|  |  |
| --- | --- |
| Mission 5 – Améliorer la sécurisation des informations | **LLMECA** |
| Durée : 30’ | Homme avec un remplissage uniouDeux hommes avec un remplissage uni | Source |

**Contexte professionnel**

L'entreprise accueille régulièrement des stagiaires dont les compétences en matière de sécurité informatique ne sont pas toujours au niveau des exigences souhaitées. Par ailleurs, les responsables de service ne sont pas suffisamment vigilants dans les habilitations accordées aux stagiaires. Le responsable du SI vous demande de rédiger une note d’information destinée aux responsables de services afin qu’ils définissent mieux les habilitations accordées aux stagiaires à l’aide d’un profil type et une autre destinée aux stagiaires pour les aider à créer leur mot de passe lequel devra être communiqué au responsable informatique sous peine de voir le compte bloqué.

**Travail à faire**

1. Concevez la note d’information destinée aux chefs de services.
2. Concevez la note d’information destinée aux stagiaires.

**Doc. 1 Créer un mot de passe fort en 7 étapes**

*Source : Terranovasecurity.com*

1. **N’utilisez pas des lettres ou des nombres séquentiels :** n’utilisez pas 1234, azerty, jklm…
2. **N’utilisez pas votre date de naissance :** les cybercriminels peuvent facilement trouver cette information en fouillant vos réseaux sociaux.
3. **Utilisez une combinaison d’au moins huit lettres, nombres et symboles :** plus votre mot de passe est long et varié, plus il est difficile à deviner. Par exemple, *M0i#eb9Qv?* utilise une combinaison unique de lettres majuscules et minuscules, de nombres et de symboles.
4. **Combinez différents mots sans rapport dans votre mot ou phrase de passe : i**l est alors plus difficile pour les cybercriminels de le deviner. N’utilisez pas de phrases tirées de chansons, films ou émissions de télévision populaires. Choisissez trois ou quatre mots plus longs pour créer votre phrase de passe. Par exemple, *9AraignEeKetomarGiN*.
5. **N’utilisez pas des noms ou des mots trouvés dans le dictionnaire :** substituez les lettres par des nombres ou des symboles pour que le mot de passe soit plus difficile à deviner. Ou faites délibérément des fautes d’orthographe dans votre mot ou phrase de passe. Par exemple, *C0urAr!3re* pour « cour arrière ».
6. **Utilisez un gestionnaire de mot de passe :** évitez de conserver vos mots de passe dans un fichier sur votre ordinateur. Assurez-vous d’utiliser l’outil de gestion des mots de passe fourni par l’équipe de soutien informatique pour sauvegarder tous vos mots de passe professionnels et personnels.
7. **Évitez de réutiliser vos mots de passe :** prévoyez un mot de passe ou un code PIN unique pour chaque appareil, application, site Web et logiciel. Si un cybercriminel réussit à deviner un de vos mots de passe, il tentera de pirater tous vos comptes professionnels et personnels.

**Doc. 2 Gérer les comptes utilisateurs**

*Source : www.cnil.fr*

Les **habilitations** doivent adaptés au poste occupé par l’employé.

**Les précautions élémentaires :**

* Définir des profils d’habilitationdans les systèmes en séparant les tâches et les domaines de responsabilité, afin de limiter l’accès des utilisateurs aux seules données strictement nécessaires à l’accomplissement de leurs missions.
* Supprimer les permissions d’accès des utilisateurs dès qu’ils ne sont plus habilités à accéder à un local ou à une ressource informatique, ainsi qu’à la fin de leur contrat.
* Réaliser une revue annuelle des habilitationsafin d’identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

**Ce qu’il ne faut pas faire :**

* Créer ou utiliser des comptes partagés par plusieurs personnes.
* Donner des droits d’administrateurs à des utilisateurs n’en ayant pas besoin.
* Accorder à un utilisateur plus de privilèges que nécessaire.
* Oublier de retirer des autorisations temporaires accordées à un utilisateur (pour un remplacement, par exemple).
* Oublier de supprimer les comptes utilisateurs des personnes ayant quitté l’organisation ou ayant changé de fonction.

**Pour aller plus loin :**

Établir, documenter et réexaminer régulièrement **une politique de contrôle d’accès**en rapport avec les traitements mis en œuvre par l’organisation qui doit inclure :

* Les procédures à appliquer systématiquement à l’arrivée ainsi qu’au départ ou au changement d’affectation d’une personne ayant accès aux données à caractère personnel ;
* Les conséquences prévues pour les personnes ayant un accès légitime aux données en cas de non-respect des mesures de sécurité ;
* Les mesures permettant de restreindre et de contrôler l’attribution et l’utilisation des accès au traitement.

**Réponses**

1. Concevez la note d’information destinée aux chefs de services.
2. Concevez la note d’information destinée aux stagiaires.