CYBERSECURITE

Contenu extrait du MOOC SecNumAcadémie de l'ANSSI et rédigé par Pascal Escalière
SAS Atlantice

1. PANORAMA SSI

1.1. Réglementations et menaces

SI : un Système d'Information sert à faire transiter de l'information.

- Un espace de non droit qui entraîne des textes :
  - Loi française informatique et libertés réglemente le fichage des personnes 1978 CNIL.
  - Loi française Godfrain 1988 réprime les criminels informatiques.
    STAD (Système de Traitement Automatique des Données) : le responsable doit garantir la sécurité des données.
  - Loi française LCEN (Loi pour la Confiance dans l'Economie Numérique) 2004 : promouvoir le e-commerce dans l'UE.
  - Le secret des correspondances est garanti par directive européenne du 15/12/1997 (1 an de prison et 45000 euros d'amende et jusqu'à 3 ans de prison)
  - RGS (Référentiel Général de Sécurité) : réglementation de la relation administrations/citoyens.
    Etat de l'art des bonnes pratiques pour toute la société.

En France, les différents rôles :

- Protection des données personnelles : CNIL
- Confiance des utilisateurs : RGS
- Protéger de la fraude informatique : Godfrain

A l'international :

- Directive NIS (Directive Network and Information Security) européenne 2013 dessine un cyberespace libre et sécurisé.
- RGPD (Règlement Général sur la Protection des Données) appliqué en 2018 au niveau européen.
- ICANN (Internet Corporation for Assigned Names and Numbers), de droit californien, peut suspendre un nom de domaine.

Intrusion : fait de s'introduire de façon inopportune dans un groupe, un milieu, sans y être invité.

Les surfaces d'attaque sont de plus en plus grandes à cause des éléments connectés (objets) : Botnet, réseau piraté.

La multiplicité des points d'accès permet un effet de surprise des attaques.

4 menaces principales :

- Cybercriminalité.
- Atteinte à l'image.
- Espionnage.
- Sabotage.

1.2. ANSSI / SGDSN

1.2.1. SGDSN : Le Secrétariat Général de la Défense et de la Sécurité Nationale.

Anciennement secrétariat général à la Défense (SGDN), est un organe gouvernemental français, service du Premier ministre, chargé d'assister le chef du Gouvernement dans l'exercice de ses responsabilités en matière de Défense nationale et de Sécurité nationale. Il assure le secrétariat du Conseil de Défense et de Sécurité nationale.

Le SGDSN est, avec le Secrétariat général du gouvernement, le Secrétariat général des affaires européennes et le Secrétariat général de la mer, l'un des principaux secrétariats généraux sur lesquels s'appuie le Premier ministre pour l'animation et la coordination interministérielles de l'action du Gouvernement.

Le SGDSN assiste le Premier ministre dans l'exercice de ses responsabilités en matière de Défense et de Sécurité nationale. À ce titre :

- Il anime et coordonne les travaux interministériels relatifs à la politique de Défense et de Sécurité nationale et aux politiques publiques qui y concourent ;
- En liaison avec les départements ministériels concernés, il suit l'évolution des crises et des conflits internationaux pouvant affecter les intérêts de la France en matière de Défense et de Sécurité nationale et étudie les dispositions susceptibles d'être prises. Il est associé à la préparation et au déroulement des négociations ou des réunions internationales ayant des implications sur la Défense et la Sécurité nationale et est tenu informé de leurs résultats ;
- Il propose, diffuse et fait appliquer et contrôler les mesures nécessaires à la protection du secret de la Défense nationale. Il prépare la réglementation interministérielle en matière de Défense et de Sécurité nationale, en assure la diffusion et en suit l'application ;
- En appui du coordonnateur national du renseignement, il concourt à l'adaptation du cadre juridique dans lequel s'inscrit l'action des services de renseignement et à la planification de leurs moyens et assure l'organisation des groupes interministériels d'analyse et de synthèse en matière de renseignement ;
- Il élabore la planification interministérielle de Défense et de Sécurité nationale, veille à son application et conduit des exercices interministériels la mettant en œuvre. Il coordonne la préparation et la mise en œuvre des mesures de Défense et de Sécurité nationale incombant aux divers départements ministériels et s'assure de la coordination des moyens civils et militaires prévus en cas de crise majeure ;
- Il s'assure que le Président de la République et le Gouvernement disposent des moyens de commandement et de communications électroniques nécessaires en matière de Défense et de Sécurité nationale et en fait assurer le fonctionnement ;
- Il propose au Premier ministre et met en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information. Il dispose à cette fin du service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » ;
- Il veille à la cohérence des actions entreprises en matière de politique de recherche scientifique et de projets technologiques intéressant la Défense et la Sécurité nationale et contribue à la protection des intérêts nationaux stratégiques dans ce domaine7.

1.2.2. ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information.

C'est un service français créé par décret en juillet 2009. Ce service à compétence nationale est rattaché au SGDSN. L'ANSSI remplace la Direction centrale de la sécurité des systèmes d'information, créée par décret en juillet 2001.

L'ANSSI présente ses missions comme suit :

- « L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. À ce titre elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. »
- L'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV).
- Elle est chargée de la promotion des technologies, des produits et services de confiance, des systèmes et des savoir-faire nationaux auprès des experts comme du grand public. Elle contribue ainsi au développement de la confiance dans les usages du numérique.
- Son action auprès de différents publics comprend la veille et la réaction, le développement de produits pour la société civile, l'information et le conseil, la formation ainsi que la labellisation de produits et de prestataires de confiance.

1.3. Défense en profondeur

Son but est de retarder l'ennemi en multipliant les systèmes de protection avec plusieurs lignes de défense indépendantes qui coopèrent.

