Sensibilisation et initiation à la cybersécurité

Module 2 : règles d'hygiène informatique

12/10/2017
Légèrement adapté par E. VIENNET
Pour la LP ASUR Oct 2018

Ce document pédagogique a été rédigé par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité.

Plan du module

1. Connaitre le Système d'Information
2. Maîtriser le réseau
3. Sécuriser les terminaux
4. Gérer les utilisateurs
5. Sécuriser physiquement
6. Contrôler la sécurité du S.I.

1. Connaître le Système d'Information

a) Identifier les composants du S.I.
b) Inventorier les biens
c) Types de réseau
d) Interconnexion

1. Connaître le Système d'Information

a. Identifier les composants du S.I.

Au-delà de la connaissance des composants du S.I., l'inventaire permettra par la suite de mieux déterminer les menaces et les mesures de protection applicables.

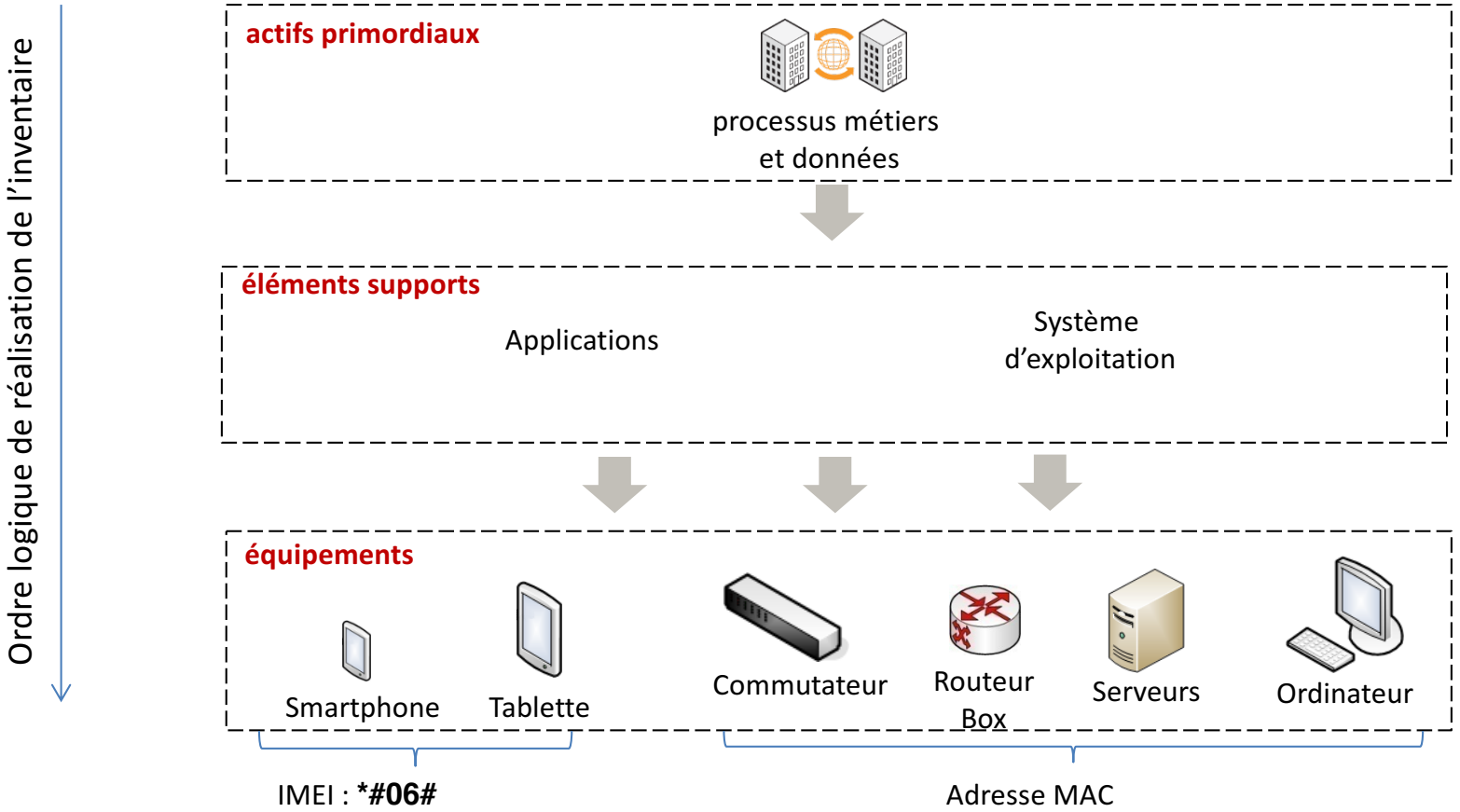
Tout projet sécurité doit donc forcément intégrer un inventaire des biens.

L'inventaire des biens doit suivre une méthodologie logique afin d'être exhaustif, en commençant par l'inventaire des métiers.

1. Connaître le Système d'Information

a. Identifier les composants du S.I.

Différents éléments composent le SI



Comprendre son S.I. passe par l'identification de ses composants.

1. Connaître le Système d'Information

b. Inventorier les biens

Identifier

- Les **données sensibles** :
  - mots de passe, cartes de crédit, documents personnels, etc.
  - plan marketing, fichier client, brevets, contrats, etc.
- Les **applications** avec leur version : Office 2016, navigateurs Web, etc.
- Les **systèmes d'exploitation** : Android, iOS, Windows, Linux, MacOS, etc.
- **Equipements** : ordinateur, tablette, téléphone, serveur, box, routeur, etc.

Inventorier

- Outil d'identification des ordinateurs en réseau
  - Exemple : ServiceNow, HP OpenView, GLPI (Open Source);
- Outil d'identification des logiciels installés sur un ordinateur/téléphone ainsi que des versions
  - Exemple : Everest.

1. Connaître le Système d'Information

c. Types de réseau

- BAN (Body Area Network) : réseau composé de télé transmetteur utilisé dans le domaine de la santé ;
- PAN (Personal Area Network) : réseau centré autour d'une personne interconnectant ordinateur, téléphone, tablette, voiture... (moins de 10m) ;
- WPAN (Wireless PAN) : réseau PAN sans fil utilisant des technologies telles que : IrDA, ZigBee, Bluetooth, Wireless USB ;
- LAN (Local Area Network) : Réseau local interconnectant plusieurs périphériques et permettant l'échange d'informations entre plusieurs individus ;
- MAN (Metropolitan Area Network) : réseau plus large qu'un LAN et étendu par exemple sur une ville ;
- CAN (Campus Area Network) : réseau s'étendant sur plusieurs LAN, et de la taille d'une université ;
- WAN (Wide Area Network) : réseau d'une étendue nationale ou internationale. Exemple : Internet.

1. Connaître le Système d'Information

d. Interconnexion

Connaitre et maîtriser les points d'interconnexion

- Accès Internet via :
  - Box Internet (ADSL, Fibre, …) ;
  - téléphone/carte 3G/4G, etc.

- Interconnexion avec d'autres réseaux (universités, partenaires, prestataires, etc.)
  - Liaison dédiée : E1/T1 carrier, fibre noire ;
  - Réseau privé virtuel (VPN) sur un WAN appartenant à un opérateur ou sur Internet ;
  - Liaison satellite.

