WWW.SOLBYSEC.AT

SOLBYSEC
CYBER SECURITY ANALYTICS

INFO@SOLBYSEC.AT

NIS-2-Richtlinie: So gelingt die Umsetzung.

Die NIS 2 Richtlinie der Europäischen Union hat das Ziel, ein hohes gemeinsames Cybersicherheitsniveau zu schaffen. Angesichts der zunehmenden Digitalisierung der Geschäftsbeziehungen und der Vielfalt an digitalen Gefährdungen werden die Regelungen nun auf einen größeren Teil der Wirtschaft ausgeweitet: in Österreich sind um die 15.000 Betriebe von den Neuerungen betroffen.

Welche Betriebe betroffen sind und welche Maßnahmen gesetzt werden müssen erfahren Sie in den folgenden Absätzen.

Wer ist betroffen?

Unternehmen mit einem Jahresumsatz von:
10 - 50 Mio €

Unternehmen mit
50 - 249 Mitarbeiter*innen

Tätigkeit in Sektoren mit hoher Kritikalität:

Energie, Verkehr, Bank- und Finanzwesen. Gesundheitswesen, Wasserversorgung, Digitale Infrastruktur, ITK-Dienste, Öffentliche Verwaltung, Weltraum

Tätigkeit in sonstigen kritischen Sektoren:

Post- und Kurierdienste, Abfallwirtschaft, Chemie, Ernährung, Herstellung von Waren, Digitale Dienste, Forschung

Check

Sie sind sich unsicher, ob Ihr Unternehmen den Reglungen der NIS2 unterliegt?
Dann machen Sie den Check unter: **www.ratgeber.wko.at/nis2/**

Welche Anforderungen müssen erfüllt werden?

Diverse Maßnahmen im Rahmen der NIS2 sollen das **Risiko- und Vorfallmanagement** stärken, die **Geschäftskontinuität** und Stabilität der **Lieferkette** sichern, sowie das **Reporting** anhand eines schlüssigen Meldeverfahren beschleunigen. Unternehmen sind dazu verpflichtet, den folgenden Anforderungen* nachzukommen:

* 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

Risikoanalyse und Sicherheit für Informationssysteme

- Verfahren zur regelmäßigen Risikoanalyse und Schwachstellenbewertung einführen
- Asset Discovery, Beschreibung und Softwareinventarisierung
- Bestehende Schwachstellen und Sicherheitslücken identifizieren
- Regelmäßige Penetrationstest der eigenen Infrastruktur und bisher ergriffen Sicherheitsmaßnahmen
- ISMS nach ISO 27001, TISAX, etc. 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

Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management

- Störung der Prozesse durch Sicherheitsmaßnahmen vermeiden
- Business-Continuity-Plan erstellen
- Mehrstufiges Backup-Management etablieren
- Schnelle Notfallwiederherstellung ermöglichen
- Professionelle Krisenbewältigung und -kommunikation einrichten

Bewertung der Effektivität von Cybersicherheit und Risikomanagement

- Die Wirksamkeit des Cybersicherheit-Systems fortlaufend überprüfen und verbessern mit Hilfe von automatisierten Pentests
- Cybersicherheitslage und Risikoexposition regelmäßig neu bewerten

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

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

Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit

- Die technische Kommunikation 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)

Multi-Faktor Authentisierung und kontinuierliche Authentisierung

- Unbefugten Zugriff auf digitale Assets verhindern. Überwachung aller Logins und Loginversuche
- Personalisierte Multi-Faktor-Authentifizierung sicherstellen
- Sichere digitale Kommunikation gewährleisten

Schulungen Cybersicherheit und Cyberhygiene

- Defense-in-Depth-Architektur aufbauen, um Versagen der Perimetersicherung frühzeitig zu erkennen und interne Netzwerk Kommunikation umfang 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

Personalsicherheit, Zugriffskontrolle und Anlagenmanagement

- Zugriffe auf kritische Dateien und Verzeichnisse Unternehmensweit überwachen.
- Sicherheitsüberprüfungen und -sensibilisierung in das Einstellungs- und Vertragsvergabeverfahren integrieren
- Unbefugten physischen Zugriff auf Assets verhindern

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. Informationen zu Schweregrad, interne und grenzüberschreitende Auswirkungen, Ursache, Abhilfemaßnahmen)