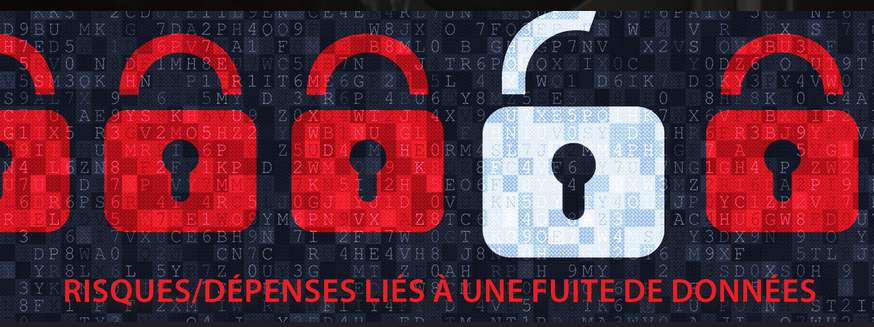
L'authentification multifacteur ROI

Quatre à six pour cent des gens utilisent systématiquement des mots de passe vulnérables ou partagés... Combien d'entre eux travaillent dans votre entreprise ?

Étant donné qu'il suffit d'un seul mot de passe volé pour usurper votre réseau, vous devez vous poser cette question : quelle est la probabilité qu'un ou plusieurs de vos employés aient une mauvaise gestion de leurs mots de passe ? Encore plus alarmant, les coûts liés à une fuite de données peuvent se chiffrer à plusieurs millions d'euros si l'on prend en compte les amendes directes, les frais d'investigation et de résolution ainsi que les dépenses indirectes engendrées par la perte de clients et de productivité des employés. Les statistiques suivantes peuvent vous aider à mesurer les risques et à les comparer au coût anticipé d'une solution de MFA.



RISQUES/DÉPENSES LIÉS À UNE FUITE DE DONNÉES

9 350
Nombre moyen de données volées

En moyenne, la quantité de **données volées** lors d'une fuite s'élève à **9 350 données**
2017 Ponemon State of SMB Cybersecurity Report

1,32 M $
Coût moyen des fuites de données

Le coût moyen d'une fuite de données = **141 $** par donnée compromise contenant des informations sensibles
2017 Ponemon Institute Cost of Data Breach Study

81 %
Pourcentage des fuites facilitées par des mots de passe vulnérables/volés

Il s'agit de la **tactique la plus souvent utilisée** par les pirates informatiques
Verizon, « 2017 Data Breach Investigations Report » (Rapport 2017 sur les atteintes à la sécurité des données)

3
Pourcentage d'utilisateurs dont le mot de passe est 123456

10 % des gens ont déjà utilisé au moins l'un des 25 mots de passe les pires , et près de 3 % des gens ont déjà utilisé le mot de passe : **123456**
Http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/

6
pourcentage d'utilisateurs qui utilisent le même mot de passe pour toutes leurs identifications en ligne

6 % des utilisateurs d'Internet aux États-Unis utilisent le **même mot de passe** pour tous leurs comptes en 2017
(https://www.statista.com/statistics/763091/us-use-of-same-online-passwords/)

1
Nombre de mots de passe perdus/volés nécessaires pour usurper un réseau sans authentification multifacteur (MFA)

Fichier contenant **1,4 milliards** de mots de passe piratés/ayant fait l'objet d'une fuite trouvés sur Dark Web « les pirates informatiques potentiels sont prêts à lancer des attaques "credential stuffing" »
(Forbes, 11 décembre 2017)

ESTIMATION DE L'INVESTISSEMENT DANS UNE SOLUTION DE MFA BASÉE DANS LE CLOUD

0 $
Infrastructure supplémentaire pour héberger Authentication Mgmt.

La gestion est possible avec l'informatique Cloud et **incluse dans le prix.** Certaines fonctionnalités nécessitent un logiciel sur la passerelle et les agents

0 $
Achats d'un jeton physique

L'application mobile totalement gratuite fait office d'authentificateur sur **smartphone** – aucun matériel supplémentaire n'est requis

2 700 $
Coût annuel estimé du service MFA pour 100 employés

Cela revient à **2,25 $/utilisateur/mois** – valeur à titre indicatif Veuillez prendre contact avec un partenaire WatchGuard afin de recevoir un devis AuthPoint spécifique

Minimal
Dépenses du personnel informatique

Le déploiement du token est **automatique,** les activités récurrentes du personnel informatique concernent donc principalement la maintenance et la surveillance

LES AVANTAGES DE LA MFA BASÉE DANS LE CLOUD COMPENSENT LARGEMENT LES FRAIS ENGAGÉS

Il vous suffit d'investir 2,50 $ par utilisateur et par mois, ou moins, pour réduire les chances d'une fuite de données en raison d'un mot de passe volé. La MFA basée dans le Cloud n'implique pas de dépenses pour une infrastructure supplémentaire, des tokens physiques, et des services de support et de maintenance de logiciels.

WatchGuard AuthPoint

La solution AuthPoint offre une authentification multifacteur (MFA) sur une plateforme Cloud simple d'utilisation. L'application mobile AuthPoint rend visible toute tentative d'identification, et comme il s'agit d'un service basé dans le Cloud, il n'est pas nécessaire de déployer du matériel. Elle peut être gérée de n'importe où et peut être intégrée à des applications tierces, dont les applications Cloud populaires, les services Web, les VPN et les réseaux. **Pour en savoir plus, veuillez consulter le site www.watchguard.com/authpoint**