Trellix

KURZVORSTELLUNG

NIS2-Richtlinie

Mit Trellix® die Cyber-Resilienz und Cyber-Compliance steigern

Was ist die NIS2-Richtlinie?

Die Richtlinie EU 2022/2555, besser bekannt als „NIS2-Richtlinie“ ist eine EU-Richtlinie, die das Ziel hat, die Cyber-Sicherheit und Cyber-Resilienz in der gesamten EU zu verbessern. Es handelt sich nicht um ein Framework für konkrete Sicherheitskontrollen, sondern um einen vorgeschriebenen kontinuierlichen Ansatz für die Risikoverwaltung, mit dem der Reifegrad der Cyber-Sicherheitsmaßnahmen, die Zwischenfallverwaltung und der Austausch von Informationen in Unternehmen der kritischen Infrastruktur und den Mitgliedsstaaten konsistent verbessert werden sollen.

Wer ist von der NIS2-Richtlinie betroffen?

Die Liste der von der NIS2-Richtlinie betroffenen Unternehmensarten ist umfangreich und umfasst Einrichtungen aus Sektoren, die grundlegende Dienstleistungen bereitstellen, z. B. Energieversorgung, Transportwesen, Bankwesen, Gesundheitswesen, Wasserversorgung, digitale Infrastruktur sowie die öffentliche Verwaltung. Dazu zählen zudem Einrichtungen, die wichtige Dienstleistungen bereitstellen, z. B. Post- und Kurierdienste, Abfallbewirtschaftung, Herstellung und Handel mit chemischen Stoffen, Informations- und Kommunikationstechnologien (IKT), Produktion, Verarbeitung und Vertrieb von Lebensmitteln sowie bestimmte Fertigungsunternehmen. Eine vollständige Liste der betroffenen Unternehmen finden Sie im Volltext der NIS2-Richtlinie.

Welche Vorteile bietet Trellix bei der Einhaltung der NIS2-Vorgaben?

Trellix beschleunigt die Implementierung der NIS2-Vorgaben. Trellix Helix stellt Funktionen zur Erkennung und Abwehr von Bedrohungen bereit, die Informationstechnologie (IT), operative Technologie (OT) und die Cloud abdecken, um die Transparenz in Ihrem Unternehmen zu steigern. Für Analysen integriert Trellix Helix Daten von Trellix-Sensoren und mehr als 500 externen Anbietern, um Bedrohungen aus mehreren Vektoren basierend auf Daten von mehreren Anbietern zu erhalten und mit KI-gestützter Automatisierung die Reaktion auf Vorfälle zu beschleunigen. Das komplette Trellix-Sicherheitsportfolio stellt die erweiterten Sicherheitskontrollen zur Verfügung, die für verbesserte Cyber-Hygiene für Endgeräte, Server, Netzwerke, Daten, Cloud und Mobilgeräte erforderlich sind. Die Trellix Consulting Services können Ihr aktuelles Sicherheitsprogramm dahingehend bewerten, ob internationale und europäische Standards eingehalten werden. Außerdem erhalten Sie Bewertungen Ihres aktuellen Reifegrads sowie Bedrohungsdaten, die kontinuierliche Risikoanalysen ermöglichen.

Die Compliance-Anforderungen können je nach den Anwendungsleitlinien für den jeweiligen Mitgliedsstaat variieren, doch zur Einhaltung der NIS2-Compliance ist es in jedem Fall erforderlich, die Cyber-Risiken zu reduzieren und die Resilienz zu steigern. Nachfolgend stellen wir die fünf Bereiche vor, in denen Trellix (in Zusammenarbeit mit Lösungen unserer Partner) Sie unterstützen kann, die NIS2-Vorgaben einzuhalten und Ihr Risiko durch neue Bedrohungen zu reduzieren.

