Fondamentaux de la sécurité informatique utilisateur

Benoît Prieur

Fondamentaux de la sécurité informatique utilisateur

V 0.1 (19 mars 2020) - IT-Akademy (Lyon, mars 2020)

Benoît Prieur - Soarthec - CC-By-SA 4.0

Présentation et objectifs du cours

- Benoît Prieur (société Soarthec)
- Objectifs :
  - Connaître les bases relatives aux diverses menaces
  - Améliorer la connaissance de bonnes pratiques relatives à la sécurité du poste de travail dans un cadre individuel ou collectif

Panorama des menaces : malware

- Logiciel malveillant (*malware*)
- Définition générale :
  - *logiciel développé dans le but de nuire à un système informatique*
- Inclus la notion de virus mais va bien au-delà

Malware : virus (1)

- automate autoréplicatif à la base non malveillant
- Se répand via les réseaux, les périphériques etc.
- En 1986, ARPANET (réseau à transfert de paquets) en renommant les entités de démarrage d'un poste
- Assez généralement écrit en assembleur

Malware : virus (2)

- Notion de charge utile (qui se déclenche à plus ou moins long terme)
- On parle également de bombe logique
    - Exemple du virus Tchernobyl qui s'est activé le le 26 avril 1999 (13e anniversaire de la catastrophe)

Malware : virus (3)

Typologie :

- Virus de boot (clé USB, disque, programme de boot)
- Macrovirus (dans un document type Excel, Powerpoint etc.) : programme fallacieux en VBA par exemple
- Virus “ver” (“worm”)
- Virus par batch (relativement désuet)

Malware : virus (4)

Virus “ver” :

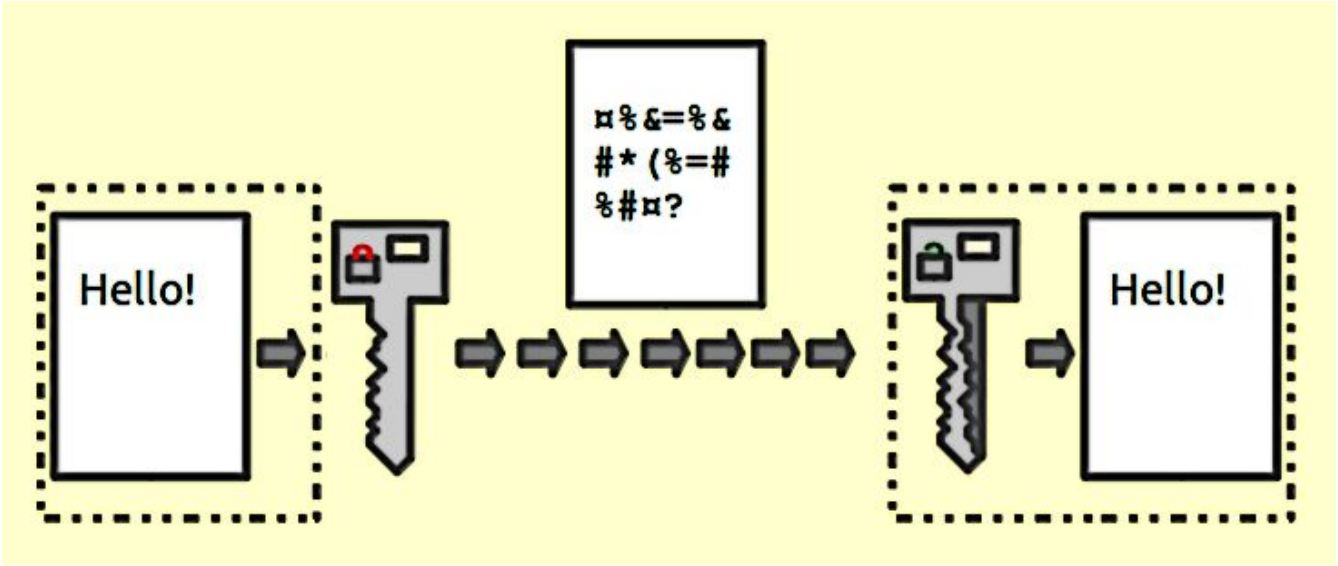
- Lié au réseau (failles de sécurité)
- Action discrète et parfois non-destructrice sur la machine hôte
- Visée large (par exemple attaque dans un second temps depuis les machines infectées de type *DoS*, *Denial of Service*)

Malware : virus (5)

Caractéristiques :

