GUIDE À L'USAGE DES RESPONSABLES SÉCURITÉ : AUTHENTIFICATION MULTI-FACTEURS

Mot de passe : ce n'est pourtant pas un gros mot mais c'est un mot qui hérisse le poil de tous les responsables sécurité. Inutile de lire toutes les études ou toutes les publications sur les faiblesses des mots de passe, et elles sont nombreuses, pour savoir que l'authentification à un seul facteur fait courir des risques à votre entreprise.

L'authentification à deux facteurs (2FA) offre une couche supplémentaire de protection. Sommes-nous sur la bonne voie ? Oui, bien sûr ! Mais, en termes de sécurité et d'expérience, cela n'est pas encore totalement satisfaisant. Si l'authentification à deux facteurs est très impopulaire auprès de vos utilisateurs, elle ne compte pas non plus parmi les outils de sécurité les plus affutés, en particulier si le second facteur est fourni via SMS.

> « [Pour ceux qui] offrent seulement des protections à deux facteurs reposant sur les SMS, il est temps de se réveiller, de débusquer les attaques ciblées et de proposer aux utilisateurs de meilleures options.[2] »
>
> Andy Greenberg, Wired

Le public a eu connaissance de cette faiblesse en 2016 lorsque des attaques visant des personnalités politiques se sont avérées être le résultat de messages SMS interceptés. À la même période, le NIST (National Institute for Standards and Technology) a cessé de recommander les systèmes 2FA utilisant les SMS en raison de leurs nombreuses faiblesses en matière de sécurité. En théorie, la méthode 2FA est correcte car « l'utilisation de SMS n'est techniquement pas du tout l'équivalent de deux facteurs », explique Jonathan Zdziarski,[1] chercheur en sécurité et expert en science forensique. Il affirme qu'il existe de meilleurs outils capables de prouver la possession du facteur « ce que j'ai ».

Il a raison. L'authentification multi-facteurs (ou MFA) est ce type d'outils.

[1] Andy Greenberg, « So Hey You Should Stop Using Texts for Two-Factor Authentication », Wired, 26 juin 2016, accès 23 fév. 2017 sur https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/

[2] Ibid

01

COMMENT ET POURQUOI L'AUTHENTIFICATION MULTI-FACTEURS FONCTIONNE-TELLE ?

L'authentification multi-facteurs repose sur la notion suivante : vous pouvez et devez fournir plusieurs facteurs pour l'authentification, et pas seulement un moyen statique unique. La méthode MFA va au-delà de la méthode 2FA puisqu'elle exige des utilisateurs de s'authentifier via deux facteurs différents ou plus, comme le montre la Figure 1. Par définition, le nombre de facteurs d'authentification n'est pas limité, mais l'utilisation d'une palette plus vaste est encouragée, dans trois catégories de facteurs principales : ce que je sais, ce que j'ai et ce que je suis. Cela améliore la flexibilité et l'expérience utilisateur, sans parler d'une position renforcée en termes de sécurité.

En combinant plusieurs facteurs d'authentification, on obtient un niveau de confiance supérieur (LoA, Level of Assurance) sur le fait que l'utilisateur qui tente de s'authentifier est bien celui qu'il prétend être. La théorie est la suivante : si l'un des facteurs a été corrompu, il y a peu de chances que l'autre facteur l'ait également été.

Les mécanismes d'authentification ne sont pas tous identiques : ils peuvent utiliser le même canal via lequel l'utilisateur accède à l'application ou dédier un canal distinct à l'authentification. Il est également intéressant de permettre une authentification via plusieurs facteurs de même type, dans la mesure où un facteur corrompu ne risque pas d'en compromettre un autre.

