ASSURMER

LA MISE A DISPOSITION DES NOUVEAUX EQUIPEMENTS AUX UTILISATEURS

LE CLAINCHE
Killian

Date :
08/12/2023

Sommaire

I. Bonne pratiques relatives à la sécurité de l'équipement

A) Mise en place d'un mot de passe UEFI

Afin de renforcer la sécurité des tablettes dès le démarrage, nous avons configuré un mot de passe administrateur dans l'interface **UEFI** (BIOS) de chaque appareil.
Voici les détails de cette configuration :

- **Un mot de passe unique pour toutes les tablettes**, répondant aux critères suivants :
    - Longueur minimale de 18 caractères.
    - Utilisation combinée de majuscules, de minuscules et de chiffres.
- **Fonctionnalités sécurisées** :
    - Le mot de passe UEFI verrouille toutes les modifications de paramètres et fonctionnalités du BIOS.
    - Les utilisateurs peuvent accéder et consulter les paramètres du BIOS, mais aucune modification n'est possible sans fournir le mot de passe administrateur.

Objectif : Cette protection vise à prévenir toute tentative d'accès non autorisé au BIOS, que ce soit par un collaborateur mal intentionné ou une personne externe. Elle empêche ainsi toute manipulation susceptible de compromettre la sécurité des données ou des systèmes d'exploitation.

B) Chiffrement des disques via BitLocker

Pour renforcer davantage la sécurité des données, nous avons opté pour l'utilisation de **BitLocker**, la solution de chiffrement intégrée à Windows.

Principaux avantages de BitLocker :

- **Chiffrement complet du disque** :
    - Protège l'ensemble des données, y compris le système d'exploitation, les fichiers système et les données utilisateur.
    - Rend les données inaccessibles sans la clé de déchiffrement, même en cas de vol ou de perte de la tablette.
- **Sécurité renforcée** : Empêche les accès non autorisés aux données sans la clé de récupération.

Problème rencontré :
Nous avons toutefois identifié une problématique concernant le stockage des clés de récupération BitLocker. Différentes options de sauvegarde existent, mais elles se sont avérées peu pratiques ou non adaptées à nos besoins :

1. **Sauvegarde sur clé USB ou fichier local** : Jugée peu sécurisée et difficile à gérer pour un grand nombre de tablettes.
2. **Impression des clés de récupération** : Irréalisable en raison du temps et des efforts nécessaires.

Solution envisagée :
Une option réellement viable serait d'enregistrer les clés de récupération via **Azure Active Directory (Azure AD)**.
De plus, la sauvegarde sur un NAS pourrait aussi être envisager.

Cependant, nous ne disposons actuellement pas d'un environnement Azure AD et d'un NAS. Ces solutions pourraient être envisagées à l'avenir si nous décidons d'implémenter **Azure Active Directory** ou un NAS dans nos infrastructures.