cmt GmbH

60+
SECURITY-SEMINARE
IM PROGRAMM

NIS2 & Cybersecurity.

Compliance, Schutzkonzepte und Qualifizierung - dein Wegweiser durch die neue Sicherheitslandschaft

NIS2 · BSI IT-GRUNDSCHUTZ · ISO 27001 · INCIDENT RESPONSE · ZERO TRUST · KI-SECURITY · KRITIS

Stand: Mai 2026

cmt GmbH · cmt.de

Warum jetzt? Die Bedrohungslage

Cyberangriffe auf Rekordniveau - und kein Ende in Sicht

289 Milliarden Euro Schaden durch digitale und analoge Angriffe auf die deutsche Wirtschaft - allein im Jahr 2025. 87 Prozent aller Unternehmen sind betroffen. Die Frage ist nicht mehr ob, sondern wann dein Unternehmen angegriffen wird.

289 Mrd.	202 Mrd.	119/Tag
Euro Gesamtschaden pro Jahr (Bitkom 2025)	Euro davon durch Cyberattacken (70%)	Neue Schwachstellen in IT-Systemen (BSI)

Zentrale Trends 2025/2026

01 Ransomware bleibt die größte Bedrohung

34 Prozent der Unternehmen waren 2025 von Ransomware betroffen - fast dreimal so viele wie noch 2022. 72 Prozent der Angriffe gehen mit einem zusätzlichen Datenleak einher. Rund 80 Prozent richten sich gegen kleine und mittlere Unternehmen (BSI Lagebericht 2025).

02 KI beschleunigt die Angriffe

Die Erwähnungen bösartiger KI-Tools in Cybercrime-Foren sind um 200 Prozent gestiegen. Spezialisierte Modelle wie FraudGPT generieren überzeugende Phishing-Mails, erstellen Schadcode und automatisieren komplexe Angriffsketten - die Angriffsgeschwindigkeit hat sich von Tagen auf Minuten verkürzt.

03 Schwachstellen nehmen massiv zu

Die Zahl täglich neu entdeckter Schwachstellen ist laut BSI um 24 Prozent gestiegen. Supply-Chain-Angriffe und Schwachstellen in Open-Source-Komponenten machen die Absicherung komplexer als je zuvor.

NIS2 im Überblick

Die EU-Richtlinie, die Cybersicherheit zur Chefsache macht

Die NIS2-Richtlinie (Network and Information Security Directive 2) ist die bislang umfassendste EU-Regulierung für Cybersicherheit. Sie betrifft in Deutschland rund 30.000 Unternehmen in 18 Sektoren - und ist seit Dezember 2025 geltendes Recht.

Was hat sich geändert?

Besonders wichtige Einrichtungen

Ca. 8.000 Unternehmen in Sektoren hoher Kritikalität (Energie, Transport, Gesundheit, Bankwesen, digitale Infrastruktur) mit mindestens 250 Mitarbeitern oder über 50 Mio. EUR Umsatz.

- Proaktive Aufsicht durch das BSI
- Bußgelder bis 10 Mio. EUR oder 2% des weltweiten Jahresumsatzes
- BSI kann Betriebsgenehmigung aussetzen

Wichtige Einrichtungen

Ca. 22.000 Unternehmen in weiteren Sektoren (Lebensmittel, Chemie, verarbeitendes Gewerbe, Post, Abfall) ab 50 Mitarbeitern oder 10 Mio. EUR Umsatz.

