

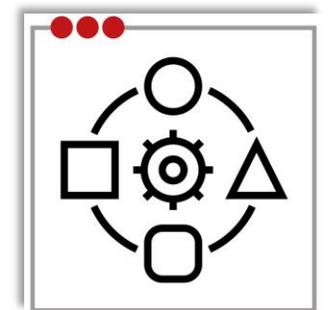
NIS 2 RICHTLINIE

NIS 2 – WAS IST DAS GENAU?

AUS „NICE TO HAVE“ WIRD OBLIGATORISCH



- The **Network and Information Security (NIS) Directive**
 - Richtlinie des EU-Parlaments über Maßnahmen zur Erhöhung der Cybersicherheit in der Europäischen Union
 - NIS 2 ergänzt und aktualisiert die erste Richtlinie von 2016
- Alle EU-Mitgliedsstaaten müssen die NIS2-Richtlinie bis Oktober 2024 in nationale Gesetze umwandeln und anwenden
- Referentenentwurf für die Umsetzung von NIS2 (Juli 2023)
 - Enthält spezifische Maßnahmen, die grundsätzlich umzusetzen sind (Mindestvorgaben)
- Kreis der betroffenen Unternehmen wird in NIS2 ausgeweitet
Einteilung der Unternehmen in
 - "besonders wichtige Einrichtungen" und "wichtige Einrichtungen"
 - Sektorübergreifend
 - Einführung neuer Schwellenwerte – Mitarbeitende, Umsatz, Bilanz



NIS 2 RICHTLINIE – SIND SIE BETROFFEN?

JA, WENN FOLGENDE FAKTOREN ZUTREFFEN



Geltungsbereich gemäß NIS2:

- **Große Unternehmen:**
 - >250 Mitarbeitende oder
 - ≥ 50 Mio. € Umsatz
 - und > 43 Mio. € Jahresbilanzsumme
- **Mittlere Unternehmen:**
 - ≥ 50 Mitarbeitende oder
 - ≥ 10 Mio. € Umsatz
 - und ≥ 10 Mio. € Jahresbilanzsumme

Wesentliche Sektoren

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastruktur
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten
- Öffentliche Verwaltung
- Weltraum

Wichtige Sektoren

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Chemische Stoffe
- Lebensmittel
- Verarbeitendes Gewerbe/Herstellung von Waren
- Anbieter digitaler Dienste
- Forschungseinrichtungen

NIS 2 RICHTLINIE

LERNEN SIE IHRE HAFTUNGSRISIKEN KENNEN



Besonderheiten für wesentliche Einrichtungen

- Erweiterte Aufsichts- und Durchsetzungsmaßnahmen der zuständigen Behörden
- Zusätzliche Pflicht zur Registrierung für Dienstleister von Cloudangeboten, Rechenzentrums-Dienstleistern und Telekommunikations-Dienstleistern
- Aktive Kontrolle durch den Gesetzgeber

Besonderheiten für wichtige Einrichtungen

- Reaktive Kontrolle durch den Gesetzgeber

Sanktionen / Bußgeldrahmen

- 10 Mio. EUR bzw. 2% Jahresumsatzes für wesentliche Einrichtungen
- 7 Mio. EUR bzw. 1,4% Jahresumsatzes für wichtige Einrichtungen
- Erweiterter Bußgeldrahmen

Personenbezogene Haftung

- Die Geschäftsführung / Leitungsebene ist persönlich haftbar

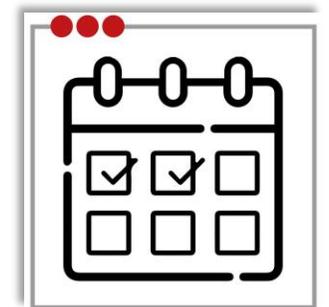


NIS 2 – WAS MUSS GETAN WERDEN?

