

NIS2 Übersicht

Mit Trend Micro Unterstützung zur NIS2-Compliance

Dezember 2023



NIS2-Übersicht

Inhalte

01	Einleitung	4
	Executive Summary	5
	NIS-Richtlinie	6
	NIS2-Richtlinie.....	6
	Mindestharmonisierung.....	7
02	NIS2-Übersicht	8
	Sektoren	9
	Wesentliche und wichtige Einrichtungen	10
	Selbstregistrierung	11
	Maßnahmen zum Risikomanagement der Cybersicherheit	11
	Meldung von Vorfällen	12
	Supervision	12
	Durchsetzung und Sanktionen	13
	Managementverantwortung	13
03	Wie unterstützt Trend Micro Ihre NIS2-Compliance?	14
	Trend Vision One™	15
	Schäden begrenzen mit XDR.....	16
	Threat Hunting und Incident Reporting.....	16
	Cyber-Risikomanagement leicht gemacht mit ASRM.....	16
	Wie ASRM und XDR zusammenarbeiten.....	17
	Implementierung von Zero Trust.....	17
	Beschleunigung von SOC-Aufgaben mit Companion AI	18
	Schutz von (hybriden) Cloud-Infrastrukturen.....	19
	Phish Insight	20
	Trend Service One™.....	20
04	Anhang	21
	Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen (CER)	22
	Digital Operational Resilience Act (DORA).....	22
	Zuordnung von Anforderungen und Trend Micro Lösungen	22
	NIS2-Sektoren	24

01

Einleitung

Einleitung

Executive Summary

Im Jahr 2016 wurde die Network and Information Systems Directive (NIS, [EU 2016/1148](#)) eingeführt, um die Cybersicherheit in allen EU-Mitgliedsstaaten zu stärken. Seitdem hat sich die Cyber-Resilienz der Europäischen Union deutlich verbessert. Die rechtlichen Rahmenbedingungen für die Cybersicherheit in den einzelnen Mitgliedsstaaten sind allerdings immer noch unterschiedlich. Um die Sicherheitsmaßnahmen in der gesamten Region zu verbessern, wurde am 16. Januar 2023 die NIS2-Richtlinie ([EU 2022/2555](#)) eingeführt. NIS2 etabliert einen gemeinsamen Anforderungsrahmen für Unternehmen und Mitgliedstaaten. Durch die Erweiterung der Sektoren und das Absenken der Relevanzschwellen sind heute wesentlich mehr Unternehmen betroffen. NIS2 schreibt ein Cyber-Risikomanagement vor und verlangt Mitarbeiterschulungen sowie regelmäßige Audits. Die Geschäftsleitung wird bei Nichteinhaltung der Vorschriften zur Rechenschaft gezogen, und Verstöße werden mit empfindlichen Strafen geahndet.

Trend Vision One™ ist die Lösung zur Umsetzung der von NIS2 geforderten technischen Maßnahmen. Die enthaltenen Funktionen für Risikomanagement und Threat Hunting bilden eine solide Grundlage für qualifizierte Risikomanagementprozesse und liefern sofort verwertbare Informationen für das Reporting im Ernstfall.

NIS-Richtlinie

Die erste Network and Information Systems Directive (NIS, [EU 2016/1148](#)) wurde 2016 eingeführt, um die grundlegende Cybersicherheit in der EU zu stärken. Alle Mitgliedsstaaten wurden verpflichtet, Computer Security Incident Response Teams (**CSIRTs**) zu ernennen und nationale Aufsichtsbehörden für Cybersicherheit einzurichten. Seit der Einführung hat sich die Cyber-Resilienz der Europäischen Union deutlich verbessert. Die Richtlinie wirkte dabei wie ein Katalysator für regulatorische und institutionelle Cybersicherheitsansätze in der EU, wodurch es zu einem Umdenken gekommen ist.

In den Mitgliedsstaaten wurden nationale Strategien eingeführt und regulatorische Maßnahmen für kritische Infrastrukturen und Organisationen umgesetzt. Damit sorgte die Richtlinie für die Etablierung nationaler Rahmenwerke zur Sicherheit von Netzwerk- und Informationssystemen. Trotz der wachsenden Cyber-Resilienz sind die rechtlichen Rahmenbedingungen für Cybersicherheit in der EU aber immer noch unterschiedlich.

Darüber hinaus kündigte die EU eine „**Neue Cybersicherheitsstrategie der EU und neue Vorschriften zur Erhöhung der Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen**.“ Dabei sollte bedacht werden, dass sich die Angriffsoberflächen seit 2016 dramatisch verändert haben. Zu den Änderungen gehören zum Beispiel die Auswirkungen von COVID-19 und die angepassten Taktiken der Cyberangreifer. Die Kommission konsultierte alle Interessengruppen umfassend, um die Folgen zu untersuchen und Schwachstellen der NIS-Richtlinie zu ermitteln. Die Kommission identifizierte die folgenden Bereiche:

- Unzureichende Cyber-Resilienz der in der EU tätigen Unternehmen
- Abweichende Widerstandsfähigkeit in den Mitgliedsstaaten und Sektoren
- Kein gemeinsames Verständnis der wichtigsten Bedrohungen und Herausforderungen in den Mitgliedsstaaten
- Fehlende gemeinsame Krisenreaktionen

NIS2-Richtlinie

Am 16. Januar 2023 trat die NIS2-Richtlinie ([EU 2022/2555](#)) in Kraft. Die Richtlinie soll Cybersicherheitsmaßnahmen in der gesamten EU verbessern, indem ein gemeinsamer Anforderungsrahmen für die Cybersicherheit von Unternehmen und Mitgliedsstaaten festgelegt wird. Bis zum 17. Oktober 2024 muss die Richtlinie in nationales Recht überführt werden, einige Mitgliedsstaaten könnten NIS2 aber auch schon früher umsetzen.

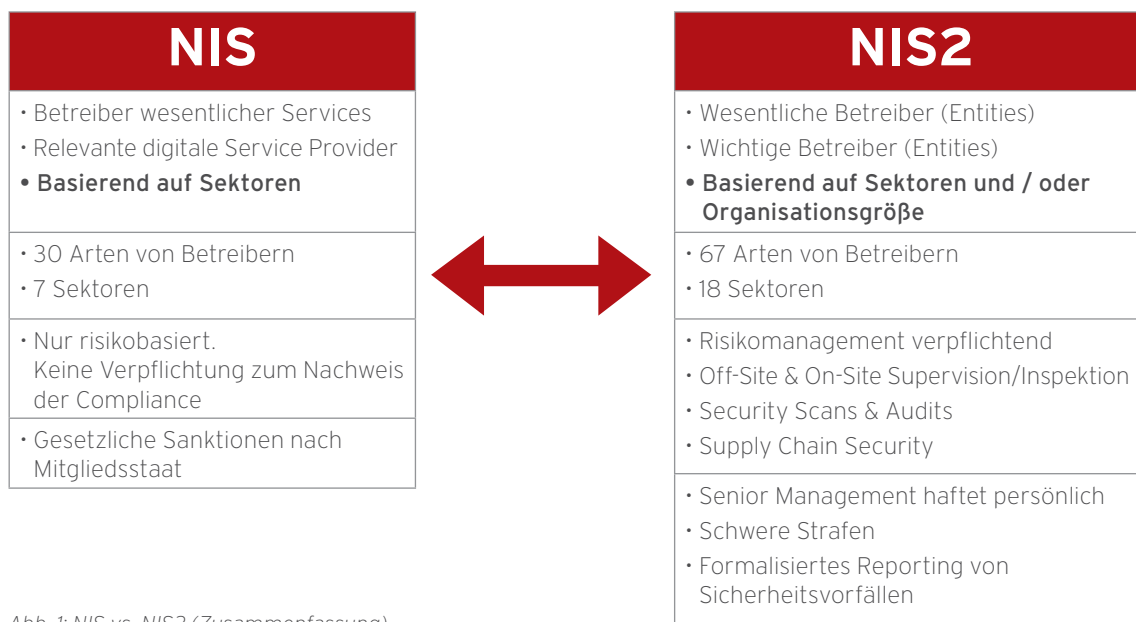


Abb. 1: NIS vs. NIS2 (Zusammenfassung)

Mit NIS2 werden im Vergleich zur ursprünglichen NIS-Richtlinie zusätzliche Maßnahmen und Anforderungen zur Cybersicherheit eingeführt.

- Supply-Chain-Sicherheit ist eine der Prioritäten.
- Cyberrisikomanagement ist verpflichtend vorgeschrieben.
- Unternehmen müssen Mitarbeiter schulen und regelmäßige Audits zur Cybersicherheit durchführen.
- Die Unternehmensleitung wird bei fehlender Compliance persönlich zur Verantwortung gezogen.
- Verstöße werden mit empfindlichen Strafen geahndet.
- Für die Reaktion auf Vorfälle gibt es nun formalisierte Meldefristen.

Mit NIS2 wird auch der Bereich der betroffenen Sektoren erweitert und die Schwelle für betroffene Einrichtungen gesenkt:

- Mehr Sektoren/Industrien sind von NIS2 betroffen.
- Viel mehr Einrichtungen fallen unter NIS2.

