Summary

NIS2 – Direktive mit Biss

Was Unternehmen jetzt wissen müssen

Die Europäische Union hat die NIS2-Richtlinie (Network and Information Security Directive 2) verabschiedet, um die Cybersicherheit in Europa zu stärken und auf die weiterentwickelten Bedrohungen für digitale Systeme und Dienste zu reagieren. Die Richtlinie ist eine überarbeitete Version der ursprünglichen NIS-Richtlinie und bringt eine Reihe von wichtigen Neuerungen mit sich. In Deutschland wird das Gesetz unter dem Namen NIS2UmsuCG voraussichtlich Anfang 2024 das IT-SiG 2.0 ergänzen. Alle Mitgliedstaaten müssen NIS2 bis zum 17. Oktober 2024 in lokales Recht überführen.

Da noch keine finale Fassung vorliegt, können sich die nachfolgend vorgestellten Inhalte ändern. Zudem wird es wahrscheinlich Übergangsfristen für bestimmte Unternehmen geben, die aber noch nicht festgelegt wurden.

Rund 25.000 deutsche Unternehmen erstmals betroffen

Im Vergleich zur ursprünglichen Richtlinie, die hauptsächlich auf kritische Infrastrukturen wie Energie, Verkehr und Gesundheitswesen abzielte, gilt NIS2 nun für alle öffentlichen oder privaten Einrichtungen, die:

- Mindestens 50 Mitarbeiter haben
- Mehr als 10 Millionen Euro Jahresumsatz erwirtschaften
- In einem von 18 Wirtschaftssektoren tätig sind

In bestimmten Fällen kann NIS2 aber auch unabhängig von der Unternehmensgröße greifen. Laut Aussage des BMI werden rund 25.000 Unternehmen neu von NIS2 erfasst, die nicht bereits zu den KRITIS-Betreibern gehören. Die erwartbaren Kosten für die Umsetzung von NIS2 beziffert das BMI mit 1,6 Milliarden Euro im ersten Jahr. Ob das eigene Unternehmen von NIS2 betroffen ist, lässt sich hier überprüfen.

Stark erweiterte Meldepflichten

Zu den bedeutendsten Änderungen in NIS2 gehört die Meldepflicht für alle Sicherheitsvorfälle, die sich auf die Dienste von Unternehmen auswirken könnten. Innerhalb von 24 Stunden nach Feststellung ist ein solcher Vorfall an das BSI zu melden. Nach 72 Stunden muss ein konkretisierter Bericht folgen und nach einem Monat eine ausführliche Analyse.

Finanzielle Strafen und Geschäftsführerhaftung

Bei fehlender Compliance müssen Unternehmen mit Geldbußen rechnen, die sich nach dem Wirtschaftssektor richten, in dem das Unternehmen tätig ist. Für besonders wichtige Sektoren können Strafen von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes verhängt werden. Für wichtige Sektoren liegt die Höchststrafe bei 7 Millionen Euro oder 1,4 % des Umsatzes.

In einigen Fällen können Geschäftsführer und Führungskräfte auch persönlich haftbar gemacht werden, wenn notwendige Sicherheitsmaßnahmen nicht ergriffen, Sicherheitsrisiken nicht angemessen bewertet oder Sicherheitsverstöße nicht gemeldet wurden.

Verpflichtende Weiterbildung für Mitarbeiter & Management

Die Geschäftsführung kann sich nicht mehr auf fehlende oder veraltete Kenntnisse der Cybersicherheit und Bedrohungslage berufen, sondern ist verpflichtet, das eigene Wissen aktuell zu halten und bei Bedarf zu erweitern. Außerdem sind Schulungen zu relevanten Themen der Cybersicherheit für alle Mitarbeiter vorgeschrieben. Dies soll gewährleisten, dass alle Unternehmensebenen über die erforderlichen Kenntnisse und Fähigkeiten verfügen, um angemessen auf Sicherheitsrisiken zu reagieren.

Kontinuierliches Risikomanagement wird Pflicht

NIS2 betont Cyberrisikomanagement als Teil des unternehmerischen Risikomanagements. Für die IT-Sicherheit entstehen daraus erhebliche Herausforderungen, denn Angriffsoberflächen ändern sich schnell und manchmal sogar über Nacht wie im Fall von Log4Shell. Risikobetrachtungen müssen daher kontinuierlich erfolgen und können nicht auf gelegentliche Schnappschüsse begrenzt werden. Ohne einen stets aktuellen Überblick zur Bedrohungslage lassen sich weder Eintrittswahrscheinlichkeiten noch Schadenspotenziale sinnvoll bestimmen.

