

KLARE ZIELE. SICHERE WEGE. NEUE PERSPEKTIVEN.

Cybersicherheit und NIS2-Compliance

Dr.-Ing. Peter Samulat



1

VORSTELLUNG EXPERTPLACE

<p>Business-Beratung</p> <p>Unsere Experten beraten in signifikanten Bereichen wie Strategie, Organisation, Prozess-, Architektur und Risikomanagement.</p>	<p>IT-Beratung</p> <p>Unsere Experten beraten in signifikanten Bereichen wie Strategie, Governance, Sicherheit, Infrastruktur-, Service-, Architektur- und Risikomanagement.</p>	<p>Methodik und Wissen</p> <p>Mit unserer academy vermitteln wir Methodik und Wissen auf höchstem Niveau.</p>	<p>Experten-netzwerk</p> <p>Neben unseren festen Beratern verfügen wir über ein breites und langjähriges Netzwerk an freien Mitarbeitenden.</p>	<p>Arbeitnehmer-überlassung</p> <p>Mit unserem Team der professionals bieten wir Arbeitnehmerüberlassung und Direktvermittlung an.</p>	<p>Business Transformation</p> <ul style="list-style-type: none"> Business Software Prozesse & Digitalisierung Unternehmensstrukturen 	<p>M365 Beratung</p> <ul style="list-style-type: none"> M365 Core M365 Factory M365 Transition
<p>Transformation Management</p> <p>Projekt- und Programm</p> <ul style="list-style-type: none"> Management Advisory PMO 					<p>IT-Transformation</p> <ul style="list-style-type: none"> IT Due Diligence IT Strategie & Architektur IT Service & Infrastruktur Management 	<p>IT-Security</p> <ul style="list-style-type: none"> NIS-2-Compliance IT Security Governance & Awareness Information Security Management System

<p>2007</p> <p>Gründung der Expert Place GmbH</p>	<p>2008</p> <p>Umfirmierung in expertplace networks group AG</p>	<p>2009</p> <p>Start der expertplace academy</p>	<p>2014</p> <p>Gründung expertplace professionals GmbH</p>	<p>2015</p> <p>ISO 9001 Zertifizierung expertplace networks group</p> <p>Top Consultant 2015</p>	<p>2017</p> <p>Top Job 2017</p> <p>Top Consultant 2017</p>	<p>2018</p> <p>Gründung der expertplace advisors GmbH</p>	<p>2019</p> <p>Top Job 2019</p> <p>Top Consultant 2019</p>	<p>2021</p> <p>Re-Zertifizierung EN ISO 9001:2015</p> <p>Top Consultant 2021</p>	<p>2022</p> <p>Re-Zertifizierung DIN EN ISO 9001:2015</p> <p>Mitglied im BVMW e.V.</p>	<p>2023</p> <p>Top Job 2023</p>	<p>2024</p> <p>Re-Zertifizierung DIN EN ISO 9001:2015</p> <p>Top Consultant 2024</p> <p>Carbon Disclosure Project (DCP) Siegel</p>	<p>2025</p>
--	---	---	---	---	---	--	---	---	---	--	---	--------------------



2

2

NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2 (NIS2)

„Die IT-Bedrohungslage ist weiterhin angespannt und das ist und bleibt besorgniserregend. Insbesondere Ransomware, Spionage und Desinformation bedrohen unseren Wohlstand und gefährden unsere Demokratie.

(...)

Wir müssen unsere Demokratie auch im Digitalen schützen. Wir müssen uns gegen Bedrohungen durch Hackerangriffe, Manipulationen und Desinformation besonders wappnen. Diese hybriden Bedrohungen gehen vor allem von Putins Regime in Russland, aber auch von anderen Akteuren aus. Umso wichtiger ist es, Schutzmaßnahmen zu verstärken. Cybersicherheit ist zentral für unsere Gesellschaft und betrifft jeden von uns.“

BSI-Präsidentin Claudia Plattner. Bericht zur Lage der IT-Sicherheit in Deutschland. 12.11.2024.

3

NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2 (NIS2)

NIS2 nimmt Unternehmen in die Pflicht

Bedrohungslage

„Die Bedrohung im Cyberraum ist so hoch wie nie zuvor.

Cyberangriffe werden nicht nur zunehmend professioneller, sie treffen auch immer öfter kleine und mittlere Organisationen, Kommunen und staatliche Institutionen.

Hinzu kommen vollkommen neue Risiken durch künstliche Intelligenz.“

(BSI, [Bericht zur Lage der IT-Sicherheit in Deutschland 2023](#))

Gegenmaßnahme

Als Antwort drauf reagiert die EU mit der NIS2-Richtlinie, die zum 17. Oktober 2024 in Deutschland in nationales Recht umgesetzt werden sollte, um die Cybersicherheit zu stärken.

Mit der Einführung der NIS2 sind Unternehmen verpflichtet,

- sich selbst einzustufen,
- sich bei der zuständigen Behörde zu registrieren,
- Sicherheitsvorfälle zu melden und
- eine Reihe von Sicherheitsmaßnahmen zu ergreifen, einschließlich Risikomanagement, Sicherheit in der Lieferkette und angemessene Reaktion auf Sicherheitsvorfälle.

