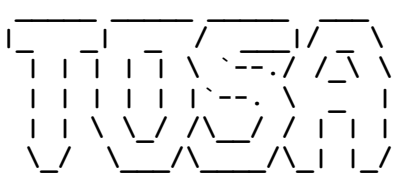

1) Cloud et Sauvegarde de fichiers

Nos documents sont souvent éparpillés à plusieurs endroits; sur des clefs USB, dans nos boîtes mails, sur un autre ordinateur etc. et ça se peut qu'il y ai eu plusieurs modifications au cours du temps. Pour gérer plus facilement ça et automatiser le tout on utilise une GED, ou un outil de Gestion Electronique de Documents.

Les fonctionnements et avantages d'une GED sont:

- **Digitaliser et archiver des documents**

  Les documents physiques doivent être scannés et ajoutés avec les autres documents (digitaux) à l'outil de GED. D'ici les utilisateurs peuvent créer, enregistrer, rechercher et archiver leurs fichiers digitalement. Ceci réduit les frais d'impression et d'archivage physique et facilite la recherche grâce aux différents tags et descriptions rajoutés aux documents tels que le nom du fichier, l'auteur, la date de publication etc.

- **Partager des documents**

  Grâce à la Gestion Electronique des Documents le partage de fichier est plus rapide, il ne faut plus partager ses fichiers par clé USB ou par mail vu que tout se trouve sur un même système central. On peut aussi décider qui a accès aux dossiers et qui peut les modifier.

- **Travail collaboratif**

  Les documents peuvent être utilisés en même temps par plusieurs personnes et sont mis-a-jours en temps réel pour que tout le monde ait la même version. Il ne faut donc plus attendre que la personne A ait fini et qu'il l'envoie à la personne B pour continuer le travail. Ceci est surtout utile dans des projets à grande échelle.

- **Contrôler la version des documents**

  Contrôler la version du dossier est utile quand plusieurs personnes travaillent sur un même document et que la version de celui-ci change sans arrêt. Cela permet de vérifier qui a fait les changements et de retourner vers une version antérieure si nécessaire. Il ne faut donc plus faire plein de sauvegardes séparées pour chaque version du fichier.

- **Améliorer le workflow**

  Le workflow est un processus qui est utilisé pour bien mener un projet et l'automatiser. Ça permet de voir quelles tâches il reste à faire, qui travaille sur le dossier, quand ça doit être rendu etc. et tout ça en temps réel.

  Les points au-dessus aident tous à améliorer le workflow d'une entreprise.

2) Les fichiers externes

Les différentes sources :

- Téléchargement sur un site

  Dans un premier temps, il est toujours mieux de télécharger sur un site uniquement si le site en question est fiable (vérifié l'URL, site connu et réputé, site du fabricant, github,...) . Pour ce qui est des logiciels, toujours privilégier le site du fabricant/développeur ou le github. Si possible toujours prendre le réflexe de check le MD5SUM.

- Clé USB

  Bien entendu ne jamais brancher une clé USB de source inconnue. Mais lorsque la source est connue, ne pas pensez que le ou les fichier(s) qu'elle contient est forcément inoffensif.

- Collègue / Ami

  Le risque 0 n'existe pas, il est tout à fait possible qu'un collègue (surtout dans notre milieu) ou un ami nous donne un fichier malveillant (Par exemple si un ami s'est fait piraté et que le hacker usurpe son identité pour diffuser son virus)

- Mail

  Toujours vérifié la provenance des fichiers en pièce jointe de mail, et surtout de mail. Même les .pdf ou .png ne sont pas sûrs.

Comment vérifier si un fichier est malveillant ?

Premièrement, il est toujours bien d'analyser le fichier avec un ou plusieurs antivirus. Beaucoup conseille VirusTotal qui est disponible en logiciel ou sur le site virustotal.com qui est un antivirus qui utilise plusieurs antivirus et qui donne une donnée assez globale de la dangerosité ou non du fichier. Attention qu'avec VirusTotal certains antivirus sont très sensibles.

Deuxièmement, il est important de vérifier la signature numérique. (la signature numérique, c'est quoi ? Lorsqu'un éditeur crée un fichier il a la possibilité de le signer numériquement afin de prouver l'origine du fichier (societe par exemple). Dans la grande majorité des cas, les fichiers malveillants n'ont pas de signature, mais attention un fichier sans signature ne veut pas forcément dire fichiers dangereux.

