IBM Security

Guide d'optimisation – Risques liés à l'identité numérique et expérience de l'accès adaptatif

Le pouvoir de l'identité

Nos identités numériques influencent de façon fondamentale nos interactions les uns avec les autres et avec l'univers en ligne.[1] La capacité à prouver qui nous sommes nous permet de conserver le contrôle et d'accéder aux personnes, à l'information et aux économies. La validation numérique de ces identités constitue une forme de pouvoir.

Toutefois, il peut être difficile de créer une identité numérique digne de confiance. L'identité recouvre un réseau complexe d'instruments traditionnels de formes d'identification : nom, adresse, date de naissance, numéro de sécurité sociale et données telles qu'adresse email, nom d'utilisateur et mot de passe, habitudes de recherche, comportements d'achat, et ainsi de suite.

Ces données personnelles se composent de caractéristiques uniques associées à un individu et constituent une passerelle pour chaque échange en ligne. Ces actions dépendent du contexte pour déterminer l'identité.

La multiplication des échanges entraîne aussi celle des vulnérabilités.[2] Des intervenants malveillants découvrent en permanence de nouveaux systèmes leur permettant d'exploiter les données personnelles pour identifier le vol ou pirater des données précieuses dans les entreprises. En 2018, le nombre de données utilisateur exposées contenant des informations personnelles sensibles a fait un bond de 126 %.[3] En 2019, le coût d'une violation de données a atteint environ $4 millions.[4]

Des entreprises qui tergiversent

Le problème vient du fait que le cybersécurité reste mal comprise,[5] et que de nombreuses entreprises continuent de protéger des applications critiques avec des combinaisons nom d'utilisateur/mot de passe alors qu'il existe des solutions plus sûres. L'authentification ajoute une couche de sécurité supplémentaire et rend plus difficile l'accès aux utilisateurs non autorisés. Alors, pourquoi tant d'entreprises semblent-elles vouloir mettre des oreillères et continuent-elles à tergiverser ?

Alors même que l'authentification multi-facteurs est appelée à se répandre et constitue un gage de sécurité accrue, elle n'est utilisée que par un très petit nombre d'entreprises.

POINT CLE

Alors même que l'authentification multi-facteurs est appelée à se répandre et constitue un gage de sécurité accrue, elle n'est utilisée que par un très petit nombre d'entreprises.

En effet, elles croient souvent à tort que le risque de provoquer la frustration des utilisateurs finaux, des employés et des clients est plus important que celui d'une violation de données. Alors même que l'authentification multi-facteurs est appelée à se répandre et constitue un gage de sécurité accrue, elle n'est utilisée que par un très petit nombre d'entreprises. Selon Gartner, "en 2022, 60 % des systèmes de gestion des accès feront appel à l'analyse du comportement des utilisateurs et des entités (UEBA) et à d'autres contrôles pour assurer en continu l'authentification, l'autorisation et la détection des fraudes en ligne, contre seulement 10 % aujourd'hui."[6]

L'expérience opposée à la sécurité

Les utilisateurs professionnels gèrent en moyenne 191 mots de passe[7] en général de façon peu recommandable, c'est-à-dire en réutilisant constamment le même mot de passe. Comme si cette difficulté ne suffisait pas, imaginez qu'ils doivent de plus attendre de recevoir un SMS ou un email contenant un code de connexion.

Autre exemple : contraignez-les à identifier des photos en leur demandant d'indiquer les parties représentant une voiture ou un feu de signalisation, alors que les images proposées laissent souvent place au doute. Ensuite, bombardez-les d'un énième email les avertissant de leur nouvelle tentative de connexion, alors qu'ils ont dû franchir toutes ces étapes pour y parvenir, si tant est qu'ils sont arrivés jusqu'à ce stade. Aux Etats-Unis, seuls 28 % des utilisateurs adultes sont capables d'identifier un exemple d'authentification à deux facteurs.[8]

Si vous tentez d'appliquer ce processus contraignant aux clients, il y a de fortes chances que vous les fassiez fuir définitivement. L'expérience est aujourd'hui un facteur de différenciation primordial et le fait de traiter vos clients comme des cybercriminels en puissance est plus que risqué.

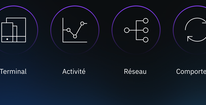
La gestion des accès ne doit pas nécessairement se résumer à une approche du tout ou rien. L'authentification multi-facteur n'est pas un obstacle si elle est conçue intelligemment. La facilité d'utilisation et la sécurité peuvent être optimisées si les mécanismes de sécurité agissent en toute discrétion en arrière-plan, en collectant du contexte sur l'utilisateur et son comportement. Ce contexte peut ensuite être mis à profit pour déterminer le processus d'authentification le mieux adapté à la situation, et permet de créer des expériences adaptatives totalement transparentes.

POINT CLE

Aux Etats-Unis, seuls 28 % des utilisateurs adultes sont capables d'identifier un exemple d'authentification à deux facteurs.[8]

Sortez sans risque

Une gestion des accès qui n'impose l'authentification multi-facteur que si des risques sont détectés libère les utilisateurs de toute cette lourdeur. La validation est obtenue par une détermination du contexte qui commence avec l'utilisateur et s'étend à son terminal, son activité, son environnement réseau et son comportement.

