TECHNOPOLIS
STORIE DI ECCELLENZA E INNOVAZIONE

CYBERSECURITY

SICUREZZA, PERCHÉ NON SEMPRE FUNZIONA?

Errori umani, compromissioni del backup, inganni del phishing e attacchi sempre più sofisticati. Sono alcune delle ragioni che rendono inefficaci le strategie di difesa.

Se le persone sono l'anello debole nella catena della cybersicurezza, come sentiamo ripetere da tempo, la soluzione al problema del rischio informatico non può essere soltanto tecnologica. Quello delle competenze è un tema ricorrente nelle ricerche, nelle argomentazioni dei vendor, nelle disquisizioni degli analisti. Ed è un tema, purtroppo, ancora molto attuale. Tra gli addetti ai lavori, uno tra i dati più citati in assoluto è quello, tratto da un report del **World Economic Forum,** secondo cui ben il 95% degli incidenti di cybersicurezza dipenderebbe dall'errore umano. Il caso più tipico e più frequente è quello del phishing veicolato dalla posta elettronica: leggerezza, fretta, superficialità e, in certi casi, la capacità di questi messaggi di apparire convincenti alimentano una categoria di minaccia informatica non certo nuova ma ancora efficace.

Errare è umano

A fare danni è soprattutto il cosiddetto spear phishing, cioè quello mirato su specifica azienda o persona. Rispetto ad altri tipi di minaccia veicolata dall'email, come il ransomware o più in generale il malware, il volume di questo genere di attacchi è basso, ma in compenso sono ampiamente diffusi e hanno un'alta percentuale di successo. Lo spear phishing corrisponde, infatti, ad appena lo 0,1% del totale delle minacce email osservate da **Barracuda** nel 2022, ma è responsabile del 66% delle violazioni. Gli esiti sono notevoli: il 55% degli intervistati colpiti da spear phishing ha segnalato macchine infettate da malware o virus, quasi la metà ha subìto il furto di dati sensibili (49%) o di credenziali di login (48%) e il 39% ha riportato danni economici diretti. "Anche se il volume dello spear phishing è basso, questa minaccia, che sfrutta tattiche di social engineering e di attacco mirato, produce un numero enorme di violazioni che vanno a buon fine, e l'impatto di un singolo attacco può essere devastante", ha commentato il Cto di Barracuda, **Fleming Shi.** Le statistiche della società di cybersicurezza mostrano anche che, mediamente, i tempi di rilevamento e risposta agli attacchi sono più rapidi nelle aziende che hanno investito per portare competenze digitali ai dipendenti. Oltre alle leggerezze e alla scarsa capacità di intuito delle persone, il problema sta però anche nelle scelte tecnologiche compiute a monte. I meccanismi di rilevamento basati su regole possono risultare inefficaci per lo

LA DEBOLEZZA **ITALIANA**

Dall'ultimo report del **Clusit** risulta che gli attacchi di impatto rilevante o grave andati a segno in Italia sono cresciuti del 69% nel 2022 rispetto all'anno precedente. Sul totale degli episodi registrati a livello mondiale, il 7,6% è stato diretto verso il nostro Paese. Sovrapponendo questo dato a un altro, frutto dei monitoraggi di **Fortinet,** emerge un fatto degno di nota. Sul totale dei 530 miliardi di minacce rilevate dai Fortiguard Labs l'anno scorso, su scala mondiale, la percentuale diretta all'Italia è inferiore all'1%. Si tratta, in questo caso, di rilevamenti sui tentativi di attacco, mentre la quota tricolore del 7,6% evidenziata da Clusit si riferisce alle minacce che hanno effettivamente provocato danni. "Questo significa che, molto più che in altre nazioni, in Italia i tentati attacchi riescono ad andare a segno", ha sottolineato **Massimo Palermo,** country manager di Fortinet. Molti degli attacchi andati a bersaglio hanno sfruttato le leggerezze, le ingenuità e talvolta l'ignoranza delle persone in fatto di sicurezza informatica o, come si suol dire oggi, di regole di "igiene digitale". L'ultima edizione del "Global Ransomware Report" di Fortinet, realizzata su 569 leader di sicurezza informatica di aziende di 31 Paesi (inclusa l'Italia), ha confermato il **ransomware** come minaccia globale endemica: il 50% delle organizzazioni è stato colpito almeno una volta nel corso del 2022, e quasi una su quattro è stata presa di mira ripetutamente (due o più volte). Il riscatto è stato pagato in circa tre casi su quattro.

