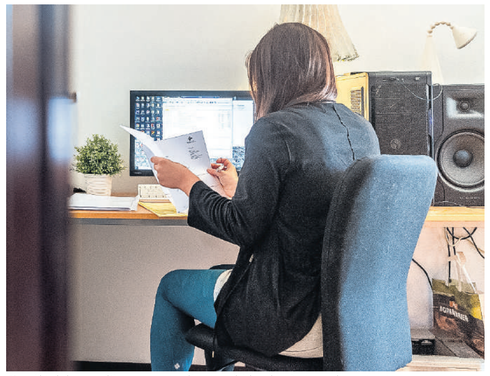
Telelavoro sotto attacco

Negli ultimi mesi si sono moltiplicate le aggressioni hacker ai danni delle aziende Esperti in allarme «Aumento devastante con l'home working, ma proteggersi è possibile»

La criminalità informatica oggi si è industrializzata e il rischio di subire un attacco è diventato la norma e non più un'eccezione. ©CDT/ARCHIVIO

DI **Andrea Bertagni**

Tempo di lettura: 5'21"



Con il telelavoro l'incremento di attacchi hacker è stato devastante. ©CDT/ARCHIVIO

Estorsioni, truffe, furti. Sempre più aziende in Ticino finiscono nel mirino degli hacker. Complice il telelavoro molte imprese si scoprono inermi, indifese, vulnerabili. «In passato gli attacchi andavano a ondate, oggi l'onda è costante», sintetizza Alessandro Trivilini, responsabile del Servizio di informatica forense della Scuola universitaria professionale della Svizzera italiana (SUPSI). Alberto Redi, che con la sua ditta si occupa di CyberSecurity, è ancora più esplicito. «L'aumento delle minacce è devastante». Cifre esatte non ce ne sono. Perché chi viene attaccato non lo dice, rimedia alla falla, va avanti e incrocia le dita. Di sicuro però il Servizio di informatica forense della SUPSI riceve «ogni settimana 4-5 chiamate da parte di aziende e privati che hanno il sentore di essere stati violati o che non sanno come proteggersi». Pochi giorni fa il Centro nazionale per la cibersicurezza ha fatto il punto: le segnalazioni sono raddoppiate, passando da 10.833 nel 2020 a 21.714 nel 2021. L'esplosione di casi è emersa anche mercoledì scorso, quando si è saputo che il Servizio delle attività informative (SIC) si è mosso un po' troppo liberamente nel raccogliere dati sugli attacchi hacker compiuti in Svizzera dall'estero e per questo è stato «richiamato» dal Dipartimento federale della difesa.

Puntare sulla formazione

Proteggersi è però possibile, anche se «l'incidente informatico va dato ormai per scontato, non è più solo un rischio come in passato», avverte Trivilini. «Un'azienda piccola che non può permettersi spese folli in sicurezza può anche salvare i propri dati con un backup periodicamente», segnala Antonio Carzaniga, decano della Facoltà di informatica dell'Università della Svizzera italiana (USI). Un'altra strada, anzi una delle vie per resistere e cercare di mettersi il più possibile al sicuro è quella di «puntare sulla formazione», sottolinea Carzaniga. Soprattutto ai dipendenti. Visto che sono loro che si collegano da casa o fuori ufficio per lavorare. Smart working e home working «non sono infatti la stessa cosa - precisa Trivilini - certo, servono le stesse preperazioni e attenzioni, ma quando si usa una rete che non è quella di casa occorre essere ancora più prudenti». Anche perché, spiega Alessandro Doninelli, che ha una società informatica con 20 anni di esperienza, «è proprio l'utente la parte più vulnerabile della catena». Ecco perché un espediente è quello di «affidarsi alle infrastrutture cloud, perché i server aziendali, se non si fa sufficiente manutenzione, sono anch'essi molto vulnerabili agli attacchi».

> ***Da ottobre riceviamo una chiamata al giorno da aziende o privati vittime di attacchi o presunti tali***
>
> *Alessandro Trivilini*
> *responsabile Informatica Forense SUPSI*

> ***I criminali fanno parte di organizzazioni malavitose dell'Europa dell'Est e dell'Africa***
>
> *Alessandro Doninelli*
> *imprenditore informatico*

Minaccia costante

Una minaccia costante. Che non conosce confini, limiti. Che usa tutti gli stratagemmi possibili e immaginabili. È quella della criminalità informatica. «Che ormai si è industrializzata - annota Redi - una volta gli attacchi non erano ben fatti, oggi sono sempre più sofisticati. Dal 2020 al 2021 il numero di ransomware in circolazione, programmi informatici che bloccano i dispositivi infettati e richiedono un riscatto da pagare per riavere indietro i dati, sono ad esempio raddoppiati».

Parola d'ordine prevenzione

Conoscere per mettersi al riparo, dunque. Carzaniga ne è convinto. «Nella sicurezza informatica bisogna investire, non si scappa. Serve formazione per le aziende e per i dipendenti. Perché la tecnologia è importante, ma serve conoscerla, serve sapere come muoversi». Senza i giusti accorgimenti un computer, un tablet o uno smartphone potrebbero essere infettati da uno o più software dannosi in pochissimo tempo. Tutti i dati salvati potrebbero quindi essere visualizzati, manipolati o completamente cancellati da sconosciuti. O peggio da criminali. Prevenire. Sembra essere questa una delle parole magiche per combattere contro criminali informatici, «che ormai fanno parte di vere e proprie organizzazioni - osserva Doninelli - e spesso provengono dai Paesi dell'Est e dall'Africa». Prevenire con un vero e proprio «piano di risposta agli incidenti - fa presente Trivilini - anche perché se si subisce un atta cco e si vuole fare denuncia bisogna essere in grado di dimostrare di aver fatto tutto il possibile per impedire la minaccia». Tutto questo anche in ottica assicurativa. Perché se non si riesce a provare di essere stati a prova di attacco, potrebbe essere difficile ottenere risarcimenti.