Mindestharmonisierung

NIS2 beruht auf dem Prinzip der Mindestharmonisierung. Diesem Prinzip zufolge müssen alle Mitgliedsstaaten Gesetze erlassen, die mindestens so streng sind wie die EU-Richtlinie. Die Länder können jedoch strengere Vorschriften als NIS2 erlassen, indem sie zusätzliche Sektoren einbeziehen oder strengere Anforderungen an die Cybersicherheit stellen. Diese Flexibilität bedeutet, dass Unternehmen keine absolute Gewissheit über die Einzelheiten von NIS2 in ihrem Land haben können, bis ein nationales Gesetz verabschiedet ist.

02

NIS2-Übersicht

NIS2-Übersicht

Sektoren

NIS2 umfasst mehr Sektoren als die vorherige NIS-Richtlinie. Außerdem werden Sektoren nun unterteilt in „Sektoren mit hoher Kritikalität“ und „andere kritische Sektoren“, wie in den Anhängen 1 und 2 definiert. Durch das Hinzufügen von sieben neuen „anderen kritischen Sektoren“ ist die Gesamtzahl der Sektoren auf jetzt 18 angewachsen. Es ist nicht erforderlich, dass Technologie zum Kerngeschäft eines betroffenen Unternehmens gehört, wie am Beispiel des Sektors „Produktion“ zu sehen ist.



Abb. 2: Sektoren mit hoher Kritikalität (Anhang 1)

Wesentliche und wichtige Einrichtungen

Die Begriffe „Betreiber wesentlicher Dienste“ und „relevante Anbieter digitaler Dienste“ werden im Zuge von NIS2 durch „wesentliche Einrichtungen“ und „wichtige Einrichtungen“ ersetzt. Diese Änderung der Terminologie verdeutlicht, dass der Anwendungsbereich von NIS2 weit über „kritische Infrastrukturen“ hinausgeht. Stattdessen legt die NIS2-Richtlinie die Unternehmensgröße als universelles Kriterium für die Identifizierung betroffener Unternehmen fest. Dies bedeutet, dass alle mittleren und großen Unternehmen, die in einem der erfassten Sektoren tätig sind oder Dienstleistungen anbieten, in den Anwendungsbereich der Richtlinie fallen. In den meisten Sektoren hängt die Einstufung einer Organisation als „wesentlich“ oder „wichtig“ ebenfalls von der Größe ab. Die Definition der Unternehmensgröße stützt sich auf die **„Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen“**.

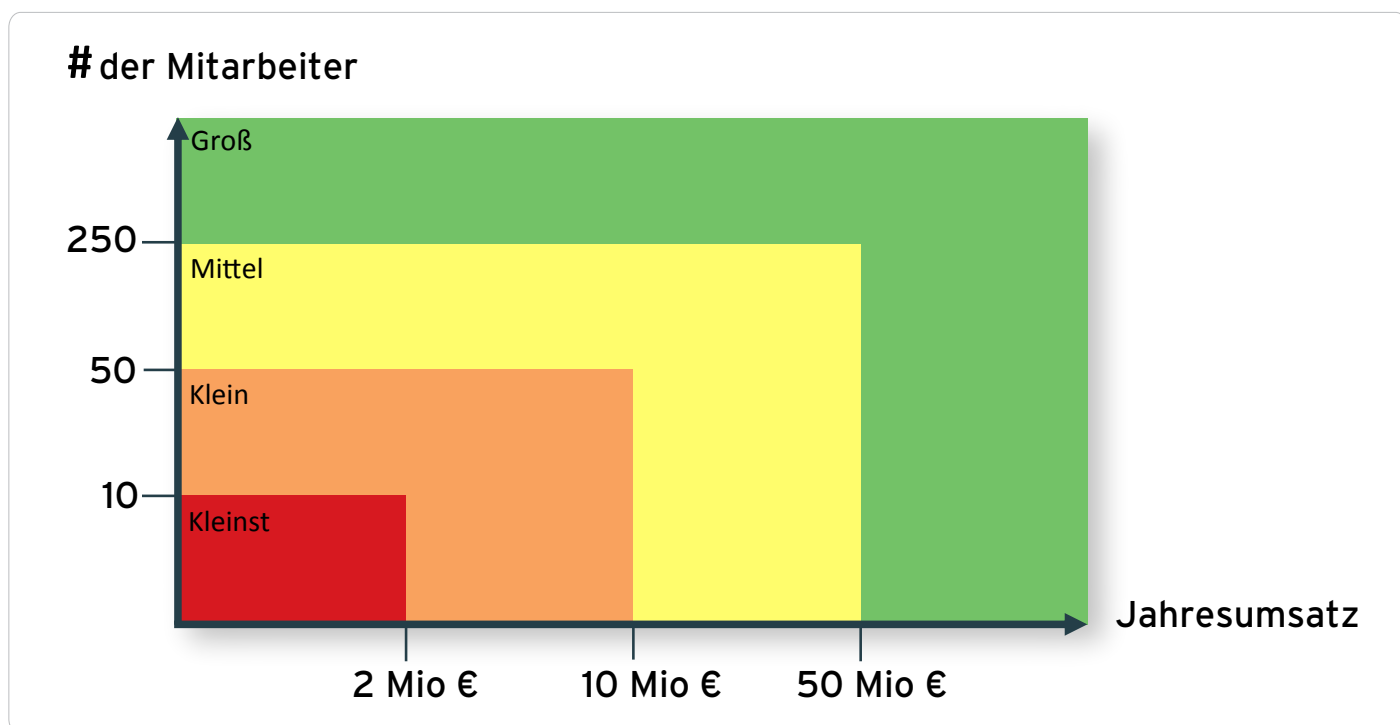


Abb. 4: Größeneinteilungen gemäß „Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen“

Durch die Kombination der Unternehmensgröße und des betroffenen Sektors/Teilsektors erhalten wir erste Informationen darüber, ob eine Organisation als wesentlich/wichtig einzustufen ist oder nicht in den Anwendungsbereich von NIS2 fällt.

„...Von der NIS-2-Richtlinie erfasste Unternehmen müssen zukünftig Risikomanagementmaßnahmen im Cybersicherheitsbereich vorweisen und Meldepflichten im Fall von Cybervorfällen erfüllen. Nach Schätzungen des Statistischen Bundesamts betrifft das in Deutschland insgesamt rund 29.000 Unternehmen - mehr als fünfmal so viele wie zuvor...“

<https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2023/01/eu-richtlinien-kritis.html>

Bundesministerium des Innern und für Heimat (BMI)

		# der Mitarbeiter	Jahresumsatz	Jahresbilanz
Großunternehmen		≥ 250	≥ 50 Mio. EUR	≥ 53 Mio. EUR
Kleinstunternehmen sowie kleine und mittlere Unternehmen (KMU)	Mittel	< 250	< 50 Mio. EUR	< 43 Mio. EUR
	Klein	< 50	< 10 Mio. EUR	< 10 Mio. EUR
	Kleinst	< 10	< 2 Mio. EUR	< 2 Mio. EUR

Tabella 1: Größeneinteilungen gemäß „Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen“

Selbstregistrierung

Ab dem 18. Oktober 2024 müssen sich Unternehmen, die in den Geltungsbereich von NIS2 fallen, bei der zuständigen nationalen Behörde registrieren. Außerdem müssen sie bedeutende Vorfälle melden und die in der Richtlinie festgelegten Pflichten erfüllen. Unternehmen müssen offizielle Zertifizierungen erhalten oder sich regelmäßigen Audits unterziehen, um die Compliance nachzuweisen. Bis zum 17. April 2025 müssen die Mitgliedstaaten eine Liste der wesentlichen und wichtigen Einrichtungen erstellen, inklusive der Registrierungsdienste für Domain-Namen. Von NIS2 betroffene Einrichtungen müssen den Behörden mindestens die folgenden Informationen zur Verfügung stellen:

- Name
- Anschrift und aktuelle Kontaktinformationen, einschließlich E-Mail-Adressen
- IP-Bereiche
- Telefonnummern
- Relevanter Sektor und Teilsektor (falls zutreffend)
- Liste der Mitgliedstaaten, in denen NIS2-relevante Dienstleistungen erbracht werden (falls zutreffend)

Maßnahmen zum Risikomanagement der Cybersicherheit

Wesentliche und wichtige Organisationen müssen geeignete und verhältnismäßige technische, betriebliche und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit von Netzen und Informationssystemen zu beherrschen, die sie für ihre Tätigkeiten oder Dienste nutzen. Außerdem sollten Unternehmen versuchen, die Auswirkungen von Vorfällen auf ihre Dienstleistungsempfänger und andere Dienste zu verhindern oder zu minimieren.

