Giovanni Villarosa (*)

ANTINTRUSIONE IN CLOUD: E LA SICUREZZA CYBER?

Installazione for Dummies, rubrica di "suggerimenti in pillole" ideata per tutti i professionisti della Security (installatori e progettisti), torna sull'argomento spinoso della sicurezza cyber dei sistemi antintrusione collegati in Cloud!

(*) Laureato in Scienze dell'Intelligence e della Sicurezza, esperto di Sicurezza Fisica per Infrastrutture, CSO e DPO, membro del comitato tecnico-scientifico del CESPIS, Centro Studi Prevenzione, Investigazione e Sicurezza **www.cespis.it**

È noto a tutti come le tecnologie trasferite sulla "nuvola" stiano trasformando la società in una collettività digitalizzata sempre più connessa e interdipendente; ebbene, da questa "digital revolution" non è rimasto ovviamente immune il settore della sicurezza integrata, che - sfruttando le potenzialità disponibili da remoto nella piattaforma cloud - può gestire in maniera efficiente, attraverso una semplice App disponibile su smartphone o tablet, sistemi complessi come il controllo degli accessi, l'antintrusione, la videosorveglianza, o i sistemi antincendio.

Entro il 2025 l'edge computing si attesterà sui 31 miliardi di dollari (erano 12 nel 2020)

Intrusione e cloud

Per meglio comprendere il salto tecnologico compiuto dalla nuvola, pensiamo alla "stagionata" antintrusione, una volta gestita esclusivamente attraverso il classico doppino telefonico analogico (combinatore PSTN con comandi DTMF): questo balzo però non ha riguardato solo le connessioni cablate, perché soppianta contemporaneamente anche il mondo (per allora) "avanzato" dei combinatori telefonici GSM, seppur più affidabili dei PSTN giacché meno soggetti ai sabotaggi, ma pur sempre limitati nell'operatività (comandi interattivi tramite elementare messaggeria SMS).
Quindi il cloud computing ha saputo "scaricare a terra" un'ulteriore capacità estranea alle classiche infrastrutture IT: quella di condividere risorse tra dispositivi eterogenei e diametralmente opposti tra loro, garantendo una coabitazione dei sistemi e la perfetta integrazione operativa dei dati ricevuti (allarmi, segnali video, etc).

Bello ma...

Sul tema del pieno utilizzo della nuvola nel campo della security si riscontra purtroppo ancora molta superficialità: leggendo qua e là nel web, all'interno delle discussioni tra professionisti nei vari blog riguardo alle connessione e gestione in rete di tutta la catena dei sistemi di sicurezza, preoccupa la totale mancanza di consapevolezza sull'esposizione al rischio cyber dei sistemi inseriti in cloud. Non è pensabile che un installatore – oggi - non tenga conto dei pericoli (privacy e trattamento dati) provenienti dal cyber crime, delle minacce e della crescita delle superfici di attacco che la trasformazione digitale e l'adozione dei device IoT hanno materializzato, esponendo gli impianti ad ogni tipologia di attacco. Parliamo di impianti complessi per composizione e finalità d'uso: per un professionista la sicurezza logica dovrebbe dunque essere la prima vulnerabilità considerata quando stilerà l'elenco nella sua analisi del rischio.

Opportunità e rischi

Insomma, la tecnologia introdotta dal cloud ha creato grosse opportunità, tanto operative quanto manutentive, riducendo ad esempio la presenza in sito - inutile e dispendiosa - per la stragrande maggioranza dei malfunzionamenti temporanei (software, connettività reti, segnali gsm, etc) il più delle volte risolvibili da remoto, creando in cambio un'efficace indipendenza nella gestione degli impianti da parte della proprietà (gestione password, verifica log, guasti, ricerca eventi, notifiche push, etc), come pure una gestione condivisa con le sale operative degli istituti di vigilanza privata. Tutte opportunità che andranno però sempre bilanciate con i rischi connessi!

Opportunità	**Meno presenza in loco dell'installatore/manutentore**
	L'utente gestisce gli impianti in autonomia
	Gestione condivisa con le sale operative degli IVP
Rischi	**Attacchi cyber**

Mitigazione e convergenza

Mitigazione e convergenza - due argomenti molto sentiti, e i dati sono abbastanza chiari: 8 responsabili IT su 10 auspicano un ambiente di sicurezza (fisica e logica) più unificato, integrato e convergente, mentre un'azienda su due opera con l'infrastruttura di sicurezza fisica e quella di rete dati disconnesse o male integrate tra loro; dunque, il complesso panorama della sicurezza integrata di oggi richiede molta più attenzione.

Edge Computing

Infine, due parole sull'Edge Computing, ossia l'elaborazione dei dati a "margine": una tecnologia che potenzierà ulteriormente (nelle intenzioni) l'operatività dei sistemi di sicurezza basati sulla sensoristica antintrusione, divenuta ormai un componente essenziale dell'internet delle cose (IoT). E' noto come l'archiviazione su cloud (nella sicurezza si usa quello di terze parti) comporta da sempre anche degli svantaggi: problemi di latenza, problemi di sicurezza dei dati, difficoltà nella scalabilità dei sistemi. Ebbene, l'edge computing potrebbe aprire nuovi scenari nella gestione in cloud di tali sistemi. Da ultimo: stime di mercato accreditano entro il 2025 l'edge computing intorno ai 31 miliardi $ rispetto ai 12 miliardi del 2020. Dati che devono far riflettere sulle figure professionali che saranno richieste nell'immediato futuro...

Sulla cybersecurity negli impianti di sicurezza integrata, l'autore ha dedicato ampio spazio formativo, teorico e pratico, all'interno del nuovo programma didattico del laboratorio Sicurezza Integrata 4.0, attivato presso il centro formazione Ragazzi Don Bosco di Roma - un progetto didattico focalizzato sulla formazione, a tutto tondo, dei nuovi professionisti della security, con diverse ore di lezioni dedicate alla sicurezza logica degli impianti speciali connessi alla rete. Questo sia all'interno del terzo anno di corso, dove i ragazzi imparano i "fondamentali" elettrotecnici dei sistemi e la loro basica integrazione, sia nella formazione di livello "avanzato" per gli studenti del quarto anno, con lezioni più dettagliate sulle vulnerabilità e le contromisure necessarie da progettare e realizzare poi nel concreto per salvaguardare "informaticamente" le molteplici e differenti infrastrutture digitali create (accessi, videosorveglianza, domotica, antintrusione, etc).