ComplianceCollege

NIS-2 / DORA
Was steckt konkret dahinter?

DZ CompliancePartner

Network & Information Security 2 – Richtlinien

„Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, um das Niveau der Cyberresilienz in der Union zu stärken"

Meldung bsi

– 3. Bundeskabinett bringt Umsetzung der NIS-2-Richtlinie auf den Weg

Um die Resilienz der Cybernation Deutschland zu stärken, kommt es auf das verantwortungsvolle Handeln vieler verschiedener Akteure an. Mit dem in der vergangenen Woche vom Bundeskabinett verabschiedeten Gesetz zur Stärkung der Cybersicherheit werden auch bestimmte Unternehmen stärker in die Pflicht genommen. Dazu gehören etwa die Betreiber kritischer Infrastrukturen sowie IT-Zulieferer, Maschinenbauunternehmen oder Gesundheitseinrichtungen. Rund 30.000 Betriebe in Deutschland werden künftig etwa zur Schulung ihrer Mitarbeitenden sowie zur Meldung von Cyberangriffen verpflichtet sein.

Es berichtete (u. a.) Tagesschau.de: https://www.tagesschau.de/wirtschaft/technologie/cybersicherheit-richtlinie-100.html

#nis2know: Wie das BSI Unternehmen bei der Umsetzung des neuen Gesetzes unterstützt: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html

DORA – Digital Operational Resillience Act

„Verordnung der EU über die digitale operationale Resilienz im Finanzsektor zur Stärkung der digitalen operationalen Resilienz"

NIS-2 vs. DORA

- Beide Vorschriften behandeln Cybersicherheit
  - Risikomanagement von IKT
  - Anforderungen an Finanzdienstleister
  - Richtlinien beziehen Lieferketten mit ein
  - Definition von Strafen bei Nichteinhaltung

- Welche Norm wenn beide anzuwenden sind?
  - DORA vorrangig wegen weitere Ausführungen
  - Was DORA nicht regelt NIS-2

  DORA hat die genauere Ausgestaltung und dient zudem als Vorbereitung zu NIS-2

NIS-2 vs. DORA

NIS-2

- Fokus auf Cybersicherheit mit Austausch von Informationen
- Anforderungen an Informationssicherheit vor allem an das Risikomanagement
- Anforderungen an Reporting
- Umsetzung bis 18.10.2024

DORA

- Fokus auf Betriebsstabilität
- Trotz Angriffen soll Funktionsfähigkeit gewährleistet sein
- Konkrete Anforderungen an Penetrations-Test und Sicherheitsaudits
- Umsetzung bis 17.01.2025

Wen betrifft diese Regelung?

Wesentliche Einrichtungen

Energie
(Elektrizität, Fernwärme, Erdöl, Erdgas, Wasserstoff)

Verkehr
(Luft-/Schiene-/Straße-/Schiff-)

Bankwesen
(Banken und Kreditinstitute)

Finanzmärkte
(Handelsplätze)

Gesundheit
(Dienstleister, Hersteller, Labore, R&D)

Trinkwasser
(Lieferanten u. Versorger)

Abwasser
(Entsorgung Industriell, Kommunal, Häuslich)

Digitale Infrastruktur
(Betreiber von Internetknoten, Cloud Computing, Rechenzentren, Kommunikationsnetzen)

IKT Dienste
(Anbieter verwalteter Dienste und Sicherheitsdienste)

Öffentliche Verwaltung
(Zentrale und Regionale Einrichtungen)

Weltraum
(Bodeninfrastruktur und Erbringung weltraumgestützter Dienste)

Wen betrifft diese Regelung?

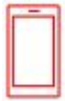
Wichtige Einrichtungen

Post und Kurier
(Anbieter dieser Dienste)

Abfallwirtschaft
(Unternehmen der Abfallbewirtschaftung)

Chemie
(Produktion, Herstellung und Handel)

Lebensmittel
(Produktion, Verarbeitung und Vertrieb)



Digitale Dienste
(Anbietern von Online Marktplätzen, Suchmaschinen, Sozialen Netzwerken)

Forschung
(Forschungseinrichtungen)

Verarbeitendes Gewerbe/Herstellung von Waren
(Medizinprodukte, DV (Computer), Elektronik, Optik, Elektrische Ausrüstung, Herstellung von Kraftwagen und Teilen, Maschinenbau, Sonstiger Fahrzeugbau)

Für wen gilt NIS2?

Mittelgroße Unternehmen / Gesellschaften

50 –249 Mitarbeiter

10 –50 Mio. € Umsatz

<43 Mio. € Bilanzsumme

Große Unternehmen / Gesellschaften

ab 250 Mitarbeitern

ab 50 Mio. € Umsatz

>43 Mio. € Bilanzsumme

Strafen und Geldbußen

Was droht bei Nichteinhaltung?

1. **Aussetzung** von **Zertifizierungen oder Genehmigungen**
2. **Geschäftsführungs-**bzw. Vorstandsebene **untersagen**, **Leitungsaufgaben wahrzunehmen**
3. **Bußgelder**
    1. Wesentliche Einrichtungen: **min. 10 Mio EUR oder 2%** des gesamten weltweiten **Umsatzes**, je nachdem welcher Betrag höher ist
    2. Wichtige Einrichtungen: **min. 7 Mio EUR oder 1,4%** des gesamten weltweiten **Umsatzes**, je nachdem welcher Betrag höher ist

Wen betrifft NIS-2 bzw. DORA

Im Rahmen der Steuerung von Drittdienstleistern sollten alle Unternehmen (auch die die es nicht direkt betrifft), die dauerhaft Leistungen (keine reine Beratung), Hard- und Software für Unternehmen erbringen diese gesetzlichen Anforderungen umsetzen.

