Cybercrime, alle imprese costa 9 miliardi di euro si investe poco nella difesa

Andrea Frollà


focus paese digitale

Cybercrime, alle imprese costa 9 miliardi di euro si investe poco nella difesa

In campo le potenze del G7: "Uniti per la sicurezza"

Milano A rchivi giganteschi di account e-mail e password finiti in vendita a prezzo di saldo nel deep web. Banche, ospedali e istituzioni pubbliche di tutto il mondo infettati e tenuti sotto scacco da un ransomware. Attacchi informatici ai giganti del cinema e delle serie tv, accompagnati in alcuni casi dalla diffusione online di contenuti inediti. Si potrebbe continuare con altre offensive meno eclatanti, ma bastano i data leak Anti Public e Exploit. IN, il caso Wannacry e le incursioni negli archivi digitali di Netflix e della Disney a segnalare la portata assunta dal fenomeno del cybercrime. I sostenitori del bicchiere mezzo pieno sottolineano che la portata e la qualità di questi attacchi ha finalmente concesso al tema della sicurezza informatica una vetrina mainstream, facendolo uscire dai confini tradizionali degli addetti ai lavori. La maggiore sensibilità deve però tradursi in concretezza, di cui c' è molto bisogno alla luce di uno stato dell' arte che gli esperti non esitano a definire disastroso. Soprattutto lato aziende e anche in Italia. La trasformazione digitale delle imprese, spinta oggi dal binomio connessione-interconnessione dei processi produttivi in nome dell' industria 4.0, rischia infatti di arrecare più danni che benefici senza un' adeguata protezione contro le nuove frontiere del cybercrime. Un pericolo concreto nel nostro Paese, a causa di investimenti insufficienti, approcci di brevissimo periodo e sottostime dei pericoli. Gli attacchi informatici, stima il rapporto Italia Eurispes 2017, costano alle imprese italiane 9 miliardi l' anno. E il dato potrebbe anche essere superiore, visto che molte aggressioni informatiche non diventano subito di dominio pubblico (perché scoperte solo molto tempo dopo e perché, salvo alcuni casi regolamentati, non esiste un obbligo di notifica pubblica). Per non parlare poi dei danni alla reputazione aziendale. Lo scorso anno, rileva l' Associazione italiana per la sicurezza informatica (Clusit), è stato il peggiore di

sempre in termini di evoluzione, qualitativa e quantitativa, delle minacce e dei relativi impatti. L' allarme rosso è ormai quotidiano. «L' attenzione sul tema si sta sviluppando molto in questi mesi anche per la pressione mediatica. Ma la cultura generale in tema di sicurezza informatica è molto bassa così come la percezione dei rischi. Questo sia nel mondo privato sia in quello pubblico. E anche nella vita quotidiana», spiega Gabriele Faggioli, presidente del Clusit. Negli ultimi 3 anni, avverte il rapporto annuale dell' associazione, il cybercrime si è evoluto più rapidamente dei sistemi di sicurezza, garantendosi un ottimo rapporto fra profitti e rischi. Dal punto di vista statistico ogni organizzazione, di qualunque dimensione e settore, ha la certezza di subire almeno un attacco significativo nel corso di un anno. Ecco perché, avverte l' associazione che rappresenta oltre 500 aziende ed enti di sicurezza IT, l' affidamento alla buona sorte, la sottostima dei rischi e il rinvio dell' adozione di strumenti adeguati non sono più opzioni percorribili. Il mercato italiano delle soluzioni di information security ha sfiorato il miliardo di euro nel 2016, raggiungendo quota 972 milioni e facendo segnare un aumento del 5% rispetto al 2015 (dati Osservatori Digital Innovation). Ma, sottolinea il Clusit, il problema è che questa cifra rappresenta l' 1,5% di tutta la spesa Ict, a testimonianza di come la sicurezza informatica non sia ancora concepita come una colonna portante della dotazione tecnologica aziendale. In deciso ritardo le Pmi, alle prese con usi promiscui dei de- vice, server tenuti in luoghi non protetti e assenza di catalogazione di dati aziendali. «La prevalenza di piccole e medie aziende incide in modo decisivo - sottolinea Faggioli - Gli investimenti possibili sono ovviamente scarsi e se si ha poca consapevolezza da un lato e pochi soldi dall' altro, la combinazione è drammatica». Uno dei problemi principali riguarda l' assenza di un' ottica di medio-lungo periodo. Eppure i calcoli del Consorzio interuniversitario nazionale per l' informatica (Cini) dimostrano che aprire il portafoglio conviene. Tra danni d' affari e di immagine, costi del recupero dei dati e tempi di inattività, gli attacchi informatici costano in media a una Pmi 175mila euro in 5 anni. Per evitare questo salasso dotandosi di alcuni standard minimi di difesa, calcola il Cini, una piccola impresa del manifatturiero dovrebbe spendere circa 42mila euro (2.700 subito, 7.800 ogni anno). Mentre l' investimento per una media impresa di trasporti sarebbe di 103mila euro (4.600 subito, quasi 20mila ogni anno). L' innalzamento delle barriere informatiche da parte delle Pmi aiuterebbe anche le grandi aziende che svolgono il ruolo di capi-filiera. Sempre più, infatti, i criminali informatici sfruttano la debolezza di fornitori e partner per arrivare a colpire il big. L' incursione degli hacker culminata con la messa in onda pirata di una serie di Netflix è avvenuta proprio sfruttando le falle di un distributore della compagnia californiana. Il tema della cybersecurity assume infine una particolare rilevanza nei settori critici come l' energia, i trasporti, le banche, la sanità e le infrastrutture digitali. Ambiti in cui gli hacker possono provocare effetti devastanti. Per informazioni chiedere alla compagnia ucraina Oblenergo, vittima di un attacco incrociato contro la centrale di controllo, i sistemi di recovery e i call center dell' assistenza. E soprattutto ai suoi clienti, rimasti senza elettricità con il termometro ampiamente sotto zero a fine dicembre 2016. © RIPRODUZIONE RISERVATA Gli hacker si dimostrano sempre più aggressivi e negli ultimi tempi hanno compiuto

attacchi informatici che hanno provocato guai seri in diverse parti del mondo Sul fronte della sicurezza informatica, Ibm tenta di giocare d' anticipo con il team di Ricerca Ibm X-Force. "Tramite Watson for Cyber Security abbiamo più possibilità di prevedere dove avverrà un attacco" spiega Teodonno Segui Paese Digitale anche su: www.paesedigitale.it.