CyberEdu
La sécurité par l'enseignement supérieur des NTIC

2. Maitriser le réseau

a) Sécuriser le réseau interne
b) BYOD (Bring Your Own Device)
c) Contrôler les échanges internes
d) Protéger le réseau interne d'Internet
e) Accès distant
f) Sécuriser l'administration
g) Wifi

2. Maitriser le réseau

a. Sécuriser le réseau interne

Créer des zones dans le réseau interne

- Zones distinctes pour les serveurs, postes de travail, visiteurs ;
- Assurer la confiance par l'authentification mutuelle des composants :
  - chaque composant s'authentifie avant le début de l'échange ;
  - permet d'éviter l'usurpation d'identité.
- Assurer le cloisonnement au moyen de : VLAN, VRF, sous-réseaux et ne pas oublier d'implémenter un mécanisme de filtrage !

Restreindre les accès aux réseaux internes

- 802.1X permet de contrôler l'accès réseau et de s'assurer que l'autorisation n'est accordé qu'après authentification de l'utilisateur ;
- Recourir à l'authentification avant d'autoriser l'accès au réseau :
  - l'authentification peut se faire par l'usage d'un certificat ou d'une carte à puce ;
  - l'authentification est centralisée sur un serveur qui donne les accès en fonction de l'identité de l'utilisateur (Exemple : Serveur Radius).

2. Maitriser le réseau

b. BYOD (Bring Your Own Device)

- Le réseau permet de partager des informations, mais aussi de propager les infections de codes malveillants.
- Les terminaux personnels n'ont pas le même niveau de sécurité que les terminaux de l'entreprise / université :
  - Sur un terminal personnel, un utilisateur installe les logiciels de son choix, avec la configuration de son choix. L'antivirus n'est pas forcément à jour ;
  - Sur un terminal professionnel, les logiciels sont installés de manière centralisée, et les sources vérifiées.
- Les terminaux personnels sont connus pour être une source de fuite de données sensibles pour l'entreprise (de façon volontaire ou par erreur).

Le S.I. est un tout, un maillon faible peut affaiblir tout l'ensemble.

2. Maitriser le réseau

c. Contrôler les échanges internes

- Filtrer les flux pouvant être échangés entre les zones :
  - identifier les ports réseau utiles ;
  - identifier les protocoles réseau autorisés ;
  - disposer d'une matrice de flux indiquant les flux autorisés et interdits entre les zones.

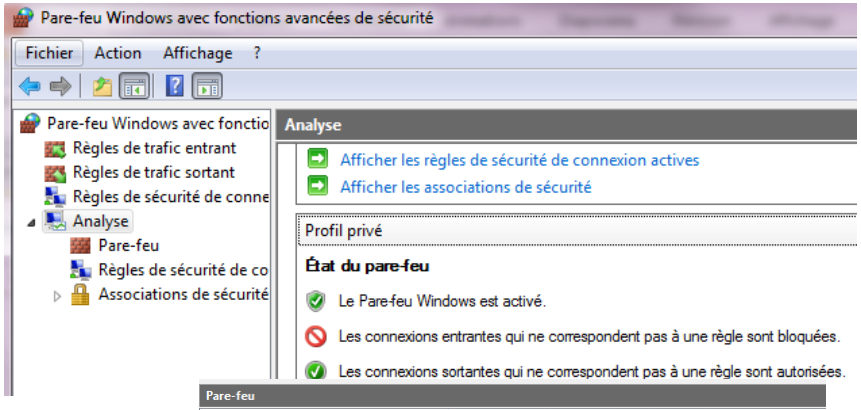
- Autoriser explicitement des adresses IP (machines) d'une zone à échanger avec les adresses IP (machines) d'une autre zone
  - Utiliser une « liste blanche » d'adresse IP pour les échanges, et non pas une liste noire. Une liste noire ne peut en effet jamais être exhaustive, et est forcément d'un intérêt limité.

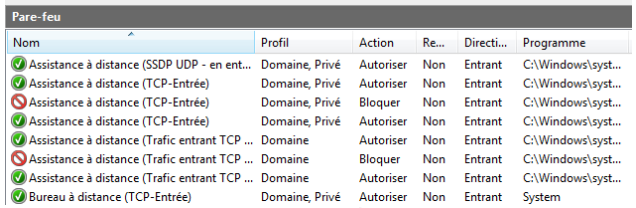
Appliquer le principe « *Tout ce qui n'est explicitement autorisé est interdit* » lors de la gestion des flux.

2. Maitriser le réseau

d. Protéger le réseau interne d'Internet

- Le réseau interne est à protéger et est considéré comme « **de confiance** » ;
- Les équipements interagissant avec Internet peuvent être
  - placés dans une zone spéciale appelée « **Zone Démilitarisée (DMZ)** » ;
    - avec un niveau de filtrage et de contrôle plus accru que le réseau interne.
  - protégés d'Internet par des « pare-feux » filtrant les échanges de flux
    - Équipement dédié protégeant le réseau ou logiciel « pare-feu personnel »
      - sous Windows, utiliser le pare-feu par défaut ou un pare-feu tiers (exemple Zone Alarm) ;
      - toujours contrôler les connexions entrantes ;
      - autoriser les applications au travers du pare-feu, au cas par cas.





  - protégés derrière des IDS et des IPS qui peuvent
    - détecter les tentatives d'intrusion ;
    - prévenir les attaques.

2. Maitriser le réseau

e. Accès distant

- Il est possible d'accéder à distance à un réseau pour faire :
  - du télétravail ;
  - de la téléassistance ;
  - de la téléadministration.

- Il est recommandé d'avoir des points d'entrée identifiés pour les accès distants :
  - Serveurs d'authentification : TACACS+, RADIUS ;
  - Concentrateurs VPN ;
  - Remote Access Server (RAS).

2. Maitriser le réseau

e. Accès distant

- Utiliser des moyens sécurisés pour les accès distants :
  - **SSH** au lieu de telnet : pour l'établissement de connexion à distance sur un équipement ;
  - Secure remote desktop : pour la prise en main à distance d'un bureau ;
  - **SFTP** ou **SCP** : pour la copie distante ;
  - **HTTPS** : pour l'accès à une interface Web (Exemple : Teamviewer) ;
  - Réseau Privé Virtuel (**VPN**) établit sur un réseau qu'on ne maitrise pas, tel que Internet :
    - VPN IPSEC : permet l'authentification et le chiffrement. Il est utilisé pour protéger le trafic réseau ;
    - VPN SSL : protège essentiellement le trafic Web, et est facile à déployer.

2. Maitriser le réseau

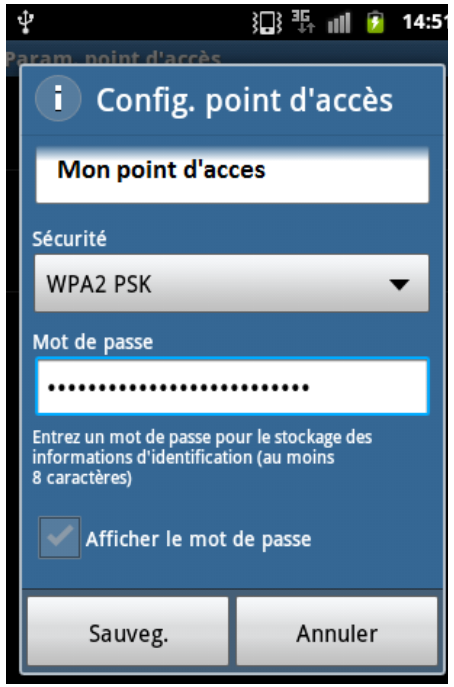
f. Sécuriser l'administration

- Restreindre/Interdire les interfaces d'administration depuis Internet
  - L'administration d'un composant ne doit pouvoir se faire que depuis le réseau interne (ouvrir un accès VPN en cas de nécessité d'accéder à distance) ;
- Restreindre les accès aux interfaces d'administration sur les sites Web :
  - Pour des sites web développés avec des CMS (Content Management System) comme Joomla ou WordPress :
    - Le lien de la page d'administration peut être facilement trouvé (sauf à la modifier) ;
    - Des attaques en « brute force » peuvent être menées pour deviner le mot de passe administrateur ;
    - Modifier le compte « admin » par défaut.
- Utiliser un réseau d'administration dédié :
  - Ce réseau doit être séparé du réseau de production de manière à ce que seul les postes autorisés puissent s'y connecter ;
  - Avoir une liste blanche des administrateurs autorisés à se connecter à ce réseau ;
  - Authentifier mutuellement les postes des administrateurs et les équipements à administrer.

