Il fattore umano

proofpoint.

Cybersecurity, ransomware e frodi via email nell'anno che ha cambiato il mondo

Mentre la pandemia globale stravolgeva le routine lavorative e familiari, i criminali informatici coglievano la palla al balzo. E ora, nel 2021, questi criminali informatici spavaldi fanno leva sul loro vantaggio moltiplicando gli attacchi.

Per contrastare gli attacchi incentrati sulle persone è necessaria una protezione su misura, in grado di affrontare i tre aspetti fondamentali del rischio della cybersecurity...

Vulnerabilità

Quante probabilità ci sono che i tuoi utenti si lascino ingannare da un attacco informatico?

20%

degli utenti non ha superato le simulazioni di attacchi **basati sugli allegati**

Attacchi che includono un file pericoloso.

12%

degli utenti non ha superato le simulazioni di attacchi **basati sui link**

Attacchi che includono un URL non sicuro che reindirizza gli utenti verso malware e siti web pericolosi.

4%

degli utenti non ha superato le simulazioni di attacchi **basati sull'immissione dei dati**

Attacchi che conducono l'utente a una pagina di accesso falsificata al fine di sottrargli credenziali e dati personali.

Alcune delle tecniche di attacco più efficaci del 2020 sono state anche quelle più mirate, usate in campagne che a volte comprendevano solo una manciata di email.

Steganografia: occultamento di codice dannoso in immagini e altri tipi di file. Più di **1 persona su 3** colpita ha fatto clic su un'email dannosa che utilizza la steganografia

CAPTCHA: tecnica che utilizza testi visuali per distinguere le persone dalle macchine. Le percentuali di clic sono **50 volte** più elevate di quelle dell'anno precedente

Attacchi

Quali minacce prendono di mira i tuoi utenti?

La pandemia è stata l'esca più usata nel 2020. A un certo punto del 2020, la maggior parte dei criminali informatici ha sfruttato il tema del COVID.

Indipendentemente dall'esca, i metodi d'attacco variano...

Il phishing delle credenziali di accesso ha rappresentato quasi i **due terzi** dei messaggi dannosi.

Il **25% delle campagne d'attacco** nascondeva malware all'interno di file eseguibili compressi.

Il **10% delle email dannose correlate a questa campagna** ha cercato di distribuire il malware Emotet.

I trojan con accesso remoto sono stati coinvolti in quasi il **25% di tutte le campagne delle minacce tramite email**.

Oltre 48 milioni di messaggi contenevano malware che poteva essere utilizzato come punto di ingresso per attacchi ransomware.

Decuplicati

gli attacchi tramite macro di Excel 4.0

Quintuplicati

gli attacchi che sfruttano file protetti con password

18%

in più di attacchi di hijacking del thread di discussione

2019 vs 2020

Privilegi

Quali danni può causare un attacco?

Maggiori sono i privilegi elevati di cui gode l'account compromesso, tanto maggiore è l'accesso a dati sensibili e preziosi. Le conseguenze di un attacco informatico saranno quindi ancor più drammatiche.

Il telelavoro e il lavoro ibrido hanno incrementato il rischio di minacce interne, dovute ad azioni dannose o negligenti.

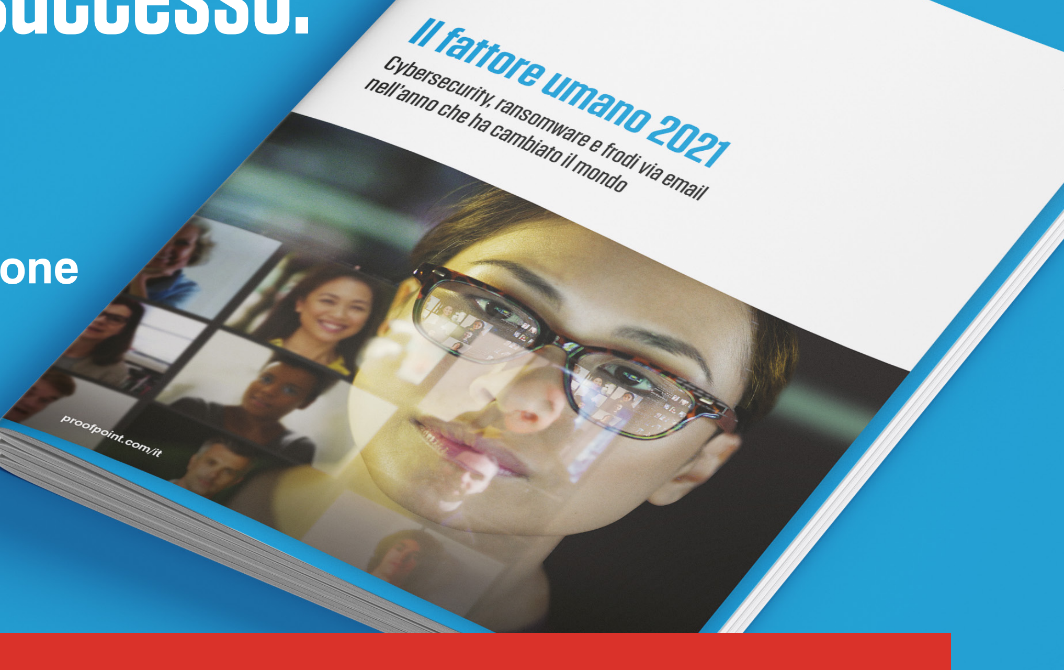
Principali allarmi relativi alla gestione delle minacce interne rivolte contro il top management:

- ⚠ Connessione di un drive USB non approvato per la copia
- ⚠ Esfiltrazione di un file monitorato verso il web tramite upload
- ⚠ Apertura di un file di testo che potrebbe contenere delle password
- ⚠ Download di file con un'estensione potenzialmente dannosa
- ⚠ Copia di un file o cartella di grandi dimensioni in momenti desueti
- ⚠ Esfiltrazione di file su un drive USB non approvato
- ⚠ Installazione di strumenti di hacking o spoofing
- ⚠ Accesso a servizi cloud di caricamento e condivisione

Risoluzione del problema "umano"

Gli attacchi informatici sono inevitabili. Ma la maggior parte di loro ha bisogno dell'intervento umano per avere successo.

Fornisci ai tuoi dipendenti i mezzi per proteggere la tua azienda attraverso una formazione di sensibilizzazione alla sicurezza informatica e controlli basati sui rischi. Per saperne di più...



SCARICA IL REPORT IL FATTORE UMANO 2021

Per maggiori informazioni, visita proofpoint.com/it.

proofpoint.

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.