Corriere del Ticino
LUNEDÌ 26 NOVEMBRE 2018

L'OPINIONE LORENZA BERNASCONI*

INTERNET DELLE COSE (IoT), LE SPIE TRA NOI

L'acronimo IoT o meglio «Internet delle cose» indica qualsiasi oggetto che può connettersi e comunicare tramite la stessa Internet.
Il fulcro dell'intelligenza dello IoT consiste nei servizi associati tra la rete web e ogni singolo oggetto facendo diventare «smart» un frigorifero di casa, un contatore di uova, un dispender digitale per il cibo dei nostri piccoli amici a quattro zampe o una coperta che permette di raccogliere i dati sulle abitudini notturne e predispone la temperatura del letto.
L'Internet delle cose non è una tecnologia ma una sintesi di tecnologia estesa nella rete dove tutto è possibile. Viene sfruttata l'innovazione digitale associata all'evoluzione mobile e questo binomio rende intelligente tutta la filiera degli oggetti.
Questa estensione di Internet sta connettendo un numero quasi infinito di oggetti. Si stimano oltre 30 miliardi di oggetti connessi entro il 2020 ovvero tra soli due anni da oggi. Conseguentemente a questa vera e propria esplosione dell'uso dello IoT, tutte le problematiche di sicurezza sono cresciute di pari passo.
Ogni singolo dispositivo IoT è connesso con la rete di casa e quindi al web e questo rappresenta una potenziale porta di accesso per i nuovi malintenzionati. In molti dispositivi IoT ci sono un chip, una telecamera, un microfono o un sensore. Di conseguenza, le preoccupazioni per la privacy sono fortemente incrementate e i timori di spionaggio digitale sono accresciuti a livello globale.
Qual è la cosa peggiore che potrebbe accadere nell'uso di questa evoluzione della rete?
Anche se non esistono ancora dei microonde che identificano i loro proprietari, molti altri dispositivi domestici nell'internet degli oggetti hanno una comprovata esperienza nella raccolta di informazioni personali.
Ecco alcuni esempi che potrebbero interessarvi per meglio comprendere le potenziali criticità di sicurezza.
Chi entra in qualsiasi stanza dei bambini trova animali di peluche o bambole. Parte di questi giocattoli possono essere collegati alla rete e possono sapere molto su di te. L'ultima generazione di bambole parlanti può raccogliere informazioni sui bambini e trasmettere i dati ai server dei produttori di giocattoli che potrebbero anche non essere opportunamente protetti. Oltre un milione di registrazioni vocali di bambini sono state archiviate all'aperto su server rivolti al pubblico, accessibili a chiunque e molti in America hanno suggerito di disfarsi immediatamente di queste bambole.
Anche le telecamere IP possono essere lontane dall'essere sicure. Molti di loro utilizzano password predefinite, rendendo la sicurezza una banalità. Se non adeguatamente gestite, questo fatto è allarmante considerando che questi dispositivi registrano audio e video della vita delle persone, spesso dando uno sguardo agli spazi privati e alle conversazioni. A peggiorare le cose, le telecamere di sicurezza non adeguatamente protette sono spesso disponibili su Internet tramite specifici siti tipo Shodan per essere viste da chiunque. Proprio come i bollitori Wi-Fi, anche le lampadine intelligenti sono state violate in passato per rubare password wireless. Alcuni marchi di famosi produttori di tali oggetti sono potenzialmente esposti ai worm IoT che si diffondono da un bulbo all'altro e consentono agli hacker di controllare e svolgere le loro attività ben lontane dalle norme di sicurezza che dovrebbero esistere.
Recentemente alcuni hacker hanno dimostrato che le lampadine collegate possono essere utilizzate per estrapolare silenziosamente i dati da reti apparentemente sicure.
Per concludere uno dei casi più sensazionali di spionaggio IoT riguarda, il Governo russo che ha accusato i cinesi di vendere ferri da stiro con chip Wi-Fi incorporati all'interno di essi. Quando sono collegati, questi smart ferri cercano le reti wireless aperte.
Una volta collegati, i ferri diffondono il malware, inviano spam o registrano i suoni attraverso un piccolissimo microfono interno. Sebbene non ci siano conferme riguardo queste accuse, è interessante sapere che anche i dispositivi che ritieni più banali e stupidi potrebbero essere più offensivi ed intelligenti di quanto si possa pensare, spiando migliaia di utenti inconsapevoli.
Quindi cosa fare per mitigare i rischi? I dispositivi intelligenti possono sicuramente essere utili e rivoluzionari e molto spesso facilitano la vita. È però sempre importante valutare le potenziali vulnerabilità che possono essere introdotte nella nostra vita e implementare e incrementare preventivamente le regole di un corretto approccio di ciber security.

* imprenditrice