Diese Maßnahmen schützen Netz- und Informationssysteme und ihre physische Umgebung vor Zwischenfällen auf der Grundlage eines Allgefahrenansatzes. Maßnahmen müssen mindestens Folgendes umfassen:

- a) Strategien zur Risikoanalyse und zur Sicherheit von Informationssystemen
- b) Behandlung von Zwischenfällen
- c) Geschäftskontinuität, z. B. Backup-Management, Notfallwiederherstellung und Krisenmanagement
- d) Supply-Chain-Sicherheit, inklusive sicherheitsrelevanter Aspekte der Beziehungen zwischen jedem Bestandteil und den jeweiligen direkten Lieferanten oder Dienstleistern
- e) Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netzen und Informationssystemen, einschließlich der Behandlung von Schwachstellen und Offenlegung
- f) Strategien und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen des Risikomanagements im Bereich der Cybersicherheit
- g) Grundlegende Praktiken der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- h) Grundsätze und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
- i) Sicherheit des Personalwesens, Richtlinien für Zugangskontrollen und Asset-Management
- j) Einsatz von Lösungen für Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation
- k) Sichere Kommunikation und bei Bedarf Notfallkommunikationssysteme innerhalb der Einrichtung

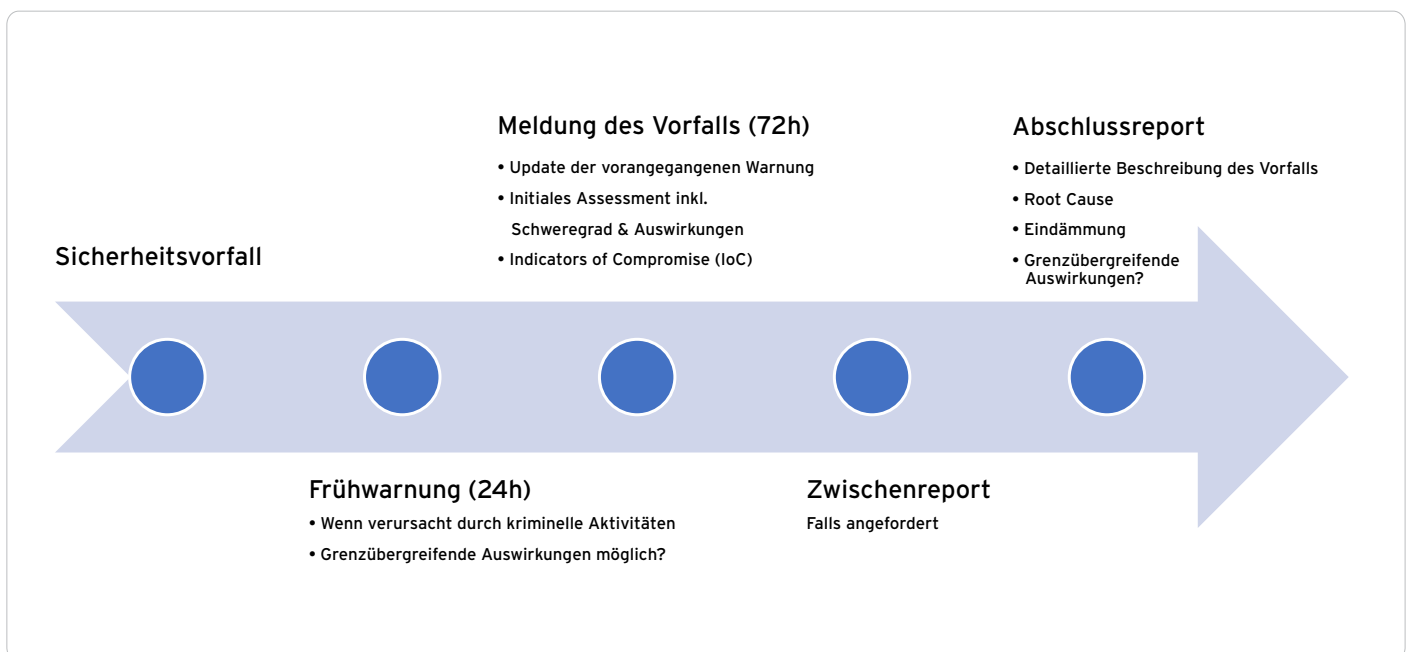
Um die Sicherheit von Netz- und Informationssystemen zu gewährleisten, sollten geeignete Maßnahmen getroffen werden, die dem aktuellen Stand der Technologie und den einschlägigen europäischen und internationalen Normen wie der ISO/IEC27000-Reihe entsprechen. Bei der Bestimmung der Angemessenheit von Maßnahmen sollten Faktoren wie die Risikoexposition der Einrichtung, ihre Größe sowie die Wahrscheinlichkeit und Schwere von Zwischenfällen berücksichtigt werden. Dazu gehören auch mögliche Auswirkungen auf Gesellschaft und Wirtschaft. Die Europäische Union kann Risikobewertungen durchführen für kritische Systeme, Dienste und Lieferketten. Zudem können in delegierten Rechtsakten weitere technische Anforderungen festgelegt werden.

Meldung von Vorfällen

Als wesentlich oder wichtig eingestufte Einrichtungen müssen bei einem bedeutsamen Sicherheitsvorfall strenge Meldepflichten erfüllen und innerhalb von 24 Stunden Frühwarnungen übermitteln. Offizielle Meldungen von Vorfällen sind innerhalb von 72 Stunden erforderlich, gefolgt von Zwischenberichten (falls vom CSIRT angefordert). Innerhalb eines Monats muss ein Abschlussbericht eingereicht werden. Wenn der Vorfall noch andauert, sind weitere Fortschrittsberichte erforderlich.

Ein Vorfall gilt als bedeutsam, wenn er eine schwerwiegende betriebliche Unterbrechung der Dienste oder einen finanziellen Schaden für die betroffene Einrichtung verursacht hat oder verursachen könnte. Darüber hinaus gilt er als bedeutsam, wenn er das Potenzial hat, anderen natürlichen oder juristischen Personen einen erheblichen materiellen oder immateriellen Schaden zuzufügen.

Es ist wichtig zu beachten, dass das CSIRT beschließen kann, die Dienstleistungsempfänger oder die Öffentlichkeit zu informieren (oder die meldende Stelle dazu aufzufordern), wenn dies im Interesse der Öffentlichkeit liegt.



Supervision

Im Rahmen von NIS2 ersetzen „wesentliche“ und „wichtige“ Einrichtungen die Begriffe „Betreiber wesentlicher Dienste“ und „Digital Service Providers“ aus der NIS-Richtlinie. Der Hauptunterschied zwischen den Kategorien „wesentlich“ und „wichtig“ besteht in dem Umfang und der Dauer der Beaufsichtigung. Die Mitgliedstaaten können ihren zuständigen Behörden gestatten, die Aufsicht von Einrichtungen zu priorisieren. Eine solche Priorisierung muss auf einem risikobasierten Ansatz beruhen.

	Wesentliche Einrichtungen	Wichtige Einrichtungen
Off-Site Supervision	Vor und nach Vorfällen	Nach Vorfällen
On-Site Inspektionen	✓	✓
Stichprobenkontrollen	✓	
Security Audits	Regulär & gezielt & ad hoc	Gezielt
Security Scans	✓	✓
Informationsanfragen	Assessment der implementierten Maßnahmen des Risikomanagements (durch externen Auditor) & Compliance mit der Pflicht zur Informationsweitergabe an Aufsichtsbehörden	Assessment der nach Vorfällen implementierten Maßnahmen des Risikomanagements
Ad-hoc-Audits (z.B. nach Vorfällen)	✓	✗

Durchsetzung und Sanktionen

NIS2 stellt den nationalen Behörden eine umfassende Liste von Maßnahmen zur Verfügung, um die Einhaltung der Vorschriften durchzusetzen oder Sanktionen zu verhängen, falls über einen gewissen Zeitraum keine Compliance hergestellt wurde.

Unternehmen, die die Bestimmungen der Richtlinie nicht einhalten, müssen mit verschiedenen Maßnahmen rechnen. Dazu gehören Verwarnungen, verbindliche Anweisungen oder Anordnungen zur Behebung von Mängeln oder Verstößen.

Unternehmen können auch aufgefordert werden, alle nicht richtlinienkonformen Verhaltensweisen einzustellen. Außerdem kann verlangt werden, dass Maßnahmen zum Risikomanagement der Cybersicherheit eingeführt und Berichtspflichten erfüllt werden. Darüber hinaus kann Unternehmen auferlegt werden, Partner oder Kunden über potenzielle Cyberbedrohungen und Abhilfemaßnahmen zu informieren, innerhalb einer bestimmten Frist Sicherheitsaudits durchzuführen, Beauftragte für die Überwachung der Artikel 21 und 23 zu benennen und Datenschutzvorfälle offenzulegen. Zusätzlich ist die Verhängung von Geldstrafen nach Artikel 34 möglich.

Strafen für wesentliche Einrichtungen	Strafen für wichtige Einrichtungen
Maximal 10 Mio. Euro oder 2% des weltweiten Jahresumsatzes (je nachdem, was höher ist)	Maximal 7 Mio. Euro oder 1,4% des weltweiten Jahresumsatzes (je nachdem, was höher ist)
(Vorübergehende) Aussetzung der Zertifizierung oder Zulassung für einen Teil oder die Gesamtheit der einschlägigen Dienste oder Tätigkeiten der Einrichtung.	X
(Vorübergehendes) Verbot für natürliche Personen, die mit der Wahrnehmung von Leitungsfunktionen auf Ebene der Geschäftsführung oder rechtlichen Repräsentanz betraut sind, diese Leitungsfunktionen auszuüben.	X

Managementverantwortung

Die Leitungsorgane einer Organisation haben mehrere Verantwortlichkeiten, wenn es um das Management von Cybersicherheitsrisiken geht. Sie müssen die Angemessenheit der von der Organisation getroffenen Risikomanagementmaßnahmen genehmigen und die Umsetzung dieser Maßnahmen überwachen. Gleichzeitig müssen sie sich durch Schulungen selbst fortbilden, um ausreichende Kenntnisse und Fähigkeiten zur Identifizierung von Risiken und zur Bewertung von Praktiken des Cyberrisikomanagements aufzubauen. Außerdem müssen die Leitungsorgane den Mitarbeitern regelmäßig Schulungen zu ähnlichen Themen anbieten. Bei fehlender Compliance mit den Vorschriften zum Cyberrisikomanagement können die Leitungsorgane zur Verantwortung gezogen werden.

