SMART BUILDING EXPO

19 | 20 | 21
NOVEMBRE 2025
FIERA MILANO

PIAZZA FROM BUILDING TO CITY

La twin transition di edifici e città

A CURA

SBA
SMART BUILDINGS ALLIANCE FOR SMART CITIES

SBA
SMART BUILDINGS ALLIANCE FOR SMART CITIES

CYBERSECURITY NEGLI SMART BUILDING

Best Practice e strategie di difesa

- Gli smart building integrano IoT, cloud e automazione per migliorare efficienza e comfort
- Questa interconnessione espone però a nuovi rischi informatici
- Obiettivo: garantire sicurezza, resilienza e continuità operativa

SMART BUILDING

=

Maggiori punti di vulnerabilità

Punti di vulnerabilità

- Reti interconnesse (IT + OT + IoT)
- Dispositivi con firmware obsoleto o non sicuro
- Accessi remoti non controllati (tecnici, manutentori, fornitori)
- Dati gestiti da piattaforme cloud

PRIMA LINEA DI DIFESA

Separare IT e IoT

- Reti dedicate e VLAN per sistemi OT
- Firewall industriali e policy «deny by default»
- Applicare il modello ISA/IEC 62443 - zone e conduits
- Isolamento rapido in caso di compromissione

TRACCIABILITA' E CONTROLLO

Gli accessi: controllo e vulnerabilità

- Sistema IAM centralizzato
- Autenticazione multifattore (MFA) per operatori
- Principio del minimo privilegio
- Audit e log delle attività di configurazione

I DEVICE IoT

Rafforzare i punti più deboli

- Cambiare credenziali di default
- Aggiornare regolarmente firmware e software
- Disabilitare servizi non necessari
- Preferire fornitori con conformità ETSI EN 303 645

LE MINACCE

Visibilità e risposta alle minacce

- Soluzioni SIEM per raccogliere e correlare eventi
- NDR/IDS OT per individuare traffico anomalo
- Integrazione con SOC per analisi in tempo reale
- Alert e response automatizzati

GESTIONE DELLE VULNERABILITA’

Gestire le vulnerabilità in modo proattivo

- Scansioni periodiche delle reti
- Valutazioni di rischio basate sulla criticità
- Pianificazione di patch senza interrompere i servizi
- Inventario aggiornato degli asset OT/IoT
- Vulnerability assessment / Penetration test prima del rilascio della soluzione e da replicare periodicamente

LA SICUREZZA VA CONDIVISA

La gestione dei Partner

- Contratti con clausole di sicurezza (ISO 27001, IEC 62443)
- Accessi remoti protetti con VPN e MFA
- Sessioni registrate e monitorate
- Notifica obbligatoria di incidenti

GLI IMPREVISTI

Prepararsi agli imprevisti

- Backup cifrati e test di ripristino periodici
- Incident Response Plan (IRP) dedicato all’ambiente OT
- Procedure chiare per isolamento e recovery
- Coordinamento con facility management

SICUREZZA

=

PERSONE

La sicurezza è anche «Human Factor»

- Formazione continua su phishing e social engineering
- Procedure chiare per l'uso sicuro dei dispositivi
- Coinvolgimento del personale facility e IT
- Promuovere una cultura della sicurezza digitale
- "Un edificio è veramente smart solo se è anche sicuro"

WG 15 Cybersecurity Soon…

- Entro Febbraio 2026 primo Position Paper sarà presentato
- Creazione documenti dedicati agli Stakeholder dei progetti
- Apertura nuovi progetti NIS2 e Best Tools

Luca Girodo
WG 15
Cybersecurity