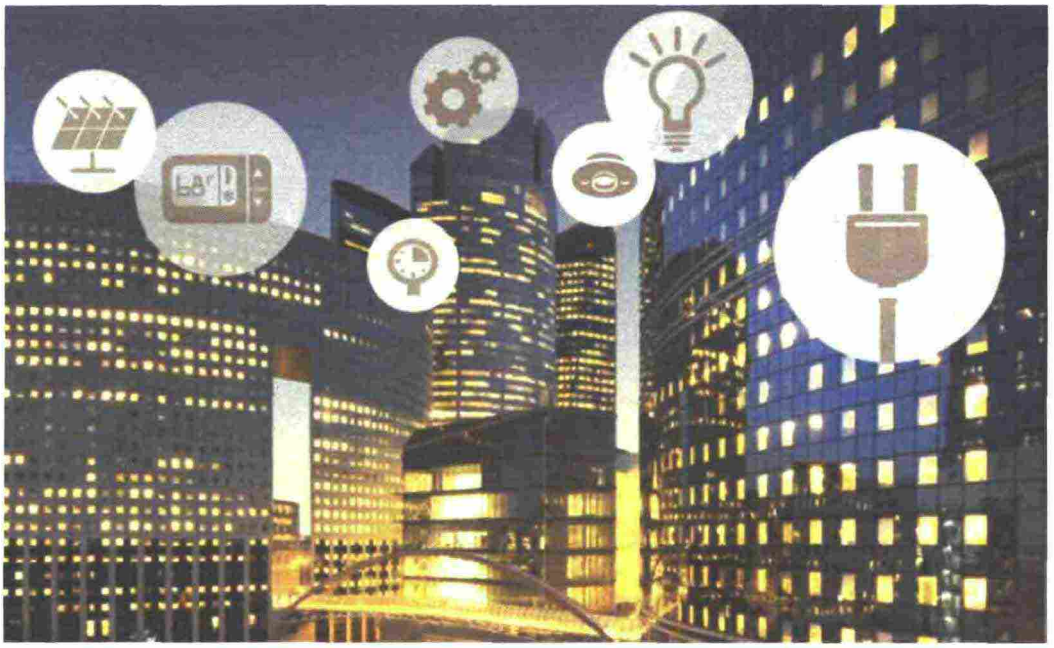
Sommario Rassegna Stampa

Progetti Concorsi
Il Sole 24 ORE
Settimanale
Data 19-03-2016
Pagina 1
Foglio 1

La sicurezza informatica diventa un parametro da considerare nella progettazione

Edifici a rischio hacker, ecco come proteggersi

DI MILA FIORDALISI



Dove c'è una connessione Internet e un traffico di dati esiste anche una minaccia di intrusione da parte di soggetti non autorizzati. Non fa eccezione il settore dell'edilizia in cui la rete è già una realtà con l'nternet of Things, con il building automation e - soprattutto - con il Bim, che implica una gestione totalmente fondata sulla collaborazione e comunicazione via rete.

Anche per gli edifici - sostengono pertanto gli esperti - si apre la partita della sicurezza informatica. Una partita che dovrà vedere in campo tutta la filiera delle costruzioni, a partire dai progettisti fino ad arrivare agli inquilini. La questione non è affatto futuristica.

Già si sono registrati a livello mondiale - e il fenomeno è in crescita - una serie di eventi "anomali" che hanno coinvolto obiettivi cosiddetti "sensibili" (edifici governativi, ospedali, scuole). Eventi attuati con il deliberato scopo di entrare in possesso di dati riservati, ma anche per interrompere servizi fondamentali come l'erogazione di elettricità o acqua. A dimostrazione di quanto il tema stia assumendo i contorni di un fenomeno da non sottovalutare, basti pensare che fra le vittime illustri c'è persino Google: nell'edificio che ospita la sede di Sidney, in Australia, è stato "hackerato" il sistema di building management dell'impianto di climatizzazione estiva e invernale.

«Il mercato è in evoluzione e le aziende devono muoversi da subito», dice Andrea Natale (coordinatore del gruppo Sicurezza integrata dell'Anie). «La cyber security va calata nell'intera filiera integrata del progetto», spiega Mario Caputi, amministratore delegato di in2it.