03

**Wie unterstützt
Trend Micro Ihre
NIS2-Compliance?**

Wie unterstützt Trend Micro Ihre NIS2-Compliance?

IT-Sicherheitsmanager stehen vor der Herausforderung, die NIS2-Richtlinie umzusetzen, die in Artikel 21 die Mindestanforderungen für Cybersicherheit auflistet. Zu diesen Anforderungen gehören Backup-Management, Incident-Management sowie Konzepte und Verfahren für Kryptographie, Zugangskontrollen und Identitätsmanagement. Wenn jedoch bereits bewährte Best Practices für Sicherheit umgesetzt wurden, lassen sich viele dieser Anforderungen leicht erfüllen.

Für ein effektives Cyberrisikomanagement müssen CISOs und IT-Sicherheitsbeauftragte in der Lage sein, der Geschäftsleitung jederzeit den aktuellen Risikostatus zu präsentieren. Außerdem müssen sie die dringlichsten Risiken kennen und dem Unternehmen geeignete Maßnahmen empfehlen. Das Cyberrisikomanagement muss ständig aktualisiert werden, wenn sich die Bedrohungslage ändert.

Trend Micro ist ein globaler Anbieter von Cybersicherheitslösungen mit über 35 Jahren Erfahrung und mehr als 500.000 Unternehmenskunden. Neun der Top-10-Fortune-500-Unternehmen, sechs der Top-10-Gesundheitsdienstleister und alle Top-10-Finanzinstitute vertrauen auf uns. Wir kennen die Herausforderungen der digitalen Transformation und haben eine Plattform mit umfassender Funktionalität entwickelt, um unsere Kunden beim Management von Cyberrisiken zu unterstützen.

Unsere Lösungen decken alle Sicherheitsebenen der IT-Umgebung ab, von E-Mail und Endgeräten bis hin zu Netzwerken, Servern und hybriden Cloud-Umgebungen. Wir konzentrieren uns auf effiziente Funktionsbereitstellung, indem wir so viele Funktionen wie möglich über eine einzige Plattform anbieten. Außerdem trägt unsere optionale SaaS-Bereitstellung dazu bei, die Sicherheit für unsere Kunden zu vereinfachen.

Trend Vision One™

Die aktuelle Bedrohungslandschaft entwickelt sich ständig weiter, daher ist Sicherheit zu einem integralen Bestandteil moderner Unternehmen geworden. Unsere Cybersicherheitsplattform Trend Vision One™ bietet einen umfassenden und proaktiven Ansatz, der alle diese Herausforderungen adressiert. Ihr Team wird mit intuitiven Anwendungen ausgestattet, die Risiken und Bedrohungen in jeder Phase erkennen, aufspüren, untersuchen, analysieren und mit angemessenen Reaktionen beantworten. Die Plattform identifiziert und priorisiert automatisch Risiken und Schwachstellen, wodurch die Menge der täglichen Sicherheitswarnungen reduziert und der Sicherheitsbetrieb vereinfacht wird. Dieser Ansatz ermöglicht es Ihnen, Pläne zur Minimierung von Bedrohungen zu entwickeln und wichtige Leistungsindikatoren zu verbessern, wie z. B. die Zeit bis zur Erkennung, Korrektur und Reaktion.



Abb. 5: Trend Vision One™ Cybersicherheitsplattform

Trend Vision One™ bietet robustes **Attack Surface Risk Management** (ASRM) und mehrschichtigen Schutz in hybriden Umgebungen. Extended Detection & Response (XDR) der nächsten Generation deckt alle Ebenen der IT-Infrastruktur ab, darunter Endpunkte, Server, E-Mail, Cloud-Dienste, Netzwerke, 5G und OT (Operational Technology). Außerdem unterstützt Trend Vision One™ hybride Cloud-Umgebungen mit einer einzigen Plattform, integriert Produkte und Services von Drittanbietern und nutzt Bedrohungsdaten von Trend Micro, um branchenführende XDR-Funktionalität und proaktive, präventionsbasierte Sicherheit bereitzustellen.

Schäden begrenzen mit XDR

Selbst mit den besten Sicherheitsvorkehrungen lassen sich nicht alle Risiken ausschließen. Deshalb ist es entscheidend, Angriffe schnell zu erkennen und zu stoppen, um Schäden zu minimieren. Trend Micro XDR (Extended Detection and Response) schafft Transparenz in Ihrer gesamten IT-Umgebung und sammelt Bedrohungsinformationen von allen angeschlossenen Systemen, sodass Daten korreliert und mithilfe von KI analysiert werden können. Die Technologie liefert damit präzisere, sofort umsetzbare Alarme und minimiert die Anzahl der Fehlalarme. Sicherheitsteams können viel leichter erkennen, was gerade passiert, welche Systeme betroffen sind und wo Handlungsbedarf besteht.

Threat Hunting und Incident Reporting

Threat Hunting und Incident Reporting sind wichtige Aspekte der Cybersicherheit. XDR ist ein leistungsstarkes Tool, das die Untersuchung von Verdachtsfällen durch interaktive Graphen, MITRE ATT&CK-Mapping und vereinfachte Suchtechniken unterstützt. Mit XDR können Reaktionen priorisiert, automatisiert und über mehrere Sicherheitsvektoren hinweg umgesetzt werden - und das alles von einem einzigen Ort aus und mit einer einzigen Aktion. Zudem lassen sich detaillierte Aktivitätsdaten über verschiedene Sicherheitsvektoren hinweg miteinander verknüpfen, um Erkennung und Nachforschung zu verbessern. Verdächtige Ereignisse können so schneller identifiziert und Indikatoren für eine Gefährdung (Indicators of Compromise, IoC) für ein präzises Reporting extrahiert werden. Die XDR-Analyse- und Erkennungsmodelle von Trend Micro profitieren von der marktführenden Abdeckung durch eigene Sensoren und Daten von Drittanbietern.

Cyberisikomanagement leicht gemacht mit ASRM

Das Attack Surface Risk Management (ASRM) von Trend Micro ist ein Werkzeug, das mithilfe von KI automatisch den Risk Score Ihrer IT-Umgebung ermittelt. Risk Insights sammelt Informationen aus verschiedenen Quellen und ermöglicht ein intuitives und umfassendes Verständnis der Sicherheitslage Ihres Unternehmens sowie der Benchmarks und Trends im Zeitverlauf. Interne Daten von angeschlossenen Sensoren werden gesammelt und mit Sicherheitsinformationen aus externen Quellen korreliert, darunter zum Beispiel Regierungsbehörden, Polizeiorganisationen und Sicherheitsunternehmen. Analysten können Anlagen, Schwachstellen und Schlüsselkennzahlen detailliert untersuchen und filtern.

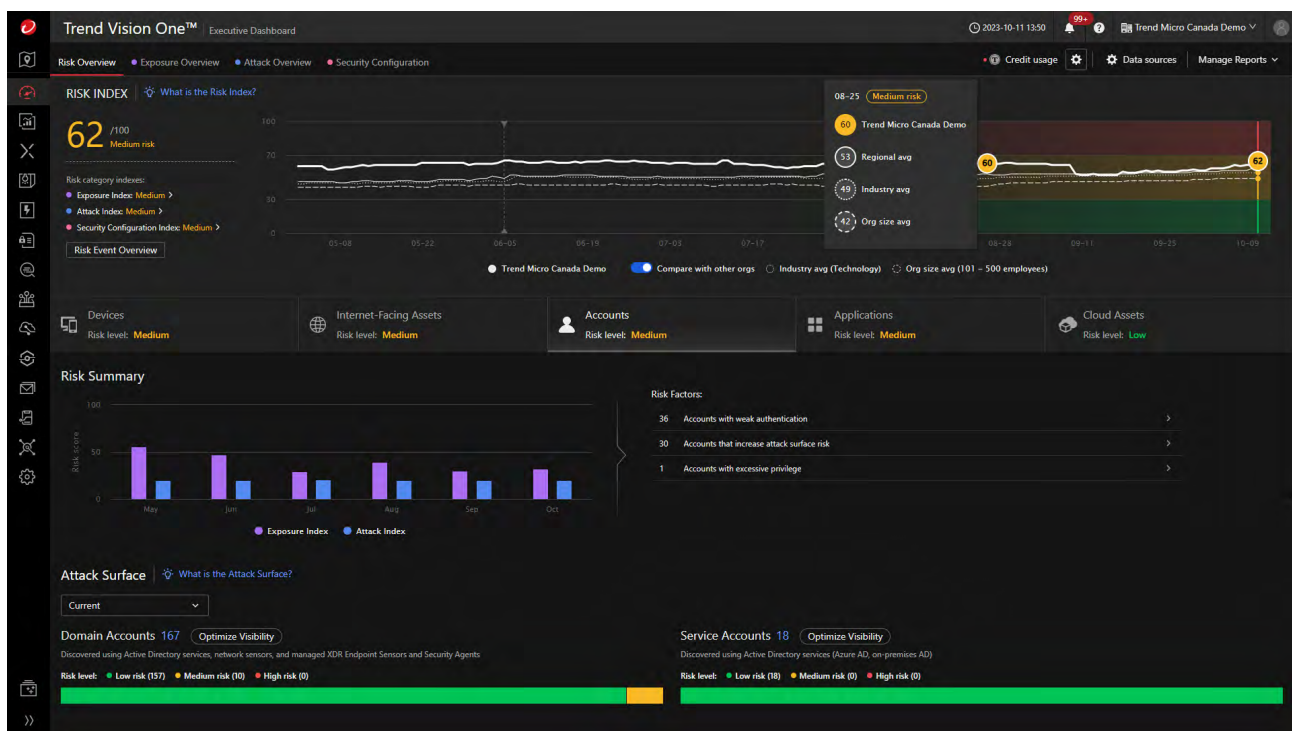


Abb. 6: Trend Vision One™ – Attack Surface Risk Management (ASRM) Dashboards und Reporting

ASRM bietet einen Überblick Ihrer IT-Umgebung in einem Dashboard, das mithilfe einer Ampelanzeige den Schweregrad der identifizierten Risiken anzeigt. Wenn ein bestimmter Schwellenwert überschritten wird, gibt die Lösung eine Warnung aus und zeigt an, welche Systeme betroffen sind. Darüber hinaus werden Gegenmaßnahmen empfohlen, die identifizierte Risiken eindämmen und eine Automatisierung ermöglichen.

