Akamai

DOCUMENT

La MFA d'aujourd'hui : une illusion en matière de sécurité ?

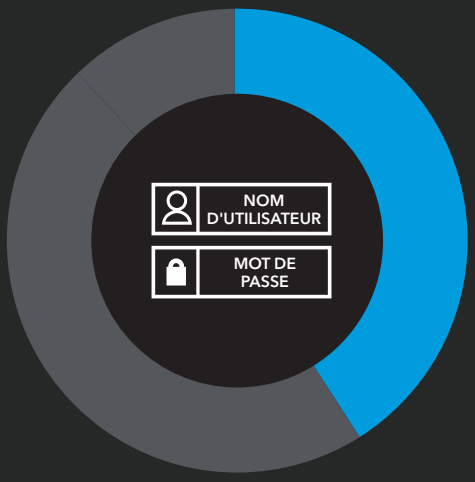
Les noms d'utilisateur et les mots de passe ne suffisent pas

80 % des violations de sécurité signalées concernent des informations d'identification utilisateur compromises.[1] Bien que les mots de passe peu sécurisés soient en partie responsables, les mots de passes complexes et indéchiffrables développés par des algorithmes peuvent également poser problème.[2] Un audit récemment mené sur le Dark Web a révélé le vol de 15 milliards d'identifiants suite à 100 000 violations.[3]

L'importance cruciale de la connectivité digitale, le recours aux services cloud et la réalité des environnements hybrides, associés au recours aux mots de passe, rendent les utilisateurs vulnérables à une multitude de vecteurs d'attaque d'authentification :

- **Credential stuffing**
- **Pulvérisation de mot de passe et autres mécanismes d'attaque en force**
- **Découverte locale et attaques d'initiés**
- **Hameçonnage et ingénierie sociale**
- **Enregistrement des frappes**
- **Proxy malveillant et campagnes de réponses**

De plus, la pandémie mondiale a exacerbé ce statu quo, démontrant la nécessité d'un accès sécurisé indépendant aux terminaux et aux emplacements. Lorsque l'on réalise que 100 % des violations d'informations d'identification se produisent après l'authentification d'un utilisateur, il semble évident que les mots de passe ne sont pas adaptés pour une authentification précise.



Malgré la mise en évidence de ces faiblesses, 41 % des entreprises considèrent encore les noms d'utilisateur et les mots de passe comme des outils de gestion des accès des plus efficaces.[4]

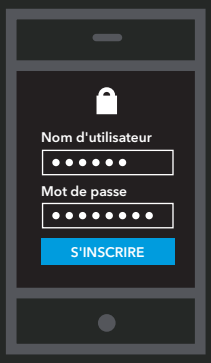
500 %

Akamai a constaté une augmentation des attaques d'hameçonnage, d'ingénierie sociale, de credential stuffing et d'attaques en force. Entre mars et mai 2020, nous avons constaté une hausse de près de 500 % des programmes malveillants.

Les avantages de l'authentification multifactorielle

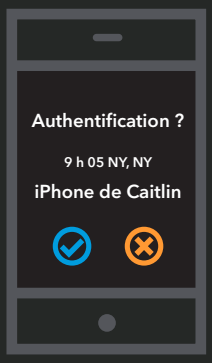
La popularité croissante de la technologie d'authentification multifactorielle (MFA) n'a donc rien d'étonnant. Pour faire simple, la MFA protège votre entreprise en ayant recours à plusieurs sources de validation pour vérifier l'identité d'un utilisateur avant de lui accorder l'accès.

La MFA nécessite une combinaison réussie d'au moins deux des trois informations d'authentification suivantes :



Quelque chose que vous savez

Il s'agit d'une authentification basée sur les connaissances. Elle peut prendre la forme d'un mot de passe, d'un code PIN, d'une réponse à une question de sécurité ou même d'un pictogramme.



Quelque chose que vous avez

Il s'agit d'une authentification par jeton, matériel ou logiciel. Elle peut prendre la forme d'une carte intelligente ou d'une clé de sécurité, d'un mot de passe à usage unique, d'une notification push ou d'un code SMS envoyés sur un terminal mobile.