2. Maitriser le réseau

g. Wifi

- Pour sécuriser son réseau Wifi (fourni par sa box ou son téléphone), il faut :
  - Protéger la confidentialité des communications en effectuant un chiffrement à l'aide d'une clé :
    - La clé doit être composée de plusieurs caractères alphanumérique(au moins 15).
  - Choisir la technologie WPA2 (**W**i-Fi **P**rotected **A**ccess **2**) ;
  - Choisir l'algorithme de chiffrement CCMP (**C**ounter **C**ipher **M**ode **P**rotocol) lorsque possible ;
  - Modifier le SSID (nom du réseau Wifi fourni) ;
  - Modifier les identifiants fournis par défaut pour accéder à l'interface d'administration :
    - en général, sur les box, saisir l'url « http:192.168.1.1 » pour atteindre l'interface d'administration.
  - Ne pas divulguer sa clé WIFI.



2. Maitriser le réseau

g. Wifi : WPS

- Ne pas utiliser le WPS (Wi-Fi Protected Setup), notamment fourni sur certaines box internet, car reconnu vulnérable à une attaque par force brute sur le code PIN. Sur les box internet, il est donc préférable de configurer la connexion Wi-Fi manuellement et choisir son propre mot de passe (robuste) ;

- ou cocher l'option qui permet de désactiver automatiquement le WPS au-delà de 5 tentatives de clé.

2. Maitriser le réseau

g. Wifi : Wifi privé vs Wifi public

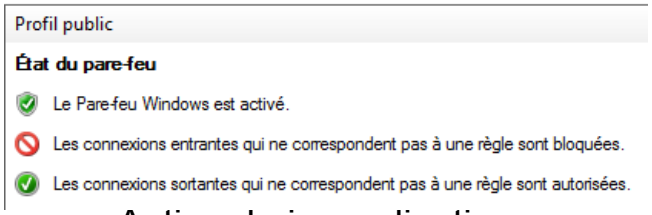
- Le Wifi privé peut être utilisé dans le réseau interne pour donner l'accès à des personnes de confiance. Dans un LAN, on peut utiliser le wifi comme moyen d'interconnexion. On parle alors de WLAN ;
  - Pour ces wifi en entreprise, mettre en place si possible une authentification par certificats, cela évite que tous les utilisateurs partagent le même mot de passe.

- Le Wifi public (hotspots) : est fourni aux personnes « de non confiance » ou au grand public, et est généralement fourni pour un accès Internet uniquement :
  - Hotspot Wifi : Wifi dans les aéroports, McDo, etc.
  - Être conscient que tous les utilisateurs connectés sur le même hotspot peuvent écouter toutes les conversations (sauf si la page WEB visitée est en HTTPS).

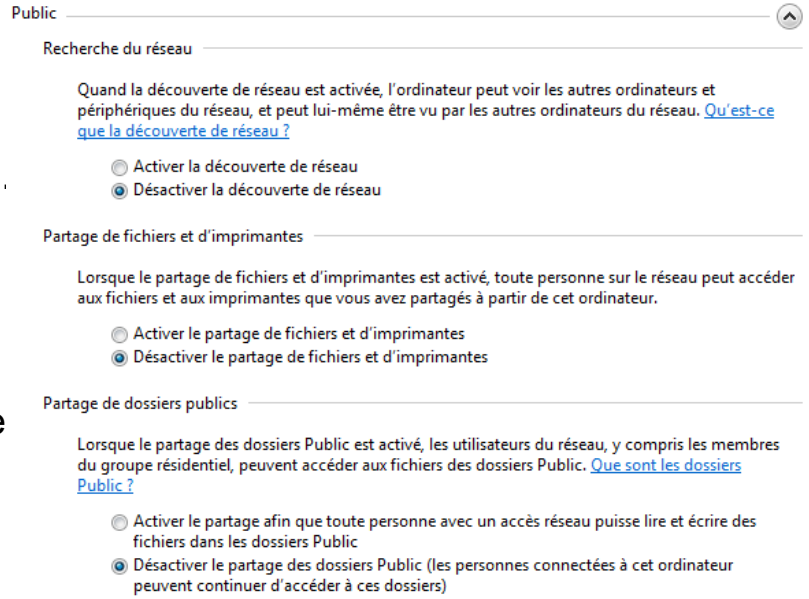
2. Maitriser le réseau

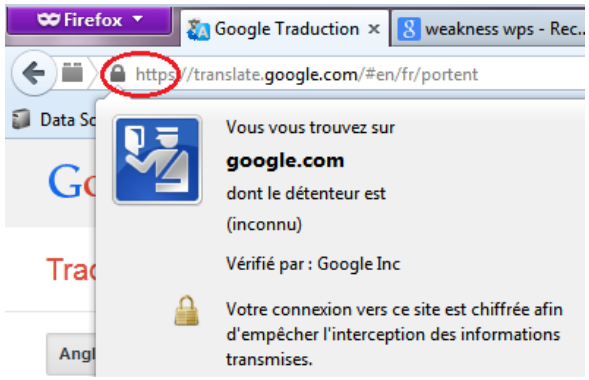
g. Wifi : Bonnes pratiques en cas d'usage du Wifi Public

- désactiver les options de partage :
  - arrêter la découverte réseau ;
  - arrêter le partage de fichier et d'imprimantes.
- Activer le pare-feu du poste
  - Sous Windows, Mac et Linux, un pare-feu existe par défaut :
    - Contrôler les connexions entrantes et lorsque possible, les connexions sortantes ;



    - Activer la journalisation.
  - Éviter de se connecter sur des sites peu sécurisés (utilisant du HTTP) ;
  - Vérifier que les communications vers les sites Internet se font en HTTPS.





Si cela est possible, utiliser un VPN sur un Wifi public.

CyberEdu
La sécurité par l'enseignement supérieur des NTIC

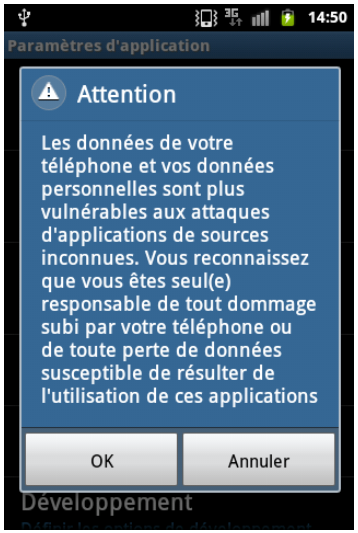
3. Sécuriser les terminaux

a) Choisir les applications
b) Mises à jour logicielles et systèmes
c) Antivirus / Antimalware / Antispyware
d) Symptômes de présence des codes malicieux
e) Protéger les données
f) Durcissement de configuration des équipements

