La proprietà intellettuale è riconducibile alla fonte specificata in testa alla pagina. Il ritaglio stampa è da intendersi per uso privato

Esg

LA PANDEMIA SPINGE SULLA CYBERSECURITY

La crisi ha visto l'esplosione degli attacchi informatici, mentre l'accelerazione sul telelavoro ha esposte le debolezze delle reti aziendali, facendo emergere nuove opportunità sul fronte dei servizi di sicurezza. Il futuro? Cloud e architettura Zero-trust

Gaia Giorgio Fedi

La pandemia è stata in qualche modo l'Eldorado degli hacker, e ha fatto emergere di conseguenza nuove opportunità sulla cybersecurity. "La crisi del Covid-19, come tutte le crisi, è stata accompagnata da una fortissima crescita del numero di attacchi informatici in tutto il mondo", commentano Frédéric Dupraz e Matthieu Rolin, gestori del Thematics Safety Fund di Thematics Am, affiliata di Natixis IM: "gli hacker si nutrono del caos e vediamo attori considerati molto sicuri, come il broker online Usa Robinhood o la società di servizi digitali Steria Sopra in Francia, che sono stati vittime di attacchi".

Secondo un recente report del colosso israeliano di Cyber Security Check Point Software Technologies, durante il lockdown "il numero di attacchi informatici è passato dai 5.000 a settimana di febbraio 2020 ai 200.000 a settimana di aprile", osserva Riccardo Volpi, fund manager di Pharus Sicav. Non solo. "Questa crisi è stata anche unica, in quanto ha portato a una profonda trasformazione nel modo in cui lavoriamo", sottolineano gli esperti di Thematics Am, riferendosi alla straordinaria accelerazione del telelavoro. "La rete aziendale ha subìto una profonda trasformazione, con centinaia, migliaia di connessioni provenienti da reti private spesso poco protette, a volte da terminali non protetti; i responsabili della sicurezza IT hanno dovuto gestire questa trasformazione con strumenti spesso inadeguati", dicono Dupraz e Rolin.

Quali opportunità stanno emergendo da queste dinamiche? "Crediamo che ce ne siano due principali - interviene Rahul Bhushan, co-founder di Rize Etf - La prima è legata alle tecnologie basate su cloud. Uno studio Microsoft ha rivelato quest'anno che le aziende che hanno segnalato il maggior numero di attacchi di phishing riusciti avevano risorse definite come locali anziché cloud-based. La seconda è l'architettura Zero Trust. Non è mai stato così importante come oggi garantire, in una configurazione di lavoro a distanza, che l'afflusso di nuovi dispositivi potenzialmente non protetti che accedono alle reti aziendali siano effettivamente dipendenti che accedono dalle loro case", osserva Bhushan. Lo zero trust è "un modello di sicurezza basato su un processo molto severo di controllo dell'identità, che impone che solo gli utenti e i terminali autenticati e autorizzati possano accedere a dati e applicazioni. È invece finita l'architettura classica basata sul firewall a protezione della rete aziendale. Anzi, con lo zero-trust è la stessa nozione di rete a scomparire", spiegano ancora da Thematics Am.

> Frédéric Dupraz
senior portfolio manager di Thematics Am

> Matthieu Rolin
gestore di Thematics Am

> Riccardo Volpi
fund manager di Pharus Sicav

CHART L'indice Ice Cyber Security

Fonte: Investing.com - Andamento a 5 anni

Insomma, la cybersecurity ha potenzialità esplosive. Volpi di Pharus ricorda che, "secondo Gartner, nei prossimi 5 anni il Cybercrime costerà circa 5,2 trilioni di dollari alle aziende". Inoltre, il rischio informatico colpisce tutti i settori, e non risparmia le piccole aziende: "il 43% degli attacchi informatici ha infatti come obiettivo le piccole medie aziende e solo il 14% delle aziende era pronto a difendersi". Tra i singoli titoli da tenere d'occhio, Volpi spiega che il fondo Pharus Next Revolution, in cui la cybersecurity ha un peso elevato, si focalizza "sia su società leader di settore e più tradizionali come Cisco, sia su quelle più incentrate alla protezione delle piattaforme cloud, come Cloudfare (+120 % quest'anno), e Crowdstrike (171% quest'anno)". Anche Bhushan cita tra i titoli interessanti alcune aziende "cloud native", come appunto Crowdstrike e Cloudflare, ma anche Zscaler e Sailpoint. "Siamo anche grandi fan delle società attive nell'Identity Access Management, come Okta e Ping Identity".