ISEO Ultimate Access Technologies

NIS2: decalogo per la conformità del controllo accessi

Nell'ambito dell'entrata in vigore della Direttiva europea "Network and Information Security 2", ISEO Ultimate Access Technologies pubblica un decalogo operativo dedicato ai responsabili della sicurezza di infrastrutture critiche: dieci best practice imprescindibili per allineare i sistemi di controllo accessi ai vincoli della NIS2, requisito centrale per la resilienza cyber-fisica di queste organizzazioni.

Il tallone d'Achille della sicurezza

La direttiva segna un cambio di paradigma nella sicurezza delle infrastrutture critiche, introducendo per la prima volta **l'obbligo esplicito di adottare un approccio omnicomprensivo ovvero non più solo in termini di cyber-security, ma di integrazione tra protezione informatica e fisica.** Già nella premessa della NIS2 infatti si precisa che "Le misure di gestione del rischio di cybersicurezza devono basarsi su un approccio 'All-Hazards' volto a proteggere i sistemi di rete e informatici e l'ambiente fisico di tali sistemi da eventi quali **furto, incendio, inondazione, guasti delle telecomunicazioni o dell'alimentazione elettrica, o accesso fisico non autorizzato".**

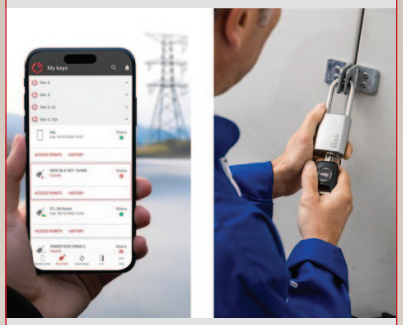
Un obbligo che risponde a un rischio molto spesso sottovalutato: l'accesso fisico non controllato può rappresentare una vulnerabilità per gli attacchi cyber-fisici, come evidenziato anche da ENISA (l'Agenzia dell'Unione europea per la cybersicurezza) nella sua "Technical Implementation Guidance" alla NIS2. Tuttavia molte imprese dei settori critici hanno investito massicciamente in soluzioni di rilevamento e contrasto delle intrusioni digitali, ma hanno sottovalutato la sicurezza fisica e quanto può essere un punto debole per l'intera infrastruttura. L'UE ha infatti incluso la sicurezza fisica e il controllo degli accessi tra gli obblighi, riconoscendo che **la cybersecurity non può essere separata dalla protezione fisica delle infrastrutture nei settori essenziali** come energia, telecomunicazioni, trasporti e sanità, dove la compromissione fisica può avere conseguenze tanto gravi quanto un attacco informatico. Un hacker o un attaccante interno (come un ex-dipendente) che ottiene accesso fisico a un data center o a un server oppure ad apparecchiature di rete può bypassare le protezioni digitali, installare dispositivi di intercettazione, rubare hardware o sabotare direttamente le infrastrutture critiche.

Oltre la compliance: da dictat normativo a resilienza operativa

Il decalogo elaborato da ISEO Ultimate Access Technologies identifica 10 best practice che trasformano **il controllo accessi da semplice obbligo normativo a pilastro della business continuity.** Passi che se implementati possono inoltre generare vantaggi concreti come **maggiore resilienza ed efficienza operativa,** riduzione dei costi e tutela della reputazione aziendale:

1. Adottare un approccio "All-Hazards" alla sicurezza - Integrare la protezione fisica con quella digitale seguendo il principio cyber-fisico richiesto da NIS2. L'accesso fisico non autorizzato rappresenta la "backdoor più grande" per i criminali informatici: proteggere server, rack, armadi e aree critiche è fondamentale quanto proteggere i sistemi informatici.

2. Implementare il modello di sicurezza a strati (Onion Shell) - Strutturare la sicurezza secondo le classi di protezione (da -1 a 4) come previsto dallo standard EN 50600, aumentando progressivamente i livelli di sicurezza dall'esterno verso le aree critiche. Ogni strato deve essere dotato di controlli di accesso adeguati al livello di criticità.



10 best practice

che trasformano il controllo accessi da obbligo normativo a pilastro della business continuity

1
Adottare un approccio **"All-Hazards"** alla sicurezza

2
Implementare il modello di **sicurezza a strati** (Onion Shell)

3
Digitalizzare i sistemi di controllo accessi

4
Garantire **tracciabilità e auditabilità** completa

5
Centralizzare la gestione delle credenziali

6
Implementare sistemi **multi-credenziale**

7
Proteggere ogni punto di accesso fisico

8
Garantire la **continuità operativa**

9
Abilitare la **revoca immediata** delle credenziali

10
Documentare e **aggiornare** costantemente le policy di accesso

3. Digitalizzare i sistemi di controllo accessi - Sostituire i sistemi meccanici obsoleti con soluzioni digitali e connesse. I sistemi meccanici con brevetti scaduti rappresentano rischi significativi: le chiavi possono essere duplicate senza verifica e la tracciabilità è praticamente impossibile.

4. Garantire tracciabilità e auditabilità completa - Implementare sistemi che registrino ogni evento di accesso con log dettagliati: chi, dove, quando, perché e come. La conformità NIS2 richiede la possibilità di verificare a posteriori tutti gli accessi alle aree critiche per investigazioni e compliance.

5. Centralizzare la gestione delle credenziali - Adottare piattaforme che permettano la gestione centralizzata (locale o cloud) di tutte le credenziali di accesso, dalla periferia al core. Questo consente di rispondere rapidamente a smarrimenti, cambi di ruolo e situazioni di emergenza.

6. Implementare sistemi multi-credenziale - Utilizzare diverse tipologie di autenticazione (smart key, RFID, mobile key, PIN) in base alla criticità dell'area. Le zone di massima criticità (Classe 4) richiedono autenticazione multifattore.

7. Proteggere ogni punto di accesso fisico - Estendere il controllo accessi non solo alle porte, ma anche a: rack server, armadi, cancelli, ascensori, cassette di sicurezza, depositi esterni. Ogni punto che può essere "aperto" deve essere protetto da manomissioni e attacchi intelligenti.

8. Garantire la continuità operativa - Implementare sistemi che funzionino anche in caso di blackout o interruzioni di rete. Soluzioni con dispositivi di chiusura senza alimentazione o backup batteria garantiscono che le aree critiche rimangano protette anche durante emergenze.

9. Abilitare la revoca immediata delle credenziali - Assicurarsi che le credenziali possano essere disattivate con un click in caso di smarrimento, cessazione del rapporto di lavoro o compromissione. I sistemi digitali permettono la revoca istantanea, mentre i sistemi meccanici richiedono la sostituzione fisica di serrature.

10. Documentare e aggiornare costantemente le policy di accesso - Mantenere aggiornate le policy di accesso con permessi basati su ruolo, tempo e location. Condurre audit periodici per verificare che i diritti di accesso siano allineati alle responsabilità effettive e rimuovere tempestivamente i permessi non più necessari.