

Riduzione del rischio con la sicurezza incentrata sulle persone

Esplora una strategia più efficace per restare un passo avanti al prossimo attacco informatico

Vantaggi principali

Acquisisci visibilità e controllo scoprendo:

- Come le minacce prendono di mira il tuo personale
- Come le persone lavorano in modalità ad alto rischio
- Come le persone accedono ai dati preziosi

Il panorama delle minacce di oggi è essenzialmente caratterizzato dal social engineering. Gli attacchi prendono sempre più di mira le persone, non la tecnologia o le infrastrutture, e lo spostamento verso il cloud sta intensificando tale tendenza. Proofpoint può consentirti di acquisire visibilità, ricavare informazioni utili e applicare controlli adattivi sulla base del maggiore rischio per la sicurezza informatica: le persone. E non solo delle persone che lavorano per te, ma anche dei dati a cui accedono e dei comportamenti che segnalano che hanno abboccato o abbotcheranno a un moderno attacco di social engineering.

Gli aggressori prendono di mira le persone

Oggi gli aggressori sono abili a utilizzare strumenti quali Google e LinkedIn per passare al setaccio Internet e lanciare campagne contro le organizzazioni servendosi di tattiche di attacco più sofisticate e mirando in grande. La maggior parte dei professionisti del settore IT e della sicurezza informatica opera con la rete o l'indirizzo IP al centro del mondo. Tuttavia, la trasformazione digitale in forza lavoro remota aggiunge più complessità, poiché gli utenti bypassano le reti aziendali per accedere ai dati della società - e gli approcci di sicurezza tradizionali non forniscono lo stesso livello di protezione. Così gli aggressori non vedono il mondo come se fosse uno schema di rete. Inoltre, l'adozione di app e piattaforme cloud, come Microsoft 365 e Google Workspace, mette in discussione l'approccio difensivo basato sulle reti. Le app cloud veicolano preziose informazioni aziendali attraverso Internet senza passare attraverso i firewall o altri controlli di rete. È pertanto difficile acquisire visibilità su tutti i tipi di minacce che interessano le persone e dare la precedenza ad allarmi e incidenti in base al rischio relativo per l'organizzazione.

Quantifica il rischio con il Proofpoint Attack Index

Un parametro che consente di quantificare il rischio incentrato sulle persone è il Proofpoint Attack Index. Proofpoint ha creato e implementato l'Attack Index per identificare le persone prese di mira e portare alla luce minacce interessanti facendole emergere dal rumore dell'attività quotidiana delle minacce. L'Attack Index è un punteggio composito ponderato di tutte le minacce che una persona riceve. È basato su quattro fattori chiave:

- **Volume degli attacchi.** Indica il numero vero e proprio delle minacce.
- **Tipo di attacco.** Riguarda il tipo di malware utilizzato. Questo punteggio considera il grado di pericolo rappresentato dalla minaccia e lo sforzo compiuto per sferrare l'attacco. Un RAT o stealer, ad esempio, otterrà un punteggio più alto rispetto a un tentativo di phishing delle credenziali generico focalizzato sui clienti.
- **Obiettivo di attacco.** Considera il grado di presa di mira coinvolto. La minaccia ha colpito un solo utente a livello globale? Era focalizzata su uno specifico utente, un'azienda, un settore o un'area geografica? Oppure era una campagna ad ampio spettro, sferrata contro mezzo mondo? La prima riceverà un punteggio maggiore della seconda.
- **Sofisticatezza degli autori.** Considera il livello di sofisticatezza dei criminali. Ad esempio, un malintenzionato con stato APT riceverà un punteggio più alto rispetto a un comune malintenzionato di bassa lega.

Con l'Attack Index puoi valutare e segnalare il rischio singolo e complessivo che colpisce le persone e assegnare quindi la priorità al metodo più efficace per risolvere le minacce.