3. Sécuriser les terminaux

a. Choisir les applications

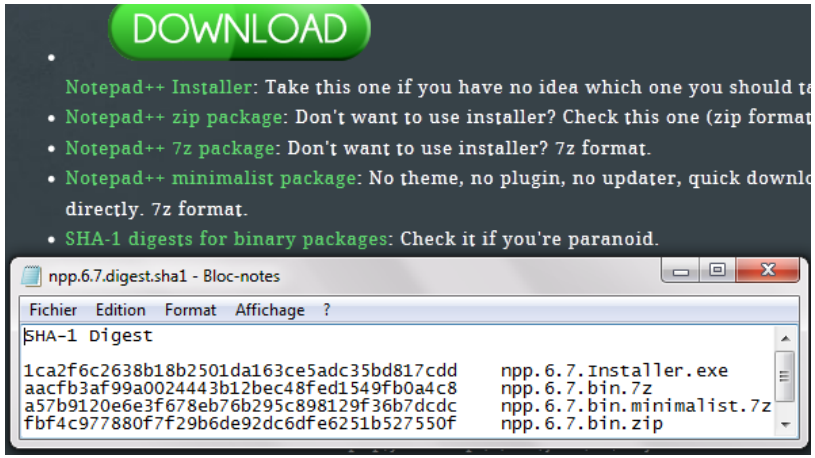
- Pourquoi faut-il être vigilant concernant les logiciels téléchargeables ?
  - On ne connait pas forcément ni l'auteur, ni le site hébergeant ce logiciel ;
  - Certains escrocs sont spécialisés dans la fourniture de chevaux de Troie : un malware est fourni avec le logiciel, dont l'objectif peut être de récupérer login, mot de passe, numéro de carte bancaire.
- Préférer des sources « sûres »
  - utiliser des sources « de confiance » pour télécharger les logiciels ;
    - Sous Android : interdire le téléchargement d'application depuis des sources inconnues.
  - utiliser les sites officiels (site de l'éditeur) pour les téléchargements.

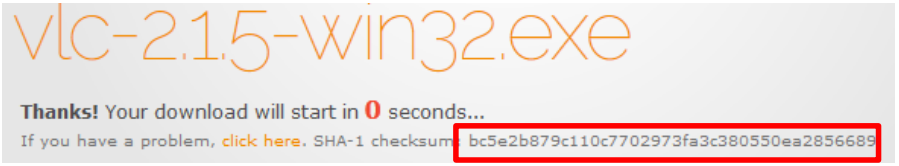


3. Sécuriser les terminaux

a. Choisir les applications

- Vérifier la signature d'un logiciel
  - recalculer la signature du fichier téléchargé avec la signature (checksum) indiquée sur le site, et comparer.





3. Sécuriser les terminaux

a. Choisir les applications

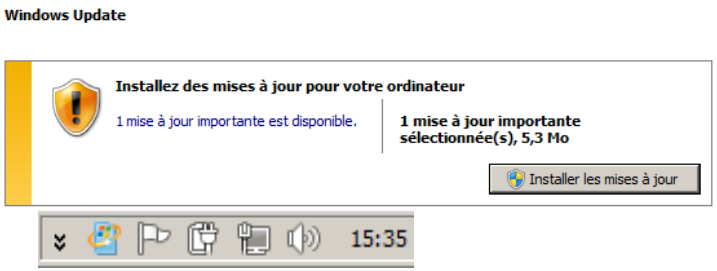
- « Crack » logiciels
  - les sites proposant les « cracks » ou clés gratuites pour les logiciels payants sont souvent truffés de logiciels malveillants ;
  - les versions « crackées » de logiciels contiennent souvent des logiciels malveillants.

- Les logiciels gratuits
  - SnapDo est un pirate de navigateur qui infiltre les navigateurs Internet (Internet Explorer, Google Chrome, et Mozilla Firefox) via des téléchargements de logiciels gratuits.

3. Sécuriser les terminaux

b. Mises à jour logicielles et systèmes

- Rôle : apporter des corrections à un(e) logiciel/application afin de corriger un dysfonctionnement ou une vulnérabilité ;
- Les mises à jour s'appliquent :
  - aux applications, aux systèmes d'exploitation, etc.



- En entreprise, les mises à jour s'effectuent de manière centralisée
  - Téléchargement sur des serveurs dédiés exemple serveur WSUS pour Windows ;
  - Déploiement et observation sur des machines de test ;
  - Sauvegarde des machines de production ;
  - Déploiement sur les machines de production.

3. Sécuriser les terminaux

b. Mises à jour logicielles et systèmes

- Les mises à jour ne concernent pas que le système d'exploitation : tous les logiciels peuvent présenter des failles et doivent être mis à jour régulièrement également ;
  - Flash, Shockwave, Javascript, les lecteurs PDF sont connus pour nécessiter des mises à jour régulières ;
  - La plupart des logiciels ont une option qui permet une « mise à jour automatique », il est recommandé de l'activer.

- Attention en entreprise, c'est à l'administrateur de planifier et valider les mises à jour (cela inclut notamment des tests préalables de non régression).

3. Sécuriser les terminaux

c. Antivirus / Antimalware / Antispyware

- Ces logiciels peuvent être :
  - Gratuits :
    - installé par défaut lors de l'achat du terminal ou par l'éditeur du système d'exploitation (Microsoft Security Essential) ;
    - ou manuellement : Avast, Malwarebytes.
  - Payants : par exemple McAfee, Norton Antivirus.
- Ils nécessitent des mises à jour régulières du **moteur** et de la **base antivirale** pour détecter les nouveaux codes malveillants ;
- Lors de l'apparition d'un nouveau code malveillant, des éditeurs de solutions antivirales effectuent des analyses afin de :
  - déterminer la « **signature** » de ce code malveillant pour l'identifier de manière unique ;
  - identifier les moyens de protection et des corrections ;
  - enrichir leur base antivirale avec ces informations.

Éviter d'exécuter les scans gratuits depuis les pages Internet vous indiquant que votre ordinateur est infecté.

3. Sécuriser les terminaux

c. Antivirus / Antimalware / Antispyware

- Doivent être configurés de manière à :
  - Télécharger automatiquement les nouvelles signatures (base antivirale) ;
  - Être toujours actif (faire attention si votre antivirus est désactivé) ;
  - Scanner tout l'ordinateur sans exception de répertoires / fichiers ;
  - Effectuer des analyses complètes de manière périodique ;
  - Analyser automatiquement de nouveaux périphériques tel que les clés USB ;
  - Analyser les emails (entrants et sortants) et la messagerie instantanée.
- **Limites**
  - Il n'y a pas de base exhaustive pour les virus ;
  - Un code malveillant peut sévir dans un système disposant d'un antivirus et y demeuré indétecté ;
  - Les antivirus ne détectent que les virus dont les signatures sont « *connues* » ;
  - De très nombreux codes malveillants sont créés chaque jour.

L'antivirus n'est pas une « arme absolue ». La mise à jour des systèmes et des applications, ainsi qu'une bonne hygiène informatique sont indispensables.

3. Sécuriser les terminaux

d. Symptômes de présence des codes malveillants

- Ralentissement
  - du terminal : exemple pendant l'arrêt et le redémarrage ;
  - du débit : la bande passante semble partagée.
- Ouvertures régulières de fenêtres de pop-up et de publicités ;
- Modification de la configuration de votre navigateur web
  - Modification de votre page d'accueil ou de votre moteur de recherche ;
    - Exemple : Snapdo.
  - Présence de nouvelles extensions que vous n'avez pas installées.
- Surconsommation des ressources
  - Réduction de l'espace libre sur disque sans raison ;
  - surcharge du processeur.
- L'antivirus/antimalware ou pare-feu est désactivé sans votre intervention ;
- Les mises à jour système/antivirus/antimalware échouent systématiquement ;
- Messagerie
  - vos contacts (amis/famille) reçoivent des messages que vous n'avez pas envoyés ;
  - votre boite d'envoi contient des messages que vous n'avez pas envoyé.

