La Redazione

La sicurezza fisica nell'era della NIS2

La Direttiva NIS2 diventerà legge in EU ad ottobre 2024. La normativa impone, a numerose grandi e medie imprese e ad altre organizzazioni di rilievo nazionale, responsabilità rigorose in materia di cybersecurity, interessando anche la sicurezza fisica (protezione perimetrale, accesso ai locali, gestione delle aree critiche e dei visitatori e gestione dei disastri naturali) e prevedendo sanzioni severe.

La NIS2 è la continuazione della Direttiva comunitaria sulla cybersecurity introdotta nel 2016 ed interessa diverse organizzazioni di un maggior numero di settori, compresi i loro fornitori e partner in outsourcing.

La NIS2 ha implicazioni per gli entry point della sicurezza fisica e della cybersecurity; ciò può implicare la necessità di rafforzare la sicurezza in prossimità degli edifici e nei punti di accesso, la gestione di aree critiche (data center, camere bianche e apparecchiature), dei visitatori e disastri naturali.

Una protezione aggiuntiva potrebbe prevedere recinzioni e illuminazione automatica, oltre a telecamere di sorveglianza, rilevatori di movimento e adeguati sistemi di controllo accessi.

Controllo accessi e cybersecurity

I sistemi di controllo accessi di vecchia generazione possono essere particolarmente a rischio di attacchi cyber come:

- attacchi Man-in-the-middle - gli aggressori accedono a una rete, carpendo informazioni scambiate tra dispositivi (es. codici di apertura porte o login e password dei dispositivi);
- skimming e relay attack - i criminali clonano le informazioni presenti sulla carta per entrare;
- attacchi al controller - gli aggressori sovrascrivono il firmware del controller, rendendo il dispositivo inutilizzabile. Dopo aver violato la rete di un'organizzazione, i cyber criminali possono controllare altri sistemi e sottrarre informazioni sensibili da archivi interni o lanciare attacchi per disabilitare i sistemi chiave. In tal senso è essenziale che ci si occupi delle vulnerabilità dalle credenziali fino al livello dell'applicazione software. Ad esempio, con le credenziali, solo le persone autorizzate dovrebbero avere accesso tramite app sul telefono cellulare, impronte digitali, carte e altro. A volte l'anello debole sono i permessi utente troppo estesi, che consentono di accedere a dati riservati o di apportare modifiche non autorizzate al sistema.

Guarda l'intervento di GENETEC a secsolutionforum2024

Cinque aree chiave per semplificare la compliance secondo Genetec

1 Controllo accessi: semplificare i flussi di lavoro in un ambiente sicuro

La NIS2 prescrive l'implementazione di misure tecniche, come il controllo accessi e la crittografia, per proteggere i sistemi informativi.
Il controllo accessi è un ottimo punto di partenza per rivalutare i metodi adottati per proteggere i beni, le persone e l'organizzazione dalle minacce fisiche e di cybersecurity. Per evitare errori o dimenticanze nel provisioning delle credenziali e nella gestione dei diritti di accesso, esistono soluzioni[1] per tenere al sicuro le persone e le risorse nelle strutture, lungo le aree perimetrali e negli armadietti tecnici.
Si tratta di sistemi di controllo accessi robusti, basati sui ruoli utente e sulle credenziali che permettono anche di gestire le identità degli utenti e le autorizzazioni in modo standardizzato e automatizzato.
La crittografia avanzata e l'autenticazione basata sulle attestazioni garantiscono comunicazioni sicure, proteggono l'identità dei cardholder e preservano l'integrità del sistema.

2 In caso di incidente: il rispetto dei tempi di risposta alle notifiche

La NIS2 stabilisce che i soggetti interessati da episodi di cybersecurity con un impatto significativo sulla fornitura dei servizi debbano notificare il fatto alle autorità competenti.
Le notifiche devono dettagliare la natura e l'impatto dell'incidente, oltre al numero di utenti interessati e le misure adottate.
La notifica deve avvenire entro 24 ore, 72 ore e 30 giorni dalla conoscenza dell'incidente (in base al tipo di minaccia). Per semplificare le operazioni[2], esistono soluzioni che aiutano ad identificare la natura e l'impatto degli incidenti, a tenere traccia degli utenti interessati e a documentare le misure di mitigazione, acquisendo dati critici sugli incidenti per un impact assessment accurato.