- Notion de réplication du virus
- Chiffrement à chaque réplication
    - Rappel concernant le chiffrement/déchiffrement (slide suivant)
- Polymorphisme : modalité de chiffrement change à chaque réplication
- Furtivité

Cryptage, chiffrement, déchiffrement (1)



Cryptage, chiffrement, déchiffrement (2)

- Notion de clé
- Chiffrage symétrique : une clé privée (personne n'y a accès) permet de chiffrer et déchiffrer à l'aide d'un algorithme qui lui est public
- Chiffrage asymétrique : il y a deux clés : l'une publique, l'une privée

Chiffrage symétrique

Exemples :

- Rijndael
- AED
- DES

Chiffrage asymétrique

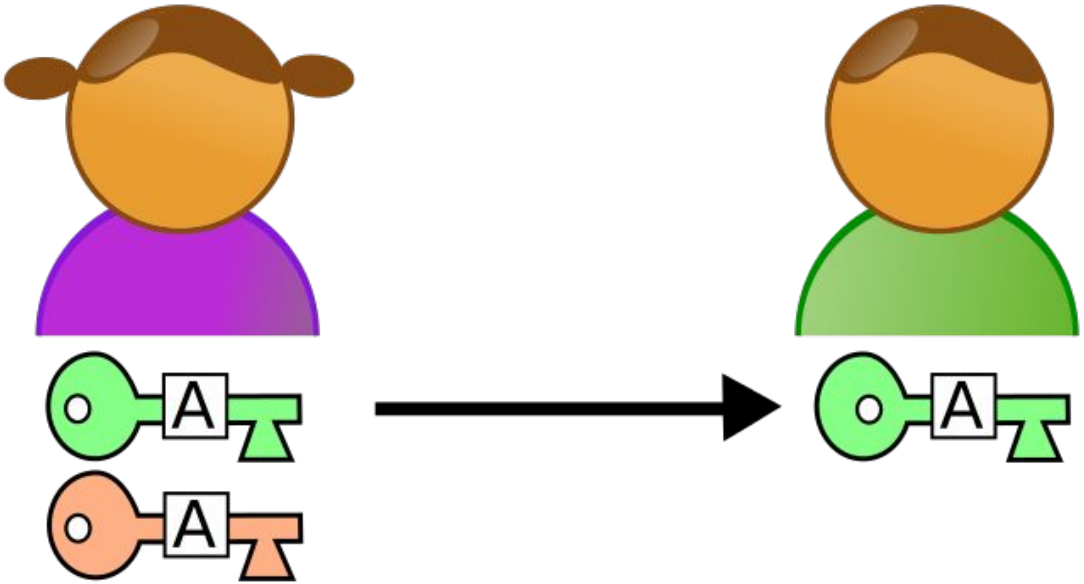
Exemples :

- DSA
- EDD
- ECD
- RSA

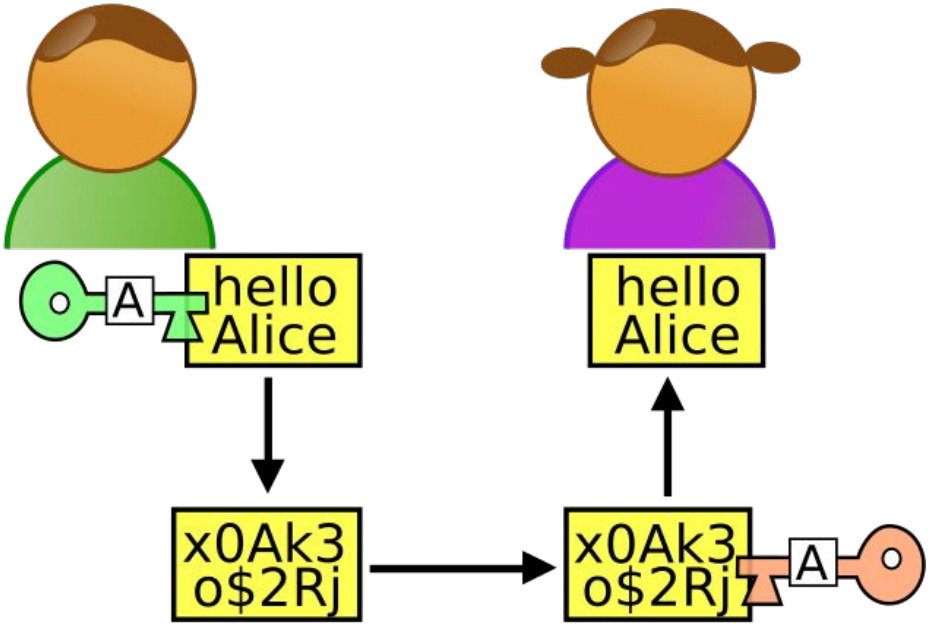
Chiffrage symétrique

- Chiffrage historique
- Une seule clé connue par l'émetteur et le récepteur
- La clé permet de chiffrer et de déchiffrer
- Exemple :
    - Chiffrage de "Il fait beau"