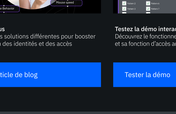


Score de confiance

La détection des risques basée sur l'IA utilise des modèles d'apprentissage automatique pour synthétiser le contexte sur les appareils mobiles, les sessions Web et les VPN. Elle applique des critères tels que les fraudeurs connus, les infections par des malware et d'autres anomalies pour recommander automatiquement l'authentification multi-facteur dans les scénarios à haut risque.

L'analyse du contexte associe à la fois des facteurs positifs et négatifs pour créer un indicateur de confiance unique. Ce score vous permet de passer d'une stratégie du tout ou rien à une approche plus nuancée du niveau de confiance établi entre vous-même et vos utilisateurs. C'est cette souplesse qui est à la base d'une stratégie d'accès adaptative.

Dès que vous avez un score de confiance, des règles statiques d'authentification deviennent superflues. A la place, vous pouvez créer une stratégie d'authentification intelligente qui offre un accès non frustrant à vos utilisateurs dignes de confiance et qui limite l'accès au fur et à mesure que le risque s'accentue. Cette approche permet aux utilisateurs à faible risque de bénéficier d'une expérience où il ne leur est demandé aucun mot de passe, ainsi que d'un accès sans aucune intervention manuelle de leur part pour confirmer leurs identités.



L'authentification intelligente est capable de répondre aux questions suivantes :

- S'agit-il d'un être humain ou d'un bot ?
- Y a-t-il des preuves indiquant une activité malveillante ?
- Le téléphone est-il pré-payé, rooté ou débridé ?
- Le numéro de téléphone ou l'adresse email est-il légitime ?
- Les tendances constatées font-elles penser à une malveillance ?
- L'authentification hors bande a-t- elle été contournée ?
- Existe-t-il un proxy de connexion ?
- Le schéma du comportement utilisateur est-il connu ?
- Les mouvements de la souris semblent-ils inhabituels ou automatisés ?

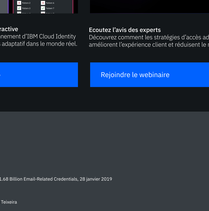
POINT CLE

L'analyse du contexte associe à la fois des facteurs positifs et négatifs pour créer un indicateur de confiance unique.

Score de confiance : fonctionnement

Un utilisateur chez qui des anomalies mineures sont observées peut recevoir une autorisation moyennant l'application de certaines restrictions à ses transactions ou à son activité. Les utilisateurs ayant un très haut score de confiance, dont les terminaux sont connus, et présentant des scores biométriques comportementaux positifs, peuvent bénéficier d'une autorisation sans mot de passe.

Testez la démo



La promesse de l'accès adaptatif

Les règles statiques placent trop haut ou trop bas la barre de la vérification. IBM Cloud Identity, qui utilise l'accès adaptatif, est une plateforme de gestion des accès intelligente. Elle associe une détection des risques avancée à un moteur robuste de politique d'accès qui permet d'évaluer le contexte complet de l'identité d'un utilisateur lors de sa tentative de connexion à un service numérique. La promesse d'une expérience numérique exempte de toute frustration est donc possible, sans sacrifier les impératifs de la sécurité.

Apportant une réponse aux entreprises qui peinent à optimiser le risque lié aux identités et la convivialité des solutions d'accès, IBM Cloud Identity, avec sa fonction d'accès adaptatif, limite les difficultés d'authentification en mettant en place un accès intelligent et non frustrant aux applications et aux données.

La solution s'intègre aisément aux applications, avec peu de codage, voire aucun, via une API pour les applications personnalisées et des modèles prédéfinis pour les applications cloud couramment utilisées.

POINT CLE

Apportant une réponse aux entreprises qui peinent à optimiser le risque lié aux identités et la convivialité des solutions d'accès, IBM Cloud Identity et sa fonction d'accès adaptatif limite les difficultés d'authentification en mettant en place un accès intelligent et non frustrant aux applications et aux données.

L'authentification doit être intelligente. Une authentification intelligente sait s'adapter.

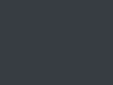
Etapes suivantes

En savoir plus
Explorez trois solutions différentes pour booster votre gestion des identités et des accès

Lire l'article de blog

Testez la démo interactive
Découvrez le fonctionnement d'IBM Cloud Identity et sa fonction d'accès adaptatif dans le monde réel.

Tester la démo



Ecoutez l'avis des experts
Découvrez comment les stratégies d'accès adaptatif améliorent l'expérience client et réduisent le risque

Rejoindre le webinaire

Sources

1. IBM. Digital identity management: How much of your personal information do you control?
2. IBM Institute for Business Value, Trust me: Digital identity on blockchain, avril 2017
3. Identity Theft Resource Center, Consumers At Risk: 126% Increase In Exposed Consumer Data, 1.68 Billion Email-Related Credentials, 28 janvier 2019
4. IBM, Cost of a Data Breach, 2019
5. Pew Research Center, What the Public Knows About Cybersecurity, Aaron Smith, 22 mars 2017
6. Gartner, Magic Quadrant 2019 sur la gestion des accès, Abhyuday Data, Michael Kelley, Henrique Teixeira
7. Security Magazine, Average Business User Has 191 Passwords, 6 novembre 2017
8. Pew Research Center, Americans and Digital Knowledge, Monica Anderson et Emily Vogels, 9 octobre 2019

IBM