3. Sécuriser les terminaux

e. Protéger les données

- Lors des échanges par mail
  - chiffrer les pièces jointes ou les données sensibles
    - exemple : AxCrypt, Zed Container ;
    - envoyer le mot de passe (Clé) par un autre moyen : SMS.
- Lors de l'usage du Cloud
  - utiliser des logiciels spécialisés pour protéger/chiffrer vos données dans le Cloud (DropBox, Box, SkyDrive…).

VIVO EnCrypted Cloud alephcloud Safebox

- En effectuant des sauvegardes
  - disque externe ;
  - Cloud.

Chiffrer vos données sensibles avant de les stocker.

3. Sécuriser les terminaux

f. Durcissement de configuration des équipements

- Modifier les mots de passe des comptes par défaut ;
  - exemple : administrateur.
- Désinstaller les logiciels/services inutiles (exemple : partage de fichiers) ;
- Désactiver les ports/lecteurs non utilisés ;
  - port série / port USB ;
  - lecteur de disquette ;
  - désactiver le « débogage USB » sur les téléphones.

- Mettre un mot de passe BIOS lors de la phase de démarrage ;
  - Lors du démarrage du poste, appuyer sur « F2 » pour rentrer dans le Setup ;
  - Aller dans l'onglet « Security » pour saisir les mots de passe.
- Désactiver le boot sur des périphériques externes (clé USB, CD Rom) ;
  - Dans le setup (Touche « F2 » lors du démarrage), configurer l'ordre de démarrage pour avoir le disque dur en premier.
- Activer la journalisation.

4. Gérer les utilisateurs

a) Attribution de privilèges
b) Rôles utilisateur
c) Mots de passe
d) Autres méthodes d'authentification
e) Sensibilisation des utilisateurs
f) Spam
g) Phishing / Spear phishing / Social engineering
h) Réagir en tant que victime

4. Gérer les utilisateurs

a. Attribution de privilèges : grands principes

- « Moindre privilège » : n'attribuer aux utilisateurs que les droits dont ils ont besoin pour effectuer leurs tâches ;
  - ne pas donner les privilèges importants à tous les utilisateurs, seulement à ceux qui en ont besoin ;
    - Exemple : le privilège « Administrateur »
  - pour un visiteur qui a juste besoin d'accéder à Internet : ne pas lui donner un accès aux disques ou aux applications sensibles.

- « Besoin d'en connaitre » : donner les accès et les privilèges appropriés aux utilisateurs :
  - donner accès seulement aux données nécessaires aux utilisateurs ;
  - restreindre l'accès aux répertoires contenant les données sensibles.

4. Gérer les utilisateurs

a. Attribution de privilèges : recommandations

- Attribuer les comptes aux utilisateurs de manière nominative ;
  - Un utilisateur = un compte ;
  - Tracer les actions effectuées par chaque utilisateur ;
  - Éviter les comptes partagés entre plusieurs utilisateurs.
- Faire signer une charte d'utilisation du SI, informant sur :
  - La conduite à tenir lors de l'usage du SI ;
    - Actions encouragées :
      - Utiliser son poste pour des recherches, pour le travail qui est confié ;
      - protéger ses moyens d'accès : badge, identifiant, etc.
    - Actions interdites :
      - installer des logiciels malveillants / arrêter les outils de détection de codes malveillants ;
      - porter atteinte à un autre utilisateur du SI.
  - Les conditions et les règles d'utilisation des ressources du S.I. ;
  - Les responsabilités de l'utilisateur et ceux de l'entreprise/université ;
  - Les sanctions internes, pénales, civiles encourues ;
- Sous Windows, la commande « **GPEDIT.msc** » permet de configurer de manière fine les droits des utilisateurs.

4. Gérer les utilisateurs

a. Attribution de privilèges : procédures d'attribution / retrait de privilèges

- Définir une procédure d'attribution/retrait de privilèges.
  - Tenir à jour une liste des droits attribués à chaque utilisateur ;
  - Chaque nouveau compte utilisateur doit être créé en respectant les principes d'attribution de privilège ;
  - Au besoin, chaque utilisateur doit avoir son répertoire personnel et sa boite aux lettres ;
  - Lorsque qu'un utilisateur n'a plus besoin d'accéder au système (démission, changement de poste…), la procédure de retrait de droit doit :
    - Décrire la désactivation de son compte et la suppression de son compte ;
    - Décrire la procédure de retrait des accès aux locaux (badge, clés).

4. Gérer les utilisateurs

b. Rôles utilisateur

- Le rôle « **administrateur** » : ayant les privilèges les plus élevés sur le système. Il peut être de plusieurs types :
  - Administrateur système : en charge de l'administration des systèmes, de la gestion des disques ;
  - Administrateur réseau : en charge des équipements réseaux, des règles de filtrage ;
  - Administrateur sécurité : en charge de la journalisation, de la supervision.

- Le rôle « **utilisateur** » : ayant le droit d'utiliser le système et d'accéder à des répertoires sensibles ;

- Le rôle « **invité** » : ayant peu de droits, et pas d'accès aux répertoires contenant les informations sensibles.

4. Gérer les utilisateurs

c. Mots de passe : politique de mots de passe

- Définir une politique de mot de passe qui oblige à
  - Créer un mot de passe complexe :
    - différent d'un mot sorti du dictionnaire ;
    - différent d'une date de naissance (celle de votre conjoint, enfant…) ;
    - différent d'une partie du nom d'utilisateur, du nom, ou du prénom, etc.
  - Avoir un mot de passe d'au moins **8** caractères (**10** pour les admin) ;
  - Changer régulièrement les mots de passe (tous les 6 mois) ;
    - la fréquence des changements dépend de la sensibilité des systèmes accédés, par exemple le code pour accéder en ligne à son compte bancaire sera changé plus régulièrement.
  - Utiliser un mot de passe pour déverrouiller l'écran de veille.
- Consulter les recommandations élaborées par l'ANSSI.
  http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/mot-de-passe.html

4. Gérer les utilisateurs

c. Mots de passe : mémorisation

- Ne pas choisir le même mot de passe pour différents comptes.
  - Même si ce principe devient difficile à respecter au vu du nombre de mots de passe que les utilisateurs doivent se rappeler ;
  - A minima, **ne jamais réutiliser son mot de passe de messagerie**. Le compte email devient en effet le pivot numérique de chacun.
    - En cas de perte de mot de passe, c'est souvent grâce à la boite email que l'on est en mesure d'en régénérer un nouveau ;
    - L'email sert aux sites marchands pour nous identifier lors de l'ouverture d'un compte ;
    - Si le compte email se fait pirater, c'est une partie significative de la vie numérique de l'utilisateur qui est affectée (usurpation d'identité, suppression malveillante de documents, changement forcé de mots de passe et impossibilité de les régénérer…).