SERVIZIO E INTERVISTE ALLE PAGINE II-III

Progetti Concorsi
Il Sole 24 ORE
Settimanale
Data 19-03-2016
Pagina 3
Foglio 1 / 2

Parla Andrea Natale, coordinatore gruppo Sicurezza di Anie

«La cyber security parte dalla fase progettuale»

Il mercato è in evoluzione ma chi si arrocca perde la partita. Ne è convinto Andrea Natale, coordinatore del gruppo Sicurezza integrata di Anie Sicurezza, l'organismo che, in seno all'Anie, rappresenta le imprese (circa una novantina per 3.500 addetti) attive nei comparti dell'antintrusione, del controllo accessi, della videosorveglianza, della rivelazione automatica incendio e della building automation, per un giro d'affari annuo di circa 2 miliardi.

«Tutti i sistemi, anche quelli più tradizionali si sono evoluti e sono stati investiti dalla rivoluzione digitale e informatica - esosrdisce Andrea Natale -. Basti pensare che oggi moltissime soluzioni hanno una app associata e che la gestione a distanza degli impianti sta diventando sempre più una consuetudine. Il nostro comparto è stato coinvolto molto dalla rivoluzione digitale e la questione della cybersecurity diventerà importantissima».


Andrea Natale

Come si fa a raggiungere l'obiettivo di garantire la sicurezza impiantistica?

Bisogna partire dalla progettazione. L'edificio deve essere pensato all'inizio come soggetto a possibili intrusioni informatiche oltre che fisiche. E quindi vanno fatte simulazioni ad hoc, anche critiche. E prevedere ad esempio il back up dei dati gestiti attraverso la building automation in modo da poter ripristinare il più possibile in caso di attacco, ma anche di banali guasti o anomalie. Va da sé che le competenze informatiche diventano determinanti.

Anche quelle dei progettisti?

Certamente. Se il progettista non ragiona in questa logica e non ha adeguate competenze non darà indicazioni adeguate all'impiantista. E a catena ciò impatta su tutta la catena. La sfida informatica riguarda tutti: chi sviluppa il progetto, chi lo realizza e persino l'acquirente finale. Oggi la progettazione è sempre più integrata, c'è una forte interdipendenza di tutti i sistemi in campo. Non esistono più i "silos", ossia i sistemi stand alone. La "catena", insomma, deve essere tutta informata altrimenti si creano delle falle e la sicurezza non può essere garantita appieno.

Sembra un lavoro non da poco.

Per cominciare bisogna uscire dalla logica "hardware", quella tipica della progettazione di qualcosa che viene considerato solo un prodotto, ed entrare invece in quella di servizio. Bisogna pensare a tutto il ciclo di vita dell'edificio. Molte aziende si sono già evolute, passando da una produzione tradizionale a una produzione innovativa, cioè che fa leva su forti fondamenti dell'Information Technology. E sono nati nuovi attori; e altri ne nasceranno in futuro. Ma per tutti il trait d'union è quello della competenza informatica.

E in Italia esistono queste competenze specifiche?

Ci sono aziende molto preparate su questo fronte. Aziende che investono molte risorse. Poi c'è stata anche parecchia selezione naturale; ma del resto chi non si adegua alle nuove istanze, qualsiasi esse siano, sparisce sempre dal mercato prima o poi. Una cosa è certa: il driver non può essere il prezzo basso. Molti servizi innovativi sono ancora considerati un "optional" nelle nuove costruzioni e sull'esistente al momento sono pochi gli interventi che riguardano la disponibilità di funzioni evolute. Ma non ci si rende conto che "accedere" a distanza negli edifici è già possibile: attraverso le app ad esempio. E ciò quindi rappresenta già un problema, visto che ci sono potenziali "varchi" di

accesso di cui gli hacker possono approfittare anche semplicemente per virus che possono creare malfunzionamenti degli impianti.

E Quindi?

Quindi la questione va affrontata. Noi in Anie Sicurezza stiamo valutando di avviare un approfondimento sulla questione con i nostri associati e più in generale con chi viene interessato dalla questione. E non escludiamo corsi di formazione ad hoc. Inoltre riteniamo fondamentale il ruolo delle assicurazioni.

Qual è il ruolo delle Compagnie di assicurazioni e quando intervengono sulla questione?

Se le compagnie di assicurazioni nelle polizze per gli edifici considerassero chiave la qualità dell'impianto, ciò potrebbe stimolare a fare bene gli impianti in vista dell'analisi del rischio. Molta tecnologia oggi è commodity: non bisogna sottovalutare la questione, potrebbe esserci un proliferare di soggetti poco competenti, che vendono a prezzi competitivi ma non propongono soluzioni di qualità in grado di proteggere gli edifici da eventuali rischi di natura informatica.


«La cyber security parte dalla fase progettuale»