TECNOLOGIA/SICUREZZA INFORMATICA

PAGARE O NON PAGARE...

È QUESTO IL DILEMMA DELLE AZIENDE VITTIME DI UN ATTACCO MEDIANTE RANSOMWARE, CHE CRIPTA I FILE RENDENDOLI INUTILIZZABILI. IL MIGLIOR RIMEDIO, COME SEMPRE, È LA PREVENZIONE. CHE IN AMBITO INFORMATICO HA UN NOME BEN PRECISO: BACKUP

DI ALBERTO GEROSA

Se non fosse una realtà preoccupante, ci sarebbe quasi da ridere. Sì, perché **le organizzazioni criminali che praticano il ransomware, infettando computer e reti con programmi che criptano i dati fino a quando il malcapitato non acquista la password in grado di sbloccarli, hanno un servizio clienti**. Che si prodiga per aiutare la vittima del cyberattacco non appena decide di allentare i cordoni della borsa. Chi crea i ransomware deve infatti essere "credibile": se la decrittazione non funziona, nessuno pagherà più.

"Sono un pesce troppo piccolo, non mi riguarda", penserà magari qualcuno di voi, valutando di voltare subito pagina. I dati dicono il contrario: **se le grandi aziende sono sempre dotate di uno specialista IT che monitora le minacce provenienti dal cyberspazio, le Pmi sono solitamente meno strutturate e, di conseguenza, più vulnerabili**.

Quanto ai settori, secondo il Cefriel, il centro di innovazione digitale fondato dal Politecnico di Milano, l'industria

segna l'aumento più significativo, dal 7% al 18% di attacchi in un anno, pur rimanendo la finanza, le assicurazioni e la pubblica amministrazione gli ambiti maggiormente colpiti.

I RISCHI DEL LAVORO A DISTANZA

Gli esperti fanno notare che quando siamo entrati in lockdown, gli attacchi hanno subito un'impennata importante, perché nel lavoro ibrido la sicurezza è più difficile da mantenere. Come difendersi? Il primo consiglio è quello di assoldare un consulente, che verificherà sul luogo l'esposizione al pericolo di server, reti, switch, firewall e software, stilando poi un preventivo personalizzato in base alle esigenze dell'azienda.

Il secondo consiglio è quello di fare un backup serio dei propri dati: è infatti lapalissiano che il riscatto non ha più mordente se si dispone di uno o più duplicati dei documenti criptati. "I file vanno centralizzati, non decentralizzati – afferma **Matteo Discardi**, *autore di numerosi libri di divulgazione informatica e titolare dell'azienda di consulenza 1802.it* –; vanno cioè messi tutti sul server, mentre i client non dovrebbero contenere documenti di sorta. La situazione ideale è quella di arrivare la mattina in ufficio, collegarsi al server, prelevare i file di cui si ha bisogno, lavorarli e poi alla fine della giornata rimetterli sul server, cancellandoli in locale. **Il computer deve essere sempre vuoto in termini di file e documenti di lavoro, a differenza del server che rimane pieno e di quest'ultimo si fanno backup regolari**".

Il backup va eseguito in modalità offline, quindi in un contesto non accessibile direttamente ai computer. Le aziende più attente fanno backup alternati: il server effettua il backup su un altro disco o server, una volta finito il backup si scollega il cavo dal server/disco e lo si attacca a un altro disco. In pratica, una notte si fa il backup sul volume A, un'altra notte sul volume B, e così via; in questo modo, l'attacco ransomware corromperà uno solo dei backup, non entrambi.

