ivanti

La fin des mots de passe, c’est maintenant

Zero Sign-On. C’est facile, quand votre périphérique mobile sécurise l’accès à l’entreprise.

Introduction

Les mots de passe. Le principal risque pour la sécurité et, tout le monde le sait, une corvée pour les utilisateurs finaux. Mais ce sera bientôt du passé. Ivanti élimine les mots de passe en utilisant votre périphérique mobile pour gérer votre identité et votre accès sécurisé à l'entreprise.

Nous simplifions également les opérations. En effet, votre système UEM (Ivanti Unified Endpoint Management) est au centre de cette avancée : il sert de base à notre approche de sécurité Zero Trust de bout en bout. Autrement dit, vous possédez déjà les éléments nécessaires pour faire de votre entreprise une zone sans mot de passe afin de fluidifier l'expérience et d'augmenter la productivité.

Cet ebook explique comment Ivanti Zero Sign-On (ZSO) met fin aux problèmes de mot de passe, et les avantages de cette avancée spectaculaire pour la sécurité si votre entreprise exploite son investissement Ivanti UEM.

Les problèmes de mot de passe

Aujourd'hui, les mots de passe représentent plus un danger pour la sécurité qu'une solution de protection. Ils causent des maux de tête au département IT et des soucis aux utilisateurs finaux. Les efforts pour améliorer la situation ont échoué, parce que les mots de passe ont été limités mais pas totalement éliminés de l'équation.

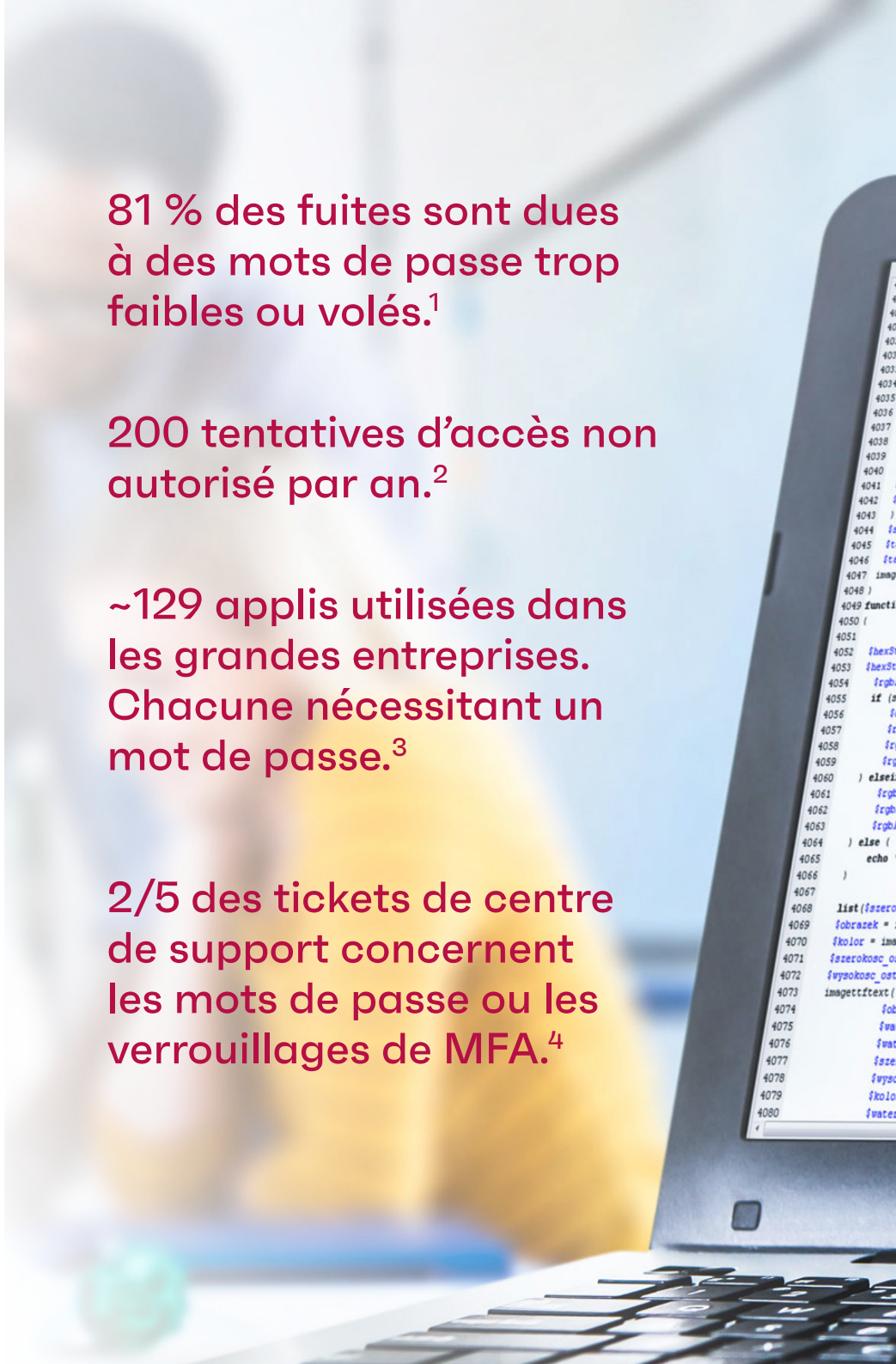
Problèmes de sécurité pour le département IT