4

NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2 (NIS2)

Risikomanagement als Grundpfeiler der NIS2-Compliance

Operative und organisatorische Maßnahmen sind gefordert

Unternehmen, die als wesentliche oder wichtige Einrichtungen eingestuft werden, sind verpflichtet, angemessene und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu verhindern oder zu minimieren.

Die NIS2-Richtlinie fordert somit technische und organisatorische Maßnahmen (TOM) gemäß dem sogenannten „Stand der Technik“.

Durch ein strukturiertes Risikomanagement sollen Unternehmen potenzielle Bedrohungen und Schwachstellen in ihren Netz- und Informationssystemen frühzeitig erkennen.

Dies umfasst sowohl interne als auch externe Bedrohungen, wie etwa Cyberangriffe, Datenschutzverletzungen, Systemausfälle oder menschliches Versagen.



Klare Ziele. Sichere Wege. Neue Perspektiven.

5

5

NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2 (NIS2)

Verpflichtung der Geschäftsleitung und Folgen einer Nichteinhaltung

Pflichten

Geschäftsleitungen von Einrichtungen müssen

- die Risikomanagement-Maßnahmen für Cybersecurity billigen und
- die Umsetzung in der Einrichtung überwachen. §38(1).

Geschäftsleiter müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Bewertung von Risiken und Maßnahmen sicherzustellen. §38 (3).

Mögliche Folgen einer Nichteinhaltung

Werden diese Pflichten verletzt, ergibt sich aus allgemeinen Grundsätzen (bspw. §93 AktG) eine Binnenhaftung der Geschäftsleitung gegenüber der Einrichtung.

Im Rahmen der neuen Verordnung können nationale Behörden wesentliche Einrichtungen mit einer maximalen Geldbuße in Höhe von 10 Millionen Euro oder 2 % des weltweiten Umsatzes belegen, je nachdem, welcher Betrag höher ist. Für wichtige Einrichtungen beträgt die maximale Höhe der Geldbußen 7 Millionen Euro oder 1,4 % des weltweiten Umsatzes, je nachdem, welcher Betrag höher ist.

Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



Klare Ziele. Sichere Wege. Neue Perspektiven.

6

6

NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2 (NIS2)

Mindest-Maßnahmenkatalog nach §30(2): Expertenwissen ist gefordert!

1. Risikoanalyse und Sicherheit für Informationssysteme
2. Bewältigung von Sicherheitsvorfällen
3. Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management
4. Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
5. Sicherheit in der Entwicklung, Beschaffung und Wartung
6. Management von Schwachstellen
7. Bewertung der Effektivität von Cybersicherheit und Risiko-Management
8. Schulungen Cybersicherheit und Cyberhygiene
9. Kryptografie und Verschlüsselung
10. Personalsicherheit, Zugriffskontrolle und Anlagen-Management
11. Multi-Faktor Authentisierung und kontinuierliche Authentisierung
12. Sichere Kommunikation (Sprach, Video- und Text)
13. Sichere Notfallkommunikation

Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



Klare Ziele. Sichere Wege. Neue Perspektiven.

7

7

NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2 (NIS2)

BSI-Empfehlungen: Was Sie konkret tun können (Auszug)

1. Benennen Sie zuständige Personen

Suchen, benennen und befähigen Sie mindestens zwei Personen Ihres Unternehmens, eine koordinierende Rolle für die Informationssicherheit zu übernehmen. [IT-Grundschutz-Baustein ORP.2 Personal](#)

2. Übernehmen Sie als Leitung die Verantwortung

Bereiten Sie sich als Unternehmensleitung darauf vor, Verantwortung im Bereich Risikomanagement übernehmen zu können und informieren Sie sich über entsprechende Schulungsangebote.

Auf der Webseite [Management von Cyber-Risiken](#) der [Allianz für Cyber-Sicherheit](#) finden Sie ein [Handbuch](#) und ein [Toolkit](#) für Unternehmensleitungen.

3. (...)

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-was-tun/NIS-2-was-tun_node.html



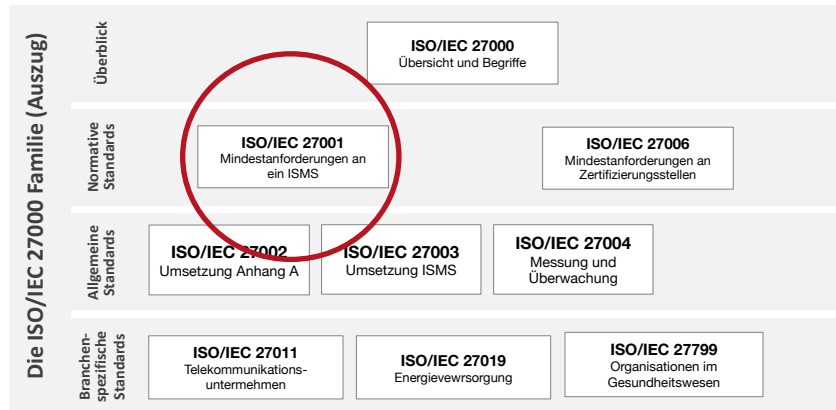
Klare Ziele. Sichere Wege. Neue Perspektiven.

