IL VIRUS È (ANCHE) ONLINE

di GIACOMO CORVI

LA SPINTA DIGITALE DATA DAL COVID-19, SECONDO SERGIO MATTIUZ DI ANIA SAFE, POTRÀ COMPORTARE UN AUMENTO DEGLI ATTACCHI INFORMATICI. L'ATTIVITÀ DEGLI HACKER STA EVOLVENDO, MENTRE RESTA ANCORA DIFFICILE IL SUPERAMENTO DI CATTIVE ABITUDINI CHE FACILITANO IL LAVORO DEI CRIMINALI DEL WEB

Il coronavirus infetta anche i computer. A marzo, secondo un rapporto della società statunitense di sicurezza informatica **WMware Carbon Clark**, il numero di attacchi ransomware in tutto il mondo è cresciuto del 148% rispetto al mese precedente. "È chiaro ormai che, mentre prosegue la lotta contro il Covid-19 a livello globale, gli autori di questo genere di attacchi continueranno a prendere di mira i cittadini e le società più vulnerabili", avevano scritto ad aprile i curatori dell'analisi. Già, perché la pandemia di Covid-19 mostra i suoi effetti anche online. E l'emergenza sanitaria è già diventata un'emergenza informatica.

"Temo che la pandemia di coronavirus provocherà un ulteriore aumento degli attacchi informatici", afferma **Sergio Mattiuz**, amministratore delegato di **Ania Safe**. "Ho paura – aggiunge – che non sarà un aumento graduale, ma netto e piuttosto considerevole". Alla base delle preoccupazioni c'è soprattutto la spinta alla digitalizzazione data dall'emergenza coronavirus: tutti chiusi in casa, tutti connessi al proprio computer per continuare a lavorare anche lontano dell'ufficio, tutti protetti dalle quattro mura domestiche, al riparo dal virus che circola per la strada ma non da quelli che corrono online. Lo smart working, in quest'ottica, è un'inaspettata fonte di rischio. "Lavorare da casa significa utilizzare device personali, che magari non dispongono neppure dei sistemi di protezione più elementari, e connettersi a reti che non presentano standard adeguati di sicurezza: tutto ciò – commenta Mattiuz – allarga il perimetro di attacco, estendendo il classico network chiuso dell'impresa ai tablet e ai computer dei dipendenti".

UN TEMA CULTURALE, NON TECNOLOGICO

Già il 2019 non era stato un anno facile per la sicurezza informatica. Secondo l'ultimo rapporto del **Clusit**, l'annata si era chiusa con un totale di 1.670 attacchi a livello globale, con una crescita del 7% su base annua. Calcolatrice alla mano, fanno più 139 attacchi al mese: giusto per avere un'idea, nei cinque anni precedenti la media mensile si era fermata a 94 episodi.

Il rischio informatico non è dunque l'ennesima novità portata dal coronavirus: il fenomeno esiste da tempo ed è in crescita. Però non sembra che imprese e cittadini abbiano ancora colto pienamente la portata del rischio. "Si rileva ancora una certa debolezza culturale, che fati-

***Sergio Mattiuz**, amministratore delegato di Ania Safe*

UN OSSERVATORIO SUL DEEP WEB

Ania Safe ha presentato a fine maggio il suo *Osservatorio Cyber Intelligence*. "Si tratta di uno servizio di security intelligence che ricerca nel deep/dark web tutte le compromissioni e vulnerabilità cyber di un'impresa, ovvero gli elementi che costituiscono la base di qualsiasi attacco informatico", illustra Sergio Mattiuz, amministratore delegato di Ania Safe. "Il sistema – spiega – cerca le criticità dell'impresa proprio come farebbe un hacker per predisporre un attacco". Una volta terminata l'attività di scouting, il servizio di Ania Safe prevede la redazione di un report personalizzato sulle vulnerabilità rilevate ed eventualmente l'offerta di un'azione di *remediation* finalizzata a mitigare il rischio.
La soluzione è rivolta principalmente alle imprese assicurative ma, spiega Mattiuz, "vista la tipologia di attività, stiamo pensando di presentarla anche ad aziende che operano in altri settori".

ca a essere superata", afferma Mattiuz. "Il terreno principale per la fioritura di attacchi informatici – prosegue – è dato dal comportamento umano: disattenzione e cattive abitudini costituiscono ancora la causa principale di attacchi". Ecco perché, a detta di Mattiuz, "la protezione contro il rischio informatico è un tema culturale prima ancora che tecnologico". Ed ecco perché, se le nostre abitudini non cambiano, la spinta digitale del coronavirus potrà tradursi in un forte aumento del rischio informatico.

UN FENOMENO IN EVOLUZIONE

A fronte di abitudini che restano dure a morire, il fenomeno degli attacchi informatici mostra invece una forte vitalità. E non soltanto in termini di numeri, ma anche di qualità dei modelli operativi. Una recente ricerca di **CyberCube**, a tal proposito, è arrivata a coniare la formula "ransomware as a service". Secondo il rapporto, il crimine informatico non è più paragonabile a una sorta di attività artigianale, in cui il singolo hacker prepara il virus, predispone l'attacco e, se le cose vanno bene, raccoglie i frutti del proprio lavoro: oggi il modello di business ha assunto tutti i tratti di una vera e propria filiera industriale, in cui i diversi componenti agiscono in maniera complementare per portare a termine con successo un attacco.


© iBrave - iStock

"È un cambiamento piuttosto radicale nel modo di operare dei criminali informatici. Per organizzare un attacco – osserva – basta fare un giro nel deep web: in maniera gratuita o a prezzi davvero irrisori, sono disponibili dati e informazioni sulle vulnerabilità, strumenti e software che possono consentire a chiunque di portare a termine un attacco". Il cyber risk oggi non è più appannaggio delle sole organizzazioni criminali o di enti governativi particolarmente aggressivi. "Anche un ragazzino, nella sua cameretta, può trovare facilmente tutto quello che gli serve per muovere i suoi primi passi da criminale informatico", avverte Mattiuz.

UN APPROCCIO INTEGRATO

La speranza dell'ad di Ania Safe è che la percezione della minaccia, accresciuta dal coronavirus e dalle nuove modalità di lavoro dei criminali informatici, possa favorire quel salto culturale che cittadini e piccole e medie imprese fanno ancora fatica a compiere. "Il livello di attenzione è cresciuto negli ultimi anni, ma non abbastanza da garantire una protezione adeguata", afferma. Solo da qui sarà possibile partire per arrivare a un approccio integrato di sistemi e comportamenti virtuosi che possano ridurre (eliminarlo sarà impossibile) il rischio informatico. "È necessario che si prenda innanzitutto consapevolezza della minaccia: un semplice antivirus non basta più per fronteggiare un fenomeno che è in crescita anche a causa della crisi economica generata dall'emergenza sanitaria. Una realtà che si è rivelata redditizia per i criminali informatici e che, essendo in continua evoluzione, rende rapidamente obsolete le misure di protezione fino al giorno prima considerate affidabili. Ancora oggi – conclude Mattiuz – imprese e cittadini non sono sufficientemente consapevoli dei rischi che stanno correndo".