4. Gérer les utilisateurs

c. Mots de passe : aide-mémoire

- Aide-mémoire pour construire des mots de passe complexes :
  - Choisir une phrase comme mot de passe, on parle encore de « **passphrase** ».
    - Exemple : « Aujourd'hui je vais à l'aéroport. »
  - Ne garder que la première lettre de chaque mot puis un mot complet
    - **Ajvàlaéroport**
  - remplacer « s » par « **$** », les « e » par « **3** » ;
  - Ajvàl@3r0port

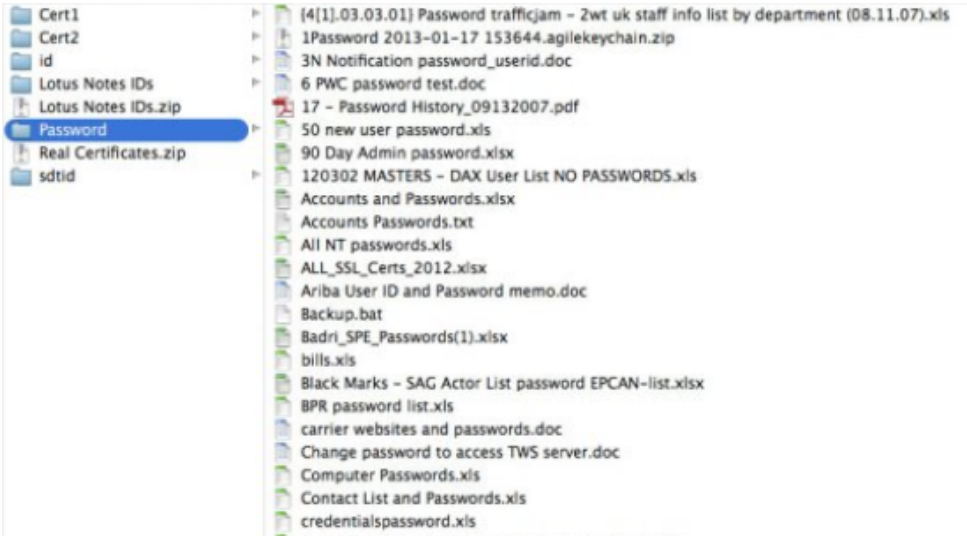
- Le mot de passe est personnel et doit être mémorisé
  - ne pas écrire les mots de passe sur les post-it ;
  - Il existe des solutions pour stocker les mots de passe sous forme sécurisée (voir diapositive suivante).

Les outils pour deviner les mots de passe, prennent parfois en compte le remplacement de « a » par « @ ».

4. Gérer les utilisateurs

c. Mots de passe : stockage des mots de passe

- Toujours stocker les mots de passe sous forme chiffrés
  - Mauvais exemple : Sony, répertoire nommé « Password » et contenant les mots de passe « en clair » ;
- Utiliser des « porte-feuilles » de mots de passe :
  - Dashlane - KeyPass – 1Password ;
  - ou créer votre « porte-feuille », chiffré et protégé par un mot de passe fort.
- ***Ne pas enregistrer les mots de passe sur les navigateurs Web.***



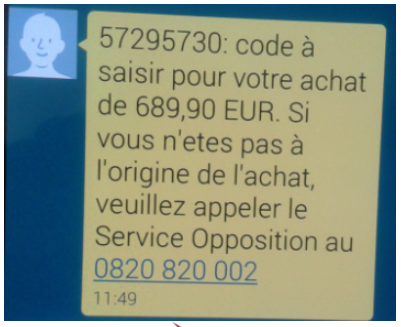
Face aux limites des mots de passe et à leur difficulté d'utilisation, de nouveaux moyens d'authentification sont proposés.

4. Gérer les utilisateurs

d. Autres méthodes d'authentification

- Biométrie ;
  - permet l'authentification par la lecture des attributs physiques peu changeant d'une personne : empreinte digitale, voix, rétine, etc. ;
- Carte à puce + code pin ;
- SSO : Single Sign-On ;
  - L'utilisation du SSO permet d'éviter que les utilisateurs aient à ressaisir leurs mots de passe (utilisation d'un seul formulaire d'authentification pour accéder à diffrents services).
- OTP(One Time Password).
  - Généré à chaque demande et utilisable une seule fois. Sa durée de validité très courte :
    - un OTP peut être un code de validation de paiement en ligne reçu par sms ;
    - ou généré par un générateur matériel de jetons sécurisés.

Token Safenet



4. Gérer les utilisateurs

e. Sensibilisation des utilisateurs

- Se tenir informé de l'actualité liée à la sécurité :
  - des vulnérabilités publiées ;
  - fuite d'information : trop nombreux exemples Sony, Yahoo, Equifax;
  - « scam » arnaques sur Internet : arnaque à la nigériane, etc.

- Faire attention aux pièces jointes (même pour les expéditeurs connus).
  - télécharger d'abord et faire un scan avec l'antivirus, avant d'ouvrir la pièce jointe.

4. Gérer les utilisateurs

e. Sensibilisation des utilisateurs

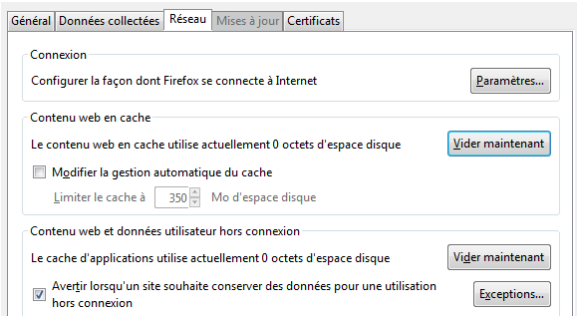
- Désactiver l'exécution des liens hypertextes et l'affichage des images dans les mails ;
  - Il est préférable de copier et coller le lien hypertexte dans le navigateur. En effet, une technique dans le phishing consiste à faire afficher un lien qui parait légitime à la lecture, mais qui pointe en fait vers une site malveillant. Cette technique ne fonctionne que si on clique sur le lien.
- Faire attention aux ralentissements/lenteurs de son poste ;
- Applications web : penser à cliquer sur le bouton déconnecter lorsqu'on a finit de surfer sur le site afin de désactiver le cookie (attention, ceci n'évite pas tout traçage).
- Déconnecter son poste lorsqu'il n'est pas utilisé.

4. Gérer les utilisateurs

e. Sensibilisation des utilisateurs

- Éviter les sites dont les certificats proposés ne sont pas reconnus ;

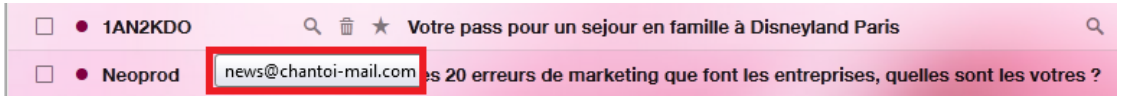
- Dans la mesure du possible, naviguer toujours en « https »
  - Cela est d'autant plus important sur les hotspots publics !
- Effacer régulièrement l'historique de navigation, les fichiers temporaires, les cookies votre navigateur Web.



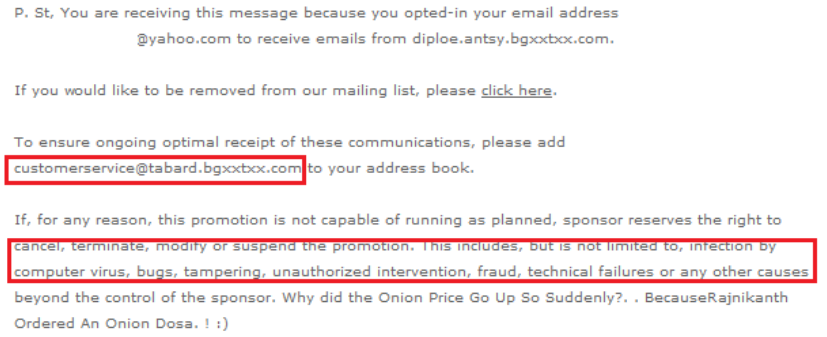
4. Gérer les utilisateurs

f. Spam

- Traiter le spam
  - protéger son adresse mail ;
  - au besoin, créer une adresse poubelle : xxx@yopmail.com ;
  - marquer les mails indésirables comme tel afin d'affiner la politique de détection des spams ;
  - ne pas ouvrir les spams, et ne pas cliquer sur les liens contenus.
- Faire attention aux mails envoyés dont l'émetteur est inconnu ;



- Faire attention aux contenus des mails.


