

NIS2 UMSETZUNG LEICHT GEMACHT

SO GELINGT DIE UMSETZUNG UND DER NACHWEIS VON NIS2-COMPLIANCE

www.neam.de

NIS2 – NEUE ANFORDERUNGEN FÜR IT-VERANTWORTLICHE IN DER EU

Die europäische NIS2-Richtlinie (Netz- und Informationssystemsicherheit) verfolgt das Ziel, ein einheitlich hohes Maß an Cybersicherheit in der gesamten EU sicherzustellen. In Deutschland ist die Richtlinie inzwischen vollständig umgesetzt: Das NIS2-Umsetzungsgesetz ist am 6. Dezember 2025 in Kraft getreten und gilt seitdem verbindlich, ohne Übergangsfrist.

Mit der neuen Regelung wurden die Anforderungen deutlich verschärft und der Anwendungsbereich massiv ausgeweitet: Rund 30.000 Unternehmen aus 18 Sektoren fallen nun unter die gesetzlichen Vorgaben. Neben Betreibern kritischer Infrastrukturen sind erstmals auch zahlreiche mittelständische Unternehmen betroffen.

Unternehmen sind verpflichtet, umfassende Maßnahmen zum Cyber-Risikomanagement umzusetzen, Sicherheitsvorfälle zeitnah zu melden und sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zu registrieren. Die entsprechenden Registrierungsfristen sind bereits im März 2026 ausgelaufen.

Eine zentrale Neuerung ist die deutlich gestärkte Verantwortung der Unternehmensleitung: Geschäftsführung und Aufsichtsgremien sind nun gesetzlich zur Überwachung der Cybersicherheitsmaßnahmen verpflichtet und haften persönlich bei Verstößen.

Die NIS2-Regulierung bringt zudem strengere Meldepflichten, höhere Sicherheitsstandards sowie verschärfte Sanktionen und fördert die Zusammenarbeit der EU-Staaten im Bereich Cyberabwehr.

Unternehmen stehen damit vor der Aufgabe, ihre Sicherheitsstrategien kurzfristig anzupassen, Prozesse zu professionalisieren und Kompetenzen gezielt aufzubauen. Wer jetzt handelt, stellt nicht nur die Einhaltung gesetzlicher Vorgaben sicher, sondern stärkt nachhaltig die eigene Widerstandsfähigkeit gegenüber Cyberbedrohungen.

WER IST BETROFFEN?

Betroffen sind Unternehmen ab 10 Mio. € Jahresumsatz und ab 50 Mitarbeiter aus bestimmten Sektoren; wobei NIS2 Einrichtungen in kritische Infrastrukturen, besonders wichtige und wichtige Unternehmen unterteilt. Ungeachtet der Einstufung sind Anbieter öffentlicher Kommunikationsnetze und -dienste sowie Vertrauensdiensteanbieter und Namensregister der obersten Domäne (inkl. DNS-Diensteanbieter) stets erfasst. Sektoren mit hoher Kritikalität (Anhang I): Energie, Verkehr, Bank- und Finanzwesen. Gesundheitswesen, Wasserversorgung, Digitale Infrastruktur, ITK-Dienste, Öffentliche Verwaltung, Weltraum.

Sonstige kritische Sektoren (Anhang II): Post- und Kurierdienste, Abfallwirtschaft, Chemie, Ernährung, Herstellung von Waren, Digitale Dienste, Forschung Konkrete technische Maßnahmen gibt die Richtlinie nicht vor. Branchenstandards wie etwa B3S (KRITIS), IT-Grundschutz (BSI), ISO/IEC 27001, TISAX® werden in diesem Fall hinzugezogen.



NIS2 Geschäftsleitungsschulung

ab 330,- €

Gemäß §38 der NIS2-Richtlinie müssen Mitglieder der Geschäftsleitung sicherstellen, dass Sie über das nötige Wissen und die Fähigkeiten verfügen, um Ihre Verantwortung in der Cybersicherheit wahrzunehmen.

Dies beinhaltet unter anderem die Pflicht, angemessene Maßnahmen zur Risikominimierung zu ergreifen und die Einhaltung gesetzlicher Vorgaben zu gewährleisten. Unsere Schulung vermittelt Ihnen das notwendige Fachwissen, um diesen Anforderungen gerecht zu werden und Ihr Unternehmen zukunftssicher aufzustellen.