Wie ASRM und XDR zusammenarbeiten

Die Trend Vision One Cybersicherheitsplattform integriert ASRM und XDR, um so zentrale Überwachung und Kontrolle zu ermöglichen. Beide Technologien nutzen dieselben Sensoren und kommunizieren miteinander. Wenn ASRM ein Risiko feststellt, kann XDR es näher untersuchen. Ebenso wird der Risikostatus in ASRM sofort aktualisiert, wenn XDR Anzeichen eines Cyberangriffs feststellt. Zusammen tragen diese Technologien dazu bei, die Wahrscheinlichkeit eines Cyberangriffs zu verringern und Auswirkungen zu minimieren.

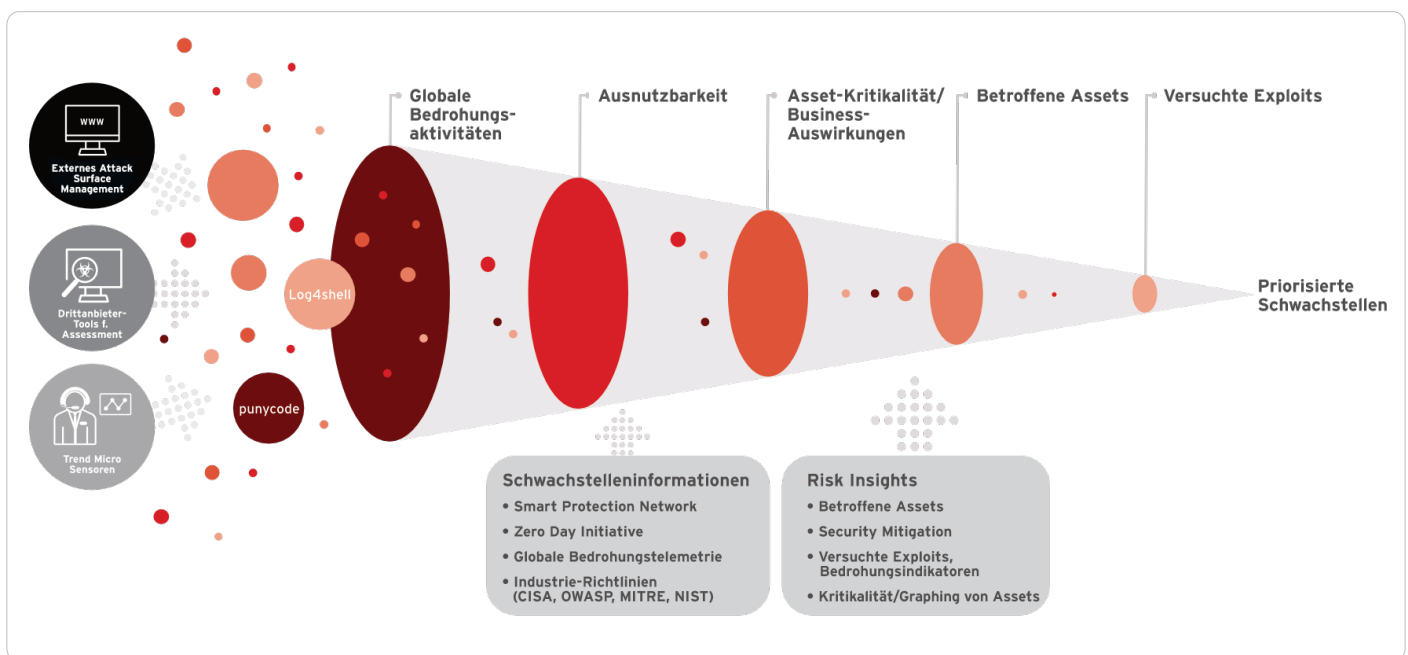


Abb. 7: Trend Micro™ Risk Insights

Implementierung von Zero Trust

Die Umsetzung eines Zero-Trust-Sicherheitsmodells kann für Unternehmen komplex und herausfordernd sein. Zero Trust erfordert ein umfassendes Verständnis der vernetzten Assets, des Nutzerverhaltens und der Datenflüsse. Identifizierung und Behebung potenzieller Sicherheitsrisiken sind wichtig, aber ohne Einblick in diese Bereiche können Unternehmen anfällig für Angriffe sein. Veraltete Systeme, Anwendungen und Geräte machen die Risikobewertung im gesamten Unternehmen kompliziert. Dies gilt insbesondere, wenn sich die Technologielandschaft weiterentwickelt und damit die Angriffsfläche wächst, was das Risiko von Sicherheitsverletzungen erhöht. Um das tatsächliche Risiko einschätzen zu können, ist es wichtig, alle Assets des Unternehmens zu identifizieren und zu katalogisieren.

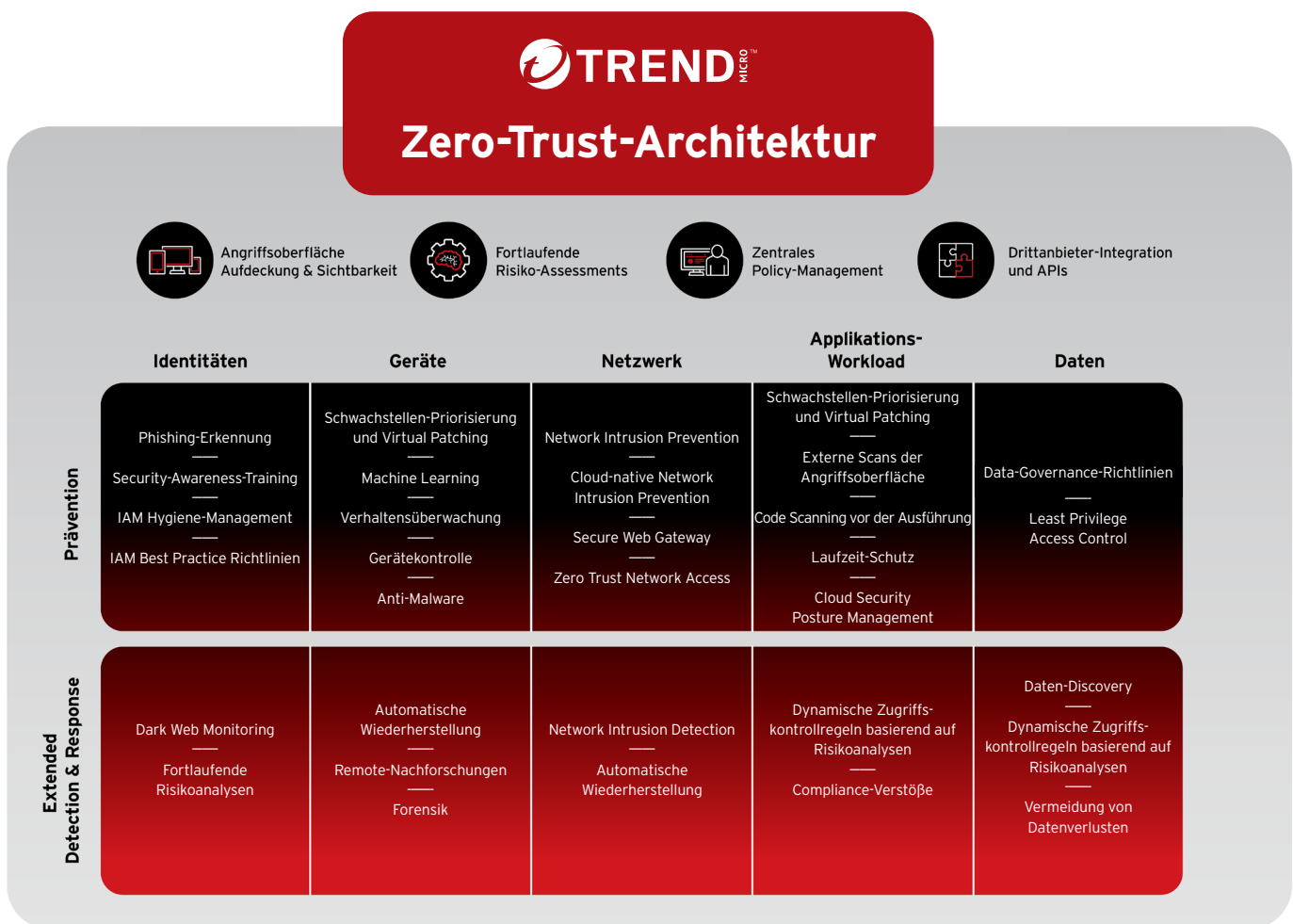


Abb. 8: Trend Micro Zero-Trust-Architektur

Ohne einen Plattformansatz, der Sichtbarkeit und Analytik unternehmensweit konsolidiert, kann die Implementierung eines Zero-Trust-Modells bei gleichzeitiger Einbindung vorhandener Technologien eine erhebliche Herausforderung darstellen. Der Ansatz von Trend Micro steht im Einklang mit Branchen-Frameworks wie NIST, wovon Kunden direkt profitieren. Durch den Einsatz von XDR mit Sensoren in verschiedenen Domänen und die **Integration von Drittanbietern** können Kunden ihre Angriffsoberfläche präzise bestimmen, potenzielle Bedrohungen überwachen und unsere globalen Bedrohungsinformationen nutzen. Daten werden in Trend Vision One eingespeist, wo Kunden die Risiken in Echtzeit analysieren und bewerten können. Die generierten Risk Scores validieren die Identität aller Entitäten für Autorisierung und Authentifizierung.