P. St, You are receiving this message because you opted-in your email address
@yahoo.com to receive emails from diploe.antsy.bgxxtxx.com.

If you would like to be removed from our mailing list, please click here.

To ensure ongoing optimal receipt of these communications, please add customerservice@tabard.bgxxtxx.com to your address book.

If, for any reason, this promotion is not capable of running as planned, sponsor reserves the right to cancel, terminate, modify or suspend the promotion. This includes, but is not limited to, infection by computer virus, bugs, tampering, unauthorized intervention, fraud, technical failures or any other causes beyond the control of the sponsor. Why did the Onion Price Go Up So Suddenly?. . BecauseRajnikanth Ordered An Onion Dosa. ! :)

4. Gérer les utilisateurs

g. Phishing / Spear phishing / Social engineering

- Ne pas donner suite au mail, coup de fil vous demandant de :
  - Rappeler rapidement votre conseiller bancaire alors que vous ne l'avez pas contacté ;
  - Donner des informations personnelles parce que vous avez gagné un voyage, un prix, etc.
  - D'envoyer votre mot de passe/code bancaire/code pin par mail sous le prétexte urgent :
    - d'éviter la fermeture de votre adresse mail (car vérification en cours) ;
    - de valider l'existence de votre carte bancaire désactivée, etc.
  - De faire un transfert d'argent à un de vos contacts dans le besoin à l'étranger.

En cas de doute, renseignez-vous mais ne répondez pas au mail.

4. Gérer les utilisateurs

g. Phishing / Spear phishing / Social engineering

- Limiter les informations que vous partagez par les réseaux sociaux ou mail ;
  - Date de départ en voyage ;
    - http://pleaserobme.com : sur la base de tweet (position) indique les maisons vides.
  - Informations personnelles ;
  - Données (photos/vidéos) potentiellement compromettantes ;
    - Chantage menant à des suicides d'adolescents « **chantage à webcam** »
      - « Le jeune homme, prénommé Gauthier, a mis fin a ses jours le 10 octobre après avoir été victime d'un chantage sur Facebook de la part d'une jeune fille avec qui il venait de faire virtuellement connaissance. »
      - En janvier, Cédric, 17 ans, s'est pendu dans sa chambre à Marseille, 3 mois après avoir été piégé au cours d'un "plan webcam".
- Quelques liens utiles :
  - http://www.arnaque-chantage-webcam.com/
  - http://www.laveudunet.com/
  - http://blog.mavieprivee.fr/post/34628211803/chantage-a-la-webcam.

4. Gérer les utilisateurs

h. Réagir en tant que victime

- Ne jamais payer de rançons ;
- En cas de chantage / usurpation d'identité / atteinte à la réputation :
  - Ne communiquez plus avec l'escroc ;
    - bloquer ses messages / son contact.
  - Signalez et recevez de l'aide ;
    - faire bloquer ce contact sur le site du chat, ou sur Facebook ou Skype ;
    - exercer le droit à l'oubli sur Google : https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr;
    - signaler : https://www.internet-signalement.gouv.fr/
    - pour les mineurs : http://www.netecoute.fr/
- En cas de ransomware (rançongiciel) :
  - En entreprise ou à l'université : signalez aux responsables informatiques ;
  - A la maison : rechercher de l'aide sur des sites et forums spécialisés :
    - http://stopransomware.fr/nettoyer-son-ordinateur/
    - Les sites d'éditeurs de solutions antivirales : Symantec, etc.
- Porter plainte à la police ou à la gendarmerie.

4. Gérer les utilisateurs

h. Réagir en tant que victime

- Vidéo: conseils de la revue Wired aux victimes d'un ransomware
- https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

CyberEdu
La sécurité par l'enseignement supérieur des NTIC

5. Sécuriser physiquement

a) Protection physique des locaux
b) Imprimantes / Photocopieuses
c) Sécuriser les équipements

5. Sécuriser physiquement

a. Protection physique des locaux

- Protéger physiquement les locaux contenant les biens sensibles :
  - Contrôler l'accès aux locaux : usage de badges par exemple ;
  - Utiliser des alarmes pour identifier les intrusions ;
  - Protéger les clés ou badges dans des coffres par exemple.

- Les prises d'accès réseau doivent être protégées de manière à être inaccessibles aux visiteurs/personnes mal intentionnées ;
  - Si les prises d'accès réseau doivent être exposées, ne pas les connecter au réseau. Mais plutôt le faire au besoin et désactiver ensuite.

- Protéger contre les incidents environnementaux :
  - Incendie : extincteur, détecteur de fumée, etc.
  - Inondation : s'installer en zone non inondable, surélever les éléments, etc.
  - Panne électrique : utiliser des onduleurs, etc.

5. Sécuriser physiquement

a. Protection physique des locaux

- Exemple: protection contre les incendies des salles serveurs

5. Sécuriser physiquement

b. Imprimantes / Photocopieuses

- Réduire au maximum les impressions sur papier;
- Faire attention lors des photocopies à ne pas oublier les originaux ;
- Aller rapidement retirer les documents imprimés pour éviter que des informations sensibles soient révélées ;
- Ne pas oublier que les imprimantes disposent :
  - De disques durs ;
  - D'historique des impressions : dont les titres de documents pourraient être révélateurs ;
  - De configuration IP pouvant être usurpée.
- Les imprimantes ne doivent être accessibles depuis Internet.

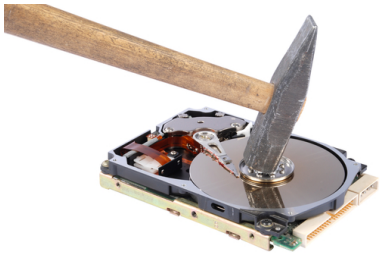
5. Sécuriser physiquement

b. Imprimantes / Photocopieuses

- Les documents papiers sensibles doivent détruits à la déchiqueteuse :

b. Disque durs au rebut

- Les supports (disques, clés USB, anciens ordinateurs portables) peuvent contenir des données sensibles: les détruire soigneusement avant recyclage:

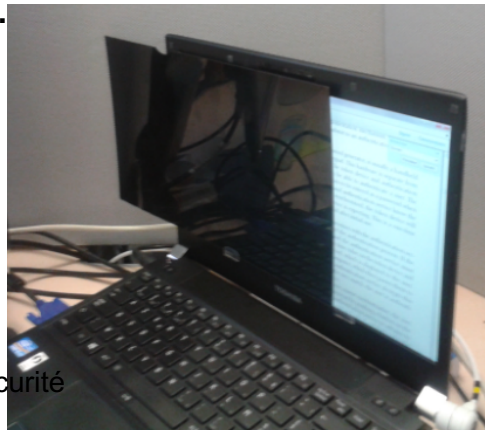


5. Sécuriser physiquement

c. Sécuriser les équipements

- Attacher avec un câble de sécurité les équipements le permettant ;

- Protéger l'accès aux équipements :
  - Avoir un code/mot de passe pour restreindre l'accès :
    - lecteur d'empreinte ou signe sur téléphone ;
    - code PIN ou mot de passe ;
  - Demander un code/mot de passe pour sortir de la veille.
- Verrouiller son écran en cas d'inactivité de quelques minutes ;
- Faire attention aux médias USB :
  - Des clés USB piégées sont parfois offertes ou abandonnées ;
  - Toujours scanner (anti-virus) une clé USB avant de l'utiliser.
- Utiliser les filtres de confidentialité d'écran ;
  - Écran d'ordinateur (fixe, portable) ;
  - Écran de téléphone.