Online buchbar

alle Preise zzgl. der ges. MwSt.

NIS2 Manager

1.690,- €

Der NIS2 Manager unterstützt Sie bei der Umsetzung der NIS2-Richtlinie, von der ersten Einschätzung bis zur Konformität. Unabhängig vom Reifegrad Ihrer IT-Sicherheit begleiten wir Sie strukturiert durch alle Phasen und sorgen für eine praxisnahe Umsetzung der gesetzlichen Anforderungen.

Dabei unterstützen wir Sie bei der Einführung von Risikomanagement-Maßnahmen, der Umsetzung vom Business Continuity Management, der Etablierung von Melde- und Registrierungsprozessen sowie der Einhaltung der Pflichten der Geschäftsführung. Ziel ist es, die Anforderungen effizient und nachhaltig in Ihrer Organisation zu verankern.

Online buchbar

alle Preise zzgl. der ges. MwSt.

NIS2 Audit als Start in Ihr ISMS

2.990,- €

Wie steht es um die Informationssicherheit in Ihrer Organisation? Sie brauchen einen Nachweis für Kunden und /oder Partner, dass sie bestimmte Sicherheitsstandards zur Informationssicherheit einhalten.

Gesamteindruck der Organisation / Ansprechpartner und Verantwortlichkeiten / Bessere Vorbereitung des Projekts durch Statusanalyse / Wiederverwendbarkeit der Ergebnisse für Zertifizierungsvorbereitung / Differenzierteres Vorgehen auf Basis der Ergebnisse / genauere Kalkulation des Projekts anhand der erhobenen Daten

Online buchbar

alle Preise zzgl. der ges. MwSt.

MEHR ALS 25 JAHRE IT-SERVICES

Wir unterstützen Sie mit umfangreicher Projekterfahrung, unserem Expertenteam und starken Best Practices.

1 IT-Allrounder

- ✓ Wir realisieren zeitgemäße Konzepte & Lösungen für eine performante, hochverfügbare IT.
- ✓ Storage, Server, Netzwerk, Firewall, WLAN, Desktop, Backup, Wiederanlaufpläne, Virtualisierung, Betriebssysteme, M365- Architektur, Azure, Exchange, IT-Monitoring

2 Starkes IT-Expertenteam

- ✓ Innovative Fachteams
- ✓ Tiefgreifendes Know-how
- ✓ Zahlreiche Hersteller-Zertifizierungen
- ✓ Umfassende Projekterfahrung
- ✓ Dedizierter Projekt-Ansprechpartner
- ✓ Projektmanagement nach ITIL & Prince2

3 Technische IT-Sicherheit

- ✓ Penetrationstests
- ✓ SIEM (Angriffserkennung)
- ✓ Incident Response
- ✓ Endpoint Sicherheit (EDR, XDR & MDR)
- ✓ E-Mail Security
- ✓ Security Awareness & Phishing
- ✓ Passwort Sicherheit
- ✓ Pentest & Schwachstellenscans
- ✓ Aktives Patchmanagement
- ✓ BCM (Notfallmanagement)

4 Professioneller Support

- ✓ Helpdesk auf Wunsch auch 24/7/365
- ✓ Wir patchen 1000 Server jeden Monat
- ✓ Wir betreuen 600 aktive Kunden
- ✓ Für unsere Kunden pflegen und warten wir mehr als 100 IT-Infrastrukturen jeden Monat
- ✓ Alle Leistungen als Full-Service oder als Projektunterstützung für Ihr IT-Team

Prävention, Detektion & Reaktion – schützen Sie Ihre Organisation vor Cyberangriffen durch innovative Security Lösungen & Services. Sprechen Sie uns an, wir bieten zahlreiche weitere Managed Services für Ihre IT. Sorgen Sie gemeinsam mit uns für mehr IT-Sicherheit.

JETZT HANDELN!



KOMPETENZ INFORMATIONSSICHERHEIT

Wir unterstützen Sie mit umfangreicher ISMS-Projekterfahrung und unseren Best Practices für alle Branchen und Standards.

