AvePoint

SCHEDA RIASSUNTIVA

Gestione della sicurezza dei dati (DSPM) e NIST CSF 2.0

Guida rapida per il settore pubblico

Con NIST CSF 2.0 e DSPM, le agenzie del settore pubblico possono sviluppare una strategia di difesa proattiva e a prova di futuro che protegga ciò che conta di più: la fiducia del pubblico, la continuità operativa e il successo della missione.

Elementi fondamentali del NIST CSF 2.0

Il Cybersecurity Framework (CSF) del NIST fornisce una guida flessibile e orientata ai risultati. La versione 2.0 introduce aggiornamenti chiave su misura per il settore pubblico:

Pilastro	Novità	Impatto
Governance	Responsabilità a livello aziendale del rischio informatico	Integra la sicurezza nella strategia aziendale
Zero trust	Modello "Non fidarti mai, verifica sempre"	Controllo degli accessi più rigoroso e segmentazione
Rischio della catena di approvvigionamento	Responsabilità di terzi	Limita le vulnerabilità ereditate
Sicurezza del cloud e dell'intelligenza artificiale	Enfasi sull'orientamento al futuro	È in linea con gli obiettivi di trasformazione digitale

Roadmap per l'implementazione del DSPM

01. Valutare la propria posizione attuale e le vulnerabilità

02. Definire obiettivi in linea con gli obiettivi aziendali e normativi

03. Sviluppare una strategia per le politiche, la tecnologia e la mitigazione dei rischi

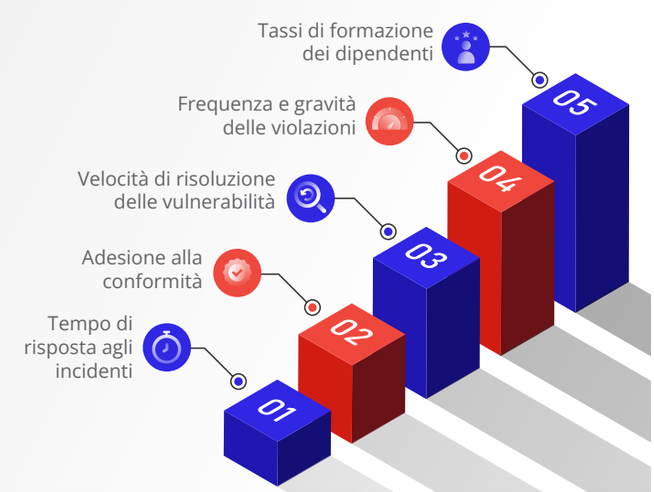
04. Implementare strumenti unificati e automatizzare ove possibile

05. Formare il personale sui rischi reali e sulle abitudini sicure

06. Monitorare e adattarsi continuamente alle minacce in tempo reale

07. Rivedere e migliorare attraverso audit e KPI

Monitora il successo con questi KPI



La sicurezza informatica è una maratona, non uno sprint. AvePoint aiuta le agenzie governative a stare al passo con i tempi.

AvePoint semplifica alle organizzazioni del settore pubblico l'allineamento con NIST CSF 2.0 e l'adozione di un approccio proattivo alla sicurezza informatica.

Con AvePoint, le agenzie possono:

- **Identificare e classificare** i dati sensibili per garantire una protezione adeguata.
- **Applicare il modello zero trust** con controlli di accesso automatizzati e politiche basate sul rischio.
- **Rilevare e rispondere** alle minacce con un monitoraggio continuo e una correzione automatizzata.
- **Garantire la conformità** alle normative in continua evoluzione.

Per ulteriori informazioni sulle soluzioni AvePoint per il settore pubblico, visitate il nostro sito web all'indirizzo **AvePoint.com**.

Prenota una demo