Nella rete degli hacker

NICOLA CAROSIELLI

CYBERSECURITY Non solo Campari, Enel e Luxottica. I crimini informatici aumentano con il lockdown e impensieriscono anche il Vaticano. Le aziende però stanno correndo ai ripari, creando occasioni anche in borsa

Nella rete degli hacker

di Nicola Carosielli

L'ultima azienda finita sotto attacco hacker è stata Campari, alla quale dopo essere stati sottratti circa 2 terabyte di dati riservati è stato chiesto un riscatto di 15 milioni di euro per ripristinare le attività. Poche settimane prima è stato il turno di Enel, che si è vista rubare 5 terabyte di informazioni a fronte di una richiesta di 14 milioni. E ancora: Luxottica, Geox e Carraro (costretta a far slittare contratti per 15 milioni). Pochi esempi che la dicono lunga su una tendenza in costante crescita già da fine 2018 e acuitasi con l' insorgere della pandemia, che ha obbligato tutte le industrie al rapido trasloco delle attività sulla rete, spesso senza dotarsi di adeguati sistemi di sicurezza. Basti pensare che dallo scoppio del Covid sul tavolo della polizia postale sono finiti quasi 30 dossier riguardanti grandi società, enti istituzionali e società di servizi. Attacchi arrivati a preoccupare anche la Santa Sede, con la Biblioteca Vaticana al lavoro sulla creazione di una rete di bot basata su intelligenza artificiale a guardia del sito web e delle infrastrutture di server che custodiscono le repliche digitali di oltre 80mila volumi. La stretta correlazione tra lockdown e attacchi hacker è stata recentemente sottolineata dall' ultimo Osservatorio sulla Cybersecurity di Exprivia, secondo cui nel periodo luglio-settembre si sono registrati 148 eventi tra attacchi, violazioni della

privacy e incidenti, rispetto ai 171 del periodo aprile-giugno e ai 49 tra gennaio e marzo. Tra i comparti presi maggiormente di mira si segnala la Pubblica Amministrazione con 34 attacchi, il doppio dei casi rispetto al trimestre precedente, seguita dal comparto finanziario con 23 casi (+44%). Sul totale degli episodi registrati, 16 hanno riguardato casi di violazione della privacy (quasi il triplo dei tre mesi precedenti) per un totale di circa18 milioni di euro di sanzioni irrogate dal Garante per la protezione dei dati personali. Sulla stessa linea è andato poi il Rapporto 2020 di Clusit, l' associazione italiana per la sicurezza informatica, che ha evidenziato un aumento degli attacchi del 7% su base annua nel primo semestre dell' anno con 850 attacchi noti analizzati. Come nota Domenico Raguseo, direttore Cybersecurity di Exprivia, «la pandemia ha accelerato la trasformazione digitale costringendo l' Italia a colmare velocemente quel gap digitale che l' aveva storicamente caratterizzata ed è per questo che si rende necessario sviluppare quanto più possibile una cultura digitale orientata alla cybersecurity che consenta di non sprecare questa opportunità». Come si può osservare nella tabella in pagina, il furto dei dati è costantemente la causa principale di un cyber attacco. Il che può non stupire se si collega alle spese sostenute dalle aziende in per tentare di prevenire tale eventualità, voce che nel 2019 ha visto il giro d' affari legato alle soluzioni per la sicurezza e la data protection in Italia toccare quota 1,317 miliardi di euro, secondo l' Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano. La crescita in questo senso sarà esponenziale e a livello globale si prevede che crescerà fino a raggiungere i 250 miliardi di dollari entro il 2023 (fonte Statista). Quel che però serve comprendere, precisa Raguseo, «è l' assoluta necessità di investire anche nella formazione dei dipendenti, nella consapevolezza dei singoli, perché poi è quello che si riversa sull' azienda». Basti pensare che la tecnica di attacco più diffusa, spiega ancora il manager, è la cosiddetta «frode del cfo» in cui (sintetizzando) l' hacker si finge una figura manageriale apicale e invia al cfo del gruppo preso di mira un iban diverso dal solito sul quale effettuare dei versamenti. Sostanzialmente sfruttando la tecnica del phishing. Le aziende della cybersecurity, insomma, hanno ancora molto da fare. Una situazione che sembra essere stata ben recepita anche dal mercato. Basti pensare che l' indice di riferimento del comparto, il Foxberry Tematica Research Cybersecurity & Data Privacy Usd Pr Index, solo da inizio anno ha guadagnato il 26,74%. (riproduzione riservata)