okta

Les 6 atouts d’une authentification forte des clients pour optimiser l’expérience utilisateur

Pour satisfaire les clients qui exigent une expérience numérique simple et sûre, les entreprises se tournent vers une authentification forte, intégrée à une solution avancée de gestion des identités et des accès clients (CIAM). Voici 6 atouts de la protection renforcée des identités qui permettent de réduire les points de friction et d’améliorer la fluidité de l’expérience utilisateur.

1

Connexion simple, appréciée des clients

Les mots de passe sont difficiles à retenir et faciles à pirater. Une solution CIAM avancée vous permet de proposer plusieurs options de connexion pratiques, par exemple l’authentification unique (SSO) et la connexion par un compte de réseau social, ce qui élimine les risques liés aux noms d’utilisateur et mots de passe vulnérables.

83 %

des clients ont déjà abandonné une interaction en cours en cas de procédure de connexion trop lente

Source : AuthO, Expectation vs Reality at the Log Inn

53 %

des clients se connectent parfois ou toujours avec leurs identifiants de réseaux sociaux

Source : AuthO, Expectation vs Reality at the Log Inn

2

Couche de sécurité supplémentaire avec le MFA

Des mots de passe compromis ailleurs pourraient être utilisés pour attaquer vos systèmes. L’authentification multifacteur (MFA) ajoute une couche de sécurité supplémentaire en demandant aux utilisateurs un autre facteur de validation, par exemple un code à usage unique, afin de protéger votre entreprise même en cas d’utilisation d’un mot de passe compromis.

86 %

des clients réutilisent des mots de passe sur plusieurs sites

Source : AuthO, Expectation vs Reality at the Log Inn

70 %

des mots de passe compromis sont toujours utilisés

Source : SpyCloud, 2022 Annual Identity Exposure Report

3

Sécurité s’adaptant au contexte

Des mesures de sécurité uniformes en toutes circonstances introduisent des points de friction inutiles pour les utilisateurs à faible risque. L’authentification multifacteur (MFA) adaptative vous permet d’exiger une vérification supplémentaire uniquement lorsqu’elle est nécessaire, par exemple lorsque votre client communique des informations sensibles ou semble se connecter depuis un emplacement ou un terminal inhabituel.

49 %

des clients sont plus susceptibles de s’inscrire à une application s’ils peuvent utiliser le MFA

Source : AuthO, Expectation vs Reality at the Log Inn

75 %

de réduction des risques de brèches de sécurité avec le MFA adaptatif

Source : Okta

4

Détection automatique des menaces

Les attaques d’usurpation d’identité impliquant le vol d’identifiants sont en forte hausse et peuvent coûter cher à l’entreprise, en termes d’atteinte à la réputation et de perte de confiance. Une solution CIAM inclut des fonctionnalités de sécurité capables de repérer les activités suspectes, de détecter les mots de passe compromis et de bloquer les adresses IP malveillantes avant qu’elles ne puissent attaquer vos systèmes.

61 %

des cyberattaques en 2021 impliquaient des identifiants volés

Source : Verizon, 2021 Data Breach Investigations Report

3 attaques qui menacent la sécurité des identités

- **Phishing**
- **Credential stuffing**
- **Password spray**

Source : Okta, Cinq attaques d’usurpation d’identités exploitant les failles de votre système d’authentification

5

Expériences confidentielles et conformes

La confidentialité des données à caractère personnel devient une préoccupation majeure pour les clients. Une solution CIAM offre une vue unifiée de chaque utilisateur sur tous les systèmes et vous permet de savoir exactement où les informations de consentement résident, afin de pouvoir respecter facilement les exigences de conformité.

65 %

de la population mondiale bénéficiera d’une protection de ses données personnelles en vertu de réglementations en matière de confidentialité des données en 2023

Source : Gartner

71 %

des clients sont prêts à couper les ponts avec une société si celle-ci a communiqué des informations sensibles sans leur consentement

Source : McKinsey

6

Possibilités d’innovation pour les développeurs

Comme les développeurs sont une denrée rare, il est préférable qu’ils consacrent leur précieux temps à concevoir des produits exceptionnels. Une solution de gestion des identités avancée offre une approche standardisée d’intégration de l’identité qui permet aux développeurs de se concentrer sur ce qu’ils font le mieux.

4 millions

de développeurs à temps plein viendront à manquer d’ici 2025

Source : IDC

Créer des expériences numériques optimales avec Okta

Utilisez les solutions de gestion des identités clients (CIAM) d’Okta pour créer des expériences d’inscription et de connexion fluides qui séduiront vos clients et développeurs. Grâce à plus de 7 000 intégrations avec des applications et fournisseurs d’infrastructures, Okta est adopté par plus de 14 000 marques pour sécuriser les interactions numériques et accélérer l’innovation.

Pour en savoir plus sur la façon dont l’authentification forte des clients peut renforcer la sécurité de votre entreprise, **regardez notre podcast vidéo** avec Brian Glick, rédacteur en chef de Computer Weekly, et Ian Lowe d’Okta.