ESET Lösungen für NIS2-Compliance

Wichtige Hinweise:

In der folgenden Übersicht nutzen wir die Formulierungen aus der NIS2-Richtlinie der Europäischen Union. Die erforderliche Umsetzung in nationales Recht steht sowohl für Deutschland als auch für Österreich noch aus. Es ist jedoch zu erwarten, dass die in Artikel 21 der NIS2-Richtlinie genannten Maßnahmen übernommen werden.

Bitte beachten Sie, dass unsere Inhalte keine rechtliche Beratung ersetzen. Bitte wenden Sie sich für Ihren konkreten Fall an eine Rechtsanwältin oder einen Rechtsanwalt Ihres Vertrauens.

Übrigens: Die NIS2-Richtlinie sieht für die unter die Richtlinie fallenden privaten und öffentlichen Einrichtungen **umfangreiche Berichtspflichten** vor. Dazu gehört, dass Einrichtungen laut Art. 23, Abs. 4 NIS2-Richtlinie einen Sicherheitsvorfall **innerhalb von 24 Stunden** der zuständigen Behörde melden müssen, wenn er einen erheblichen Einfluss auf die Funktionsfähigkeit der Systeme und Dienste des Unternehmens haben kann. **Innerhalb von 72 Stunden** sollen zudem **Kompromittierungsindikatoren** (IoCs) benannt werden und **nach einem Monat soll ein Abschlussbericht** vorgelegt werden. Bei der Bereitstellung solch umfangreicher Dokumentationen können Endpoint Detection & Response (EDR) Lösungen wie ESET Inspect unterstützen.

Art. 21, Abs. 2 NIS2-Richtlinie:

„Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:"

NIS2-Richtlinie im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;	Wir von ESET bzw. unsere Vertriebspartner unterstützen Sie bei der technischen Bewertung, Erstellung und Umsetzung von passenden IT-Sicherheitskonzepten entsprechend Ihrer Kundenumgebung.		Unter Umständen Bestandteil der Presales-Phase			
	Mit unserer Management-Konsole haben Sie dank Hard- und Software-Inventarisierung Ihre schützenswerten Assets im Blick und verfügen damit über eine zuverlässige Grundlage für die Risikoanalyse sowie die Erstellung Ihres Sicherheitskonzepts.	ESET PROTECT	✓	✓	✓	✓
b) Bewältigung von Sicherheitsvorfällen;	Unser Endpoint Detection & Response Tool ermöglicht eine umfassende Gefahrensuche und -abwehr. Ereignisse im Netzwerk werden protokolliert und zu Vorfällen zusammengefasst, sodass Sie einen Überblick darüber haben, was in Ihrer IT-Umgebung vor sich geht. So können Sie bei einem Sicherheitsvorfall schnell reagieren. Dank festgelegter Reaktionsmaßnahmen wird das Sicherheitsniveau zudem weiter gesteigert.	ESET Inspect (in Kombination mit ESET PROTECT)	✓	✓	✓	
	ESET Experten übernehmen den operativen Betrieb Ihrer ESET Inspect Instanz und damit die Überprüfung, Auswertung und Interpretation aller Daten sowie die Reaktion auf mögliche Sicherheitsvorfälle.	ESET Detection & Response Ultimate	✓			
	Mit dem KI-gestützten Managed Detection & Response Service haben auch Unternehmen mit weniger finanziellen Ressourcen die Möglichkeit, von der Expertise der ESET Spezialisten zu profitieren. Durch die Anbindung an das ESET-eigene Security Information and Event Management Tool wird ESET Inspect mit den nötigen Daten versorgt, um automatisiert auf verdächtige Aktivitäten innerhalb der Unternehmensumgebung zu reagieren.	ESET MDR		✓		
c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;	ESET bietet keine spezielle Backup-Management-Lösung.					
	ESET Experten übernehmen für Sie den operativen Betrieb Ihrer ESET Inspect Instanz – dazu gehört auch die Reaktion auf akute Vorfälle, einschließlich der Eindämmung und Isolierung einer Bedrohung – und unterstützen Sie so dabei, den Betrieb im Falle eines Vorfalls aufrecht zu erhalten.	ESET Detection & Response Ultimate	✓			