Software-Supply-Chain muss geschützt werden

Im Rahmen von NIS2 müssen Unternehmen auch ihre Lieferkette als potenzielles Risiko der Cybersicherheit einkalkulieren. Wie hoch ist die Wahrscheinlichkeit, dass ein Unternehmen durch IT-Verbindungen mit einem anderen Unternehmen angegriffen werden kann? Im Fokus steht dabei neben dem Selbstschutz insbesondere auch der Schutz weiterer Unternehmen in der Kette. Es ist zu erwarten, dass NIS2-konforme Cybersicherheit daher ein Faktor bei Entscheidungen zu Geschäftsbeziehungen und der Lieferantenauswahl sein wird.

NIS2-Compliance: Wie kann Trend Micro helfen?

Trend Micro Vision One ist eine speziell entwickelte Plattform für erweiterte Detection & Response (XDR) in der gesamten IT-Infrastruktur. Über Sensoren werden sicherheitsrelevante Daten über Email, Endpunkte, Server, Cloud Workloads und Netzwerke hinweg gesammelt und intelligent miteinander in Beziehung gesetzt. Damit lassen sich auch komplexe, mehrstufige Angriffe frühzeitig identifizieren und abwehren. Trend Micro Vision One gewährleistet die Compliance der Angriffserkennung und minimiert den Betriebsaufwand:

- **Schnell:** Bewertung von Vorfällen im Kontext sorgt für Priorisierung und Reduktion von Alarmen.
- **Aktuell:** Laufende Aktualisierung der Erkennungsregeln auf Basis von Erkenntnissen aus dem globalen Trend Micro Threat Protection Network.
- **Detailliert:** Vollständige Aktivitätsdaten erlauben die lückenlose Nachverfolgung von Angriffen im Zeitverlauf.
- **Integriert:** Offene APIs und Anbindung an SIEM, SOAR und weitere Systeme.

Risk Score: Aktuelle Risikolage auf einen Blick

Informationen werden in verschiedenen Dashboards prägnant aufbereitet, jeweils im Detailgrad abgestimmt auf die Bedürfnisse von CISOs/Geschäftsführung und technischen Mitarbeitern. Ein individueller Risk Score gibt sofortigen Aufschluss über die Security Posture im Zeitverlauf. Darüber hinaus werden die aktuell größten Risiken aufgezeigt und Vorschläge zur aktiven Senkung des Risk Score gemacht. Zur Berechnung wird die gesamte Angriffsoberfläche herangezogen, darunter:

- **Häufig angegriffene Schwachstellen** auf Servern oder Endpunkten.
- **Auffällige Anwender und Geräte** z,B. Aufruf unsicherer Webseiten, häufige Malware-Infektionen, Phishing-Email-Versand
- **Verdächtige Logins**, die zeitliche oder geografische Anomalien aufweisen.
- **Ungewöhnliche Datenbewegungen**, die nicht zu bekannten Mustern passen.
- **Unsichere Account-Daten**, die bereits an externer Stelle als kompromittiert bekannt sind.

Trend Micro hat die Technologie, um nahezu alle NIS2-Anforderungen aus einer Hand abzudecken. Für weiterführende Informationen und detaillierte Einblicke zu NIS2 schauen Sie gerne auf unserer Webseite vorbei. Sie können auch jederzeit direkt mit unseren Experten über Ihren individuellen Weg zur NIS2-Compliance sprechen. Vereinbaren Sie hier Ihren Termin!

Warum Unternehmen jetzt handeln müssen

- Im Oktober 2024 wird NIS2 bei vielen Unternehmen schlagartig auf die Agenda rücken.
- Engpässe bei Personalressourcen und Technologiepartnern sind zu erwarten.
- Unternehmen müssen zunächst entscheiden, für welche Aufgaben überhaupt ein Partner benötigt wird. Erst danach kann ein passender Partner gefunden werden.
- Implementierung und Koordination von Technologien und Prozessen können einige Zeit in Anspruch nehmen.

Ermitteln Sie jetzt frühzeitig Ihren Bedarf! Falls Sie sich noch nicht sicher sind, sprechen Sie uns einfach an. Wir helfen gerne.

Copyright © 2023 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: https://www.trendmicro.com/de_de/about/legal/privacy.html.