German American Chambers of Commerce
Deutsch-Amerikanische Handelskammern

TeleTrusT
Pioneers in IT security.
IT Security Association Germany

German-American IT Security Forum

IT Security Association Germany (TeleTrusT) in cooperation with GACC – German American Chamber of Commerce

San Francisco, 06.05.2024

Navigating the New Frontiers: Understanding the NIS 2 Directive

Chris Wojzechowski, AWARE7

Digital Security. For Human & Machine

M.Sc. Chris Wojzechowski

Managing Director AWARE7 GmbH

Bachelor of Science
Westfälische Hochschule Bocholt – *Business Informatics*

Master of Science
Westfälische Hochschule Gelsenkirchen – *Internet-Security*

IT-Grundschutz Praktiker (TÜV)
Development and expansion of ISMS systems according to ISO 27001 on the basis of IT baseline protection

IT-Risk-Manager (DGI)
IT risk analysis and assessment according to ISO 31000

Veröffentlichungen:

- Compass IT encryption study for the Federal Ministry for Economic Affairs and Energy *(BMWi)*
- My digital security - tips and tricks for dummies , Wiley, 06.10.2021
- My digital security for dummies Wiley, 14.02.2024

About us

We are an ISO 27001 certified cybersecurity company.

We are committed to increasing the use of technology and training in Europe.

The promotion of academic education is anchored in our DNA.

Dealing with technology and the further development and training of our skills are part of our identity.

44
Employes

500
aqm Office Space

ca. 70 %
with academic degree

2
on-going doctoral projects

Overview of the NIS-2 Directive

Purpose: Achieve a high common level of cybersecurity across the European Union

Scope: Applies to various sectors, including energy, transport, health, and digital infrastructure.

Repeal: Replaces the previous NIS Directive (EU 2016/1148), which takes effect on 18 October 2024.

Key Objectives of NIS-2 Directive

High Common Level of Cybersecurity

- Establishing consistent standards and practices for essential and important entities.

Scope of Application

- A wide range of sectors, including energy, transport, health, digital infrastructure, banking, and public administration.

Risk Management and Prevention

- Emphasizes an all-hazards approach, addressing a wide variety of potential risks and incidents.

Enhanced Cooperation and Oversight

- Establishes the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) to support coordinated incident management.

Directive Timeline & Deadlines

- Published in December 2022
- Member States must adopt and publish compliance measures by 17th October 2024
- Effective implementation from 18th October 2024
- By 17th July 2024, EU-CyCLONe must submit its first report
- By 17th April 2025, Member States must establish a list of essential and important entities
- 17th October 2027: The Commission reviews the functioning of the directive

Compliance Requirements

Compliance with Cybersecurity Measures

Entities must take appropriate and proportionate technical, operational, and organizational measures to manage risks to network and information systems.

All-Hazards Approach

Requires entities to consider a comprehensive range of risks, from cyber threats to physical threats like fire, flood, or unauthorized access

Governance and Accountability

Management Bodies' Role

Management bodies can be held liable for non-compliance with the directive.

Mandatory Cybersecurity Training

Management bodies must receive training to understand and manage cybersecurity risks effectively.

Encourages training for employees to ensure a consistent cybersecurity culture throughout the organization.

Cybersecurity Risk management Measures

Based on "state-of-the-art" standards

- Entities must consider the latest cybersecurity practices and technologies.
- "State-of-the-art" encompasses relevant European and international standards.

Measures include the following

- Risk Analysis
- Incident Handling
- Business Continuity
- Supply Chain Security
- Security in Network and Information Systems Acquisition, Development, and Maintenance
- Assessing Risk-Management Effectiveness
- Basic Cyber Hygiene Practices and Training
- Use of Cryptography and Encryption
- HR Security, Access Control, Asset Management
- Use of MFA or Continuous Authentication Solutions

CSIRT - Computer Security Incident Response Team

Member States shall designate one or more CSIRTs to

- enhance cybersecurity incident response capabilities
- foster collaboration among stakeholders for effective incident handling
- promote information sharing and best practices to mitigate cyber threats

Main Tasks

- monitoring and analyzing cyber threats, vulnerabilities and incidents at national level
- providing assistance to essential and important entities
- providing early warnings, alerts, announcements and dissemination of information
- upon request, proactive scanning of the network and information systems

Essential and important Entities

Categorization by size

More than 250 Persons an annual turnover exceeding EUR 50 million and/or annual balance sheer exceeding EUR 43 million

Categorization by sector

Energy, Transport, Banks, Financial markets, Health, Drinking water, Waste water, Digital infrastructure, ICT service management, public administration, Space

Reporting Obligations and Incident Handling

Notification of significant incidents

- EU member states shall ensure that essential and important entities notify its CSIRT or competent authority in case of incidents with significant impact.
- Where appropriate entities shall notify, without undue delay, the recipients of their services.

