La sicurezza (al 100%) non esiste

Ott 07, 2019 F-Secure F-Secure Partner Space, RSS 1

Le moderne tecniche di attacco sfruttano le caratteristiche dei nuovi servizi e sono sempre più difficili da individuare prima che avvenga la violazione.

C'era una volta il concetto di protezione perimetrale, cioè l'idea che la cyber-security potesse rappresentare un "argine" agli attacchi dei pirati informatici nei confronti dell'azienda allo stesso modo in cui un muro di cinta può proteggere un castello dagli attacchi dei nemici.

Quei tempi, però, sono finiti. **Nel panorama di oggi, l'idea di poter controllare tutti i possibili accessi all'infrastruttura e intercettare qualsiasi attacco è relegata al mondo dei sogni**. In una realtà in cui comunichiamo attraverso decine di piattaforme diverse, deleghiamo funzioni e servizi alla cloud e viviamo connessi 24 ore su 24, pensare di "chiudere" gli spazi per eventuali attacchi è pura fantasia.

Per capirlo, basta fare un piccolo sforzo di fantasia. Proviamo a immaginare di ricevere una "soffiata" in cui ci viene detto che siamo finiti nel mirino di un hacker che ha deciso di attaccarci. **Non sappiamo quando, non sappiamo come, sappiamo solo che l'attacco arriverà**.

La nostra vita si trasformerebbe immediatamente in un inferno. Cominceremmo a vedere una minaccia nascosta in ogni email, ogni link e ogni messaggio che riceviamo. Esiteremmo prima di collegarci a qualsiasi sito Internet sconosciuto e ci troveremmo a pensare due volte prima di accettare qualsiasi

richiesta di contatto su Linkedin.

Nel giro di qualche giorno, ci renderemmo conto che l'unico modo per annullare qualsiasi rischio di finire vittima di un attacco sarebbe quello di staccare il cavo di rete e rinunciare per sempre all'utilizzo di Internet.



Traslato in ambito aziendale, tutto questo significa una sola cosa: è impossibile lavorare normalmente senza esporsi alla possibilità di un attacco. **Il semplice fatto di svolgere le "normali" attività di ogni giorno espone l'infrastruttura ad attacchi di qualsiasi genere**.

Se un cyber-criminale decide di prendere di mira la nostra infrastruttura, ha tutte le possibilità di studiare il modo migliore per farlo. Di solito i professionisti specializzati negli attacchi alle aziende utilizzano come vettore di attacco la tecnica dello spear-phishing: email o messaggi confezionati su misura per attirare l'attenzione di uno specifico impiegato o dirigente dell'azienda.

In altri casi, i pirati cercano un punto debole

nell’infrastruttura (per esempio un dispositivo non aggiornato o una falla nel software di un server esposto su Internet) e sfruttano quell’opportunità per utilizzare la falla come testa di ponte per il loro attacco.

Insomma: dobbiamo rassegnarci all’idea che un’intrusione da parte di un pirata informatico non è solo possibile: dobbiamo considerarla molto probabile. **Il problema, quindi, non diventa tanto bloccare gli attacchi a livello di perimetro, quanto essere in grado di individuarli e contrastarli quando avvengono**.

In quest’ottica, i nostri sistemi di sicurezza non dovrebbero somigliare a un castello protetto da mura di cinta, ma a un campo di calcio sul quale abbiamo steso centinaia di fili trasparenti in cui un intruso finirebbe per inciampare, rilevando la sua presenza.

Condividi l’articolo

Security nella pratica: il caso MTV

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/07/la-sicurezza-al-100-non-esiste/