SÉANCE SÉCURITÉ: SÉCURITÉ INFORMATIQUE

Objectif : La sécurité des systèmes d'informations est bien souvent pensée d'un point de vue technique. Il est cependant primordial de renforcer un des aspects les plus oublié de la sécurité :« le comportement humain». Les systèmes informatiques présentent des risques d'atteintes à l'intégrité et à la disponibilité du système et des données. L'usager doit en permanence se prémunir de ces risques et y remédier. L'usager analyse les risques en fonction des systèmes et logiciels qu'il utilise, et fait les choix les plus adaptés à sa situation.

A - Les risques informatiques

Les risques informatiques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités, donc il faudra identifier ces risques, les évaluer et les traiter.
Un **risque** est la conjonction de trois facteurs :

« RISQUE = MENACE * VULNÉRABILITÉ * IMPACT »

- Une vulnérabilité : un point faible
- Une probabilité de réalisation d'une menace : possibilité que quelqu'un utilise ce point faible
- Un impact : je suis affecté si la menace se réalise (exemple : perte de données précieuses, perte d'image/réputation, pertes financières...etc.)

Exemple : risque de pertes de données expérimentales

- Vulnérabilité : je prends le train tous les jours avec mon ordinateur portable
- Menace : à cette heure tardive il y a beaucoup d'agressions dans ce train
- Impact : si je perds mon portable, je perds les données expérimentales recueillies pour ma thèse.

Évaluer un risque : c'est estimer l'importance du risque afin d'appliquer le traitement approprié

Traiter un risque c'est soit : le refuser, le transférer, le réduire ou l'accepter.

B - Sécuriser son poste de travail

MACHINE WINDOWS :

- Désactiver le compte invité et limiter les droits administrateur
- Choisir un mot de passe sécurisé pour votre session utilisateur
- Affecter les permissions sur les dossiers et les fichiers partagés
- Désactiver les partages inutiles
- Désactiver les services inutiles
- Pensez à toujours protéger votre ordinateur avec un Antivirus à jour et un Firewall
- Il est essentiel que le poste de travail soit toujours à jour
- Chiffrer les données confidentielles

MACHINE UNIX (LINUX) :

- Utiliser "sudo" pour que chaque application dispose d'un mot de passe. Ceci permettra de limiter les privilèges des utilisateurs
- Désactiver les services inutiles
- Localiser et supprimer/modifier tous les SUID/SGID inutiles
- Configurer un pare-feu efficace
- Mettre à jour les paquets installés
- Enregistrer les événements des applications via le démon syslogd

C - Sécurité des réseaux et des données

Deux **types** de sécurité :

- Sécurité des données : concerne exclusivement les données à l'intérieur d'un système.
- Sécurité des réseaux : concerne les données quand elles transitent entre des systèmes

SÉCURITÉ DES RÉSEAUX

Un réseau est constitué de plusieurs nœuds interconnectés et a pour but de permettre l'échanger d'informations, qui sont appelées des ressources.

La sécurité du réseau consiste à veiller à l'intégrité des ressources d'un réseau, ainsi qu'à leur disponibilité.

Quelques solutions pour protéger son réseau « efficacement »

- La protection des entrées et sorties du réseau (pare-feu, compte réseau…)
- La mise en place d'un pare-feu…
- La création de comptes réseau…
- La protection contre les virus, les espions, les spams et le phishing
- Protéger et limiter les connexions sans fil (Lan, wifi, bluetooth…)
- Mettre en place un système de sauvegarde automatisée
- La signature électronique ou l'authentification des données

SÉCURITÉ DES DONNÉES

Améliorer la sécurité des données face aux risques identifiés, c'est pouvoir assurer :

- Disponibilité (**D**): exemple : un virus a effacé mon disque dur, mon pc a été dérobé
- Intégrité (**I**): exemple : le contenu a été modifié (un virus a modifié mes fichiers)
- Confidentialité (**C**): mon dossier de dépôt de brevet a été piraté
- Traçabilité (**T**) : *Journalisation* (les traces laissés par l'utilisateur sur un ordinateur) et suivi des événements sur le réseau

Panorama des menaces

- Malware : cheval de Troie, enregistreur de frappe, virus, spyware, vers
- Messagerie : canulars (Hoax), phishing, spam
- Web : cookies (petits fichiers laissés sur nos machines par les sites web que nous visitons)
- Smartphone : de plus en plus attaqués !
- *Spoofing* : l'IP Spoofing signifie usurpation d'adresse IP
- *Social engineering* : entraîne une fuite de données
- Techniques : attaque en force, par déni de service, botnet, correctifs, buffer overflow

Comment sécuriser son espace de travail local ?