En tant que cause numéro 1 de fuites de données, les mots de passe représentent un danger énorme pour les entreprises, et des problèmes de sécurité constants pour le département IT. Les mots de passe sont, potentiellement, un trésor pour les pirates car des programmes automatisés en force brute permettent, assez facilement, de deviner et de voler les références d'authentification, ou de craquer les mots de passe. Les pirates disposent de toute une gamme de tactiques d'ingénierie sociale pour voler les références d'authentification, notamment les attaques par hameçonnage, qui utilisent des e-mails ou des sites Web malveillants pour demander à l'utilisateur d'entrer son mot de passe. D'autres types d'exploitation, comme le « vishing » (hameçonnage vocal) et le « smishing » (hameçonnage par SMS), se multiplient également. Et pourtant, n'ayez pas peur. C'est l'occasion de changer.

Expérience utilisateur médiocre

C'est une vérité universelle : les utilisateurs détestent les mots de passe. Et cette frustration, toujours plus grande, les rend encore plus dangereux. Pour se renforcer, les mots de passe sont devenus plus complexes, si bien qu'il est encore plus difficile de les mémoriser. Les utilisateurs doivent désormais se souvenir de mots de passe qui comptent plus de huit caractères, avec des minuscules, des majuscules et des caractères spéciaux, et ne pas réutiliser le même pendant trois mois. Et la frustration augmente encore lorsqu'il s'agit de taper ces chaînes de caractères sur périphérique mobile. Le simple volume de mots de passe que les collaborateurs doivent mémoriser accentue le problème. Et cette frustration liée aux mots de passe se répète pour tous les services de Cloud et toutes les applications de l'entreprise. Résultat : des oublis, des réinitialisations, des verrouillages et un schéma nocif de non-productivité qui se répète.

ivanti



81 % des fuites sont dues à des mots de passe trop faibles ou volés.[1]

200 tentatives d'accès non autorisé par an.[2]

~129 applis utilisées dans les grandes entreprises. Chacune nécessitant un mot de passe.[3]

2/5 des tickets de centre de support concernent les mots de passe ou les verrouillages de MFA.[4]

Des contournements risqués

Plus les exigences de mot de passe sont strictes, plus les utilisateurs sont enclins à adopter un comportement risqué pour les gérer. Pour éviter de réinitialiser leur mot de passe ou d'être bloqué en cas de tentative infructueuse, les utilisateurs :

- Utilisent le même mot de passe pour plusieurs comptes.
- Collent des post-its avec leur mot de passe sur leurs périphériques.
- Stockent tous leurs mots de passe dans un fichier au nom évocateur.

Le SSO a seulement réduit les mots de passe, sans les éliminer. Le MFA n'a fait que compliquer la situation. C'est alors qu'Ivanti a résolu les problèmes de mot de passe.

SSO. C'est encore une identification de trop.

Le secteur a tenté de contrer la complexité des mots de passe en adoptant la connexion avec identification unique (SSO) et en renforçant la sécurité avec l'authentification multifacteur (MFA). Avec le SSO, l'utilisateur n'a besoin de mémoriser qu'un seul mot de passe pour accéder à toutes ses ressources d'entreprise. C'était une bonne nouvelle pour les utilisateurs… mais encore plus pour les pirates. Le SSO est encore plus favorable pour les pirates, puisqu'il leur suffit de craquer un seul mot de passe pour accéder à tous vos services d'entreprise. Le MFA a été conçu pour créer une protection multiniveau afin de rendre plus difficile l'accès non autorisé. L'accès n'est octroyé à l'utilisateur que s'il a présenté avec succès au moins deux éléments de référence indépendants : ce qu'il sait (mot de passe), ce qu'il possède (jeton de sécurité) et/ou qui il est (vérification biométrique). Donc, maintenant, en plus de gérer le mot de passe, les utilisateurs doivent entrer un code numérique spécifique pour accéder aux services d'entreprise. Comme les applications et systèmes concernés utilisent souvent des types de MFA différents, c'est encore plus pénible que d'avoir un mot de passe distinct pour chaque application.