Beschleunigung von SOC-Aufgaben mit Companion AI

Effektives Zeitmanagement ist bei einem Cybersicherheitsvorfall entscheidend. Jede Sekunde, die mit Fehlalarmen, wiederkehrenden Alarmen oder Routineaufgaben vergeudet wird, beeinträchtigt die Produktivität des Teams.

Trend Vision One™ - Companion, ein KI-gestützter Sicherheitsassistent, wurde entwickelt, um SOC-Teams dabei zu helfen, ihre Leistung und Effizienz zu verbessern. Die Plattform nutzt jahrzehntelange Erfahrungen einer Gruppe führender Experten für Machine Learning und KI. Mit Companion können SOC-Teams ihre täglichen Arbeitsabläufe beschleunigen, Alarm-Überlastung vermeiden und Sicherheitsabläufe (SecOps) optimieren. So wird sichergestellt, dass die gesamte digitale Angriffsoberfläche Ihres Unternehmens geschützt ist, von E-Mail über Endpunkte bis hin zu Netzwerk und Cloud.

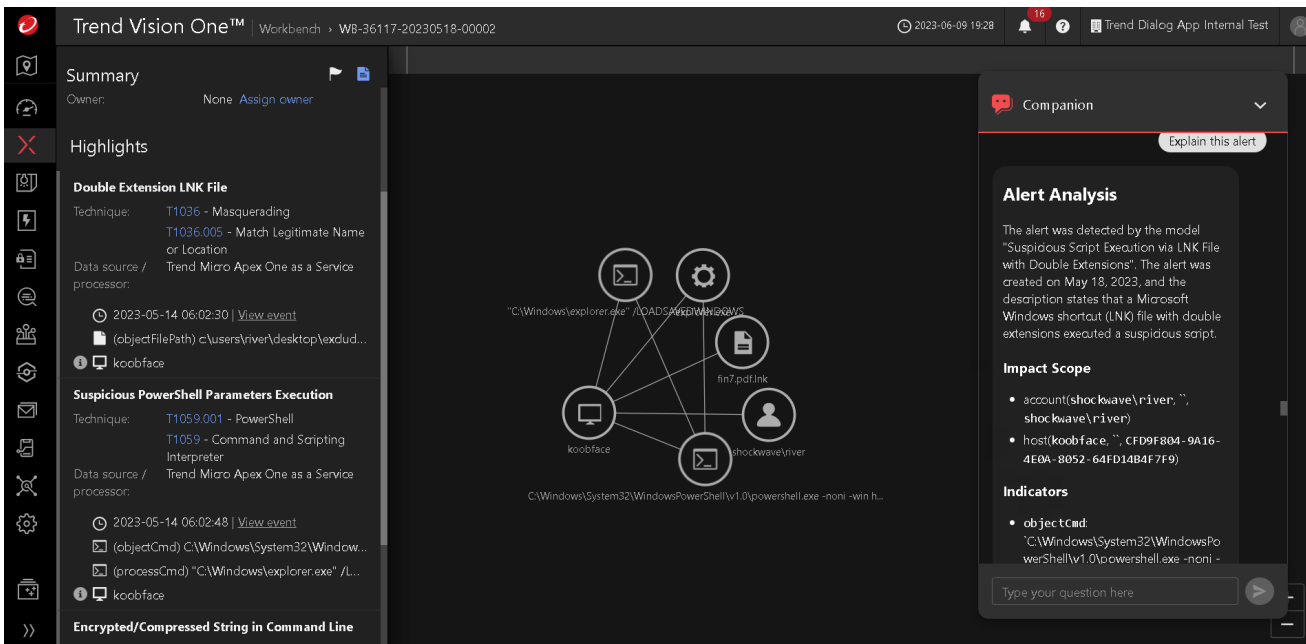
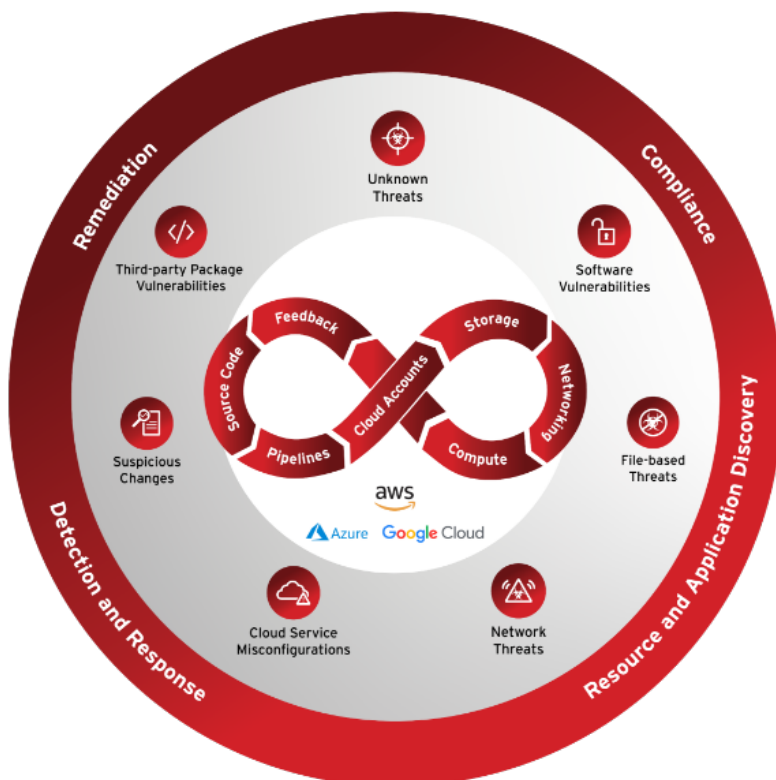


Abb. 9: Trend Vision One™ - Companion Alarmanalyse

Companion ist eine intuitive Plattform, die eine generative KI nutzt, um Anwendern aller Qualifikationsstufen robuste analytische Fähigkeiten zu bieten. Sie verfügt über wertvolle Funktionen, wie z. B. Kontextualisierung und Erläuterung von Warnungen, Priorisierung und Empfehlung von Maßnahmen, Dekodierung komplexer Skripte sowie Entwicklung und Test fortgeschrittener Suchanfragen. Mit Companion können Sie problemlos durch komplexe Daten navigieren und wertvolle Erkenntnisse gewinnen, auch wenn Sie nicht über fortgeschrittene technische Kenntnisse verfügen.

Schutz von (hybriden) Cloud-Infrastrukturen

Cloud-Infrastrukturdienste wachsen schnell, deshalb müssen immer mehr Beteiligte in Entscheidungen über die Infrastruktur und Sicherheit einbezogen werden. Um Geschäftsziele zu erreichen und die Vorteile der Cloud wirklich auszuschöpfen, sollte Cloud-Sicherheit daher vereinfacht werden. Geschäftsanforderungen und DevOps-Prozesse erfordern eine schnellere



Bereitstellung von Anwendungen. Wenn aber die Bereitstellungsgeschwindigkeit steigt, müssen auch alle anderen Aspekte Schritt halten. Dazu gehören die Compliance, die sich je nach Branche, Standort und Infrastruktur ändert, und der Schutz vor neuen und immer komplexeren Bedrohungsvektoren. In dieser Situation ist es wenig sinnvoll, auf Punktlösungen zu setzen, die nur einzelne Anforderungen der Infrastruktur erfüllen. Auch das Beharren auf bestehenden Prozessen führt nicht weiter. Die **Trend Vision One™ Cloud-Sicherheitsplattform** bietet hingegen ein umfassendes Angebot an Services, die speziell für die Cloud entwickelt wurden. Mit Trend Vision One™ schützen Sie die verschiedenen Aspekte Ihrer Umgebung über eine einzige, einfach zu bedienende Plattform.

Abb. 10: Trend Vision One™ Cloud-Sicherheitsplattform

Telemetrie ermöglicht Cloud Detection and Response (CDR) und erweitert XDR auf Cloud-Anbieter und Cloud-native Technologien, einschließlich Workloads, Containern, File Storage und Cloud-Netzwerkverkehr. On-Demand- und Laufzeitschutz für die Hybrid-Cloud umfassen Integritätsüberwachung, Anwendungskontrolle, Virtual Patching, Intrusion Prevention, Compliance, Anti-Malware und Container Security. Damit können Sie Schwachstellen und Malware in allen Workloads erkennen und blockieren, inklusiven Servern, Containern und Pipelines, IAC-Speicher, VPC und Datenbanken. Sie erhalten Einblick in Ihre Container-Angriffsoberfläche und in die Risiken innerhalb von Containern. Das ermöglicht Schutz für den gesamten Lebenszyklus, während Sie Laufzeitbedrohungen und andere verdächtige Aktivitäten erkennen und Reaktionen einleiten, inklusive Schwachstellen, Ransomware, SBOM-Scans, Image-Scans und Drift-Erkennung.

