CONSULENZA
E RISORSE

Cyber spionaggio:

La frontiera del crimine informatico

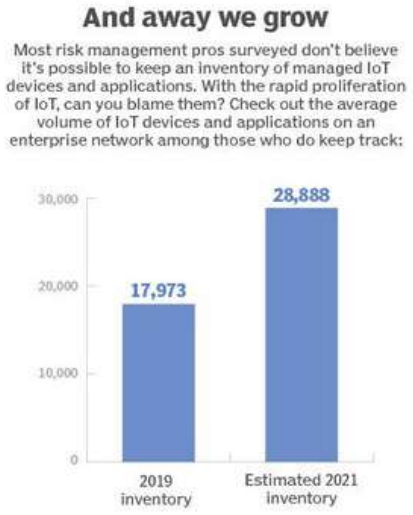
– A cura del Dott. Alessandro Sigismondi –

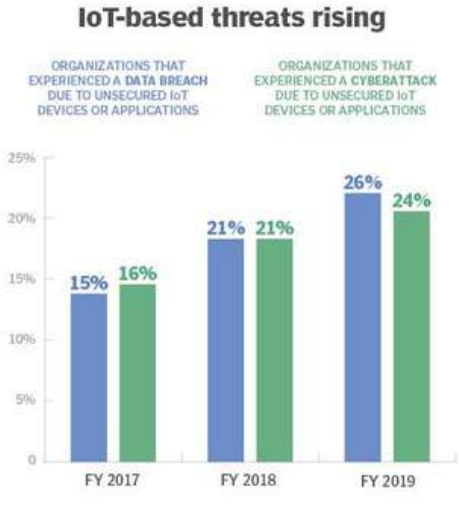
Introduzione

I cyber criminali operano ormai con tecniche militari come il ricorso a mercenari e specializzate su diverse categorie di aziende, senza particolari distinzioni di settore e tecnologie.

Negli ultimi mesi gli obiettivi più sfidanti per gli attaccanti hanno interessato l'ambito dell'Internet of Things, (IOT); l'impatto di questi ultimi con il tempo sarà sempre più invasivo poiché l'area di attacco aumenterà vertiginosamente con la diffusione della tecnologia e oltre alla mera acquisizione o modifica fraudolenta dei dati, si potranno registrare anche ripercussioni sull'incolumità delle persone.

Tra le attività di hacking non ci sono solo attacchi distruttivi ma anche lo **spionaggio industriale** attraverso le vulnerabilità dei dispositivi. Quando si pensa a un attacco informatico, **il pensiero corre ai ransomware e ad altri malware in grado di danneggiare i sistemi IT dell'azienda.**
In realtà, uno dei maggiori rischi legati alla security riguarda lo spionaggio industriale e commerciale, che è vecchio come il mondo e addirittura anteriore a quello militare e che nel nuovo panorama iper-digitalizzato, rappresenta ormai un fenomeno dalle dimensioni in costante crescita.





Fonte: searchsecurity.techtarget.com

Internet e le nuove minacce informatiche

Tutti i sistemi connessi a Internet sono sempre soggetti a minacce, non importa quanto siano protetti. **Nessuna barriera creata da un software può prevenire completamente l'errore umano nel codice di un programma o nel comportamento dell'utente**. Per questo, i dispositivi che hanno funzionalità importanti o che contengono informazioni top secret non sono normalmente connessi a Internet.

È sempre meglio convivere con questa scomodità piuttosto che dover poi affrontare le conseguenze di una intrusione o di un intervento esterno su dati o dispositivi. È così che sono protetti, ad esempio, i sistemi di controllo di grandi impianti industriali e i computer di alcune banche.

Si potrebbe pensare che offline ogni segreto sia al sicuro: senza Internet, non dovrebbe esserci fuga di dati. Purtroppo non funziona così: le tecniche di trasferimento dati in remoto adottate già da tempo dai servizi segreti sono diventati sempre più accessibili agli utenti comuni e alcuni metodi utilizzati nei film di spionaggio sono ormai alla portata di tutti.

continua...

CONSULENZA
E RISORSE

info@consulenzaerisorse.it
P.IVA IT02093620686

MILANO
SEDE LEGALE E OPERATIVA
Viale Gran Sasso, 11
20131 Milano
Tel. +39 02 40702009

PESCARA
SEDE OPERATIVA
Via A. Caldora, 4
65125 Pescara
Tel. +39 085 9561670

Il nostro Sito

Il nostro Company Profile

Il nostro Video