Chiffrage asymétrique - exemple 1



Chiffrage asymétrique - exemple (suite)



Fonctions de hachage crypotgraphiques

- MD5 (considéré comme dépassé)
- SHA

Nommage et caractérisation des virus

- CARO (Computer Antivirus Research Organization)
  - en préfixe, le mode d'infection (macrovirus, ver) ou le système d'exploitation concerné
  - un mot exprimant une de ses particularités ou la faille qu'il exploite)
  - en suffixe un numéro de version

Nommage et caractérisation des virus (2)

- Standardisation très relative, y compris dans le nommage :
  - NetSky dans sa variante Q est appelé W32
    - Q@mm (Symantec)
    - WORM_NETSKY. Q (Trend Micro)
    - W32/Netsky. Q.worm (Panda Security)
    - I-Worm. NetSky. r (Kaspersky)

Quelques virus célèbres

- Cabir (premier à réellement infecter les mobiles), faille : BlueTooth
- MyDoom.A (2004), faille relative au P2P
- Tchernobyl (précédemment évoqué)
- Conficker, faille : Windows Service sur les OS Windows 2000 (entre autres)
- Zeus Bot (2014). Faille : dans les logiciels Adobe
- *Ransomwares* : Cryptolocker, Locker (chiffrement de données et demande de rançon)
- I Love You : mentionné par la suite

Retour sur le type de virus “ver”

- Propagation par courrier électronique ; Internet ; IRC
- Mais également par partage de fichier (macrovirus)
- Ver célèbre : I Love You (2000)
  - Cache un script VBS malicieux
  - Diffusion massive *via* Outlook
  - Ajout de clefs dans la base de registre : lancement à chaque démarrage de Windows
  - Insertion dans des fichiers .JPG, .CSS, .DOC ; renommage en .VBS

Cheval de Troie (1)

- En apparence légitime, mais inclut une malveillance
- *L'Iliade* (Homère), Ulysse
- Origine : source de document peu sûr (téléchargement P2P, clé USB, ingénierie sociale, etc.)

Cheval de Troie (2)

Quelques exemples :

- Socket23
- Back Orifice
- Beast
- Netbus
- ZeroAccess
- Koobface

Notion de porte dérobée (backdoor)

- En général logiciel (mais peut être matériel)
- Malveillance , surveillance de masse
- Lien avec le Cheval de Troie
  - F5 Big-IP et Enterprise Manager (années 2010)
  - ProFTPd (années 2010)
  - Cisco Unified Videoconferencing ((années 2010)

Notion de pourriel (spam)

- Envoi massif
- Lien fallacieux inclus
- Agit sur le caractère massif de l'envoi
- Phénomène équivalent avec téléphone, SMS etc.
- Coût minime rentabilisé par une victime 1/10 000

Notion de publiciel (adware)

- Cible souvent le navigateur web
- Lien avec le spam

Notion de rogueware

- rogue : escroc en anglais
- Marketing non éthique
- Suggestion d’un logiciel antivirus qui se trouve être malveillant

Rançongiciel, ransomware, crypto-rançongiciel

- Chiffrage asymétrique
- Fourniture de la clé privée contre une rançon
- 320 000 rançongiciels bloqués (2017, Symantec)

Notion d'hameçonnage (*fishing*)

- Email fallacieux (par exemple) permettant d'obtenir des données privées (bancaires notamment)
  - Vérifier l'émetteur et la crédibilité du nom de domaine
  - Vérifier l'orthographe, la vraisemblance du courriel
- Affaire récente du *Faux Le Drian*

Notion de déni de service (DoS)

- Réseau surchargé afin d'empêcher son fonctionnement
- Perturbation des connexions entre deux machines
- Obstruction d'accès à un service pour une personne
- Requêtes multiples sur un site web, une API
    - Nécessité de se prémunir *a minima*
    - Vérifier les plages d’IP pour éventuellement les bloquer

