Wie Sie souverän die NIS-2-Compliance Ihrer Kund:innen vorantreiben

Die NIS-2-Richtlinie ist für Unternehmen von entscheidender Bedeutung. Sie führt strengere Cybersicherheitsmaßnahmen und eine größere Verantwortlichkeit ein, um kritische Dienste in der gesamten EU zu schützen.

Aufgrund der Komplexität der Richtlinie, der umfangreichen Anforderungen und der oft mehrdeutigen Formulierungen kann es jedoch eine große Herausforderung sein, die Maßnahmen in der NIS-2-Richtlinie zu verstehen und umzusetzen. Dies macht es schwierig, klare, umsetzbare Schritte aus der Richtlinie abzuleiten, sodass viele Unternehmen unsicher sind, wo sie anfangen sollen und wie sie die vollständige Einhaltung der Richtlinie sicherstellen können.

Dieses Dokument ist als Leitfaden gedacht. Es vereinfacht die NIS-2-Richtlinie, indem es die Anforderungen auf das Wesentliche reduziert und einen entsprechenden Bezug zu den Produkten von Acronis herstellt. Dieser Leitfaden bietet Unternehmen klare und umsetzbare Schritte, um sie bei der erfolgreichen Umsetzung der Richtlinie zu unterstützen und ihnen die Gewissheit zu geben, dass sie diese einhalten können.

Acronis kann Ihnen dabei helfen, das breite Spektrum an NIS-2-Maßnahmen zu erfüllen:

NIS-2-Maßnahmen	Funktionen von Acronis	Wie Acronis helfen kann
Risikomanagement und Governance Identifizierung, Bewältigung und Überwachung von Cybersicherheitsrisiken, um einen wirksamen Schutz und die Compliance zu gewährleisten. **Artikel 20** (Governance-Anforderungen) **Artikel 21** (Risikomanagement-Maßnahmen)	**Endpoint Management** Verfügbar für Acronis Cyber Protect **Advanced**	Umfassende Inventarisierungstools erkennen, verfolgen und melden automatisch alle Hardware- und Software-Ressourcen.
	Endpoint Management – Schwachstellenbewertung Verfügbar für Acronis Cyber Protect **Standard**, **Advanced** und **Backup Advanced**	Erkennt Schwachstellen, bevor sie ausgenutzt werden.
Bewältigung und Meldung von Vorfällen Effektive Erkennung und unverzügliche Meldung von Cybersicherheitsvorfällen an die zuständigen Stellen. **Artikel 10** (Computer-Notfallteams, CSIRTs) **Artikel 23** (Berichtspflichten)	**Endpoint Detection and Response (EDR)** Verfügbar für Acronis Cyber Protect **Advanced**	Sammelt sicherheitsrelevante Telemetriedaten von Endpunkten und Systemprotokollen, um Anomalien zu erkennen und fundierte Reaktionen für betroffene Endpunkte zu ermöglichen. Integration mit Threat Intelligence-Feeds Automatisierte Reaktion und Schadensbehebung
	Grundlegende Funktionen zum Schutz vor Malware und zur Sicherheitsverwaltung Verfügbar für Acronis Cyber Protect **Standard** und **Advanced**	Patch-Verwaltung mit ausfallsicherem Patching: Backup von Endpunkten vor der Installation von Patches. Erstellung von Block- und Positivlisten für URLs und Durchführung von Schaddatenanalysen für schädliche URLs.
	Erweiterte Funktionen zum Schutz vor Malware und zur Sicherheitsverwaltung Verfügbar für Acronis Cyber Protect **Advanced**	Blockiert Malware, bevor diese Ihre Daten beeinträchtigen kann. KI-basierter statischer und verhaltensheuristischer Echtzeitschutz gegen Viren, Malware, Ransomware und Krypto-Jacking.
	Cyber Security: Cyber Protection Operation Centers (CPOCs)	CPOCs überwachen kontinuierlich die Cybersicherheitslandschaft und veröffentlichen Echtzeitwarnungen zu potenziellen Bedrohungen wie Malware, Schwachstellen, Naturkatastrophen und anderen globalen Sicherheitsereignissen.

NIS-2-Maßnahme	Funktionen von Acronis	Wie Acronis helfen kann
Geschäftskontinuität Aufrechterhaltung geschäftskritischer Prozesse und schnelle Wiederherstellung nach Ausfällen oder Cybervorfällen. **Artikel 21** (Risikomanagement-Maßnahmen)	**Grundlegende Backup-Funktionen** Verfügbar für Acronis Cyber Protect **Standard**, **Advanced und Backup Advanced**	Backup: Image-basiert, Datei-basiert oder Wiederherstellung auf fabrikneuer, abweichender Hardware (Bare Metal Recovery). Data Protection für physische und virtuelle Server, Applikationen und Datenbanken, Workstations sowie Microsoft 365- und Google Workspace-Arbeitsplätzen. Unveränderlicher Cloud Storage.
	Disaster Recovery Add-on für Acronis Cyber Protect **Standard**, **Advanced oder Backup Advanced**	Mit der One-Click Recovery-Funktion können Benutzer:innen einen ausgefallenen Endpunkt ohne Eingreifen der IT-Abteilung wiederherstellen. Mit der Disaster Recovery-Erweiterung können Sie Ihre Geschäftsprozesse nach einem großflächigen Ausfall schnell wieder aufnehmen. Automatische Disaster Recovery-Tests sowie automatische Failover- und Failback-Prozesse für physische und virtuelle Workloads
	Erweiterte Funktionen zum Schutz vor Malware und zur Sicherheitsverwaltung Verfügbar für Acronis Cyber Protect **Advanced**	Backup-Scans finden und beseitigen Malware und Schwachstellen vor der Wiederherstellung, was ein sicheres Recovery gewährleistet.

Die Produkte und Services von Acronis sind unverzichtbare Tools für Unternehmen jeder Größe, die NIS-2-Compliance in wichtigen Bereichen wie Cyber Security und Vorfallmanagement anstreben. Doch echte Compliance erfordert auch robuste Prozesse, Governance und eine proaktive Beaufsichtigung.

Acronis

Weitere Informationen finden Sie auf www.acronis.com