- La sécurité en profondeur est l'affaire de tous et l'utilisation d'un pare-feu et d'un antivirus ne suffit pas à nous protéger.
- Choisir un mot de passe fort car un attaquant pourrait avec celui-ci récupérer mes informations personnelles, usurper mon identité, porter atteinte à mon image ou à ma réputation, essayer de piéger mes contacts à leur tour.
  De ce fait :
  - Changer les mots de passe par défaut de type 0000 ou admin pu 1234, etc…
  - Utiliser un mot de passe différent par système ou logiciel ou boîte mail.
  - Utiliser des mots de passe dont la robustesse dépend de la sensibilité des données auxquelles il donne accès.
  - Choisir un mot de passe de qualité, par exemple : 12 caractères dont 1 majuscule, 1 minuscule, 1 chiffre, 1 caractère spécial en évitant les phrases.
  - Utiliser un coffre-fort de mots de passe.
  - Ne pas communiquer son mot de passe, ne pas l'écrire sur un post-it.
  - Utiliser des combinaisons aléatoires.
- Mettre à jour ses logiciels.
- Bien connaitre les utilisateurs et les prestataires.
- Effectuer des sauvegardes régulières par exemple : 1 par année, 1 pour chaque mois de l'année en cours, 1 pour chaque semaine du mois en cours.
- Sécuriser l'accès Wi-Fi en utilisant le protocole WPA2 et un mot de passe fort car les protocoles précédents ont trop de failles.
- Être prudent avec son Smartphone et sa tablette car ils ne présentent pas le même niveau de sécurité qu'un ordinateur.
- Protéger ses données lors d'un déplacement en les chiffrant par exemple.
- Être prudent avec l'utilisation de sa messagerie : surveiller le contenu, l'adresse mail de l'expéditeur car une personne peut être intercalée entre vous et votre correspondant.
- Télécharger ses programmes sur les sites officiels des éditeurs.

- Être vigilant lors de paiements sur internet.
- Séparer les usages personnels et professionnels.
- Prendre soin de son identité numérique.

1.4. Les règles d'or de la sécurité

1.4.1. Données

- Les données doivent être classées par degré de criticité. C'est à chacun de faire ce travail.
- Cette classification donne des catégories de sensibilité.
- Donner des droits d'accès selon ces catégories en fonction du travail de chaque personne pour limiter la divulgation des données les plus sensibles.
- Donner des droits différents selon le poste occupé : administration, modification ou simplement lecture.
- Une donnée doit avoir une durée de vie : destruction lorsque l'information n'est plus utile.
- Les modalités d'accès, de droits et de destruction doivent dépendre du niveau de classification de la donnée à sa création.

1.4.2. Risques sur les données

Perte de :

- Disponibilité : à la suite d'un déni de service (pour un site marchand par exemple).
- Intégrité : modification d'une donnée (prix d'un produit par exemple).
- Confidentialité : divulgation d'information (secret de fabrication par exemple).

1.4.3. Protéger les données

- En les classant par degré de criticité.
- En engageant la responsabilité des utilisateurs grâce à des habilitations. Permet :
    - Obligation de sauvegardes.
    - De ne pas modifier les données lorsque cela n'est pas nécessaire.
    - De s'assurer que les données ne sont pas accessibles à n'importe qui.
- Suivre la charte informatique de l'entreprise.
- Eviter et dénoncer les mauvais comportements :
    - Ordinateur non verrouillé sans surveillance.
    - Mot de passe sur un post-it.
    - Droits d'accès trop larges.
    - Visiteur non accompagné.
    - Etc…
- Mettre en place un contrôle d'accès aux serveurs.
- Utiliser des outils de chiffrement.
- Assurer une redondance des sauvegardes.
- Etc…

1.4.4. Responsabilités face aux risques

Chacun peut être désigné responsable s'il n'a pas respecté la charte informatique en tant qu'utilisateur.

Attention donc et surtout il faut réagir rapidement en cas de problème détecté.

2. SECURITE DE L'AUTHENTIFICATION

2.1. Mot de passe

Comment les choisir, comment les retenir, quels sont les risques en cas de vol de mot de passe et que faire.

2.1.1. Authentifier dans quels buts :

- Accès à des services en ligne grâce au contrôle d'accès.
- Imputabilité, preuve de qui a fait quoi.
- Traçabilité des actions, historique des actions.

Exemple, télédéclaration de l'impôt : imputabilité = lien entre la déclaration et la personne, traçabilité = connaître l'heure et la date de la déclaration.

2.1.2. Facteurs d'authentification :

- La connaissance.
- La possession.
- Les caractéristiques biométriques.

2.1.3. Limites à la biométrie :

- Chers car il faut employer de lourds moyens.
- Des problèmes juridiques car il faut stocker des caractéristiques morphologiques.
- Contournable avec une photo par exemple.
- Mauvais fonctionnement avec une main brûlée ou une voix enrouée par exemples.
- Peut utiliser la multimodalité mais alors les coûts s'envolent.

2.1.4. Risques du mot de passe :

- Divulgation :
    - Par négligence : faiblesse d'une personne, support amovible, diffusion à un tiers.
    - Par un service non sécurisé : protocoles https, imaps, pop3s, etc… à privilégier.
    - Par l'utilisation d'un vecteur infecté.
    - Mot de passe enregistré sans protection.
- Malveillance :
    - Authentification sur un service illégitime.
    - Attaque par ingénierie sociale, piège.
    - Attaque par force brute ou divulgation d'une base de données mal sécurisée.
- Ces deux cas de figure peuvent entraîner :
    - La compromission des messages personnels.
    - La destruction de données.
    - La publication de messages ou photos préjudiciables sur les réseaux sociaux par exemple.
    - Des achats.
    - Des virements bancaires.
    - Etc…

2.1.5. En cas d'usurpation d'identité :

- Prévenir le responsable SI.
- Déposer plainte auprès des services de l'ordre.
- Signaler l'usurpation aux institutions administratives.
- Demander à vos amis sur les réseaux sociaux d'effacer les messages préjudiciables déposés par l'usurpateur.

