Perché le aziende non cyber sicure sono destinate a fallire. Parla Melissa Hathaway

Michele Pierri

JAMES BOND

Che cosa rischiano oggi le aziende che sottovalutano il rischio cyber? Moltissimo, talvolta persino la loro stessa presenza sul mercato, secondo Melissa Hathaway, una delle più note esperte di sicurezza informatica in circolazione, intervenuta a Milano in una tavola rotonda promossa a Milano dall'AmCham Italy, la Camera di Commercio americana in Italia

FOTO

Tutte le foto di Boschi, Renzi e Rosato alla Camera

La visita di Giuseppe Conte in Qatar. Le foto

Virginia Raggi presenta il campionato di Formula E in Campidoglio. Le foto

Che cosa rischiano oggi le aziende che sottovalutano il rischio cyber? Moltissimo, talvolta persino la loro stessa presenza sul mercato, secondo **Melissa Hathaway**, una delle più note esperte di sicurezza informatica in circolazione, intervenuta a Milano in una tavola rotonda promossa dall'AmCham Italy, la Camera di Commercio americana in Italia.

IL PROFILO DELL'ESPERTA

Già membro del National Security Council Usa con delega alla cyber security sotto la presidenze Bush e Obama, Hathaway, classe 1968, è oggi presidente della consultancy firm Hathaway Global Strategies e senior fellow del Potomac Institute for Policy Studies, all'interno del quale ha elaborato il noto Cyber Readiness Index che misura il livello di preparazione dei Paesi in tema di sicurezza informatica.

LA GENESI DELLA 'CYBER INSICUREZZA'

"Negli ultimi 30 anni", ha ricordato l'esperta, "governi, compagnie e cittadini sono diventati dipendenti in modo critico da Internet e dall'Ict, ma purtroppo l'infrastruttura sottostante e i device sono insicuri".
Questa 'cyber insicurezza', ha spiegato Hathaway, deriva fondamentalmente dall'intersezione di tre elementi: "elementi malamente progettati che stanno inondando il mercato, soprattutto nell'IoT; ampia disponibilità a buon mercato di tool e di incentivi a sfruttare le vulnerabilità esistenti; e le crescenti opportunità economiche derivanti dall'agenda digitale".

I NUMERI DEL MERCATO

Con riferimento a quest'ultime, Hathaway ha elencato un po' di numeri: 3,8 trilioni di dollari è la spesa Ict prevista a livello globale nel 2019; 19 trilioni di dollari le opportunità a breve termine legate a device che connettono persone, posti e oggetti; 32 trilioni di dollari le possibilità a lungo termine per quanto concerne la modernizzazione delle infrastrutture industriali (somma equivalente a circa il 46% dell'economia mondiale); mentre già oggi il Pil mondiale conta su un 7% – destinato a crescere – derivante dall'Ict.

I RISCHI DELL'IPERCONNESSIONE

Fin qui le opportunità. Tuttavia, in questo contesto nel quale ogni settore è già, o è destinato a essere, iperconnesso – energia, difesa, trasporti, agricoltura, salute, industria, commercio, per elencarne alcuni – è necessario non perdere di vista quanto la gestione e la mitigazione del rischio cyber siano fondamentali. "Il costo del cyber crime è stimato in 2,1 milioni di dollari nel 2019, con una previsione di incremento del 2,1%), ha detto Hathaway. A costituire un pericolo nel cyber spazio sono naturalmente diversi Stati, ma, ha ricordato l'esperta, "sono tantissime le armi informatiche o le informazioni personali utili a condurre attacchi che sono oggi disponibili a bassissimo costo nel Dark Web". Qualche esempio? "Un'offensiva contro il Cms di un sito web costa 300 dollari, un trojan per spiare un dispositivo 200 dollari, 50 dollari un tool per rubare password, 700 dollari per un attacco DDos capace di paralizzare un sistema e, addirittura, bastano soli 3 dollari per ottenere i dati di una social security card per utilizzare servizi a nome di un cittadino ignaro".

AZIENDE NEL MIRINO

Se si guarda alle aziende colpite in questi anni, ha evidenziato l'esperta, c'è solo l'imbarazzo della scelta. "Sono moltissimi gli episodi. Nel 2015 il malware

Tutti gli incontri di Jean-Claude Juncker in Italia. Le foto

Giuliano Amato al Csa per i 70 anni della Nato. Foto di Pizzi

Angel Gurria e Giovanni Tria al Mef per il Rapporto Ocse. Le foto

Chi ha celebrato con Eisenberg i 70 anni della Nato al Centro studi americani. Foto di Pizzi

BlackEnergy e Crash Override sono stati usati simultaneamente per colpire tre compagnie ucraine regionali di distribuzione dell'elettricità, lasciando oltre 225mila residenti senza corrente elettrica. Il noto gruppo Carbanak ha colpito tra il 2013 e il 2018 oltre 100 istituzioni finanziarie in 40 Paesi, arrivando a rubare in un periodo di due anni circa 1 miliardo di dollari. Senza contare gli effetti disastrosi prodotti da due attacchi più recenti come Wannacry – che nel 2017 ha colpito tra le altre Deutsche Bahn, Nissan, Renault, Telefonica e il sistema sanitario nazionale del Regno Unito – e NotPetya, che nello stesso anno ha avuto un impatto di 100 miliardi di dollari in termini di asset distrutti a livello mondiale, colpendo aziende del calibro di Maersk, Saint Gobain, WPP, Reckitt Benckiser, TNT e altre ancora".

LA RISPOSTA

Come rispondere a queste minacce, che se non affrontate rischiano "di affossare per sempre un'azienda"? Davanti a questo scenario, le imprese, ha spiegato Melissa Hathaway, hanno due possibilità: subire passivamente gli effetti negativi della digitalizzazione o sfruttarne i lati positivi mettendo contestualmente in campo una serie di misure che possono renderle più sicure e resilienti nei confronti della crescente minaccia cyber. "Per diventare 'cyber ready' c'è bisogno di una pianificazione robusta e integrata, con una visione di business da qui a 5 anni, un'attenzione alla compliance della regolazione emergente e dell'ambiente legale, una strategia di digitalizzazione accorta e anche un occhio di riguardo alle dinamiche geopolitiche". Per l'esperta, "serve innanzitutto conoscere bene la propria postura e i propri rischi informatici, un processo che non può che partire da una valutazione accurata della propria, specifica situazione. Necessario inoltre che la cyber security diventi parte integrante dei rischi aziendali affrontati in modo costante dai board". Sullo sfondo, ha concluso l'esperta, ci sono le tecnologie emergenti che cambieranno ulteriormente il mondo così come oggi lo conosciamo. "5G, blockchain, intelligenza artificiale, quantum computing: sono tutti elementi destinati a portare innovazione e benefici, ma anche nuovi rischi per la nostra sicurezza. La cosa più importante è farsi trovare pronti, tenendo sempre presente che la digitalizzazione non è di per sé un male, ma sarebbe saggio avere sempre un modo per tornare indietro in caso di problematiche che dovessero fermare le nostre infrastrutture critiche".

Roberto Baldoni, il nuovo cyber zar del Dis di Pansa. Le foto

Ciardi, Franchina e Galante parlano di cyber security al Csa. Foto di Pizzi

Ecco i giovani hacker premiati da CIS-Sapienza e Laboratorio Cybersecurity. Foto di Pizzi