Sécurité informatique

La sécurité informatique est vécue comme une contrainte par la plupart des utilisateurs. En effet, elle rajoute un peu plus à la charge mentale. Cependant, les données ont une valeur importante, il faut donc les protéger.
En effet, une donnée qui peut paraître sans valeur à vos yeux peut donner à une personne malveillante des clés pour usurper votre identité.

De plus, l'attaque peut venir de tout côté, d'un smartphone, d'un wifi non protégé, d'un accès à un compte utilisateur protégé par un mot de passe faible...

Il y a des bonnes pratiques simples à mettre en place pour commencer à sécuriser ses données.

1. Choisir avec soin ses mots de passe

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 à l'aide d'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.
On peut s'aider de moyens mnémotechniques simples comme :

- 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!

Utilisez un mot de passe différent pour chaque service (outil). La réutilisation de MDP permettra d'accéder à tous les services que vous utilisez.
En entreprise :

- déterminez des règles de choix et de dimensionnement (longueur) des mots de passe et faites les respecter.
- modifiez toujours les éléments d'authentification (identifiants, mots de passe) définis par défaut sur les équipements (imprimantes, serveurs, box…).
- rappelez aux collaborateurs de ne pas conserver les mots de passe dans des fichiers ou sur des post-it.
- sensibilisez les collaborateurs au fait qu'ils ne doivent pas pré-enregistrer leurs mots de passe.

2. Mettre à jour régulièrement vos logiciels

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.

Il convient donc de mettre en place certaines règles :

- définissez et faites appliquer une politique de mises à jour régulières
- configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible.
- utilisez exclusivement les sites Internet officiels des éditeurs

3. Effectuer des sauvegardes régulières

La stratégie de sauvegarde doit être fonction de multiples critères comme :

- la criticité des données : si la donnée est utilisée quotidiennement par bcp d'utilisateur et est souvent mise à jour, il faudra la sauvegarder plus fréquemment. Si la donnée est consultée rarement et jamais modifiée, une sauvegarde plus ponctuelle peut être envisagée.
- la fréquence idéale (on peut aller de sauvegarde hebdomadaire à des sauvegardes temps réel)
- la pérennité du support : Cd, clés usb, système DD, bandes, cloud,…
- le lieu de stockage : si les sauvegardes sont toutes internes, cela peut entraîner une perte totale de données en cas d'incendie, vol, inondation… Il convient donc d'avoir des sauvegardes externes à l'entreprise qui peuvent être sur le cloud, sur un DD stocké hors de l'entreprise tous les soirs...
- Versionning : selon les types de données, du versionning dans la sauvegarde peut être envisagée. On garde les X dernières sauvegardes quotidiennes, les Y hebdomadaires et les Z annuelles.
- Chiffrement des données : les données sauvegardées peuvent être chiffrées afin de la rendre non exploitable par un tiers.

4. Sécuriser l'accès Wi-Fi de votre entreprise

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.
Si son utilisation est obligatoire :

- ne divulguez votre clé de connexion qu'à des tiers de confiance et changez la régulièrement
- activez la fonction pare-feu de votre box
- désactivez votre borne d'accès lorsqu'elle n'est pas utilisée
- n'utilisez pas les Wi-Fi « publics » pour des raisons de sécurité et de confidentialité
- assurez-vous que votre ordinateur est bien protégé par un antivirus et un pare-feu.
- préférez avoir recours à une borne d'accès dédiée si vous devez absolument fournir un accès tiers. Ne partagez pas votre connexion

5. Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur

Les smartphones sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires de sécurité informatique :

- n'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger
- en plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et le configurer pour qu'il se verrouille automatiquement
- effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les conserver en cas de restauration de votre appareil dans son état initial
- ne pré-enregistrez pas vos mots de passe

6. Protéger ses données lors de ses déplacements

Voyager avec ces appareils nomades fait peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences.

Avant de partir en mission :

- n'utilisez que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission, et ne contenant que les données nécessaires.
- sauvegardez ces données, pour les retrouver en cas de perte
- si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur
- apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport
- vérifiez que vos mots de passe ne sont pas préenregistrés.