- En sauvegardant régulièrement ses données sur des supports amovibles ou distants.
- En limitant l'accès à son espace de travail et ses fichiers.
- En maîtrisant ses traces.
- En protégeant son système des logiciels malveillants.
- En identifiant les situations à risques.
- En étant capable de restaurer l'intégrité de son système

Comment sécuriser son espace de travail distant ?

- En déposant ses fichiers dans un espace privé
- En limitant tout risque d'usurpation d'identité

Comment sécuriser ses communications sur les réseaux, dont Internet ?

Les trois propriétés requises pour une communication sécurisée :

- L'authentification : celle du serveur est obligatoire mais pas celle du client
- La confidentialité : assurée par des chiffrements symétriques
- L'intégrité : hashage des données (voir somme de hashage hash)

D - Les logiciels malveillants

Un logiciel malveillant ou maliciel, aussi dénommé logiciel nuisible ou programme malveillant ou pourriciel (« malware » en anglais), est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.

QU'EST-CE QU'UN VIRUS ?

Un virus informatique est un programme qui se répand à travers les ordinateurs et les réseaux en créant ses propres copies.

COMMENT LE VIRUS INFECTE-T-IL L'ORDINATEUR ?

Pour infecter votre ordinateur ou votre smartphone, un programme de virus doit au préalable être exécuté. On peut recevoir ce programme (un fichier) infecté depuis une clé usb, une pièce jointe à un mail, ou le web lors d'un téléchargement.

LES TYPES DE VIRUS :

Ransomware : ce programme a pour but de crypter les données d'une machine ou d'un serveur informatique. Le déblocage des données est soumis au paiement d'une rançon.

Trojan : Un cheval de Troie (*Trojan horse* en anglais) est un type de logiciel malveillant, qui ne doit pas être confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Le rôle du cheval de Troie est de faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'utilisateur.

Les botnets : Réseau de robots, de machines zombies : grands ensembles de machines infectées, contrôlables à distance, permettant divers usages malhonnêtes du réseau(envoi de spam,...etc.)

Ver : Virus capable de s'installer sur une machine sans action de l'utilisateur, via une faille de sécurité du système d'exploitation.

Enregistreur de frappe (*Keylogger*) programme capable de récupérer les touches tapées sur le clavier d'un ordinateur.

QUE FAIRE LORSQUE SA MACHINE A ÉTÉ INFECTÉE PAR UN VIRUS ?

En prévention, il est indispensable d'utiliser un logiciel **antivirus**.

En cas d'infection, un simple passage d'**antivirus à jour** peut suffire. Mais il est parfois nécessaire de remettre la machine à zéro pour s'assurer qu'il ne reste plus aucune «trace» du programme.

E - Les parades

POUR SE PRÉMUNIR DES ATTAQUES SUR SON ORDINATEUR, SMARTPHONE OU TABLETTE:

- Mettre à jour son système, ses programmes et ses applications.
- Utiliser des logiciels de protection
- Être vigilant et pas naïf !
- Se méfier des logiciels gratuits (préférer les logiciels libres de source web connue)

PRÉVENIR LA PERTE DE DONNÉES

- Sauvegardes : duplication sur une autre ressource (Disque externe et serveur distant)
- Régularité des sauvegardes

PRÉVENIR LA PERTE DE CONFIDENTIALITÉ DE SES DONNÉES

- Ne pas stocker vos données sur un support non maîtrisé
  - Attention aux services gratuits
  - Lire et comprendre le contrat d'utilisateur final (CLUF)
- Chiffrer les données sensibles (répertoires, disques, sites…)

PRÉVENIR LA PERTE DE CONFIDENTIALITÉ DE SES COMMUNICATIONS

- Vérifier les URL sensibles
  - Utilisation d'une mauvaise adresse URL : si vous avez l'habitude d'accéder au site de votre banque par l'intermédiaire d'une adresse en particulier et que l'adresse du site auquel vous accédez n'est pas la même, vous pouvez être certain que vous n'avez pas accès à un vrai site. Assurez-vous de toujours vérifier que l'adresse du site auquel vous accédez est exacte.
- Chiffrer de bout en bout (*end-to-end privacy*) les communications sensibles (ex. certains mails, chat..etc.)

CHIFFRER SES COMMUNICATIONS :

- Le chiffrement se répand dans les communications !
- Distinguer chiffrement symétrique et chiffrement asymétrique (par paires de clés, privée et publique).
- Exemples de chiffrement de mails :
  - le logiciel client de mail libre et gratuit Thunderbird, avec l'extension Enigma, peut chiffrer les mails de bout en bout.
  - le service de mail Protonmail permet aussi de chiffrer de bout en bout nativement entre 2 utilisateurs de Protonmail (aucune démarche requise), et propose une autre solution de lecture sécurisée des mails si l'interlocuteur ne sait pas chiffrer et déchiffrer un mail.
- Enjeu de société pour éviter la surveillance de masse entre autres
- Et donc argument commercial ! Whatsapp,...etc,
- Contexte actuel de lutte contre le terrorisme : le chiffrement mis en question (cf affaire Apple versus FBI)
- Problème récurrent des sociétés démocratiques : la liberté versus la sécurité des personnes

