TAMDA Zohir
BTS SIO 1
Bloc 3 - Cybersécurité

Le 14 janvier 2024

Conseils sur l'authentification

Sommaire

Recommandations

Pour obtenir une authentification forte, il y a au minimum 8 recommandations qui sont indispensables, selon l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

Premièrement, il faut utiliser un mot de passe différent pour chaque compte qu'on utilise car cela permet de réduire le risque de piratage de comptes.

Deuxièmement, éviter au maximum de se connecter au réseau public et aux réseaux inconnus car les attaquants utilisent ces réseaux pour voler les informations sensibles des utilisateurs. Il est possible de se protéger en utilisant un VPN (Virtual Private Network) qui sécurise les échanges d'informations.

La troisième recommandation de l'ANSSI consiste à éviter de se rendre sur des faux sites car ces dernières peuvent dangereusement collecter des informations sensibles comme l'adresse email, le mot de passe, le numéro de téléphone voire des informations bancaires. Pour éviter cela, il faut aller sur les sites de confiance.

Quatrièmement, il est nécessaire de maîtriser les informations que l'on diffuse sur Internet car elles peuvent être visibles par d'autres utilisateurs, y compris des organisations.

Cinquièmement, activer une double authentification est recommandé par l'ANSSI car cela permet d'ajouter une couche de sécurité au compte.

La sixième recommandation est de mettre à jour régulièrement les logiciels qu'on utilise, ceux qui ne sont pas utilisés doivent être supprimés, ce qui permet de limiter les vulnérabilités.

Septièmement, il faut séparer les informations personnelles des informations à caractères professionnelles pour être anonyme.

Dernièrement, l'ANSSI recommande de surveiller les équipements informatiques car une personne mal intentionnée peut les utiliser pour voler les informations personnelles.

Stratégie & méthodes

Pour utiliser un mot de passe plus robuste, il faut le générer en utilisant des lettres, des chiffres ainsi que des caractères spéciaux aléatoires avec une taille raisonnable (*12 au minimum, selon la CNIL*). On évite ainsi l'utilisation des mots qui référencent à des informations personnelles (nom, prénom, date de naissance, département...) dans un mot de passe.

Lorsqu'il a été généré, on peut le stocker dans une base de données. Pour cela, on peut utiliser des gestionnaires de mots de passe comme KeePass, 1Password ou Bitwarden. Ces logiciels les chiffrent pour la protection et peuvent être déchiffrés avec une passphrase.

On peut aussi utiliser l'authentification à double facteurs (A2F) pour mieux sécuriser le compte.

Webographie

https://cyber.gouv.fr/bonnes-pratiques-protegez-vous

https://cyber.gouv.fr/dix-regles-dor-preventives

https://www.blogdumoderateur.com/tools/productivite/gestionnaire-mots-de-passe

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe

https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite