Réduire les risques grâce à une approche de la sécurité centrée sur les personnes

Une stratégie plus efficace pour garder une longueur d'avance sur la prochaine cyberattaque

Principaux avantages

Améliorez la visibilité et le contrôle grâce à une bonne compréhension des éléments suivants :

- La façon dont vos collaborateurs sont ciblés par les menaces
- La dangerosité du comportement de vos collaborateurs
- La manière dont vos collaborateurs accèdent aux données de valeur

Le paysage des menaces actuel est profondément marqué par l'ingénierie sociale. Les attaques ciblent de plus en plus les personnes, plutôt que les technologies et l'infrastructure, et la migration vers le cloud ne fait qu'amplifier ce phénomène. Proofpoint vous aide à améliorer la visibilité, à obtenir des renseignements et à mettre en place des contrôles adaptatifs en fonction des ressources les plus à risque de votre entreprise : vos collaborateurs. Et pas seulement vos collaborateurs, mais aussi les données auxquelles ils ont accès et les comportements qui indiquent qu'ils sont tombés dans le piège d'une attaque d'ingénierie sociale moderne ou sont susceptibles de le faire.

Les personnes prises pour cible

De nos jours, les cybercriminels sont passés maîtres dans l'art d'utiliser des outils tels que Google et LinkedIn pour lancer des campagnes à l'encontre des entreprises. Leurs tactiques sont de plus en plus sophistiquées et ciblent un nombre toujours plus important de personnes. Pour la plupart des professionnels informatiques et de la cybersécurité, le monde tourne toujours autour de l'adresse IP ou du réseau. La transition vers le télétravail accroît la complexité, car les utilisateurs contournent les réseaux d'entreprise pour accéder aux données de l'entreprise, et les approches de sécurité traditionnelles n'offrent pas le même niveau de protection. Malheureusement, les cybercriminels ne voient pas le monde en termes de topologie réseau. L'adoption d'applications et de plates-formes cloud, telles que Microsoft 365 et Google Workspace (anciennement G Suite), remet en outre en question cette approche de défense axée sur le réseau. En effet, les applications cloud regorgent d'informations d'entreprise précieuses qui transitent sur Internet sans traverser de pare-feux ni subir d'autres formes de contrôles réseau. Il est donc difficile d'obtenir une visibilité sur tous les types de menaces qui ciblent les personnes et de hiérarchiser les alertes et les incidents en fonction de leur risque relatif pour l'entreprise.

Quantifiez le risque avec Proofpoint Attack Index

Proofpoint Attack Index vous permet de quantifier le risque lié aux utilisateurs à l'aide d'un indice unique. Proofpoint a créé et implémenté Proofpoint Attack Index pour identifier les personnes ciblées et distinguer les menaces présentant un intérêt particulier parmi toutes les activités malveillantes observées au quotidien. Cet indice consiste en un score composite pondéré de toutes les menaces reçues par une personne déterminée, sur la base de quatre facteurs clés :

- **Le volume d'attaques**. Indique le nombre de menaces.
- **Le type d'attaque**. Indique le type de malware utilisé. Cet indice prend en compte le degré de dangerosité de l'attaque et l'ampleur des efforts déployés pour la lancer. Un cheval de Troie d'accès à distance (RAT) ou un malware voleur d'informations obtiendra un score plus élevé qu'un phishing d'identifiants de connexion générique ciblant des consommateurs.
- **La cible de l'attaque**. Prend en compte le degré de ciblage. La menace a-t-elle touché un seul utilisateur ou avait-elle une portée mondiale ? Visait-elle un utilisateur, une entreprise, un secteur ou une zone géographique en particulier ? Ou s'agissait-il d'une campagne à large spectre, qui a touché la moitié de la planète ? Le premier type de campagne obtiendra une note plus élevée que le second.
- **La sophistication de l'attaquant.** Prend en compte le niveau de sophistication du cybercriminel. Par exemple, l'auteur d'une menace persistante avancée à la solde d'un État recevra une note plus élevée qu'un cybercriminel de petite envergure motivé par l'appât du gain.

Proofpoint Attack Index vous permet d'évaluer et de signaler le risque individuel et global pour l'utilisateur, puis d'identifier la solution la plus efficace à appliquer en priorité pour neutraliser les menaces.

