Trellix

KURZVORSTELLUNG

NIS-2-Richtlinie

Mit Trellix die Cyber-Resilienz und Cyber-Compliance steigern

Was ist die NIS-2-Richtlinie?

Die Richtlinie EU 2022/2555, besser bekannt als „NIS-2-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, das Incident-Management und der Austausch von Informationen in Unternehmen der kritischen Infrastruktur und den Mitgliedsstaaten konsistent verbessert werden sollen.

Wer ist von der NIS-2-Richtlinie betroffen?

Die Liste der von der NIS-2-Richtlinie betroffenen Unternehmensarten ist umfangreich und umfasst Einrichtungen aus Sektoren, die grundlegende Dienstleistungen bereitstellen, z. B. Energieversorgung, Transportwesen, Bankwesen, Gesundheitswesen, Wasserversorgung, digitale Infrastruktur und 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 NIS-2-Richtlinie.

Welche Vorteile bietet Trellix bei der Einhaltung der NIS 2-Vorgaben?

Trellix beschleunigt die Implementierung der NIS 2-Vorgaben. Trellix Helix Connect stellt erweiterte Funktionen zur Erkennung und Abwehr von Bedrohungen (eXtended Threat Detection and Response, XDR) bereit, die Informationstechnologie (IT), operative Technologie (OT) und die Cloud abdecken, um die Transparenz in Ihrem Unternehmen zu steigern. Für Analysen integriert Trellix Helix Connect Daten von Trellix-Sensoren und mehr als 490 externen Anbietern, um Bedrohungen aus mehreren Vektoren basierend auf Daten von mehreren Anbietern zu erhalten und KI-gestützte Automatisierung anzubieten, die die Reaktion auf Vorfälle beschleunigt. Die komplette Trellix XDR-Plattform 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.

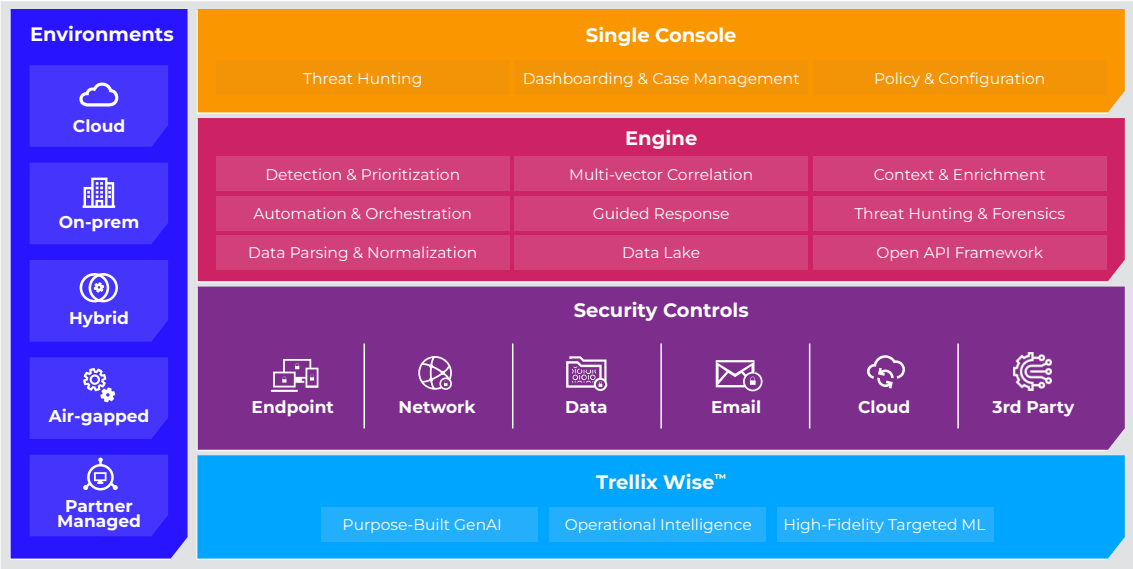

Abbildung 1: Trellix XDR-Plattform

Die Compliance-Anforderungen können je nach den Anwendungsleitlinien für den jeweiligen Mitgliedsstaat variieren, doch zur Einhaltung der NIS 2-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) Ihnen helfen kann, die NIS 2-Vorgaben einzuhalten und Ihr Risiko durch neue Bedrohungen zu reduzieren.

Identifizierung Ihrer Risiken mit Trellix Assessment Services

Die NIS-2-Richtlinie schreibt vor, dass Unternehmen Risikobewertungen durchführen und internationale oder europäische Standards wie ISO 27001 bzw. „koordinierte Rahmen für die Cybersicherheit“ wie das Cyber-Sicherheits-Framework NIST umsetzen, um Cyber-Risiken kontinuierlich reduzieren zu können. Der Stichtag für die Einhaltung der Compliance-Vorgaben kommt schnell näher. Es ist daher wichtig, Ihren aktuellen Status bei der Einhaltung dieser Standards und 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-Lösungen	Beschreibung der Lösung	NIS 2-Artikel
Cyber Security 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, XDR-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 Cyberthreats-Report vom Juni 2024 beleuchtet, wie neue Ransomware-Familien die Gefährlichkeit dieser Angriffe erheblich steigern. Ransomware ist eine schwerwiegende Bedrohung für Anbieter grundlegender Dienstleistungen, die der NIS-2-Richtlinie unterliegen. Schlagzeilenträchtige Angriffe richten sich gegen Energieversorger, Transportwesen sowie gegen Einrichtungen der öffentlicher Verwaltung 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	NIS 2-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 Collaboration Security	Vermeidung und Erkennung von Ransomware bei Phishing-Angriffen 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 Connect	Bereitstellung von XDR-Funktionen zur Verbesserung der Bedrohungserkennung und Reaktion auf Ransomware	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 NIS-2-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 Connect die Analysten und reduziert die mittlere Reaktionszeit (Mean Time to Respond, MTTR) mit einer offenen Plattform, die Daten von Trellix-Sensoren und mehr als 490 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 Connect und SOC-Bewertungen empfehlen wir die folgenden Trellix-Lösungen zur Bereitstellung vollständiger Transparenz und Bedrohungserkennung für das gesamte Unternehmen:

Trellix-Lösungen	Beschreibung der Lösung	NIS 2-Artikel
Trellix EDR 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 Enterprise	Stark skalierbare Cloud-Malware-Analysen	21.2b, 21.2g
Trellix Helix Connect	Bereitstellung von XDR-Funktionen 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
Semperis (Partner)	Schutz für Verzeichnisdienste und Integration mit Helix Connect 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 NIS-2-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 erweiterten Bedrohungen schützen. Zudem wird die OT-Sicherheitsüberwachung typischerweise nicht von den IT-Sicherheitsteams, sondern von unerfahrenen Anwendern durchgeführt. Die Trellix XDR-Plattform 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	NIS 2-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)	Erkennung von Details zu SCADA-Ressourcen und Schwachstellen, Integration mit XDR für die Erkennung und Abwehr von Bedrohungen	21.2e, 21.2b
Trellix Helix Connect	Bereitstellung von XDR-Funktionen zur Verbesserung der Erkennung und Behebung von Zwischenfällen in OT- und IoT-Netzwerken	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. Fakt ist, dass die Zahl der Datenkompromittierungen laut der Cloud Security Alliance im Jahr 2023 trotz gestiegener Ausgaben für Sicherheit um 78 % gestiegen ist. Externe APT-Akteure nutzen KI, um schneller Exploits zu erstellen. Dadurch sind Ihre vertraulichen Kunden- und Unternehmensdaten durch anfällige Anwendungen gefährdet. Zusätzlich hat der Trellix-Bericht zu den Bedrohungsprognosen für 2024 auf eine Zunahme der Insider-Risiken bei versehentlichen und böswilligen Datenkompromittierungen hingewiesen. All diese Faktoren erhöhen die Wahrscheinlichkeit, dass eine Kompromittierung oder ein Datenverlust gemeldet werden muss. Da die NIS-2-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	NIS 2-Artikel
Trellix Endpoint Data Protection and Discovery	Erkennung, Klassifizierung und Schutz von Daten auf Endgeräten	21.2h, 21.2i
Trellix Network Data Protection and Discovery	Erkennung, Klassifizierung und Schutz von Daten im gesamten Netzwerk	21.2i
Trellix Database Security	Überwachung und Kontrolle von Zugriffen auf vertrauliche Informationen in Anwendungsdatenbanken	21.2i
Skyhigh Security (Partner)	Überwachung und Kontrolle von Zugriffen auf vertrauliche Informationen in Cloud-Anwendungen	21.2d, 21.2i, 21.2j
Trellix Helix Connect	Bereitstellung von XDR-Funktionen zur Verbesserung der Datenerkennung und Reaktion	21.2d, 21.2c, 21.2e, 21.2g, 21.2i, 21.2j

Wenn Sie mehr über Trellix und NIS 2 erfahren möchten, sehen Sie sich unser On-Demand-Webinar „Mit Trellix NIS 2-Compliance erreichen“ an oder vereinbaren Sie einen Workshop bei Ihrem Trellix-Vertreter.