Pendant la mission :

- gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour
- désactivez les fonctions Wi-Fi et Bluetooth de vos appareils
- retirez la carte SIM et la batterie si vous êtes contraint de vous séparer de votre téléphone
- informez votre entreprise en cas d'inspection ou de saisie de votre matériel par des autorités étrangères
- n'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance
- évitez de connecter vos équipements à des postes qui ne sont pas de confiance.
- refusez la connexion d'équipements appartenant à des tiers à vos propres équipements

Après la mission :

- effacez l'historique des appels et de navigation
- changez les mots de passe que vous avez utilisés pendant le voyage
- n'utilisez jamais les clés USB qui peuvent vous avoir été offertes lors de vos déplacements

7. Être prudent lors de l’utilisation de sa messagerie

Lorsque vous recevez des mails, 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
- si des liens figurent dans un courriel, passez votre souris dessus avant de cliquer. L’adresse complète du site s’affichera dans la barre d’état du navigateur située en bas à gauche de la fenêtre (à condition de l’avoir préalablement activée). Vous pourrez ainsi en vérifier la cohérence
- ne répondez jamais par mail à une demande d’informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des mails circulent aux couleurs d’institutions comme les Impôts 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.
- désactivez l’ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu’ils ne contiennent aucune charge virale connue

8. Télécharger ses programmes sur les sites officiels des éditeurs

- téléchargez vos programmes sur les sites de leurs éditeurs ou d’autres sites de confiance
- pensez à décocher ou désactiver toutes les cases proposant d’installer des logiciels complémentaires
- restez vigilants concernant les liens sponsorisés et réfléchir avant de cliquer sur des liens
- désactivez l’ouverture automatique des documents téléchargés et lancez une analyse antivirus* avant de les ouvrir afin de vérifier qu’ils ne contiennent aucune charge virale connue

9. Être vigilant lors d’un paiement sur Internet

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 mention « https:// » apparaît 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
- De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire
- n'hésitez pas à vous rapprocher votre banque pour connaître et utiliser les moyens sécurisés qu'elle propose

10. Séparer les usages personnels des usages professionnels

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
- de la même façon, évitez de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.

11. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Des personnes malveillantes pratiquent l'ingénierie sociale, c'est-à-dire récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité ou de conduire des activités d'espionnage industriel.

Dans ce contexte, une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet :

- soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir :
  - ne transmettez que les informations strictement nécessaires
  - pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données
- ne donnez accès qu'à un minimum d'informations personnelles et professionnelles sur les réseaux sociaux, et soyez vigilant lors de vos interactions avec les autres utilisateurs
- pensez à régulièrement vérifier vos paramètres de sécurité et de confidentialité
- utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle…) et une adresse destinée aux autres services en ligne (forums, jeux concours…).

Sensibiliser les collaborateurs à la sécurité informatique

Comme nous l'avons évoqué rapidement, on peut mettre en place toutes les sécurités d'infrastructure possibles, il reste un pan non métrisable qui est le facteur humain.
C'est pour cela qu'il faut faire preuve de pédagogie, accompagner et expliquer les bonnes pratiques.
Pour ce faire, nous allons donner quelques chiffres mais aussi quelques point de sensibilisation.

Plus de 90 % des incidents de sécurité dus à une erreur humaine

Que risquent les entreprises ?

1. Perdre de l'argent

Le coût réel d'une attaque doit prendre en compte également les dommages collatéraux dus à la perturbation temporaire de l'activité de l'entreprise ou à la perte définitive de leurs données :

- Impact sur les ventes
- Diminution de la productivité
- Coûts liés à la récupération du système (recrutement de personnel expérimenté ou d'experts externes…)

Pour mettre en perspective chiffrée, voici l'impact financier **moyen** des actions inappropriées des salariés :
Pour une PME :

- Perte matérielle d'appareils mobiles exposant l'organisation à des risques : 87k€
- Partage inapproprié de données : 77k€
- Perte matérielle d'appareils ou de supports contenant des données : 71k€
- Utilisation inappropriée des ressources informatiques par un salarié : 59k€

Pour une grande entreprise :

- Partage inapproprié de données via des appareils mobiles : 407k€
- Utilisation inappropriée des ressources informatiques par un salarié : 510k€
- Perte matérielle d'appareils ou de supports contenant des données : 960k€
- Incidents impliquant des objets connectés : 1400k€

Pour une société fragile, l'impact peut être dévastateur.

2. La perte permanente de données peut avoir des conséquences encore plus graves :

Imaginez perdre l'accès à tous vos registres de ventes, aux dossiers des clients, aux données comptables, aux informations produits et aux données de conception…
Ce type de données stratégiques ne sont pas appelées ainsi par hasard, elles sont utilisées par le business au quotidien et constitues une part de la valeur de la société.

En quoi cela peut impacter votre société :

- Nuire de façon permanente à la position concurrentielle de l'entreprise
- Nuire à la réputation de l'entreprise
- Réduire le carnet de commandes à long terme
- Empêcher l'accès permanent à la propriété intellectuelle et aux données de conception et même mettre en péril l'ensemble de l'entreprise

Qui les criminels ciblent-ils et pourquoi ?

Tous les salariés

Les questions de sécurité concernent toute l'échelle hiérarchique.
Il convient de bâtir une culture d'entreprise fondée sur une prise de conscience collective de l'importance de la cybersécurité.
Cette prise de conscience doit atteindre toutes les strates de la pyramide hiérarchique.

