SBA
SMART BUILDINGS ALLIANCE
FOR SMART CITIES

SUMMIT FOR TERRITORIES 2026

GIOVEDÌ 21 MAGGIO 2026
SEDE ANCE ROMA – ACER

La Cybersecurity negli Smart Building

Linee guida per edifici
Intelligenti, sicuri e resilienti

Luca Girodo | Alfa Due

In/luca-girodo

White paper = tema strategico

- Nel 2025 è nato il Working Group 15 sulla Cybersecurity
- Obiettivo: definire linee guida per la sicurezza delle piattaforme OT negli Smart Building
- Oggi presentiamo il whitepaper *«Linee Guida per la Cybersecurity degli Smart Building»*

Perché siamo qui

La crescita degli Smart Building aumenta il rischio cyber

Punti chiave:

- crescita accelerata di IoT e building automation
- convergenza IT / OT / IoT
- aumento della superficie di attacco
- impatti su business e sicurezza fisica

> Uno Smart Building è una infrastruttura digitale critica

Architettura di uno Smart Building

Dal sensore al cloud

Schema:
- Sensori e attuatori
- BMS/BAS/HVAC
- Edge devices
- Server e analytics
- Cloud platform

Focus:
- forte interconnessione tra sistemi
- dati in tempo reale
- automazione intelligente

Principali minacce cyber

Dove nascono i rischi

Minacce:

- ransomware e DDoS
- accessi remoti compromessi
- dispositivi IoT vulnerabili
- firmware obsoleti
- protocolli non cifrati
- attacchi laterali IT → OT

> Ogni dispositivo connesso può diventare un punto d’ingresso

Impatti di un attacco

Cybersecurity = sicurezza fisica

Possibili conseguenze:

- blocco HVAC
- indisponibilità accessi
- fermo operativo edificio
- violazione dati
- danni economici
- rischi safety

Principi fondamentali di difesa

Security By Design

Elementi chiave:

- segmentazione rete
- MFA
- least privilege
- patch management
- monitoring continuo
- backup e resilienza

> La cybersecurity deve essere progettata fin dall’inizio

Standard e Compliance

Il nuovo scenario normativo

Framework principali:

- ISO 27001
- IEC 62443
- NIS2
- GDPR
- Cyber Resilience Act
- RED e Cybersecurity Act

Focus:

- Obblighi crescenti
- Governance del rischio
- Supply chain security

Zero Trust e convergenza IT/OT

Never Trust | Always Verify

Concetti:

- micro-segmentazione
- verifica continua identità
- controllo accessi
- IDMZ tra IT e OT
- monitoraggio centralizzato

Strategia Operativa

Come costruire uno
Smart Building resiliente

Roadmap:

- Asset inventory
- Risk assessment
- Segmentazione
- Hardening
- Monitoring SOC
- Incident response

> La cybersecurity è un processo continuo

Conclusioni

Il futuro degli Smart Building

Takeaway finali:

- digitalizzazione e cyber devono crescere insieme
- sicurezza IT e OT non sono più separate
- compliance europea sempre più centrale
- resilienza e continuità operativa diventano priorità strategiche

> Un edificio intelligente è sicuro tanto quanto è sicuro il suo componente più debole

Q & A