Whitepaper

WHITEPAPER

NIS2 & Trend Micro

In unserer modernen Welt sind digitale Dienste nicht mehr wegzudenken. IT und IT-gestützte Systeme werden zum Reisen, zum Handeln, zur Kommunikation und Information oder auch für bürgernahe Dienstleistungen, wie KfZ-Zulassungen, genutzt. Ein Ausfall oder eine Beeinträchtigung dieser Systeme kann weitreichende Folgen und Auswirkungen auf das Privatleben, die Wirtschaft und die öffentliche Ordnung haben.

Die Europäische Union hat bereits 2016 die "Network and Information Security" Richtlinie (NIS, EU 2016/1148) erlassen und damit Maßnahmen zur Verbesserung der Cybersicherheit bei Betreibern wesentlicher Dienste und Anbietern digitaler Dienste formuliert. Die Direktive musste durch die EU-Mitgliedsstaaten in nationales Recht umgesetzt werden.
Verschärfte Bedrohungslagen, die zunehmende Nutzung von Cloud-Technologien sowie die Auswirkungen erfolgreicher Cyberangriffe haben zu einer Neufassung der Richtlinie im Jahr 2022 geführt (NIS2, EU 2022/2555). Auch hier sind die EU-Mitgliedsstaaten verpflichtet, die neue Richtlinie in nationales Recht umzusetzen.

Ausführliche Informationen zur NIS2-Richtlinie und wer davon in welcher Form betroffen ist, finden Sie auf unserer **Webseite**

Mit Trend Micro NIS2-Vorgaben erfüllen

Bislang (Stand: 13.Mai 2024) existieren drei Referentenentwürfe und ein Diskussionspapier zum NIS2 Umsetzungsgesetz (NIS2UmsuCG). Inwieweit eine Verkündung des Gesetzes und ein Inkrafttreten zu Oktober 2024 durchführbar ist, bleibt zum aktuellen Zeitpunkt fraglich. Fest steht jedoch, dass das Gesetz kommen wird und betroffene Einrichtungen zum Handeln zwingt.

Ohne die richtige Benutzung der richtigen Technologie an der richtigen Stelle sind von NIS2 betroffene Einrichtungen kaum in der Lage, die gesetzlichen Anforderungen zeitgerecht (6 Monate Frist ab Verkündung des Gesetzes bis zur Umsetzung der enthaltenen Verpflichtungen) umzusetzen.

Trend Micro bietet mit einer einheitlichen Plattform und einer darauf ausgerichteten Portfolio-Strategie maßgeschneiderte Lösungen und Dienstleistungen an, die zur Erfüllung von NIS2-Vorgaben eingesetzt werden können. Die folgende Übersicht zeigt die Anwendbarkeit von Trend Micro Angeboten in einzelnen Bereichen des NIS2UmsuCG.

Die einzelnen Komponenten, sowie deren Voraussetzungen sind dabei modular kombinierbar und können somit bedarfsorientiert beschafft und betrieben werden.

