Guide
Propre infrastructure

Que vous utilisiez votre propre serveur ou que toute votre infrastructure soit hébergée et gérée pour vous par votre partenaire informatique : Certains appareils se trouvent toujours chez vous. Vous trouvez dans ce guide les points qu'il est important de savoir.

1. Disques durs non cryptés

Si vous utilisez des notebooks et que vous stockez des données localement sur ces appareils, il est recommandé de crypter les disques durs afin de protéger les données sensibles et d'éviter qu'elles ne tombent entre des mains étrangères, par exemple en cas de perte ou de vol du matériel. Un mot de passe est nécessaire pour décrypter le disque dur. Si vous n'enregistrez pas de données sensibles localement sur votre ordinateur portable ou de bureau, mais que vous les stockez exclusivement chez votre fournisseur informatique ou dans le nuage, aucun cryptage n'est nécessaire. En revanche, si vous enregistrez des fichiers localement, le cryptage du disque dur est indiqué.

Si vous disposez de votre propre infrastructure de serveurs, nous vous recommandons de la faire contrôler par un expert en sécurité.

☞ **Liste de contrôle :**

- □ Vérifiez avec votre partenaire informatique si vous stockez des données localement sur votre PC ou votre ordinateur portable. Le cas échéant, chargez-le de crypter le disque dur.

2. Ecran de veille / verrouillage de l'ordinateur

Lorsqu'ils sont laissés sans surveillance, les ordinateurs et les moniteurs devraient être verrouillés à l'aide d'un écran de veille. Positionnez de plus votre écran de manière à ce que personne ne puisse voir les données.

☞ **Liste de contrôle :**

- □ Activez manuellement l'économiseur d'écran dès que vous quittez votre poste de travail.
- □ Régler la mise en veille de l'écran après 5 minutes d'inactivité pour tous les collaborateurs.

3. Moniteur avec feuille d'écran

Dès que des tiers ont une vue libre sur les moniteurs, les données ne sont plus suffisamment protégées (visual hacking). Cela peut être le cas lors de l'utilisation d'ordinateurs portables dans les transports publics, mais aussi lorsque les écrans sont visibles par exemple à travers des baies vitrées, des portes vitrées ou dans des bureaux partagés avec le public. Le repositionnement des écrans et l'utilisation de films de feuille d'écran permettent de protéger les données de manière adéquate.

☞ **Liste de contrôle :**

- □ Vérifier la possibilité de voir vos écrans à travers les fenêtres, etc. et les repositionner si nécessaire.
- □ Equipez les ordinateurs portables et les tablettes avec des feuilles d'écran.

4. Mots de passe

Les mots de passe tels que « 123456 », « qwertz » et « hello » sont toujours parmi les plus populaires, bien qu'il soit de notoriété publique que des mots de passe plus sûrs devraient être utilisés. Actuellement, il est recommandé de créer des mots de passe comme suit :

- Au moins dix caractères : Cette longueur de mot de passe est nécessaire pour une sécurité moyenne.

- Ils contiennent des lettres majuscules et minuscules, des chiffres et des caractères spéciaux, mais pas d'accents.
- Ils ne contiennent pas de suites de mots figurant dans un dictionnaire.
- Un mot de passe différent est utilisé pour chaque compte. Si un mot de passe est découvert, les autres comptes sont protégés.
- En plus de la protection par mot de passe, une **authentification à deux facteurs** est recommandée.

Comme presque personne ne peut se souvenir de tels mots de passe, il est recommandé d'utiliser un gestionnaire de mots de passe. Il s'agit d'une application ou d'un service en ligne qui stocke tous vos mots de passe de manière cryptée et protégée par un mot de passe. Ce mot de passe est le seul dont vous devez vous souvenir. Pour les données d'accès aux différents comptes, vous pouvez créer des combinaisons de caractères sûres et difficiles à deviner à l'aide du générateur intégré et définir un mot de passe séparé pour chaque accès. En option, de nombreux gestionnaires de mots de passe permettent une authentification à deux facteurs, ce qui assure une protection supplémentaire.

Un partenaire de FIDUCIAIRE|SUISSE, SecureSafe, offre un tel gestionnaire de mots de passe et les membres bénéficient de 10% de rabais : https://www.securesafe.com/fr/fiducaire-suisse

☞ **Liste de contrôle :**

- □ Instaurer un gestionnaire de mots de passe dans votre entreprise.
- □ Fixer aux collaborateurs un délai pour remplacer tous les mots de passe par des mots de passe sûrs.

5. WLAN crypté / WLAN pour les invités

Les réseaux WLAN ouverts sont particulièrement vulnérables aux attaques des pirates informatiques. Pour protéger les données commerciales internes, il est nécessaire de travailler avec une connexion réseau virtuelle privée (VPN). En effet, même si un pirate parvient à intercepter la connexion, les données resteront hautement cryptées. Avec un réseau local sans fil pour invités, les entreprises peuvent accorder aux clients l'accès à Internet sans porter atteinte à la sécurité du réseau domestique. Comme les deux réseaux sont séparés, le pare-feu du routeur intercepte les virus qui pourraient infecter les appareils des clients.

Si vous travaillez à domicile, veillez à protéger votre réseau WLAN par un mot de passe fort.

☞ **Liste de contrôle :**

- □ Éviter les réseaux WLAN publics / désactiver le WLAN dès qu'il n'est plus nécessaire.
- □ Dans le réseau WLAN public, travailler avec une connexion réseau virtuelle privée (VPN).
- □ Mettre en place un WLAN séparé et distinct pour les invités. Adressez-vous à votre partenaire informatique.
- □ Au bureau à domicile, protéger le WLAN avec un mot de passe fort.

6. Utilisation de clés USB et de supports de données étrangers

La prudence est de mise lors de l'utilisation de clés USB étrangères, car l'une des plus anciennes astuces des pirates consiste à accéder au réseau de l'entreprise par le biais d'une clé USB infectée par un logiciel malveillant ou un logiciel espion. Les fabricants proposent des verrous USB qui permettent de verrouiller les entrées USB des PC et des ordinateurs portables. Il s'agit de petits dispositifs qui peuvent être insérés dans les entrées USB. Il est également possible de désactiver les entrées USB directement par le biais d'un logiciel.

☞ **Liste de contrôle :**

- □ Sécuriser les PC non surveillés, par exemple dans les salles de réunion, avec des verrous USB.

7. En déplacement avec le notebook / l'ordinateur portable

En voyage, les données confidentielles tombent souvent entre les mains de personnes non autorisées. Pour éviter cela autant que possible, il convient de respecter les mesures de précaution suivantes :

- Ne jamais laisser les appareils sans surveillance.
- Utiliser une feuille d'écran.
- Ne pas se connecter en ligne avec un réseau WLAN non sécurisé.
- Avant de partir à l'étranger, s'informer sur les risques et les usages du pays de destination en matière de protection des données.
- Dans la chambre d'hôtel, ne jamais laisser son ordinateur portable / notebook ouvert, mais utiliser le coffre-fort.
- Emporter le moins de données possible sur un ordinateur portable aussi « vide » que possible.
- Crypter les données sur le disque dur.