A DISPOSITION DES MILITANTS FFMC

Infos sur le cloud pcloud

https://www.pcloud.com/fr/features/security.html

Conseils sur la mise en place de la sécurité des données

https://www.orange-business.com/fr/blogs/cloud-computing/infrastructure-as-a-service/4-conseils-pour-ameliorer-la-securite-des-donnees-dans-le-cloud

8 points clefs pour sécuriser votre informatique d'entreprise ou association
https://www.idline.fr/8-points-clefs-pour-securiser-votre-informatique-dentreprise/

LES GUIDES DE LA CNIL LA SÉCURITE DES DONNÉES PERSONNELLES

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

CHARTE DE SÉCURITÉ

- **TABLE DES MATIÈRES**
  - EN QUELQUES MOTS
  - Les 3 principes généraux
  - Les 3 objectifs de la sécurité
  - Les 11 commandements
  - Les bons réflexes
  - Les aspects légaux

↑ Retour en haut

- **TAGS**
  - aspects légaux
  - bonnes pratiques
  - charte de sécurité
  - objectif sécurité

TAG CLOUD

Politique de sécurité bons réflexes menaces bonnes pratiques PME Analyse des risquesprotection mesures techniques de protectiongestion des risques logiciels malveillantsauthentification courrier électronique aspects légauxmots de passe panne

En quelques mots

Établir une charte de sécurité est une étape indispensable pour toute organisation lorsque que celle-ci souhaite faire respecter les bonnes pratiques dans le domaine de sécurité. Elle se présente sous forme d'un document court, d'une à plusieurs pages, sur lequel est décrit en grands traits la stratégie de l'organisation du point de vue sécurité de l'information et les règles de base à appliquer par tout membre.

Ci-dessous vous trouverez un exemple de sections d'une charte de sécurité.

Les 3 principes généraux

- **La sécurité est l'affaire de tous.**
- **Chacun est responsable à son niveau de la sécurité de l'information de toute l'organisation**.
- **Chacun se doit d'avertir le responsable sécurité lors de la détection d'un problème de sécurité.**

Les 3 objectifs de la sécurité

CONFIDENTIALITÉ

La confidentialité fait référence à la propriété de l'information d'être uniquement disponible ou divulguée à des individus, entités ou processus autorisés. L'accès à l'information est en quelque sorte réservé aux seules personnes admises à la connaître pour des besoins clairement identifiés.

INTÉGRITÉ

L'intégrité d'une information concerne le caractère d'exactitude et d'entièreté des ressources relatives à l'information. C'est-à-dire il s'agit de protéger la véracité et l'entièreté de l'information, ainsi que les méthodes de traitement de cette information.

DISPONIBILITÉ

Il s'agit de la propriété (pour un système d'information) d'être accessible et de remplir les fonctions envisagées au moment de la demande d'une entité autorisée, dans les conditions de délais et de performance prévues. C'est-à-dire il s'agit ici de protéger l'aptitude d'un système d'information à remplir une fonction dans des conditions définies d'horaires, de délais et de performances.

PREUVE

Cette notion concerne l'assurance de pouvoir justifier toute information.
Elle repose sur les principes d'authentification, de non-répudiation et d'imputabilité.
La preuve est parfois considérée comme le quatrième pilier de la sécurité de l'information.

Les 11 commandements

1. Suivez les règles et procédures de la sécurité de l'information
Consultez régulièrement les règles et procédures disponibles. En vous tenant au courant des évolutions de la politique de sécurité, vous serez mieux protégés.
2. Protégez vos mots de passe
Ne révélez jamais vos mots de passe. Si quelqu'un vous les demande, refusez. Notre sécurité implique de ne jamais donner vos mots de passe.
3. Sachez garder un secret
Ne révélez jamais de données confidentielles, quel que soit le cas de figure.
Ne discutez pas en public de sujets devant rester secrets.
4. Bloquez l'accès à votre ordinateur
Si vous quittez votre bureau, bloquez l'accès à votre ordinateur.
5. Sauvegardez correctement vos données
Ne stockez jamais des données sur votre espace personnel. Utilisez plutôt un serveur de fichiers, qui fera partie d'une stratégie de sauvegarde. Appliquer ces consignes

vous permettra de récupérer vos données si elles ont été perdues et d'y avoir accès à tout moment.

6. Résister aux méthodes "d'ingénierie sociale"

Lors d'une conversation par e-mail ou par téléphone, assurez-vous de l'identité de votre interlocuteur. Soyez prudents à chaque fois que l'on vous demande des informations personnelles, confidentielles, ou importantes au niveau de l'entreprise. L'ingénierie sociale exploite des vulnérabilités humaines pour accéder à des informations confidentielles.

7. Soyez attentifs à vos e-mails

Les e-mails peuvent représenter une menace pour votre ordinateur et pour l'ensemble du réseau informatique. Ne répondez jamais aux e-mail vous demandant des informations personnelles et/ou confidentielles. Vérifiez la provenance, l'inocuité et l'intégrité de chaque pièce jointe.

