TPE/PME

9 règles de base pour mieux **protéger l'informatique** de votre **entreprise**

Un guide conçu par le CLUSIR Tahiti

CLUSIR TAHITI

Ce guide a été rédigé par :

Jonas **FERNANDEZ**
Olivier **GACH**
Patrick **GASSION**
Fabrice **LEUNENS**

Le mot du président

La mise en place de la sécurité informatique dans les TPE et les PME est souvent considérée comme complexe, onéreuse, chronophage ou peu utile. Les enjeux de la cybersécurité ne sont malheureusement appréciés qu'après un incident de sécurité tel que la perte ou le vol de données, une fraude informatique, une attaque d'un virus. Ces incidents peuvent aller jusqu'à mettre en péril une entreprise.

Face à ce constat, des membres du CLUSIR Tahiti, association à but non lucratif visant à promouvoir la sécurité des systèmes d'information, se sont réunis en groupe de travail pour élaborer ce guide de sécurité pour les TPE et PME polynésiennes. Ce document propose de façon pragmatique des recommandations simples et rapides à mettre en œuvre pour garantir à minima la sécurité des données de ces entreprises.

François PILLONNEAU
Président du CLUSIR Tahiti

Table des Matières

1 Choisir avec soin ses mots de passe

Dans le cadre de ses fonctions de comptable, Vetea consulte régulièrement l'état des comptes de son entreprise sur le site Internet mis à disposition par la banque. Par simplicité, il a choisi un mot de passe faible : 123456. Ce mot de passe a très facilement été reconstitué lors d'une attaque utilisant un outil automatisé : l'entreprise s'est fait voler 500 000 francs.

Le mot de passe est un outil d'authentification utilisé notamment pour accéder à un équipement numérique et à ses données. Pour bien protéger vos informations, choisissez des mots de passe difficiles à retrouver par des outils automatisés ou à deviner par une tierce personne.

Choisissez des mots de passe composés si possible de 12 caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vous (nom, date de naissance...) et ne figurant pas dans le dictionnaire.
Plusieurs méthodes simples peuvent vous aider à définir vos mots de passe :

- La méthode phonétique : «J'ai acheté 5 CDs pour cent euros cet après-midi» : ght5CDs%E7am.
- La méthode des premières lettres : «Allons enfants de la patrie, le jour de gloire est arrivé» : aE2lP,lJ2Géa!
- La méthode de remplacement des lettres par des chiffres : «J'ai deux voitures» : J'a12v01tures
- Et enfin si vous avez des difficultés à vous souvenir d'un mot de passe trop long, n'hésitez pas à le doubler ou le triplé : 1&2font31&2font3

Définissez un mot de passe unique pour chaque service sensible. Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle...) ne doivent jamais être réutilisés pour d'autres services. Si l'un de vos mots de passe est compromis, il n'y a pas de risque pour les autres contenus.

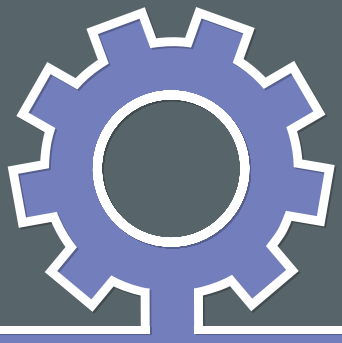
En entreprise :

- Déterminez des règles de choix et de dimensionnement (longueur) des mots de passe et faites les respecter via une stratégie de groupe dans votre domaine*.
- Faites les modifier de façon très régulière.
- Modifiez toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs, logiciels...) Ex : admin/admin…
- Rappelez aux collaborateurs de ne pas conserver les mots de passe dans des fichiers, sur des post-it ou sous le clavier.
- Sensibilisez les collaborateurs au fait qu'ils ne doivent pas préenregistrer leurs mots de passe dans les navigateurs, notamment lors de l'utilisation ou la connexion à un ordinateur public ou partagé (salons, déplacements...).

**Domaine : Regroupement logique d'ordinateurs Windows pour en faciliter la gestion.*

2 Mettre à jour régulièrement vos logiciels

Teriimoana est le comptable et responsable informatique d'un importateur automobile, il ne met pas toujours les logiciels de son entreprise à jour.
Il a ouvert par mégarde une pièce jointe piégée dans un mail.
Suite à cette erreur, des attaquants ont pu utiliser une vulnérabilité logicielle et ont pénétré son ordinateur pour effacer des fichiers.