Valutazione della superficie di attacco umana

Proofpoint ti aiuta a gestire il rischio per la sicurezza concentrandosi sulle minacce che prendono di mira e sfruttano le persone. Tutto ha inizio con l'identificazione dei VAP (Very Attacked People). Benché identificare i VAP sia un buon inizio, non è sufficiente per capire appieno il rischio delle persone. Poiché il rischio delle persone è costituito da diverse variabili, Proofpoint gode di una posizione strategica che gli consente di identificare il rischio tramite il nostro prodotto Nexus People Risk Explorer e fornire informazioni utili su:

- **Come le persone lavorano in modalità ad alto rischio.** Se, volontariamente o meno, sono note per avere fatto clic su collegamenti o allegati dannosi o per avere interagito con app vulnerabili.
- **Come le minacce prendono di mira il tuo personale.** Il tuo personale è stato vittima di attacchi altamente mirati, estremamente sofisticati e in grandi volumi?
- **Come le persone accedono ai dati preziosi.** Accedono o gestiscono sistemi o dati sensibili? Se è così, potrebbero correre un rischio maggiore di abuso, perdita o fuoriuscita dei dati tramite sistemi business-critical o app di terze parti.

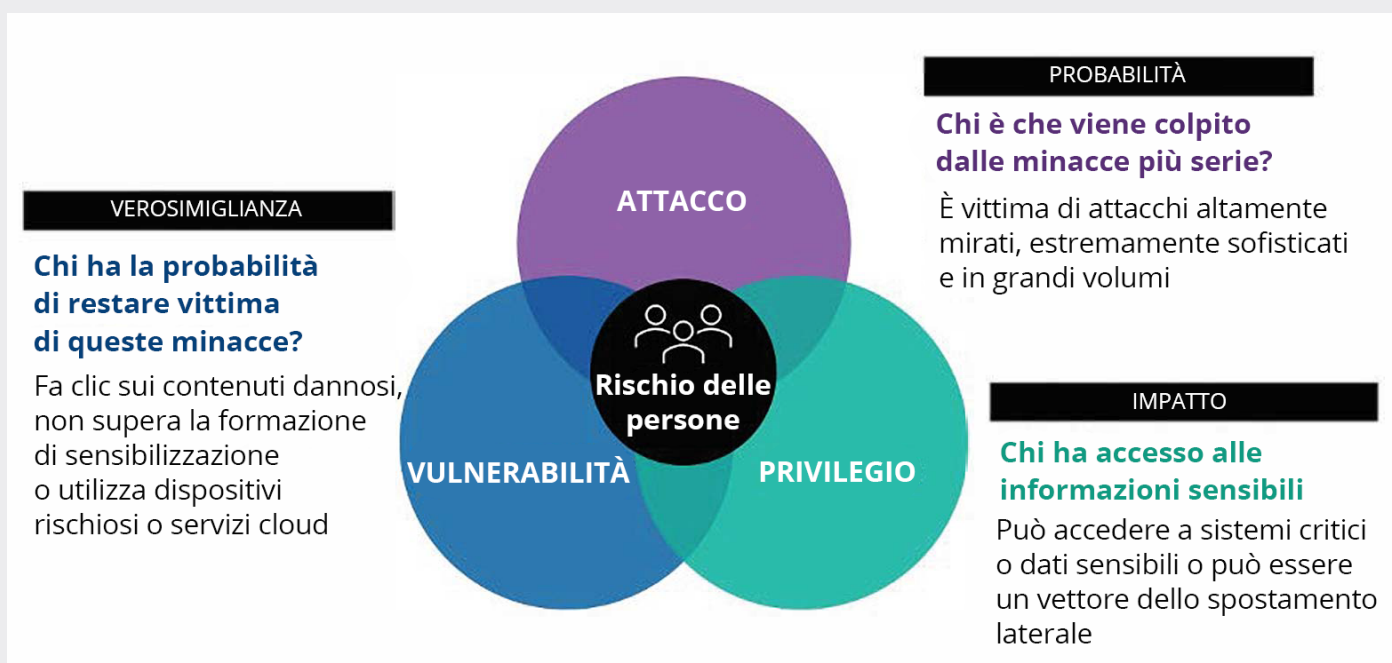


Figura 1: il diagramma di Venn mostra come Proofpoint visualizza le variabili che si intersecano per informare il rischio.

