Installation sécurisée : Concept clés

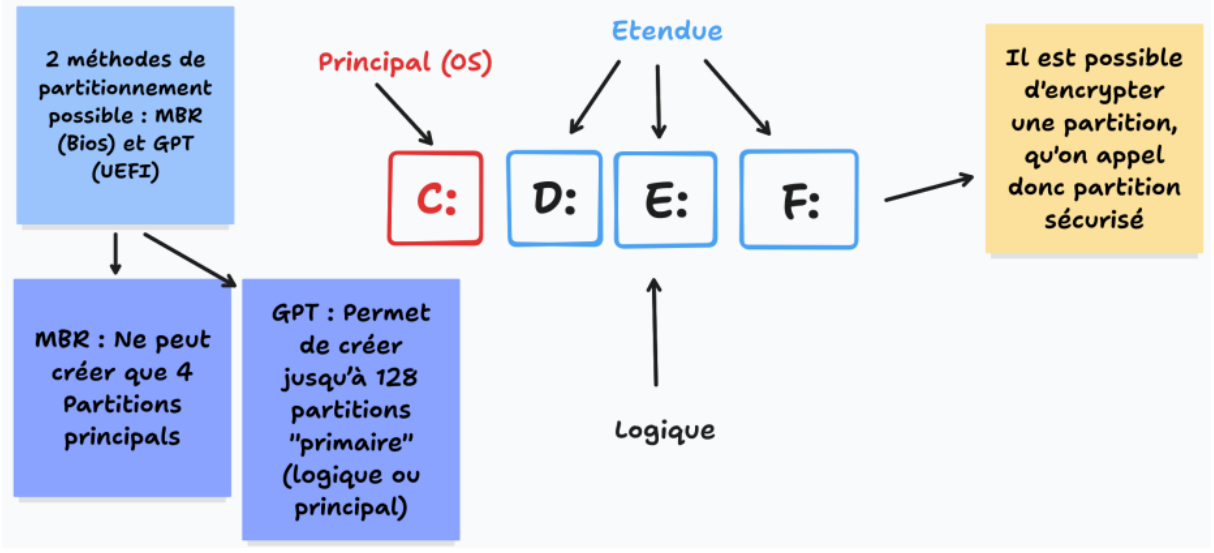
Partitionnement sécurisé

Définition et types (principale, étendue, logique)

Le partitionnement est une technique qui consiste à diviser un disque dur en plusieurs sections indépendantes, appelées partitions. Cela permet une meilleure organisation des données et peut améliorer la sécurité et les performances du système.

Il existe trois principaux types de partitions :

-Partition principale : C'est la partition de base qui peut contenir un système d'exploitation. Un disque peut avoir plusieurs partitions principales, mais une seule peut être active à la fois.
-Partition étendue : Elle sert à contourner la limite du nombre de partitions principales. Une partition étendue peut contenir plusieurs partitions logiques.
-Partition logique : Située à l'intérieur d'une partition étendue, elle permet de créer plusieurs espaces de stockage indépendants sans dépasser la limite des partitions principales.



Stratégies de partitionnement optimisé pour sécurité/performance

Quelques stratégies recommandées :

-Séparation des données sensibles : Stocker les fichiers système et les données utilisateur sur des partitions distinctes permet de limiter les risques en cas de corruption ou d'attaque.
-Utilisation de partitions dédiées : Une partition spécifique pour les fichiers temporaires ou les journaux système peut éviter l'encombrement du disque principal et améliorer la réactivité.
-Chiffrement des partitions : Protéger les données sensibles avec un chiffrement robuste renforce la sécurité contre les accès non autorisés.
-Optimisation des performances : Un partitionnement bien pensé peut réduire la fragmentation des fichiers et accélérer l'accès aux données, notamment en utilisant des systèmes de fichiers adaptés à chaque type de partition.

Source :

Datacamp, *Microsoft*, *Datasunrise*

Chiffrement

Introduction à BitLocker (Windows) et LUKS (Linux)

Le chiffrement est une technique essentielle pour protéger les données contre les accès non autorisés.

