

So gelingt die Umsetzung und der Nachweis von NIS2-Compliance

Die novellierte europäische Richtlinie zur Netz- und Informationssicherheit (NIS2) verpflichtet die EU-Mitgliedsstaaten, gesetzliche Regeln zu definieren, damit wesentliche und wichtige Einrichtungen in ihrem Land nicht durch Cybervorfälle gestört werden. In Deutschland erfolgt die Umsetzung über das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG). Das Gesetz gilt seit dem 06.12.2025 unmittelbar – eine allgemeine Übergangsfrist ist nicht vorgesehen. Die Richtlinie und das Gesetz definieren zehn Kategorien für das CyberRisikomanagement sowie strenge Verpflichtungen (u. a. Registrierung und Meldung) bei Sicherheitsvorfällen. Betroffene Unternehmen und Einrichtungen müssen entsprechende Maßnahmen und Technologien einführen, deren Wirksamkeit dokumentieren und die Einhaltung der gesetzlichen Vorgaben nachweisen. Die Geschäftsführung wird ausdrücklich verantwortlich für die Umsetzung und Überwachung und kann bei Pflichtverstößen haftungsrechtlich in Anspruch genommen werden. Bußgelder und Sanktionen: Je nach Einordnung und Verstoß drohen empfindliche Bußgelder – bei „besonders wichtigen“ Einrichtungen grundsätzlich bis 10 Mio. € (bzw. bei sehr großen Unternehmen bis 2 % des weltweiten Jahresumsatzes) und bei „wichtigen“ Einrichtungen bis 7 Mio. € (bzw. bis 1,4 % des weltweiten Jahresumsatzes). Sanktionen können ab Inkrafttreten u. a. auch bei Verstößen gegen Registrierungs- oder Meldepflichten greifen.

WER IST BETROFFEN?
Betroffen sind in der Regel mittlere und große Unternehmen (typischerweise ab 50 Mitarbeitenden und/oder > 10 Mio. € Jahresumsatz/Jahresbilanzsumme) aus bestimmten Sektoren; NIS2 unterscheidet dabei insbesondere zwischen besonders wichtigen und wichtigen Einrichtungen. Ungeachtet der Einstufung sind Anbieter öffentlicher Kommunikationsnetze und -dienste sowie Vertrauensdiensteanbieter und Namensregister der obersten Domäne (inkl. DNS-Diensteanbieter) stets erfasst. Neben vielen Unternehmen fallen auch zahlreiche Einrichtungen der Bundesverwaltung unter NIS2 und müssen verbindliche IT-Sicherheitsanforderungen erfüllen.

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 im Detail vor. Hierfür wird auf Branchenstandards verwiesen, wie etwa B3S. Es gibt generell eine große Überlappung mit der ISO/IEC 27001. Dieses Poster gibt einen Überblick über die grundlegenden Sicherheitsziele, die hinter den Kategorien und Verpflichtungen stehen. Es zeigt, wo Enginsight seine Kund:innen bei der Umsetzung und kontinuierlichen Einhaltung von NIS2 unterstützt.