Phish Insight

Immer noch beginnen 91 % der Datenschutzverletzungen mit einer Phishing-E-Mail. Es ist wichtig, Schwachstellen vor den Cyberkriminellen zu erkennen. Indem Sie Ihre Mitarbeiter mit fingierten Phishing-E-Mails schulen, können Sie individuelle Schwachstellen von Mitarbeitern erkennen und Maßnahmen ergreifen, um den Schutz zu verbessern.

Phish Insight ist eine Komplettplattform, die kulturell angepasste Phishing-Vorlagen in mehreren Sprachen bietet. Die automatisierten Simulationen basieren auf realen Bedrohungen und können auf die Bedürfnisse Ihres Unternehmens zugeschnitten werden. Mit randomisierten Kampagnen und leistungsstarken Dashboards lassen sich die aktuelle Fähigkeiten Ihrer Mitarbeiter sowie die Fortschritte im Umgang mit Phishing-Angriffen messen. Die Plattform bietet außerdem Schulungen in verschiedenen Formaten und Sprachen. Die Kommunikation ist anpassbar und die leicht verständlichen Dashboards ermöglichen die Nachverfolgung von Teilnahme und Quiz-Ergebnissen. Beginnen Sie noch heute mit der Planung Ihres Schulungsprogramms!

Trend Service One™

Da Cyberangriffe immer komplexer und ausgefeilter werden, müssen Sicherheitsteams in der Lage sein, Bedrohungen schnell zu erkennen und passende Reaktionen einzuleiten. Trend Service One filtert Fehlalarme und liefert qualitativ hochwertige Alarme, die von globalen Bedrohungsanalysten mit neuesten Threat-Hunting-Techniken verifiziert wurden. Mit diesem Werkzeug entlasten Sie Teams, die sich wieder ganz auf Innovationen und die Erreichung von Geschäftszielen konzentrieren können.

Trend Service One ist eine umfassende Cybersicherheitslösung, die eine ganze Reihe von Vorteilen kombiniert, darunter Premium Support Services, globale 24/7-Unterstützung mit priorisierter Fallbehandlung, ein designierter Service Manager sowie ein exklusiver Onboarding Service.

Darüber hinaus ermöglicht Trend Service One die Erkennung gezielter Angriffe (Targeted Attack Detection). Kontinuierlich suchen Bedrohungsanalysten nach frühen Gefährdungsanzeichen (Indicators of Compromise, IoC) und liefern validierte Hoch-Risiko-Warnungen. Die Cybersecurity-Experten von Trend Service One sind ständig auf der Suche nach Bedrohungen und verdächtigen Aktivitäten. Aus all Ihren Trend Lösungen werden Daten korreliert, um mit schnellen Reaktionen und geführten Anleitungen Ihren Schutz zu erweitern.

Darüber hinaus bietet Service One einen Incident Response Service, der Ihnen jederzeit mit Experten und modernsten Werkzeugen zur Seite steht, um Cyberangriffe einzudämmen und zu beherrschen. Trend Service One Kunden erhalten priorisierten Zugang zum Incident Response Team und können bei Bedarf garantierten Zugang hinzufügen.

Außerdem bietet Trend standardisierte und maßgeschneiderte Produktschulungen sowie ein vollständig anpassbares Phishing-Simulationstool, um Ihre Mitarbeiter in den Best Practices der Cybersicherheit zu schulen und das Risiko menschlicher Fehler zu verringern.

Trend Service One liefert Unternehmen die Cybersicherheitslösungen, -services und -kenntnisse, die sie benötigen, um NIS2 zu erfüllen und die allgemeine Security Posture zu verbessern.

04

Anhang

Anhang

Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen (CER)

Die Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen (**(EU) 2022/2557**) verpflichtet die EU-Mitgliedstaaten, die Funktionsfähigkeit von Einrichtungen sicherzustellen, wenn diese wesentliche Dienstleistungen zur Aufrechterhaltung lebenswichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten im Binnenmarkt erbringen. Bestimmte Wirtschaftssektoren, wie Energie und Verkehr, waren früher bereits Gegenstand von sektorspezifischen Regelungen, die sich aber nur auf bestimmte Aspekte der Widerstandsfähigkeit erstreckten.

Die Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen bietet nun einen übergreifenden Rahmen, der die Widerstandsfähigkeit kritischer Einrichtungen gegenüber allen natürlichen oder vom Menschen verursachten, zufälligen oder vorsätzlichen Gefahren adressiert.

Kritische Einrichtungen müssen die relevanten Risiken, denen sie ausgesetzt sind, umfassend verstehen und analysieren. Um dies zu erreichen, müssen sie Risikobewertungen unter Berücksichtigung ihrer besonderen Umstände und der Entwicklung dieser Risiken durchführen. Alle vier Jahre muss eine Risikobewertung für kritische Unternehmen durchgeführt werden, um alle relevanten Risiken zu identifizieren, die eine Unterbrechung wesentlicher Dienstleistungen verursachen könnten.

Einrichtungen, die ansonsten nicht in den Anwendungsbereich der NIS2 fallen, können ebenfalls in den Anwendungsbereich dieser Richtlinie fallen.

Digital Operational Resilience Act (DORA)

Der Digital Operational Resilience Act (**Verordnung (EU) 2022/2554**) löst ein kritisches Problem in der EU-Finanzregulierung. Vor DORA war die Kapitalallokation die primäre Methode, die von Finanzinstituten für das Management operationeller Risikokategorien verwendet wurde. Allerdings berücksichtigte dieser Ansatz nicht alle Komponenten der operationellen Widerstandsfähigkeit. Mit der Einführung von DORA müssen die Finanzinstitute strenge Vorschriften für Schutz, Erkennung, Eindämmung, Wiederherstellung und Reparatur von IKT-bezogenen Vorfällen befolgen. DORA befasst sich speziell mit dem IKT-Risikomanagement, der Meldung von Vorfällen, dem Testen der operationellen Widerstandsfähigkeit und der IKT-Risikoüberwachung durch Dritte.









Die Verordnung erkennt an, dass IKT-Vorfälle und ein Mangel an operativer Widerstandsfähigkeit die Stabilität des gesamten Finanzsystems bedrohen können, selbst wenn für traditionelle Risikokategorien „angemessenes“ Kapital vorhanden ist. DORA stützt sich auf die NIS2-Richtlinie, vermeidet aber Überschneidungen, indem eine Lex-Specialis-Ausnahme für Banken und Infrastrukturorganisationen des Finanzmarktes eingeführt wird. DORA wird am 17. Januar 2025 in Kraft treten und für die betroffenen Unternehmen unmittelbar gelten.











Zuordnung von Anforderungen und Trend Micro Lösungen

Referenz	Maßnahmen	Trend Micro Lösungen
Art. 21(2.a)	Regeln zur Risikoanalyse und Sicherheit von Informationssystemen	Trend Vision One™ - Attack Surface Risk Management (ASRM) Identifikation von internen und externen Identitäten, Diensten, Geräten und Konfigurationen. Risiko-Assessment auf Basis von Sicherheitsinformationen. Umfassender Bericht zur Priorisierung von Aktivitäten und Risikominimierung.
Art. 21(2.b)	Incident Handling	Trend Vision One™ - XDR und Trend Service One™ Complete Trend Micro bietet verschiedene Services zur Erkennung potenzieller Cyberangriffe und Einleitung angemessener Reaktionen. Mit Managed XDR erhalten Sie rund um die Uhr Überwachung und Reaktion durch das Trend Micro Expertenteam. Targeted Attack Detection überwacht proaktiv die Datenbank von Trend Micro auf Anzeichen für potenzielle Angriffe. Breach Assessment liefert gezielte Analysen von Bewegungen, die wahrscheinlich im Zusammenhang mit einem Angriff stehen. Im Falle eines Vorfalls können Sie darüber hinaus das Trend Micro Incident Response Team nutzen, um schnell und effektiv zu reagieren.
Art. 21(2.c)	Business-Kontinuität	Trend Vision One™ Die Trend Vision One™ Cybersicherheitsplattform umfasst die Bereiche Governance, Identifikation, Schutz, Erkennung und Reaktion. Lösungen von Drittanbietern decken die Wiederherstellung ab.