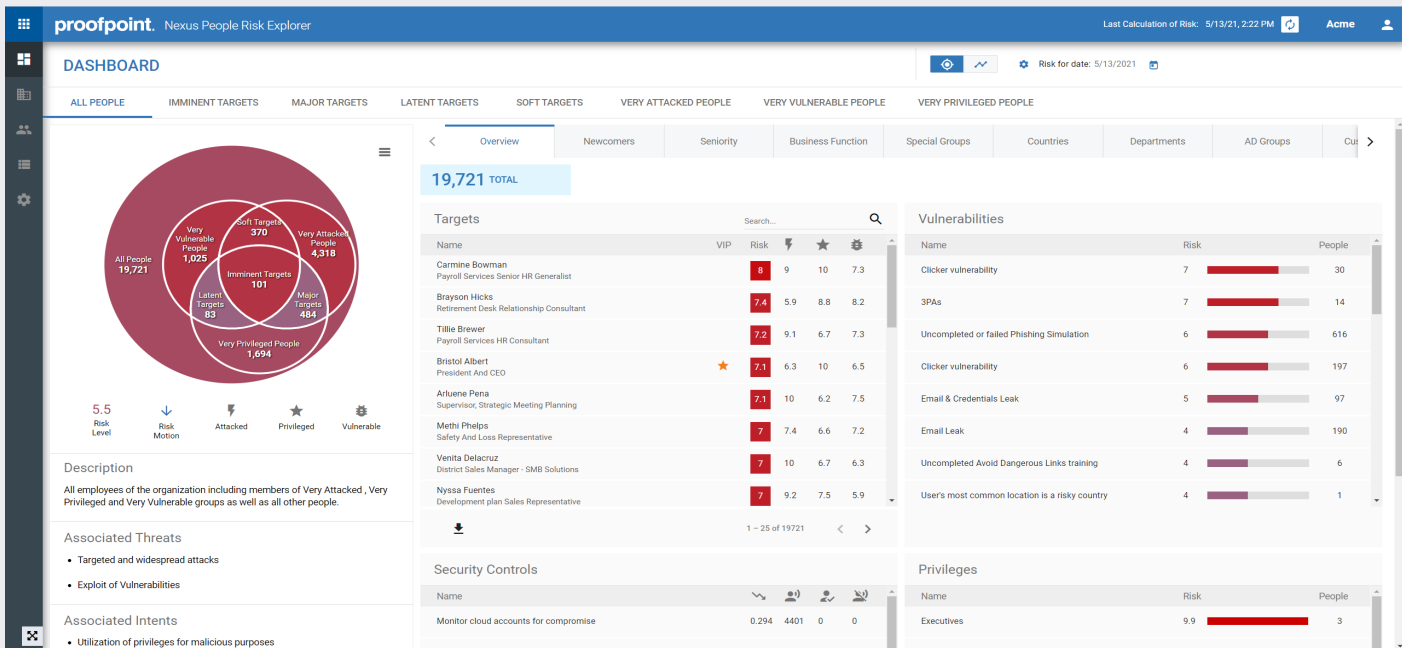


Figura 2: schermata iniziale della dashboard di Nexus People Risk Explorer che fornisce visibilità sul rischio delle persone.

Adozione di un approccio incentrato sulle persone

Proofpoint offre soluzioni che possono agevolare la tua organizzazione nel cammino destinato a sviluppare maggiori funzionalità di sicurezza incentrate sulle persone.

Proteggi il tuo principale vettore di minacce e ottieni visibilità sui VAP in azienda

Comincia risolvendo le minacce email su tutta la catena degli attacchi, dal rilevamento alla risposta. Ottieni visibilità su chi è stato attaccato, in che modo, se ha fatto clic su un messaggio di phishing o lo ha segnalato e se è stato violato.

Espandi la tua protezione incentrata sulle persone e inizia a tutelare gli account cloud

Protezione contro le minacce e la perdita di dati nei principali vettori di minacce incentrate sulle persone, comprese email esterna, account cloud, webmail personale e email interna. Addestra i tuoi utenti a essere la tua ultima linea di difesa. Attrezzali per riconoscere e segnalare gli attacchi di phishing e formali sulle best practice per mantenere le loro identità, credenziali e i loro dati al sicuro.

Crea un programma di sicurezza completo incentrato sulle persone

Amplia la protezione per coprire l'intera superficie umana di attacco, compreso l'ecosistema aziendale. Assicurati che le persone con cui fai affari non mettano a rischio la tua organizzazione. Inoltre, integra il tuo ecosistema di sicurezza per sfruttare al massimo gli investimenti esistenti. Proteggi i tuoi VAP grazie a controlli adattivi e per l'isolamento più integrati.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita [proofpoint.com/it](https://www.proofpoint.com/it).

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.

©Proofpoint, Inc. Proofpoint è un marchio commerciale di Proofpoint, Inc. negli Stati Uniti e negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.