Authentication Multifacteur (MFA)

Authentification & Sécurité

Face à la croissance des cybermenaces, le recours à une authentification simple (par mot de passe) expose les comptes des utilisateurs à des menaces, notamment, les attaques par brute force, le phishing et l'usurpation d'identité. Par conséquent, l'adoption de l'authentification multi-facteurs (MFA) est nécessaire en particulier pour renforcer la sécurité des comptes.

Qu'est-ce que la MFA et comment fonctionne-t-elle ?

La **MFA** est une **méthode d'authentification** qui exige que l'utilisateur fournisse **plusieurs facteurs de vérification** (au moins deux) d'identité avant d'accéder à une ressource (application, messagerie, etc.). Ces facteurs appartiennent à l'une des catégories suivantes :

- **Un facteur de connaissance (ce que l'on connaît) :** un mot de passe, une expression, un code PIN, etc.
- **Un facteur de possession (ce que l'on possède) :** un smartphone, un ordinateur, un badge, etc.
- **Un facteur d'héritage (ce que l'on est) :** une empreinte digitale, la reconnaissance faciale, etc.

Avantages de la MFA

- **Réduction du risque de compromission des comptes :** En obligeant les utilisateurs à fournir des informations supplémentaires pour prouver leur identité, la MFA réduit les risques d'usurpation d'identité et d'accès illégitime aux données sensibles.
- **Flexibilité et personnalisation :** La MFA offre une gamme d'options d'authentification, permettant aux entreprises de choisir celles qui conviennent le mieux à leurs besoins et à ceux de leurs utilisateurs.
- **Compatibilité avec le Single Sign-On (SSO) :** La MFA peut être intégrée au SSO, simplifiant ainsi l'accès aux multiples applications tout en garantissant une sécurité accrue.
- **Conformité réglementaire :** Dans de nombreux secteurs l'utilisation de la MFA est souvent exigée pour se conformer aux normes de sécurité et aux réglementations en vigueur.

Bonnes pratiques dans le cadre de la MFA

- **Activer la MFA pour tous les comptes :** Assurez-vous d'activer l'Authentification Multifacteur pour tous les comptes en particulier pour les comptes les plus sensibles (ex : comptes d'administration).
- **Utiliser une combinaison de différents types de facteurs d'authentification :** Privilégiez une combinaison de facteurs différents, tels que quelque chose que vous savez, quelque chose que vous possédez, et éventuellement quelque chose que vous êtes.
- **Privilégier l'utilisation de moyens d'authentification sécurisés :** Utilisez des applications d'authentification qui permettent de générer des codes d'authentification ou des outils d'identification physique (ex : carte CPS) permettant une protection notamment contre les attaques de phishing et de logiciels malveillants.
- **Sécurisation des appareils :** Assurez-vous que les appareils utilisés pour recevoir les codes d'authentification sont sécurisés avec des mots de passe forts et des fonctionnalités de verrouillage automatique.
- **Surveillance des tentatives d'authentification :** Configurez des alertes pour être informé en cas de tentatives d'authentification suspectes ou inhabituelles.

Ressources mises à disposition

- **Le guide de l'ANSSI** présentant des recommandations sur l'authentification MFA et par mot de passe [PDF]
- La **CNIL** qui propose un document visant à sensibiliser à l'utilisation de la MFA [Site WEB]
- **Le NIST** qui fournit des recommandations détaillées pour mettre en place l'authentification multi-facteurs [Site WEB]
- **L'OWASP** qui propose un document autour des bonnes pratiques pour l'authentification multi-facteurs [Site WEB]