2.2. Attaques sur les mots de passe

- Directes, en « devinant » le mot de passe.
- Indirectes, en utilisant la ruse pour le récupérer.

2.2.1. Attaques directes :

- Par force brute.
- Par dictionnaire, en général avant l'attaque par force brute.
- Par permutation en échangeant des caractères (exemple : E par 3 ou O par 0).

2.2.1.1. Vitesse d'attaque :

La vitesse de l'attaque dépend du fait qu'elle se déroule « en ligne » ou « hors ligne ». « En ligne » les attaques peuvent être limitées par :

- La vitesse du réseau.
- Les performances du serveur.
- La limitation du nombre d'essais de connexion.

2.2.1.2. Attaques distribuées :

Ces attaques répartissent la charge de travail sur plusieurs ordinateurs pour être plus rapides.

2.2.1.3. Attaques de proximité :

C'est le fait d'avoir une vue directe sur le mot de passe, en regardant par-dessus l'épaule ou en détectant électromagnétiquement des frappes clavier (possible jusqu'à 20 m) par exemples.

2.2.1.4. Piégeage de poste :

- Par un Keylogger USB.
- Par un logiciel malveillant.

2.2.1.5. Attaque sur mémoire :

- Chiffrer des espaces de données sensibles.
- Démarrage à froid : lors d'une coupure d'alimentation électrique et d'un redémarrage, les systèmes gardent les mots de passe en mémoire vive RAM.

2.2.2. Attaques indirectes :

- Ingénierie sociale, par la ruse.
- Nom de domaine proche : typo squattage.
- Hameçonnage : via un site pour récupérer un identifiant et un mot de passe par exemple.
- Réutilisation de mots de passe issus de sites moins protégés.
- Interception sur le réseau.

2.3. Sécuriser ses mots de passe

- Comment les créer.

- Comment s'en souvenir.
- Comment éviter sa divulgation.

Problèmes rencontrés : compromission, divulgation et oubli.

2.3.1. Mot de passe fort :

Il apporte un niveau de sécurité suffisant, c'est-à-dire difficile à découvrir par un attaquant dans un temps raisonnable à l'aide d'outils automatisés de recherche qui mettent en œuvre les différentes techniques d'attaque.

Il doit être composé au minimum de 10 caractères et ceux-ci doivent être de tout type.

2.3.2. Mémorisation :

- Grâce à une phrase de passe avec des mots concaténés.
- Par phonétique.
- Les premières lettres des mots d'une phrase, citation, chanson, etc…
- Mixer les trois méthodes.

2.3.3. Lutter contre la divulgation du mot de passe :

2.3.3.1. Gérer ses mots de passe :

- Point d'authentification unique : pratique mais possède 2 contraintes :
  - En cas de divulgation, tous les sites seront accessibles au pirate.
  - Peut récupérer les informations des différents services dans un but commercial par exemple.
- Coffre-fort de mots de passe :
  - Avantages :
    - Plus besoin de retenir ses mots de passe.
    - Génération de mots de passe robustes.
  - Inconvénient : pas d'accès à tout moment car il faut disposer de l'équipement informatique support pour le lire.

2.3.3.2. Configuration des logiciels :

- Ne pas mémoriser le mot de passe dans l'application et/ou l'identifiant.
- Utiliser un compte utilisateur au quotidien avec un accès restreint et un mot de passe plus fort pour le compte administrateur.
- Activer le verrouillage automatique de son Smartphone.

2.3.3.3. Cryptographie :

On parle de chiffrement, de déchiffrement et de décryptement. Le verbe crypter n'existe pas car décrypter consiste à chercher à trouver un message chiffré sans détenir la clé de chiffrement. De ce fait il est impossible de crypter.

- Chiffrement symétrique : échange d'une clé qui doit rester secrète. Une clé très longue permet de lutter contre les attaques par force brute.
  - Avantage : simple à mettre en œuvre.
  - Inconvénients :
    - Echange de la clé secrète.
    - Il faut une clé par couple d'interlocuteurs.

- Chiffrement asymétrique : une clé publique chiffre le message et une clé privée déchiffre le message.
    - Avantage : pas d'échange de clé de déchiffrement.
    - Inconvénient : complexité algorithmique élevée donc convient à une petite quantité de données échangées.

- Chiffrement hybride : utilise les deux solutions précédentes. Envoi de la clé secrète par chiffrement asymétrique puis échanges par chiffrement symétrique.

- Signature électronique et Infrastructures de Gestion des Clés (IGC) : la clé privée permet la signature, la clé publique vérifie la signature. Le certificat délivré par l'IGC certifie l'identité de la signature.

3. SECURITE SUR INTERNET

3.1. Internet

Internet n'est pas uniquement le WWW (World Wide Web) qui consiste à consulter des pages web. Il s'agit de ce qui permet de relier des ordinateurs entre eux. Le protocole utilisé pour cela est l'équivalent du code de la route sur notre réseau routier.

3.2. Les fichiers en provenance d'internet

Comme le fait de connecter une clé USB à notre système peut constituer un danger, le fait d'ouvrir ou de télécharger un fichier issu d'internet peut aussi s'avérer dangereux. Cela peut par exemple provoquer le chiffrement des données et ainsi permettre le rançonnage.

3.2.1. Formats et extensions :

Un fichier est une suite de 0 et de 1. Son format est l'agencement de ces 0 et 1 au sein du fichier.

L'extension est le nom qui permet d'identifier le logiciel capable d'ouvrir le fichier par défaut en fonction du format.

Le malveillant exploite les formats et les extensions courants. Par exemple il est possible de cacher un fichier « CV.exe » derrière un nom de fichier en « CV.pdf » dont l'ouverture parait inoffensive.

C'est pourquoi, il est recommandé de :

- Désactiver l'exécution automatique de périphériques amovibles.
- Afficher systématiquement l'extension des fichiers.

