Cosa possono fare le aziende per fronteggiare le attività cybercriminali?

STT per l'ICT Security e per la Cyber Defence

Infrastrutture chiavi in mano COMSEC per garantire la sicurezza delle comunicazioni, sistemi integrati per la protezione della Rete ed approccio strutturato.


Paolo Calzolari, Direttore Tecnico STT

Con l'innovazione tecnologica (Internet, Cloud, Mobile,...) e in un mondo sempre più iperconnesso grazie all'**IoT**, le aziende sono soggette da più lati a nuovi attacchi e il **concetto di sicurezza informatica ICT si espande** in quello più vasto di **cyber security**.
Le minacce si moltiplicano e cercano di violare l'integrità, l'affidabilità della rete, i dati sensibili e quelli personali attraverso sia la tradizionale rete informatica sia nuove tecniche, che vedono come veicolo di attacco i dispositivi di sicurezza fisica (videosorveglianza, controllo accessi, IoT, etc.).
Il **Sans Institute**, ente di riferimento a livello internazionale per la Security, mostra come i costi generati globalmente dalle attività cybercriminali sono quintuplicati in pochi anni (da 100 miliardi di Dollari nel 2011 ad oltre 500 miliardi nel 2017 nel settore privato) e come il Cyber Espionage abbia generato negli Stati Uniti danni per oltre 600 Miliardi di Dollari.
A livello nazionale ciò è ribadito dal **Rapporto Clusit 2017** sull'**Industria italiana**: gli **investimenti nell'ICT Security sono cresciuti** in un solo anno **del 5%**, sfiorando il miliardo di Euro, a fronte di un crescente numero di attacchi informatici che sono ormai all'ordine del giorno per aziende e privati.

Quali sono, quindi, le strategie che le aziende devono implementare per fronteggiare questa **nuova, impellente necessità**?
Le parole d'ordine sono tre: **ICT Security, Cyber Defence ed Approccio strutturato**. Se da un lato, cioè, è fondamentale sviluppare un **sistema integrato di contromisure** alle minacce alle infrastrutture critiche ed alla protezione dei dati sensibili, dall'altro è bene che **tutte le aree aziendali** siano coinvolte nel processo di Cyber Defence tanto da coinvolgere sempre più spesso il **Risk Manager** oltre che l'**ICT Manager**.
Alla base di questo, è essenziale affidarsi ad operatori del settore preparati e con una visione globale, capaci di garantire un supporto al problema a 360 gradi.
STT, System Integrator presente dal 1988 sul mercato delle Telecomunicazioni italiano, **offre una serie di servizi focalizzati sul tema dell'ICT Security e della Cyber Security**: dalla consulenza, alla progettazione fino all'installazione di soluzioni specifiche per la Cyber Defence.
Una specializzazione questa che **STT ha maturato soprattutto nel settore della Difesa,** con Clienti di primaria importanza presenti sul territorio **nazionale ed estero**, dove la richiesta di sicurezza informatica e fisica è ai massimi livelli.
Tra le Soluzioni offerte vi è la **realizzazione chiavi in mano di infrastrutture omologate COMSEC**, che riguardano la creazione degli assetti edili e di schermature, sistemi di sicurezza fisica ed antincendio, impianti di videosorveglianza, cablaggi strutturati in F.O., installazione di apparati di rete classificati.
Inoltre, in ambito ICT, STT propone un **sistema integrato** di prodotti SIEM, antivirus endpoint centralizzato e UTM **per migliorare la visibilità della sicurezza del Network**.
La recente partecipazione dell'azienda in qualità di **Partner Tecnologico a TaoSicurezza 2018** *(n.d.r. S News N. 45, questo numero, pagg. 18 – 23)*, evento di riferimento per l'intera filiera nazionale della security, ha ribadito **l'attenzione che sta ponendo a questa area tecnologica, sempre più strategica nel settore delle Telecomunicazioni**.
Paolo Calzolari, Direttore Tecnico STT: ***"Gli investimenti in ICT Security*** *da parte delle aziende italiane* **crescono** *di anno in anno. Si tratta di un dato significativo,* ***ma insufficiente*** *se paragonato al valore del mercato italiano di beni e servizi ICT e alla percentuale di PIL".*
"Si evince che ***in Italia*** *il mondo imprenditoriale sta maturando una conoscenza dei rischi che incorre, ma la strada verso una consapevolezza completa è ancora lunga, perché* ***le minacce e gli attacchi informatici riguardano più fonti, non solo più la rete IT****: dai computers, ai devices di rete, ai protocolli di comunicazione, ai devices mobili, alle applicazioni, etc."*
"La soluzione è quella di lavorare ad un ***approccio alla sicurezza strutturato e integrato****: avere cioè una* ***visione globale della propria azienda*** *e sapere quali sono le informazioni strategiche da proteggere e come tali informazioni fluiscono all'interno dei propri* ***sistemi ICT e OT****".*