- **Beispiel Auszug DORA:**

– Finanzunternehmen dürfen vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die angemessene Standards der Informationssicherheit einhalten. Bei Kritischen oder wichtigen Funktionen ist zu prüfen ob der Dienstleister die aktuellsten und höchsten Qualitätsstandards an die Informationssicherheit anwendet.

Bausteine zur Umsetzung

Planen und Steuern

- Risiko- und Sicherheitsstrategie
- IT-Sicherheitskonzept
- Rollen- und Verantwortlichkeiten
- Dokumentenmanagement

Bausteine zur Umsetzung

Identifizieren

- Asset- und Risikomanagement
- Penetration Test
- Schwachstellen Scan
- Phishing Simulation

Bausteine zur Umsetzung

Schützen

- Awareness Trainings
- Antivir
- Datenspeicherung
- Remote Access
- Firewall
- Kommunikation / Datenaustausch
- Netzwerksicherheit
- Endgerätemanagement
- Zugriffsmanagement

Bausteine zur Umsetzung

Erkennen

- SOC (Sercurity Operation Center)
- IDS (Intrusion Detection System)
- EDR, NDR, XDR (Endpiont Detection Protection, Network Detection Protection, eXtendend Detection & Response)
- SIEM (Security Information Event Management)
- Interne Audits

Bausteine zur Umsetzung

Reagieren

- IT-Notfallplan
- BCM-Strategie
- IT-Forensik
- Incident Response
- Notfallkommunikation
- Mitigation / Remidation

Bausteine zur Umsetzung

Wiederherstellen

- Backup
- Disaster Recovery
- Public Relation
- Lessons Learned

Backups

Public Relations

Disaster Recovery

Lessons Learned

IT-Notfallplan

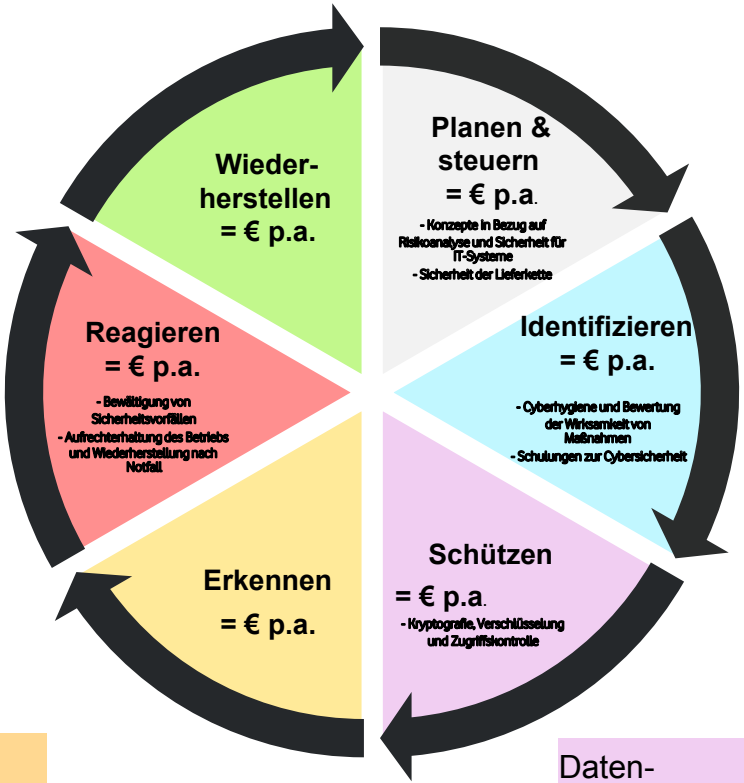
IT-Forensik

BCM-Strategie

Incident Response

Notfall-kommunikation

Mitigation / Remediation



Risiko-& Sicherheits-strategie

IT-Sicherheits-konzept

Rollen & Verant-wortlichkeiten

Dokumenten-management

Asset-/ & Risikomanagement

Penetration Test

Schwachstellen-Scan

Phishing-Simulation

Awarenes s Trainings

Antivir

SOC / MDR

IDS

Daten-speicherung

Remote Access

Firewall/DDOS

EDR, NDR, XDR

SIEM

Interne Audits

Kommunikation / Datenaustausch

Netzwerk-sicherheit

Endgeräte-management

Zugriffs-management

Sandra Sitter

Sandra Sitter
Prokuristin
Bereichsleiterin IT & Projekte
Telefon 069 580024-230
Mobil 0174 3004771
E-Mail sandra.sitter@dz-cp.de

DZ CompliancePartner

Düsseldorf

Ludwig-Erhard-Allee 20
40227 Düsseldorf

Hannover

Berliner Allee 5
30175 Hannover

Neu-Isenburg (Hauptsitz)

Wilhelm-Haas-Platz
63263 Neu-Isenburg

Stuttgart

Heilbronner Straße 72
70191 Stuttgart

Telefon 069 580024-0
Telefax 069 580024-900
E-Mail info@dz-cp.de
Internet www.dz-cp.de