[1] Come il sistema di controllo degli accessi Synergis™.

[2] Come Synergis Integration for Incident Notification.

3 Fornitori: applicazione della due diligence

Il 61% delle violazioni informatiche di successo proviene da attacchi perpetrati indirettamente, attraverso la supply chain. La NIS2 richiede di implementare misure per garantire la sicurezza della supply chain, tra cui la due diligence e gli accordi contrattuali con i fornitori. Utilizzando il controllo degli accessi per la sicurezza della supply chain, è possibile limitarne l'accesso fisico e digitale alle strutture. È poi fondamentale stabilire un livello di riferimento per la sicurezza per ogni vendor e per ogni prodotto ed individuare vendor che siano in grado di rafforzare la privacy delle informazioni e la cybersecurity.

4 Esternalizzazione: abbinare agilità e sicurezza

La NIS2 obbliga le organizzazioni a mettere in atto misure per rendere sicuri i rapporti in outsourcing. Ciò include la due diligence e gli accordi contrattuali con i fornitori di servizi.
Quando si esternalizzano i servizi, le misure di sicurezza per il controllo accessi sono fondamentali per proteggere i dati e i sistemi sensibili: aiutano a garantire che i fornitori si attengano a controlli più severi e robusti. Occorre assicurarsi che i fornitori di servizi in outsourcing aderiscano a protocolli di sicurezza rigorosi: tali protocolli possono essere contenuti nella due diligence e negli accordi contrattuali.

5 Politiche e assessment: essere pronti per il futuro

La NIS2 richiede di definire politiche e procedure per la gestione dei rischi di cybersecurity. Questi includono piani di risposta agli incidenti e piani di continuità operativa aziendale. È inoltre necessario condurre assessment periodici e gestire i rischi identificati.
Adottando un approccio unificato alla sicurezza ci si trova in una posizione di vantaggio per concentrarsi sull'identificazione, la mitigazione dei rischi e comunicazioni trasparenti e aperte. È infatti molto più facile ed efficace essere compliant, se tutto si trova in un unico posto[3].

[3] Genetec Security Center raggruppa i dati, consentendo di gestire i criteri di sicurezza, monitorare gli eventi e svolgere indagini. È una piattaforma di sicurezza unificata che offre il controllo accessi, la gestione video e altre funzioni di sicurezza avanzate e sviluppate integrando la cybersecurity e la privacy "by-design".

Rientrano nel campo di applicazione della Direttiva NIS2 le organizzazioni di grandi (> 50 milioni di fatturato o > 249 dipendenti) e medie dimensioni (> 10 milioni di fatturato o > 50 dipendenti) in settori ritenuti essenziali:

- ENERGIA
- SANITÀ
- APPROVVIGIONAMENTO DI ACQUA POTABILE
- TRASPORTI
- INFRASTRUTTURE DIGITALI
- BANCHE E INFRASTRUTTURE DEI MERCATI FINANZIARI
- FORNITORI DI SERVIZI DIGITALI
- SETTORE PUBBLICO
- SERVIZI POSTALI E LOGISTICA
- GESTIONE DELLE ACQUE REFLUE E DEI RIFIUTI
- INDUSTRIA CHIMICA
- INDUSTRIA ALIMENTARE
- FABBRICAZIONE DI PRODOTTI CRITICI (COMPRESI QUELLI MEDICI, INFORMATICI E PER IL TRASPORTO)
- FORNITORI DIGITALI (COME I SOCIAL NETWORK E I DATA CENTER)
- RICERCA
- AGENZIE SPAZIALI

Scarica il white paper Genetec "La sicurezza fisica nell'era della NIS2"