- Reaktive Aufsicht (bei Vorfällen)
- Bußgelder bis 7 Mio. EUR oder 1,4% des Umsatzes
- Gleiche Meldepflichten wie besonders wichtige Einrichtungen

Die 18 regulierten Sektoren

Anlage 1 - Hohe Kritikalität (11 Sektoren)

- Energie (Strom, Gas, Öl, Wasserstoff, Fernwärme)
- Transport und Verkehr
- Bankwesen und Finanzmarktinfrastruktur
- Gesundheitswesen
- Trinkwasser und Abwasser
- Digitale Infrastruktur und IT-Dienste
- Öffentliche Verwaltung
- Weltraum

Anlage 2 - Sonstige kritische Sektoren (7 Sektoren)

- Post- und Kurierdienste
- Abfallwirtschaft
- Chemie
- Lebensmittelproduktion und -vertrieb
- Verarbeitendes Gewerbe
- Digitale Dienste (Marktplätze, Suchmaschinen)
- Forschung

Zeitplan: NIS2 in Deutschland

13. Nov. 2025: Bundestag verabschiedet NIS2UmsuCG
21. Nov. 2025: Bundesrat stimmt zu
6. Dez. 2025: Inkrafttreten - ohne Übergangsfrist
6. März 2026: Ablauf BSI-Registrierungsfrist

NIS2-Anforderungen im Detail

Was das Gesetz konkret von deinem Unternehmen verlangt

Das NIS2UmsuCG definiert in §30 BSIG zehn Mindestmassnahmen, die betroffene Unternehmen umsetzen müssen. Die Geschäftsleitung trägt die persönliche Verantwortung - und kann diese nicht delegieren.

01

Risikomanagement

Systematische Identifikation, Bewertung und Behandlung von Cyberrisiken. Regelmäßige Risikobewertungen mit dokumentierten Maßnahmen. Risikobasierter Ansatz nach dem Stand der Technik.

02

Incident Reporting - Dreistufige Meldepflicht

24 Stunden: Frühwarnung mit Einstufung des Vorfalls an das BSI. **72 Stunden:** Folgemeldung mit ersten Analyseergebnissen. **1 Monat:** Abschlussbericht mit vollständiger Bewertung. Die Frist beginnt ab Kenntnis, nicht ab Abschluss der Analyse.

03

Supply Chain Security

Sicherheit der Lieferkette einschließlich der unmittelbaren Zulieferer. Vertragliche Sicherheitsanforderungen, Auditrechte und Überwachung der Einhaltung.

04

Geschäftsleiterhaftung (§38 NIS2UmsuCG)

Die Geschäftsleitung muss Risikomanagement-Maßnahmen persönlich billigen und deren Umsetzung überwachen. Diese Pflicht ist nicht delegierbar. Bei Verstößen haften Geschäftsführer und Vorstände persönlich.

Weitere Pflichtmassnahmen im Überblick

- Business Continuity Management
- Kryptografie und Verschlüsselung
- Zugangs- und Zugriffskontrolle
- Multi-Faktor-Authentifizierung
- Sicherheit bei Beschaffung und Entwicklung
- Schulung und Cyberhygiene

Bußgelder und Konsequenzen

Besonders wichtige Einrichtungen: bis 10 Mio. EUR oder 2% des weltweiten Jahresumsatzes. Wichtige Einrichtungen: bis 7 Mio. EUR oder 1,4%. Bei schweren Verstößen kann das BSI die Betriebsgenehmigung aussetzen und der Geschäftsleitung die Tätigkeit untersagen.

KRITIS und deutsche Umsetzung

NIS2UmsuCG, KRITIS-Dachgesetz und BSI-Anforderungen

Deutschland hat 2025 und 2026 gleich zwei zentrale Gesetze zur Cybersicherheit und Resilienz verabschiedet. Gemeinsam bilden sie den umfassendsten Regulierungsrahmen, den es in Deutschland je für IT-Sicherheit gab.

01 NIS2UmsuCG - Das NIS2-Umsetzungsgesetz

In Kraft seit 6. Dezember 2025

Setzt die EU-Richtlinie NIS2 in deutsches Recht um. Ändert das BSI-Gesetz (BSIG) grundlegend. Erweitert den Geltungsbereich von ca. 4.500 auf rund 30.000 betroffene Unternehmen in 18 Sektoren.