Pour vérifier la signature d'un fichier :

- Windows
    1. Faire un clic droit sur le fichier et "Propriété"
    2. Aller sur l'onglet "signature numérique"
    3. Vérifier le nom
    4. Si pas de signature numérique, allez dans détails et regarder le Copyright

Le MD5SUM est un moyen de vérifier si un document a été modifié par un tiers et est donc différent de celui d'origine. On convertit notre fichier en hash MD5 qui nous donne une ligne de caractères. Comparez-la à celle fournie par l'auteur du fichier téléchargé. Si les signatures sont identiques, votre fichier est intègre, sinon, il est corrompu.

Les risques liés

Télécharger un fichier externe nous exposent possiblement à des logiciels malveillants:

- Ransomware
    - Chiffrement des données, récupération en échange d'un ranson
- Virus
    - Logiciels malveillants qui demande une interaction humaine
- Backdoor
    - Exploitation d'une faille permettant la reconnexion à la machine cible.
- Reverse Shell
    - Faille permettant d'utiliser un terminal à distance sur la machine de la cible.
- Botnet
    - Réseau d'ordinateur contrôlé par un seul attaquant (Utilisé généralement pour le DDOS)
- Keylogger
    - Enregistreur de frappe et l'envoie à l'attaquant
- Sniffing
    - Interception de données du pc/réseau

Et de manières général tout ce qui est possible de faire en cas d'attaque informatique.

3) Vie privée et protection personnelle:

Vie privée et vie professionnelle:

Il est ici question de savoir s'installer une « barrière », nous permettant de dissocier le pro et le privé .

Deux politiques de sécurité bien distinctes seront utilisées, donc un certain jeu de mot de passe pour le pro, un tout autre pour le privé.

Bien distinct ne signifie pas juste de caractère différent mais aussi le sujet auquel il porte, la provenance de l'idée(famille, date,..) voir utilisation d'un générateur de mdp

Lors des rotations de passphrase, il est évident que l'on ne pourra pas échanger les mdp pro avec privée pour en faire une rotation…

Un renouvellement entièrement aléatoire, (inutile si générateur de mdp).. cependant définir toujours une date de changement régulier des mdp

Il n'est pas seulement question de MDP, effectivement il sera important de ne pas mélanger les utilisations.

Privilégié Exclusivement l'utilisation du poste pro pour le pro nous permettra d'éviter tout contact malveillant avec le monde extérieur,

A l'inverse, pour le post privé, cela nous permettra d'y contenir toute menace éventuellement téléchargée (volontairement ou non), chargée, téléversée,… Et ce, sans à aucun moment infecter le pro

L'utilité des diverses connexions sera aussi contrôlée, de façon à couper celles qui ne nous sont pas nécessaires et de ce fait limiter les risques.

Protection de la vie privée:

Il est important de dissocier amis et collègues, de façon à ce que chacun aie accès à ce dont il a droit. plus nos collègues et employeurs auront d'accès aux informations de notre vie privée, plus ils seront susceptibles de les utiliser.

Plusieurs scénarios sont envisageables, comme par exemple un collègue qui convoite votre poste, se servira peut être de photos compromettantes récupérées sur le net, ou un texte allant indirectement ou directement à l'encontre de la société, de sa politique.v

Pour ce qui est de la protection de la vie privée, il en va de soi qu'il est question ici d'une bonne gestion de soi et de nos interactions avec internet.
Effectivement, le fait d'accepter toute requête aveuglément, accorde de confidentialité douteuse,.. Permettront une divulgation de fichiers et/ou information et ce sans même, parfois, que vous ne vous en rendiez compte.

Ceci dit, d'autre manière de protéger sa vie privée et de minimiser l'accès à vos informations, photos, publication, localisation,... aux personnes présentes dans votre liste d'amis.

A savoir que TOUT mettre sur les réseaux sociaux laisse libre à chacun de savoir ce que vous aimez, ce qui vous déplait, l'état de votre famille, votre milieu de vie, ou vous êtes, ce que vous faites,...
Car toute publication est susceptible d'être un indice pour une personne ayant pour but d'agir de façon malveillante