Garantire la conformità alla NIS 2 con sicurezza

La NIS 2 è una direttiva strategica per le organizzazioni, perché impone misure di Cyber Security più rigorose e maggiore responsabilità a tutela di servizi essenziali, in tutta l'Unione europea.

La complessità intrinseca, i requisiti ampliati e il linguaggio spesso ambiguo, tuttavia, possono rendere estremamente difficile la comprensione e l'adozione delle misure previste dalla direttiva. Inoltre, poiché è complicato suddividere la direttiva in passaggi chiari e fruibili, molte organizzazioni sono incerte su come muovere i primi passi nell'applicazione della norma o su come garantire la piena conformità.

Questo documento serve da guida, semplificando la NIS 2, analizzando i suoi requisiti e collegandoli ai prodotti Acronis. Offre alle organizzazioni passaggi chiari e concreti per supportare i loro clienti nel raggiungere la conformità e allinearsi con sicurezza alla direttiva.

Acronis può aiutarti a ottenere la conformità a NIS 2 per un'ampia gamma di misure

Misure della direttiva NIS 2	Funzionalità di Acronis	Come Acronis può aiutarti
Gestione del rischio e governance Identificazione, gestione e supervisione dei rischi di sicurezza informatica, per garantire protezione efficace e conformità. **Articolo 20** (Requisiti di governance) **Articolo 21** (Misure di gestione del rischio)	**Gestione degli endpoint** (Incluso in Acronis Cyber Protect **Advanced**)	Strumenti di inventario completi per rilevare, tenere traccia e creare automaticamente report relativi a tutte le risorse hardware e software.
	Gestione degli endpoint - Vulnerability assessment (Incluso in Acronis Cyber Protect **Standard**, **Advanced** e **Backup Advanced**)	Individuazione delle vulnerabilità prima che vengano sfruttate.
Gestione e segnalazione degli incidenti Rilevamento efficiente degli incidenti di sicurezza informatica e tempestiva segnalazione agli utenti interessati. **Articolo 10** (Team di risposta agli incidenti di sicurezza informatica) **Articolo 23** (Obblighi di segnalazione)	**Endpoint Detection and Response (EDR)** (Incluso in Acronis Cyber Protect **Advanced**)	Raccolta di dati di telemetria rilevanti per la sicurezza dagli endpoint e dai registri di sistema per eseguire il rilevamento delle anomalie e avviare azioni di incident response informate sugli endpoint interessati. Integrazione con i feed informativi sulle minacce. Risposta e correzione automatiche.
	Funzionalità di base di gestione della sicurezza e anti-malware (Incluso in Acronis Cyber Protect **Standard** e **Advanced**)	Gestione delle patch con applicazione sicura: backup degli endpoint prima dell'installazione delle patch. Creazione di elenchi di URL consentiti e non consentiti e analisi del payload degli URL dannosi.
	Funzionalità avanzate di gestione della sicurezza e anti-malware (Incluso in Acronis Cyber Protect **Advanced**)	Blocco del malware prima che colpisca i dati. Antivirus, anti-malware, anti-ransomware e anti-cryptojacking euristici, basati su AI, in tempo reale, statici e comportamentali.
	Cyber Security: Centro operativo Acronis Cyber Protection (CPOC)	Monitorano costantemente il panorama della Cyber Security e rilasciano avvisi in tempo reale sulle potenziali minacce, tra cui malware, vulnerabilità, emergenze naturali e altri eventi di portata globale.

Misure della direttiva NIS 2	Funzionalità di Acronis	Come Acronis può aiutarti
Continuità operativa Mantenimento dell'operatività e recupero rapido dopo interruzioni o incidenti informatici. **Articolo 21** (Misure di gestione del rischio)	**Funzionalità di backup di base** (Incluso in Acronis Cyber Protect **Standard**, **Advanced e Backup Advanced**)	Backup: ripristino basato su immagine, file o bare-metal anche su hardware diverso. Protezione dati per server fisici e virtuali, applicazioni e database, workstation, Microsoft 365 e Google Workspace. Cloud storage immutabile.
	Disaster Recovery (Add-on: Acronis Cyber Protect **Standard**, **Advanced o Backup Advanced**)	La funzionalità One-Click Recovery permette a qualsiasi utente di ripristinare un endpoint malfunzionante senza l'intervento dell'IT. Torna rapidamente in attività dopo un'interruzione di ampia portata con il disaster recovery. Test del disaster recovery, failover e failback automatizzati per workload fisici e virtuali.
	Funzionalità avanzate di gestione della sicurezza e anti-malware (Incluso in Acronis Cyber Protect **Advanced**)	Ripristino sicuro con scansione e correzione dei backup prima del ripristino, per individuare malware e vulnerabilità.

I prodotti e i servizi Acronis sono strumenti essenziali per le aziende e le imprese che intendono ottemperare ai requisiti della NIS 2, perché affrontano aree chiave come la Cyber Security e la gestione degli incidenti. Per una reale conformità, tuttavia, occorre anche mettere in atto processi e attività di governance consolidati e controlli proattivi.

Acronis

Maggiori informazioni su www.acronis.com