Una risposta ai cyber attacchi

Uno staff specializzato che monitora i sistemi It supportato dalle migliori soluzioni di cybersecurity. Il presidente della Winservice illustra le buone prassi della sicurezza informatica per farsi trovare pronti

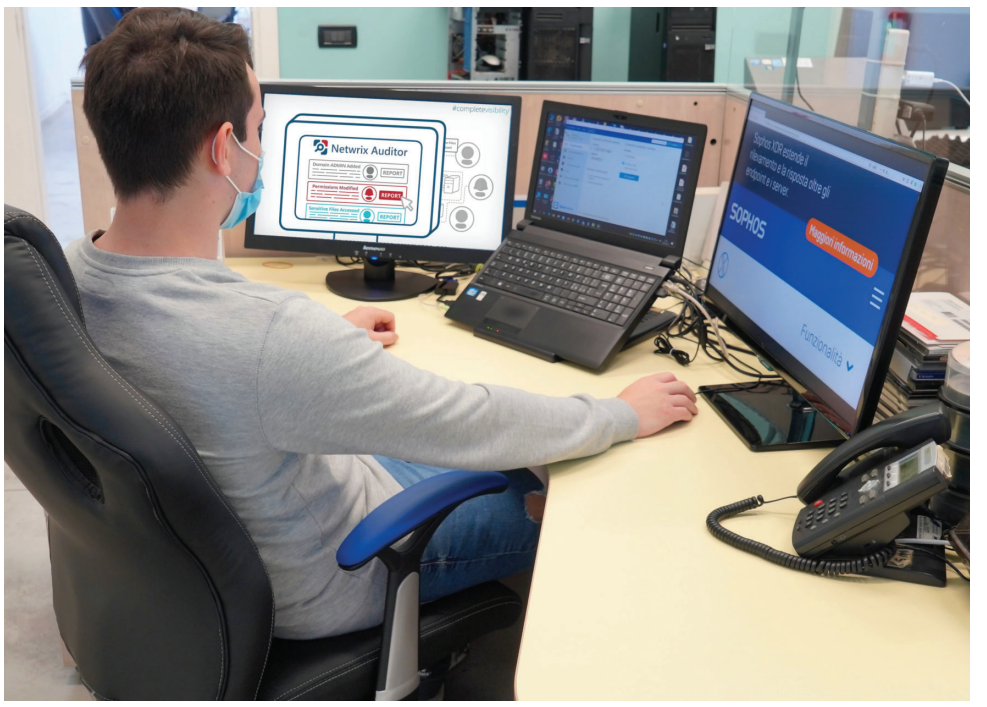
Con la pandemia sono aumentate le minacce cibernetiche. Secondo un sondaggio realizzato da Vanson Bourne per Sophos, il 37 per cento delle organizzazioni intervistate è stato colpito da ransomware. Più della metà delle organizzazioni durante l'anno passato sostiene che i cybercriminali sono riusciti a cifrare i dati. Per questo i servizi di sicurezza informatica sono sempre più richiesti dalle aziende per proteggerle da malware, attacchi informatici, intrusioni e applicazioni pericolose. «La sicurezza informatica è però fatta non solo di prodotti e soluzioni, ma anche di persone» spiega Alberto Rossetto, presidente e sales manager di Winservice, azienda specializzata in Information technology. «Come azienda, formiamo costantemente il nostro team per affiancare i clienti con uno staff specializzato e certificato dai nostri partner strategici nella gestione della cybersecurity: Netwrix e Sophos. I sistemi informatici vengono costantemente monitorati dai nostri sistemisti per intervenire, in tempo reale, nella risoluzione di qualsiasi problema o anomalia che possa rallentare o bloccare il business».

La percentuale degli attacchi che prevedono una richiesta di riscatto senza cifrare i dati è raddoppiata.

