

Cybercrime, deepfake e fattore umano le principali minacce per le aziende



Il 2021 sarà per la sicurezza informatica un anno pieno di insidie. La pandemia ha determinato una drastica accelerazione delle iniziative digitali in tutti i settori di mercato in quanto le aziende hanno dovuto adottare rapidamente tecnologie a supporto della produttività e della continuità del business.

Sia che si trattasse di portare nuovi strumenti di collaborazione o di spostare infrastrutture e applicazioni critiche nel cloud, tutto è diventato più distribuito, aumentando notevolmente, di conseguenza, le opportunità per i potenziali aggressori.

Che impatto avrà la convergenza di queste forze ed eventi sulla sicurezza informatica nei prossimi 12 mesi? Eccone due

particolarmente importanti: deepfake e dipendenti.

I deepfake diventano una minaccia anche per le aziende

Qualcosa può essere troppo enfatizzato e rappresentare comunque una minaccia emergente? Questo è il caso dei deepfake – un termine che è simulatamente abusato e un esempio di come gli attaccanti continueranno a personalizzare i loro attacchi.

In sintesi, i deepfake sono video o immagini, sintetici o manipolati, in cui una persona viene sostituita con la somiglianza di qualcun altro. Da un punto di vista culturale, il concetto di deepfake ha dominato i notiziari come una potenziale minaccia che potrebbe influenzare l'opinione pubblica, danneggiare la reputazione e altro ancora. Spesso questi attacchi fanno notizia, ma finiscono per essere relativamente poco efficaci.

Tuttavia, man mano che la tendenza della catena di attacchi personalizzati continua, vedremo l'emergere di deepfake negli attacchi alle imprese – non per seminare necessariamente confusione o caos di massa, ma più per amplificare gli attacchi di ingegneria sociale.

Video e registrazioni di dirigenti sono spesso già disponibili per attività di marketing, social media e altro ancora. Gli attaccanti potrebbero inserire deepfake in tentativi di phishing (che si allontaneranno dalla posta elettronica per sfruttare altre piattaforme come le applicazioni di chat e collaborazione) per rendere le comunicazioni manipolate ancora più autentiche. Soprattutto al giorno d'oggi, dove sempre più organizzazioni si affidano al video come mezzo di comunicazione tra dirigenti e dipendenti, gli aggressori possono approfittare di questo livello di fiducia instillato.

Sono comuni, ad esempio, le e-mail di phishing che chiedono le password – ma cosa succederebbe se a quell’e-mail seguisse un messaggio urgente del CEO su WhatsApp? Gli attaccanti potrebbero anche utilizzare video manipolati di dirigenti sui social per invogliare clienti, dipendenti, partner e altro ancora a cliccare su link dannosi – creando nuove vie di attacco più ampie per gli attori dannosi.

I dipendenti

La pandemia ha creato un’enorme tensione sui dipendenti e sulle loro famiglie. L’incertezza economica e il passaggio al lavoro e alla scuola a distanza ha messo molti in un territorio inesplorato. Queste nuove sfide potrebbero probabilmente spingere un numero maggiore di dipendenti a prendere decisioni sbagliate quando si tratta di sicurezza informatica e creare una nuova ondata di insider malintenzionati.

Come abbiamo già osservato nel 2020, gli attaccanti offrono sempre più spesso ai dipendenti con accesso privilegiato incentivi finanziari allettanti per condividere o “accidentalmente” far trapelare le proprie credenziali. Inoltre, l’accesso privilegiato sul dark web è più popolare che mai, e alcune ricerche indicano che gli aggressori sono disposti a pagare per ottenere l’accesso privilegiato alle reti aziendali, alle VPN e alle workstation.

La potenziale ricompensa finanziaria, combinata con l’aumento dell’ansia economica, porterà alla nascita di nuove minacce che le organizzazioni faticeranno a fronteggiare.

<https://www.key4biz.it/cybercrime-deepfake-e-fattore-umano-le-principali-minacce-per-le-aziende/336238/>