Les violations de données en chiffres :

- 81% des violations liées au piratage exploitent des mots de passe volés, faibles ou facilement devinables.
- 43% des violations sont des attaques sociales (attaque qui s'appuie essentiellement sur les relations humaines pour inciter de façon détournée à enfreindre les procédures de sécurité).
- 66% des programmes malveillants sont installés à partir de pièces jointes.

Toutes les entreprises

Les entreprises de moins de 1000 salariés sont majoritairement (61 % - 2017) les victimes de violation de données.

Les cybercriminels se moquent de qui vous êtes.
Que vous soyez une petite société de 100 personnes ou un fournisseur de service de taille moyenne. A partir du moment où vous avez accès aux données d'une grande entreprise, vous devenez une cible principale.

Dans de nombreux cas, les petites entreprises sont fournisseurs de grandes entreprises et ainsi ont accès à des informations confidentielles privilégiées. Elles deviennent les cibles des cybercriminels en quête de vulnérabilités.

Avec un coût moyen pour une fuite de données estimé à 33 k€ pour les petites et moyennes entreprises, la plupart ne sont pas préparées face à la perte d'une telle somme.

Techniques utilisées par les cybercriminels

Phishing / Ransomware :
En pratique, l'utilisateur reçoit un email avec un contenu qui en apparence émane d'une institution telle qu'une banque, les impôts, la CAF ou encore un fournisseur d'accès à Internet. L'utilisateur est invité à effectuer une opération de type changement de mot de passe ou encore activation de compte, mais le site web vers lequel il est dirigé est en fait une copie frauduleuse du site institutionnel.
Le salarié néophyte en informatique ne sait pas faire la différence entre un email frauduleux et une communication officielle et communiquera volontairement les informations requises.
Les banques, les boutiques en ligne et les systèmes de paiement restent les organisations les plus ciblées par ce type d'attaque.

Les bonnes questions à se poser :

- Est-ce que l'e-mail indique une URL mais se réfère en réalité à une autre ?
- Est-ce que le message demande des informations personnelles ?
- Est-ce que les informations de l'en-tête correspondent bien à l'expéditeur ?

Récupération de mots de passe (trop simples)

Environ 90 % des mots de passe sont vulnérables face au piratage

Les cybercriminels utilisent des ordinateurs pour tenter de deviner votre mot de passe à raison de milliers de tentatives par minute.
Les programmes qui devinent les mots de passe utilisent des dictionnaires prêts à l'emploi et des combinaisons simples de lettres et de chiffres. Les mots de passe longs constitués d'une combinaison de nombres, de symboles et de lettres majuscules et minuscules sont plus difficiles à deviner !

L'ingénierie sociale

Elle piège les salariés en les poussant à rompre les procédures normales de sécurité, une méthode efficace qui s'est avéré la cause principale de nombreuses attaques récentes de grandes entreprises.
Beaucoup de salariés partent du principe qu'ils ne seront jamais la cible de telles attaques.

L'ingénierie sociale est un type d'atteinte à la sécurité que les escrocs utilisent pour inciter des personnes à leur communiquer des données permettant d'accéder à des informations sensibles.
L'action consiste à tromper leurs victimes plutôt qu'à pénétrer les réseaux.
Parfois, les escrocs parviennent à obtenir les informations recherchées en les demandant tout simplement à leurs victimes.

Infection de sites Internet légitimes
Les infections de sites Internet en masse sont devenues l'un des plus grands problèmes auxquels le secteur informatique doit faire face.

Les sites renferment des scripts malveillants qui ont été injectés dans le code PHP, JS ou HTML d'origine par les auteurs des attaques.
En règle générale, ces scripts redirigent les visiteurs du site vers des URL malveillantes où des programmes malveillants attendent d'être téléchargés et exécutés sur l'ordinateur de la victime.
Dans la majorité des cas, la victime ne remarque rien de l'exécution du programme malveillant et ne voit qu'un site Internet qui semble fonctionner normalement.

Création de sites Internet frauduleux (attaques de point d'eau)

L'idée même de l'attaque de point d'eau est de trouver et d'infecter les sites que les salariés visitent le plus souvent. Lorsqu'un salarié ouvre un site infecté, le code injecté dans le corps de la page redirige le navigateur vers un site malveillant contenant un kit d'Exploits.
La plupart des salariés sont surpris d'apprendre qu'il ne suffit que d'une simple visite sur un site pour être infectés. Cliquer sur « Autoriser » ou « Confirmer » exécute souvent le code malveillant et dissimule l'attaque à l'équipe de sécurité informatique.

