Il Sole 24 ORE
Quotidiano Politico Economico Finanziario
QUOTIDIANO: MILANO



**P** **Cybersecurity** | Strategie aziendali | Attacchi e soluzioni

# L'insicurezza cambia l'impresa

La piena consapevolezza del rischio collegato alle minacce online può accelerare e guidare la trasformazione digitale

*di* **Antonio Dini**

● Winter is coming. E arriva l'offensiva d'autunno: l'armata di zombie e bot questa volta si chiama "Krebs" e sorprende anche gli esperti: «Al posto dei computer tradizionali della botnet – dice Bruce Schneier, super-guru britannico della security – sono state usate webcam e telecamere a circuito chiuso, videoregistratori digitali, router casalinghi e altri computer embedded che sono parte di quella che viene chiamata la Internet of Things». I danni dell'attacco sono stati notevoli, interi settori di Internet bloccati dopo che 1,3 terabyte di dati al secondo sono stati "sparati" contro Dyn, la torre di controllo degli indirizzi web di buona parte della rete. Chiosa Schneier: «Internet of Things è pericolosa, il governo deve intervenire con delle normative».

È il Far West. A oggi, però, quelle normative non ci sono. Ma la sensazione diffusa è che i processi di trasformazione digitale delle imprese non siano completi se non si affronta il fattore sicurezza: la gestione del rischio, la comprensione dei pericoli, le misure strategiche per mitigarli. «Non è più solo un fatto tecnologico», spiega a Nòva24 Filippo Monticelli, country manager di Fortinet, azienda quotata al Nasdaq che si occupa di proteggere grandi, medie e piccole aziende dalle insicurezze digitali. Il problema è anche culturale: ormai tutte le aziende hanno capito che l'innovazione digitale è rilevante e ineludibile. E, secondo la ricerca del Politecnico di Milano (che presentiamo in questa pagina), due aziende su tre hanno introdotto sistemi di sicurezza per le informazioni. «Sono necessari – dice Monticelli – framework di sicurezza con più elementi capaci di sfruttare anche componenti di intelligence. La protezione del singolo computer, l'ultimo modello di firewall, di per sé non basta più».

Nell'era delle smart city, dell'automazione della casa, del "quantified self", delle auto che si guidano da sole e della digitalizzazione a tappe forzate di interi settori dell'economia, ragionare per antivirus non è più la risposta. «L'Italia come spesso accade – dice Monticelli – su alcuni aspetti è indietro e su altri invece molto avanti. D'altro canto, lo scenario sta cambiando: dopo che a ottobre dello scorso anno 400mila videocamere di sorveglianza di un unico produttore cinese sono state hackerate, è diventato chiaro che la prossima tappa sia arrivare a una differente protezione».

Cosa bisogna proteggere? Quali sfide inedite si parano davanti alle aziende che imboccano la strada della trasformazione digitale? Oggi ci sono aree più presidiate di altre. Ad esempio, sono sguarnite le nuove frontiere tecnologiche come cloud, mobility e big data. Più sicuri, perché conosciuti da più tempo, i gestionali aziendali e i sistemi tradizionali.

In Italia però, secondo il Politecnico, tre aziende su quattro non hanno ancora un ruolo specifico dedicato alla gestione della sicurezza informatica. E anche la nuova normativa sulla privacy (GDPR), che entrerà in vigore a marzo 2018, è un mistero per due aziende su tre. E tra queste, oltre la metà dice di non conoscerla affatto.

«Da una parte – dice Gabriele Giacoma, AD di Assiteca, broker di assicurazioni attivo dal 1982 – c'è la percezione del rischio da parte delle aziende italiane che sta crescendo. Dall'altra la capacità di adeguarsi ai nuovi rischi è ancora molto bassa. Se guardiamo alla sicurezza come tre pilastri, fisico, logico e organizzativo, le aziende sono avanti sul primo, deboli sul secondo ma soprattutto indietro nella parte organizzativa, cioè il modo con cui le persone utilizzano i sistemi».

L'importanza del momento di passaggio che stiamo vivendo non deve essere sottovalutata. Non solo aumenta l'insicurezza digitale, cioè le opportunità per i "cattivi", ma c'è anche una finestra di opportunità per le aziende. In Italia la digitalizzazione è soprattutto un processo culturale che, come tale, impone di ripensare il modo di fare business. La conseguenza è che vengono adottati nuovi modelli e modalità organizzative, cambiano i processi e le responsabilità in azienda, emergono le persone con le loro competenze. È il momento ideale per ripensare le procedure e la sicurezza, anziché aggiungere e appesantire l'esistente, oppure ignorare completamente il tema.

Anche perché, come ha detto tempo addietro John Chambers di Cisco, «ci sono due tipi di aziende: quelle che sono state hackerate e quelle che non sanno ancora di essere state hackerate». Oltre al rischio degli hackeraggi per provocare attacchi su larga scala come quello delle telecamere di sicurezza stigmatizzato da Schneier, c'è la piaga del "ransomware", cioè di virus che attaccano silenziosamente i Pc aziendali, blindano con password impenetrabili ai legittimi proprietari tutti i documenti, magari quelli legali e contabili, e richiedono un riscatto nelle valute del web come i Bitcoin (per loro natura non tracciabili) che ovviamente non verrà mai onorato. La Polizia postale e tutti gli esperti ribadiscono che non bisogna mai pagare, piuttosto cercare una risposta dagli addetti ai lavori, perché spesso i lucchetti dei malintenzionati sono stati già rotti dagli hacker buoni.

«La cosa più emozionante del mercato della sicurezza – dice Monticelli – è che ogni sei mesi cambia tutto. Le sfide si susseguono, una diversa dall'altra, e non ci si annoia di certo». Lo sanno le aziende che, seppure spesso all'oscuro della complessità dei temi di sicurezza, ne percepiscono molto bene i rischi da un punto di vista reputazionale. Soprattutto quelle aziende che considerano la digitalizzazione come un'opportunità strategica per aprire nuovi modi di fare business resistendo alla disruption digitale, anziché come uno strumento tattico solo per l'efficientamento in azienda. È la spinta per cominciare ad abbracciare realmente il cambiamento?

@antoniodini

Il Sole 24 ORE
Quotidiano Politico Economico Finanziario
QUOTIDIANO: MILANO



Processi

## Il cambiamento contagioso

Le competenze digitali hanno portato felicità diffusa tra i lavoratori della Madi Ventura

*di* **Antonio Dini**



E-learning

## Una palestra per la sicurezza

I dipendenti della Fater si incontrano in un villaggio digitale per formarsi sulle minacce informatiche

*di* **Antonio Dini**



Infrastrutture

## La difesa non è in pericolo

Sito di replica, policy di backup, copie di dati nel caveau di una banca: la lezione di Futura

*di* **Antonio Dini**