«Sì. Alcuni hacker stanno adottando un approccio diverso basato sull'estorsione, con il quale i file, invece di essere cifrati, vengono prelevati illecitamente con la minaccia di una loro pubblicazione, a meno che non venga pagato il riscatto specificato. Nelle richieste di riscatto, i cybercriminali spesso cercano di indurre le vittime a pagare, puntando sulle pesanti sanzioni previste per i casi di violazione dei dati. Il 32 per cento delle organizzazioni intervistate ha infatti pagato il riscatto per recuperare i dati con un aumento rispetto alla ricerca dell'anno precedente. Solo il 57 per cento è riuscita a ripristinare i dati grazie ai backup».

Spesso anche pagando, le probabilità di recuperare tutti i dati sono poche.

«In media, le organizzazioni che hanno pagato il riscatto sono riuscite a riavere solo il 65 per cento dei file cifrati. Il pagamento del riscatto è solo una parte della spesa necessaria per rimediare ai danni di un attacco. Il costo complessivo di riparazione dei danni di un attacco ransomware è infatti aumentato ed è pari a 1,85 milioni di dollari. Più del doppio rispetto ai 716.106 dollari dell'anno precedente. Questa spesa è data dai tempi di inattività, le ore di lavoro del personale, i costi associati ai dispositivi di rete, la perdita di opportunità commerciali e, infine, la somma pagata per il riscatto. È meglio essere preparati e non subire un attacco, piuttosto che il contrario. In questo possono essere di grande aiuto, in particolare, le soluzioni Sophos Intercept X Advanced e Sophos Intercept X Advanced with Edr».



OCCORRE UTILIZZARE UNA PROTEZIONE A LIVELLI MULTIPLI PER BLOCCARE I CYBERCRIMINALI OVUNQUE POSSIBILE ALL'INTERNO DELL'AMBIENTE IT

Come assicurarsi che gli hacker non riescano a infiltrarsi nell'ambiente informatico dell'organizzazione?

«Occorre utilizzare una protezione a livelli multipli per bloccare i cybercriminali ovunque possibile all'interno dell'ambiente It. È necessaria una difesa in profondità che sia il risultato della combinazione tra tecnologie informatiche e supervisione umana. Le tecnologie offrono la scalabilità e i livelli di automazione necessaria, mentre gli esperti sono in grado di individuare tattiche, tecniche e procedure che indicano che un hacker molto abile sta cercando di infiltrarsi nell'ambiente informatico».

Come capire in tempo quando si è sotto attacco?

«È opportuno scegliere soluzioni di sicurezza che abbiano un approccio predittivo per intercettare e rispondere subito alle minacce. Inoltre, il controllo e il monitoraggio dei sistemi It e delle soluzioni di sicurezza informatica da parte di un team specializzato è fondamentale per verificare quanto accade e intervenire immediatamente. Ricordiamo che proteggere i propri dati implementando misure di sicurezza adeguate è anche previsto dalla nuova normativa privacy (Gdpr). La maggior parte delle organizzazioni ha invece difficoltà a gestire enormi volumi di dati aziendali, alcuni dei quali sono sotto il controllo dell'It aziendale. Ma non tutti. È consigliabile implementare un programma di governance delle informazioni (data governance) che aiuti a gestire correttamente i dati, adempiere agli obblighi legali, avere una migliore produttività dei dipendenti e ridurre il rischio aziendale associato a una gestione impropria delle informazioni come le soluzioni Netwrix Auditor e Netwrix Data Classification».

• **Leonardo Testi**

Alberto Rossetto, presidente e sales manager Winservice. L'azienda ha sede a Fossò (Ve) www.winservice.it

SOLUZIONI DI ASSISTENZA E SICUREZZA INFORMATICA

Winservice è un'azienda specializzata in Information technology. Fondata nel 1997, offre alle aziende un servizio globale per tutta la struttura informatica: software gestionali e di produzione, centralini telefonici, stampanti multifunzione, infrastruttura hardware, soluzioni cloud computing, assistenza sistemistica e servizi di sicurezza informatica. Oltre alla fornitura dei prodotti, Winservice garantisce un servizio post-vendita. Installazione, formazione e assistenza tecnica post-vendita sono eseguite dal personale specializzato e certificato.