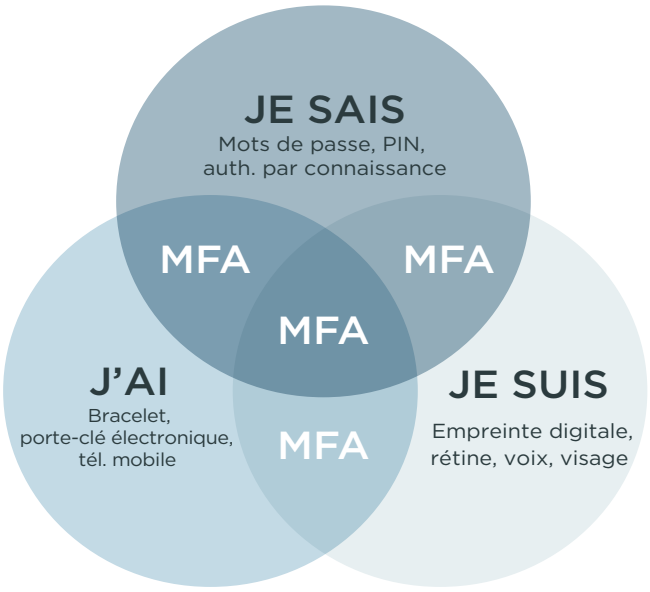

Figure 1 : L'authentification multi-facteurs exige des utilisateurs de s'authentifier via deux catégories de facteurs ou plus.

02

LES BIENFAITS DE L'AUTHENTIFICATION MULTI-FACTEURS

La transformation numérique offre de fabuleuses opportunités à l'entreprise et pose des défis sans précédent aux responsables sécurité. Pour rester compétitif, vous devez adopter de nouvelles applications et de nouvelles technologies cloud, mais aussi réduire les risques à un minimum. Qui plus est, vous devez plus que jamais placer l'expérience utilisateur au-devant de la scène afin de laisser vos concurrents derrière vous, d'encourager l'adoption et enfin de réaliser vos objectifs.

Il n'est pas si facile de remporter le tiercé gagnant sécurité, coût et expérience utilisateur. Mais c'est exactement ce que sait faire l'authentification multi-facteurs moderne.

UN RISQUE DE FAILLE RÉDUIT

Avec l'authentification multi-facteurs, les pirates ont davantage de difficulté à dérober les identifiants ou à recourir à la force brute et autres attaques pour s'introduire dans vos systèmes. Étant donné l'importance des coûts associés à une faille type (sans oublier la perte de chiffre d'affaires et les dommages subis par l'entreprise en termes de réputation), réduire le risque peut avoir un impact conséquent sur votre chiffre d'affaires et vos bénéfices.

DES COÛTS RÉDUITS

En termes de coûts, les solutions à base de jetons matériels ne peuvent pas rivaliser avec le téléphone mobile de l'utilisateur. Les solutions d'authentification multi-facteurs modernes et flexibles par nature vous permettent de renforcer ou d'assouplir les conditions en fonction du risque lié à une activité spécifique. Cela permet de réduire les coûts cumulés associés aux mots de passe par SMS à usage unique, appels vocaux ou méthodes push en employant ces contrôles uniquement s'ils sont garantis. L'investissement dans une solution d'authentification multi-facteurs est habituellement compensée par ces réductions de coûts, ainsi que par la baisse des charges administratives en raison de l'intervention réduite du support technique.

UNE MEILLEURE EXPÉRIENCE UTILISATEUR

Pour l'utilisateur, expérience exceptionnelle rime avec accès aux informations dont il a besoin, où et quand il en a besoin. C'est ce qu'offre l'authentification multi-facteurs, de manière fluide et sécurisée. Grâce à la flexibilité de choix parmi plusieurs mécanismes d'authentification selon les préférences et contraintes de vos utilisateurs, l'authentification multi-facteurs vous permet de proposer le type d'expérience qu'ils attendent avec le niveau de sécurité que vous exigez.

Une entreprise en contact avec la clientèle a tout intérêt à intégrer l'authentification multi-facteurs à son application mobile. Cela permet aux clients de se connecter de manière sécurisée sans devoir télécharger une application tierce d'authentification ou utiliser un second facteur moins fiable.