Dans chaque système d'exploitation (Android, IOS, MacOS, Linux, Windows,…), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité. Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction.

Il convient donc, au sein de l'entreprise, de mettre en place certaines règles :

- Définissez et faites appliquer une politique de mises à jour régulières :
- S'il existe un service informatique au sein de l'entreprise, il est chargé de la mise à jour du système d'exploitation et des logiciels.
- S'il n'en existe pas, il appartient aux utilisateurs de faire cette démarche, sous l'autorité du chef d'entreprise.
- Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, téléchargez les correctifs de sécurité disponibles.
- Utilisez exclusivement les sites Internet officiels des éditeurs.

3 De l'importance de réaliser des sauvegardes

Moana est un petit artisan qui s'est installé aux ateliers relais il y a quelques mois.
Un soir, son ordinateur est tombé en panne.
Mais Moana n'avait pas fait de sauvegarde de ses données et cette panne a causé la perte de ses fichiers de clients, de sa gestion commerciale et sa comptabilité.
La pérennité de sa société en a été affectée durablement.

Pour veiller à la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple). Vous pourrez alors en disposer suite à un dysfonctionnement de votre système d'exploitation ou à une attaque.

Pour sauvegarder vos données, vous pouvez utiliser des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage, ou, à défaut, un DVD enregistrable que vous rangerez ensuite dans un lieu éloigné de votre ordinateur, de préférence à l'extérieur de l'entreprise pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur contenant les données d'origine. Néanmoins, il est nécessaire d'accorder une attention particulière à la durée de vie de ces supports.

Si vous effectuez des sauvegardes sur des plateformes sur Internet (souvent appelées « cloud » ou « informatique en nuage »), soyez conscient que ces sites de stockage peuvent être la cible d'attaques informatiques et que ces solutions impliquent des risques spécifiques :

- Risques pour la disponibilité et l'intégrité des données.
- Risques pour la confidentialité des données.

Il est important de veiller à toujours pouvoir relire vos sauvegardes dans le temps, malgré les évolutions.
Les formats de fichiers ouverts, utilisés par les logiciels libres, peuvent répondre à ce besoin de pérennité.

4 Sécuriser l'accès Wi-Fi de votre entreprise

Poe est prudente, l'accès WIFI de sa boutique est sécurisé par un chiffrement WEP.

Sans que Poe ne s'en aperçoive, un voisin a réussi en moins de deux minutes, à l'aide d'un logiciel, à déchiffrer la clé de connexion. Il a utilisé ce point d'accès Wi-Fi pour participer à une attaque contre le site Internet de l'assemblée de Polynésie. Désormais, Poe est mise en cause dans l'enquête de police.

L'utilisation du Wi-Fi est à la fois pratique et simple. Il ne faut cependant pas oublier qu'un Wi-Fi mal sécurisé peut permettre à des personnes d'intercepter vos données et d'utiliser la connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes. Pour cette raison l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise : une installation filaire reste plus sécurisée et plus performante.

Le Wi-Fi peut parfois être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre borne d'accès à Internet :

- Lors de l'installation de votre borne d'accès internet, ouvrez votre navigateur Internet pour configurer votre borne d'accès.
  Dans l'interface de configuration qui s'affiche souvent à l'ouverture de votre navigateur :

  - Modifiez l'identifiant de connexion et le mot de passe par défaut qui vous ont été donnés par votre fournisseur d'accès.

  - Activer le chiffrement de votre connexion à l'aide du protocole de chiffrement WPA2*. N'utilisez jamais le chiffrement WEP** qui peut être cassé en quelques minutes.

  - Modifiez la clé de chiffrement par défaut. Remplacer cette clé qui est souvent affichée sur l'étiquette de votre borne d'accès à Internet par une clé (mot de passe) de plus de 12 caractères de types différents.

  - Activez la fonction pare-feu de votre borne d'accès.

- N'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès. Les fournisseurs d'accès à Internet peuvent vous guider lors de l'application de ces recommandations de sécurité.

- Ne divulguez la clé de cryptage de votre borne d'accès qu'à des personnes de confiance et changez-la régulièrement. L'accès à votre connexion peut, dans certains cas, faciliter l'accès au contenu de vos serveurs et vos ordinateurs.

- Ne partagez pas votre connexion. Il n'est pas recommandé de laisser vos clients, fournisseurs ou autres tiers se connecter sur votre réseau (Wi-Fi ou filaire). Préférez avoir recours à une borne d'accès dédiée si vous devez absolument fournir un accès à un tiers.