3.2.2. Formats risqués :

3.2.2.1. Fichiers :

Il n'existe pas de risque zéro quel que soit le format mais les extensions PDF, DOC et XLS de Microsoft sont très exploitées par les pirates car ce sont des fichiers très largement utilisés. Il existe donc une grande cible d'utilisateurs pour les malveillants.

Plus il existe de vulnérabilités découvertes par les pirates, plus grand est le risque d'attaques.

Sur ces formats, il existe autant de vulnérabilités que d'utilisateurs et autant que de codes malveillants diffusés !

Ceci s'explique par le fait que :

- Les recherches actives sur ces formats entrainent la découverte de beaucoup de vulnérabilités récurrentes dans les logiciels qui les interprètent (Adobe Reader, M.Word, M.Excel).
- Ces fichiers sont complexes et embarquent des codes interprétables différents de textes bruts. Du Javascript pour les fichiers PDF et du Visual Basic Pro Micro pour M.Office par exemples.

Les fichiers exécutables sont aussi de très bons vecteurs de code malveillant. Mais certainement sommes-nous plus vigilants avant l'ouverture d'un tel fichier.

3.2.2.2. Mesures à prendre :

- Maintenir les logiciels à jour.
- Détenir un antivirus à jour et lancer des analyses sur les fichiers.
- Ne pas ouvrir de fichier issu de source non fiable : expéditeur inconnu, courriel suspect, site web peu fiable, etc…
- Avoir une vigilance particulière avec les fichiers exécutables : .exe, .msi, .dmg, etc… Pour ces fichiers, définir des privilèges administrateur afin de pouvoir les ouvrir.
- Réagir immédiatement en cas d'ouverture d'un fichier malveillant en contactant dès la constatation le référent en sécurité des systèmes d'informations de votre entreprise.

La meilleure arme contre l'ingénierie sociale est le bon sens et la réflexion.

3.2.3. Des sources plus sures que d'autres ?

La réponse est OUI !

- Télécharger les logiciels depuis le site de l'éditeur. Un « tick » vert donne le niveau de sécurité du fichier à télécharger. Sans la présence de cette sécurité, le risque est au mieux de télécharger de la publicité ou une extension inutile pour le navigateur, au pire du code malveillant.
- Les logiciels crackés sont utopiques :
    - Pour des raisons éthiques
    - Ils sont illégaux
    - Ils sont un moyen pour les pirates de faire installer des codes malveillants à l'insu des utilisateurs et cela dans un but lucratif.
- Utiliser les plateformes de vidéos à la demande pour télécharger un film sinon il existe des risques pour son système d'exploitation.
- Sur une messagerie, l'identité de l'expéditeur est falsifiable. Il faut donc vérifier la véracité du message en contactant l'expéditeur par un autre canal en cas de doute.

Si vous avez déjà pratiqué une des actions évoquées ci-dessus et que vous n'avez rien constaté sur votre ordinateur, soit, et c'est très improbable, vous avez eu beaucoup de chance soit un code malveillant s'est installé. Plusieurs possibilités :

- Votre machine fait ou a fait partie d'un Botnet en tant que machine Zombie. Elle a donc pu participer à une attaque dans un déni de service distribué ou dans un envoi massif de courriels indésirables.
- Des données ont été exfiltrés (webcam, son, frappes clavier, etc…) avec tout ce que cela peut entrainer : usurpation d'identité, chantage ou autre.

Les attaques les plus efficaces sont les plus discrètes et les attaques les plus persistantes sont conçues pour durer.

Personne n'est à l'abri, aucun système n'est parfaitement étanche.

3.2.4. Se protéger des rançongiciels :

Prévenir :

- Disposer d'une sauvegarde de ses données précieuses : une pour chaque année, une pour chaque mois de l'année en cours, une pour chaque semaine du mois en cours. Ceci assure le plan de continuité d'activité (PCA).
- Vérifier les sauvegardes comme on vérifie son système d'exploitation.
- Tester une à deux fois par an une restauration.
- La restauration doit être déconnectée du système de sauvegarde pour éviter que ce dernier soit affecté lui aussi par un rançongiciel.
- Mettre à jour les logiciels et systèmes (Windows, logiciels favoris, etc…). Cette action corrige les failles identifiées. Si la maintenance n'est plus assurée, changer de solution. Exemple, si votre S.E n'est plus mis à jour, changez-en.
- Repérer les courriels frauduleux en développant de la prudence dans l'utilisation de la messagerie.

Réagir :

- Ne pas payer de rançon.
- Déconnexion immédiate du réseau pour bloquer la propagation.
- Signaler l'attaque à son référent.
- Déposer plainte pour inciter au démantèlement du groupe de pirates.
- Conserver les fichiers chiffrés par les pirates car ils peuvent donner plus tard la clé ou être déchiffrés en cas d'enquête fructueuse.

En France en cas d'attaque il existe Cybermalveillance.gouv.fr :

- Assiste les victimes
- Prévient et sensibilise à la sécurité numérique
- A créé un observatoire de la mémoire numérique

3.3. Navigation Web

Exemple : **https://www.SSI.gouv.fr**

- https : protocole d'échange entre le serveur et ses clients.
- www : world wide web
- SSI : nom de domaine
- .gouv : sous nom de domaine
- .fr : géré par l'AFNIC (Association française pour le nommage Internet en corporation)

Privilégier le protocole sécurisé https plutôt que le http.

3.3.1. Typosquatting

Le typosquatting est le fait d'utiliser un nom de domaine proche du site réel pour tromper un utilisateur. Un seul caractère différent peut renvoyer vers un site complètement différent.

Exemples : www.SSI.gou.fr, www.SSI.gov.fr, www.SSI.gouv.com

Pour diminuer ce risque, il faut réserver un maximum d'URL similaire sur le plan typographique au nom de domaine qui nous appartient avec un maximum d'extensions.

- Attention donc aux fautes de frappe lors de la saisie de l'URL dans le navigateur.
- Vérifier le contenu attendu.
- Enregistrer le site dans les favoris lorsque on est sûr de l'URL.