Identifizierung Ihrer Risiken mit Trellix Assessment Services

Die NIS2-Richtlinie schreibt vor, dass Unternehmen Risikobewertungen durchführen und internationale oder europäische Standards wie ISO 27001 bzw. „koordinierte Rahmen für die Cyber-Sicherheit“ wie das Cyber-Sicherheits-Framework NIST umsetzen müssen, um Cyber-Risiken kontinuierlich reduzieren zu können. Es ist daher wichtig, Ihren aktuellen Status bei der Einhaltung dieser Standards sowie den Reifegrad Ihrer Sicherheitsmaßnahmen in potenziell hochriskanten Bereichen zu bewerten. Nach unserer Erfahrung und uns vorliegenden Trellix-Bedrohungsdaten empfehlen wir, dass Sie sich auf diese fünf Bewertungen konzentrieren:

Trellix-Services	Beschreibung des Service-Angebots	NIS2-Artikel
Cybersecurity Assessment	Bewertung des Reifegrads in Bezug auf internationale Standards und Festlegung von Richtlinien für Informationssicherheit	20.2, 21.1, 21.2a
Intelligence as a Service	Identifizierung gezielter Bedrohungen, die Ihr Unternehmen gefährden	20.2, 21.1, 21.2a
Ransomware Readiness Assessment	Individuelle Tabletop-Übungen zur Bewertung Ihres Ransomware-Risikos	20.2, 21.1, 21.2a, 21.2c, 21.2f
SOC Readiness Assessment	Entwicklung eines Programms zur Reaktion auf Vorfälle, SOC-Bewertung und -Konzeption sowie Unterstützung bei der Reaktion auf Vorfälle in einem Notfall	20.2, 21.2a, 21.2b, 21.2f
Web Application Assessment	Bewertung von DevSecOps-Prozessen und externen Anwendungen	20.2, 21.2a, 21.2f

Vereinbaren Sie einen Termin mit unserem Trellix Assessment Services-Team über Ihren Trellix-Vertreter oder unter www.trellix.com.

Aufbau von Ransomware-Resilienz

Unser Trellix Cyberthreats-Report beschreibt die Auswirkungen aktueller Ransomware-Angriffe. Ransomware ist eine schwerwiegende Bedrohung für Anbieter grundlegender Dienstleistungen, die der NIS2-Richtlinie unterliegen. Schlagzeilenträchtige Angriffe richten sich gegen Energieversorger, Transportwesen, Einrichtungen der öffentlichen Verwaltung sowie gegen andere Branchen und führen zu Unterbrechungen bei grundlegenden Dienstleistungen. Unternehmen benötigen daher zuverlässige Schutzmaßnahmen zur Vermeidung, Erkennung und schnellen Abwehr von Ransomware-Angriffen. Zusätzlich zu den Trellix Ransomware Readiness Assessments empfehlen wir die folgenden Trellix-Lösungen, um Lücken im Malware-Schutz zu schließen und das Ransomware-Risiko für Geschäftsabläufe zu reduzieren:

Trellix-Lösungen	Beschreibung der Lösung	NIS2-Artikel
Trellix Endpoint Security und Trellix EDRF	Erweiterter Ransomware-Schutz und Erkennung für Endbenutzer-Systeme, Server und Mobilgeräte	21.1, 21.2b, 21.2c, 21.2f, 21.2g, 21.2h, 21.2i, 21.2j
Trellix IVX for Collaboration Platforms	Vermeidung und Erkennung von Ransomware bei Phishing-E-Mails und über Anwendungen für die Zusammenarbeit	21.2g, 21.2j
Trellix File Protect	Identifizierung von Ransomware, die sich in Massenspeichern und in unternehmensspezifischen Geschäftsanwendungen verbergen	21.2c, 21.2g
Trellix Network Security	Verhinderung und Erkennung von Bewegungen innerhalb des Netzwerks und von nachgelagerten Ransomware-Techniken	21.2e, 21.2b
Trellix Helix	Integration und Analyse von Daten aus Trellix- und Drittanbieter-Tools, um die Erkennung und Reaktion auf Ransomware zu beschleunigen	21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j

Wenn Sie mehr darüber erfahren möchten, wie Trellix Ihr Unternehmen vor Ransomware schützen kann, besuchen Sie bitte www.trellix.com.

Beschleunigung der Bedrohungserkennung und Reaktion durch SecOps

Eines der primären Ziele der NIS2-Richtlinie ist die Verbesserung der Erkennung und Behebung von Zwischenfällen im gesamten Unternehmen. Viele Betreiber grundlegender Dienstleistungen sehen sich wahrscheinlich mit typischen Herausforderungen in Bezug auf Sicherheitskontrollzentren (Security Operation Centers, SOCs) konfrontiert, z. B. Transparenzlücken, Fachkräftemangel und fehlender Automatisierung. Unsere Bewertungen von SOCs und Programmen zur Reaktion auf Vorfälle decken diese Lücken auf und helfen Ihnen bei der Entwicklung eines Plans, mit dem diese Lücken geschlossen werden und der Reifegrad des Programms gesteigert wird.

