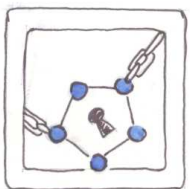

Lentezza, superficialità, mancanza di conoscenza e sottostima: i quattro ingredienti per favorire i cyberattacchi

Cyberattacchi alle aziende: come difendersi dalle nuove minacce?

Le aziende di oggi sono bersagli sempre più appetibili per i cybercriminali, che adottano tecniche sempre più sofisticate per rubare dati e denaro. In questo articolo, analizziamo le cinque principali sfide per la sicurezza informatica aziendale secondo Philip Larbey, EMEA Lead del Verizon Threat Advisory Team, e offriamo consigli concreti su come difendersi validi

Gli elementi più preoccupanti che sono emersi dalla chiacchierata con Philip Larbey sono la lentezza che le aziende evidenziano quando devono proteggersi da vulnerabilità note, la scarsa importanza che viene data alla gestione dell'identità digitale dei propri utenti e la cattiva abitudine di non segmentare la rete interna. Purtroppo, per coprire tutti i punti necessari a rendere ragionevolmente sicura un'azienda servono molte competenze e personale, ma la quantità e qualità dei gruppi criminali impone che il tema venga affrontato in maniera seria, magari con l'aiuto di aziende esterne che possano fornire il supporto di cui abbiamo bisogno.

Quello del cybercrimine è un fenomeno che sembra inarrestabile. Le statistiche ci raccontano che ogni anno il numero degli attacchi andati a buon fine è in crescita, ma quello che rende il quadro preoccupante è l'opinione degli esperti: un plebiscito di voci che racconta come i malintenzionati di Internet diventino sempre più bravi e organizzati.

Verizone Business ha recentemente rilasciato un nuovo report in cui si delinea il solito, buio, scenario, ma stavolta invece di mostrare i dati abbiamo scelto di chiedere a Philip Larbey, EMEA Lead del Verizon Threat Advisory Team, di commentarli per noi, andando a cercare le motivazioni che stanno dietro a questa apparentemente impossibilità di bloccare gli attacchi informatici da parte delle aziende.

Primo: proteggere l'identità personale è più complesso di quanto non si pensi

Philip Larbey ha identificato per noi cinque punti focali e il primo è già una sentenza: "Negli ultimi cinque anni, le violazioni informatiche ottenute tramite l'utilizzo di credenziali rubate è cresciuto a dismisura. La gestione dell'identità digitale deve essere presa molto seriamente perché per le infrastrutture di sicurezza è molto difficile capire se chi usa delle credenziali lecite è un criminale o il legittimo proprietario". Username e password, quindi, sono ancora le chiavi predilette dagli attaccanti per entrare nelle reti aziendali e i criminali stanno diventando sempre più bravi anche a eludere l'autenticazione a due o più fattori, quella tecnologia che richiede un'azione in aggiunta all'inserimento della password. Che sia un codice via sms, un clic sullo schermo dello smartphone o un numero generato da una chiavetta, i criminali inventano sistemi sempre più efficaci per intercettarli o farseli consegnare. "Il numero di attacchi in cui i criminali riescono ad aggirare l'autenticazione a più fattori" – specifica Larbey – "è molto più alto quando il codice o il pulsante da premere si trova sullo stesso dispositivo usato per l'autenticazione." Questo significa che se dobbiamo collegarci a un sito "sensibile" come quello aziendale da pc è importante usare un dispositivo diverso per ricevere e inserire il codice di conferma: se si accede da PC è bene usare una app o chiedere un sms, se si accede da smartphone è meglio usare un sistema di verifica che funziona sul pc o su di una chiavetta esterna.

Secondo: gli attacchi condotti da gruppi molto organizzati sono in aumento e difficili da fermare

Il secondo tipo di attacco che sembra inarrestabile è quello della violazione informatica che implica più tecniche. Si tratta di attacchi condotti da personale molto qualificato che attraversa diversi stadi prima di arrivare a conclusione. Spesso partono con il furto di credenziali con le quali accedono a un computer dell'azienda bersaglio su cui scaricano un malware. Tramite questo programma si va a caccia di altri computer che è possibile compromettere fino a ottenere una mappa completa delle risorse aziendali e una lista di bersagli da colpire. "Questo tipo di attacco" – dice Larbey – "è quello solitamente che fa più male." E il motivo è evidente: quando i criminali hanno una mappa completa alle risorse e libero accesso alle stesse, possono scegliere cosa rubare, cosa codificare e cosa lasciare com'è per mettere in ginocchio il bersaglio e costringerlo a pagare un riscatto o, peggio, a chiudere.