Quelque chose qui vous représente

Il s'agit de l'authentification contextuelle ou biométrique. Elle peut prendre la forme d'un comportement, de signaux ou de temps de localisation, d'une empreinte digitale, d'une reconnaissance faciale, d'une empreinte ou d'un modèle vocal ou encore d'une signature.

La mise en place d'une solution MFA réduit considérablement le risque d'accès non autorisé et de violations du système. Les organisations qui utilisent la MFA sont 99,9 % moins susceptibles d'être compromises que les autres.[5] La MFA rationalise et offre un accès sécurisé à tous les environnements : applications cloud, sur site, basées sur le Web, SaaS et IaaS. Une solution MFA est également un élément essentiel dans la migration de la sécurité d'entreprise vers des structures de type Zero Trust et SASE.

En exigeant plus que des noms d'utilisateur et des mots de passe, en harmonisant l'expérience de connexion et en s'intégrant à d'autres outils de sécurité natifs du cloud, les technologies MFA permettent également d'accroître la productivité des utilisateurs et la convivialité. De plus, l'authentification gérée de manière centralisée répond à de nombreuses exigences et préoccupations en matière de conformité.

Mais la MFA traditionnelle n'est pas aussi sécurisée que vous le pensez

Un service MFA basé sur un push standard peut être facilement manipulé par un hacker pour prendre le contrôle de votre compte. À moins qu'elles ne soient consolidées par une sécurité supplémentaire, les technologies MFA actuelles vous exposent à des risques.

La MFA est une forme de sécurité de périmètre, cependant, le cloud et les méthodes de travail actuelles n'ont pas de périmètre. La MFA n'est pas conçue pour bloquer les attaques sans lien avec les identifiants. Elle sécurise uniquement la connexion au niveau du périmètre, lorsque l'utilisateur souhaite accéder au système. Les cybercriminels ont développé des mécanismes d'ingénierie sociale et d'hameçonnage relativement simples mais très efficaces pour contourner cette réalité.

Imaginons le scénario suivant :

1. **Suite à une attaque d'ingénierie sociale, un(e) employé(e) saisit un vrai nom d'utilisateur et un mot de passe dans un faux site (hameçonnage) configuré par un hacker.**
2. **Une fois ces informations d'identification obtenues, le hacker les saisit sur le véritable portail de connexion.**
3. **Cela entraîne l'envoi d'une notification push sur le téléphone de l'employé(e).**
4. **L'employé(e) accepte la notification push comme s'il s'agissait d'une connexion normale.**
5. **Le hacker a ainsi validé deux formes de vérification et peut accéder au système.**

Il s'agit de la défaillance critique d'une notification push standard en matière de sécurité : n'importe quel hacker possédant des informations d'identification volées peut envoyer des notifications push sur le téléphone d'un employé. Le seul élément qui sépare la violation de sécurité des activités habituelles est la capacité de l'employé à discerner une notification légitime d'une escroquerie. Il suffit d'une seule tentative réussie parmi des milliers d'employés pour permettre au hacker d'accéder au système.

MFA anti-hameçonnage

Une solution MFA véritablement sécurisée utilise la norme FIDO2. Pour faire simple, cela signifie que la sécurité est assurée par la technologie au lieu de dépendre des décisions de l'utilisateur.

Comment y parvenir ? La norme FIDO2 utilise deux techniques qui empêchent l'hameçonnage.

Dans un premier temps, la demande d'authentification (le défi de la solution MFA) est toujours envoyée sur le poste de travail à l'origine de la demande d'accès. Le navigateur du poste de travail redirige alors la demande d'authentification vers la ou les clés de sécurité connectées localement. Sur la base du scénario ci-dessus : plutôt que de réussir à faire en sorte que le service MFA envoie la notification push sur le téléphone de l'employé, le hacker reçoit le défi MFA sur son propre poste de travail. Étant donné qu'il ne possède pas la clé de sécurité de l'employé, aucune réponse ne peut être donnée. La prise de contrôle d'un compte est donc impossible.