spear phishing, mentre la nuova frontiera tecnologica sono le soluzioni basate su intelligenza artificiale e analisi contestuale.

L'AI al servizio degli attacchi

E c'è anche lei, l'intelligenza artificiale, tra le ragioni del successo dei "cattivi" e dell'insuccesso delle procedure di sicurezza. "Da un lato, l'AI viene usata per il data mining, per individuare le minacce in tempo reale", ha osservato **Massimo Palermo,** country manager di **Fortinet,** in occasione di un recente incontro con la stampa. "Ma vale anche il contrario: è sempre più al servizio del cybercrimine. Con l'AI potenzialmente molta più gente può creare codice malevolo, per esempio, oppure essa può servire per raffinare le attività di phishing".

Un'altra società di sicurezza informatica, l'israeliana **Cynet,** recentemente ha osservato una tendenza in atto: ChatGPT-4 (la versione più evoluta del software di OpenAI) e altri modelli Generative Pre-trained Transformer stanno aiutando i criminali


Massimo Palermo

informatici a creare attacchi più sofisticati ed efficaci, con email linguisticamente accurate e dunque convincenti. In passato gli attacchi di phishing complessi venivano creati da sviluppatori, da persone con competenze tecniche elevate, e condotti materialmente da altri attori malevoli, cioè gli ideatori della truffa. Adesso invece, grazie all'AI generativa, l'ideatore della truffa può anche materialmente confezionare e scagliare l'attacco. Cynet sottolinea che il *go-to-market* del cybercrime non cambia, ma la novità è che con i modelli linguistici generativi si possono creare attacchi molto sofisticati e su larga scala in modo relativamente facile.

Tra crimine industrializzato e vecchie vulnerabilità

Oltre a sfruttare il fattore umano e l'efficacia dell'intelligenza artificiale, oggi il cybercrimine può contare su una struttura organizzativa sempre più articolata, solida e quasi "industriale". "Oggi", ha fatto notare, ancora, Massimo Palermo di Fortinet, "non solo la superficie d'attacco aumenta ma si assiste a una industrializzazione del cybercrimine, che ha cambiato volto. Molti mettono le proprie competenze in vendita sul Dark Web e questo ha democratizzato la possibilità di sferrare attacchi, ha abbassato l'asticella". Fortinet prevede che quest'anno il fenomeno del cybercrimine "as a Service" continuerà a svilupparsi, ma questa non sarà l'unica fonte di preoccupazione. C'è anche l'annoso problema delle vecchie vulnerabilità non sanate da patch (il caso di Log4Shell docet), mentre nel frattempo si affermano modalità di attacco sempre più sempre più sofisticate, come il *drive by download* (che può scatenare l'infezione anche se l'utente non clicca su alcun file malevolo, ma semplicemente visita un determinato sito Web e visualizza un banner). Per quanto riguarda le vulnerabilità, la mancata installazione degli aggiornamenti non è necessariamente una questione di negligenza: nelle aziende più grandi la gestione delle patch può essere complessa e l'eterogeneità degli ambienti IT può creare dei "punti ciechi" in cui possono nascondersi falle.

