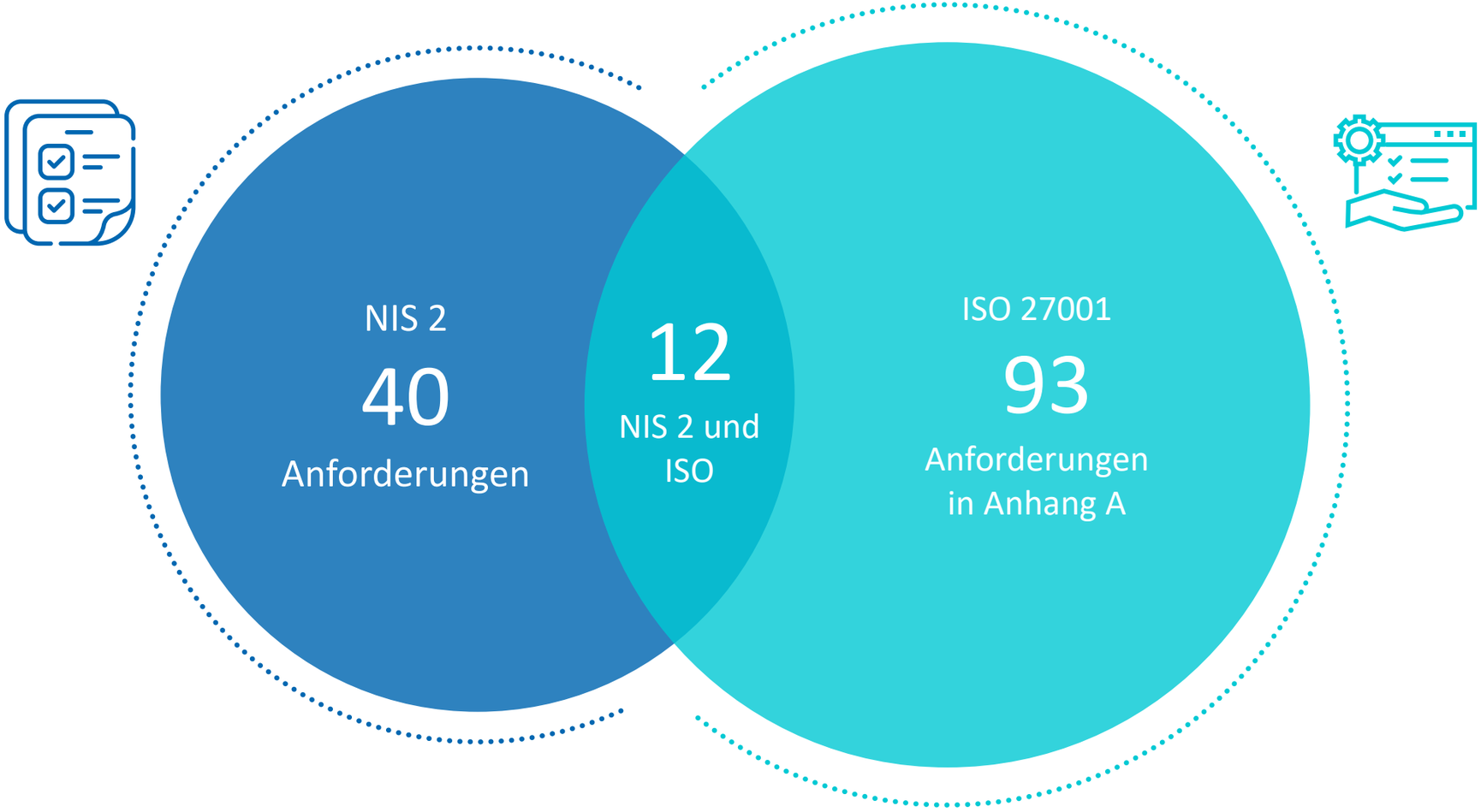
Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

BSI-Grundschutz

- Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung
- Prüfung des IT-Grundschutzes
- Risikoanalyse

Vergleich der Anforderungen von NIS 2 mit den Anforderungen von ISO27001 Anhang A

Fokussiert auf wichtige und besonders wichtige Einrichtungen



Womit Sie bei NIS 2 anfangen können

1

Prüfen Sie mit Ihrer Rechtsabteilung, ob NIS 2 für Sie gilt

- Prüfen Sie Ihren Sektor anhand von Anhang 1 und 2
- Relevante Mitarbeiterzahlen und Umsätze
- Wesentliches oder wichtiges Unternehmen?
- Überprüfen Sie dies mit der Rechtsabteilung
- Bereiten Sie die Anmeldung bei der nationalen Behörde vor.

2

Melden schwerer Zwischenfälle

- Erstmeldung innerhalb der ersten 24h
- Zwischenbericht innerhalb von 72h
- 30 Tage für die Vorlage eines Abschlussberichts bei der Aufsichtsbeörde

3

Identifizierung relevanter neuer Prozesse und Systeme

- z.B.
- Verantwortlichkeiten der Geschäftsleitung
- Multifaktor Authentifizierung
- Schwachstellen-Überprüfung
- Netzwerksegmentierung

4

Identifizierung relevanter bestehender Prozesse und Systeme mit Änderungsbedarf

- z.B.
- Incident Management
- Backup und Wiederherstellung
- Verwaltung und Meldung von Schwachstellen
- Patchmanagement

5

Schulung der Geschäftsleitung

- Risikoerkennung
- Risikobewertung
- Risikomanagement
- Krisenmanagement
- Cybersecurity-Kultur

CRA

Cyber Resilience Act
(COM(2022) 454 final)[1)]

FTI CONSULTING

1) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

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

CE

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

24h 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

1) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

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.