Sicurezza delle infrastrutture critiche? Serve un approccio olistico



“Per infrastruttura critica si intende qualunque sistema essenziale per il mantenimento delle funzioni cruciali della società e dell’economia: la sanità, l’alimentazione, la sicurezza, i trasporti, l’energia, i sistemi informatici, i servizi finanziari (…)”. È questa la definizione con cui la Commissione Europea presenta una iniziativa volta a raccogliere pareri pubblici in materia di nuove norme a protezione delle infrastrutture critiche nel territorio dell’Unione.

Le infrastrutture critiche rappresentano la spina dorsale della nostra economia, sicurezza e salute. Pensiamo, per esempio, all’energia elettrica che usiamo nelle nostre case, all’acqua che beviamo, ai trasporti che ci consentono di viaggiare ovunque desideriamo e ai sistemi di comunicazione su cui facciamo affidamento per scambiarci informazioni in ogni momento e luogo.

Poiché urbanizzazione, globalizzazione e interdipendenza delle infrastrutture fisiche e digitali hanno un impatto sulla nostra società ed economia, un’infrastruttura sicura, funzionante, sostenibile e resiliente è fondamentale per far funzionare il nostro mondo.

Funzionalità e sicurezza

Le aziende che operano nel settore delle infrastrutture critiche spesso necessitano dell’intera gamma di servizi e opzioni di sicurezza per garantire la funzionalità e la protezione degli asset e di tutto ciò che ruota attorno ad

essi. La competitività del mercato, tuttavia, le spinge a ridurre costi e ottimizzare i processi. È qui che deve entrare in gioco un partner tecnologico affidabile, capace, cioè, di affrontare ogni tipologia di problematica, dall'eliminazione dei tempi di inattività al miglioramento dell'ambiente di lavoro e della sicurezza, collegando tutto attraverso una gestione completa degli edifici.

Mantenere le operazioni ai massimi livelli di efficienza e affidabilità è fondamentale per tutte le aziende che consentono alla nostra società di funzionare. Tutte le aree di queste imprese sono, tuttavia, particolarmente vulnerabili a una serie di attività criminali come lo spionaggio industriale, il vandalismo, la criminalità organizzata, il crimine informatico e il terrorismo, i disastri naturali e le sfortunate conseguenze di errori umani o malfunzionamenti tecnici.

Un approccio a 360° con un focus sulla sicurezza

Centrali elettriche, raffinerie di petrolio, sistemi di trasporto pubblico o siti militari richiedono, come detto, operazioni efficienti, funzionalità continua e sicurezza per beni e persone. A tal fine è fondamentale, nella scelta del partner tecnologico, valutare chi sia in grado di adottare un approccio olistico che possa garantire efficienza e affidabilità dalla protezione perimetrale – per esempio affidandosi al sistema di gestione di security ed eventi C-CURE 9000 e ai collaudati controller di porte iSTAR, capaci di garantire sicurezza aziendale mission-critical e protezione delle persone – alle installazioni HVAC, dalla videosorveglianza – con le piattaforme hardware e software a marchio **American Dynamics** che assicurano agli utenti il massimo livello di sicurezza e visibilità attraverso l'efficientamento delle risorse con video streaming intelligente ad alte prestazioni e Cloudvue la tecnologia di

videosorveglianza cloud a cui si affidano migliaia di aziende per semplificare la sorveglianza, perfezionare il controllo degli accessi e disporre dell'intelligence necessaria per ottimizzare le operazioni di sicurezza e l'efficienza organizzativa – fino alla gestione completa degli edifici. I vantaggi consistono nell'avere un unico punto di contatto per la progettazione, integrazione e funzionamento continuo dell'infrastruttura critica.

La sicurezza fisica e informatica è, senza dubbio, l'aspetto sui cui porre una attenzione maggiore, considerata l'importanza degli asset in gioco.

In riferimento alla seconda, i facility manager oggi richiedono che le soluzioni per gli smart building, siano anche cyber-resistenti. Per questo abbiamo sviluppato un approccio completo al ciclo di vita dei sistemi e una serie di best practice che sono in grado di contribuire a proteggere una determinata infrastruttura contro una serie di potenziali minacce informatiche.

Il nostro team di esperti di cybersecurity progetta, implementa e supporta i sistemi connessi degli edifici, allineandoli con i programmi di sicurezza in essere nell'infrastruttura, creando una difesa a strati per informazioni, beni e privacy, capace di rispondere rapidamente quando si presentano attacchi.

Se la sicurezza informatica ha spostato la linea di confine per la Security in tempi recenti, non è assolutamente da trascurare la protezione fisica delle strutture. Oggigiorno, infatti, estrema attenzione viene posta sulle minacce che provengono dal mondo informatico ma i temi della sicurezza tradizionale, se affrontati con scarsi o errati investimenti, possono rendere vulnerabili le infrastrutture critiche anche da classici attacchi come tentativi di intrusione e sabotaggi. La protezione di questi siti va affrontata attraverso la correlazione di tutti i sistemi di sicurezza storicamente

preposti ad essa, videosorveglianza, controllo degli accessi, antintrusione, facendo leva sulle moderne possibilità di analisi dettate dall'intelligenza artificiale e da piattaforme di integrazione (tipicamente PSIM) che diano vita a una consapevolezza situazionale garantita dall'unione di tutti i sottosistemi e la gestione degli stessi tramite delle chiare procedure operative (SOP) per il personale di vigilanza o chiunque sia la figura aziendale preposta all'utilizzo operativo di questi sistemi.

La gamma di soluzioni che Johnson Controls ha a disposizione per rispondere a questo tipo di sfida è estremamente estesa, passando da soluzioni di controllo accessi ad elevati standard di sicurezza con moderne tecnologie biometriche (impronta, facial recognition…) alla videosorveglianza, sempre più terreno di applicazioni di Intelligenza Artificiale, alla più classica antintrusione ma affrontata con soluzioni all'avanguardia, come la tecnologia PowerG.

L'importanza dell'analisi dei dati

Oltre a tutto questo, inoltre, Johnson Controls sviluppa e commercializza soluzioni di livello militare – come il Tyco Radar – a costi commerciali per la difesa delle aree più delicate e dei perimetri, unendo tecnologie di rilevazione radar ai più moderni algoritmi di video-analisi e machine learning per la classificazione delle intrusioni e la diminuzione dei falsi allarmi.

Un partner tecnologico come Johnson Controls è in grado di supportare le aziende nel raggiungimento degli obiettivi posti dalle sfide di sicurezza contemporanee, ed è in grado di farlo anche attraverso le nuove "soluzioni digitali" Open Blue che consentono di portare la sicurezza al di fuori delle mura, combinando tecniche di calcolo e valutazione del rischio ad informazioni provenienti dal web e all'analisi dei sistemi di sicurezza tradizionale esistenti.

Il vantaggio principale nella scelta di Johnson Controls risiede quindi proprio nella capacità di affrontare le minacce di attacco, siano esse fisiche o informatiche, con la possibilità di attingere ad un'ampia gamma di soluzioni e fornirne una olistica all'utente finale, rispettando i benefici indicati dal significato stesso del concetto che vuole che in un sistema complesso il tutto sia maggiore della somma delle parti.

A cura di **Ivan Mazzoni**, *Sales Manager Building Solutions, Continental Europe, di Johnson Controls*

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/sicurezza-delle-infrastrutture-critiche-serve-un-approccio-olistico/