Proteggere i data center da intrusioni e manomissioni interne

di Marco Censi, Regional Sales Manager Italia per OPTEX

I data center sono fondamentali nella maggior parte delle operazioni istituzionali e commerciali odierne. Con server collegati in rete e apparecchiature di comunicazione, permettono ad aziende e istituzioni di accedere, trasferire e archiviare le informazioni digitali. I computer di questi centri sono raffreddati meccanicamente per evitare surriscaldamenti e si predispongono sistemi di alimentazione alternativa per evitare interruzioni del servizio. Il tipo di dati che gestiscono e proteggono può variare, ma di certo si tratta di dati importanti e sensibili.

Di conseguenza, gli ambienti occupati da sistemi tanto complessi, costosi e interdipendenti devono essere difesi da qualsiasi accesso non autorizzato.

È normale che gli edifici che ospitano i data center siano tutelati da un primo livello di sicurezza costituito da recinzioni perimetrali e barriere ma è indispensabile progettare un secondo livello nelle sale dei generatori e dei rack dei server, onde evitare che criminose intrusioni provochino danni o manomissioni gravi quanto quelli causati dai cyber-attacchi.

Soluzioni di sicurezza perimetrale ed esterna

Come tutti i siti sensibili, i data center richiedono più livelli di protezione tramite la messa in sicurezza di un'eventuale recinzione (che può essere tagliata o scavalcata), la protezione del perimetro mediante barriere e/o dei tetti e delle pareti esterne (protezione da eventuali scalate, perforazioni o semplici ingressi da uscite di sicurezza). Per questo si consiglia una combinazione di più livelli di sicurezza: un sistema recinzione/muri esterni e un "muro virtuale" per rilevare eventuali intrusioni ed essere in grado di fornire una risposta tempestiva.

Tipicamente, i sensori a fibra ottica sono applicabili direttamente su recinzioni o muri oppure a terra, perché registrano le vibrazioni causate dai tentativi di tagliare la linea perimetrale o di scavalcarla. Estremamente affidabile, tale soluzione offre anche un basso costo di gestione.

Mediante i sensori **OPTEX** a tecnologia LiDAR, i **REDSCAN**, è possibile creare delle pareti virtuali nelle varie zone d'accesso come cancelli, tornelli pedonali, banchine di carico, uscite d'emergenza; perfino coprire un'intera parete dell'edificio.

È inoltre capitato che gli intrusi siano riusciti a perforare le pareti o a entrare da lucernari sui tetti degli edifici. Per la protezione delle pareti, OPTEX suggerisce due tecnologie, a seconda dell'uso: i sensori a fibra ottica potranno rilevare le vibrazioni del trapano sul muro mentre il muro virtuale creato dal sensore laser rileverà chiunque si avvicini all'area delimitata. Il laser virtuale LiDAR potrà proteggere il tetto esterno con estrema precisione, dal momento che non risente minimamente delle condizioni di luce o di quelle atmosferiche. Inoltre, la stessa tecnologia potrà creare un soffitto virtuale per l'interno, funzionando anche nell'oscurità più totale o a basse temperature, condizioni queste comuni all'interno dei data center.

Inoltre, se si desidera aggiungere una verifica visiva e una protezione a lungo raggio, REDSCAN Pro è munito di una telecamera integrata che permette una copertura ideale per le strutture molto ampie.

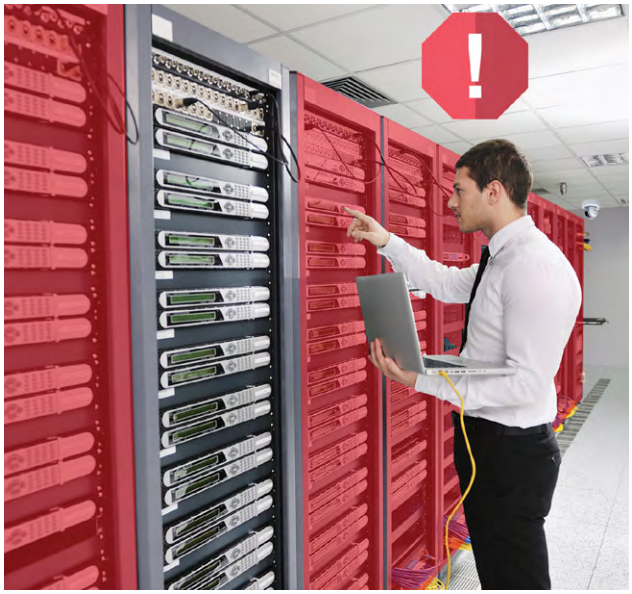
Soluzioni di sicurezza interna e piattaforme software di gestione

I sensori **REDSCAN** forniscono una rilevazione talmente accurata da offrire addirittura le coordinate X, Y esatte dell'intrusione. Ecco perché questo tipo di tecnologia è molto ricercata per proteggere i rack all'interno delle server room: è infatti in grado di individuare esattamente il luogo in cui è avvenuta una manomissione, il che permette di velocizzare i tempi di risposta e affrontare gli incidenti con maggiore consapevolezza.

REDSCAN consente di creare diverse aree di rilevamento, ad esempio corrispondenti ad ogni rack, e disattivare la zona quando un tecnico si sta occupando della manutenzione, mantenendo al contempo in sicurezza tutte le altre aree.

Quando si desidera sfruttare appieno tali e tante informazioni, i sensori vanno utilizzati unitamente a piattaforme software che abbiano le coordinate integrate, come le piattaforme **Genetec**.

Una piattaforma di sicurezza unificata, come il **Security Center Genetec**, può migliorare i tempi di risposta e aumentare la sicurezza del sito. Un sistema unificato con un'interfaccia basata su mappa permette al personale di trovare rapidamente, grazie alle coordinate X, Y e al supporto delle riprese video, il punto esatto dell'intrusione e una visione completa della scena. Grazie all'unificazione, la soluzione inoltre consente di visualizzare sulla dashboard anche il sistema di controllo accessi. In questo modo, le porte nella server room potranno essere chiuse se LiDAR rileverà un accesso non autorizzato o una manomissione.



Il Ministero per l'Innovazione tecnologica e la transizione digitale ha inserito tra le priorità del nostro Paese la *"realizzazione di un Polo Strategico Nazionale per i servizi che trattano dati critici, sotto controllo e indirizzo pubblico, per dotare la Pubblica Amministrazione di tecnologie e infrastrutture cloud che possano beneficiare delle più alte garanzie di affidabilità, resilienza e indipendenza."*[1] In tale ottica è stato lanciato un concorso per la realizzazione del parco data center della Pubblica Amministrazione.

Considerando i rischi che tali infrastrutture possono correre, è evidente come si debba progettare con cura la loro protezione e attraverso sistemi di sicurezza flessibili, precisi e affidabili.

REDSCAN Pro, la nuova generazione LiDAR di OPTEX

OPTEX
Sensing Innovation

Contatto:
OPTEX
Tel. +39 351 9272789
enquiry-it@optex-europe.com
www.optex-europe.com/it

[1] https://innovazione.gov.it/progetti/infrastrutture-digitali-e-cloud/