F - Les métadonnées

Les bibliothèques et autres organismes qui doivent gérer de très nombreuses ressources documentaires utilisent depuis longtemps des métadonnées. L'objectif étant d'indexer les documents pour en optimiser la recherche et la localisation. Ces métadonnées sont renseignées manuellement, par des humains : par le passé sur des fiches papier, depuis l'informatique, dans des bases de données.
A l'ère du numérique et d'Internet, les métadonnées sont apparues comme un moyen d'optimiser les recherches dans l'immensité des documents disponible-s que ce soit dans les bibliothèques ou sur le Web. Ces métadonnées peuvent être intégrées dans l'entête (invisible) de chaque page HTML par l'auteur de la page (balise <META>). On pourra ainsi préciser le titre de la page, une description et des mots clés.
Mais elles existent aussi pour de simples fichiers locaux sur notre ordinateur.
Et des métadonnées sont indexées par le système d'exploitation des ordinateurs.

INTÉRÊT DES MÉTADONNÉES

- Faciliter la recherche d'information (ex : l'auteur, la date de modification du fichier...etc.) : penser au moteur de recherche interne des systèmes d'exploitation, ou aux moteurs web.
- Faciliter l'interopérabilité
- Faciliter la gestion et l'archivage
- Gérer et protéger les droits
- Authentifier un texte

QUELS SONT LES RISQUES ASSOCIÉS AUX MÉTADONNÉES?

Les applications logicielles qui semblent les plus touchées par la question des métadonnées sont les applications bureautiques telles que Office Microsoft et OpenOffice. Les métadonnées constituent un cas classique d'arme à double tranchant : elles peuvent être à la fois utiles et néfastes.

À titre d'exemple, les métadonnées d'un document contribuent à la catégorisation et à la recherche d'information intelligente (p. ex. par des mots-clés), au contrôle de la version et au déroulement des opérations. La possibilité de voir les commentaires d'autres personnes et les modifications proposées à un document à l'aide de la fonction « suivi des modifications » est essentielle à la collaboration de collègues à un projet. Cependant, les modifications qui ne sont pas acceptées sont toujours conservées dans le document même si elles ne sont pas immédiatement visibles. Et pourraient être vues par inadvertance par des personnes non autorisées lorsque le document est communiqué sous forme de pièce jointe à un courriel ou par disque USB ou encore mis sur le web.

G - Identification et authentification. Protection des mots de passe

IDENTIFICATION ET AUTHENTIFICATION

Identification : déclaratif. On déclare qui on est. Ex. saisir son login (*username)*
Authentification : probatif. On prouve qu'on est celui qu'on prétend. Ex. Mot de passe, qu'on est le seul à connaître.

MODALITÉS DE L'AUTHENTIFICATION

Authentifier un acteur peut se faire en utilisant un ou plusieurs de ses éléments.

- Ce qu'il sait. Par exemple : votre mot de passe, la date anniversaire de votre grand-mère
- Ce qu'il a. Par exemple : une carte à puce
- Ce qu'il est. Par exemple : la biométrie (empreinte digitale, oculaire ou vocale)

RÔLE DE L'AUTHENTIFICATION

Donner accès à une ressource : physque (accès à un bâtiment) ou numérique (donner accès à son mail, à son compte sur un service en ligne ex. réseau social).

QUELQUES USAGES PARTICULIERS

La **double authentification** (ou authentification à deux étapes) consiste pour un système informatique, un service sur le web etc. à demander 2 preuves et non 1 seule.
Le paiement par CB en est déjà un exemple (objet physique + code à taper).
Autre exemple : lors d'un paiement en ligne, il faut à la fois de saisir son numéro de CB etc. mais aussi un code envoyé par sms.
L'authenfication peut se transmettre : c'est la **fédération d'identité** (qui vous permet par ex. d'accéder aux réseaux wifi d'autres universités, aux BU...via eduspot ou eduroam).
Le **SSO (Single Sign On)** est une technique permettant aux utilisateurs d'un réseau de s'authentifier une seule fois pour avoir accès ensuite à plusieurs services (ex. une fois loggué pour consulter son webmail, tant que la session est active, on a aussi accès à ecampus ou à Wims sans se relogguer)

LES CONSEILS DE LA CNIL POUR UN BON MOT DE PASSE

- Un mot de passe en béton : au moins **12 caractères et de 4 types différents**
- Il ne dit rien sur vous
- Un compte, un mot de passe
- Ne jamais l'abandonner en pleine nature
- Deux cadenas valent mieux qu'un
- Les retenir sans les écrire
- Utilisez un gestionnaire de mots de passe

Un gestionnaire de mots de passe permet de constituer une base de données de mots de passe chiffrée par un unique mot de passe « maître » dont la sécurité a pu être vérifiée.