Kernpflichten: Risikomanagement, Meldepflichten, Registrierung beim BSI, Geschäftsleiterhaftung, Nachweispflichten

02 KRITIS-Dachgesetz

In Kraft seit März 2026

Setzt die EU CER-Richtlinie um. Erstmals sektorübergreifende Anforderungen an physische Sicherheit, Business Continuity, Personalscreening und Krisenmanagement für Betreiber kritischer Anlagen.

Frist: Registrierung beim BBK bis 17. Juli 2026. Betrifft rund 1.300 Betreiber kritischer Infrastrukturen in 11 Sektoren.

03 BSI als zentrale Aufsichtsbehörde

Erweiterte Befugnisse seit NIS2UmsuCG

Das BSI übernimmt die zentrale Aufsicht über die Einhaltung der NIS2-Pflichten. Proaktive Überwachung bei besonders wichtigen Einrichtungen, reaktive bei wichtigen Einrichtungen.

BSI IT-Grundschutz bleibt der anerkannte Standard für die Umsetzung: BSI-Standards 200-1 bis 200-4 und das IT-Grundschutz-Kompendium bieten den methodischen Rahmen.

Qualifizierung: BSI-Zertifizierungen bei cmt

BSI IT-Grundschutz-Praktiker - BSI IT-Sicherheitsberater - BSI IT-Auditor Training - BSI IT-Grundschutz Praxis Training - Business Continuity Management

Security-Maßnahmen

Technische und organisatorische Absicherung nach Stand der Technik

NIS2 fordert Maßnahmen nach dem "Stand der Technik". Aber was bedeutet das konkret? Zwei Konzepte bilden das Fundament moderner Sicherheitsarchitekturen: Defense in Depth und Zero Trust.

Defense in Depth - Sicherheit in Schichten

1. **Perimeter Security**
   Firewalls, IDS/IPS, DDoS-Schutz, Network Segmentation
2. **Netzwerk-Sicherheit**
   Segmentierung, VPN, NAC, Micro-Segmentation
3. **Endpoint Security**
   EDR/XDR, Application Whitelisting, Patch Management
4. **Applikations-Sicherheit**
   Secure Coding, SAST/DAST, WAF, API Security
5. **Daten-Sicherheit**
   Verschlüsselung, DLP, Backup, Klassifikation
6. **Identity & Access**
   MFA, PAM, IAM, Least Privilege, RBAC

Zero Trust - Vertraue nichts, verifiziere alles

Zero Trust ist kein Produkt, sondern ein Sicherheitsparadigma: Kein Nutzer, kein Gerät und kein Netzwerk wird automatisch als vertrauenswürdig eingestuft. Jeder Zugriff wird kontinuierlich verifiziert.

Verify Explicitly	Least Privilege	Assume Breach
Authentifizierung und Autorisierung bei jedem Zugriff	Minimale Rechte, Just-in-Time und Just-Enough-Access	Immer davon ausgehen, dass das Netzwerk kompromittiert ist

Seminare zu diesem Thema

Cybersecurity-Training für Techniker - IT-Sicherheit: (Anti-) Hacking für Admins - Linux Security Intensivkurs - AZ-500: Azure Security Technologies - LFS482: Zero Trust Security

Incident Response & Business Continuity

Vorfälle erkennen, melden und den Betrieb sichern

NIS2 macht professionelles Incident Management zur Pflicht. Die 24-Stunden-Meldefrist lässt keinen Raum für Improvisation - du brauchst etablierte Prozesse, bevor der Ernstfall eintritt.

CSIRT aufbauen - Computer Security Incident Response Team

01 Vorbereitung

Incident-Response-Plan erstellen und testen. Rollen und Verantwortlichkeiten definieren. Kommunikationswege festlegen - intern und gegenüber BSI, Kunden und Öffentlichkeit.

02 Erkennung & Analyse

SIEM-Systeme, EDR/XDR, Threat Intelligence und Anomalie-Erkennung für die frühzeitige Identifikation von Vorfällen. Klassifikation nach Schweregrad und Eskalation.

03 Eindämmung & Beseitigung

Sofortige Isolation betroffener Systeme, forensische Sicherung von Beweismaterial, Beseitigung der Ursache und Wiederherstellung aus Backups.

04 Nachbereitung & Lessons Learned

Abschlussbericht (spätestens 1 Monat nach Frühwarnung), Root-Cause-Analyse, Anpassung der Sicherheitsmassnahmen und Aktualisierung des Incident-Response-Plans.

Business Continuity & Disaster Recovery

BC-Planung nach BSI 200-4

- Business Impact Analyse (BIA) durchführen
- Kritische Geschäftsprozesse identifizieren
- Recovery Time Objectives (RTO) definieren
- Notfallpläne erstellen und testen
- Regelmäßige BC-Übungen

NIS2-Meldepflichten einhalten

- Meldeprozess vorab definieren und üben
- Vorlagen für Frühmeldung bereithalten
- Kontaktdaten BSI-Meldestelle aktuell halten
- Forensik-Kapazitäten sicherstellen
- Juristische Beratung einbinden

Weiterbildung bei cmt

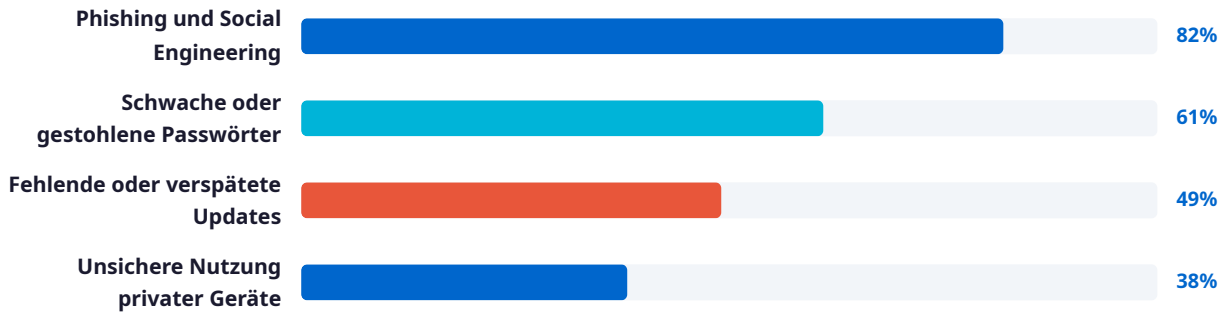
Certified Incident Handler (ECIH v3) - Business Continuity Management (BSI 200-4 & ISO 27001) - SRE Deep Dive: Incident Automation - CHFI v10 - Digitale Forensik Grundkurs

Security Awareness

Der Mensch als stärkste Verteidigungslinie

NIS2 schreibt Cyberhygiene und Schulungen ausdrücklich vor (§30 Abs. 2 Nr. 10 BSIG). Der menschliche Faktor bleibt der Hauptangriffsvektor - Phishing, Social Engineering und Fehlkonfigurationen verursachen die Mehrheit aller erfolgreichen Angriffe.

Die größten Risikofaktoren



Wirksames Schulungskonzept in vier Stufen

A

Awareness für alle Mitarbeitenden

Grundlegende Sensibilisierung: Phishing erkennen, sichere Passwörter, Clean Desk Policy, Meldewege. Regelmäßige Wiederholung und aktuelle Bedrohungsszenarien.

B

Vertiefung für IT-Teams

Technische Schulungen zu Secure Configuration, Hardening, Logging und Monitoring. Hands-on Labs mit realen Angriffsszenarien.

C

Spezialisierung für Security-Teams

Zertifizierungen (CEH, ECIH, CompTIA Security+), Penetration Testing, digitale Forensik, Threat Intelligence und SOC-Betrieb.

