Synthèse Mission 7:

Module 4 - Sécurité du poste de travail et nomadisme

- ## Applications et mise à jour

Lors d'une utilisation prudente d'Internet, il reste possible d'avoir affaire à des fichiers corrompus. En effet, les personnes cherchant à mieux connaître les systèmes informatiques que nous utilisons tous les jours sont nombreuses. Il peut s'agir de criminels, d'organisations mafieuses, de services de renseignement mais aussi de chercheurs du domaine privé ou universitaire.Quel que soit le profil de la personne qui travaille sur cette recherche, une fois qu'une défaillance est détectée dans la sécurité du système, on parle de vulnérabilité.

Il existe deux types de chercheurs de vulnérabilités : les "black hats," qui exploitent les failles pour des fins malveillantes, et les "white hats," qui les signalent aux éditeurs pour renforcer la sécurité. Les vulnérabilités étant courantes, il est essentiel de maintenir les systèmes à jour rapidement pour éviter qu'un attaquant n'exploite les failles sur des systèmes non protégés. La mise à jour automatique est fortement recommandée, surtout si elle n'est pas gérée par un service informatique centralisé, car elle assure que les appareils sont homogènes et sécurisés sans intervention directe.

Lorsque vous mettez à jour manuellement, vérifiez la disponibilité des correctifs directement depuis le logiciel ou sur le site de l'éditeur pour éviter les risques de programmes malveillants. En entreprise, un service informatique est idéal pour gérer les installations, mais si cela n'est pas possible, adoptez de bonnes pratiques : limitez le nombre de logiciels, installez uniquement depuis des sources fiables, et évitez les programmes inutiles.

Pour résumer, la protection contre les failles dépend de la rapidité de mise à jour et de la prudence dans le choix des logiciels. Les éditeurs et chercheurs travaillent en continu pour sécuriser les applications, mais les attaquants sont aussi actifs. Ainsi, il est crucial de ne pas bloquer les mises à jour, de privilégier les sources sûres et d'éviter les installations superflues pour garantir la sécurité de vos systèmes.

- ## Options de configuration de base

La configuration de base d'un terminal, dès le premier démarrage, commence par l'activation du système et le paramétrage des langues, fuseaux horaires, et connexion réseau. Une fois le terminal initialisé, la mise en place de **méthodes de déverrouillage et d'authentification** est essentielle, incluant l'activation de mots de passe robustes, d'identification biométrique (empreinte digitale ou reconnaissance faciale), ou de codes PIN pour limiter l'accès.

Les logiciels de sécurité viennent ensuite renforcer la protection des appareils : installation d'un antivirus, activation du pare-feu, et configuration d'un anti-malware pour détecter et prévenir les attaques. La configuration des **options de sécurité spécifiques aux données mobiles** comprend la gestion des autorisations d'applications, l'activation de la localisation

pour le suivi en cas de perte ou de vol, et le contrôle de l'accès aux informations sensibles (contacts, messages, etc.).

Le **chiffrement de l'appareil** est une autre mesure essentielle : il protège les données en les rendant illisibles sans clé de déchiffrement, ce qui garantit leur confidentialité, même en cas de perte. Ces options de base permettent de sécuriser les données et d'assurer une utilisation efficace et sécurisée des terminaux dans un environnement professionnel.

● Configurations complémentaires

En complément des configurations de base, les **configurations complémentaires** permettent une gestion avancée des comptes utilisateurs, la sécurisation des accès, et la sauvegarde des données pour assurer la continuité des services.

- **Gestion de base des comptes utilisateurs** : consiste à créer et supprimer des comptes, à définir des mots de passe et des droits d'accès pour chaque utilisateur afin de contrôler l'accès aux ressources. La gestion des groupes simplifie les permissions et les politiques de sécurité en attribuant des accès par ensemble d'utilisateurs.
- **Gestion avancée des comptes utilisateurs** : inclut la configuration de profils itinérants (pour permettre aux utilisateurs d'accéder à leurs paramètres sur différents appareils), la mise en place de politiques de sécurité (mots de passe complexes, expiration des mots de passe, tentatives de connexion limitées), et l'utilisation de l'authentification à plusieurs facteurs (MFA) pour renforcer la sécurité des accès.
- **Sauvegarde et connexion de l'appareil** : il est essentiel d'établir des stratégies de sauvegarde automatique pour protéger les données en cas de panne. La sauvegarde sur un serveur dédié ou dans le cloud permet une récupération rapide et sécurisée. Enfin, les connexions doivent être sécurisées via VPN ou réseaux privés pour les accès distants, limitant ainsi les risques d'intrusions.

Ces configurations assurent la sécurité, la flexibilité et la continuité des services dans un environnement professionnel.

● Sécurité des périphériques amovibles

La **sécurité des périphériques amovibles** est cruciale pour protéger les données et éviter les menaces en entreprise.

- **Risques au branchement** : les périphériques amovibles (clés USB, disques externes) peuvent introduire des malwares ou faciliter le vol de données sensibles lors de la connexion ; il est recommandé d'analyser ces périphériques avec un antivirus avant de les utiliser.
- **Chiffrement des périphériques de stockage amovibles** : chiffrer les données stockées sur les périphériques amovibles garantit leur confidentialité, car seules les personnes autorisées peuvent y accéder, même en cas de perte ou de vol.
- **Durabilité** : les périphériques doivent être de bonne qualité et régulièrement contrôlés pour éviter les risques de corruption de données dues à l'usure, car ils sont souvent transportés et exposés à des conditions variables.
- **Séparation des usages** : il est conseillé de distinguer les périphériques à usage personnel de ceux à usage professionnel afin d'éviter le mélange des données et de réduire les risques d'infection d'un environnement à un autre.

- **Effacement sécurisé** : lors de la réutilisation ou de la mise au rebut d'un périphérique amovible, l'effacement sécurisé des données garantit qu'elles ne peuvent pas être récupérées, protégeant ainsi la confidentialité de l'entreprise.

Ces pratiques assurent une utilisation plus sûre et contrôlée des périphériques amovibles dans un environnement professionnel.

• Séparation des usages

La **séparation des usages** entre vie personnelle et professionnelle est une mesure essentielle pour sécuriser les systèmes d'information et éviter les risques de compromission des données.

- **Mélange des usages et ses dangers** : lorsqu'un même appareil (ordinateur, smartphone) est utilisé pour des activités personnelles et professionnelles, les risques augmentent de manière significative. Un fichier infecté, un lien malveillant, ou des applications non contrôlées peuvent compromettre la sécurité de l'appareil et des données professionnelles sensibles, rendant l'entreprise vulnérable aux cyberattaques.
- **Étude de cas** : de nombreux cas réels montrent les conséquences du mélange des usages, comme des entreprises ayant subi des fuites de données après qu'un collaborateur a ouvert un email personnel piégé ou installé un logiciel non sécurisé. Ces incidents rappellent l'importance de séparer les usages pour minimiser les risques.
- **Bonnes pratiques** : il est conseillé de fournir des appareils dédiés aux tâches professionnelles et de restreindre l'accès aux ressources personnelles sur ces équipements. L'utilisation de profils distincts, l'application de politiques de sécurité spécifiques, et la sensibilisation des utilisateurs aux risques contribuent à réduire le mélange des usages.

En structurant ainsi les usages, l'entreprise améliore la sécurité, évite les erreurs coûteuses et assure la protection des informations sensibles.