Significant Incident

- it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned.
- it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

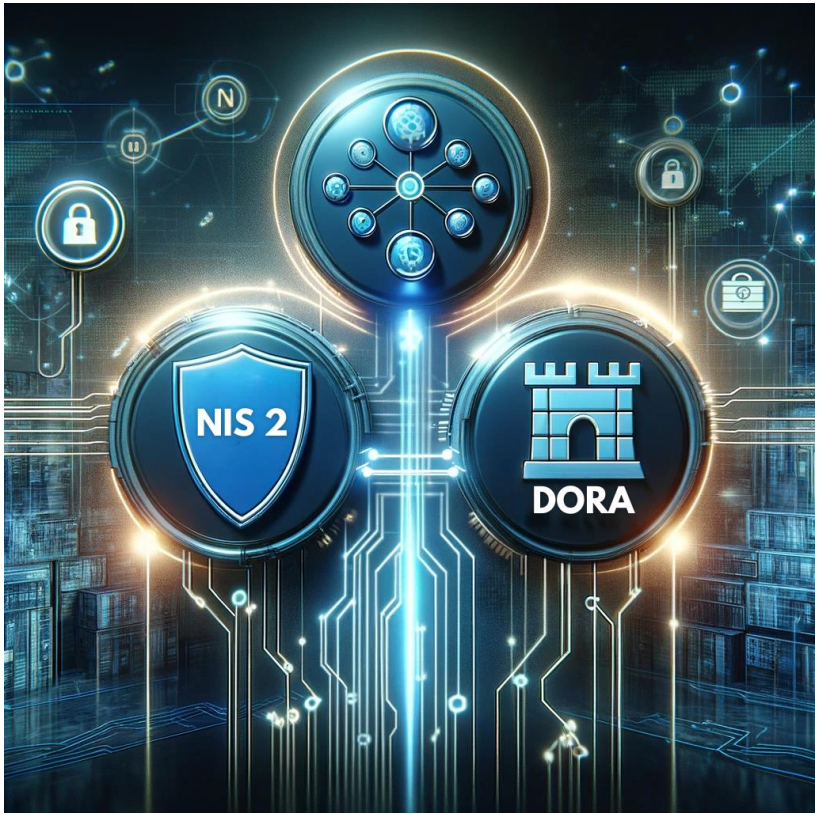
NIS-2 & DORA

Applicability of Sector-Specific Legal Acts

Entities covered by sector-specific Union laws (e.g., DORA) are exempt from NIS 2 provisions if their cybersecurity measures are equivalent or stricter.

DORA Provisions Override NIS-2 Directive

DORA, a sector-specific Union law, takes precedence over NIS 2 for financial entities, covering ICT risk management, incident reporting, resilience testing, information sharing, and third-party risk.



Enforcement and Sanctions

Non-monetary Remedies

National authorities can enforce non-monetary penalties such as compliance orders, binding instructions, security audits, and threat notifications to customers.

Administrative Fines

Differentiates fines for essential and important entities. Essential entities face fines up to €10 million or 2% of global annual revenue, while important entities face fines up to €7 million or 1.4% of global annual revenue.

Criminal Sanctions for Management

NIS2 introduces measures to hold top management personally liable for gross negligence after a cyber incident, including public disclosure of violations, identifying responsible parties, and temporary bans on management positions for repeated violations.

Summary

Expanded Scope: NIS-2 covers more sectors, enhancing security for Europe's critical infrastructures.

Stricter Requirements: Introduces tougher security and mandatory reporting, improving protections and response times.

Enhanced Cooperation: Facilitates better coordination and information sharing across EU states to tackle cyber threats.

Robust Risk Management: Mandates comprehensive risk assessments and regular audits, boosting resilience.

Cultural Shift: Promotes a stronger cybersecurity culture, increasing awareness and expertise across the EU.

AWARE 7

Thanks for your attention. Questions?

AWARE 7 GmbH
Full Service Awareness Agency

Munscheidstrasse 14
45886 Gelsenkirchen

+49 (0) 209 8830 6760 1
info@aware7.de