D

Führungskräfte-Briefing

NIS2-Compliance, Haftungsfragen, Risikosteuerung und strategische Security-Investitionsentscheidungen. Pflicht nach §38 BSIG.

Passende Schulungen

IT-Security Awareness - Mitarbeitersensibilisierung - NIS2-Richtlinie für Unternehmen - A4Q Security Essentials - Internet Security

KI und Cybersecurity

Künstliche Intelligenz als Waffe und als Schutzschild

KI verändert die Cybersicherheit grundlegend - auf beiden Seiten. Angreifer nutzen Large Language Models für automatisiertes Phishing und Code-Generierung. Verteidiger setzen KI für Anomalie-Erkennung und Echtzeit-Analyse ein. KI-Security-Kompetenz wird deshalb zunehmend wichtiger.

KI-basierte Bedrohungen

Automatisiertes Phishing & Social Engineering

KI-generierte Nachrichten sind kaum noch von echten zu unterscheiden. Deepfakes ergänzen Voice-Phishing und CEO-Fraud. Die Erfolgsquote steigt massiv.

KI-gestützte Malware

Schadsoftware, die sich automatisch an die Zielumgebung anpasst, Sandbox-Erkennung umgeht und polymorphen Code generiert.

Prompt Injection & Data Poisoning

Angreifer verstecken Befehle in E-Mails und Dokumenten, die von LLMs als Instruktionen ausgeführt werden. Vergiftete Trainingsdaten manipulieren KI-Modelle.

Shadow AI

Mitarbeitende nutzen KI-Tools unkontrolliert und laden sensible Unternehmensdaten in öffentliche Modelle hoch - ein Datenschutz- und Compliance-Risiko.

KI für die Verteidigung

Anomalie-Erkennung
KI analysiert Milliarden Datenpunkte in Echtzeit und erkennt Bedrohungen auf Basis von Verhaltensmustern

Security Copilots
KI-Assistenten im SOC beschleunigen Triage, Analyse und Response um den Faktor 10

Threat Intelligence
Automatische Korrelation von Bedrohungsdaten aus Millionen von Quellen

KI-Security-Seminare bei cmt

KI Securitykurs: Schutz vor bösartigen LLMs - LLM Security: Injections erkennen & abwehren - Shadow AI stoppen - Defensive KI - Security Copilots Grundkurs - Malware-Analyse mit KI

Zertifizierungen & Karrierepfade

Die wichtigsten Security-Zertifizierungen im Überblick

NIS2 erhöht den Bedarf an qualifiziertem Security-Personal massiv. Anerkannte Zertifizierungen belegen Kompetenz und schaffen Vertrauen - bei Auditoren, Kunden und Regulierungsbehörden.

Zertifizierung	Fokus	Zielgruppe
BSI IT-Grundschutz-Praktiker	BSI-Standards, Grundschutz-Methodik	ISB, IT-Leiter, Berater
ISO 27001 Security Officer	ISMS aufbauen und betreiben	Security Officers, ISB
ISO 27001 Kompakt	Foundation & Security Officer	Einsteiger, Projektleiter
Certified Ethical Hacker (CEH v13)	Ethical Hacking, Penetration Testing	Pentester, Security Analysts
Certified Incident Handler (ECIH)	Incident Response, Forensik	CSIRT-Mitglieder, SOC
Certified Network Defender (CND)	Netzwerksicherheit, Monitoring	Netzwerkadmins, SOC Tier 1
Certified Penetration Testing Professional	Fortgeschrittene Penetration Tests	Senior Pentester
Certified Threat Intelligence Analyst	Threat Intelligence Lifecycle	Threat Analysts, SOC Tier 2/3
Certified Cloud Security Engineer	Cloud Security Architecture	Cloud Architects, DevSecOps
CKS: Kubernetes Security Specialist	Container- und Kubernetes-Security	DevOps, Platform Engineers

