LastPass ••• | by LogMeIn

10 raisons de choisir l'authentification adaptative plutôt que l'A2F

À l'heure où 80 % des failles de sécurité sont provoquées par des mots de passe faibles, il est évident qu'ils ne peuvent pas à eux seuls protéger votre entreprise.

L'authentification à deux facteurs (A2F) est un bon point de départ, mais les approches indifférenciées ne fonctionnent pas lorsque les utilisateurs ont différents comportements, appareils, niveaux d'accès et attributs.

1. L'expérience utilisateur est primordiale

Les employés ont besoin d'une expérience utilisateur simple pour accéder à leur travail. Sans quoi ils perdront en productivité. L'A2F fournit la même expérience à tous, que les requêtes soient légitimes ou frauduleuses.

2. Les notifications push ne suffisent pas

Les cybermenaces sont de plus en plus sophistiquées et la sécurité doit donc suivre. Les organisations ont besoin d'être sûres et certaines de l'identité des utilisateurs, au-delà de ce que les notifications push peuvent garantir.

3. Les solutions d'authentification doivent s'intégrer

Votre entreprise compte tout un éventail d'apps, d'utilisateurs et d'appareils. Les solutions d'authentification doivent s'intégrer à cet environnement, pour que vous ayez une visibilité rationalisée sur l'activité et les accès.

4. La souplesse est essentielle

Plus vous disposez de facteurs d'authentification, du push à la biométrie, plus vous bénéficiez de souplesse pour gérer l'authentification de manière adaptée à votre activité.

5. Sans contrôle granulaire, vous n'avez pas le contrôle

L'authentification vise à garantir que les utilisateurs sont bien qui ils prétendent être. Vous devez pouvoir gérer qui est authentifié, quand et à partir d'où, au niveau de l'organisation, des groupes et des individus.

6. L'A2F ne fournit pas assez d'informations

L'A2F fournit un deuxième facteur, mais vous devez savoir précisément qui accède à quelles ressources, depuis quel appareil et quel lieu, pour être certain que les bons utilisateurs disposent des bons accès.

7. La biométrie ne peut pas être copiée

Quel meilleur moyen de vérifier qui sont les utilisateurs que d'exploiter ce qu'ils sont ? Les facteurs d'A2F comme TOTP peuvent être copiés, alors qu'une empreinte digitale, une voix ou un visage est propre à un individu seul.

8. Le contexte renforce l'authentification

Pour être totalement certain de la légitimité d'un utilisateur, vous avez besoin de plus de contexte qu'un nom et un mot de passe. L'emplacement, l'adresse IP et l'appareil sont tous des éléments critiques pour valider une requête.

9. L'A2F ne peut pas s'adapter à vos utilisateurs

Il n'y a pas deux utilisateurs identiques. C'est pourquoi l'authentification doit s'adapter au contexte de la requête pour fournir l'authentification appropriée, sans ajouter de complexité.

10. L'authentification générique ne fonctionne plus

L'authentification intelligente n'est pas forcément compliquée. Grâce à l'authentification adaptative, vous pouvez valider l'identité d'un utilisateur à l'aide d'une combinaison de facteurs, sans augmenter la friction associée à l'expérience de connexion.

En savoir plus sur l'authentification adaptative :

www.lastpass.com/solutions/authentication

05.31.2019/POF/LM0638d