Terzo: Le vulnerabilità accadono, ma devono essere chiuse in tempi brevi

Il terzo pericolo identificato dal nostro esperto è quello dello sfruttamento delle vulnerabilità nei software. Succede abbastanza spesso di trovare delle vulnerabilità, cioè degli errori che possono essere sfruttati dai criminali, nei programmi che si usano in azienda. E le aziende che usano più programmi per trattare dati sensibili o di importanza strategica sono più esposte di altri agli attacchi. "Di solito," - dice Larbey - "le aziende nei settori bancari, finanziari e medici sono le più esposte da questo punto di vista" - e la scarsa attenzione da parte di buona parte dei potenziali bersagli fa gioco ai criminali. Secondo il report di Verizon, infatti, servono solo cinque giorni ai pirati per studiare e mettere a frutto una vulnerabilità quando viene resa nota, ma metà delle aziende impiega fino a 55 giorni per eliminare questa debolezza dai propri computer e, addirittura, a distanza di un anno risulta che il 10% delle aziende ancora non ha provveduto a sistemare la falla. Questo permette agli attaccanti di avere sconfinati margini di azione per grandi periodi di tempo. Aggiornare i programmi usati in azienda deve essere una priorità per evitare di subire attacchi potenzialmente devastanti.

Quarto: procedure e formazione sono alla base della sicurezza informatica

Al quarto posto di questo elenco di situazioni propizie ai cybercriminali, Philip Larbey piazza l'invio di informazioni alle persone sbagliate. Questa evenienza copre un ventaglio molto ampio di possibilità che va dall'inviare le proprie credenziali ai pirati che sfruttano una campagna di phishing fino a rendere disponibili via e-mail o altri mezzi informazioni che dovrebbero restare riservate, passando per configurazioni errate di servizi informatici che permettono l'accesso non autorizzato a dati condivisi con colleghi, fornitori e clienti. Il report indica che ben due terzi degli attacchi andati a segno nello scorso anno hanno registrato a un certo punto proprio un invio di dati a persone non autorizzate che è poi risultato determinante per il successo della violazione. La soluzione è molto complessa perché passa per lo più attraverso la definizione di pratiche e procedure molto ben definite e dall'addestramento del personale.

Quinto: Bisogna complicare la vita dei criminali quando vanno a caccia dei nostri dati

Infine, il quinto punto è quello della mancata segmentazione della rete interna e dell'esagerato potere che viene troppo spesso lasciato a qualsiasi utente dell'azienda. Quando un criminale attacca un'azienda, spesso sfruttando delle

credenziali che ha rubato o più semplicemente comprato sul dark web, va a caccia delle informazioni più preziose e se non ci sono cancelli informatici che gli impediscono di saltare da un server all'altro, ha gioco facile nel trovarle. Inoltre, se i permessi concessi a qualsiasi utente sono molto elevati, i criminali non hanno bisogno di compiere azioni che lasciano molte tracce come quella di cercare di elevare i privilegi a loro disposizione per saltare su computer inizialmente inaccessibili, rendendo molto difficile scovarli. Eppure segmentare una rete e assegnare i privilegi di rete agli utenti sono operazioni relativamente semplici da effettuare, anche se in ambienti molto grandi può portar via molto tempo. Bisogna trovare il tempo per farlo, perché complicare la vita agli attaccanti fa la differenza tra un attacco andato a buon fine e uno che viene scoperto in tempo.

In conclusione: non è una battaglia persa, ma sicuramente molto dura

Gli elementi più preoccupanti che sono emersi dalla chiacchierata con Philip Larbey sono la lentezza che le aziende evidenziano quando devono proteggersi da vulnerabilità note, la scarsa importanza che viene data alla gestione dell'identità digitale dei propri utenti e la cattiva abitudine di non segmentare la rete interna. Purtroppo, per coprire tutti i punti necessari a rendere ragionevolmente sicura un'azienda servono molte competenze e personale, ma la quantità e qualità dei gruppi criminali impone che il tema venga affrontato in maniera seria, magari con l'aiuto di aziende esterne che possano fornire il supporto di cui abbiamo bisogno.

Fonte: di Giancarlo Calzetta (Il Sole 24 Ore)