PRO E CONTRO DEL CLOUD

In alternativa a questo metodo di trasferimento "fisico" dei dati si può valutare il backup su cloud. Che però è più costoso, inoltre richiede particolari attenzioni: **l'infezione dei file non avviene tutta subito, al contrario può manifestarsi in maniera diluita nel tempo, prendendo di mira un file oggi, un secondo file domani, ecc. Di conseguenza, l'utente non se ne accorge subito e i file infettati rischiano di essere archiviati anch'essi sul cloud**: "Il backup su cloud – commenta Discardi – è una buona idea, anche perché oggi il lavoro ibrido sta prendendo sempre più piede; tuttavia, deve essere eseguito con software che analizzano i file e rilevano la presenza di quelli criptati. Per esempio, OneDrive for Business, servizio cloud offerto da Microsoft 365, si accorge subito di simili file e avvisa l'utente, chiedendogli se procedere con l'inclusione del documento nel server oppure no".

L'EFFICACIA DEGLI ANTIVIRUS

E gli antivirus? Sono efficaci contro il ransomware? "Siamo nel campo delle probabilità – risponde Discardi –; dipende dal ransomware, da quanto è recente, da come è costruito. **Al pari per esempio di Microsoft Word, Adobe Photoshop, Winzip, anche il ransomware è un**

applicativo, quindi l'antivirus nella migliore delle ipotesi lo blocca, però può anche non riconoscerlo e scambiarlo per un applicativo qualsiasi. Windows 11 e in particolare la sua versione per le aziende, Enterprise, hanno una gamma molto completa di routine di sicurezza attive di default, però è l'utente che ha in mano il sistema operativo. E l'utente è la falla più grande".

SISTEMI OPERATIVI, NESSUNO È IMMUNE

"Io tanto lavoro in ambiente Mac/Linux, immune ai virus": è un'obiezione che si sente ripetere spesso, ma da sfatare, perché priva di fondamento. **Purtroppo, nessun sistema operativo è totalmente al sicuro dai virus e immune ad essi**. Negli anni passati alcuni server di importanti brand di settore – in particolare nel mondo Nas (network attached storage), cioè dispositivi connessi a una rete che consentono la memorizzazione e l'accesso ai dati – sono stati oggetto di pesanti attacchi ransomware. E i Nas hanno sistemi operativi basati proprio su Linux.

SOFTWARE SEMPRE AGGIORNATI

E veniamo al consiglio numero tre: **scaricare i software solo dai siti delle case madri, non dai vari 'mirror' o pagine non ufficiali**. Inoltre, i software vanno aggiornati, ivi inclusi ovviamente quelli della suite Office: "Microsoft 365 si aggiorna una volta al mese, non automaticamente – spiega il titolare di 1802.it –, un tempo abbastanza stretto, che riduce le possibilità di chi scrive software malevolo. Se qualcuno dice che non si fida ad aggiornare il suo sistema, allora non ha capito niente: se io uso Office e Office lo sviluppa Microsoft, io di Microsoft mi devo fidare".

Caso limite: i consigli finora dispensati non sono serviti a proteggere la nostra rete dall'attacco ransomware. Che fare? Pagare o no? Una risposta univoca non c'è, anche sa va sottolineato che scendere a patti con i criminali non è mai una buona idea e il mostrarsi remissivi ci espone ad essere attaccati nuovamente in futuro. Ribadita questa premessa – che ha un valore etico, prima ancora che pratico – qualora proprio volessimo fare esercizio di pragmatismo, bisogna quantificare l'esborso a cui andremmo incontro. "Se la richiesta è 5.000 euro per decrittare tutto il server – afferma Discardi – è chiaro che per un'azienda di 50 dipendenti non si tratta di un danno rilevante. Diverso se l'importo richiesto sono 100.000 euro. **Rimane comunque decisiva la valutazione economica della propria realtà e di quanto valgono i file in questione**. Se, per esempio, posseggo una foto d'autore oppure di un personaggio importante in una situazione del tutto imprevista, quello scatto vale moltissimi soldi (e andrebbe 'backuppato' in sette posti diversi). Se ho la foto di un tramonto e mi viene criptata, tutto sommato domani vado in terrazza e ne faccio un'altra...".