- Désactivez votre borne d'accès lorsqu'elle n'est pas utilisée.

**WPA2 : Système de chiffrement des communications Wifi réputé fiable.*
**WEP : Système de chiffrement, mais réputé non sécurisé depuis plusieurs années.*

5 Être prudent lors de l'utilisation de sa messagerie

Suite à la réception d'un courriel semblant provenir d'un de ses collègues, Hinano a cliqué sur un lien présent dans le message.
Ce lien était piégé.
Sans que Hinano le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées, etc.).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- L'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail.
- N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts.
- Ne cliquez pas sur les liens présents dans des courriels dont vous ignorez l'origine.
- Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d'institutions comme les Contributions ou les banques pour récupérer vos données. Il s'agit d'attaques par hameçonnage ou « phishing »*.
- N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. Ces informations sont pour la plupart fausses et vous ne feriez que participer à la propagation d'un virus.
- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus** avant de les ouvrir afin de vérifier qu'ils ne contiennent aucun virus connu.

** phishing (hameçonnage) : méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.*

***antivirus : logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants.*

6 Être vigilant lors d'un paiement sur Internet

Louise est directrice d'une garderie. Elle commande régulièrement des fournitures sur internet.
Elle n'a jamais fait attention si les sites qu'elle utilisait étaient sécurisés ou non.

Lors de sa dernière commande le site ne l'était pas. Des attaquants ont intercepté le numéro de la carte bancaire de sa garderie et l'ont utilisés.
Elle a perdu 100.000 Francs.

Lorsque vous réalisez des achats sur Internet, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand. Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- Contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs).
- Assurez-vous que la menton « htps:// » apparait au début de l'adresse du site Internet.
- Vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple.

Si possible, lors d'un achat en ligne :

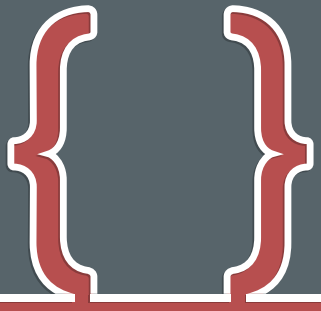
- Privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS.
- Ne transmettez jamais le code confidentiel de votre carte bancaire.

N'hésitez pas à vous rapprocher de votre banque pour connaître et utiliser les moyens sécurisés qu'elle propose.

7 Séparer les usages personnels des usages professionnels

Heiarii rapporte souvent du travail chez lui le soir.

Sans qu'il s'en aperçoive, sa messagerie personnelle a été piratée. Grâce aux informations qu'elle contenait, l'attaquant a pu pénétrer le réseau interne de son entreprise. Des informations sensibles ont été volées puis transmises à ses concurrents.



Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, smartphone…) personnels et professionnels.

La pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, smartphone, tablette, etc.) dans un contexte professionnel est pourtant une solution de plus en plus utilisée aujourd'hui.

Ce mode de travail pose de nombreux problèmes en matière de sécurité des données : vol ou perte des appareils, piratage, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur...

Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :

- Ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles.
- N'hébergez pas de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne.
- Évitez de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.
- Ne rechargez pas les téléphones et tablettes sur le port USB d'un ordinateur. Privilégiez des chargeurs que l'on connecte sur le secteur.

Si vous n'appliquez pas ces bonnes pratiques, vous prenez le risque que des personnes malveillantes volent des informations sensibles de votre entreprise après avoir réussi à prendre le contrôle de votre machine personnelle.

8 Les dangers du cloud.

Léon, comptable, partage des données avec ses collègues sur un serveur de cloud computing type Google Drive, Dropbox, ...
C'est en effet très pratique et cela rend le partage très simple.

Tellement simple que Léon stocke même des fichiers importants et qu'il se reconnecte sur son espace de Cloud depuis chez lui, pour travailler.

Le Cloud Computing est une offre dématérialisée très simple d'utilisation, offrant un service de stockage ou d'application accessible depuis n'importe quel accès à Internet, que ce soit à votre domicile, au bureau ou sur votre lieu de vacances.

Il permet de stocker les données sur un serveur exactement comme si on copiait les données sur un lecteur réseau ou disque local.

Avantage considérable, les fichiers sont accessibles de partout dans le monde.

Il existe actuellement une offre pléthorique de Cloud grand public pour le stockage principalement (Google Drive, Dropbox, Microsoft, Amazon,...).