3.3.2. Moteur de recherche

L'utilisateur considère le meilleur moteur de recherche comme étant celui qui fournit les résultats par rapport au mot clé saisi. 93% des internautes se limitent à la première page de recherche de Google.

La saisie automatique de formulaire s'avère pratique mais donne accès à des données personnelles au pirate introduit dans le navigateur. Cet usage est donc à utiliser avec modération et surtout pas pour les identifiants et mots de passe :

- La messagerie : elle est une mine de données personnelles car le pirate peut y réinitialiser tous vos comptes en ligne et usurper votre identité.
- Mémorisation du numéro de CB à bannir.
- Effacer les historiques de navigation pour éviter de donner les habitudes de navigation.

3.3.3. Cookies

En France, les sites doivent nous demander d'accepter les cookies avant de continuer la navigation.

Ils permettent le stockage d'informations utiles au site sur l'ordinateur de l'utilisateur et plus précisément dans le navigateur. Ils sont réutilisés lors de la visite suivante :

- Ne pas les accepter du tout peut entrainer une mauvaise utilisation du site. Il est préférable de les filtrer pour ne garder que les indispensables à une bonne navigation sur le site.
- Effacer les cookies après avoir visité le site est une bonne pratique.

La navigation privée permet uniquement l'effacement de l'historique de navigation sur l'équipement utilisé. Les demandes de non-traçage associées sont appliquées par les serveurs de site à leur bon vouloir.

3.3.4. Mon navigateur est-il bienveillant ?

Il faut se poser la question.

- Si le message affiché est suspect du type détection de virus, ne pas cliquer sur le lien et fermer la page web.
- Un site web ne peut pas analyser les performances de votre machine. Si un message vous propose ce type d'analyse, fermer la page web.
- Attention aux extensions des navigateurs. Avant de télécharger une nouvelle fonctionnalité, il faut s'assurer de ce qu'elle contient.
- Toutes les extensions Flash et Java sont à proscrire car elles présentent des failles.
- Activer les extensions à la demande et non pas par défaut.

3.3.5. Contrôle parental

Il restreint le périmètre d'accès au web. Attention il n'existe pas de contrôle parental sur smartphone ou tablette, il faut utiliser un moteur de recherche adapté aux enfants comme Qwant Junior.

Si des modifications sont apparues dans le navigateur sans le consentement de l'utilisateur, ne pas hésiter à réinstaller le navigateur.

3.4. Messagerie électronique ou instantanée

3.4.1. Mail/courriel description

- Il peut être envoyé à plusieurs destinataires.
- Son acheminement est gratuit.
- Il n'y a pas besoin de se déplacer physiquement.
- Il est remis presque immédiatement.
- C'est le moyen de communication privilégié par beaucoup.

L'adresse électronique est constituée d'un nom d'utilisateur et d'un nom de domaine séparés par « @ ».

Le serveur de messagerie sert de facteur.

Smtp :

- Protocole qui s'occupe de trouver le destinataire.
- Ne vérifie pas l'expéditeur et le contenu :
    - Le champ expéditeur peut être modifié, il est purement déclaratif.
    - Il faut vérifier la cohérence du contenu et faire attention aux demandes d'informations personnelles. Elles sont souvent l'origine d'escroqueries.
    - L'adresse mail n'est pas un critère d'identification fiable.

3.4.2. Les menaces

3.4.2.1. Ingénierie sociale

Il s'agit d'une tentative de faire exécuter des maliciels derrières des pièces jointes (PDF, Excel, autres) mais plus souvent derrière des liens hypertextes.

Pour faire cliquer, les pirates utilisent des techniques d'hameçonnage associées à de faux expéditeurs. L'objectif est d'obtenir des renseignements personnels tels que le numéro de CB par exemple.

3.4.2.2. Comment les repérer

- Les courriels « piégés » sont souvent peu ou pas personnalisés pour pouvoir concerner un maximum de personnes (message trop vague).
- Ils portent sur un sujet qui ne vous parle pas.
- Attention aux adresses électroniques inconnues.
- Des courriels mal écris (de moins en moins vrai) avec des erreurs de frappe, de mauvaises formulations, des fautes de frappe ne doivent pas être considérés comme crédibles.
- Avant de cliquer sur un lien, passer la souris au-dessus. Le survol permet de lire l'URL du lien.
- Attention au typosquatting.

3.4.2.3. Pourriel

Communication électronique non sollicitée.

Il existe la possibilité de les déclarer en SPAM (courriers indésirables). Cette action est un bon réflexe car elle fait entrer l'adresse dans une base commune pour les internautes et participe à l'effort global de lutte contre les courriers frauduleux.

3.4.3. Bonnes pratiques

- Avoir un mot de passe robuste.
- Créer plusieurs adresses en fonction des usages : ceci permet d'identifier plus facilement les pourriels. Exemple : demande de numéro de CB sur une adresse d'achats en ligne reçue sur une adresse à partir de laquelle aucun achet n'est réalisé.
- Avoir un mot de passe par compte de messagerie. Pour ne pas oublier ses mots de passe, cela il faudra utiliser un coffre-coffre numérique.
- Ne pas diffuser systématiquement son adresse mail. Elle peut être récupérée par des robots sur les forums par exemple. Il faut privilégier les messages privés et utiliser une adresse « poubelle » pour les forums.
- Déconnecter les comptes en ligne :
    - Utiliser la navigation privée.
    - Déconnecter les comptes ouverts.
    - Vider le cache.
    - Nettoyer les Cookies.
    - Fermer le navigateur après avoir consulté son Webmail.

3.4.4. Clients de messagerie

Un client lourd de messagerie doit proposer au minimum :

- Des mises à jour.
- La gestion des courriers indésirables.
- La prise en charge des protocoles sécurisés POP3S et IMAPS.