8

8

NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2 (NIS2)

Die ISO/IEC 27001 Familie (Auszug)



9

NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2 (NIS2)

Unser Angebot: Ein systematischer, proaktiver und herstellernerutraler Ansatz zur Cybersicherheit:

01. Risikomanagement als zentrale Anforderung:

Eine ehrliche, praxisnahe GAP-Analyse, um Schwachstellen zu identifizieren.

02. Sicherheitsmaßnahmen und Kontrollen:

Konkrete, angemessene und verhältnismäßige Maßnahmen zur Verbesserung der Cybersicherheit identifizieren, umsetzen und kontrollieren.

03. Incident-Management und Meldepflichten:

Design und Etablierung von Prozessen zur Erkennung, Meldung und Bewältigung von Sicherheitsvorfällen bis hin zum Notfallmanagement.

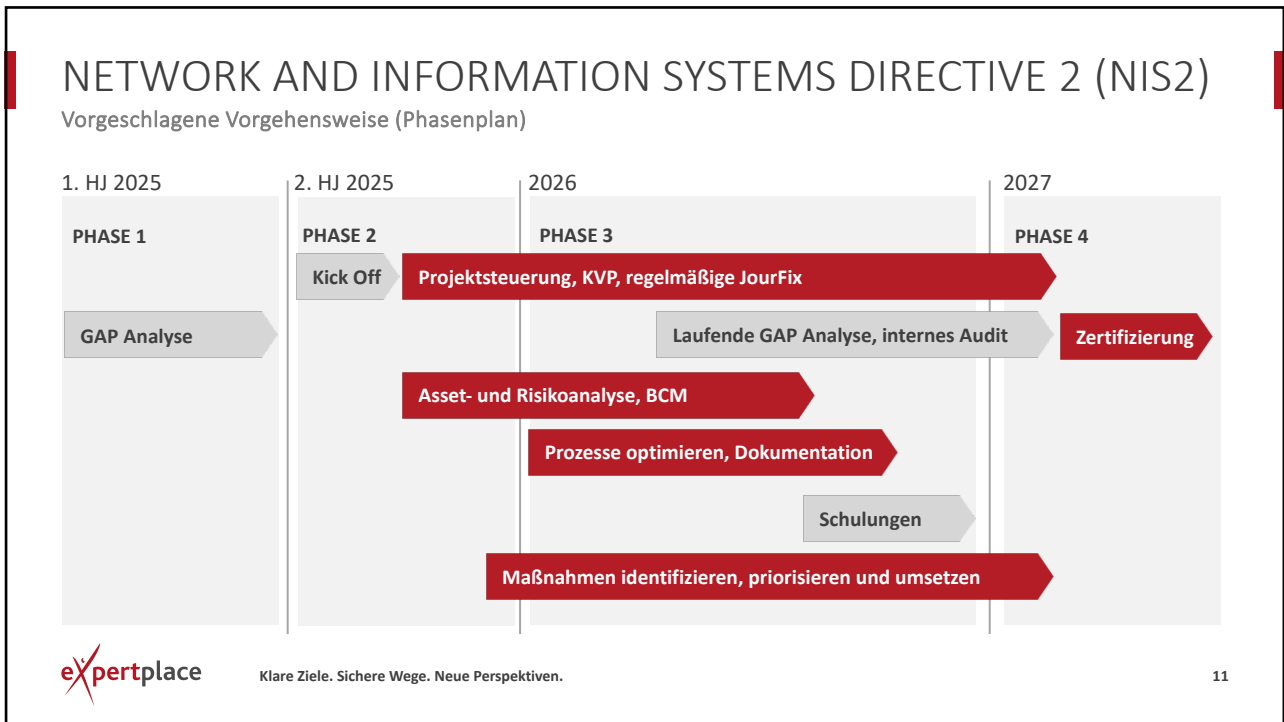
04. Lieferketten- und Drittanbieter-Risiken:

Bewertung und Absicherung von Drittanbietern und Partnern, z. B. durch Verträge, Audits und Sicherheitsrichtlinien.

05. Governance, Schulung und Sensibilisierung:

Schulungsprogramme und Sicherheitsrichtlinien, um Führungskräfte und Mitarbeiter für die Cybersicherheit zu sensibilisieren.

10



11

IHR ANSPRECHPARTNER

Dr.-Ing. Peter Samulat



Dr.-Ing. Peter Samulat
Principal Consultant

expertplace networks group AG
Oberländer Ufer 186
50968 Köln

Telefon +49 221 800 335 00
Mail peter.samulat@expertplace.de
Web www.expertplace.de

expertplace Klare Ziele. Sichere Wege. Neue Perspektiven. 12

12

KLARE ZIELE. SICHERE WEGE. NEUE PERSPEKTIVEN.

Cybersicherheit und NIS2-Compliance

expertplace