Évaluez votre surface d'attaque humaine

Proofpoint peut vous aider à gérer vos risques de sécurité en mettant l'accent sur les attaques qui ciblent et cherchent à exploiter vos collaborateurs. Notre approche commence par l'identification de vos VAP (Very Attacked People, ou personnes très attaquées). Cette identification, bien que nécessaire, est toutefois insuffisante pour appréhender tous les risques liés à vos collaborateurs. En effet, ces risques dépendent de plusieurs variables, et Proofpoint est idéalement placé pour vous aider à les identifier grâce à Nexus People Risk Explorer et vous fournir des informations détaillées sur les aspects suivants :

- **La dangerosité du comportement de vos collaborateurs.** Ont-ils tendance, intentionnellement ou non, à cliquer sur des liens ou des pièces jointes malveillantes ou à interagir avec des applications vulnérables ?
- **La façon dont vos collaborateurs sont ciblés par les menaces.** Font-ils l'objet d'attaques très ciblées, extrêmement sophistiquées ou en nombre ?
- **La façon dont vos collaborateurs accèdent aux données de valeur.** Gèrent-ils ou accèdent-ils à des systèmes critiques ou des données sensibles ? Si tel est le cas, cela accroît le risque d'utilisation inappropriée, de perte ou de fuite de données via des systèmes critiques ou des applications tierces.

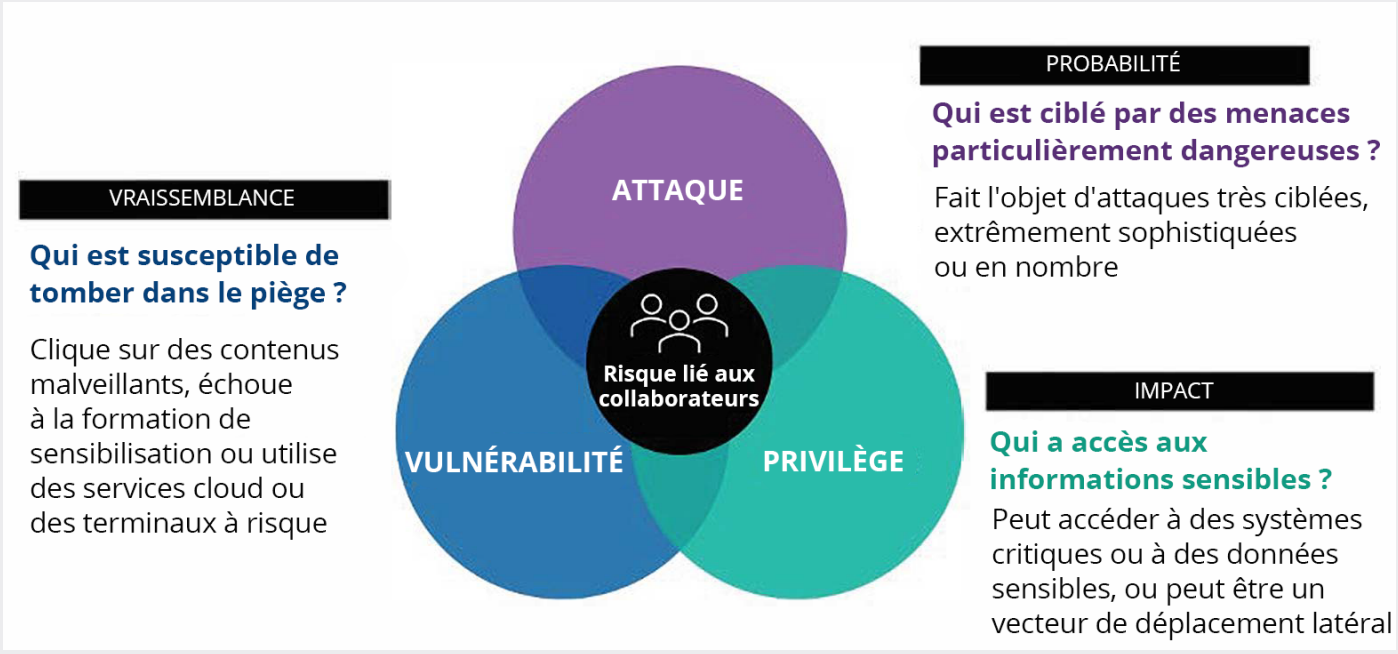

Figure 1. Diagramme de Venn montrant comment Proofpoint prend en compte les variables qui se combinent pour déterminer le risque