Aus technologischer Sicht entlastet Trellix Helix mit der integrierten KI Trellix Wise die Analysten und reduziert die mittlere Reaktionszeit (Mean Time to Respond, MTTR) mit einer offenen Sicherheitsplattform, die Daten von Trellix-Sensoren und mehr als 500 Integrationen erfasst. Wir reichern diese Informationen mit integrierten Bedrohungsdaten und KI-gestützer Automatisierung an, um für alle IT-, OT- und Cloud-Netzwerke schnelle Erkennung und Reaktion zu ermöglichen. Zusätzlich zu Trellix Helix und SOC-Bewertungen empfehlen wir die folgenden Trellix-Lösungen zur Bereitstellung vollständiger Transparenz und Bedrohungserkennung für das gesamte Unternehmen:

Trellix-Lösungen	Beschreibung der Lösung	NIS2-Artikel
Trellix EDRF und Trellix Endpoint Forensics	Bereitstellung von umfassender Endgerätetransparenz, Erkennung böswilliger Aktivitäten und Forensik für die Reaktion auf Vorfälle	21.2b, 21.2g
Trellix NDR und Trellix Network Forensics	Bereitstellung von vollständiger Netzwerk-Paketerfassung und Erkennung böswilliger Netzwerkaktivitäten	21.2e, 21.2b
Trellix IVX for Enterprise Applications	Stark skalierbare Cloud-Malware-Analysen	21.2b, 21.2g
Trellix Helix	Integration und Analyse von Daten aus Trellix- und Drittanbieter-Tools mit integrierten Bedrohungsdaten, KI und Analysen, um die mittlere Zeit für Erkennung und Reaktion (MTTD und MTTR) zu verkürzen	21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j
Trellix Second Sight	Proaktiver Service, der nach neuen Bedrohungen sucht und Kunden bei potenziellen neuen Zwischenfällen warnt, sodass die Verweildauer von Angreifern deutlich reduziert wird	21.2a, 21.2b, 21.2c, 21.2d, 21.2e, 21.2f, 21.2g
Semperis (Partner)	Schutz für Verzeichnisdienste und Integration mit Trellix Helix für Funktionen zur Erkennung und Reaktion für Identitäten	21.2g, 21.2i

Schutz für Ihre OT-Netzwerke und -Systeme

Viele Einrichtungen, die grundlegende Dienstleistungen bereitstellen und der NIS2-Richtlinie unterliegen, betreiben OT-Systeme und -Netzwerke. Diese OT-Systeme sind für den Geschäftsbetrieb des Unternehmens unverzichtbar und heute das Ziel von Bedrohungsakteuren. Die Risiken für operative Technologien sind besonders hoch, da Sicherheitskontrollen häufig nur unzureichend vor hochentwickelten Bedrohungen schützen. Zudem wird die OT-Sicherheitsüberwachung typischerweise nicht von den IT-Sicherheitsteams, sondern von unerfahrenen Anwendern durchgeführt. Das Trellix-Sicherheitsportfolio hilft Ihnen bei der Absicherung Ihrer kritischen OT-Systeme. Trellix Endpoint Security bietet grundlegende und erweiterte Kontrollen für OT-Systeme und ist von jedem großen SCADA-Hersteller (Supervisory Control and Data Acquisition) zertifiziert.

Endgerätesicherheit allein bietet jedoch keinen ausreichenden Schutz. Stattdessen benötigen Unternehmen einen Überblick über ihre Ressourcen, Netzwerksicherheitskontrollen am Perimeter sowie Überwachungsfunktionen zur Erkennung von ungewöhnlichem Verhalten. Zusätzlich zu Trellix Endpoint Security empfehlen wir die folgenden Trellix-Lösungen, um Lücken im Malware-Schutz zu schließen, einen Überblick über ihre SCADA-Ressourcen zu erhalten und potenzielle Bedrohungen zu erkennen:

Trellix-Lösungen	Beschreibung der Lösung	NIS2-Artikel
Trellix Endpoint Security	Erweiterter Ransomware-Schutz für Endbenutzer-Systeme, Server und Mobilgeräte	21.1, 21.2b, 21.2c, 21.2f, 21.2g, 21.2h, 21.2i, 21.2j
Trellix Embedded Security	Erweiterter Ransomware-Schutz für Endbenutzergeräte und Server in OT-Umgebungen	21.1, 21.2b, 21.2c, 21.2f, 21.2g, 21.2h, 21.2i, 21.2j
Trellix Network Detection and Response Security	Erkennung böswilliger Netzwerkaktivitäten zwischen IT- und OT-Netzwerken	21.2e, 21.2b
Nozomi Networks (Partner), Tenable (Partner), Armis (Partner)	Erkennung von Details zu SCADA-Ressourcen und Schwachstellen, Integration mit Trellix NDR und Trellix ePO für die Erkennung und Abwehr von Bedrohungen	21.2b, 21.2c, 21.2e
Trellix Helix	Integration und Analyse von Daten aus Trellix- und Drittanbieter-Tools, um die Erkennung und Reaktion auf Zwischenfälle in OT- und IoT-Netzwerken zu beschleunigen	21.2b, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j

Wenn Sie mehr darüber erfahren möchten, wie Trellix Ihre OT-Systeme schützen kann, besuchen Sie bitte www.trellix.com.

Reduzierung der Risiken durch Datenkompromittierungen

Der Schutz vertraulicher und proprietärer Daten wird immer schwerer. Zunächst einmal befinden sich die Daten überall – in Kundenanwendungen, Cloud-Speichern, Datenbanken und auf privaten Geräten. Zudem sind diese Daten durch externe und interne Bedrohungen gefährdet. Externe APT-Akteure nutzen KI, um schneller Exploits zu erstellen. Dadurch sind Ihre vertraulichen Kunden- und Unternehmensdaten durch anfällige Anwendungen gefährdet. Darüber hinaus wächst das Risiko durch versehentliche und böswillige Datenkompromittierungen durch Insider. All diese Faktoren erhöhen die Wahrscheinlichkeit, dass eine Kompromittierung oder ein Datenverlust gemeldet werden muss. Da die NIS2-Richtlinie kurze Fristen für die Meldung von Datenkompromittierungen vorschreibt, müssen Sie sich auf die Verbesserung Ihres Programms für Datensicherheit konzentrieren.

Trellix Consulting Services kann Sie beim Start Ihres Datensicherheitsprogramms unterstützen, indem die Prioritäten in Bezug auf die Sicherheit Ihrer Unternehmensdaten mit den Schutzkontrollen abgestimmt werden. Zudem kann Trellix DLP Discover Ihr Netzwerk sowie Repositorys wie SharePoint scannen, um die Transparenz und Klassifizierung zu verbessern. Außerdem empfehlen wir Ihnen die Implementierung der folgenden Trellix-Lösungen für Datensicherheit, mit denen die Risiken für Datenkompromittierungen vom Endgerät bis zur Cloud minimiert werden:

Trellix-Lösungen	Beschreibung der Lösung	NIS2-Artikel
Trellix Data Loss Prevention (DLP) Endpoint Complete, Trellix Drive Encryption, Trellix File and Removable Media Protection	Erkennung und Klassifizierung von Daten, Schutz vor Datenverlust auf Endgeräten, Verschlüsselung abgelegter Daten	21.2h, 21.2i
Trellix DLP Network Suite	Erkennung und Klassifizierung von Daten, Schutz vor Datenverlust im gesamten Netzwerk	21.2i
Trellix Database Security	Überwachung und Kontrolle von Zugriffen auf vertrauliche Informationen in Anwendungsdatenbanken	21.2i
Trellix AI Risk Dashboard	Erkennung und Überwachung der Nutzung von KI-Diensten	21.2a
Skyhigh Security (Partner)	Überwachung und Kontrolle von Zugriffen auf vertrauliche Informationen in Cloud-Anwendungen	21.2d, 21.2i, 21.2j

Wenn Sie mehr über Trellix und NIS2 erfahren möchten, besuchen Sie bitte www.trellix.com, oder vereinbaren Sie einen Workshop bei Ihrem Trellix-Vertreter.