1 Umfassende Informationssicherheitsberatung

- ✓ Für mehr als 100 Organisationen stellen wir den ISB
- ✓ mehr als 2000 erfolgreich umgesetzte ISMS-Projekte in mehr als 25 Jahren
- ✓ Durchführung von mehr als 500 Audits & Zertifizierungen.

2 Branchen & öffentliche Einrichtungen

- ✓ Kritische Infrastrukturen
- ✓ Finanzdienstleister, Banken, Versicherungen
- ✓ Öffentlicher Dienst, Sozialversicherungsträger
- ✓ Gesundheitswesen
- ✓ Groß- und Einzelhandel
- ✓ Verkehrsunternehmen, Fluggesellschaften
- ✓ Industrie, Maschinenbau

3 Unser Know-how für zahlreiche Standards

- ✓ Kritische Infrastrukturen (KRITIS)
- ✓ Branchenstandard (B3S)
- ✓ KRITIS-Prüfung (§8a BSIG)
- ✓ NIS2
- ✓ ISO 27001
- ✓ IT-Grundschutz (BSI)
- ✓ TISAX®-Norm
- ✓ BSI C5 Prüfung

4 Großes Team von qualifizierten Beratern

- ✓ IT-Grundschutz-Praktiker
- ✓ IT-Grundschutz-Berater
- ✓ Informationssicherheitsbeauftragte(r) (TÜV)
- ✓ ISO Lead Implementer
- ✓ ISO Lead Auditor
- ✓ Business Continuity Manager
- ✓ Prüfverfahrenskompetenz für § 8a (3) BSIG

5 Unsere Best Practices für Ihr ISMS

- ✓ Tool gestützte Umsetzung (verinice, fuentis, R2C_GRC, HISCOUT etc.)
- ✓ Vorlagen Pakete
- ✓ Risikoanalysen
- ✓ ISMS-Handbuch
- ✓ Richtlinien Vorlagen
- ✓ Optimierung der Prozesse

6 Lassen Sie Ihr Team von Profis schulen

- ✓ Unsere Trainer/-innen sind projekterfahrene Mitarbeiter/-innen (BSI- oder ISO 27001-Umfeld bzw. im Bereich Penetrationstests)
- ✓ Vor Ort oder remote

