Le facteur humain

proofpoint.

Cybersécurité, ransomwares et fraude par email en cette année qui a changé le monde

Tandis que la pandémie bouleversait les habitudes de travail et la vie familiale, les cybercriminels s'en donnaient à cœur joie. Et à présent, en 2021, ces cybercriminels enhardis poussent leur avantage en multipliant les attaques.

Les attaques centrées sur les personnes nécessitent une défense adaptée, capable de prendre en compte les trois facettes fondamentales du risque de cybersécurité...

Vulnérabilité

Quelle est la probabilité que vos utilisateurs se laissent piéger ?

20 %

des utilisateurs ont échoué aux simulations d'attaques basées sur des **pièces jointes**

Attaques recourant à un fichier malveillant

12 %

des utilisateurs ont échoué aux simulations d'attaques basées sur des **liens**

Attaques incluant une URL dangereuse qui redirige les utilisateurs vers des sites Web malveillants et des malwares

4 %

des utilisateurs ont échoué aux simulations d'attaques basées sur la **saisie de données**

Attaques dirigeant l'utilisateur vers une fausse page de connexion afin de dérober des identifiants de connexion et d'autres données personnelles

Certaines des techniques d'attaque les plus efficaces en 2020 étaient également extrêmement ciblées et ont été utilisées dans le cadre de campagnes parfois constituées de quelques emails seulement.

Stéganographie : dissimulation de code malveillant dans des images et autres types de fichiers. Plus de **1 personne ciblée sur 3** a cliqué sur un email malveillant utilisant la stéganographie

CAPTCHA : technique utilisant des tests visuels pour distinguer les personnes des machines. Les taux de clic sont **50 fois supérieurs** à ceux de l'année précédente

Attaques

Quelles menaces ciblent vos utilisateurs ?

En 2020, la pandémie a été le leurre le plus utilisé. La plupart des cybercriminels ont exploité le thème de la COVID à un moment ou un autre.

Quel que soit le leurre, ils ont utilisé des méthodes d'attaque variées...

Le phishing d'identifiants de connexion représente près de **deux tiers** des messages malveillants.

25 % des campagnes d'attaque dissimulaient des malwares dans des fichiers exécutables compressés.

10 % des emails malveillants liés à des campagnes ont tenté de distribuer le malware Emotet.

Les chevaux de Troie d'accès à distance ont été impliqués dans près de **25 % de toutes les campagnes d'attaque par email**.

Plus de 48 millions de messages contenaient un malware pouvant servir de point d'entrée à des attaques de ransomwares.

10x

plus d'attaques par macro Excel 4.0

5x

plus d'attaques exploitant des fichiers protégés par mot de passe

18 %

en plus d'attaques de piratage de fils de discussion

2019 vs 2020

Privilèges

Quels dommages peut causer une attaque ?

Plus le compte compromis possède des privilèges élevés, plus il a accès à des données sensibles et de valeur. Les conséquences d'une cyberattaque seront dès lors encore plus dramatiques.

Le télétravail et le travail hybride ont augmenté le risque de menaces internes, tant malveillantes qu'accidentelles.

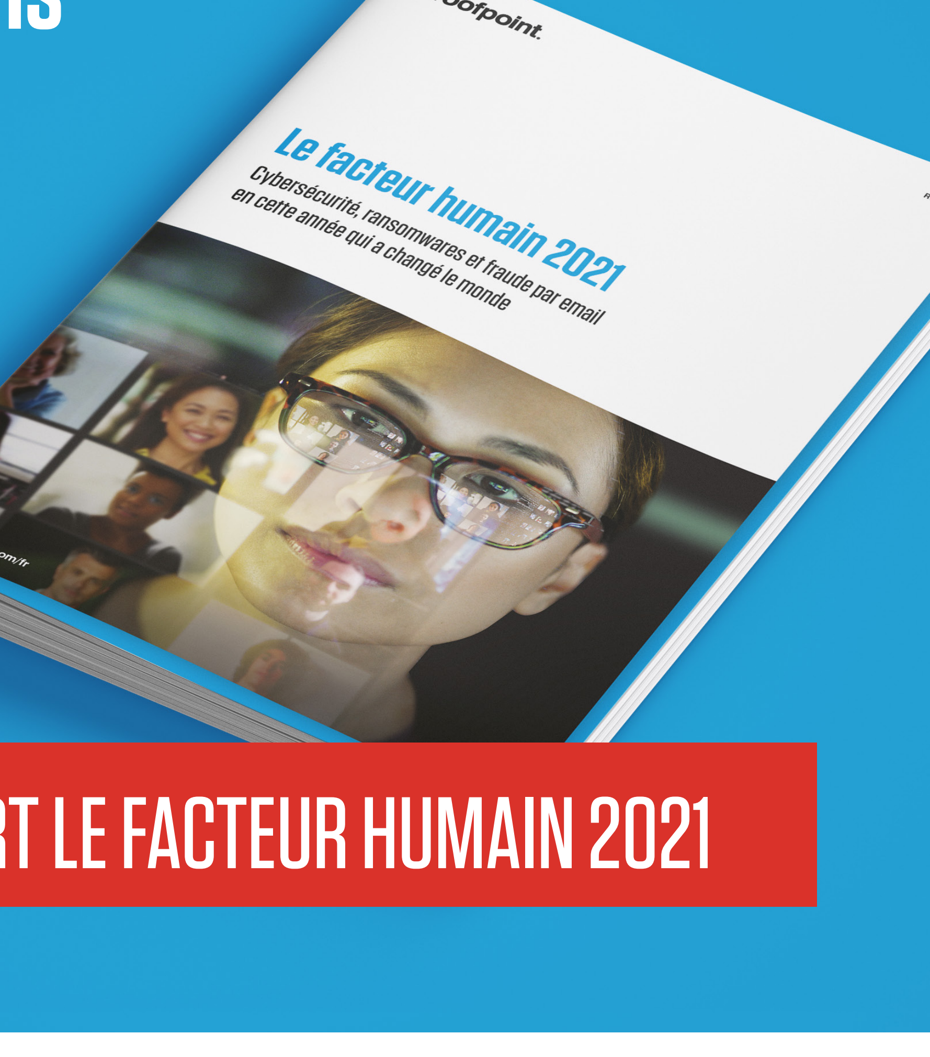
Principales alertes liées à la gestion des menaces internes ciblant l'équipe de direction :

- ⚠ Connexion d'une clé USB non approuvée à des fins de copie
- ⚠ Exfiltration d'un fichier surveillé vers le Web par chargement
- ⚠ Ouverture d'un fichier texte susceptible de contenir des mots de passe
- ⚠ Téléchargement de fichiers avec des extensions potentiellement malveillantes
- ⚠ Copie de dossiers ou fichiers volumineux à des heures inhabituelles
- ⚠ Exfiltration d'un fichier vers une clé USB non approuvée
- ⚠ Installation d'outils de piratage ou d'usurpation d'identité
- ⚠ Accès à des services cloud de chargement et de partage

Résolution du problème « humain »

Les cyberattaques sont inévitables. Mais la plupart d'entre elles ne peuvent aboutir sans intervention humaine.

Donnez à vos collaborateurs les moyens de protéger votre entreprise grâce à des formations de sensibilisation à la sécurité informatique et à des contrôles basés sur les risques.
Pour en savoir plus...



TÉLÉCHARGER LE RAPPORT LE FACTEUR HUMAIN 2021

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

proofpoint.

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**.