Notion d'ingénierie sociale

- Relatif à la manipulation psychologique pour obtenir des informations
- Lien fort avec la présence sur les réseaux sociaux et les données implicites ou explicites exposées
- Hameçonnage sous certains aspects est déjà de l'ingénierie sociale
- Série *Mr. Robot*
- *Spyware* (logiciel espion) glane de l'information sur une machine cible

Notion de *spyware* et assimilés

- Logiciel espion sur la machine cible
- Similarité avec un *keylogger* (enregistreur de frappe)

Au-delà du DoS : d'autres types d'attaques sur le réseau

- Sniffing
- Hijacking
- Attaque de l'homme du milieu
- Attaque par dictionnaire
- Attaque par force brute

Notion de bombe de décompression

- Décompression (ZIP ou autres) occupe beaucoup de ressources et en particulier l’antivirus et laisse le champ à un virus véritable

Sniffing

- Utilisation de logiciels d'analyseurs de paquets sur un réseau commuté (TCP/IP)
- Analyse de paquets
- Pratique également sur d'autres moyens de communication
    - Risque quand les paquets ne sont pas chiffrés
    - SMS par exemple, non chiffrés

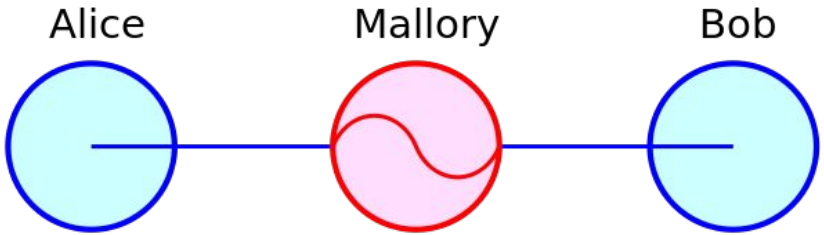
Hijacking

- Cookie hijacking : récupération du cookie de session d'un utilisateur d'un site Web (logiciel sslstrip)
- Domain hijacking : détournement de domaine
- IP hijacking : détournement d'adresse IP
- Page hijacking : détournement de site web

Intérêt du HTTPS (au passage)

- Le certificat garantit au visiteur la validité du site consulté
- Les données qui transitent, potentiellement confidentielles, via formulaire, sont chiffrées

Attaque de l'homme du milieu (1)



Attaque de l'homme du milieu (2)

- Chiffrement symétrique : nécessité de transmettre la clé de chiffrement dans un canal sécurisé
  - SSL est une réponse possible
- DNS Poisoning
- Attaque sur le réseau GSM non chiffré

Attaque de l'homme du milieu (3)

Chiffrement asymétrique (fonctionnement habituel) :

- Alice et Bob échangent leur clé publique. Carole peut les lire, elle connaît donc Ap et Bp. Alice envoie un message à Bob, elle chiffre ce message avec Bp. Bob le déchiffre avec Bs. Carole ne peut pas lire le message.

Attaque de l’homme du milieu (4)

L’attaque elle même :

- Bob envoie sa clé publique à Alice. Carole l'intercepte. Elle envoie à Alice sa propre clé publique (Cp) en se faisant passer pour Bob. Lorsque Alice veut envoyer un message à Bob, elle utilise donc la clé publique de Carole. Alice chiffre le message avec la clé publique de Carole et l'envoie à celui qu'elle croit être Bob. Carole intercepte le message, le déchiffre avec sa clé privée (Cs) et peut lire le message. Puis elle chiffre à nouveau le message avec la clé publique de Bob (Bp), après l'avoir éventuellement modifié. Bob déchiffre son message avec sa clé privée.

Attaque de l'homme du milieu (5)

Solution (?) :

- Que l'échange de clés publiques se fasse par un tiers de confiance
- +/- le principe de HTTPS et la notion de certificat

Attaque par dictionnaire

- Utilisation d’un dictionnaire pour identifier un mot de passe
- Un algorithme peut coupler un dictionnaire avec certains éléments issus d’ingénierie sociale

Attaque par force brute

- Similaire à l’attaque précédente
- Ici on cherche à tester toutes les combinatoires possibles

Discussion sur les différents OS face aux menaces, attaques et virus

- Retours d’expériences personnelles : discussion
  - Les spécificités de MacOS
  - Linux
  - Windows

Administration d'une machine ou d'un réseau local

- Comptes utilisateurs et droits
  - "Coller" au plus juste aux besoin
  - Politique du "moins-disant" : ne pas donner des droits pour un besoin hypothétique
- Droits d'accès aux fichiers et ressources
  - N'offrir des droits particuliers que strictement à celles et ceux qui en ont réellement besoin