Microsoft Security-Zertifizierungen

SC-100: Cybersecurity Architect - SC-200: Security Operations Analyst - SC-900: Security Fundamentals - SC-401: Information Security - AZ-500: Azure Security

Seminarübersicht

NIS2-Compliance, Management-Systeme & Offensive Security

NIS2-Compliance & Governance

Seminar	Schwerpunkt
NIS2-Richtlinie für Unternehmen	NIS2, Compliance, Haftung
BSI IT-Grundschutz-Praktiker	BSI-Standards, ISMS
BSI IT-Sicherheitsberater	Beratung, Audit
BSI IT-Auditor Training	IT-Revision, Audit
ISO 27001 Security Officer	ISMS, Risikomanagement
ISO 27001 Kompakt (Foundation & Security Officer)	Einstieg ISMS
Business Continuity Management (BSI 200-4 & ISO 27001)	BCM, Notfallplanung
BSI Grundschutz für die Rüstungsindustrie	VS-NfD, Sonderanforderungen
BSI IT-Grundschutz Praxis Training	Hands-on Grundschutz
KI Compliance: Rechtssicherer Einsatz	KI-Regulierung, EU AI Act
Risikomanagement für KI	KI-Risiken, Governance

Offensive Security & Ethical Hacking

Seminar	Schwerpunkt
Certified Ethical Hacker v13 (CEH)	Ethical Hacking, Zertifizierung
Certified Penetration Testing Professional (CPENT)	Fortgeschrittene Pentests
IT-Sicherheit: (Anti-) Hacking für Admins	Angriffstechniken verstehen
Ethical Hacking Essentials (EHE)	Einstieg Ethical Hacking
Web Application Security Kompaktkurs	OWASP, Web-Sicherheit
EC-Council Web Application Hacking (WAHS)	Web App Pentesting

Seminarübersicht

Incident Response, Forensik, Netzwerk- & Cloud-Security

Incident Response & Forensik

Seminar	Schwerpunkt
Certified Incident Handler (ECIH v3)	Incident Response, Zertifizierung
Computer Hacking Forensic Investigator v10 (CHFI)	Digitale Forensik, Zertifizierung
EC-Council Digital Forensics Essentials (DFE)	Einstieg Forensik
Digitale Forensik Grundkurs	Praxis-Forensik
Digitale Forensik: Linux/Unix	Linux-Forensik
Digitale Forensik: Windows	Windows-Forensik
SRE Deep Dive: Incident Automation	Automatisierung, SRE
Certified Threat Intelligence Analyst (CTIA)	Threat Intelligence

Netzwerk-, Cloud- & Infrastruktur-Security

Seminar	Schwerpunkt
Certified Network Defender (CNDv3)	Netzwerksicherheit
Netzwerktechnik Intensivkurs: TCP/IP	Netzwerk-Grundlagen
Certified Cloud Security Engineer (CCSE)	Cloud Security
Cloud Native Security & Governance	Cloud Native, Compliance
CKS: Kubernetes Security Specialist	Container Security
LFS460: Kubernetes Security Fundamentals	K8s Security Basics
LFS482: Zero Trust Security (SPIFFE/SPIRE)	Zero Trust, Service Mesh
LFD441: Security and the Linux Kernel	Kernel Security
Linux Security Intensivkurs	Linux Hardening
pfSense Grundkurs: Firewall, VPN, Routing	Firewall, Open Source
IoT-Netzwerke & Edge Security	IoT, Edge Computing

Seminarübersicht

Microsoft Security, Hersteller-Trainings, KI-Security & Entwicklung

Microsoft Security

Seminar	Schwerpunkt
SC-100: Microsoft Cybersecurity Architect	Security Architecture
SC-200: Security Operations Analyst	SOC, Sentinel, Defender
SC-900: Security Fundamentals	Einstieg MS Security
SC-401: Information Security Administrator	Information Protection
AZ-500: Azure Security Technologies	Azure Security
SC-5001: SIEM mit Microsoft Sentinel	SIEM, Log Analytics
SC-5004: Microsoft Defender XDR	XDR, Threat Protection
SC-5006: Microsoft Copilot für Sicherheit	KI im SOC
Microsoft Defender for Identity	Identity Threat Detection
Microsoft 365 Security & Compliance	M365 Absicherung