Referenz Referentenentwurf / Diskussionspapier			Inhalt	Trend Micro unterstützt?	Trend Micro Lösung	Anwendungsbeispiel
Paragraf	Absatz	Satz				
6			Informationsaustausch	✔	Vision One - Threat Intelligence	Informationen zu Indicators of Compromise und Indicators of Attack können manuell, per TAXII oder MISP importiert werden.
11	5		Wiederherstellung der Sicherheit - Durchführung	✔	Incident Response	Trend Micro Incident Response Services sind gemäß BSI als qualifizierte APT Dienstleister eingestuft.
			Wiederherstellung der Sicherheit - Kosten	✔	Service One Complete	5 Tagessätze Incident Response sind im Serviceangebot enthalten.
30	1		Ausmaß der Risikoexposition	✔	Vision One - Attack Surface Risk Management	ASRM liefert sowohl allgemeine Informationen zur Risikobewertung der gesamten Einrichtung, als auch einzelner Assets.
			Eintrittswahrscheinlichkeit	✔	Vision One - Attack Surface Risk Management	Unter anderem Schwachstellen werden in ASRM nicht nur auf Basis der Kritikalität, sondern insbesondere aufgrund des globalen Ausnutzungspotenzials eingestuft.
	2	1	Konzepte für Risikoanalyse und Sicherheit	✔	Vision One - Attack Surface Risk Management	Die externe Angriffsfläche, identifizierte Angriffe und auch die Sicherheitskonfiguration eingesetzter Trend Micro Lösungen wird in ASRM automatisch bewertet.
				✔	Vision One - Extended Detection & Response	XDR unterstützt bei der Identifizierung und Qualifikation von Sicherheitsvorfällen und geeigneten Reaktionsmaßnahmen auf diese.
				✔	Service One Complete	Der Service Manager liefert im Rahmen von beispielsweise Roadmap Meetings, Quarterly Business Reviews, Strategiecalls oder durch die Vermittlung von Cybersecurity- und CISO-Experten erhebliche Mehrwerte bei der Entwicklung und Umsetzung der geforderten Konzepte.
		2	Bewältigung von Sicherheitsvorfällen	✔	Vision One - Extended Detection & Response	XDR unterstützt bei der Identifizierung und Qualifikation von Sicherheitsvorfällen und geeigneten Reaktionsmaßnahmen auf diese.
				✔	Vision One - Forensics	Forensics bietet Werkzeuge zur Sicherstellung von Beweismaterial, welches im Falle der Analyse von Sicherheitsvorfällen relevant werden kann.
				✔	Service One Complete	Managed Detection & Response (24x7) sowie 5 Tagessätze Incident Response sind bereits im Serviceangebot enthalten.
		3	Wiederherstellung nach einem Vorfall	✔	Service One Complete	5 Tagessätze Incident Response sind bereits im Serviceangebot enthalten.
		4	Sicherheit der Lieferkette	✔	Vision One - Attack Surface Risk Management	External Attack Surface Discovery, netzwerkinterne Assetidentifizierung und -bewertung sowie die kommende Funktion „Predictive Attack Path Analysis" unterstützen bei der Identifizierung von nicht selbst verwalteten Systemen, die mit der eigenen Infrastruktur kommunizieren
		5	Sicherheit bei Erwerb, Entwicklung und Wartung on IT Systemen	✔	Service One Complete	Der Service Manager stellt das Bindeglied zwischen Nutzern von Trend Micro Lösungen und Trend Micro selbst dar.
