INADATTI ALL'INTERNET OF THINGS

di MARIA MORO

LE NUOVE TECNOLOGIE E LE POTENZIALITÀ DEI SISTEMI INFORMATICI POSSONO FARE L'EFFETTO DEL "PAESE DEI BALOCCHI", INVITANDO A FARE TUTTO IN PIENA LIBERTÀ. MA COME NEL LUOGO MAGICO DI COLLODI, LA REALTÀ NASCOSTA DIETRO AI LUSTRINI PUÒ RISERVARE INSIDIE, DI CUI È BENE PRENDERE LE MISURE

Non si fa in tempo a imparare come accendere il forno dallo smartphone che già Mark Zuckerberg, il fondatore di Facebook, presenta al mondo il maggiordomo artificiale Jarvis. Le tecnologie evolvono a una velocità tale da far sembrare obsoleto qualsiasi oggetto nel giro di pochi mesi. Tenere il passo con le potenzialità dei sistemi informativi è sicuramente una grande sfida per l'industria globale, che ha di fronte a sé le grandi praterie dell'*Industry 4.0*. Ma questa corsa verso le nuove applicazioni non lascia il tempo di consolidare i risultati raggiunti e rischia di essere costruita su fondamenta fragili. A mettere in guardia sui possibili rischi di un utilizzo non pienamente consapevole delle tecnologie, in primo luogo quelle *web based*, è **Alessandro Curioni**, consulente in ambito di sicurezza informatica e scrittore di testi divulgativi sui rischi della rete (*Come pesci nella rete,* **Mimesis**).

L'utilizzo pervasivo del web è un'evoluzione ineluttabile delle cose?
Sicuramente indietro non si torna. Accertato questo, la questione principale è che noi, come utenti, abbiamo una bassissima percezione del rischio, siamo *biologicamente inadatti* alla rete. L'essere umano si è sviluppato usando i cinque sensi per difendersi ma oggi questi sono inutili per internet, dove anche quello che vediamo è ciò che appare e spesso non ciò che è: ad esempio, qualcuno ha mai letto le condizioni di adesione ai social che si accettano come un automatismo? Siamo vittime del fatto che, dal nostro isolamento di fronte a un pc o a uno smartphone, non ci rendiamo conto di essere in realtà sulla pubblica piazza.

Il caso del malware Mirai è un primo avviso sui rischi dell'IoT?
È una delle tante cose che possono succedere. Il tema generale dell'IoT è correlato al fatto che nel momento in cui un oggetto è raggiungibile tramite una rete, possiamo escludere che sia raggiungibile solo da chi è autorizzato. C'è un problema oggettivo dato dalla natura originaria di internet: il limite della rete è di essere nata per la condivisione delle informazioni e non per mantenere riservato ciò che contiene. E c'è poi un problema culturale: con il web ci siamo abituati a considerare acriticamente utile e normale tutto ciò che è possibile fare.

Anche la compatibilità delle tecnologie è un limite?
A titolo di esempio, possiamo dire che se l'impianto di videosorveglianza di casa è gestibile da smartphone, è come se lo fosse da un pc, potenzialmente quindi qualcuno potrebbe prenderne il controllo. Si consideri poi che l'aspetto utilitario della rete fa sì che la sua applicazione a qualsiasi dispositivo si possa trasformare in un vantaggio per chi lo usa. Ma chi fino a ieri progettava elettrodomestici per il loro uso specifico, non è mentalmente portato a considerare il frigorifero anche dal punto di vista della sicurezza rispetto alle minacce di internet. Ora stiamo parlando di piccole cose, ma non

dimentichiamoci dei rischi che corrono le infrastrutture critiche, dietro le quali ci sono investimenti enormi. La continuità operativa si basa oggi sulla *compatibilità retroattiva*, che permette di aggiornare parzialmente i sistemi o i macchinari con nuove soluzioni compatibili con quelle già installate. I componenti più recenti sono più sicuri, ma quelli vecchi li costringono a un downgrade per potere funzionare insieme e, se avevano delle vulnerabilità, influenzano negativamente il nuovo componente rendendo il sistema non sicuro.