Définitions : spécifications et normes d'authentification

Fast IDentity Online (FIDO) Alliance

Organisme responsable du développement, de l'utilisation et du respect des normes d'authentification.

FIDO2

Nom général du dernier ensemble de spécifications d'authentification de FIDO Alliance. Les normes incluses sont CTAP1, CTAP2 et WebAuthn. FIDO2 permet aux utilisateurs de tirer parti des terminaux courants pour s'authentifier facilement auprès des services en ligne dans les environnements mobiles et de bureau.

WebAuthn

Une norme Web publiée par le World Wide Web Consortium (W3C) et un élément essentiel de la norme FIDO2. Ce projet a pour but de normaliser une interface d'authentification utilisateur pour les applications et services Web grâce au chiffrement à clé publique.

Protocole client-authentifiant (CTAP)

Une spécification développée par FIDO Alliance qui permet une communication sécurisée entre un authentifiant itinérant (exemple : un smartphone) et un authentifiant interne (le client ou la plateforme).

Ensuite, le navigateur envoie des données à la clé de sécurité en même temps que la demande d'authentification. Ces données comprennent le nom de domaine du poste de travail à l'origine de la demande d'authentification, tel que vu par le navigateur. Si le hacker transmettait simplement la demande d'authentification reçue au poste de travail de l'employé, ces données contiendraient le nom de domaine du site d'hameçonnage. La clé de sécurité ferait alors la différence entre le nom de domaine du site sur lequel elle était enregistrée à l'origine et le nom de domaine demandant l'authentification et refusant de répondre. L'attaque serait à nouveau bloquée.

Si une MFA anti-hameçonnage et plus sécurisée est possible, pourquoi n'est-elle pas plus largement mise en place ? Parce que cela nécessite des clés de sécurité physiques, coûteuses et encombrantes. En tout cas, cela en nécessitait jusqu'à présent.

MFA nouvelle génération en bordure de l'Internet

Lors de l'évaluation et de la mise en place des technologies de MFA, le service informatique a dû trouver un compromis. Pour garantir la meilleure sécurité, il faut dépenser davantage pour déployer du matériel, acheter des clés de sécurité physiques pour chaque employé et gérer la distribution et le fonctionnement de toutes ces clés. Le service informatique doit également faire adopter à chaque utilisateur les complications que représentent les clés, avec un nouveau matériel à utiliser et à contrôler.

L'alternative moins sécurisée est l'envoi de notifications push pratiques sur les smartphones des employés sans coûts supplémentaires. La facilité de cette alternative est la raison pour laquelle la MFA push est si largement utilisée aujourd'hui. Et c'est aussi la raison pour laquelle tant d'entreprises sont exposées à des risques de violation.

Mais il n'est plus nécessaire pour la sécurité de faire un compromis entre les coûts et la facilité d'adoption.

La MFA d'Akamai présente un nouveau facteur d'authentification. Elle numérise la sécurité de FIDO2 avec un simple smartphone et un navigateur Web, et l'associe à l'expérience conviviale et familière d'une notification push, pouvant être utilisée comme authentifiant itinérant sur n'importe quelle plateforme. Aucune clé de sécurité physique n'est requise. Cette solution offre les fonctionnalités les plus sécurisées de la norme FIDO2 à un coût réduit, avec une facilité d'installation et d'utilisation, ainsi qu'une interopérabilité avec les fournisseurs d'identités communs.

Protégez votre entreprise de l'hameçonnage, du credential stuffing et du piratage de comptes avec la MFA d'Akamai. Apprenez-en davantage sur la technologie MFA d'Akamai unique en son genre et préparez-vous pour un avenir sécurisé et sans mot de passe.

Pour en savoir plus, rendez-vous sur akamai.com/mfa.

Sources :

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://www.infosecurity-magazine.com/opinions/problem-password-everything-1/
3. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=27fa6368180f
4. https://www.businesswire.com/news/home/20200616005047/en/Weakest-Link-Prevails-Overreliance-Passwords-Continues-Compromise
5. https://www.hipaajournal.com/multi-factor-authentication-blocks-99-9-of-automated-cyberattacks/