Guide
Infrastructure externe (partenaire informatiques et fournisseurs de nuage / cloud)

De nombreuses sociétés fiduciaires travaillent avec un fournisseur informatique externe qui gère le réseau, installe les logiciels et est également responsable de la sécurité de cette infrastructure. Même si vos systèmes informatiques sont gérés par une entreprise externe ou si vous stockez toutes vos données dans le cloud, il y a tout de même quelques mesures de sécurité et règles à respecter. Celles-ci sont décrites plus en détail dans le guide suivant.

1. Accounts / comptes en ligne

Avec un seul mot de passe pour tous les comptes en ligne, les pirates ont la partie facile. Pour des raisons de sécurité, utilisez un mot de passe différent pour chaque compte. Dans la mesure du possible, ne partagez pas vos comptes en ligne avec d'autres personnes. Chaque collaborateur devrait avoir son propre compte afin qu'il soit possible de savoir qui a été actif et comment.

2. 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/de/treuhand-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.

3. Cryptage des données

La plupart des fournisseurs de cloud proposent un cryptage des données. En règle générale, des procédures de cryptage sont également utilisées lors du transfert des données de votre ordinateur vers le serveur en nuage. Mais comme vous n'avez aucune garantie que des tiers ne puissent pas accéder aux données sur le serveur cloud, il est conseillé de sécuriser en plus les données confidentielles de l'entreprise avec votre propre méthode de cryptage avant même de les télécharger.
Il existe différentes solutions de cryptage à installer sur le terminal et à associer ensuite au service de stockage choisi.

Un outil répandu pour le cryptage est https://www.boxcryptor.com/fr/.

☞ **Liste de contrôle :**

- □ Choisir un fournisseur de cloud avec des procédures de cryptage.
- □ Mettre en place un outil de cryptage des données sensibles.

4. Données à l'étranger

Les entreprises doivent se conformer aux dispositions légales lors de la transmission de données à l'étranger. Lorsque des données personnelles sont transmises ou stockées à l'étranger, elles doivent être protégées contre l'accès des autorités étrangères. En règle générale, les données peuvent être stockées sans problème chez les fournisseurs dont le siège principal se trouve dans l'Union européenne (UE). En cas de traitement des données en dehors de l'Europe, il faut vérifier si les États présentent un niveau de protection des données adéquat. En cliquant sur le lien suivant, vous trouverez une liste d'Etats qui, selon le Préposé fédéral à la protection des données et à la transparence (PFPDT), offrent une protection des données adéquate :

https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html

Selon la Fédération suisse des avocats, si les données sont cryptées avant d'être transmises au fournisseur de services d'informatique en nuage et que ce dernier ne dispose pas de la clé nécessaire pour les décrypter, l'utilisation de services d'informatique en nuage ne pose aucun problème en termes de droit pénal et de protection des données.

☞ **Liste de contrôle :**

- □ Si vous utilisez des services de cloud et stockez des données personnelles, vérifiez qu'une protection des données adéquate est garantie.

5. Back-up (savegarde)

La sauvegarde des données pertinentes est d'une grande importance pour les entreprises, car une perte de données peut avoir de graves conséquences pour l'image et le succès économique d'une entreprise. Les sauvegardes locales et les sauvegardes dans le nuage permettent de remédier à cette situation. Les points suivants doivent être pris en compte lors d'une sauvegarde :

- Le service informatique devrait vérifier régulièrement la fonctionnalité de la sauvegarde en nuage afin que la restauration des données soit facilement réalisable en cas d'urgence.
- périodiquement les prestations de sauvegarde de votre partenaire informatique. Supprimez un fichier test et demandez à votre partenaire informatique de le restaurer.

☞ **Liste de contrôle :**

- □ Notez dans votre agenda au moins deux fois par an un test de votre sauvegarde.

6. Services basés sur le cloud

Dans le cas des services basés sur le cloud, certaines données confidentielles sont transférées à des fournisseurs de cloud externes. Il convient donc de veiller au sérieux des fournisseurs de services en nuage lors de leur sélection.

☞ **Liste de contrôle :**

- □ Certificats et attestations de tiers : le fournisseur de cloud répond-il aux exigences de sécurité nécessaires ?
- □ Communication transparente de la part du fournisseur de cloud : envoi d'informations sur ce qui se passe avec les données de l'entreprise, où elles sont stockées et comment elles sont protégées contre les accès étrangers.
- □ Demander ce qui se passe en cas de cyber-attaque contre le fournisseur de cloud (sauvegarde du cloud, temps d'arrêt, etc.).
- □ Cryptage des données : le fournisseur de cloud prend des mesures pour sécuriser la transmission et le stockage des données.

7. Connexion / authentification sécurisée

Que ce soit sur les réseaux sociaux, chez le fournisseur de cloud ou chez les fournisseurs de services en ligne professionnels : Aujourd'hui, les internautes utilisent quotidiennement de nombreux identifiants. En Allemagne, une personne utilise en moyenne plus de 78 comptes en ligne. Par défaut, la plupart des comptes d'utilisateurs sur le réseau sont protégés par une combinaison de nom d'utilisateur et de mot de passe. Les règles suivantes sont à respecter pour une connexion sécurisée :

- Utiliser un mot de passe différent pour chaque compte (gestionnaire de mots de passe).
- Utiliser des mots de passe « forts ».
- Garder votre login secret.
- Activer la fonction de notification en cas de connexion inhabituelle à votre compte.

Si possible, une authentification à deux facteurs devrait être utilisée. Entre-temps, non seulement les banques, mais aussi de nombreux autres prestataires de services en ligne proposent cette possibilité d'authentification. Elle sert à vérifier l'identité de l'utilisateur. Le deuxième facteur se fait généralement par l'utilisation d'appareils mobiles : des codes sont envoyés aux smartphones par push notification (notification poussée) , un code QR doit être scanné sur l'écran ou une application affiche un code.

☞ **Liste de contrôle :**

- □ Vérifiez vos logins par rapport aux règles mentionnées.
- □ Activez l'authentification à deux facteurs, si elle est disponible.