**BEING
HUMAN
AND MAKING IT
BETTER**

Schutzbedarf auf Basis IT-Grundschutz (BSI)	NORMAL			
Risikoanalyse und Sicherheit für Informationssysteme	Asset Discovery, Beschreibung und Softwareinventarisierung Managed Client & Server	Bestehende Schwachstellen und Sicherheitslücken identifizieren Managed Schwachstellenscan mit Enginesight	Regelmäßige Penetrationstests der IT-Infrastruktur und bisher umgesetzter Sicherheitsmaßnahmen Zahlreiche Pentests, auch für individuelle Anforderungen	Implementierung von Schutzmaßnahmen für Endpoints & Server Einsatz von Sophos, Cybereason oder Microsoft Defender als EDR, MDR, XDR
Bewältigung von Sicherheitsvorfällen	Angriffe, fehlerhafte oder ungewöhnliche Aktivitäten im Netzwerk, die sich auf kritische Dienste auswirken könnten, frühzeitig erkennen SIEM mit Microsoft Sentinel oder Enginesight	Schadsoftware und Angreifende an Netzwerkgrenzen bestmöglich abwehren Einsatz von Sophos, Cybereason oder Microsoft Defender als EDR, MDR, XDR, NextGen Firewall	i Schnelle Reaktion auf Cybervorfälle sicherstellen (Incident Response) Managed Service Incident Response in Verbindung mit dem Managed Service ISB	
Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management	Mehrstufiges Backup-Management etablieren Pragmatische Backup Konzepte mit veeam & arcserve auf Wunsch auch nach BSI	Datensicherung und Redundanz Pragmatische Backup Konzepte mit veeam & arcserve, in Verbindung mit Wiederanlaufplänen und Hochverfügbarkeitskonzepten	Notbetrieb und schnelle Wiederherstellung der IT-Infratraktur im Notfall ermöglichen Technische Wiederanlaufpläne für IT-Infrastrukturen und Testung	
Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit	Die technische Kommunikation der Schnittstellen überwachen, auswerten und ggf. automatisierte Maßnahmen etablieren SIEM mit Microsoft Sentinel oder Enginesight	i Sicheren Lieferanten-Zugang zum Netzwerk gewährleisten (z.B. sichere Passwörter, VPN) Lösungen von Sophos Firewall & Mateso Passwordsafe, Beratung ISMS nach ISO/BSI auch als Managed Service ISB	Sichere Datenübertragung über verschlüsselte Medien E-Mail Security Consulting mit NoSpam-Proxy & Microsoft M365 Security	
Sicherheit in der Entwicklung, Beschaffung und Wartung; Management von Schwachstellen	Regelmäßige Penetrationstests von Software und IT-Infrastruktur Vielseitige Pentests für unterschiedliche Anforderungen sowie Managed Schwachstellenscan mit Enginesight	Dauerhaftes Monitoring von Schwachstellen Managed Schwachstellenscan mit Enginesight	Effektive und sichere Behandlung von Schwachstellen Managed Schwachstellenscan mit Enginesight, Managed Service für Clients & Server sowie Systempflege der IT-Infrastruktur	Sicherheit von Endgeräten und operativen Systemen Einsatz von Sophos, Cybereason oder Microsoft Defender als EDR, MDR, XDR
Bewertung der Effektivität von Cybersicherheit und Risikomanagement	Die Wirksamkeit der technischen Cybersicherheitsmaßnahmen fortlaufend überprüfen und verbessern Vielseitige Pentests für unterschiedliche Anforderungen sowie Managed Service Schwachstellenscan mit Enginesight	i Cybersicherheitslage und Risikoexposition regelmäßig neu bewerten Jährliches Security Assement auf Wunsch auch Managed Service ISB	i Bewerten von Sicherheitsereignissen, um Sicherheitsvorfälle zu identifizieren Incident Response Service in Verbindung mit Beratung ISMS nach ISO/BSI auch als Managed Service ISB	
