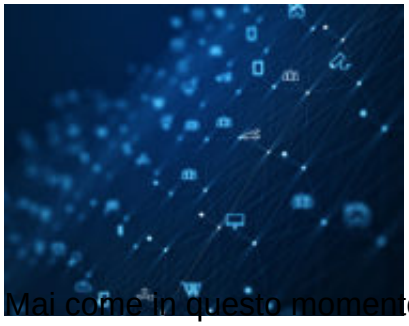
Cybersecurity vs Internet delle cose. Quale scenario ci attende?

Author : Raffaele Bisegna

Date : 29 Luglio 2020



Mai come in questo momento storico c'è stata una **trasformazione digitale** così capillare. Lo chiamano Internet delle cose, ma forse sarebbe più coretto chiamarla Internet della vita. Sì, perché ogni oggetto, azione e pensiero presto sarà gestito e veicolato attraverso la rete Internet. Alcuni esempi? All'interno di un'abitazione ormai molte persone hanno il proprio termostato collegato a un'app e, dunque, raggiungibile dal proprio smarthphone. Tutti (o quasi tutti) abbiamo un'app che permette di collegarci ed effettuare movimenti attraverso il proprio conto corrente bancario.
Presto - anzi molto presto - questo proliferare di interconnessioni aumenterà vertiginosamente, arrivando a connettere praticamente tutto quello che ci circonda.

Ma l'internet della vita non si ferma solo nel quotidiano. Va molto oltre e riguarda, o riguarderà a breve, una serie di **dispositivi "salva-vita" applicati in medicina** come *pacemaker*, sonde, siringhe intelligenti, che saranno interconnesse via Internet. Per non parlare di tutta una serie di *asset* strategici tipici di tutte le nazioni quali porti, aeroporti, dighe o centrali energetiche (comprese quelle nucleari), che saranno sempre più interconnesse in una sola rete, ovvero la rete Internet.

Lo scenario è indubbiamente positivo, perché l'interconnessione di tutto quello che ci circonda permette un utilizzo più rapido, semplice ed efficiente, miglioramento quindi sensibilmente la qualità della nostra vita. Tutto molto bello se non fosse per il **problema della sicurezza**, o per meglio dire della *Cybersecurity:* perché se tutto questo presto sarà così capillarmente interconnesso, saranno invitabili scenari di grande incertezza per quanto riguarda la sicurezza delle informazioni e dei dati coinvolti. È necessario, quindi, sviluppare piani adeguati e risolutivi per prevenire e gestire gli accessi non autorizzati.

Basti pensare alle possibilità nefaste che un **accesso non autorizzato** presso una qualsiasi infrastruttura informatica potrebbe generare: parliamo ad esempio di server dati di tribunali o ospedali. E perché non ricordare che, già sei anni or sono (settembre 2014), la multinazionale FCA, guidata dal manager di origini abruzzesi Sergio Marchionne, fu costretta a richiamare un milione e quattrocentomila veicoli a causa di una falla informatica nelle centraline delle automobili, potenzialmente accessibile dall'esterno da persone non autorizzate e mentre l'auto

fosse stata in marcia?

Bene, lo scenario futuro è ormai chiaro. Ma come ci proteggeremo dai possibili attacchi informatici e quali saranno i protocolli da adottare?

Internet non è un luogo sicuro

C'è un problema di fondo da non sottovalutare, anzi probabilmente è il problema più rilevante: la rete più famosa e utilizzata oggi nel mondo, ovvero la rete Internet, non è stata ideata per comunicare fra persone che non si fidano e non si conoscono. Questo non è un dettaglio da poco, anzi! La reteInternet infatti nasce per permettere la comunicazione fra alcune università americane; comunicazioni cioè fra soggetti che si conoscevano e che condividevano informazioni sicure, ovvero prive di software malevolo. Su questa stessa rete, oggi, seppur con protocolli di sicurezza e gestioni diverse, stiamo implementando l'interconnessione di tutti i nostri oggetti e servizi, anche i più i delicati come poc'anzi elencato. Volendo utilizzare un paragone, è come voler pretendere di entrare all'interno di un laboratorio pieno di agenti chimici estremamente pericolosi, farlo senza indossare alcuna protezione e ipotizzare che tutto andrà bene. Ovviamente, non andrà tutto bene. A meno che non vengano adottate opportune precauzioni.

Internet delle cose e cybersecurity, come difendersi?

Volendo evitare di entrare in trattazioni troppo tecniche, è chiaro che sarà necessario per evitare conseguenze disastrose causate dall'utilizzo dell'internet delle cose, procedere all'attuazione di processi e protocolli per garantire un utilizzo sicuro dei nostri servizi e dei nostri oggetti interconnessi. È un lavoro che dovrà essere svolto su più livelli e da tutti gli attori protagonisti. In particolare:

- gli Stati dovranno definire le linee guida di attuazione, ovvero le regole di sicurezza che tutti i produttori di servizi dovranno rispettare con estrema attenzione. Qui sorge evidentemente la necessità di implementare un **organo internazionale indipendente** e autorevole di gestione e controllo, esattamente come oggi avviene per la gestione della sanità tramite l'OMS. È impensabile che ci possano essere protocolli e indicazioni diverse da paese a paese: tutti nel mondo dovranno rispettare gli stessi protocolli, la forma spinta di globalizzazione oggi presente nel mondo non lascia altra via d'uscita;
- i produttori di beni e servizi interconnessi dovranno rispettare con attenzione tutte le prescrizioni fornite dagli organi competenti, fornendo quindi **certificazioni** sulla sicurezza in rete dei propri prodotti e servizi e fornendo, inoltre, la possibilità alle autorità competenti di accedere al proprio codice sorgente in un qualsiasi momento;
- l'interconnessione e lo scambio dei dati dovrà avvenire con **protocolli sicuri e cifrati**, anche qui nel pieno rispetto di prescrizioni forniti dagli organi competenti;
- le aziende di ogni dimensione dovranno attuare precise **procedure di sicurezza informatica** specifiche per lo scambio di informazioni in rete, con il supporto anche di specialisti esterni qualora all'interno non vi fossero le opportune competenze necessarie;

- i registri delle operazioni di interconnessione (*log*) dovranno essere riclassati come *asset* di carattere strategico da parte delle nazioni, in quanto ogni processo di interconnessione dovrà fornire **opportune tracce**, limitando e combattendo la possibilità di connessioni *bridge* anonime su server "di rimbalzo".

Naturalmente, anche l’utilizzatore finale potrà adottare una serie di precauzioni per limitare la possibilità di accessi abusivi. Ma qualsiasi buon comportamento è da ritenersi del tutto inefficace se il sistema di interconnessione (rete Internet) non verrà resa realmente sicura e affidabile. È da qui che si inizia a combattere la battaglia sulla sicurezza informatica dei prossimi 20 anni.

Articolo a cura di **Raffaele Bisegna**