Autoren:

Aida Stelter, Expertin für innere & äußere Sicherheit
Detecon International GmbH I Aida.Stelter@detecon.com

Stefan Schult, Partner für innere & äußere Sicherheit
Detecon International GmbH I Stefan.Schult@detecon.com

Eva Ziegler, Referentin Cyber/IT
BDSV e.V. I E.Ziegler@bdsv.eu

Annabel Nerlich, Referentin Mittelstand
BDSV e.V. I A.Nerlich@bdsv.eu

BDSV
Bundesverband der Deutschen
Sicherheits- und Verteidigungsindustrie e.V.

NIS-2 Richtlinie
(Network and Information Security)

DETECON
Think. *Do.* Transform.

DETECON

Member of

NIS-2 Richtlinie

Die NIS-2-Richtlinie („Network and Information Security (NIS) Directive“) ist eine wichtige Initiative zur Stärkung der Sicherheit und Integrität von Netzwerken und Informationssystemen in der Europäischen Union. NIS-2 wurde am 27. Dezember 2022 im Amtsblatt L333 der Europäischen Union veröffentlicht und ist am 16.01.2023 in Kraft getreten. Die EU-Mitgliedsstaaten müssen die Richtlinie bis Oktober 2024 in ein nationales Recht überführen und seit Juli 2023 existiert in Deutschland ein Referentenentwurf zur Umsetzung des Bundesministeriums: NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2UmsuCG).*

Die NIS-2 Richtlinie baut auf der festgelegten NIS-Richtlinie aus dem Jahr 2016 auf und definiert neue Anforderungen für die Cybersicherheit kritischer Infrastrukturen (KRITIS) in der EU. Die Richtlinie ist eine wichtige Komponente der europäischen Cybersecurity-Strategie, welche das Ziel hat, kritische Infrastrukturen vor Cyberbedrohungen besser zu schützen und für ein hohes, EU-weites Sicherheitsniveau zu sorgen.

Es wurden zahlreiche neue Maßnahmen definiert, wie z.B. der Aufbau nationaler Computer-Emergency-Response-Teams (spezialisierte Teams zur Erkennung, Analyse und Reaktion auf Cyberbedrohungen und Sicherheitsvorfälle), die Erstellung eines koordinierten Incident-Response-Plans (strukturierter Ansatz zur Bewältigung von Sicherheitsvorfällen) oder die Verbesserung der Zusammenarbeit privater und öffentlicher Einrichtungen.

Die NIS-2-Richtlinie enthält strengere Anforderungen für öffentliche und private Einrichtungen in 18 kritischen Sektoren mit mehr als 50 Beschäftigten oder mindestens 10 Mio. € Jahresumsatz. Zu den 11 hochkritischen Sektoren mit hoher Kritikalität zählen: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten, öffentliche Verwaltung und Weltraum. Darüber hinaus gibt es 7 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 und Forschung.

Unternehmen, die keine der Voraussetzungen erfüllen, können auch durch Lieferanten und weitere Dienstleister betroffen werden, wenn eine Abhängigkeit durch einen betroffenen Partner besteht. Hierbei ist zu beachten, dass jedes Unternehmen in der Eigenverantwortung steht selbst herauszufinden, ob die NIS-2 Richtlinie für das eigene Unternehmen gilt und wenn dies der Fall ist, muss das Unternehmen sich selbst identifizieren und registrieren.

Die betroffenen Unternehmen und Organisationen müssen sich mit den Themen wie Cyber-Risikomanagement, Kontrolle, Überwachung und Umgang mit Zwischenfällen und Geschäftskontinuität befassen.

*Quelle: Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022

Die Erkennung von erheblichen Sicherheitsvorfällen muss dem BSI innerhalb der festgelegten Fristen unverzüglich gemeldet werden:

1. **Sofortige Meldung:** Für schwerwiegende Sicherheitsvorfälle, die einen erheblichen Einfluss auf den Betrieb von wesentlichen Diensten oder digitalen Diensten haben, ist eine sofortige Meldung innerhalb 24 Stunden erforderlich. Dies ist ins-besondere der Fall, wenn die Sicherheit des Netz- oder Informationssystems unmittelbar gefährdet ist.
2. **Kurzfristige Meldung:** Eine Frühwarnung muss binnen 24 Stunden nach der Feststellung eines Sicherheitsvorfalls übermittelt werden, falls Anzeichen für eine mutmaßlich böswillige oder rechtswidrige Ursache vorliegen oder der Vorfall potenzielle grenzüberschreitende Auswirkungen hat.
3. **Langfristige Meldung:** Innerhalb von 72 Stunden nach der Kenntnisnahme des signifikanten Sicherheitsvorfalls muss eine Meldung darüber erfolgen. Diese Meldung kann, die in der Frühwarnung genannten Informationen aktualisieren und eine erste Bewertung des Vorfalls liefern, einschließlich seiner Schwere und Auswirkungen. Zusätzlich können mögliche Kompromittierungsindikatoren genannt werden.
4. **Fortschritts-/Abschlussbericht ein Monat nach Meldung:** Innerhalb von maximal einem Monat nach der Übermittlung der Sicherheitsvorfallmeldung muss ein Abschlussbericht vorliegen. Dieser Bericht sollte eine ausführliche Beschreibung des Sicherheitsvorfalls mit Schwere und Auswirkungen, Anga ben zur Art der Bedrohung, Ursachen, Angaben zu getroffenen Abhilfemaßnahmen und ggf. die grenzüberschreitenden Auswirkungen der Bedrohung.

Die Einhaltung der NIS 2 Maßnahmen wird mit strengen Haftungsregeln für die Geschäftsleitung überwacht und bei nicht Einhaltung mit strengen Sanktionsvorschriften bestraft. Die Geschäftsführung muss die Umsetzung der Maßnahmen überwachen und bei Verstößen dafür haften. Darüber hinaus muss die Geschäftsführung an Schulungen teilnehmen und diese ihren Beschäftigten anbieten.

Bei Verstößen oder nicht Einhaltung der Maßnahmen können Strafen bis zu 10 Mio. € oder bis zu 2% des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher Betrag höher ist. Darüber hinaus birgt die NIS2-Richtlinie das Potenzial, dass Geschäftsführer persönlich haftbar gemacht werden können, was zusätzliche Rechtsfolgen und -kosten für die Unternehmensführung mit sich bringt.

Die NIS2-Richtlinie stellt einen entscheidenden Wendepunkt in der europäischen Cybersicherheitspolitik dar. Die Herausforderungen sind immens, welche mit der richtigen Vorbereitung und einem fundierten Verständnis der Anforderungen bewältigt werden kann. Als Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie stehen wir Ihnen bei Fragen zur Seite, um Sie durch den Anpassungsprozess zu begleiten und sicherzustellen, dass Ihr Unternehmen den neuen Standards entspricht.