En plus des fonctionnalités évoquées ci-dessus, avec un client léger de messagerie ou webmail, il faut être attentif à :

- L'utilisation du protocole https.
- Lire les conditions d'utilisation car certains vont jusqu'à analyser le contenu des mails.

3.4.5. Messagerie instantanée

Elle est peu ou pas sécurisée et peut être observée par un attaquant ou le fournisseur du service.

Il est possible de lutter contre cela en chiffrant les communications :

- De client à serveur mais les informations circuleront en clair côté serveur.
- De client à client ou de bout en bout. Cette solution est à privilégier.

Consulter la charte de confidentialité du service pour connaitre le niveau de protection.

Conseils :

- Bloquer les personnes inconnues ou à l'origine de messages indésirables.
- Ne pas cliquer sur des liens non sollicités.
- Privilégier un service chiffré de bout en bout.
- Rester vigilant dans la transmission d'informations.

3.4.6. Cas particuliers

La lecture de MMS peut compromettre un terminal vulnérable : ne pas les télécharger automatiquement et ignorer les MMS de numéros inconnus.

Utiliser les fonctionnalités de signature pour assurer l'identité et de chiffrement pour assurer la confidentialité et l'intégrité du message. Pour aller plus loin, mettre en place des mécanismes de cryptographie avec par exemple S/MIME et PGP.

3.5. L'envers du décor d'une connexion web

3.5.1. Connexion Web

La résolution DNS (Domain Name System), annuaire pour Internet, associe un nom à une adresse IP.

Il faut lire le nom de domaine de la droite vers la gauche : la racine générée par l'ICANN (Internet Corporation for Assigned Names and Numbers) puis en France l'AFNIC pour « .fr ». En théorie l'adresse IP est demandée à chaque requête mais pour plus d'efficacité, les fournisseurs d'accès proposent le « DNS cache » qui permet de garder en mémoire les @IP des noms de domaines pour les futurs usages.

Une requête utilise le protocole http (Hyper Text Transfert Protocol). L'affichage d'une page web peut correspondre à des dizaines voire des centaines de requêtes http pour récupérer l'ensemble des éléments.

3.5.2. Serveur mandataire

Pour éviter de charger l'ensemble des éléments communs des pages d'un site, ils sont mis en cache dans un serveur Proxy. Ceci entraîne un gain en performance mais a aussi un intérêt pour la sécurité. En effet, ce serveur mandataire permet de journaliser les requêtes et ainsi de pouvoir remonter à un incident et ainsi d'identifier, repérer les machines infectées.

Il peut aussi bloquer l'accès à des ressources malveillantes connues.

3.5.3. HTTPS et certificats

HTTP : ce protocole envoie les données en clair. Tous les équipements entre le serveur et le client voient le contenu de la requête et peuvent même le modifier.

Les cryptographes créent le protocole SSL puis TLS, HTTPS. Ce protocole est la garantie d'échanges sécurisés : personne ne peut lire le contenu. Il est conseillé voire indispensable pour les services avec identifiant et mot de passe.

HTTPS :

- D'abord un secret : certificat et crypto asymétrique.
- Ensuite échange avec crypto symétrique, en tunnel de point à point.

Le certificat contient :

- L'identité du serveur visité.
- La clé publique du serveur.
- La signature d'une autorité de certification qui garantit l'intégrité des deux informations précédentes.

Le navigateur vérifie le certificat reçu par comparaison de l'identité.

4. SECURITE DU POSTE DE TRAVAIL ET NOMADISME

4.1. Applications et mises à jour

4.1.1. Vulnérabilités

La recherche de failles dans les systèmes informatiques peut être réalisée par des criminels (black hats) ou des chercheurs (white hats) pour identifier une vulnérabilité.

4.1.1.1. Sécurité par l'obscurité

C'est le fait de maintenir un attaquant potentiel dans l'ignorance du fonctionnement interne du système.

L'utilisateur doit savoir comment faire fonctionner l'outil (partie accessible) mais ne doit pas savoir comment fonctionne l'outil (partie non-accessible).

+ Permet de ralentir l'attaquant.

- Difficile de garantir le niveau de sécurité offert par le produit ; il faut faire confiance.

4.1.1.2. Transparence sur les faiblesses

Elle est à double tranchant.

Les faiblesses trouvées sont communiquées pour que les éditeurs les corrigent. Des CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team) se chargent d'établir une Base de données des vulnérabilités.

+ Edition d'une mise à jour relayée publiquement.

- La divulgation entraîne l'infection possible d'un système non mis à jour.

4.1.1.3. Failles 0-Day

Ce sont des vulnérabilités inconnues, achetées ou vendues sur des marchés non publics. Elles ne sont pas corrigées par l'éditeur car inconnues. Plus le logiciel concerné est répandu, plus le coût d'une faille 0-Day est élevé.

4.1.2. Mise à jour

- Si un système ne propose plus de mise à jour (obsolescent), il faut installer une nouvelle version.
- Le délai important de mise à jour des systèmes embarqués dans les téléphones est exploité par les attaquants. De plus, leur grand nombre rend les attaques rentables. La fréquence de mises à jour du constructeur doit donc être un critère de choix.
- Il est aussi recommandé d'utiliser les mises à jour automatiques.
- Pour les applications de smartphones :
  - Réaliser les mises à jour.
  - Ne pas tout sélectionner sans regarder les extensions potentiellement dangereuses lors de l'installation d'une application.

4.1.3. Installation d'applications

- Limiter les outils présents à son utilisation personnelle. Chaque application a des vulnérabilités potentielles qui sont autant de points d'attaque pour une personne malveillante. Si besoin, il faut supprimer les logiciels après utilisation pour réduire la surface d'attaque (ex : TeamViewer).
- Installer des exécutables issus de sources sûres : sur le site web de l'éditeur et pas sur des plateformes de téléchargement ou un logiciel piraté.
- Ne pas installer sur un smartphone des applications demandant plus de droits que ceux nécessaires pour le service.
- Être vigilant sur le contenu installé : vérifier le contenu à chaque étape d'installation avant de cliquer sur suivant.