Cosa devono valutare le aziende che pensano di introdurre queste soluzioni?
Spesso, si sa, la sicurezza è percepita come un costo, poi il business è business…, il *time to market* rischia di allungarsi… Se non c'è un processo condiviso tra tutti, o reso obbligatorio per legge, oggi come oggi eseguire i controlli di sicurezza e i test anche sui dispositivi di connessione applicati all'oggetto non è attività compatibile con i ritmi di evoluzione del prodotto, che rischierebbe di uscire quando è già obsoleto.

La sicurezza delle informazioni potrà mai diventare un vantaggio competitivo?
Con una maggiore consapevolezza da parte dei consumatori, può diventarlo. Bisognerà arrivare a un punto in cui si comprano oggetti collegabili in rete come ora si compra l'auto, cioè informandosi sulla dotazione dei sistemi di sicurezza quali l'Abs o l'airbag. La consapevolezza del rischio da parte degli utenti sarà determinante come spinta al cambiamento, in quanto le aziende offrono quello che i consumatori chiedono. Come privato cittadino ho la sensazione che fino a che non accadrà qualcosa di veramente negativo si andrà avanti in modo inconsapevole. È già stato possibile per qualcuno prendere il controllo dei sistemi tecnologici di un'auto, geolocalizzare la posizione via *Whatsapp*, incrociare più informazioni su qualcuno raccogliendole dai siti ed entrare così nel privato di una persona: non è fantascienza. Si dovrebbe rallentare l'intero meccanismo di evoluzione tecnologica, con tempi di sviluppo più lunghi: ma il sistema lo accetterebbe? Rallentiamo l'introduzione dello IoT?

Per avere accesso alle informazioni e ai servizi internet è quindi necessario raggiungere un compromesso tra utilità e sicurezza?
Nell'accettare il rischio una dose di compromesso c'è sempre, ma deve essere consapevole. Facciamo un esempio: gli impianti elettrici degli aerei vengono revisionati ogni 12 mesi perché il loro deterioramento comporterebbe un grave rischio. Anche gli impianti elettrici di casa rischiano il deterioramento in tempi mediamente brevi, ma in genere accettiamo il rischio entro una certa soglia. Avviene così in ogni cosa che facciamo, tranne che nella società dell'informazione: quando compriamo uno smartphone, nessuno chiede la sua protezione da virus informatici.

Quali sono per le aziende le conseguenze potenziali in termini di responsabilità?
Il recente regolamento europeo sulla gestione dei dati ha alzato l'asticella sia dal punto di vista delle misure di sicurezza sia delle sanzioni, ma per gli altri aspetti quanto le aziende sono disposte ad accettare dei vincoli? Finché non sorgono problemi, possiamo pensare che tutto vada bene. Esiste un certo grado di consapevolezza ma prevale la tendenza a nascondersi la realtà, o a pensare che le cose succedano agli altri. Ma non è così, soprattutto con IoT. Il caso del malware *Mirai* è emblematico in questo senso: Mirai ha permesso a criminali di prendere il controllo da remoto di oggetti i cui sistemi presentavano una vulnerabilità e li ha messi in rete come se fossero pc.

Poi ci sono gli aspetti assicurativi…
In prospettiva cambierà inevitabilmente la valutazione del rischio e quindi i prodotti assicurativi. *Solvency* II ha inserito il rischio operativo ma questo è solo uno dei rischi, forse non il più importante per l'azienda: si dovrebbe imparare a valutare diversamente i rischi operativi, usando strumenti nuovi. Neppure le coperture sul *cyber risk* sono adeguatamente diffuse, e comunque spesso tendono a coprire voci che non prevedono l'intrusione da remoto. I prodotti assicurativi dovranno adeguarsi alle nuove problematiche legate alla rete: ad esempio, se una società che gestisce dighe e centrali elettriche vuole sottoscrivere una copertura dal rischio terrorismo, non dovrà includere solo l'attentato diretto ma anche la possibilità di attacchi informatici. Già nel 2015 un attacco con virus informatico ha spento tre centrali elettriche in Ucraina.
D'altro lato, le assicurazioni dovrebbero iniziare a richiedere determinati controlli di sicurezza e certificazioni. Ma la strada è ancora lunga: il mercato va più veloce delle azioni di controllo e dei tentativi di contenimento dei rischi; i rischi stessi non sono veramente conosciuti e ci si trova a inseguirli con anni di ritardo.