CYBERSECURITY

QUATTRO **FALSI MITI** DA SFATARE

Non sempre una maggiore quantità di dati o un maggior numero di soluzioni di protezione messe in campo equivalgono a un potenziamento della capacità di difesa. "Molti Ciso sono bruciati dallo stress", ha commentato **Henrique Teixeira,** senior director analyst di **Gartner,** "e sentono di avere scarso controllo su ciò che crea stress o sull'equilibrio tra lavoro e vita privata. I leader di cybersicurezza e i loro team ci mettono il massimo impegno, ma questo non produce il massimo impatto". Nella cybersicurezza esistono alcuni falsi miti da sfatare, come illustrato da Gartner nel corso di un summit tenutosi in Maryland. La logica di fondo è una che i Ciso dovrebbero agire pensando a massimizzare gli effetti dei loro investimenti, anziché esagerare nell'impegno e negli investimenti senza però riuscire a ottenere i risultati sperati. Per dirla nelle parole di Gartner e con una metafora strappata all'ambito farmacologico, bisogna ragionare in termini di "dose minima efficace". "Una mentalità da dose minima efficace è un approccio consapevole e basato sul Roi per portare la cybersicurezza nel futuro", ha detto **Leigh McMullen,** distinguished vice president analyst di Gartner. "L'idea di un minimo potrebbe sembrare strana ma si riferisce agli input, non ai risultati. Questo approccio permetterà ai ruoli di cybersicurezza di andare oltre alla semplice difesa della fortezza per sbloccare il loro vero potenziale nel creare valore tangibile". Vediamo insieme i quattro falsi miti da sfatare.

- **Argomentazioni basate su molti dati**
  Comunemente si crede che, per convincere i dirigenti aziendali a supportare iniziative di cybersicurezza, il miglior modo sia presentare elaborate analisi di dati, per esempio calcoli sulla probabilità che un certo evento si verifichi. In realtà non è conveniente quantificare il rischio in questo modo. A detta di Gartner, solo un Ciso su tre ha successo quando si propone al management aziendale con argomentazioni basate sulla quantificazione del rischio. Meglio, invece, adottare metriche basate sui risultati ottenibili a fronte di certi investimenti.

- **Inseguire le ultime tecnologie**
  La spesa mondiale in prodotti e servizi per la cybersicurezza e la gestione del rischio raggiungerà i 189,8 miliardi di dollari quest'anno, con una crescita del 12,7% rispetto al 2022. Nonostante l'aumento della spesa, i leader della sicurezza informatica

Immagine di Freepik

Gli errori del backup

Da qualche anno è emersa una nuova tendenza negli attacchi informatici diretti al furto o al blocco dei dati, ransomware inclusi: viene preso di mira anche il backup. Considerarlo come uno scrigno inespugnabile è un errore. Sulle 1.200 aziende di 14 nazionalità analizzate nel "Ransomware Trends Report 2023" di **Veeam,** l'85% è stata colpita da almeno un'infezione crittografica nei dodici mesi precedenti all'indagine, ma quel che più colpisce è che l'93% degli attacchi si è rivolto verso le copie di backup. La maggior parte delle aziende ha pagato il riscatto, e in un caso su quattro non ha comunque potuto recuperare i propri dati. "Indubbiamente c'è stato un cambio di strategia", ha commentato **Alessio Di Benedetto,** technical sales director Southern Emea di Veeam. "In passato si ▸

non pensano che la propria azienda sia meglio protetta. Prevale, a volte, una "mentalità dell'acquisto", alla rincorsa delle ultime novità. Anche in questo caso, secondo Gartner, dovrebbe prevalere il principio della "dotazione di strumenti minima efficace" per rilevare, bloccare e mitigare le minacce. Oltre ai risparmi, c'è il vantaggio di semplificare l'architettura di cybersicurezza aziendale, riducendo complessità e problemi di interoperabilità, ed evitando di sopraffare il personale con un numero eccessivo di strumenti.