> ***L'aumento di aggressioni è devastante. In un anno il numero di programmi-virus è raddoppiato***
>
> *Alberto Redi*
> *imprenditore informatico*

> ***Non si può non investire nella sicurezza aziendale facendo formazione anche tra i dipendenti***
>
> *Antonio Carzaniga*
> *decano Facoltà informatica USI*

Nuova legge all'orizzonte

Con una certezza. «Nessuno è al riparo. Tutti potenzialemente sono sotto attacco. Le aziende piccole, così come quelle grandi, oltre ovviamente i privati cittadini», segnalano gli esperti. «Chiaramente le imprese di grandi dimensioni sono forse quelle più bersagliate - aggiunge Carzaniga - perché lo scopo di un'aggressione informatica è anche quello di arrecare un danno di immagine. Ciò detto, tutti siamo comunque a rischio». Tutto questo quando all'orizzonte si staglia la nuova legge federale sulla protezione dei dati. Che imporrà un nuovo paradigma. A tutti. A cominciare dalle società «che per la prima volta saranno obbligate a denunciare di essere state vittime di attacchi informatici», rileva Trivilini.

Le assicurazioni

«Abbiamo nuove polizze, ma le società devono sensibilizzare il personale»

Anche le assicurazioni si organizzano contro i ciberattacchi. ©CDT/CHIARA ZOCCHETTI

DI **Giorgia Cimma Sommaruga**

Con l'aumento dei ciberattacchi ai danni delle aziende, le compagnie d'assicurazione si sono organizzate. E hanno creato polizze su misura, spingendosi in un mondo nuovo, più tecnologico, più minaccioso, che le ha costrette a «formare personale specializzato per far fronte al problema», dicono. Dalle violazioni della personalità, come cibermobbing, o di abusi nei pagamenti e nelle transazioni online, come frodi di carte di credito, nonché violazioni dei diritti d'autore in Internet. Per non parlare delle violazioni a livello aziendale. Sempre più le compagnie assicurative sono vigili su queste situazioni talvolta imbarazzanti e compromettenti.

I rischi maggiori

«I ciber attacchi fanno parte dei rischi che gli assicuratori privati considerano come rischi maggiori, a livello svizzero come a quello mondiale», spiega Samuele Donnini, presidente ASA (Associazione svizzera assicuratori) sezione Ticino. «Negli ultimi 18 mesi - aggiunge - la digitalizzazione dell'economia si è intensificata e allo stesso tempo le minacce sulla ciber sicurezza sono cresciute. Nel 2020, gli attacchi di malware e ransomware sono aumentati rispettivamente del 358% e del 435%».

Ciò che risulta rilevante è l'attenzione statale alla problematica, non a caso «gli assicuratori privati - riprende Donnini - sono stati coinvolti nello sviluppo della «Strategia nazionale per la protezione della Svizzera contro i rischi informatici» della Confederazione. Sono coinvolti nello sviluppo di standard minimi e sostengono la sensibilizzazione delle aziende ai rischi informatici attraverso le loro relazioni con i clienti aziendali».

Tuttavia per far fronte ai ciberattacchi serve una nuova consapevolezza. «Noi - spiega Michele Bertini, agente generale della società di assicurazioni La Mobiliare - proponiamo un Cyber-Training per aziende con simulazione di attacchi informatici tramite e-mail. Alla fine forniamo un resoconto e formiamo il personale».

Lo scopo delle compagnie è quello di promuovere una «cultura prudente» del dipendente affinché abbia tutti i meccanismi di difesa: «Dopo anni di esperienza abbiamo verificato che la la cuna avviene per mancanza di formazione. La cosa più importante è dunque il comportamento prudente e consapevole dei dipendenti e la loro sensibilizzazione», continua Bertini.

> ***Nel 2020 tra malware e ransomware un aumento di casi rispettivamente del 358% e del 435%***

> ***«Ciò che conta di più è il comportamento prudente e consapevole dei collaboratori»***

Diverse sfaccettature

Gli esperti osservano che i ciberattacchi possono avere diverse sfaccettature: «Tutto è possibile, da un attacco locale e mirato, a un attacco globale che interrompe intere catene di approvvigionamento. L'ASA - nota Donnini - stima che un ciberattacco su larga scala in Svizzera potrebbe causare un danno economico di circa 15 miliardi di franchi». Per quanto riguarda i ciberrischi, le compagnie forniscono varie soluzioni. Ma, sottolinea il presidente di ASA, «mentre i particolari prodotti e la copertura assicurativa sono questioni che riguardano le compagnie di assicurazione, la necessità di condurre attività d'informazione e prevenzione con i clienti assicurati - incluso quelli aziendali - è evidente».

«Mobiliare è stata fra le primissime assicurazioni in Svizzera a proporre un prodotto «a pacchetto completo» di copertura ciber per PMI: con il RedBox, un tool fisico, siamo in grado di monitorare oltre 100.000 possibili debolezze nei sistemi delle aziende», conclude Bertini.