Guide

Adresses électroniques et transmission de données

Une attention particulière devrait être accordée - outre la protection des données sur vos systèmes - à la transmission électronique des données et des informations : La surface d'attaque sur la voie de transport est particulièrement grande. Les e-mails et autres services de transmission sont souvent utilisés pour pouvoir s'introduire dans un système.

1. Mots de passe des courriels

Un mot de passe est essentiel pour se protéger des hackers. Les mots de passe tels que « 123456 », « qwertz » et « hello » restent parmi les plus populaires, bien qu'il soit de notoriété publique que des mots de passe 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.

2. Cryptage des emails

Le cryptage des e-mails est un sujet important dans le domaine de la sécurité des données, en particulier pour les données personnelles et les données confidentielles des entreprises et des clients. Lors de l'envoi d'informations confidentielles, le cryptage entre les terminaux de l'expéditeur et du destinataire offre une sécurité accrue. Il est recommandé de mettre en œuvre un cryptage uniforme des e-mails au sein de l'entreprise.

☞ Liste de contrôle :

- □ Définir les adresses électroniques pour lesquelles le cryptage doit être utilisé.

- ☐ Guide interne pour les collaborateurs concernant le cryptage des e-mails.
- ☐ Consulter, le cas échéant, un prestataire de services informatiques externe qui s'occupe du cryptage des e-mails.

3. Faux emails / hameçonnage (phishing)

L'hameçonnage est une méthode d'attaque qui consiste à essayer d'obtenir des données de connexion et des données bancaires par le biais de faux e-mails/pages web. Il s'agit d'une forme d'escroquerie qui incite les personnes à divulguer leurs données de sécurité, telles que leur identifiant ou leur mot de passe, par le biais de contenus d'apparence trompeuse provenant d'entreprises ou d'institutions sérieuses. En Suisse, les entreprises concernées sont souvent la Migros, les CFF, Swisscom, UBS et la Poste.

Critères de reconnaissance de l'hameçonnage :

- Fautes de grammaires ou d'orthographe
- Des données sont demandées.
- Pièces jointes et liens.
- Promesses trop belles pour être vraies.

☞ Liste de contrôle :

- ☐ Former les collaborateurs afin de les sensibiliser à la sécurité informatique.
- ☐ Garder sa boîte de réception propre et bien organisée : Moins elle contient d'e-mails, plus il est facile d'en garder une vue d'ensemble.
- ☐ Partage des données mesuré : moins on partage d'informations en ligne, moins les phishers ont de chances de réussir.
- ☐ Signaler l'hameçonnage : Dès que l'on reçoit un message de phishing, signaler le message et bloquer l'expéditeur.
- ☐ Gestionnaire de mots de passe : utiliser un mot de passe différent pour chaque service, cela permet de sauver les autres comptes si l'un d'eux est piraté par une attaque de phishing.
- ☐ Examiner chaque e-mail de manière très critique, même s'il provient d'expéditeurs connus, et si nécessaire, se renseigner à nouveau auprès de l'expéditeur. En cas de doute, il vaut mieux supprimer l'e-mail et ne pas cliquer sur les liens.

4. Virusen / programme malveillant (malware) en annexe

Depuis plusieurs années, les e-mails font partie des principaux moyens de communication. Malheureusement, la plupart des virus informatiques se propagent également par le biais des pièces jointes. Il convient donc d'être prudent lors de l'ouverture des pièces jointes des courriels.

☞ Liste de contrôle :

- ☐ Protection contre les virus : les programmes antivirus déjà inclus dans le système d'exploitation de Windows (Defender) et de macOS (XProtect) possèdent généralement une qualité relativement élevée et offrent une protection élevée contre les intrusions nuisibles.
- ☐ Documents avec les extensions de fichiers suivantes présentent plus de risques que les autres :
  - **Fichiers texte doc/.docx/.xls/xlsx/.ppt/.pptx:** les documents office joints aux e-mails peuvent contenir des virus macros, il ne faut donc les ouvrir que si l'identité de l'expéditeur est connue.
  - **Fichiers images jpg.:** cette extension peut être utilisée pour masquer des fichiers de programme, il est donc important que le programme de messagerie affiche l'extension du fichier.

- **Fichiers compressés *zip/rar*:** les virus peuvent être activés lors de la décompression des fichiers zippés, c'est pourquoi l'expéditeur doit également être connu..
- Les fichiers **PDF** sont certes généralement inoffensifs, mais ils peuvent aussi contenir des virus informatiques. Il est donc important, même pour ce type de fichier relativement sûr, de vérifier l'expéditeur.

5. Transmission sécurisée des données / partage de fichiers (file sharing)

Les fichiers plus volumineux et les grandes quantités de données ne peuvent pas être envoyés par courrier électronique. Au lieu de clés USB, on utilise aujourd'hui principalement des services de partage de fichiers. Selon le type de données que vous souhaitez transférer, tous les services de partage de fichiers ne sont pas adaptés. Si vous transmettez des données personnelles, il convient de tenir compte des pays dans lesquels se trouvent les serveurs du fournisseur.
Pour partager des données en toute sécurité, nous recommandons les fournisseurs suisses, comme la solution de transfert de fichiers sécurisé de SecureSafe, un partenaire de FIDUCIAIRE|SUISSE, ou le Large File Transfer (LFT) d'IncaMail de la Poste suisse. le Large File Transfer (LFT) d'IncaMail peut également être utilisé dans le cadre de procédures administratives (OCEI-PA, RS 172.021.2), dans le cas de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et faillite (OCEI-PCPP, SR 272.1).