Logiciel antivirus (1)

- En général un logiciel antivirus inclut une base de données des signatures virales (dictionnaire)
- Une signature virale : portion du code d'un virus informatique
- Exécution du code inconnu dans un environnement virtuel (méthode heuristique)

Logiciel antivirus (2)

- Effectuer la suppression du fichier contaminé
- Tenter de réparer le fichier endommagé
- Mise en quarantaine
- Faux-positifs

Logiciel antivirus (3)

- Notion de liste blanche (+/- la politique Apple)
- Approche générale :
  - Comparaison avec dictionnaire des signatures virales
  - Méthode heuristique

Logiciel antivirus (3)

- Avast Software
- Avira Internet Security
- AVG Technologies
- Bitdefender
- Kaspersky
- Symantec
- Trend Micro
- McAfee
- Autres… et expériences comparées

Logiciels antispam, antipub, etc.

- Intégration dans le navigateur web
- Intégration dans le logiciel de messagerie
- Intelligence artificielle utilisée pour identifier le spam
    - Au passage, caractérisation du “machine learning” et du “deep “learning”

Gestionnaire de mots de passe (1)

- Centralisation dans un logiciel des identifiants et des mots de passe
- Chiffrement symétrique pour chiffrer l'ensemble des informations stockées
- Nécessité de sécuriser au plus l'accès à ce gestionnaire (phrase de passe, à suivre)

Gestionnaire de mots de passe (2)

Quelques logiciels, gestionnaires de mots de passe :

- Pass
- Bitwarden
- KeePass
- Autres… et expériences comparées

Bonnes pratiques en matière de mot de passe

- La phrase de passe
- Pourquoi ?

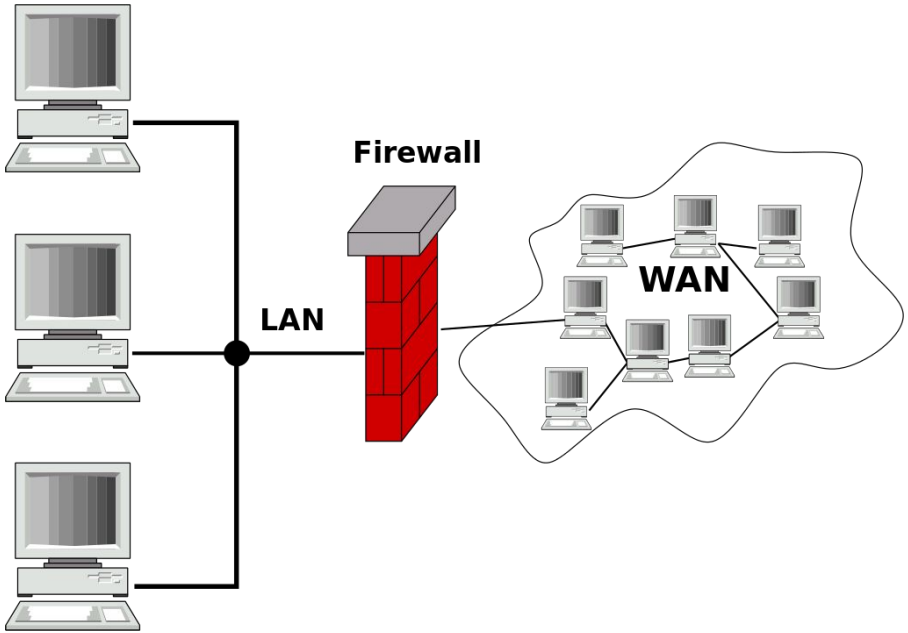
Phrase de passe, conseils et bonnes pratiques

1. Suffisamment longue pour ne pas être deviné
2. Pas une citation célèbre de la littérature (attaque par dictionnaire)
3. Ne se devine pas même si on connaît la personne (ingénierie sociale)
4. Facile à retenir (et à taper)
5. Usage unique

Notion de pare-feu (*firewall*)

- Matériel faisant respecter la politique de sécurité du réseau
- Analyse les flux de données entrants et sortants (paquets)
  - Origine ou la destination des paquets (adresse IP, port TCP)
  - Taille des données, motif à risque (signature)
  - Utilisateurs eux mêmes