6. Contrôler la sécurité du S.I.

a) Contrat/Maintenance/Professional Services
b) Surveiller/Superviser
c) Incidents de sécurité
d) Plans de secours
e) Audit

6. Contrôler la sécurité du S.I.

a. Contrat/Maintenance/Professional Services

- Lors de l'achat de :
  - matériel : souscrire à des contrats de maintenance ou d'assurance pour vous garantir une assistance en cas de difficulté ;
  - application : souscrire à des contrats de support et d'assistance.
    - niveau 1 : description et enregistrement du problème rencontré. Conseil/information basique ;
    - niveau 2 : intervention de technicien ;
    - niveau 3 : intervention d'expert.

- SLA (Service Level Agreement) : indique le niveau de service garanti par le prestataire pour une prestation de service donnée.
  - Exemple : couverture 3G ou 4G.

6. Contrôler la sécurité du S.I.

a. Contrat/Maintenance/Professional Services

- Cyber-assurance : est une assurance visant à indemniser et assister les victimes de cyber-attaque (fuite de données, attaque à la e-réputation…) :
  - Exemple : AXA propose pour les particuliers « Protection Familiale Intégr@ale »
  - Noter que la souscription d'une assurance est considérée comme une mesure de sécurité permettant de réduire les risques portant sur l'entreprise (au même titre qu'une assurance habitation n'empêchera pas un incendie, mais compensera/limitera les pertes financières de la victime).

Souscrire à des services d'assurance/support/maintenance pour les composants sensibles.

6. Contrôler la sécurité du S.I.

b. Surveiller / Superviser

- Activer la journalisation d'évènements ;
  - Enregistrer les tentatives d'accès réussies ou pas ;
  - enregistrer les tentatives de modifications d'informations sensibles ;
  - etc.

- Consulter les journaux d'évènements ;

- Définir une politique de supervision :
  - définir les seuils : au-delà de tel taux d'occupation du disque, recevoir une alerte ;
  - Définir le type d'alerte souhaité : SMS, mail, etc.

6. Contrôler la sécurité du S.I.

c. Incidents de sécurité : catégories d'incidents

- Divulgation d'information personnelle ;
  - carte de crédit, vol d'identité, numéro de sécurité sociale, etc.
- Déni de service ;
  - entrant ou sortant.
- Activité causée par un code malveillant ;
  - Vers, virus, keylogger, Rootkit.
- Enquête et activité criminelle ;
  - Vol de terminal, fraude, pornographie infantile.
- Non respect de la politique de sécurité ;
  - partage de mot de passe.
- Défacement Web ;
  - Redirection de site, défacement d'un site internet.
- Vulnérabilité non corrigée.
  - système/application vulnérable, non application d'un correctif important.

6. Contrôler la sécurité du S.I.

c. Incidents de sécurité : gestion des incidents de sécurité

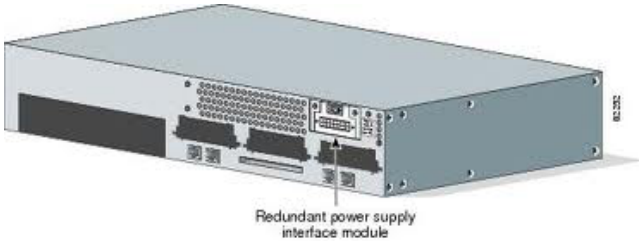
- Un processus de gestion des incidents de sécurité permet de :
  - Réagir rapidement et de réduire l'impact en cas d'incident ;
  - Améliorer la prévention et la sensibilisation ;
  - Détecter et d'identifier les incidents ;
  - Améliorer le niveau de sécurité.
- Exemple de réaction en cas d'une infection virale :
  - déconnecter le poste du réseau ou d'Internet, sans l'éteindre ;
  - S'assurer que l'antivirus/antimalware est à jour avec les dernières signatures ;
  - Exécuter le scan complet (en « mode sans échec » par exemple) avec un antivirus ;
  - Contacter un spécialiste au besoin ;
  - Chercher à identifier la cause.

La norme ISO 27035 décrit le processus de gestion des incidents.

6. Contrôler la sécurité du S.I.

d. Plan de secours

- Avoir un plan de secours en cas de dysfonctionnement important (électrique, télécom…) :
  - Double alimentation :
    - pour un téléphone : batterie de secours ;
    - ordinateur/serveur : onduleur, batterie de secours, groupe électrogène.



  - Accès Internet :
    - utiliser son téléphone comme modem en cas de dysfonctionnement de sa Box ;
    - En entreprise, souscription à une offre Internet comme ligne de secours fournie par un opérateur différent.
  - Avoir une sauvegarde de ses données en cas de panne de son disque dur.

6. Contrôler la sécurité du S.I.

d. Plan de secours (suite)

- En entreprise, il y a des :
  - PRA : Plan de Reprise d'Activité qui permet de « reprendre » après une interruption inattendue comme la perte d'un site de travail ;
    - Exemple : utilisateur d'un site de secours « B » et déplacement du personnel en cas d'incendie dans le site principal « A »
  - PCA : Plan de Continuité d'Activité qui permet de s'assurer que l'activité ne s'arrêtera pas ;
    - Exemple : usage d'une architecture réseau redondée en haute disponibilité.
      - Routeur en actif/actif.
  - Les PCA et les PRA doivent être testés et mis à jour régulièrement.

6. Contrôler la sécurité du S.I.

e. Audit : informations générales

- Un audit peut porter sur tout ou partie du S.I., une application, etc.
- Le but de l'audit est généralement :
  - d'évaluer le niveau de sécurité par rapport à un référentiel (interne ou à une norme) ;
  - obtenir un agrément ou une certification :
    - ASIP Santé, PCI-DSS, 27001, etc.
  - trouver des faiblesses et les corriger :
    - site Web ;
    - application développée « in-house »
- L'audit peut être réalisé par :
  - des experts appelés « auditeur sécurité », « pen-testeur »
  - des sociétés spécialisés.
- Un cadre légal et contractuel est requis pour les audits :
  - Pour les audits de site Web, il faut l'accord du propriétaire du site (par exemple l'association étudiante), de l'hébergeur du site (OVH ou l'université) et parfois celui de l'opérateur ;
  - L'auditeur doit indiquer à partir de quelles adresses IP publiques son audit sera effectué ;
  - L'auditeur doit s'engager à ne pas provoquer d'incident de sécurité (déni de service par exemple) au cours de son audit.

6. Contrôler la sécurité du S.I.

e. Audit : types d'audit

- Audit de conformité pour déterminer les écarts par rapport à un référentiel :
  - Politique de sécurité interne ou exigences de sécurité d'un cahier de charge ;
  - Norme internationale : exemple 27001, PCI-DSS, ASIP Santé.
- Audit en vue de l'obtention d'un(e) certification/agrément :
  - Audit physique des datacenters pour obtention d'un agrément SAS 70 ;
  - Audit 27001 en vue de démontrer la bonne application des principes de la norme.
- Audit Technique.
  - « Boite noire » ou « Pentest » : sans aucun accès, on évalue le système (site web par exemple) du point de vue d'un attaquant quelconque ;
  - « Boite grise » ou « test du stagiaire » : on dispose de quelques informations et on essaye d'élever ses privilèges ;
  - « Boite blanche » pour faire des « audits de configuration » par exemple. On dispose d'accès, y compris administrateur et on évalue le système par rapport à un référentiel ;
  - « Forensic » ou « Post-mortem » : effectuer sur un système après une attaque.

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Merci de votre attention