KI-Security & Secure Development

Seminar	Schwerpunkt
KI Securitykurs: Schutz vor bösartigen LLMs	LLM-Bedrohungen
LLM Security: Injections erkennen & abwehren	Prompt Injection
Shadow AI stoppen	KI-Governance
Defensive KI: IT-Infrastruktur absichern	KI-basierte Verteidigung
KI-Sicherheit in der Cloud Grundkurs	Cloud KI, Compliance
Malware-Analyse mit KI Grundkurs	KI-gestützte Analyse
Security Copilots Grundkurs	KI im SOC
Sichere Anwendungen mit Node.js	Secure Coding
Sichere Anwendungen mit C und C++	Secure Coding
Solidity Bootcamp: Sichere Smart Contracts	Blockchain Security

Hersteller-Trainings & Spezialkurse

Check Point, Fortinet, Trellix, AWS, Oracle und mehr

Ergänzend zu herstellerunabhängigen Seminaren bietet cmt zertifizierte Trainings führender Security-Hersteller.

Check Point R82

- Einführung in Check Point R82
- Check Point R82 Betrieb
- Sicherheitsadministration
- Sicherheitsexperte
- ClusterXL
- Remote Access VPN
- IPS (Intrusion Prevention)

Trellix / McAfee

- Trellix ENS 10.7
- Trellix ATP
- Trellix HX
- Trellix ATD
- Trellix FIRE-TH (Threat Hunting)
- Trellix FIRE-IR (Incident Response)

Fortinet

- Fortinet Azure Cloud Security
- Fortinet AWS Cloud Security
- Fortinet SD-WAN
- Fortinet Advanced Analytics

AWS Security

- Security Engineering on AWS
- AWS Security Governance at Scale
- AWS Security Best Practices
- AWS Security Essentials

Weitere Spezialkurse

- Oracle Datenbank Security
- EC-Council ICS/SCADA Cybersecurity
- EC-Council CCT
- Certified Security Specialist (ECSS)

Fahrplan zur NIS2-Compliance

In sechs Schritten zur gesetzeskonformen Cybersicherheit

Das NIS2UmsuCG gilt seit Dezember 2025 ohne Übergangsfrist. Wenn dein Unternehmen noch nicht gesetzeskonform ist, ist jetzt der Zeitpunkt zu handeln. Diese NIS2 Checkliste zeigt die wichtigsten Schritte.

1 Betroffenheit prüfen

Sofort

Fällst du unter die 18 regulierten Sektoren? Sind Schwellenwerte (50+ Mitarbeiter oder 10+ Mio. EUR Umsatz) erreicht? Bist du besonders wichtige oder wichtige Einrichtung? Nutze den BSI-Betroffenheitscheck.

2 BSI-Registrierung

Frist: 6. März 2026 (bereits abgelaufen - späte Registrierung möglich)

Registrierung beim BSI über das zentrale Meldeportal. Benennung einer verantwortlichen Person für die Kommunikation mit dem BSI. Dokumentation der Kontaktstelle.

3 Gap-Analyse & Risikobewertung

Monate 1-2

Ist-Zustand der IT-Sicherheit erfassen. Abgleich mit den zehn Mindestmassnahmen nach §30 BSIG. Risikobewertung auf Basis von BSI IT-Grundschutz oder ISO 27001.

4 Maßnahmen umsetzen

Monate 2-6

Risikomanagement einrichten, Meldeprozesse aufbauen, Supply-Chain-Anforderungen in Verträge aufnehmen, technische Maßnahmen implementieren (MFA, Verschlüsselung, Segmentierung, Backup-Konzept).