VON IHNEN MUSS FOLGENDES UMGESETZT WERDEN:

- Generell:
 - Registrierung beim BSI
 - Umsetzen der Mindestvorgaben
 - Prüfen, ob weitere Maßnahmen ergriffen werden müssen
 - Mittels eines gefahrenübergreifenden Ansatzes
 - Auf Basis der Risikobewertung
- Organisatorisch:
 - Einführen eines Risikomanagements
 - Aufbauen eines Information Security Managements (ISM)
 - Einführen eines Business Continuity Managements (BCM)
- Operative/technische Pflichten
 - Ausarbeiten von Konzepten und Verfahren für den Einsatz von Kryptografie
 - Einsetzen von Multi-Faktor-Authentifizierung (MFA)
 - Umsetzen von Maßnahmen der „Cyberhygiene“
- Meldepflicht: Meldung von Sicherheitsvorfällen an das BSI*
 - Innerhalb von 24h: Frühwarnung / etwaige Verdachtsmeldung
 - Innerhalb von 72h: Meldung / erste Bewertung
 - Innerhalb von einem Monat: Abschlussbericht inkl. Abhilfemaßnahmen

*Bundesamt für Sicherheit in der Informationstechnik



NIS 2 – WAS MUSS GETAN WERDEN?

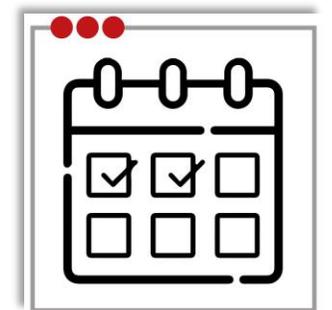
ACHTUNG! NIS 2 BEDEUTET AUCH:



Fallen Sie unter NIS2 müssen Sie die Sicherheit innerhalb von Lieferketten gewährleisten

- Risiken durch direkte Lieferanten und Diensteanbieter müssen berücksichtigt werden
 - Koordinierte Risikobewertung kritischer Lieferketten

- Lieferanten und Diensteanbieter sollten zur Informationssicherheit verpflichtet werden
 - Sicherstellung der Einhaltung durch regelmäßige Überprüfung/Audit



WIR BEGLEITEN SIE AUF DEM WEG ZUR UMSETZUNG

UNSERE METHODIK - FÜR IHRE SICHERHEIT



WIE GEHT ES WEITER

IN UNSEREM WORKSHOP ERARBEITEN WIR MIT IHNEN:



- Identifikation einzuhaltender Vorgaben der bisher bekannten Anforderungen von NIS2 und des NIS2UmsuCG
 - Aufnahme der aktuellen IST-Situation in Bezug auf die NIS2 und das NIS2UmsuCG
 - Erstellen einer GAP-Analyse
 - Empfehlung von geeigneten, priorisierten Maßnahmen
 - Abschlusspräsentation
-
- Kosten:
4.900 € zzgl. 19% MwSt
zzgl. Reisekosten



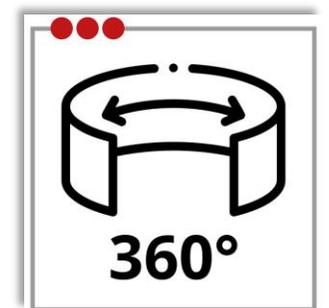
WAS HABEN SIE KONKRET DAVON?

IHRE VORTEILE AUF EINEN BLICK



- Erste Schritte für die Umsetzung von NIS 2
- Herstellen einer Dokumentation aller vorhandenen Tools und Methoden im Bereich Datenschutz und IT-Security
 - Für Compliance Richtlinien
 - KRITIS
 - Nachweis für Cyberversicherungen
- Erstellen von spezifischen Definitionen und einer Dokumentation des Security und Datenschutz „SOLL“
 - Aufdecken von Sicherheitslücken und Schwachstellen
 - Herstellen von Nachweisen für Kunden und Zulieferer
 - Verbessern der Sicherheit von Lieferketten
 - Erreichen höherer Effizienz und Produktivität

→ Erreichen eines besseren Sicherheitsniveaus im Unternehmen und damit ein geringeres oder reduziertes Risiko von Cyberangriffen.



WAS KÖNNEN WIR ERGÄNZED FÜR SIE TUN?



SO ERREICHEN SIE UNS



DV-KONTOR GmbH
Gustav-Ricker-Str. 62
39120 Magdeburg
Deutschland

- Telefon: 03916269770
- Fax: 03916269901
- E-Mail: mail@dv-kontor.com
- Web: www.dv-kontor.com