Art. 21(2.d)	Supply-Chain-Sicherheit	<u>Trend Vision One™ - Zero Trust Secure Access (ZTSA)</u> Prozesse für Risikobewertung, Verifizierung der digitalen Identität und Überprüfung von Gerätezugriffen werden genutzt, um Verbindungsanfragen zu bewerten. Der Zugang zum WWW, zu SaaS oder zu privaten Rechenzentren wird nur unter bestimmten Bedingungen gestattet, wobei das Risiko ständig neu bewertet wird. Der Zugriff von nicht verwalteten Geräten kann über sichere Webportale geleitet werden, um einen Zugang zur Supply Chain zu implementieren.
Art. 21(2.e)	Sicherheit bei der Akquisition, Entwicklung und Wartung von Netzwerk- und Informationssystemen	<u>Trend Vision One™ und Trend Cloud One™</u> Die Module von Trend Micro Endpoint & Workload Security werden zum Schutz lokaler Assets eingesetzt. Die neuen Herausforderungen in agilen Entwicklungsprozessen erfordern jedoch projektzentrierte Ansätze, um individuelle Probleme zu lösen. Dies beinhaltet die Integration von Cloud Attack Surface Management, Cloud Detection & Response sowie Schutz vor bekannten und unbekanntem Bedrohungen des Entwicklungsprozesses und der Code-Entwicklung.
Art. 21(2.f)	Richtlinien und Prozeduren für die Bewertung der Effizienz von Maßnahmen des Cybersicherheitsmanagements	<u>Trend Service One™</u> Frühzeitiger Kontakt, noch vor dem Kauf, durch Capture-the-Flag-Veranstaltungen. Red/Blue/Purple Teaming & Security Assessments auf der Vision One Plattform. Breach Assessment Partner & Incident Response Provider.
Art. 21(2.g)	Grundlegende Verfahren der Cyber-Hygiene sowie Cybersicherheits-trainings	<u>Trend Micro Education Division, Trend Micro Phish Insight und Trend Vision One™</u> Unsere Trainingsabteilung bietet technische Schulungen für Kunden, Partner und Mitarbeiter. Phish Insight stärkt das Unternehmensbewusstsein für Informationssicherheit und befähigt Mitarbeiter, die neuesten Bedrohungen zu erkennen und sich vor ihnen zu schützen. Vision One Companion, ein KI-Assistent, fördert die Sicherheit und unterstützt Analyseschritte mit Produktschulungen und toolbasierten Assessments.
Art. 21(2.j)	Multi-Faktor-Authentifizierung oder Lösungen für Continuous Authentication	<u>Trend Vision One™ - Zero Trust Secure Access (ZTSA)</u> Sicherer Zugriff auf Internet-Ressourcen, Cloud-Anwendungen und E-Mail durch kontinuierliche Überwachung von MFA und Risikobewertung.
Art. 23(4.a)	24h Frühwarnung	<u>Trend Vision One™</u> Die Trend Vision One™ Cybersicherheitsplattform bietet ein breites Funktionsspektrum für Threat Hunting und Incident Response. Es werden detaillierte Informationen zur Bewertung der Schwere und Auswirkungen von Vorfällen bereitgestellt sowie auch weiteres umfassendes Datenmaterial, einschließlich Indicators of Compromise (IoC).
Art. 23(4.b)	72h Benachrichtigung über Vorfälle	
Art. 23(4.c)	Informationsanfragen	
Art. 23(4.d)	Abschlussbericht	
Art. 23(4.e)	Fortschrittsbericht	

NIS2-Sektoren

Sektor	Subsektor	Große Einrichtungen	Mittlere Einrichtungen	Kleine & Kleinst-einrichtungen	
Anhang 1: Sektoren mit hoher Kritikalität					
Energie 	Elektrizität	Wesentlich	Wichtig	Keine Anwendung	NIS
	Fernwärme und Kühlung	Wesentlich	Wichtig	Keine Anwendung	NIS2
	Öl	Wesentlich	Wichtig	Keine Anwendung	NIS
	Gas	Wesentlich	Wichtig	Keine Anwendung	NIS2
	Wasserstoff	Wesentlich	Wichtig	Keine Anwendung	NIS2
Transport 	Luftfahrt (kommerzielle Fluglinien, Flughäfen, Luftverkehr)	Wesentlich	Wichtig	Keine Anwendung	NIS2
	Schienerverkehr (Infrastruktur und Unternehmungen)	Wesentlich	Wichtig	Keine Anwendung	NIS
	Schifffahrt (Transportunternehmen, Häfen, Verkehrsservices)	Wesentlich	Wichtig	Keine Anwendung	NIS
	Straßenverkehr (ITS und Ladestationen)	Wesentlich	Wichtig	Keine Anwendung	NIS
	Öffentlicher Transport (nur CER)	Wesentlich	Wichtig	Keine Anwendung	NIS2
Bankwesen 	Kreditinstitute (DORA Lex Specialis)	Wesentlich	Wichtig	Keine Anwendung	NIS
Finanzmarkt-Infrastrukturen 	Handelsplätze, zentrale Handelsgegenparteien	Wesentlich	Wichtig	Keine Anwendung	NIS
Gesundheitswesen 	Anbieter im Gesundheitswesen	Wesentlich	Wichtig	Keine Anwendung	NIS
	EU-Referenzlaboratorien; Forschung und Entwicklung von Arzneimitteln; Herstellung von pharmazeutischen Grundstoffen und pharmazeutischen Zubereitungen (Abschnitt C, Abteilung 21 der NACE Rev. 2); Herstellung medizinischer Geräte, die bei einem Notfall im Bereich der öffentlichen Gesundheit kritisch sind	Wesentlich	Wichtig	Keine Anwendung	NIS2
	Einrichtungen, die eine Vertriebsgenehmigung für Arzneimittel besitzen (Sonderfall nur bei CER)	Wesentlich	Wichtig	Keine Anwendung	NIS2
Trinkwasser 		Wesentlich	Wichtig	Keine Anwendung	NIS
Abwasser 	(nur wenn es ein wesentlicher Teil ihrer allgemeinen Tätigkeit ist)	Wesentlich	Wichtig	Keine Anwendung	NIS2
Digitale Infrastrukturen 	Qualifizierte Anbieter von Vertrauensdiensten	Wesentlich	Wesentlich	Wesentlich	NIS2
	DNS Service Provider (ausgenommen Root Name Server)	Wesentlich	Wesentlich	Wesentlich	NIS
	TLD Name-Registrare	Wesentlich	Wesentlich	Wesentlich	NIS
	Anbieter öffentlicher elektronischer Kommunikationsnetze	Wesentlich	Wesentlich	Wichtig	NIS2
	Nicht-qualifizierte Anbieter von Vertrauensdiensten	Wesentlich	Wichtig	Keine Anwendung	NIS2
	Internet Exchange Point Provider	Wesentlich	Wichtig	Keine Anwendung	NIS2
	Cloud Computing Service Provider	Wesentlich	Wichtig	Keine Anwendung	NIS2
	Data Center Service Provider	Wesentlich	Wichtig	Keine Anwendung	NIS2
	Content Delivery Network Provider	Wesentlich	Wichtig	Keine Anwendung	NIS2

Sektor	Subsektor	Große Einrichtungen	Mittlere Einrichtungen	Kleine & Kleinst-einrichtungen	
IKT Service Management 	Managed Service Provider, Managed Security Service Provider	Wesentlich	Wichtig	Keine Anwendung	NIS2
Öffentliche Verwaltung 	Bundeseinrichtungen (ausgenommen Justiz, Parlamente, Zentralbanken, Verteidigung, nationale oder öffentliche Sicherheit)	Wesentlich	Wesentlich	Wesentlich	NIS2
	Landesbehörden und -verwaltungen	Wichtig	Wichtig	Wichtig	NIS2
	(Optional für Mitgliedsstaaten: lokale Einrichtungen)	Wesentlich	Wichtig	Keine Anwendung	NIS2
Raumfahrt 	Betreiber bodengestützter Infrastrukturen (nach Mitgliedstaaten)	Wesentlich	Wichtig	Keine Anwendung	NIS2
Anhang 2: Andere kritische Sektoren					
Post und Kurierdienste 		Wichtig	Wichtig	Keine Anwendung	NIS2
Abfallmanagement 	(nur wenn Hauptwirtschaftstätigkeit)	Wichtig	Wichtig	Keine Anwendung	NIS2
Chemische Industrie 	Produktion und Distribution	Wichtig	Wichtig	Keine Anwendung	NIS2
Lebensmittel 	Produktion, Verarbeitung und Distribution	Wichtig	Wichtig	Keine Anwendung	NIS2
Produktion 	Medizingeräte und Geräte für In-Vitro-Diagnostik	Wichtig	Wichtig	Keine Anwendung	NIS2
	Computer, elektronische und optische Erzeugnisse (Abschnitt C, Abteilung 26 der <u>NACE Rev. 2</u>)	Wichtig	Wichtig	Keine Anwendung	NIS2
	Elektrische Anlagen (Abschnitt C Abteilung 27 der <u>NACE Rev. 2</u>)	Wichtig	Wichtig	Keine Anwendung	NIS2
	Maschinen und Anlagen, a.n.g. (Abschnitt C Abteilung 28 der <u>NACE Rev. 2</u>)	Wichtig	Wichtig	Keine Anwendung	NIS2
	Kraftfahrzeuge, Anhänger und Sattelanhänger (Abschnitt C, Abteilung 29 der <u>NACE Rev. 2</u>)	Wichtig	Wichtig	Keine Anwendung	NIS2
	Sonstiger Fahrzeugbau (Abschnitt C Abteilung 30 der <u>NACE Rev. 2</u>)	Wichtig	Wichtig	Keine Anwendung	NIS2
Digitale Provider 	Online-Marktplätze, Suchmaschinen, soziale Netzwerke	Wichtig	Wichtig	Keine Anwendung	NIS2
Forschung 	Forschungseinrichtungen (ohne Bildungseinrichtungen)	Wichtig	Wichtig	Keine Anwendung	NIS2
	(Optional für Mitgliedsstaaten: Bildungseinrichtungen)	Wichtig	Wichtig	Keine Anwendung	NIS2
Einrichtungen, die Domain Name Registration Services bereitstellen					

Für weitere Informationen besuchen Sie bitte: www.trendmicro.com/de_de

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: www.trendmicro.com/de_de/about/trust-center/privacy/notice.html