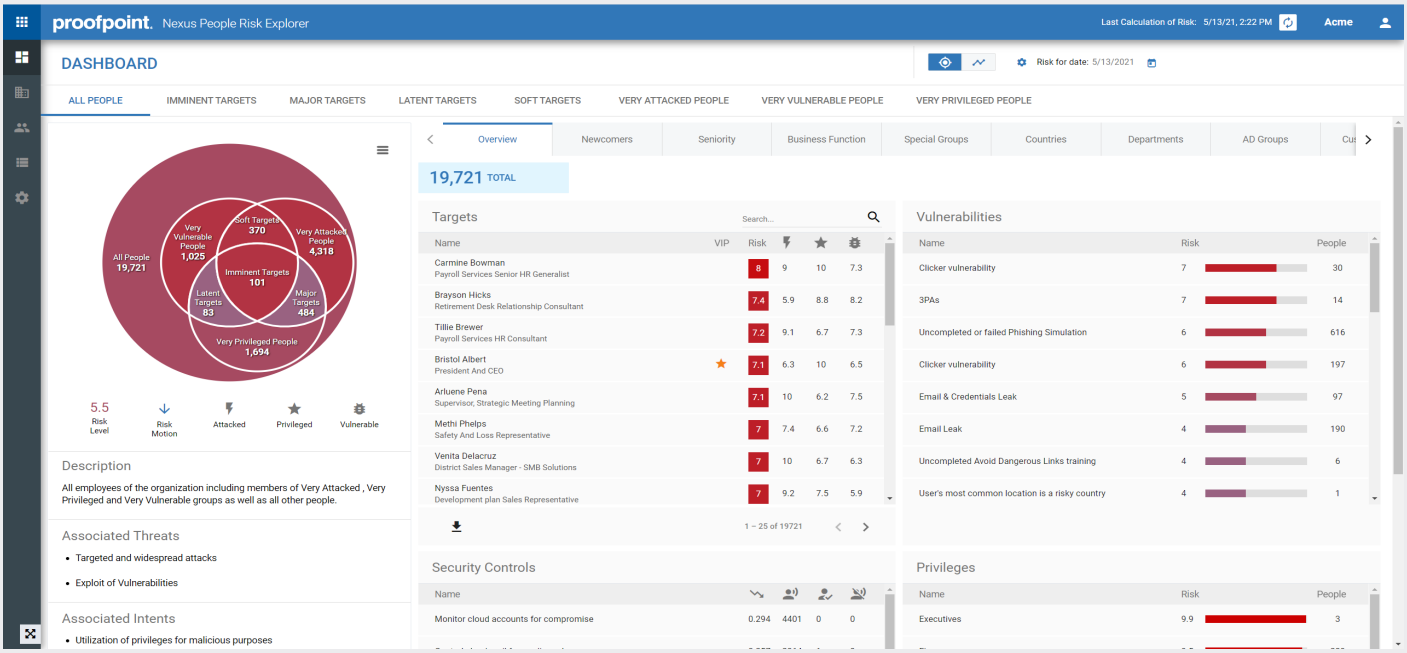

Figure 2. Écran d'accueil du tableau de bord de Nexus People Risk Explorer, qui offre une visibilité sur les risques qui pèsent sur vos collaborateurs

Adoption d'une approche de la sécurité centrée sur les personnes

Proofpoint propose des solutions qui peuvent aider votre entreprise à développer des capacités de protection optimisées axées sur les personnes.

Protégez votre principal vecteur de menaces et bénéficiez d'une visibilité sur vos VAP

Commencez par neutraliser les menaces véhiculées par la messagerie électronique à toutes les étapes de la chaîne d'attaque, de la détection à l'intervention. Bénéficiez d'une visibilité sur les cibles des attaques et les techniques d'attaque employées. Déterminez si les utilisateurs ciblés cliquent sur les emails de phishing ou les signalent, et s'ils ont été compromis.

Renforcez la protection centrée sur les personnes et sécurisez les comptes cloud

Bénéficiez d'une protection contre les menaces et les fuites de données sur tous les vecteurs de menaces axés sur les personnes, notamment les emails externes/internes, les comptes cloud et le webmail personnel. Transformez vos utilisateurs en dernière ligne de défense de votre entreprise. Apprenez-leur à identifier et signaler les attaques de phishing et informez-les sur les bonnes pratiques en matière de protection de l'identité, des identifiants de connexion et des données.

Développez un programme de sécurité complet axé sur les personnes

Assurez la protection de l'ensemble de votre surface d'attaque humaine, y compris l'écosystème de votre entreprise. Veillez à ce que vos partenaires commerciaux ne fassent pas courir un risque à votre entreprise. Pensez aussi à intégrer votre écosystème de sécurité afin de tirer le meilleur parti de vos investissements existants. Enfin, protégez vos VAP grâce à des contrôles adaptatifs plus intégrés permettant d'isoler les menaces.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.