4.2. Options de configuration de base

- Au premier démarrage : personnaliser le paramétrage via les « options avancées » ou la « personnalisation ».
- Création de comptes.
- Mises à jour.

4.2.1. Déverrouillage et authentification

- Utiliser des méthodes de déverrouillage biométriques en complément des méthodes classiques permet d'avoir un mot de passe fort et adapté à une utilisation quotidienne sur certains systèmes.
- Changer le code PIN par défaut : modifier les codes du type « 0000 » ou « 1234 ».
- Evaluer les risques liés au déverrouillage et utiliser un mot de passe adapté (plus de 8 caractères, caractères spéciaux, limitation du nombre d'essais, etc…).

4.2.2. Logiciels de sécurité

Tout outil à ses limites mais utiliser un pare-feu et un anti-malware (anti-virus, anti-spyware, etc…) peut s'avérer efficace s'ils sont lancés au démarrage. Il faut bien entendu les télécharger sur les sites des éditeurs.

- Le filtrage d'URL (adresses web) fonctionne par apprentissage et vient compléter une liste noire appelée liste d'exclusion.
- Le contrôle parental est un filtrage beaucoup plus strict :
    - Catégories de sites.
    - Limitations d'horaires.
    - Liste blanche plutôt que liste noire.
- Un anti-malware contrôle les fichiers présents sur l'ordinateur ou les supports de stockage. Ils ne sont pas fiables à 100%, s'exécutent avec des droits élevés et ne sont pas exempts de vulnérabilités. Son maintien à jour est indispensable mais rien ne remplace la vigilance de l'utilisateur car il s'agit d'un logiciel très intrusif.
- Le pare-feu surveille les connexions au réseau. Une fois la connexion établie, il ne contrôle plus rien. Il est donc un élément important de surveillance mais il ne suffit pas à protéger un ordinateur.
- Des incompatibilités dues à la mise en place de deux anti-malwares peuvent provoquer leur dysfonctionnement.

- Sur les systèmes mobiles, les protections sont intégrées au système d'exploitation par d'autres méthodes : cloisonnement des applications, droits réduits, etc…). Attention cependant car ces protections seront perdues en cas de débridage, « jailbreak » ou de « rootage » de l'appareil.

4.2.3. Terminaux mobiles

Ne pas « rooter » son terminal mobile (prendre les droits administrateur) car il sera exposé à une compromission en profondeur.

4.2.4. Données des terminaux mobiles

- Attention, limiter la collecte des informations personnelles par l'éditeur, c'est à chaque utilisateur de décider, en particulier les habitudes de navigation web, les logiciels utilisés, mais aussi les éléments plus sensibles comme les commandes vocales, les frappes du clavier ou encore les résultats des traductions automatiques.
- Désactiver le service de tracking.
- Désactiver la géolocalisation utilisée par de multiples éditeurs lorsque cela n'est pas nécessaire. Attention, la géolocalisation ne se résume pas à l'utilisation du GPS, les réseaux Wi-Fi participent aussi à la géolocalisation.

4.2.5. Chiffrement de l'appareil

Chiffrer les espaces de stockage permet de protéger les données contre un accès illégitime en cas de perte ou de vol. C'est particulièrement utile pour les appareils nomades.

4.3. Configurations complémentaires

4.3.1. Gestion des comptes utilisateurs

Il existe la possibilité de créer des comptes utilisateurs pour les équipements partagés mais pas, pour les tablettes et les smartphones. C'est pourquoi il ne faut pas laisser ces équipements à un tiers.

Il faut :

- Un compte administrateur pour modifier les paramètres système et installer des logiciels.
- Des comptes utilisateurs sans privilèges permet de naviguer sur internet et d'utiliser les logiciels.
- Le compte invité (jetable) permet un accès encore plus restreint et ne permet pas la sauvegarde de données d'une session à l'autre.

4.3.2. Sauvegardes et connexions de l'appareil

4.3.2.1. Sauvegardes

- La disponibilité d'une sauvegarde physique ou déportée sur un cloud est essentielle pour un retour en arrière éventuel.
- Chiffrer la sauvegarde peut être une bonne pratique mais peut s'avérer dangereux (en cas de perte du mot de passe) => il est intéressant d'utiliser un coffre-fort numérique.
- Elles doivent dépendre du type de compte : un utilisateur ne peut sauvegarder que ses propres données.
- Les supports amovibles de sauvegardes ne doivent être branchés que le temps de la sauvegarde et être rangés en lieu sûr.
- Les serveurs de sauvegarde doivent être accessibles mais pas connectés en permanence.

- Les sauvegardes doivent se trouver dans plusieurs lieux afin de les préserver en cas d'incendie ou autre problème : les sauvegardes amovibles dans un lieu différent que le serveur de sauvegarde.
- Les fréquences de sauvegardes sont un compromis entre perte de données et espace de stockage nécessaire. Appliquer la formule vue précédemment peut être un bon compromis.

4.3.2.2. Connexions

- La connexion Wi-Fi sans mot de passe n'offre aucune protection.
- Les connexions Wi-Fi qui utilisent un protocole WEP ou WAP n'assurent pas la protection des données. Un attaquant pourra facilement contourner les faibles sécurités.
- La connexion Wi-Fi WPA2 est recommandée même si elle peut aussi faire l'objet d'attaques. Il faut réaliser systématiquement les mises à jour.
- Lors d'une connexion à un réseau public, il faut s'assurer que les sites visités sont sécurisés et il ne faut pas réaliser d'opérations sensibles telles que des achats ou des opérations bancaires.
- Les objets connectés peuvent servir pour des attaques de masse. En effet, ils peuvent être utilisés pour des attaques par botnet dans lesquelles ils jouent le rôle de rebond.
- Le verrouillage automatique d'une connexion doit être activé avec un délai maximal de 5 minutes.