- **Allargare il team di cybersicurezza**
  Come noto, la domanda di professionisti esperti di sicurezza informatica è in crescita tra le aziende, che spesso faticano a reperire sul mercato del lavoro le persone giuste. Ma anche qui c'è un luogo comune da sfatare. "La cybersicurezza", ha spiegato McMullen, "è un enorme collo di bottiglia per la trasformazione digitale, in gran parte per via del mito che solo i professionisti della cybersicurezza possano svolgere un serio lavoro cyber". La giusta strategia? Democratizzare le competenze e l'esperienza in sicurezza informatica, anziché assumere nuovo personale. Con un approccio di "competenza efficace minima", dotando un maggior numero di dipendenti di "capacità di giudizio cyber", l'intera azienda si avvantaggia di maggiori livelli di sicurezza, per esempio perché è meno probabile che vengano installate e usate tecnologie rischiose. Parallelamente, per i Ciso e i loro team si riduce il carico di lavoro.

- **Esagerare con regole e controlli**
  Un recente sondaggio di Gartner ha evidenziato che il 69% dei dipendenti nel corso dell'anno ha aggirato le regole di cybersicurezza dell'azienda (per esempio usando applicazioni o servizi non ammessi); il 74% lo farebbe se questo servisse a raggiungere un obiettivo di lavoro. Gli addetti alla cybersicurezza conoscono il problema del mancato rispetto delle policy, e la reazione tipica è di aggiungere nuove regole e restrizioni. Ma non è la strada giusta: meglio anche in questo caso imporre le regole minime efficaci per bilanciare sicurezza ed esigenze di prestazioni delle applicazioni e tecnologie. La user experience dev'essere sempre presa in considerazione. Molte aziende stanno già andando in questa direzione, almeno quelle più strutturate. Gartner prevede che entro il 2027 nel 50% delle grandi imprese i Ciso avranno adottato pratiche di cybersicurezza umano-centriche per minimizzare i disagi di esperienza utente e massimizzare il rispetto delle regole.

mirava a cifrare i dati di produzione per bloccare l'operatività delle imprese, mentre ora si punta direttamente all'archivio di backup, per inibire l'utilizzo delle copie di ripartenza e colpire l'ultima linea di difesa".

Lo smart working è complice

A più di tre anni dalla corsa allo smart working, innescata dall'emergenza covid e dai lockdown, non mancano le evidenze di come l'ulteriore allargamento del "perimetro IT" delle aziende abbia accentuato il rischio di attacchi e fughe di dati. Accedere ad applicazioni e dati di lavoro tramite Pc e smartphone personali è diventato la norma, in abbinamento a reti Wi-Fi o mobili che non sono protette da firewall o da altri sistemi di difesa paragonabili a quelli di un'azienda. L'autenticazione multifattoriale (Multi-factor authentication, Mfa) è un valido aiuto contro gli accessi non autorizzati, ma a volte non è prevista nelle policy IT oppure è adottata in modo scorretto. Sembra incredibile ma, stando all'annuale classifica di **NordPas**, nel 2022 la password più usata al mondo è stata la parola "password" , mentre in Italia al primo posto c'è l'altrettanto poco fantasiosa "123456".

Un cloud frammentato

Parallelamente allo smart working, e alimentata anche da esso, è proseguita negli ultimi anni la migrazione in cloud. L'ultima indagine annuale di **Nutanix** (realizzata da Vanson Bourne a cavallo tra 2022 e 2023 su 1.450 decisori IT tra Americhe, Emea e Asia Pacifico) svela che il 60% delle aziende utilizza più di una infrastruttura IT, con diverse possibili combinazioni tra on-premise, cloud pubblico e privato, di uno o più fornitori. La frammentazione degli ambienti IT ha dei vantaggi di flessibilità e costi, ma comporta complessità gestionali e perdita di visibilità. Solo il 40% dei professionisti IT del campione ha detto di avere visibilità completa su dove risiedano i propri dati, e tra gli italiani la percentuale scende al 35%.

In aggiunta a tutto ciò ci sono gli errori di configurazione delle risorse cloud, praticamente ubiqui. Uno studio di **Zscaler** ("Security di Zscaler Threatlabz", basato sulle statistiche della piattaforma del vendor) svela che il 98,6% delle aziende utilizza ambienti IT in cloud contenenti errori di configurazione gravi, tali cioè da rappresentare un rischio critico per i dati e per la stabilità degli ambienti stessi.

Valentina Bernocco