Unternehmen müssen jetzt handeln!

NIS-2

Die EU-Richtlinie wird verbindlich

Das bedeutet:

Die neue Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) definiert EU-weite verbindliche Mindeststandards für technische und organisatorische Maßnahmen in Unternehmen.

Die Richtlinie tritt mit Beschluss des NIS2-Umsetzungsgesetzes in Kraft und zielt darauf ab, den dramatisch zunehmenden Cyber-Bedrohungen entgegenzuwirken und Lieferketten zu schützen.

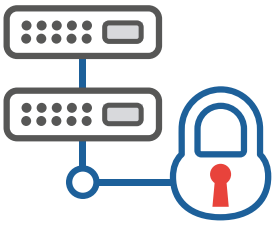
Betroffene Unternehmen sind verpflichtet, die gesetzlichen Vorgaben zur Cybersicherheit umzusetzen. Bei Nichteinhaltung oder Verstößen drohen erhebliche Bußgelder.

Betroffen sind Unternehmen die mehr als 50 Mitarbeiter oder mehr als 10 Millionen Umsatz haben und in den unten aufgeführten Branchen und Sektoren tätig sind.

Betroffene Branchen und Sektoren

SEKTOREN HOHER KRITIKALITÄT

- Energie
- Transport und Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasserversorgung
- Abwasserbeseitigung
- Digitale Infrastruktur
- IKT-Dienstverwaltung (B2B)
- Öffentliche Verwaltung
- Weltraum



NIS-2

EU-RICHTLINIE ZU NETZWERK- UND INFORMATIONSSICHERHEIT

SONSTIGE KRITISCHE SEKTOREN

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/ Herstellung von Waren
- Anbieter digitaler Dienste
- Forschung

Was ist zu tun?

EINFÜHRUNG EINES SICHERHEITSSYSTEMS

- Entwicklung eines Sicherheitskonzepts zur Identifizierung, Analyse und Beseitigung von Bedrohungen.
- Festlegung von Sicherheitsrichtlinien und -standards.
- Regelmäßige Risikobewertungen zur Identifizierung von Bedrohungen und Schwachstellen.
- Implementierung technischer und organisatorischer Maßnahmen zur Risikominderung.
- Einrichtung eines effektiven Incident-Management Prozesses.
- Entwicklung eines Business-Continuity-Managements zur Sicherstellung des Betriebs bei Vorfällen.
- Identifizierung von Schlüsselprozessen und Implementierung von Wiederherstellungsmaßnahmen.
- Einrichtung eines Meldewesens für Sicherheitsvorfälle.
- Schulung der Mitarbeiter zu Meldungen von Sicherheitsvorfällen.
- Überprüfung der Sicherheitspraktiken von Lieferanten und Dienstleistern.
- Implementierung von Sicherheitsanforderungen zur Minimierung von Risiken.
- Kontinuierliche Überwachung der Systeme zur frühzeitigen Erkennung von Sicherheitsvorfällen.

REGISTRIERUNG ÜBER BSI

Betroffene Unternehmen müssen sich innerhalb von drei Monaten nach Inkrafttreten des nationalen Umsetzungsgesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren.

BEWERTUNG DER EIGENEN CYBERSICHERHEITSKAPAZITÄTEN

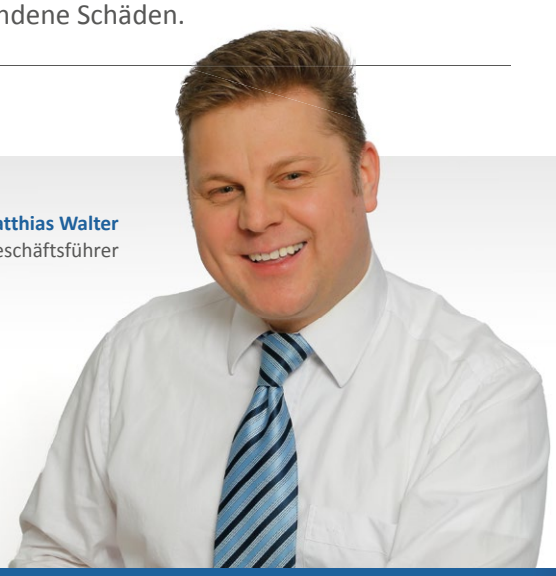
Sie müssen darlegen, wie Ihre Cybersicherheit organisiert ist und wo weitere technologische Verbesserungen geplant sind. Beachten Sie, dass Behörden Vor-Ort-Kontrollen und anlassbezogene Prüfungen durchführen können.

MELDEPFLICHT BEACHTEN

Im Falle eines Sicherheitsvorfalls muss dieser nicht nur behoben, sondern auch innerhalb von 24 Stunden nach seiner Entdeckung den zuständigen Behörden gemeldet werden. Ein Abschlussbericht ist spätestens nach einem Monat einzureichen.

SANKTIONEN UND HAFTUNG VERMEIDEN

Verstöße gegen die gesetzlichen Vorgaben können Bußgelder von bis zu 2 % des Jahresumsatzes nach sich ziehen. Bei Nichtumsetzung haften Leitungsorgane möglicherweise mit ihrem privaten Vermögen für entstandene Schäden.



Matthias Walter
Geschäftsführer

Kontaktieren Sie uns noch heute!

Unsere maßgeschneiderten und praxisorientierten Konzepte sorgen dafür, dass Sie regulatorische Vorgaben und Normen langfristig einhalten.



IHR STARKER IT-PARTNER

tec4net GmbH | Lohenstraße 13 | 82166 Gräfelfing
T +49 89 54 04 36 30 | F +49 89 54 04 36 31 | info@tec4net.com | **www.tec4net.com**