Schulungen Cybersicherheit und Cyberhygiene	Gefährdete Assets überwachen und abschirmen, bei denen Patches/ Aktualisierungen nicht möglich sind Managed Client & Server in Verbindung mit dem Einsatz der Lösung von Sophos, Cybereason oder Microsoft Defender als EDR, MDR, XDR	Regelmäßige Cybersicherheits-schulungen für Mitarbeiter umsetzen Managed Awareness durch Knowbe4 und auf Wunsch individuelle Awarness-Schulungen	i Starke Passwortrichtlinien festlegen und umsetzen Beratung ISMS nach ISO/BSI auch als Managed Service ISB Consulting & Umsetzung für gängige IT-Infrastrukturen	Firmware, Betriebssysteme nachhaltig und dauerhaft aktuell halten Managed Service für Clients & Server sowie Systempflege der IT-Infrastruktur
Kryptografie und Verschlüsselung	Überwachung und Überprüfung verschlüsselter Verbindungen nach aktuellem Stand der Technik. Abgleich TLS nach TR-03116-4 Checkliste des BSI Consulting E-Mail-Security, E-Mail-Fluss & digitale Zertifikate	Einrichtung und Sicherstellung einer durchgehenden verschlüsselten Kommunikation im internen Netz Consulting E-Mail-Security, E-Mail-Fluss & digitale Zertifikate	i Klassifizierung und Kennzeichnung von Informationen Beratung ISMS nach ISO/BSI als auch Managed Service ISB Consulting für Microsoft M365 Information Protection	
Personalsicherheit, Zugriffskontrolle und Anlagenmanagement	i Sicherheitsmaßnahmen für physische und Remote-Zugriffe Security Assement für Best Practices IT-Security auch Managed Service ISB	i Sicherheitsüberprüfungen und -sensibilisierungen in das Einstellungs- und Vertragsvergabeverfahren integrieren Beratung ISMS nach ISO/BSI auch als Managed Service ISB	i Unbefugten physischen Zugriff auf Assets verhindern Beratung ISMS nach ISO/BSI auch als Managed Service ISB	Verwalten von Zugriffskontrollen gemäß Sicherheitsrichtlinien Multifaktorlösung für OnPrem und Third-partylösungen, Schutz von Service- & Administrationsaccounts durch Silverfort
Multi-Faktor-Authentifizierung und kontinuierliche Authentifizierung	Personalisierte Multi-Faktor-Authentifizierung sicherstellen Microsoft ZeroTrust sowie Silverfort für OnPrem Instrastrukturen, Service- & Administratoraccounts	Unbefugten Zugriff auf digitale Assets verhindern. Überwachung aller Logins und Loginversuche EngineSight SIEM & Cybereason MDR	Sichere digitale Kommunikation gewährleisten Implementierung von M365 Infrastruktur in Verbindung mit M365 Sicherheitskonzept & Tenant Härtung	
Sichere Kommunikation (Sprach, Video- und Text)	Überwachung sämtlicher Kommunikationssysteme und der verschlüsselten Verbindungen E-Mail Security Consulting mit NoSpam-Proxy & Microsoft M365 Tenant & Teams Security	i Innerhalb von 24 Stunden nach einem Vorfall Frühwarnung an CSIRT übermitteln Managed Service ISB mit Incident Response Service	i Innerhalb von 72 Stunden erste Bewertung an CSIRT übermitteln (inkl. Aussagen zu Schweregrad, Auswirkungen, Quelle) Managed Service ISB mit Incident Response Service	
Schulungen & Workshops	ISMS nach ISO, IT-Grundschutz, oder technisches Know-how für IT-Lösungen:			

