Quando i rischi più gravi provengono dall’interno

Mag 28, 2020 Marco Schiaffino Approfondimenti, In evidenza, Scenario, Tecnologia 0

Le minacce non arrivano solo dall’esterno. Spesso gli incidenti informatici sono provocati da errori e da un’errata gestione a livello IT.

Gli esperti di cyber security, quando parlano di prevenzione, hanno la buona abitudine di guardare come prima cosa all’interno del perimetro. Il motivo? Nella maggior parte dei casi i veri rischi per la sicurezza si trovano proprio lì.

“Abbiamo l’abitudine a concentrarci in maniera ossessiva sui potenziali attacchi esterni” conferma **Massimo Carlotti di CyberArk**, società specializzata in *Privileged Access Management*. “La prima linea di difesa, però, deve essere schierata all’interno dei sistemi”.

D’altra parte l’esperienza (e la cronaca) dimostrano che una buona percentuale dei data breach non avvengono a causa di malware o di attacchi mirati da parte di hacker, ma da semplici errori o configurazioni errate che portano all’esposizione di dati sensibili.

Il caso ormai frequentissimo di implementazione di database e servizi privi di un’adeguata protezione è solo l’esempio più eclatante di un fenomeno che non accenna a diminuire.

Anche quando si parla di attacchi informatici a opera di cyber criminali, però, è evidente come una buona parte di questi sfrutti, in un modo o nell’altro, elementi di debolezza che provengono dall’interno.

“Sia quando si parla di incidenti provocati da errori umani, sia quando si tratta di attacchi informatici, il vero tema è quello della gestione dei privilegi” spiega Carlotti. “**In pratica il problema è sempre lo stesso: abbiamo delineato in maniera corretta il campo di azione concesso all’utente che ha provocato il danno o che ha subito l’attacco?**”

Quale che sia lo scenario, la logica è chiara: una limitazione dei privilegi, basata su rigorose policy, consente di ridurre il danno in maniera considerevole. Questo vale sia per l’errore umano, che verrà “contenuto” entro limiti che ne consentono la correzione, sia per gli attacchi veri e propri.

Spesso, infatti, gli attacchi dei pirati informatici prendono di mira utenti che, almeno teoricamente, non dovrebbero avere accesso a dati “interessanti”. In assenza di una segmentazione della rete e di una compartimentazione degli accessi basata sulle competenze, però, i cyber criminali trovano campo aperto anche quando sono riusciti a compromettere un bersaglio di basso profilo.

La soluzione, prosegue Carlotti, è quella di adottare la

filosofia **least privilege**, il principio per cui ogni utente dovrebbe avere accesso solo e soltanto alle risorse e agli strumenti di cui ha effettivamente bisogno. Un'impostazione che, secondo l'esperto di CyberArk, non viene sempre adottata.

"Il periodo che stiamo attraversando (legato all'emergenza **Covid-19** – ndr) vede per esempio un aumento esponenziale del lavoro da remoto" prosegue Carlotti. "Molte aziende hanno dovuto implementare servizi a distanza in tempi estremamente stretti, derogando alle policy di sicurezza che adottavano normalmente. Il risultato è un aumento incredibile della superficie d'attacco per i pirati e una maggiore incidenza di semplici errori".

L'implementazione di un sistema di controllo dei privilegi, oltre che dalla creazione di policy adeguate, passa necessariamente per una soluzione tecnica. La sfida, però, non è solo quella di "arginare" i possibili errori (e anche le attività dolose) ma di centrare il risultato senza introdurre ulteriori elementi di complessità.

L'introduzione di controlli e procedure di autenticazione,

infatti, rischiano di rendere le procedure complesse e il rischio, in questo caso, è che gli utenti finiscano per ignorarle o di cercare delle "scorciatoie" che finiscono inesorabilmente per compromettere gli stessi sistemi di protezione.

"Le tecnologie dovrebbero rendere le cose meno complesse" spiega Carlotti. "Quello che facciamo come CyberArk è di semplificare l'esperienza utente senza abbassare il livello di sicurezza. In caso contrario, qualsiasi precauzione rischia di rivelarsi inefficace".

Condividi l'articolo

Il malware Valak si evolve: ora punta alle grandi aziende

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/05/28/quando-i-rischi-piu-gravi-provengono-dallinterno/?utm_source=rss&utm_medium=rss&utm_campaign=quando-i-rischi-piu-gravi-provengono-dallinterno