Il ne faut pas oublier que ces services s'ils sont disponibles pour le grand public, sont adossés à de grandes sociétés commerciales, la plupart du temps américaines.

Nous savons qu'il y a eu des vols de données dans de grands groupes européens ces dernières années, la presse s'en était fait l'écho et l'utilisation du Cloud Computing peut faciliter grandement ces vols de données et donc poser de sérieux problèmes de confidentialité.

On peut utiliser le Cloud sans pour autant utiliser un service d'un fournisseur connu.
Il est possible d'utiliser un service de Cloud privatif, ce qui, dans le cadre d'une recherche de confidentialité, permet d'avoir de meilleures garanties.

- Soyez vigilant en prenant connaissance des conditions générales d'utilisation de ces services.
- Autant que possible, n'hésitez pas à recourir à des spécialistes techniques et juridiques pour la rédaction des contrats personnalisés et appropriés aux enjeux de votre entreprise.
- Veillez à la confidentialité des données en rendant leur lecture impossible à des personnes non autorisées en les chiffrant à l'aide d'un logiciel de chiffrement avant de les copier dans le «cloud».

9 Avoir un antivirus à jour

Reva tient une épicerie. Elle est prudente avec son ordinateur : elle a installé un antivirus, elle n'ouvre pas les mails des destinataires inconnus...

Pourtant, après avoir regardé les photos de son dernier week-end à la presqu'île qu'un ami lui a laissé sur une clé USB, son ordinateur à été infecté par un virus.

Il lui est maintenant impossible de démarrer l'ordinateur sur lequel est stocké l'ensemble des données relatives à son épicerie.

Les virus sont des programmes qui peuvent réellement endommager vos données et votre ordinateur s'il celui-ci n'est pas bien protégé. L'installation d'un antivirus est nécessaire sur tout ordinateur qu'il soit connecté ou non à Internet.

Si, par exemple, vous n'arrivez plus à lancer une application depuis peu, ou que votre ordinateur a des dysfonctionnements réguliers sans raison apparente, vous êtes probablement victime de malwares ou de virus !

Dès qu'un ordinateur a un souci, c'est très souvent un malware ou un virus le responsable, surtout lorsque l'ordinateur peu ou pas protégé.

Un antivirus est un programme, installé sur votre ordinateur, capable de détecter la présence de virus sur votre ordinateur et, dans la mesure du possible, de le désinfecter.

Dans ce contexte, il est recommandé de bien protéger votre ordinateur en appliquant quelques règles simples :

- Installer systématiquement un antivirus sur votre ordinateur. Aujourd'hui, de nombreux antivirus gratuits (Avast, Avira, AVG…) permettent une protection intéressante pour les besoins de la plupart des utilisateurs.
- Il est Inutile d'installer deux antivirus sur votre ordinateur. Au mieux, le second sera inefficace. Au pire, il rendra le premier inefficace…
- Assurez-vous que votre antivirus est paramétré pour se mettre à jour automatiquement. Un antivirus doit régulièrement être mis à jour pour conserver son efficacité. Selon Microsoft, il y a 5 fois plus de chances d'attraper un virus si l'on ne dispose pas d'un antivirus mis à jour.
- Si votre programme antivirus présente une fonction de détection de virus « en continu », assurez-vous qu'elle est toujours activée. Différents programmes ont différents noms pour cette fonction (protection en temps réel, realtime protection, protection résidente…), mais la plupart des antivirus comportent une telle fonction.
- Dès que vous avez un doute quant à une infection par un virus, balayez à l'aide de votre antivirus tout les fichiers qui sont stockés sur votre ordinateur afin de vérifier qu'ils n'ont pas été infectés.
- Faites attention aux antivirus fournis sur certains PC neufs, car une fois leur période d'évaluation terminée, ils deviennent obsolètes si vous n'achetez pas la version payante.

Conception **IMAGING - 87 73 83 00**

Version 1.0
Document sous licence Etalab V1
Septembre 2015
CLUSIR Tahiti

Le CLUb de la Sécurité des systèmes d'Information Régional - Région Tahiti (CLUSIR Tahiti) est une association Loi 1901.

www.clusir-tahiti.asso.pf

Ce guide s'inspire du «Guide des bonnes pratiques de l'informatique», édité par L'Agence Nationale de la Sécurité des Systèmes d'Information, dans sa version 1.1 du mois de mars 2015, sous licence Etalab - v1.