5 Personal qualifizieren

Fortlaufend

Geschäftsleitung schulen (§38 BSIG - Pflicht!). Security-Awareness für alle Mitarbeitenden. Fachkräfte mit Zertifizierungen (BSI Grundschutz-Praktiker, ISO 27001, CEH) qualifizieren.

6 Kontinuierliche Verbesserung

Dauerhaft

Regelmäßige NIS2 Audits und Penetrationstests. Incident-Response- Übungen. Anpassung an neue Bedrohungen und BSI-Anforderungen. Dokumentation aller Maßnahmen für Nachweispflichten.

Dein Qualifizierungsplan

Vier Lernpfade für unterschiedliche Rollen

Ob Geschäftsführung, Security Officer, IT-Administrator oder Entwickler - jede Rolle braucht andere Kompetenzen. Wir empfehlen vier Lernpfade, die sich am konkreten Bedarf orientieren.

A Geschäftsführung & Management

NIS2-Haftung verstehen und Compliance sicherstellen

NIS2-Richtlinie für Unternehmen → ISO 27001 Kompakt → Risikomanagement für KI

Ergebnis: Du verstehst deine Pflichten nach NIS2, kannst Risiken bewerten und Security-Investitionen steuern.

B Security Officer & ISMS-Verantwortliche

ISMS aufbauen und NIS2-konform betreiben

BSI Grundschutz-Praktiker → ISO 27001 Security Officer → Business Continuity Management → BSI IT-Auditor

Ergebnis: Du bist qualifiziert, ein ISMS nach BSI Grundschutz und ISO 27001 aufzubauen, zu betreiben und zu auditieren.

C SOC-Analyst & Incident Responder

Angriffe erkennen, analysieren und abwehren

Certified Network Defender → SC-200: Security Operations → Certified Incident Handler → Threat Intelligence Analyst

Ergebnis: Du kannst ein SOC betreiben, Sicherheitsvorfälle erkennen und die NIS2-Meldepflichten einhalten.

D Pentester & Offensive Security

Schwachstellen finden, bevor es Angreifer tun

Ethical Hacking Essentials → CEH v13 → CPENT → Web Application Security

Ergebnis: Du kannst professionelle Penetrationstests durchführen und Schwachstellen in Netzwerken und Anwendungen finden.

Warum cmt?

Dein Partner für IT-Sicherheit und Compliance

2.100+
Seminare im Programm

Von Security-Grundlagen bis zur Spezialzertifizierung - eines der größten IT-Schulungsportfolios in Deutschland.

25+
Jahre Erfahrung

Seit über 25 Jahren Weiterbildungspartner für Unternehmen, Behörden und öffentliche Auftraggeber.

60+
Security-Seminare

Breites Security-Portfolio von NIS2 über BSI Grundschutz und ISO 27001 bis zu Ethical Hacking und KI-Security.

100%
Durchführungsgarantie

Alle Termine finden garantiert statt. Kleine Gruppen für maximalen Lernerfolg.

Flexible Formate für jeden Bedarf

Offene Seminare
Feste Termine mit Durchführungsgarantie. Kleine Gruppen, intensiver Austausch.

Inhouse-Training
Maßgeschneidert auf dein Unternehmen. Inhalte, Termine und Ort nach deinen Wünschen.

Online-Live
Interaktive Remote-Schulungen mit voller Trainer-Interaktion. Ortsunabhängig, ohne Reisekosten.

Dein Ansprechpartner

Yves Hoppe - IT & Open Source
Telefon: 0800 71 20 000 - E-Mail: yves.hoppe@cmt.de
Individuelle Beratung zu Security-Schulungsprogrammen und NIS2-Qualifizierung für dein Team.

NIS2-Compliance planen?
Sprich uns an.

Yves Hoppe

IT & Open Source

0800 71 20 000 · yves.hoppe@cmt.de

cmt GmbH · Telefon: 0800 71 20 000 · info@cmt.de

www.cmt.de