NIS2-Richtlinie im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;	Prävention ist unsere Expertise. ESET Sicherheitslösungen erkennen und wehren Bedrohungen wie Viren, Ransomware, Phishing oder Spam zuverlässig ab[1] und verhindern damit auch deren Ausbreitung auf andere Organisationen. Unsere Schutzlösungen für Clients, Mobilgeräte, Server und Cloud-Anwendungen bilden die Basis. Ergänzt werden sie durch unsere cloudbasierte Sandboxing-Lösung ESET LiveGuard® Advanced, die selbst Zero Days zuverlässig erkennt.	ESET Endpoint Security | ESET Server Security | ESET Mail Security | ESET Security for Microsoft SharePoint Server ESET LiveGuard® Advanced	✓	✓	✓	✓
e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;	Der Großteil unserer Produkte und Services ist nach ISO 27001 und ISO 9001 zertifiziert. Die Zertifizierung umfasst alle Unternehmensprozesse von der sicheren Programmierung bis hin zum Vertrieb. Damit gewährleisten wir ein hohes Maß an Produktqualität sowie Informationssicherheit im eigenen Haus.		✓	✓	✓	✓
	Unsere Schwachstellen- und Patch-Management-Lösung sorgt dafür, dass Sicherheitslücken auf Endgeräten und Servern umgehend erkannt und behoben werden.	ESET Vulnerability & Patch Management	✓	✓	✓	✓
f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;	Dank regelmäßiger, automatisch generierbarer Reports mit relevanten Sicherheitsereignissen und Kennzahlen behalten Sie den Überblick über den Sicherheitsstatus in Ihrem Unternehmensnetzwerk. Hierdurch lässt sich zudem nachverfolgen und belegen, dass festgelegte Schutzmaßnahmen tatsächlich greifen. Darüber hinaus können Sie aus den Erkenntnissen der Reports Maßnahmen zur weiteren Verbesserung Ihres Schutzes ableiten und so Ihr Sicherheitsniveau kontinuierlich steigern.	ESET PROTECT + ESET Inspect	✓	✓	✓	✓*
g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;	Für alle Nutzer im Netzwerk können über dynamisch festlegbare Gerätegruppen ganz unkompliziert verschiedene Cyberhygiene-Maßnahmen durchgesetzt werden, z.B. automatisierte Updates der Sicherheitssoftware auf den Endpoints oder die Installation bzw. Deinstallation von Drittanbieter-Software. Für alle Administratoren bzw. Nutzer der Management-Konsole lassen sich spezifische Rechte für den Zugriff und die Verwaltungsmöglichkeiten festlegen.	ESET PROTECT	✓	✓	✓	✓
	Über ESET PROTECT können Sie für alle Nutzer der Festplattenverschlüsselung Passwortrichtlinien festlegen und durchsetzen. Im Falle des Austritts eines Mitarbeiters lassen sich zudem remote Zugänge zu sensiblen Systemen oder Assets sperren.	ESET Full Disk Encryption	✓	✓	✓	✓
	Unsere kostenlosen Trainings stärken das Bewusstsein für IT-Sicherheit bei allen Mitarbeitenden in Ihrem Unternehmen.	ESET Cybersecurity Awareness Trainings	✓	✓	✓	✓

[1] www.av-comparatives.org/tests/business-security-test-2023-august-november/

* ohne ESET Inspect

NIS2-Richtlinie im Wortlaut	Unser Ansatz für eine mögliche Umsetzung	ESET Lösung	ESET PROTECT Bundles			
			MDR Ultimate	MDR	Elite	Complete
h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;	Unsere inhouse entwickelte und patentierte Festplattenverschlüsselung mit Pre-Boot-Authentifizierung bietet zuverlässigen Schutz für ruhende Daten. Selbst bei Verlust oder Diebstahl eines Geräts oder im Falle des Austritts eines Mitarbeiters werden unautorisierte Zugriffe auf die Daten verhindert und die Informationssicherheit gewährleistet.	ESET Full Disk Encryption	✓	✓	✓	✓
	Mit der Endpoint-Verschlüsselungslösung können Sie neben ruhenden Daten auch Daten in Bewegung zuverlässig absichern. Hierzu zählen neben E-Mails und Anhängen insbesondere externe Medien wie USB-Sticks. Diese Lösung ist perfekt zugeschnitten auf Organisationen mit besonderen Verschlüsselungsanforderungen sowie expliziten Richtlinien für den Einsatz gemeinsam genutzter Geräte.	ESET Endpoint Encryption	*	*	*	*
i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;	Für alle Nutzer im Netzwerk können über dynamisch festlegbare Gerätegruppen ganz unkompliziert verschiedene Maßnahmen durchgesetzt werden, z.B. automatisierte Updates der Sicherheitssoftware auf den Endpoints oder die Installation bzw. Deinstallation von Drittanbieter-Software. Für alle Administratoren bzw. Nutzer der Management-Konsole lassen sich spezifische Rechte für den Zugriff und die Verwaltungsmöglichkeiten festlegen.	ESET PROTECT	✓	✓	✓	✓
	Mit unserer Endpoint-Verschlüsselungslösung können Sie Zugriffsrechte bis auf die Dateiebene festlegen. So verhindern Sie unbefugte Zugriffe auf besonders schützenswerte Daten wie z.B. Konstruktionspläne.	ESET Endpoint Encryption	*	*	*	*
j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	Unsere unkomplizierte und einfach zu implementierende Multi-Faktor-Authentifizierung funktioniert mobilbasiert und schützt den Zugang zu gemeinsam genutzten Systemen (Windows- & Server Logins, Microsoft Cloud-Dienste wie Microsoft 365 oder OWA, SAML, FIDO, ADFS 3.0, VPNs und RADIUS-basierte Dienste). Auf Wunsch lassen sich mittels biometrischen FIDO-Sticks sogar beinahe passwortlose Umgebungen realisieren.	ESET Secure Authentication	✓	✓	✓	
	Mit unserer Schutzlösung für Mailserver sichern Unternehmen ihre E-Mail-Kommunikation zuverlässig ab. Die Lösung schützt den Host selbst und verhindert so, dass digitale Bedrohungen wie Spam oder Phishing die Posteingänge der Nutzer erreichen.	ESET Mail Security	✓	✓	✓	✓
	Sofern Sie Microsoft 365 oder Google Workspace Anwendungen nutzen, sollten Sie diese zusätzlich schützen. Die Kombination aus Spam-Filter, Malware-Scanner, Anti-Phishing und Cloud Sandboxing in unserer Lösung sichert Ihre Unternehmenskommunikation, Zusammenarbeit und den vorhandenen Cloud-Speicher nachhaltig ab.	ESET Cloud Office Security	✓	✓	✓	✓

* separat buchbar