Sarah Nouvian
SIO2

Compte rendu de veille informatique

Thème : L'authentification multifacteur (MFA) et son importance en cybersécurité

1. Introduction

Dans le cadre de ma veille informatique, j'ai choisi de m'intéresser à un sujet essentiel mais accessible : l'authentification multifacteur (MFA).

Avec l'augmentation des cyberattaques (phishing, vols de mots de passe, piratages de comptes), les entreprises comme les particuliers doivent renforcer leur sécurité. La MFA est aujourd'hui l'une des solutions les plus simples et les plus efficaces pour protéger les accès.

L'objectif de cette veille est de comprendre :

- ce qu'est la MFA,
- pourquoi elle est importante,
- quelles sont les méthodes existantes,
- comment elle est utilisée en entreprise,
- quelles sont les tendances actuelles.

2. Méthodologie de veille

Pour mener cette veille, j'ai consulté différentes sources d'informations :

- Sites spécialisés en cybersécurité (Cnil.fr, Cert-FR, ZDNet, Cybermalveillance.gouv.fr)
- Blogs technologiques (LeBigData.fr, JournalDuNet)
- Actualités informatiques récentes
- Vidéos explicatives (chaînes de vulgarisation informatique)

Sarah Nouvian
SIO2

J'ai utilisé Google Alertes et les newsletters de la CNIL pour rester informée automatiquement des nouveaux articles liés à la cybersécurité et à l'authentification.

3. Définition de la MFA

La Multi-Factor Authentication, ou authentification multifacteur, consiste à sécuriser un compte en demandant au moins deux preuves d'identité différentes, par exemple :

1. Ce que l'utilisateur connaît :
    - mot de passe, code PIN
2. Ce que l'utilisateur possède :
    - smartphone
    - code reçu par SMS
    - application d'authentification (Google Authenticator, Microsoft Authenticator)
    - clé de sécurité USB (type Yubikey)
3. Ce que l'utilisateur est :
    - empreinte digitale
    - reconnaissance faciale
    - données biométriques

4. Pourquoi la MFA est-elle importante ?

Lors de ma veille, plusieurs points clés reviennent :

- 80 % des piratages de comptes sont liés à un mot de passe faible ou volé.
- Même un bon mot de passe peut être compromis par hameçonnage.
- La MFA réduit considérablement le risque : même si un pirate obtient le mot de passe, il lui manque le deuxième facteur.

Sarah Nouvian
SIO2

La MFA est aujourd'hui recommandée par :

- l'ANSSI
- la CNIL
- les grandes entreprises du numérique
- les plateformes bancaires

De nombreuses attaques récentes auraient pu être évitées grâce à cette mesure simple.

5. Les différentes méthodes de MFA

J'ai identifié plusieurs méthodes utilisées aujourd'hui :

Code SMS

- La plus courante
- Simple à mettre en place
- Mais vulnérable au vol de carte SIM ou à l'interception

Application d'authentification

- Génère des codes temporaires
- Plus sécurisée que le SMS
- Fonctionne même sans connexion internet

Notification "push"

- L'utilisateur valide sur son téléphone : "Oui, c'est bien moi"
- Rapide et pratique

Clé de sécurité physique (U2F, FIDO2)

- Très forte sécurité

- Recommandée pour les administrateurs et les entreprises

Biométrie

- Empreinte digitale, visage
- Très utilisée sur les smartphones

6. Utilisation en entreprise

Les entreprises adoptent de plus en plus la MFA pour protéger :

- Les accès aux outils internes
- Les comptes administrateurs
- Les applications cloud (Microsoft 365, Google Workspace)
- Les solutions VPN

La tendance actuelle est de passer vers un modèle “Zero Trust”, où chaque accès doit être vérifié systématiquement.

7. Limites et difficultés

Même si la MFA est efficace, ma veille souligne quelques limites :

- Certains utilisateurs trouvent cela contraignant.
- Le SMS n’est pas totalement sécurisé.
- Certaines entreprises n’ont pas encore déployé la MFA par manque de moyens ou de formation.
- La MFA peut être contournée par des attaques avancées (MFA fatigue, phishing spécialisé), d’où l’importance de sensibiliser les utilisateurs.

8. Tendances actuelles et futures

Selon les articles consultés, les tendances sont :

- Le passage à la “passwordless authentication” (connexion sans mot de passe, uniquement avec biométrie + clé FIDO2)
- L’intégration automatique de la MFA dans les services en ligne
- L’utilisation de l’intelligence artificielle pour détecter les connexions suspectes
- Le renforcement des normes de sécurité en Europe

9. Conclusion

Cette veille m’a permis de comprendre l’importance croissante de l’authentification multifacteur dans la cybersécurité moderne.

La MFA est aujourd’hui un outil essentiel pour sécuriser les comptes professionnels comme personnels.

Les entreprises la généralisent, les particuliers y ont accès plus facilement, et les évolutions technologiques tendent vers une sécurité renforcée et plus simple d’utilisation.

Cette veille m’a aussi aidée à mieux comprendre les enjeux actuels de la cybersécurité, un domaine incontournable dans le BTS SIO.