4.4. Sécurité des périphériques amovibles

4.4.1. Risques au branchement

Un périphérique amovible USB contient un microcontrôleur USB programmé par le micrologiciel qu'il intègre (firmware). Il peut être détourné de son rôle d'origine pour exécuter des commandes sur un ordinateur comme un clavier :

- Téléchargement de logiciels malveillants.
- Reprogrammation d'autres périphériques USB connecté au système.
- Compromission de la chaîne de démarrage de l'ordinateur.

Il est équivalent à un virus de dangerosité élevée car il est invisible de l'anti-virus parce que les actions sont supposées être menées par l'utilisateur (même les chargeurs de cigarette électronique).

- Cette technique est disponible à des attaquants avec peu de moyens et d'un niveau de compétences modéré.
- !!! Se méfier d'un périphérique amovible trouvé. !!!
- Ne pas autoriser la transmission de données en cas de rechargement d'un téléphone portable sur son ordinateur. Mieux vaut recharger son téléphone sur une prise plutôt que sur son ordinateur.

4.4.2. Station Blanche

C'est un ordinateur déconnecté de tous réseaux, utilisé dans le simple but de lancer des analyses virales sur les supports amovibles.

L'utilisation d'une station blanche peut s'avérer efficace pour la détection d'un malware sur un support amovible avant de connecter ce dernier sur son ordinateur mais il demande une attention particulière sur la mise à jour quasi quotidienne de l'anti-malware. Cet usage est donc chronophage et peut représenter un coût de maintenance élevé.

4.4.3. Chiffrement des périphériques amovibles

La clé USB contient-elle :

- Des éléments qui pourraient vous nuire ?
- Des données sensibles de votre entreprise ?

Avec un chiffrement efficace et un bon mot de passe, vous serez serein en cas de perte ou de vol (logiciels : GEMALTO, Bull, etc…).

4.4.4. Durabilité

Il existe plusieurs technologies qui permettent de stocker des données :

- Disque mécanique à plateaux.
- Mémoires flash (SSD, clés USB, cartes SD, etc…).
- Disques optiques (CD, DVD, Blu-ray, etc…).

Ils ont tous une durée de vie limitée en nombre de cycles d'écriture et d'heures de fonctionnement : d'un millier à des centaines de milliers.

Les clés USB sont peu robustes, les CD et DVD peuvent devenir illisibles même en restant dans leur boîte sans utilisation. Il faut donc :

- Les remplacer au premier signe de fatigue.
- Garder deux copies de sauvegarde.
- Ne jamais travailler directement sur les documents enregistrés sur les sauvegardes.

4.4.5. Séparation des usages

Il s'agit d'un concept de base. Il faut séparer les activités de l'entreprise des activités personnelles.

Cela s'applique aussi bien aux supports amovibles de sauvegarde qu'aux sauvegardes en ligne.

4.4.6. Effacement sécurisé

Un fichier effacé ne l'est jamais totalement. L'espace est simplement rendu libre mais les écritures restent jusqu'à la prochaine écriture sur cette zone.

Des logiciels de pointe peuvent même récupérer des données après plusieurs cycles de réécriture.

Le type de mémoire de stockage utilisé ainsi que le type de contrôleur d'accès au stockage jouent fortement sur le niveau de persistance des données et les possibilités d'effacement sécurisé.

Attention à la mise au rebut ou au prêt du matériel même après effacement des données. Des précautions sont à prendre :

- Plusieurs cycles d'effacement par l'utilisation de logiciels de réécritures multiples aléatoires.
- Chiffrer les données sensibles stockées.

Ces techniques ne suffisent pas face à un attaquant disposant de moyens importants.

On peut aller jusqu'à la destruction physique du support.

Les méthodes de destruction des données peuvent être différentes en fonction de la classification de la sensibilité de la donnée.

4.5. Séparation des usages

C'est élément important dans la sécurité informatique.

Vu parfois comme une contrainte, tout est question de mesure.

4.5.1. Le mélange des usages

Travailler avec un équipement personnel pour un travail professionnel est à proscrire car n'importe quel système informatique, même réputé sûr, peut contenir des programmes malveillants.

BYOD (Bring Your Own Device) est un problème pour les entreprises en cas de vol, de perte, d'intrusion, d'un manque de contrôle de l'utilisateur, d'une fuite de données lors d'un départ de l'entreprise.

L'inverse, c'est-à-dire l'utilisation d'un matériel professionnel à des fins personnelles est tout autant problématique pour les mêmes raisons.

4.5.2. Le danger du mélange des usages

- Avec le BYOD, il n'existe pas de contrôle de sécurité par l'entreprise sur les équipements personnels.
- La disponibilité ne peut pas être garantie non plus par l'entreprise car les données non sauvegardées seraient perdues en cas de vol ou d'infection.
- En cas d'utilisation de fausses licences par un personnel, la responsabilité juridique de l'entreprise peut être engagée.
- Un téléphone personnel utilisé à des fins professionnelles pour se connecter à des données stockées sur un cloud de l'entreprise comporte un risque en cas de vol : les accès peuvent être stockés sur l'équipement.
- Raccorder un téléphone pour le recharger à son ordinateur professionnel peut créer un accès non maîtrisé, et par extension atteindre le réseau de l'entreprise.

4.5.3. Bonnes pratiques

4.5.3.1. Solutions organisationnelles

- Suivre les consignes internes (charte informatique) et séparer les usages professionnels/personnels.
- Solutions physiques et politique de sécurité :
    - Réaliser les mises à jour.
    - Connexion au réseau entreprise par VPN spécifique si l'utilisateur n'est pas dans les locaux.
    - Anti-virus mis à jour.
    - Chiffrement des disques durs.

4.5.3.2. Solutions informatiques

- Utiliser des comptes avec accès différents (admin, utilisateur, visiteur).
- Sensibiliser sur les menaces.
- Interdire l'utilisation de son poste professionnel à un tiers.
- Configurer les droits du poste.