8. Utilisez intelligemment l'Internet

L'utilisation d'Internet est limitée pour des raisons de sécurité. L'accès est restreint (filtre web), mais suffisant pour votre usage professionnel. Téléchargez uniquement des fichiers nécessaires à votre travail, jamais pour votre loisir, et soyez attentifs aux fichiers reçus.

9. Utilisez un antivirus

Un antivirus est indispensable dans l'environnement professionnel actuel. Il est activé automatiquement et permet d'analyser tous vos fichiers avant même que vous les ayez ouverts. Les mises à jour sont automatiques afin de lutter au mieux contre toute nouvelle menace informatique. Si vous pensez avoir un virus, prévenez immédiatement votre département informatique.

10. Prenez soin du hardware et du software

N'installez jamais de software pirate ou non autorisé. Utilisez uniquement ceux mis à votre disposition par votre organisation. Si vous avez besoin d'un logiciel qui n'est pas installé sur votre ordinateur, introduisez une demande d'installation.
Prenez soit du hardware : les ordinateurs portables sont plus fragiles et très tentants pour les voleurs.
En ce qui concerne les supports amovibles : l'utilisation de disque dur externe et de CD est limitée. Scannez tous les supports amovibles afin de détecter d'éventuels virus. Utilisez ces supports seulement lorsque vous connaissez leur provenance et leur contenu.

11. Signalez les incidents

Tout incident doit être signalé au plus vite. Cela peut prévenir d'autres incidents similaires. Nous sommes responsables de la sécurité de notre environnement.
Le non-respect de la sécurité ou la violation des règles établies peut entraîner des sanctions disciplinaires.

Les bons réflexes

Dès que vous utilisez un outil informatique, veuillez respecter les "règles d'or" suivantes :

1. Le mot de passe : verrouiller le coffre-fort

Le mot de passe représente la clé d'accès à vos informations et à vos comptes en

ligne. Le défi consiste à en choisir un qui soit aisément mémorisable, tout en étant difficile à deviner par autrui. Évitez d'utiliser le prénom de vos enfants ou autres informations personnelles, faciles à deviner par autrui. Changez votre mot de passe régulièrement, ne le partagez avec personne, et utilisez différents mots de passe pour différentes applications.

2. L'antivirus : vacciner son ordinateur

Tout comme vous, votre ordinateur a besoin d'être vacciné pour rester en bonne santé et ainsi se préserver des virus et des vers. Installer un antivirus et le maintenir à jour est un réflexe indispensable pour la sécurité informatique.

3. Le firewall : se prémunir contre les attaques

Installez un pare-feu (firewall) et configurez-le correctement. Cela vous permettra non seulement de bloquer les attaques ou connections suspectes pouvant provenir de virus, vers ou chevaux de Troie, mais aussi d'éviter la fuite de vos informations personnelles et confidentielles.

4. L'anti-spyware : déjouer l'espionnage organisé

Sécurisez vos transactions e-banking / e-commerce en installant un anti-spyware dont l'objet est de balayer régulièrement l'ordinateur afin de repérer les logiciels malicieux qui pourraient s'y trouver.

5. Les patchs de sécurité : colmater les brèches

Pour contrer les pirates qui cherchent et trouvent continuellement des failles dans les systèmes d'exploitation, actualisez en permanence votre browser. Appliquez également les patchs adéquats. En effet, tout comme votre antvirus, votre système a besoin d'entretien. Faire les mises à jour nécessaires vous permettra de contrecarrer les dangers tels que les vers, les virus et les chevaux de Troie.

Les aspects légaux

Le non-respect de la législation (aspect légaux) dans le domaine des technologies de l'information peut mettre l'organisation dans une situation délicate à l'égard de la loi, de ses clients (image de marque) mais aussi avoir des conséquences financières (amendes) ou pénales (responsabilité des personnes).
Ainsi, la justice reconnaît et punit la :

- responsabilité de l'auteur de l'attaque;
- responsabilité de l'intermédiaire de l'attaque;
- responsabilité de la victime de l'attaque. La conséquence légale d'un manquement à l'obligation de sécurité en relation avec un traitement de données personnelles est punissable de 8 jours à 1 an de prison et de 251 à 125.000 euros d'amende.

De fait, toute organisation doit mettre en œuvre un niveau de sécurité en fonction :

- du risque d'atteinte à la vie privée;
- de l'état de l'art (ce qui implique une obligation de mise à jour et de se tenir informé);
- des coûts liés à la mise en œuvre.

NOS SERVICES

Startup Kit
Diagnostic
Monarc
Formation

NOS DOSSIERS

Cloud computing
Protéger son entreprise
Clever clicks

DERNIERS ARTICLES

RISK MANAGEMENT: FROM DIRECTIVE 95/46 TO THE GDPR

Lire la suite...

CYBERSECURITY4SUCCESS: L'ÉTAT AIDE LES ENTREPRISES À SE PROTÉGER

Les entreprises qui feront appel à des experts en matière de sécurité de l'information pourront recevoir des aides allant jusqu'à 50% des frais.
Lire la suite...

CONTACT

Cases.lu

41, avenue de la Gare
L-1611 Luxembourg

CONTACT CASES.LU