45 % utilisent le même mot de passe pour les applis personnelles et professionnelles.[5]

L'attaque Sony était liée à un répertoire de fichiers nommé « Password » (Mot de passe).

ivanti

Zero Sign-On

On vous a dit qu'il ne fallait pas avoir peur, non ? L'histoire se finit bien. Il a fallu que le leader de la sécurité mobile trouve comment remplacer le mot de passe et créer une expérience de connexion sans identification (Zero Sign-On). En utilisant le périphérique mobile comme ID et outil d'accès sécurisé, il est possible d'obtenir une expérience d'authentification transparente où que l'on se trouve. Les utilisateurs accèdent en toute sécurité à tous les périphériques, applis ou ressource de l'entreprise, d'un seul regard ou du bout du doigt. Pas de mot de passe, pas de SSO et le MFA est inutile. Simplement un accès tout simple, sans mot de passe, à tous les services sur tous les périphériques, quel que soit l'OS, et partout dans le monde. Avec l'avènement de l'Everywhere Workplace, c'est plus important que jamais.

Sécurité facile, de type grand public

Fournir un système de sécurité facile similaire aux applications grand public, c'est la progression naturelle de nos attentes en matière de périphériques mobiles. L'exemple le plus criant en est la multiplication des systèmes de paiement mobiles, comme Apple Pay et Google Pay, qui vous permettent d'enregistrer une carte bancaire. Quand vous payez avec cette carte, le système autorise la transaction en fonction d'un élément que vous possédez (téléphone, montre connectée, tablette) et de qui vous êtes (confirmation biométrique avec une technologie comme Apple Face ID ou Touch ID). Et nous apportons cette expérience de sécurité transparente sur le lieu de travail.

Approche Zero Trust de bout en bout

Tout cela fait partie de notre volonté de redéfinir la sécurité d'entreprise avec une approche Zero Trust de bout en bout, qui commence avec les fondations UEM que vous possédez déjà. L'accès n'est accordé qu'après corrélation de l'utilisateur, du périphérique, de l'appli, du réseau et des menaces… le tout sans demander aucun mot de passe.

Tous les services de Cloud.
Ce même processus sans mot de passe permet aussi de sécuriser l'accès à tous les services de Cloud dont votre entreprise a besoin, notamment Office365, Salesforce ou Dropbox.

Tous les périphériques.
Cette sécurité transparente s'étend aux périphériques que votre entreprise ne gère pas, comme ceux des sous-traitants et des partenaires qui ont besoin d'accéder à certaines applis de l'entreprise.

Ne jamais faire confiance, toujours vérifier.

Un accès sans mot de passe à tous les services sur tous les périphériques, quel que soit l'OS, partout dans le monde.

Nos périphériques utilisent déjà la biométrie pour sécuriser l'accès.

Pay G Pay

Zero Sign-On.
Fourni par Ivanti.

En convertissant votre périphérique en outil d'ID sécurisé avec sécurité Zero Trust de bout en bout, Ivanti crée un univers où vous pouvez :

- Limiter les risques de sécurité liés au vol de références d'authentification
- Éviter les comportements risqués des utilisateurs pour contourner les mots de passe
- Vous protéger des menaces mobiles qui se multiplient
- Mettre fin à la frustration qu'engendrent les oublis et les réinitialisations de mot de passe

Tout cela est rendu possible par la sécurité Zero Trust de bout en bout, qui commence avec l'installation UEM que vous possédez déjà. Exploitez-la pour éliminer les mots de passe dans votre entreprise. Les utilisateurs et le département IT vous remercieront.

En savoir plus

Copyright © 2021, Ivanti. All rights reserved. IVI-2530 04/21 RD/FG

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

1. Rapport 2017 de Verizon sur les fuites de données (DBIR)
2. IDG MobileIron MarketPulse, avril 2019.
3. Une étude montre que les collaborateurs accèdent à un nombre toujours plus important d'applis d'entreprise. WallStreet Journal, Angus Loten, 7 février 2019.
4. IDG MobileIron MarketPulse, avril 2019.
5. Rapport IDG MarketPlace, avril 2019.