LA LOTTA CONTRO UN NEMICO INVISIBILE

di BENIAMINO MUSTO

CON MODALITÀ SEMPRE PIÙ SOFISTICATE, I CRIMINALI RIESCONO A INSINUARSI ANCHE NELLE ORGANIZZAZIONI PIÙ SICURE. IL CYBER RISK È SEMPRE PIÙ PERCEPITO COME LA PRINCIPALE MINACCIA PER CHI HA UN'ATTIVITÀ COMMERCIALE: SOLO NEL 2019 IN ITALIA SONO STATI REGISTRATI QUASI 5.000 CASI DI FRODE INFORMATICA IN AMBITO FINANZIARIO

Italia, 4 dicembre 2019. Un blackout completo colpisce gli uffici dell'**Iren**, multiservizi dell'energia, con 7.000 dipendenti e due milioni e mezzo di clienti. L'azienda è finita nel mirino dei pirati informatici: archivi della clientela irraggiungibili, centrale del pronto intervento scollegata dalla rete, impossibilità di ricevere e spedire mail.

Repubblica Ceca, 23 dicembre 2019. La compagnia mineraria ceca **Okd** è vittima di un attacco informatico che per cinque giorni paralizza ogni attività. Due settimane prima, nel mirino era finito l'ospedale di Benesov, in Boemia centrale, colpito dal ransomware Ryuk, impedendo al personale l'uso di raggi x e altre strumentazioni ospedaliere.

Austria, 5 gennaio 2020. I sistemi informatici del ministero degli Esteri sono oggetto di un "grave attacco informatico", come ha ammesso lo stesso governo austriaco in una nota. "A causa della gravità e della natura del fenomeno – si legge – non si può escludere che si tratti di un attacco mirato".

Sono soltanto tre esempi, riferiti a realtà eterogenee e geograficamente distanti, ma che mostrano una comune fragilità di fronte a un nemico che fa dell'invisibilità il proprio punto di forza. Non stupisce dunque che gli attacchi cyber siano il rischio più percepito tra chi fa impresa, come emerge dall'ultimo *Allianz risk barometer 2020*, pubblicato a gennaio da **Acgs**. La minaccia informatica, secondo lo studio, è quella maggiormente percepita dalle aziende a livello globale (39% delle risposte), mentre solo sette anni fa si trovava al 15° posto (6% delle risposte): a motivare la rapida crescita è la sempre maggiore dipendenza delle imprese dai sistemi tecnologici e dai dati, ma anche le possibili conseguenze di un attacco informatico o di un incidente, sia dal punto di vista operativo, sia legale e risarcitorio.

L'ATTRAZIONE PER LE CRIPTOVALUTE

Il crimine informatico continua a maturare, e sposta la propria attenzione verso obiettivi più ampi e redditizi. È ciò che spiega l'ultimo rapporto *Iocta* (Internet organised crime threat assessment), pubblicato lo scorso ottobre dall'**Europol**, l'agenzia anticrimine europea, secondo cui le nuove minacce non derivano solo dalle nuove tecnologie, ma spesso provengono da vulnerabilità già presenti nelle tecnologie esistenti. Lo studio, molto dettagliato, individua nei ransomware crypto il nemico principale che gli investigatori europei si trovano a dover contrastare. I soli attacchi Wannacry e Notpetya, nel 2017, hanno colpito 300mila utenti nel mondo in 150 Paesi, con danni economici stimati in circa 4 miliardi di dollari.

Altrettanto allarmanti, inoltre, sono gli attacchi che hanno l'obiettivo di impadronirsi illegalmente dei dati finanziari: informazioni sulle carte di credito, credenziali bancarie online o wallet di criptovalute. "Gli exchange di criptovaluta – si legge nel report – continuano a essere una calamita per i gruppi di hacking motivati finanziariamente. Nel 2018, oltre un miliardo di dollari in criptovalute sono stati rubati dagli exchange e da altre piattaforme in tutto il mondo". Le forze dell'ordine, si legge nello Iocta, devono "continuare a costruire relazio-

IL MONDO ACCADEMICO PER LA CYBER SECURITY

Come per tutti i problemi complessi, non è pensabile fronteggiare il cybercrime senza una risposta di sistema, in cui anche il mondo accademico può fare la propria parte. Va in questo senso il nuovo *Competence center per la cyber security*, presentato lo scorso dicembre presso l'**Università La Sapienza** di Roma. Si tratta di uno degli otto poli di competenza ad alta specializzazione su tematiche Industria 4.0, previsti dal ministero dello Sviluppo economico, che aggrega università, istituzioni, centri di ricerca e imprese. Le principali missioni del nuovo polo, che mira anche ad avviare un percorso di orientamento, formazione e innovazione sul tema della cyber security, sono il contrasto della criminalità informatica e la ricerca sulla cyber-sicurezza, elaborando strategie efficaci a sostegno di imprese del territorio.
L'iniziativa è nata dalla collaborazione tra pubblico e privato (37 le imprese aderenti, tra piccole e grandi) a cui hanno aderito diversi atenei: **Luiss Guido Carli, La Sapienza, Tor Vergata, Roma Tre, Università della Tuscia, Università di Cassino, Università dell'Aquila**; tra i centri di ricerca: il **Cnr** e l'**Inail**.


© NicoElNino - iStock

ni basate sul trust con le attività legate alle criptovalute, il mondo accademico e le altre entità pertinenti del settore privato, in modo da affrontare in modo più efficace i problemi posti in essere dalle criptovalute durante le indagini".

FINANCIAL CYBERCRIME, QUASI 5.000 CASI IN ITALIA NEL 2019

Nel nostro Paese, secondo il resoconto annuale della Polizia Postale, nel 2019 ci sono stati 4.930 casi di financial cybercrime a livello nazionale. Il fenomeno del phishing, finalizzato alla captazione illecita di codici personali e dati sensibili, conosce un notevole aumento soprattutto attraverso il ricorso a malware e siti-clone. In aumento, tuttavia, sono anche i casi riguardanti il *vishing* (phishing vocale) e lo *smishing* (phishing attraverso messaggi e sms). La violazione dei sistemi bancari di privati e imprese vede un aumento nel ricorso alle tecniche criminali del cosiddetto *sim-swap*.
"Il tessuto economico-produttivo del Paese – spiega una nota della Polizia Postale – continua a essere oggetto degli attacchi noti a livello mondiale con le espressioni *Bec* (business email compromise, ndr) e *ceo fraud*". Scopo delle organizzazioni criminali è quello di intromettersi nei rapporti commerciali tra aziende dirottando ingenti somme verso conti correnti nella disponibilità dei truffatori. Bec fraud e ceo fraud sono la moderna applicazione della tecnica di attacco denominata *man in the middle*.
Su questo fronte, è emblematico un caso avvenuto lo scorso anno e segnalato dalle Forze dell'ordine, con protagonista un'azienda campana operante nel settore della commercializzazione di gas industriale. Un importo di 236mila euro è stato trasferito dal conto corrente dell'azienda vittima a saldo di una fattura commerciale, a un diverso conto, in uso ai cyber criminali che si erano sostituiti al reale partner d'affari: in questo caso, fortunatamente, la Polizia Postale è riuscita a recuperare gran parte della somma sottratta dai truffatori.