Exemple : ***Keepass***, dont la sécurité a été évaluée positivement par l'Agence nationale de sécurité des systèmes d'information (ANSSI). Sur Mac, *Trousseau d'accès* est fourni avec MacOS.

H - Maîtriser les traces numériques

Certaines traces mémorisées sur le disque dur de l'internaute lors de sa navigation sur le web pourraient être préjudiciables au respect de son identité numérique et de sa vie privée.

L'IDENTITÉ NUMÉRIQUE

L'identité numérique d'un utilisateur se construit donc à partir de plusieurs éléments :

- Les données personnelles associées à son ou ses profils
- Les informations qu'il publie sur le web

- Les informations que d'autres publient à son sujet
- Les traces qu'il laisse consciemment ou non.

Selon le contexte, l'usager peut utiliser des identifiants différents :

- Les identifiants professionnels ou institutionnels créés par l'employeur et liés à l'activité professionnelle, permettant souvent d'accéder à un environnement numérique de travail
- Les identifiants privés, qu'ils soient créés à l'initiative de l'usager pour accéder à des services en ligne pour son usage personnel

Pour maîtriser son identité numérique :

- L'usager choisit judicieusement l'identifiant à utiliser en fonction de son activité
- L'usager limite l'accès aux informations qu'il publie
- L'usager contrôle régulièrement son image sur le web

10 CONSEILS POUR RESTER NET SUR LE WEB – CNIL

- Réfléchissez avant de publier
- Respectez les autres
- Ne dites pas tout
- Sécurisez vos comptes
- Créez plusieurs adresses e-mail
- Attention aux photos et aux vidéos
- Utilisez un pseudonyme
- Attention aux mots de passe
- Faites le ménage dans vos historiques
- Vérifiez vos traces

I - Sauvegarde et synchronisation

SAUVEGARDER : POURQUOI, COMMENT ?

Personne n’est à l’abri d’un crash du disque ou d’une mauvaise manipulation, qui écrase des dizaines de méga-octets de données. Pour se préserver de ces erreurs, il faut sauvegarder ses données.

Les principaux risques auxquels la plupart des gens sont confrontés sont les suivants :

- Perte de données par effacement
- Perte de données par défaillance matérielle
- Sinistre (incendie, dégât des eaux)
- Vol de support (cambriolage).

Pour éviter de tout perdre au moindre problème matériel (panne du disque dur), logiciel (plantage de Windows) ou attaques.

QUELLE FRÉQUENCE DE SAUVEGARDE ?

Cela dépend de la fréquence d'utilisation des fichiers et de l'importance.

QUOI SAUVEGARDER ?

C'est à chacun de voir. A titre personnel, on peut penser aux photos, mails (sauf s'ils sont stockés sur internet), rapports, favoris, carnets d'adresses, etc.

La sauvegarde des données est primordiale dans tout système d'information mais attention, un support de données (obsolescence des supports) n'est viable que pour une certaine durée.

DES MÉTHODES DE SAUVEGARDE

- Simple copie sur un support amovible (il faut penser le faire régulièrement…etc.)
- Le mirroring (RAID…etc.)
- Les logiciels de backup
- Internet (grâce à l'augmentation du débit, mais risque que d'autres y accèdent donc méfiance!)

UNE BONNE POLITIQUE DE SAUVEGARDE CONSISTE À :

- Faire plusieurs sauvegardes, car une des copies peut être défectueuse
- Sauver les données de façon régulière car lorsque des données sont détruites, vous perdez toutes les modifications depuis votre dernière sauvegarde.
- Les sauvegardes ne doivent pas être toutes entreposées dans le même lieu. Si un incendie ravage votre appartement, ou si vous êtes cambriolé vous risquez de tout perdre.

LA SYNCHRONISATION

La synchronisation des données consiste à relier deux répertoires (ou fichiers) pour que leur contenu soit identique. Lorsque la liaison est active, les dernières modifications apportées sur l'un des répertoires sont répercutées sur l'autre. La synchronisation est utilisée sur :

- Les lecteurs multimédia (ex : un Ipad avec Itunes quand ce dernier existait)
- Certains systèmes de sauvegarde (Dropbox ou Google drive, Hubic)

Il est possible de synchroniser deux répertoires qui sont sur un même espace de stockage.

QUELS SONT LES USAGES DE LA SYNCHRONISATION DE DONNÉES ?

- La mise en cohérence de 2 dossiers situés le même ordinateur
- La mise en cohérence de 2 dossiers situés sur 2 ordinateurs distincts ou un ordinateur et un autre dispositif(smartphone, tablette, cloud).