NIS2-ANFORDERUNGEN	GRUNDLEGENDE SICHERHEITZIELE, DIE SICH AUS DEN ANFORDERUNGEN ABLEITEN LASSEN*						
Risikoanalyse und Sicherheit für Informationssysteme	Verfahren zur regelmäßigen Risikoanalyse und Schwachstellenbewertung einführen	Asset Discovery, Beschreibung und Softwareinventarisierung	Bestehende Schwachstellen und Sicherheitslücken identifizieren	Regelmäßige Penetrations-test der eigenen Infrastruktur und bisher ergriffen Sicherheitsmaßnahmen	ISMS nach ISO 27001, TISAX, etc. umsetzen		
Bewältigung von Sicherheitsvorfällen	End-to-end Anomalie- und Angriffserkennung umsetzen. Protokollierung aller Ereignisse und Ableitung automatischer Reaktionen.**	Angriffe, böswillige, fehlerhafte oder andere Aktivitäten im Netz, die sich auf kritische Dienste auswirken könnten, frühzeitig zu erkennen	Schnelle Reaktion auf Cybervorfälle sicherstellen (Incident Response) ermöglichen	Schnelle forensische Analyse und Abschätzung der Auswirkungen nach Vorfall sicherstellen	Schadsoftware und Angreifende an Netzwerkgrenzen bestmöglich abwehren	Managed Detection and Response Services	
Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management	Störung der Prozesse durch Sicherheitsmaßnahmen vermeiden	Business-Continuity-Plan erstellen	Mehrstufiges Backup-Management etablieren	Schnelle Notfallwiederher-stellung ermöglichen	Professionelle Krisenbewältigung und -kommunikation einrichten		
Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit	Die technische Kommunik-ation der Schnittstellen überwachen, auswerten und ggf. automatisierte Maßnahmen etablieren.	Least Privilege Access für Lieferanten etablieren	Sicheren Lieferanten-Zugang zum Netzwerk gewährleisten (z. B. sichere Passwörter, VPN)				
Sicherheit in der Entwicklung, Beschaffung und Wartung; Management von Schwachstellen	Regelmäßige Penetrationstest eigener Software und Infrastruktur	Dauerhaftes Monitoring von Schwachstellen	Effektive und sichere Behandlung und von Schwachstellen sicherstellen				
Bewertung der Effektivität von Cybersicherheit und Risikomanagement	Die Wirksamkeit des Cybersicherheit-Systems fortlaufend überprüfen und verbessern mit Hilfe von automatisierten Pentests	Cybersicherheitslage und Risikoeexposition regelmäßig neu bewerten					
Schulungen Cybersicherheit und Cyberhygiene	Defense-in-Depth-Architektur aufbauen, um Versagen der Perimetersicherung frühzeitig zu erkennen und interne Netzwerkkommunikation zu überwachen	Gefährdete Assets überwachen und abschirmen, bei denen Patches/Aktualisierungen nicht möglich sind	Ausbreitung von Angriffen eindämmen (z. B. durch Netzsegmentierung)	Digitale Ressourcen in Bezug auf Firmware, Betriebssystem usw. auf dem neusten Stand halten	Starke Passwortrichtlinien festlegen und umsetzen	Regelmäßige Cybersicherheitsschulungen für das Personal umsetzen	
Kryptografie und Verschlüsselung	Überwachung und Überprüfung verschlüsselter Verbindungen nach aktuellem Stand der Technik. Abgleich TLS nach TR-03116-4 Checkliste des BSI	Einrichtung und Sicherstellung einer durchgehenden verschlüsselten Kommunikation im internen Netz					
Personalsicherheit, Zugriffs-kontrolle und Anlagen-management	Zugriffe auf kritische Dateien und Verzeichnisse unternehmensweit überwachen	Sicherheitsüberprüfungen und -sensibilisierung in das Einstellungs- und Vertrags-vergabeverfahren integrieren	Unbefugten physischen Zugriff auf Assets verhindern				
Multi-Faktor Authentisierung und kontinuierliche Authentisierung	Unbefugten Zugriff auf digitale Assets verhindern. Überwachung aller Logins und Loginversuche	Personalisierte Multi-Faktor-Authentifizierung sicherstellen	Sichere digitale Kommuni-kation gewährleisten				
Sichere Kommunikation (Sprach, Video- und Text)	Überwachung sämtlicher Kommunikationssysteme und der verschlüsselten Verbindungen	Innerhalb von 24 Stunden nach einem Vorfall Frühwarnung an CSIRT*** übermitteln	Innerhalb von 72 Stunden erste Bewertung an CSIRT übermitteln (inkl. Aussagen zu Schweregrad, Auswirkungen, Quelle)	Auf Anfrage des CSIRT Aktualisierungen zum Status des Vorfallsmanagements bereitstellen	Innerhalb eines Monats detaillierten Berichts an das CSIRT übermitteln (inkl. Infor-mationen zu Schweregrad, interne und grenzüberschrei-tende Auswirkungen, Ursache, Abhilfemaßnahmen)		

* Die aufgeführten Ziele sind in der NIS2 nicht explizit definiert, sondern spiegeln allgemeine grundlegende Sicherheitsziele wider, wie sie in internationalen Normen wie der IEC 62443 empfohlen werden.
** Verpflichtend für kritische Infrastrukturen
*** CSIRT (Computer security incident response team) = behördliches Computer-Notfallteam

LEGENDE

Direkte Umsetzung durch Enginsight

Lösung über Enginsight Trusted-Partner verfügbar

Pulsar Agent

Watchdog

IDS

FIM

SIEM

SIEM Eventstreams

Hacktor

Observer

IPS

Mikrosegmentierung

SIEM Workflows

CVE-Cockpit

Alle Angaben ohne Gewähr.
Änderungen vorbehalten.

Enginsight GmbH
Leutragraben 1
07743 Jena