			Schwachstellenmanagement	✔	Vision One - Attack Surface Risk Management	Die Erkennung, Bewertung und Mitigation (teilweise direkt durch Trend Micro Lösungen, teilweise durch die Aussprache von Handlungsempfehlungen) von Betriebssystem- und Softwareschwachstellen ist ein wesentlicher Bestandteil von ASRM.
			Offenlegung von Schwachstellen	✔	Zero Day Initiative	Die von Trend Micro betriebene ZDI ist das weltweit größte Bug Bounty Programm für Softwareschwachstellen und Exploits und seit über 15 Jahren marktführend in diesem Bereich.
		6	Bewertung der Wirksamkeit von Risikomanagement-maßnahmen	✔	Vision One - Attack Surface Risk Management	Risk Index und Risk Score werden unmittelbar durch Maßnahmenumsetzung beeinflusst und sind messbar. So ist beispielsweise der Verlauf des Expositionsrisikos transparent einsehbar, ebenso wie klare KPIs zum Umgang mit Schwachstellen (mean time to patch, average unpatched time, etc.)
		7	Cyberhygiene	✔	Vision One - Attack Surface Risk Management	Unter anderem ungenutzte Assets (beispielsweise Benutzerkonten) oder unerwartete Verhaltensweisen von Assets (Kommunikation im Netzwerk, ungewöhnliche Anmeldevorgänge, etc.) werden in ASRM transparent dargestellt.
			Schulungen	✔	Vision One - In Product Trainings	Trainings zum Umgang mit der Plattform werden direkt innerhalb dieser angeboten.
				✔	Trend Micro Education	Das Education Portal stellt diverse on demand Lerninhalte rund um das Thema Cybersicherheit zur Verfügung.
				✔	Vision One - Awareness Trainings	Phishing Simulationen können direkt aus der Plattform gestartet werden.
		10	Multi-Faktor Authentifizierung	✔	Vision One - Rechte & Rollenkonzept	Der Zugriff auf die Vision One Plattform kann via MFA abgesichert werden.
				✔	Vision One - Attack Surface Risk Management	Identity Posture Management ist ein wesentlicher Bestandteil von ASRM und unterstützt somit bei der Identifizierung von Accounts, die via Multi-Faktor-Authentifizierung abgesichert werden sollten.
				✔	Vision One - Extended Detection & Response	Als Reaktion auf sicherheitsrelevante Vorfälle kann zukünftig MFA für betroffene Benutzerkonten erzwungen werden.
	7		Informationsaustausch	✔	Vision One - Threat Intelligence	Informationen zu Indicators of Compromise und Indicators of Attack können manuell, per TAXII oder MISP importiert werden.
31	2		Systeme zur Angriffserkennung	✔		Trend Micro hat diese Anforderung bereits Anfang 2023 im Whitepaper zum Einsatz von Systemen zur Angriffserkennung inhaltlich behandelt.
32	1	1	Erstmeldung	✔	Vision One - Extended Detection & Response	XDR qualifiziert sicherheitsrelevante Ereignisse und bietet umfassende Möglichkeiten zur Analyse. Diverse Übersichten der durch XDR generierten Workbenches können als Report bereitgestellt werden.
				✔	Vision One - Notifications	Benachrichtigungen zu Workbenches können automatisch per E-Mail, Webhook oder SMS versendet werden.
		2	Folgemeldung	✔	Service One Complete	Managed Detection & Response (24x7) ist im Serviceangebot enthalten. Mit MDR werden Workbenches mit entsprechenden Schweregraden analysiert und die Ergebnisse sowie Handlungsempfehlungen werden in Reports dokumentiert. Diese Reports können an die erforderliche Meldestelle weitergeleitet werden.