03

VOTRE SÉCURITÉ AU NIVEAU SUPÉRIEUR

Lorsque vous choisissez la méthode d'authentification adaptée à votre entreprise, vous devez examiner un certain nombre de facteurs. Cette liste non exhaustive vous en propose quelques-uns, parmi les plus importants :

- **Performance :** Protège-t-elle bien des menaces courantes ?
- **Coûts informatiques et charges :** Quel est le coût par utilisateur ? Nécessite-t-elle des ressources supplémentaires ? Possède-t-elle un SDK mobile permettant d'intégrer l'authentification multi-facteurs à vos propres applications mobiles ?
- **Convivialité :** Les utilisateurs pourront-ils facilement l'adopter ? Pourront-ils choisir parmi plusieurs mécanismes d'authentification ?
- **Facilité de mise en œuvre :** Son déploiement et sa maintenance sont-ils simples ?
- **Conformité :** Est-elle conforme aux standards que vous devez respecter ?
- **Standards :** Prend-elle en charge les standards d'identité tels que FIDO ?
- **Flexibilité :** Prendra-t-elle en charge l'authentification dynamique par étapes ?

Le dernier point concerne l'utilisation d'une authentification basée sur les risques (ou par étapes) afin d'évaluer de manière dynamique le risque associé à la demande et d'appliquer uniquement le niveau nécessaire de sécurité. Pour améliorer votre propre sécurité et expérience utilisateur, vous pouvez combiner l'authentification par étapes et des mécanismes contextuels passifs.

L'authentification multi-facteurs contextuelle collecte et analyse de manière passive des facteurs contextuels, comportementaux ou corrélés, comme la géolocalisation, l'environnement informatique et la nature de la transaction concernée. Elle collecte des données sur l'utilisateur afin d'établir un profil comportemental type. Si le comportement de l'utilisateur ne correspond pas à ce profil type, il nécessite une authentification par étapes. Ces opérations étant invisibles pour l'utilisateur, l'expérience n'est pas affectée, elle est aussi extrêmement fiable et présente une moindre vulnérabilité aux attaques.

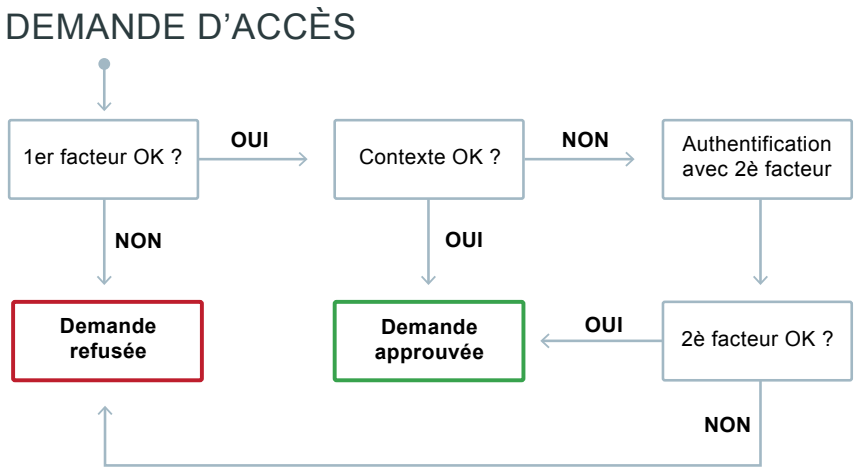

Figure 2 : L'authentification multi-facteurs par étapes, basée sur les risques, résulte d'un contexte ou d'un comportement atypique et anormal. C'est uniquement lorsque le contexte produit par le premier facteur d'authentification indique quelque chose d'inattendu qu'un second facteur est requis avant que l'accès ne soit autorisé.

04

AU-DELÀ DES MOTS DE PASSE

Selon le dernier rapport DBIR de Verizon, 81 % des failles en entreprise sont dues à des identifiants faibles ou dérobés. Et bon nombre d'entre elles, si ce n'est toutes, auraient pu être évitées grâce à une méthode d'authentification plus forte.

En authentifiant les utilisateurs sur ce qu'ils savent (comme un mot de passe), en combinaison avec ce qu'ils ont ou ce qu'ils sont, l'authentification multi-facteurs fournit un niveau supérieur de sécurité contre les attaques. Appliquer par étapes l'authentification multi-facteurs avec une approche basée sur les risques via une authentification contextuelle passive offre la combinaison idéale de sécurité, convivialité et rentabilité.

Si vous êtes prêts à aller au-delà des mots de passe, et cela ne fait aucun doute, nous vous invitons à découvrir comment l'authentification multi-facteurs peut renforcer votre approche en matière de sécurité. Lisez notre Ultimate Guide consacré à l'authentification des utilisateurs dans l'entreprise pour en savoir plus.