Summary

# NIS2 Countdown

## Was Unternehmen in Deutschland erwartet

Mit der NIS2-Direktive (Network and Information Security Directive 2) reagiert die Europäische Union auf die weiterentwickelten Bedrohungen für digitale Dienste und Systeme. In Deutschland muss die Direktive bis zum 17. Oktober 2024 in lokales Recht überführt werden. Da aber bislang keine finale Fassung vorliegt, können sich die Inhalte noch in einigen Aspekten ändern. Mögliche Übergangsfristen sind derzeit nicht definiert. Trotz dieser verbliebenen Unklarheiten ist es ratsam, jetzt mit der Vorbereitung auf NIS2 zu beginnen, bevor das Thema bis Oktober bei Tausenden Unternehmen gleichzeitig auf die Agenda rückt.

### NIS2: Ist mein Unternehmen betroffen?

Unternehmen sollten jetzt klären, ob sie unter NIS2 fallen, denn mit Inkrafttreten des deutschen Gesetzes sind sie zur Selbstregistrierung verpflichtet. Europaweit sind voraussichtlich rund 160.000 Unternehmen betroffen, in Deutschland ist mit rund 30.000 Unternehmen zu rechnen. Branchenverbände können darüber Auskunft geben, ob das eigene Unternehmen dazu gehört. Ein erster Online-Check ist hier möglich. Die Selbstregistrierung ist im Übrigen nicht nur mit erweiterten Pflichten, sondern wahrscheinlich auch mit Hilfestellungen verbunden, die aber noch nicht abschließend definiert wurden.

### Erwartbare Kosten kalkulieren

Das BMI beziffert die erwartbaren Kosten für die Umsetzung von NIS2 auf rund 1,6 Milliarden Euro im ersten Jahr. Im Durchschnitt liegen die geschätzten Kosten pro Unternehmen also bei rund 50.000 Euro, die für zusätzliche Lösungen, Prozesse und Mitarbeiter anfallen werden. In der Realität hängen die Kosten für NIS2 aber maßgeblich vom bereits erreichten Reifegrad der IT-Sicherheit ab. In Vorbereitung auf NIS2 sollten Unternehmen also jetzt analysieren, wie es um ihre aktuelle Security Posture bestellt ist, wo Schwachstellen liegen und welche Maßnahmen kosteneffiziente Verbesserungen ermöglichen.

### Auswirkungen des Fachkräftemangels abwägen

Aufgrund des anhaltenden Fachkräftemangels in der IT-Sicherheit wird es im Oktober 2024 mit hoher Wahrscheinlichkeit zu Engpässen kommen, sowohl bei internem Personal wie auch bei externen Dienstleistern. Mit gezielten Abwerbeaktionen muss gerechnet werden. Unternehmen sollten daher jetzt prüfen, ob das vorhandene Personal für NIS2 ausreicht und ob alles getan wurde, um eine Abwanderung zu verhindern. Falls das eigene Personal absehbar nicht ausreicht, ist es ratsam, jetzt Beziehungen zu externen IT-Dienstleistern aufzunehmen.

## Die wichtigsten Neuerungen in NIS2
## Cyberrisikomanagement wird Geschäftsführungsaufgabe

Cyberrisikomanagement ist eines der wichtigsten neuen Stichworte in der NIS2-Direktive, obwohl die meisten Unternehmen schon lange mit dem Konzept vertraut sein dürften:

Dieser Regelkreis gilt grundsätzlich in der IT-Sicherheit genauso wie im Business-Risikomanagement, wobei es spezielle Herausforderungen gibt: Risikolagen können sich in der IT-Sicherheit extrem kurzfristig ändern, die Effektivität von Maßnahmen lässt sich meist erst im Ernstfall bestimmen und auch die Verhältnismäßigkeit ist schwer zu bewerten, solange Eintrittswahrscheinlichkeit und Schadensausmaß unbekannt sind. Antworten auf diese Fragen können Unternehmen nur in Zusammenarbeit mit Sicherheitsherstellern liefern.

Die wichtigste Neuerung liegt aber in dem Gewicht, das dem Thema mit dem Begriff „Cyberrisikomanagement" und weiteren Formulierungen im Gesetz gegeben wird. Dies verdeutlicht, dass sich die Verantwortung für die Abwehr von Cyberrisiken auf die Geschäftsführungsebene verlagert, wo auch die entsprechenden Entscheidungen getroffen werden müssen.

Dabei reicht es nicht mehr wie bisher, nur das eigene Unternehmen zu betrachten. Bei der Bewertung der Verhältnismäßigkeit von Maßnahmen muss auch berücksichtigt werden, welche Folgen für die deutsche Gesellschaft und Wirtschaft durch einen erfolgreichen Angriff entstehen könnten. Das bedeutet nicht, dass Unternehmen de facto alle Risiken ausschließen müssen – aber es muss eine bewusste Auseinandersetzung mit dem Thema stattfinden und dokumentiert werden.

## Supply Chain in Risikomanagement einbeziehen

Angriffe auf die Software-Supply-Chain, wie zum Beispiel im Fall von Solarwinds, können verheerende Folgen für ganze Branchen haben. In der NIS2-Direktive wird daher explizit die Software-Supply-Chain als wichtiger Faktor des Risikomanagements aufgeführt. Unternehmen müssen demnach Vorkehrungen treffen, um zu verhindern, dass sich Bedrohungen durch Software-Aktualisierungen, Patches oder andere Daten in eigenen Systemen verbreiten oder sogar auf Drittsysteme überspringen. Hier zeigt sich wieder der Anspruch von NIS2, das Risikomanagement über das eigene Unternehmen hinaus zu erweitern.

## Geschäftsführerhaftung & Weiterbildungspflicht

Geschäftsführer wesentlicher und wichtiger Einrichtungen sind verpflichtet, die Umsetzung von notwendigen Maßnahmen zum Risikomanagement zu billigen und zu überwachen. Um diese Aufgaben erfüllen zu können, müssen sie regelmäßig an Schulungen teilnehmen und ausreichende Kenntnisse zur Bewertung von Risiken und Maßnahmen erwerben. Hier ist darauf hinzuweisen, dass die Begriffe „regelmäßig“ und „ausreichend“ im Gesetz nicht weiter definiert werden. Dies wird der juristischen Praxis überlassen. Schulungen und Sensibilisierungsmaßnahmen sind zudem auch für Mitarbeiter vorgeschrieben, damit alle Beteiligten im Unternehmen über ein geschärftes Bewusstsein für Sicherheitsrisiken verfügen.

Bei fehlender Compliance müssen Unternehmen mit Geldbußen rechnen, die sich nach dem Wirtschaftssektor richten, in dem das Unternehmen tätig ist. 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.

## 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. Nach aktueller Interpretation des Gesetzestextes müssen Unternehmen aber keine Strafen befürchten, falls während eines akuten Vorfalls die Reporting-Fristen nicht eingehalten werden können.

Sollten sich bei der Auswertung der Reports Hinweise auf überregionale Auswirkungen zeigen, so kann das BSI verantwortliche Behörden in anderen Mitgliedsstaaten informieren. Natürlich funktioniert dies ebenso umgekehrt. Dieses innergemeinschaftliche Frühwarnsystem ist eines der wesentlichen Ziele von NIS2.

## NIS2-Compliance: Wie kann Trend Micro helfen?

Trend 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 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 der globalen Trend Micro Threat Intelligence.

**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. Zur Berechnung des Risk Scores 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!

Copyright © 2024 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.