Deux solutions populaires sont :

-BitLocker (Windows) : Un outil de chiffrement intégré aux versions professionnelles et entreprises de Windows. Il utilise le chiffrement AES et peut être activé avec un module TPM pour une sécurité renforcée.
-LUKS (Linux Unified Key Setup) : Une solution standardisée pour le chiffrement des disques sous Linux. Elle permet de protéger les partitions avec des clés de chiffrement robustes et prend en charge plusieurs phrases de passe

Pourquoi et comment chiffrer les données ?

Le chiffrement garantit la confidentialité et l'intégrité des informations stockées sur un disque dur ou un périphérique externe.

Il est particulièrement utile pour :

-Protéger les données sensibles contre le vol ou l'accès non autorisé.
-Sécuriser les appareils mobiles en cas de perte ou de vol.
-Empêcher les attaques par accès physique sur les disques durs et les clés USB.

Chiffrer les données :

-Avec BitLocker : Activez BitLocker via le panneau de configuration Windows, choisissez un mode de protection (mot de passe, clé USB ou TPM) et laissez Windows chiffrer le disque.
-Avec LUKS : Utilisez la commande cryptsetup luksFormat pour initialiser le chiffrement d'une partition, puis cryptsetup open pour y accéder après authentification.

Source :

Redhat, *Tremplin-numérique*

Importance des mises à jour critiques

Risques liés aux systèmes non mis à jour

Ne pas appliquer les mises à jour expose les systèmes à plusieurs dangers :

-Vulnérabilités exploitables : Les cyberattaquants peuvent utiliser des failles connues pour infiltrer un système.

-Perte de données : Un système non sécurisé peut être victime de ransomwares ou d'autres formes de cyberattaques.

-Incompatibilités et dysfonctionnements : Les logiciels obsolètes peuvent ne plus fonctionner correctement avec les nouvelles technologies.

-Non-conformité réglementaire : Certaines mises à jour sont nécessaires pour respecter les normes de protection des données.

Bonnes pratiques d'application des mises à jour

Pour garantir une mise à jour efficace et sécurisée, voici quelques recommandations :

-Automatiser les mises à jour pour éviter les oublis et garantir une protection continue.

-Télécharger uniquement depuis des sources officielles pour éviter les logiciels malveillants.

-Tester les mises à jour sur un environnement de préproduction avant de les appliquer sur des systèmes critiques.

-Planifier les mises à jour en dehors des heures de production pour minimiser les interruptions.

-Maintenir une veille sur les correctifs publiés par les éditeurs de logiciels et les organismes de cybersécurité.

Source :

Cybermalveillance, *Industriel.esante.gouv.fr*, *Zenops*

Gestion des pilotes officiels

Pourquoi utiliser les pilotes certifiés par le fabricant

Les pilotes sont des logiciels essentiels qui permettent à un système d'exploitation de communiquer avec le matériel.

Utiliser des pilotes certifiés par le fabricant présente plusieurs avantages :

-Compatibilité garantie : Les pilotes officiels sont conçus pour fonctionner de manière optimale avec le matériel spécifique.

-Stabilité et performance : Les fabricants testent leurs pilotes pour éviter les conflits et assurer une bonne performance.

-Sécurité renforcée : Les pilotes certifiés sont vérifiés pour éviter les failles exploitables par des logiciels malveillants.

-Mises à jour et support : Les fabricants publient régulièrement des mises à jour pour corriger les bugs et améliorer la compatibilité avec les nouvelles versions de Windows ou Linux.

Risques des pilotes non officiels

L'installation de pilotes provenant de sources non officielles peut entraîner plusieurs problèmes :

-Failles de sécurité : Certains pilotes non officiels peuvent contenir des logiciels malveillants ou des portes dérobées.

-Instabilité du système : Un pilote non testé peut provoquer des erreurs, des plantages ou des écrans bleus.

-Incompatibilité matérielle : Un pilote non certifié peut ne pas fonctionner correctement avec le matériel, entraînant des dysfonctionnements.

-Absence de support : En cas de problème, il est difficile d'obtenir une assistance ou des mises à jour correctives.

Source :

Android Ouest France, *Microsoft*