Referenz Referentenentwurf / Diskussionspapier			Inhalt	Trend Micro unterstützt?	Trend Micro Lösung	Anwendungsbeispiel
Paragraf	Absatz	Satz				
		3	Zwischenmeldung	✔	Service One Complete	Managed Detection & Response (24x7) ist im Serviceangebot enthalten. Mit MDR werden Workbenches mit entsprechenden Schweregraden analysiert und die Ergebnisse sowie Handlungsempfehlungen werden in Reports dokumentiert. Diese Reports können an die erforderliche Meldestelle weitergeleitet werden. Darüber hinaus können explizite Service Cases eröffnet werden, um aktuelle Statusmeldungen abzufragen oder spezifische Untersuchungen durchführen zu lassen.
				✔	Service One Complete	Im Falle verifizierter Vorfälle sind 5 Tagessätze Incident Response bereits im Serviceangebot enthalten. Während der Laufzeit des Services werden regelmäßige Statusmeldungen gegeben.
		4	Abschlussmeldung	✔	Service One Complete	Managed Detection & Reponse (24x7) stellt sowohl vorfallsbezogene Reports, als auch monatliche Auswertungen zur Verfügung.
				✔	Service One Complete	Nach abgeschlossenen Incident Response Fällen werden umfangreiche Abschlussberichte erstellt.
33	1	2	Registrierung von IP-Adressbereichen	✔	Vision One - Attack Surface Risk Management	Durch external attack surface discovery werden selbst genutzte, externe IP-Adressen kontinuierlich identifiziert.
	2		Registrierung von IP-Adressbereichen bei Betreibern kritischer Anlagen	✔	Vision One - Attack Surface Risk Management	Durch external attack surface discovery werden selbst genutzte, externe IP-Adressen kontinuierlich identifiziert.
	5		Informations-aktualisierung	✔	Vision One - Attack Surface Risk Management	Durch external attack surface discovery werden selbst genutzte, externe IP-Adressen kontinuierlich identifiziert.
34	1	6	Besondere Registrierungs-pflichten	✔	Vision One - Attack Surface Risk Management	Durch external attack surface discovery werden selbst genutzte, externe IP-Adressen kontinuierlich identifiziert.
38	1		Geschäftsleiter müssen Risiko-managementmaß-nahmen überwachen	✔	Vision One - Attack Surface Risk Management	Das Executive Dashboard von ASRM stellt eine zentrale Visualisierung von Risiken für den eigenen Informationsverbund zur Verfügung.
	3		Geschäftsleiter müssen regelmäßig zu Risikomanagement-maßnahmen und deren Umsetzung geschult werden	✔	Vision One - In Product Trainings	Trainings zum Umgang mit der Plattform werden direkt innerhalb dieser angeboten.
				✔	Trend Micro Education	Das Education Portal stellt diverse on demand Lerninhalte rund um das Thema Risikomanagement zur Verfügung.
				✔	Vision One - Awareness Trainings	Phishing Simulationen können direkt aus der Plattform gestartet werden.
39	1		Nachweispflicht zur Mängelbeseitigung	✔	Service One Complete	Der Service Manager unterstützt durch regelmäßige Service Meetings, Quarterly Business Reviews und entsprechende Dokumenation
40	5		Herausgabe von Daten zur Störungs-beseitigung	✔	Vision One - Rechte & Rollen-konzept	Read Only Zugänge zu erforderlichen Bereichen der Vision One Plattform können bei Bedarf bereitgestellt werden.
				✔	Vision One - API	Über die API sind unter anderem diverse Informationen zu sicherheitsrelevanten Ereignissen abrufbar.
43	2		Teilnahme an Schulungen	✔	Vision One - In Product Trainings	Trainings zum Umgang mit der Plattform werden direkt innerhalb dieser angeboten.
				✔	Trend Micro Education	Das Education Portal stellt diverse on demand Lerninhalte rund um das Thema Risikomanagement zur Verfügung.
44	1		Vorgaben des BSI (BSI Grundschutz)	✔		Der bedarfsgerechte Einsatz von Trend Micro Lösungen unterstützt bei der Einhaltung dieser Vorgaben.
45	2		Fachkunde bei ISBs in Bundeseinrichtungen	✔	Vision One - In Product Trainings	Trainings zum Umgang mit der Plattform werden direkt innerhalb dieser angeboten.
				✔	Trend Micro Education	Das Education Portal stellt diverse on demand Lerninhalte rund um das Thema Risikomanagement zur Verfügung.
	3		Kontrolle der Maßnahmen zur Cybersicherheit	✔	Vision One - Attack Surface Risk Management	Das Executive Dashboard von ASRM stellt eine zentrale Visualisierung des Status der Cybersicherheit zur Verfügung.
				✔	Trend Micro Red Teaming	Im Red Teaming werden geplante, strukturierte und beauftrage Cyberangriffe durchgeführt. Hierdurch gewonnene Erkenntnisse können für die Bewertung zur Umsetzung von Maßnahmen genutzt werden.
46	2		Fachkunde bei ISBs der Ressorts	✔	Vision One - In Product Trainings	Trainings zum Umgang mit der Plattform werden direkt innerhalb dieser angeboten.
				✔	Trend Micro Education	Das Education Portal stellt diverse on demand Lerninhalte rund um das Thema Risikomanagement zur Verfügung.
	3		Reporting an Ressortleitung	✔	Vision One - Attack Surface Risk Management	Das Executive Dashboard von ASRM stellt eine zentrale Visualisierung des Status der Cybersicherheit zur Verfügung.
				✔	Vision One - Reporting	Diverse Reports können in exportierbaren Dokumentenformaten zur Weitergabe erstellt werden.
50	3		Planung und Umsetzung eines Sofortprogramms zur Einhaltung von Vorgaben	✔	Service One Complete	Der Service Manager unterstützt durch regelmäßige Service Meetings, Quarterly Business Reviews und entsprechende Dokumenation
				✔	Vision One - Attack Surface Risk Management	Die Priorisierung von Maßnahmen zur Verringerung des Cybersicherheitsrisikos ist wesentlicher Bestandteil von ASRM.
65	3		Nachweispflicht zu §§ 30, 31, 32	✔	Vision One - Reporting	Diverse Reports können in exportierbaren Dokumentenformaten zum Nachweis erstellt werden.
	5		Kontrolle durch Dritte	✔	Vision One - Rechte & Rollenkonzept	Read Only Zugänge zu erforderlichen Bereichen der Vision One Plattform können bei Bedarf bereitgestellt werden.