

Andrea Boggio - Intervista al Forum ICT Security 2018

Author : Redazione

Date : 13 novembre 2018



Andrea Boggio

Business Development Manager presso Fastweb Spa

Il panorama delle minacce cyber è in costante evoluzione; attualmente stiamo assistendo ad una convergenza tra mondo ICT e mondo reale delle cose, con conseguenze che possono essere dirompenti nel mondo fisico. L'IoT vede miliardi di oggetti interconnessi tra loro che sviluppano una quantità di dati mai vista prima. La conseguenza di ciò è che più si connettono oggetti più cresce la superficie di attacco andando incontro a vulnerabilità cui l'utente medio non è troppo sensibile.

Le aziende devono capire che il loro business deriva sempre più dai sistemi informativi, da qui la necessità di capire, attraverso apposite analisi del rischio cyber, quanto i rischi informatici insistono sui loro asset IT. Per un'azienda diventa una questione di costi/benefici, dovrà quindi valutare se dotarsi di strutture interne per mitigare i rischi oppure affidarsi a gestori di sistemi di sicurezza assistita. Ovviamente la situazione per aziende private e pubbliche è simile ma non uguale, dal momento che le seconde hanno maggiori vincoli soprattutto per quanto riguarda le spese. È però importante fare formazione, parlarne anche sui media più mainstream, non solo su quelli di settore, partire anche dalla scuola. Si pensi agli smartphone, perennemente connessi e di conseguenza potenzialmente sempre sotto attacco anche se non ci si pensa mai.

Il SOC è un'entità organizzativa che si caratterizza per delle capability tecniche molto evolute, legate alla difesa dagli attacchi cyber ed anche per alcuni aspetti operativi, di processo, molto specifici. Il SOC, sostanzialmente, opera su finestre temporali H24, monitora costantemente la sicurezza e, se possibile, deve operare in maniera standardizzata.

Domande:

1. Nell'attuale panorama delle minacce e di evoluzione della cybersecurity quali sono gli elementi di maggiore attenzione?
2. Come possono gli individui e le aziende/organizzazioni mitigare i rischi cyber?
3. Quali sono le principali caratteristiche di un Security Operations Center?

[Vai all'evento Forum ICT Security 2018](#)