Exploitation des vulnérabilités des applications

Les mises à jour systèmes sont maintenant devenues quasi automatiques.
Cependant, tous les programmes ne sont pas forcément mis à jour.
L'inaction de l'utilisateur face aux mises à jour proposées est exploitée comme faiblesse pour que les auteurs de codes malveillants parviennent à leur objectif.

De plus, les pirates profitent du fait que les utilisateurs ne désinstallent pas les applications qui ne sont plus supportées, donc plus mises à jour mais qui fonctionnent toujours. De nombreux utilisateurs installent en effet une application, puis l'oublient.

Pour éviter cela, il faut :

- limiter au stricte nécessaire les applications utilisées
- forcer les mises à jour
- interdire les droits administrateurs aux utilisateurs pour contrôler la prolifération d'installations d'applications

Exploitation de failles des réseaux WIFI

Les escrocs peuvent pirater les connexions WiFi à accès ouvert et espionner vos activités en ligne.
Si vous ne prenez pas des précautions en matière de sécurité, les criminels peuvent voir vos noms d'utilisateurs, mots de passe, emails et d'autres informations confidentielles.
De nombreux salariés sont équipés de périphériques mobiles, depuis lesquelles ils consultent leur messagerie et échangent des données personnelles ou professionnelles.
Si vous ne pouvez pas passer outre l'utilisation d'un WIFI gratuit, **utilisez un VPN**. Il vous permettra de chiffrer le trafic entre votre appareil et les sites que vous visiterez.

Infection via des périphériques amovibles

Un périphérique professionnel (clé usb, disque dur externe…) ne doit jamais être utilisé pour faire des transferts avec un device personnel.
Il ne doit jamais être utiliser pour des échanges directs même avec des partenaires.

De manière général, on ne devrait pas à avoir utiliser un périphérique de stockage. Les documents professionnels restent sur le réseau de l'entreprise et sont consultés via un VPN.

Pourquoi ?
Car lors de la connexion d'un périphérique infecté sur le réseau de l'entreprise, le malware infecte automatiquement la machine hôte et a ensuite la possibilité de se propager sur les autres machines.

Arnaque au Président

Le faux ordre de virement (FOVI) est devenu, depuis peu, l'arnaque la plus redoutable en France pour les entreprises. Cette escroquerie en plein essor aurait permis de détourner quelques 250 millions d'euros depuis 2010. L'art du FOVI consiste à abuser un salarié ou un assistant comptable afin d'exiger un virement bancaire.

10 règles simples à mettre en place dans votre entreprise

1. Installez une solution de sécurité fiable et utilisez toutes ses fonctionnalités, notamment la recherche de vulnérabilités, le déploiement automatique des patchs et la détection rapide des virus.
2. Protégez les salariés partout où ils travaillent. Avec le développement du travail mobile, appliquer des mesures de sécurité au seul matériel présent au bureau n'est plus suffisant.
3. Rédigez de façon claire et précise une politique de sécurité interne et communiquez-la largement (mails, réunions d'information, affichage dans les locaux).
4. Éliminez toute situation pouvant laisser la place aux comportements à risque : interdisez les applications non répertoriées (bloquer par défaut les applications inconnues).
5. Sensibilisez vos collaborateurs au fait qu'ils travaillent pour une entreprise dont les données et les informations ont beaucoup de valeur sur le marché noir de la cybercriminalité, par la communication et la formation.
6. Précisez les conséquences éventuelles d'une attaque : demande de rançon, vol de données sensibles, coût de récupération des systèmes…
7. Enseignez aux utilisateurs à faire appel à l'équipe informatique pour signaler n'importe quel incident
8. Réalisez des simulations d'attaques de phishing pour tester la réactivité de vos collaborateurs à ces types d'attaques.
9. N'affichez pas la liste de tous les salariés sur le site Web de votre entreprise.
10. Formez votre personnel aux menaces informatiques, à l'aide de cas concrets, facilement applicables dans leur quotidien

Source originale : #truecybersecurity www.kaspersky.fr

Compléments

- **Anti-virus** : Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité
- **Cryptographie** : Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques
- **Pare-feu** : Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement
- **Contrôles d'accès logiques** : Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dument habilitées
- **Sécurité physique des équipements et locaux** : Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.

- **Capacité d'audit** : Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I.
- **Clauses contractuelles avec les partenaires** : Mécanismes organisationnels destinés à s'assurer que les partenaires et prestataires mettent en œuvre les mesures nécessaires pour ne pas impacter la sécurité des S.I. de leurs clients
- **Formation et sensibilisation** : Mécanismes organisationnels dont l'objectif est d'expliquer aux utilisateurs, administrateurs, techniciens, PDG, clients, grand public, etc. en quoi leurs actions affectent la sécurité des S.I. Diffusion des bonnes pratiques de sécurité. Le cours actuel en est une illustration !