la Repubblica
AFFARI&FINANZA

Imprese in allarme

Più formazione per frenare gli hacker

RAFFAELE RICCIARDI

Per la Cyber risk survey con lo smart working sono aumentati gli attacchi alle aziende, favoriti soprattutto da errori umani: nel primo semestre del 2021 sono saliti del 180%

L'errore umano è la prima falla attraverso la quale si infilano i cyber-criminali che – complice la digitalizzazione forzata delle organizzazioni – stanno impazzando sempre più in rete. I collaboratori sono la vulnerabilità numero uno in quasi sette aziende su dieci: una debolezza riconosciuta con maggiore urgenza rispetto all'utilizzo di programmi o sistemi operativi obsoleti, a un inadeguato controllo degli accessi, a misure di protezione delle reti interne insufficienti o alla mancanza di soluzioni anti-malware. Numeri che emergono dalla Cyber Risk Survey patrocinata da Anra e curata dall'Università di Verona con Riesko su un campione di 250 società, per oltre la metà in settori di punta quali informatica e finanza.

Luciano Carta (ex Aise, ora Leonardo) a #SocialCom21 ha recentemente dato qualche numero del fenomeno: in Italia nei primi sei mesi del 2021 sono stati registrati 36 milioni di eventi malevoli, il 180% in più sul 2020. «Il 2021 è stato un anno record sul fronte cyber security, con un impatto economico che supera il 6% del Pil mondiale», spiega Guido Moscarella, direttore operativo di Innovery, citando l'ultimo Rapporto Clusit. «Solo nel primo trimestre, nel 74% degli attacchi gli effetti sono stati classificati come 'molto importanti', contro il 49% dello scorso anno». In crescita, poi, le minacce finalizzate all'estorsione, ormai l'88% del totale.

Di fronte a questa vera e propria ondata, dice la ricerca dell'ateneo veneto, la sensibilità verso il tema della sicurezza informatica è cresciuta e ormai il 72% delle aziende dichiara di averne un'alta consapevolezza. Resta però una presa di coscienza limitata alle funzioni in ambito tecnico. «La consapevolezza in azienda cresce, ma spesso è limitata ai livelli più elevati di management e nei settori It. Non basta», incalza Federica Maria Rita Livelli, consigliera Anra. «Il motto greco "conosci te stesso" vale oggi più che mai: le organizzazioni devono partire da un censimento di quel che hanno in pancia, inteso come strutture software e hardware, e diffondere la cultura della cyber-sicurezza a tutte quelle persone impegnate in un processo di digitalizzazione accelerata».

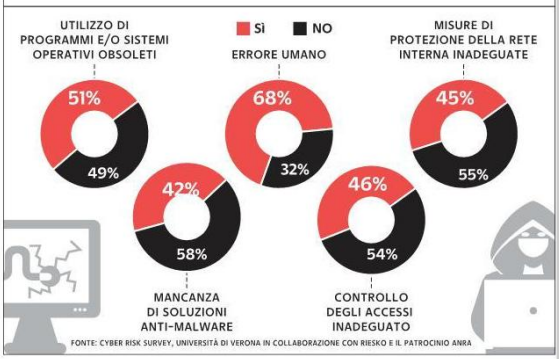
Concorda Moscarella, e non a caso Innovery ha lanciato con la Luiss Business School il laboratorio Resilient Information Management dedicato ai dirigenti: «L'idea che il tema della sicurezza informatica riguardi solo i profili tecnici crea un grosso limite alle aziende. La classe dirigente ha il compito di guidare e difendere la propria azienda da possibili minacce».

Quando si passa al "dunque", infatti, i nodi vengono al pettine. Del campione analizzato, solo poco più della metà ha approntato un piano operativo per affrontare i rischi. Ancor meno si fa sul lato della formazione dei collaboratori: solo il 49% delle aziende prevede percorsi mirati e, nella stragrande maggioranza dei casi, anche quando questi processi sono previsti l'investimento è minimo: meno del 15% del budget.

I fronti aperti sono sempre di più, dunque, e per questo «non è possibile mantenere un approccio top-down, la formazione è fondamentale e il singolo dipendente, a maggior ragione se lavora di più da casa, deve acquisire meccanismi semplici come il cambio frequente della password, o il backup dei dati in luoghi sicuri. Ci vuole un linguaggio semplice in modo che tecnici e il resto dell'organizzazione possano comunicare», dice ancora Livelli. Il tutto si trasforma in un «vantaggio competitivo per le aziende, perché i clienti sono sempre più sensibili alla gestione dei propri dati, mentre bandi e gare d'appalto richiedono la dimostrazione di cyber-resilienza e cultura del rischio». Una tendenza che risalta ancora poco dai dati: nonostante le scorribande dei cyber-criminali crescenti e le vulnerabilità latenti, il 53% delle aziende crede di essere al sicuro. Almeno fino al prossimo attacco.

I numeri

GLI ATTACCHI
PERCHÈ SI VERIFICANO



FONTE: CYBER RISK SURVEY, UNIVERSITÀ DI VERONA IN COLLABORAZIONE CON RIESKO E IL PATROCINIO ANRA