okta

Quel est le coût de l'usurpation d'identité ?

Nos données à caractère personnel valent de l'or pour les cybercriminels. C'est la raison pour laquelle le piratage de comptes connaît un essor sans précédent. Lors de ces attaques, les pirates utilisent des identifiants légitimes pour accéder aux comptes et dérober des informations. Les répercussions sur les revenus et la réputation d'une entreprise peuvent être catastrophiques. Face à un tel constat, comment les entreprises peuvent-elles réduire les risques et conserver la confiance de leurs clients ?

Le piratage de comptes a le vent en poupe

Les piratages de comptes ont été multipliés par trois pendant la pandémie, qui a contraint davantage de personnes à réaliser des achats et à travailler en ligne.

x 3
Augmentation entre 2019 et 2021
Source : SIM

L'identité des utilisateurs dans la ligne de mire

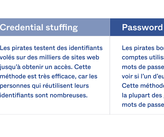
Les identifiants volés ou compromis constituaient la principale cause de brèche de données en 2021.

61 %
des brèches de données en 2021 impliquaient l'utilisation abusive d'identifiants
Source : Verizon, DBIR

> « Les pirates n'entrent pas par effraction, ils se connectent avec des identifiants légitimes. »

Les cybercriminels mettent la main sur des identifiants de différentes manières

Les utilisateurs peuvent être manipulés et ainsi divulguer leurs identifiants lors d'attaques de phishing. Des listes de mots de passe courants et volés peuvent aussi être achetées sur le Dark Web.



7 sur 10
entreprises ont observé une augmentation des attaques de phishing depuis le début de la pandémie
Source : Sophos

15 milliards
d'identifiants sont en vente sur le Dark Web
Source : Digital Shadows

La faiblesse des mots de passe n'arrange rien

Beaucoup emploient des mots de passe faciles à deviner ou réutilisent le même mot de passe sur de nombreux sites web, ce qui accroît leur exposition aux attaques.

123456
Mot de passe le plus courant en 2021
Source : NordPass

14
Nombre moyen de réutilisations d'un mot de passe
Source : LastPass

Comment les pirates infiltrent-ils vos systèmes ?

Credential stuffing	Password spray	Phishing
Les pirates testent des identifiants volés sur des milliers de sites web jusqu'à obtenir un accès. Cette méthode est très efficace, car les personnes qui réutilisent leurs identifiants sont nombreuses.	Les pirates bombardent des comptes utilisateurs avec des mots de passe courants pour voir si l'un d'eux fonctionne. Cette méthode est efficace, car la plupart des gens utilisent des mots de passe faciles à deviner.	Les utilisateurs sont incités à révéler leurs identifiants, par exemple par le biais d'un e-mail les invitant à suivre un lien vers un site web.

55 %
des brèches de données sont l'œuvre de groupes cybercriminels organisés
Source : Verizon, DBIR

Les brèches de données sont mauvaises pour les affaires

De nombreux cybercriminels utilisent des outils en ligne afin de bombarder des sites web avec un important volume de mots de passe différents pour tenter de s'y infiltrer.

47 %
des clients se détourneraient d'une marque s'ils apprenaient qu'elle avait été victime d'une brèche de données
Source : The State of Digital Trust, Okta

4,2 millions $
Coût moyen d'une brèche de données en 2021
Source : IBM, Cost of a Data Breach Report

3 façons de protéger l'identité des clients

1. Détection plus rapide des brèches

Les systèmes de détection des brèches, tels que Credential Guard d'Auth0, sont capables de détecter les brèches dès leur apparition, ainsi que de réinitialiser rapidement les mots de passe concernés.

2. Implémentation de l'authentification multifacteur (MFA)

L'authentification multifacteur (MFA) offre une couche de sécurité supplémentaire en plus du mot de passe d'un utilisateur, ce qui contribue à tenir les pirates à l'écart de vos systèmes.

3. Accès passwordless

De plus en plus d'entreprises décident d'abandonner complètement les mots de passe et proposent aux clients des méthodes de connexion sécurisées et conviviales comme la biométrie, les mots de passe à usage unique et les magic links.

Prévenez le piratage de comptes avec Okta

Okta vous aide à protéger vos clients, partenaires et collaborateurs grâce à des solutions d'authentification dans lesquelles ils peuvent avoir confiance. Appliquez des politiques de mots de passe rigoureuses, identifiez rapidement les tentatives de connexion frauduleuses et stoppez les cybercriminels grâce aux fonctionnalités automatisées de détection des menaces d'Okta.

Pour en savoir plus sur le piratage de comptes et les façons de le bloquer, regardez le podcast vidéo avec Brian Glick, rédacteur en chef de Computer Weekly, et Ian Lowe d'Okta.