

Da SOC 2 a NIS 2: Sicurezza di cui ci si può fidare

March Networks Cybersecurity
Proteggere la tua rete di videosorveglianza

Da SOC 2 a NIS 2:

March Networks Cybersecurity

Proteggere la tua rete di videosorveglianza

Whitepaper 2025

Introduzione

Con la continua evoluzione delle minacce informatiche, garantire la sicurezza dei sistemi di videosorveglianza è più che mai fondamentale. March Networks si impegna a offrire cybersecurity by design, implementando robusti controlli di accesso, crittografia e misure di conformità per proteggere le organizzazioni dai rischi informatici.

Minacce informatiche nella videosorveglianza

I sistemi di sorveglianza sono spesso bersaglio di attacchi informatici, con minacce quali:

- Accesso non autorizzato tramite credenziali deboli.
- Attacchi man-in-the-middle che compromettono l'integrità dei video.
- Malware che interrompe le operazioni.
- Spoofing della rete che porta alla manipolazione del sistema.

Per mitigare questi rischi, March Networks impiega una strategia di cybersecurity a più livelli che comprende la crittografia end-to-end, i protocolli di sicurezza della rete e i framework orientati alla conformità.

March Networks e conformità SOC 2

March Networks ha ottenuto la conformità SOC 2 di tipo 2, dimostrando solidi standard di protezione dei dati per le organizzazioni che danno priorità alla privacy, alla sicurezza e alla conformità normativa. Questa conformità riflette il fatto che i nostri servizi sono distribuiti in un ambiente che soddisfa i rigorosi standard di riservatezza, integrità e disponibilità dei dati.

La conformità SOC 2 è particolarmente importante per settori come quello bancario, della vendita al dettaglio e delle infrastrutture critiche, dove la sicurezza delle prove video e l'affidabilità del sistema sono imprescindibili.

March Networks e conformità NIS 2

La NIS 2 (Network and Information Systems Directive 2) è una direttiva dell'Unione europea che ogni Stato membro dell'UE ha dovuto implementare nella legislazione nazionale entro il 17 ottobre 2024. Lo scopo principale della direttiva è stabilire un livello forte e unificato di sicurezza informatica in tutta l'Unione europea, migliorando la sicurezza e il buon funzionamento dell'economia e della società dell'UE.

Conformità alla direttiva NIS 2:

- Obbliga le organizzazioni che forniscono servizi critici e importanti a sviluppare capacità di cybersecurity.
- Definisce la gestione del rischio di cybersecurity e le misure di applicazione.
- Richiede la mitigazione delle minacce per i sistemi di rete e di informazione.
- Assicura la continuità del servizio durante gli incidenti di sicurezza.
- Stabilisce l'obbligo di segnalazione degli incidenti alle autorità.
- Istituisce le autorità necessarie (comprese le squadre di gestione delle crisi informatiche e di risposta agli incidenti).
- Richiede agli Stati membri dell'UE di sviluppare strategie nazionali di sicurezza informatica.
- Può includere sanzioni sostanziali in caso di non conformità, tra cui multe significative e conseguenze legali.

Il NIS 2 ha un impatto diretto su entità essenziali e importanti che operano nei settori dell'energia, dei trasporti, delle banche, delle infrastrutture, della produzione, alimentare e chimica. I venditori e i fornitori di queste entità sono indirettamente interessati, poiché devono garantire che i loro prodotti e servizi soddisfino i requisiti obbligatori dei loro clienti.

March Networks è attualmente registrata presso l'ACN (Agenzia per la Cybersicurezza Nazionale) e condivide informazioni in conformità al D.lgs. 4.9.2024, n. 134, che attua la direttiva NIS 2 dell'UE in Italia.

Sicurezza by Design: L'approccio di March Networks

March Networks segue un approccio di sicurezza by design, integrando gli aspetti di cybersecurity nello sviluppo dei prodotti:

- Distinta base del software (SBOM): fornisce trasparenza sui componenti software per le valutazioni di vulnerabilità e le verifiche di conformità.
- Impostazioni di sicurezza predefinite: i dispositivi vengono forniti con impostazioni di fabbrica sicure, tra cui:
 - Nessuna password predefinita.
 - HTTPS forzato.
 - Protocolli meno sicuri disabilitati per impostazione predefinita.
- Aggiornamenti e patch regolari: March Networks fornisce patch di sicurezza e aggiornamenti tempestivi per mitigare le nuove minacce scoperte.
- Strumenti di gestione dei dispositivi: soluzioni integrate per la gestione centralizzata, la distribuzione delle credenziali, il monitoraggio e il rinnovo dei certificati HTTPS e 802.1x e gli avvisi sullo stato di sicurezza di più dispositivi.
- Controlli di autenticazione e autorizzazione: supporta la gestione degli accessi basata sui ruoli, l'autenticazione a più fattori e le integrazioni con Active Directory o LDAP, nonché il single sign-on con token SAML per prevenire gli accessi non autorizzati.
- Crittografia dei dati: implementa la crittografia AES 256 a riposo, inclusa la gestione centralizzata delle chiavi e la crittografia TLS in transito per proteggere i flussi video e le comunicazioni di rete. Consente di applicare solo i cifrari in comune tra TLS 1.2 e 1.3 per garantire la protezione e assicurare la compatibilità.
- Esportazione di video criptata con password: da una o più fonti, comprese le note e altri dati di business intelligence raccolti dai nostri sistemi, come le ricevute da POS o ATM, raccogliendo tutto in un unico file di caso, con l'autenticità protetta da un sigillo digitale, progettato per prevenire qualsiasi tentativo di manomissione.
- Segnalazione degli incidenti: March Networks segue le best practice di settore per segnalare gli incidenti di sicurezza o le vulnerabilità identificate nei nostri prodotti e servizi, in conformità con i nostri criteri di sicurezza. Vengono rese disponibili patch e correzioni di sicurezza insieme ai relativi rapporti di sicurezza per i clienti registrati al nostro Partner Portal, in anticipo rispetto alla divulgazione pubblica.

- Conformità per la privacy: March Networks rende disponibili online la nostra informativa sulla privacy e le relative dichiarazioni, delineando quali informazioni personali raccogliamo e come configurare i nostri prodotti installati presso i clienti per implementare i criteri desiderati per la privacy.
- Sicurezza della catena di approvvigionamento: March Networks implementa processi volti a garantire che tutti gli aggiornamenti del firmware e del sistema siano firmati e verificati crittograficamente per evitare modifiche non autorizzate.
- Formazione: March Networks implementa un programma interno obbligatorio di sensibilizzazione alla sicurezza per formare costantemente i dipendenti a evitare e mitigare le minacce alla sicurezza. Per i clienti registrati al nostro Partner Portal sono disponibili formazione dedicata ai prodotti e ai servizi e una guida alla protezione dei prodotti.

Cybersecurity proattiva per la videosorveglianza

March Networks rimane all'avanguardia nell'innovazione della cybersecurity, fornendo alle organizzazioni soluzioni di videosorveglianza sicure, scalabili e conformi. Adottando i framework SOC 2 e NIS 2, March Networks consente alle aziende di proteggere le risorse, garantire la conformità alle normative e rispondere in modo proattivo alle minacce emergenti.

Per maggiori dettagli sulle soluzioni di cybersecurity di March Networks, visita marchnetworks.com.

Questo documento è aggiornato al 25 settembre 2025. Lo stato di conformità e i requisiti normativi possono cambiare. Per ottenere le informazioni più aggiornate, consulta la documentazione corrente.