* Die aufgeführten Ziele sind in der NIS2 nicht explizit definiert, sondern spiegeln allgemeine grundlegende Sicherheitsziele wider, wie sie in internationalen Normen wie der IEC 27001, 62443 empfohlen werden.

AUS DEN ANFORDERUNGEN ABLEITEN LASSEN*

HOCH			SEHR HOCH
i ISMS nach IT-Grundschutz, ISO 27001, KRITIS, TISAX® Umfassendes Beratungsportfolio zu gängigen und branchenspezifischen Standards mit ISMS-Tools wie verinice und fuentis	i Rollen, Verantwortlichkeiten Beratung zur Definition von Rollen, Verantwortlichkeiten nach ISO/BSI	i Informationssicherheitspolitik und Managementverantwortung Beratung ISMS nach ISO/BSI als auch Managed Service ISB	⚙️ Verfahren zur regelmäßigen Risikoanalyse und Schwachstellenbewertung einführen Beratung und Umsetzung durch Incident Response Service
i Beurteilung, Reaktion und Berichterstattung von sicherheitsrelevanten Ereignissen Beratung ISMS nach ISO/BSI auch als Managed Service ISB	⚙️ End-to-end Anomalie- und Angriffserkennung umsetzen. Protokollierung aller Ereignisse und Ableitung automatischer Reaktionen SIEM mit Microsoft Sentinel oder Enginesight	i ⚙️ Managed Detection and Response Services Managed Services Incident Response auch in Verbindung des Managed Service ISB, sowie MDR Lösungen von Cybereason & Sophos	i Verbesserung der Sicherheitskontrollen und -prozesse auf Grundlage von Erkenntnissen aus Sicherheitsvorfällen Beratung ISMS nach ISO/BSI auch als Managed Service ISB
i ⚙️ Business-Continuity-Plan erstellen Umfassende Beratung zu Wiederanlaufplänen, Notbetrieb und ganzheitlichem Notfallmanagement nach BSI 200-4	i ⚙️ Professionelle Krisenbewältigung und -kommunikation einrichten Beratung ISMS nach ISO/BSI/BCM & Erstellung von Wiederanlaufplänen auch als Managed Service ISB	⚙️ Störung der Prozesse durch Sicherheitsmaßnahmen vermeiden Einführung von Security-Software unter Berücksichtigung einer „Do not harm“ Policy und Best Practices	i ⚙️ Schutz vor IT-Ausfällen, Kenntnisse über Prozesse und Verfahren Beratung ISMS nach ISO/BSI Wiederanlaufpläne und ganzheitliches Notfallmanagement nach BSI 200-4
i Sicherheitsmaßnahmen für Lieferantenleistung betrachten, überwachen und anpassen Beratung ISMS nach ISO/BSI auch als Managed Service ISB	⚙️ Least Privilege Access für Lieferanten etablieren Erstellung und Implementierung eines Rechte- & Rollenkonzeptes	i ⚙️ Schnelle Abschätzung der Auswirkungen nach IT-Vorfall sicherstellen Beratung und Umsetzung durch Incident Response Service auch als Managed Service ISB	
⚙️ Bedrohungs- & Schwachstellenmanagement Managed Schwachstellenscan mit Enginesight, Managed Service für Clients & Server sowie Systempflege der IT-Infrastruktur	i ⚙️ Verfahren für den sicheren Transfer von Informationen E-Mail Security Consulting mit NoSpamProxy & Microsoft M365 Security & Sicherheitskonzept M365 auf Basis BSI		
i Angemessene Reaktion auf ein IT-Sicherheitsvorfall Erstellung und Erprobung eines Incident Response Plans	i Regelmäßige und unabhängige Überprüfung des ISMS Durchführung von Audits zu allen gängigen Standards	⚙️ Erfassung, Speicherung und Analyse von Systemprotokollen für forensische Zwecke und Audits Logmanagement Lösung	
i Betriebsverfahren der Informationssicherheit dokumentieren und Mitarbeitern zugänglich machen Beratung ISMS nach ISO/BSI auch als Managed Service ISB	⚙️ Ausbreitung von Angriffen eindämmen HPE Clearpass (NAC) in Verbindung mit einem Segmentierungskonzept	i Schulungen zur Informationssicherheit Umfangreiches Schulungsangebot mit Zertifizierungsprüfungen für IT-Sicherheitsbeauftragte, IT-Verantwortliche, ISMS-Projektleiter, Datenschutzbeauftragte	⚙️ Defense-in-Depth-Architektur aufbauen, um Versagen der Perimetersicherung frühzeitig zu erkennen und interne Netzwerk Kommunikation umfangreich zu überwachen Sophos, Cybereason (MDR) und Microsoft Sentinel oder Enginesight (SIEM)
i Schutz von Aufzeichnung und personenbezogenen Informationen Beratung ISMS nach ISO/BSI auch als Managed Service ISB	i Sichere Verwaltung von Speichermedien und Datenlöschung Beratung ISMS nach ISO/BSI auch als Managed Service ISB	i Datenmaskierung, Datenverlustpräsentation und Einsatz von Kryptografie Beratung ISMS nach ISO/BSI auch als Managed Service ISB	
⚙️ Zugriffe auf kritische Dateien und Verzeichnisse unternehmensweit überwachen Microsoft Information Protection oder Einatz von Enginesight SIEM	i ⚙️ Verwaltung privilegierter Zugriffsrechte und Informationszugriffsbeschränkungen Beratung ISMS nach ISO/BSI auch als Managed Service ISB in Verbindung mit Schutz von Service- & Administrationsaccounts durch Silverfort	⚙️ Sichere Authentifizierung und Management von Entwicklungsressourcen Consulting Microsoft M365 Security sowie Multifaktorlösung für OnPrem und Thirdpartylösungen, Schutz von Service- & Administrationsaccounts durch Silverfort	
i ⚙️ Beschränkung von Informationszugang und Netzwerksicherheit Erstellung von technischen Zugangskonzepten mit Multifaktorlösung für OnPrem und Thirdpartylösungen, Schutz von Service- & Administrationsaccounts durch Silverfort auch als Managed Service ISB			
i ⚙️ Auf Anfrage des CSIRT Aktualisierungen zum Status des Vorfallmanagements bereitstellen. Innerhalb von 72 Stunden erste Bewertung an CSIRT übermitteln (inkl. Aussagen zu Schweregrad, Auswirkungen, Quelle) Managed Service ISB mit Incident Response Service	i ⚙️ Innerhalb eines Monats detaillierten Bericht an das CSIRT übermitteln (inkl. Informationen zu Schweregrad, interne und grenzüberschreitende Auswirkungen, Ursache, Abhilfemaßnahmen). Innerhalb von 72 Stunden erste Bewertung an CSIRT übermitteln (inkl. Aussagen zu Schweregrad, Auswirkungen, Quelle) Managed Service ISB mit Incident Response Service		

Lassen Sie sich von unseren Dozenten praxisnah schulen und zertifizieren, auch Inhouse & Online.