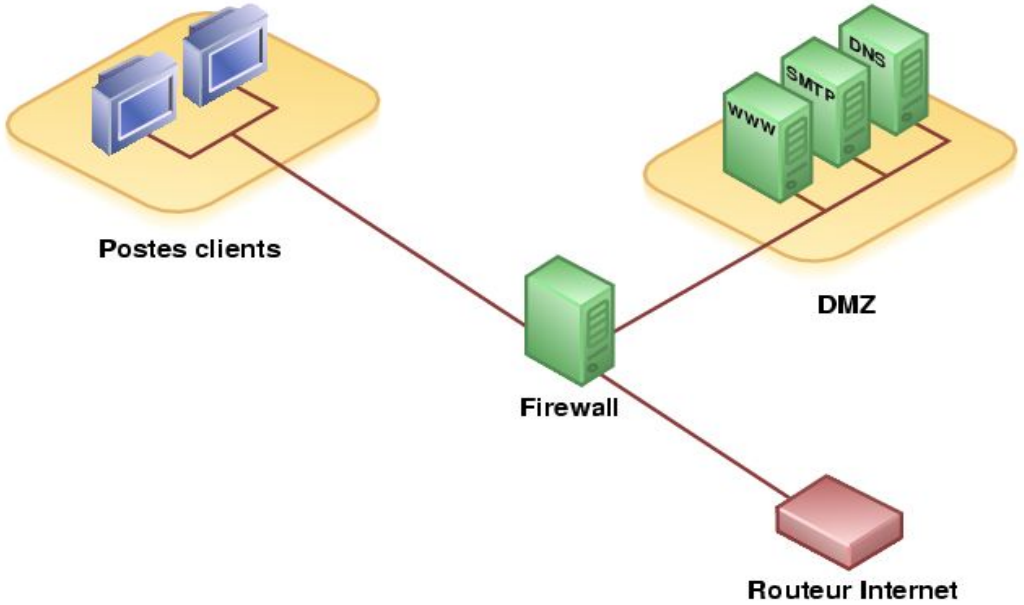
Notion de pare-feu (2)



Notion de pare-feu (3)

- Différence entre pare-feu de réseau local et pare-feu sur une machine personnelle
- Expériences comparées

Notion de DMZ (zone démilitarisée)



Crédit : Benj / Public domain

Le BYOD

- *Bring your own device*
- Pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable) en contexte d'entreprise, de formation etc.
- Gain en efficacité, en coût

Le BYOD (2)

- Par contre, induit des failles de sécurité :
  - Perte du périphérique : dépend de la politique de sécurité de l'individu (disque dur chiffré ? politique de mot de passe ? etc.)
  - Le poste n'est possiblement pas derrière le pare-feu de l'entreprise (usage d'un VPN ? Pare-feu personnel ?)
  - En France, l'ANSSI se prononce contre cette usage
    - Agence nationale de la sécurité des systèmes d'information
    - Encourage et communique les bonnes pratiques, y compris en entreprise

Politique de sécurité de l'entreprise

- Consiste en l'élaboration d'une charte
- Implique possiblement des mesures contraignantes
  - Par exemple, le pare-feu empêche l'accès à certains sites jugés douteux
- Vision stratégique (formalisée ou non dans un document)

Politique de sécurité de l'entreprise (2)

1. Sensibilisation des utilisateurs aux problématiques de sécurité (formation)
2. Sécurité de l'information
3. Sécurité des données (problématique de l'interopérabilité)
4. Sécurité des réseaux
5. Sécurité des systèmes d'exploitation
6. Sécurité des télécommunications
7. Sécurité des applications (**dépassement de tampon** par exemple)
8. Sécurité physique (infrastructures matérielles, **stratégie de reprise**)

Notion de stratégie de reprise

- Plan de reprise d'activité
- Catastrophes naturelles, cyberattaques, sinistres (incendie etc.)
- Cas concret à réaliser en groupe :
    - Conception d’un PRA relatif au système d’informations d’une petite PME

Sécurité des applications, notions

- Dépassement de tampon (*buffer overflow*) : lors de l'écriture dans un tampon, écriture à l'extérieur de l'espace alloué au tampon, écrasant ainsi des informations
- Failles de sécurité
  - Notion de tas (*heap*) et de pile (*stack*)
- Autre exemple : identification des disjonctions et des traitements associés lors de l’analyse de l’exécution

Bonnes pratiques (1)

- Recommandations par l'ANSSI
- 12 bonnes pratiques à appliquer et à faire appliquer dans l'entreprise

Bonnes pratiques (2)

1. Choisir avec soin ses mots de passe
2. Mettre à jour régulièrement vos logiciels
3. Bien connaître ses utilisateurs et ses prestataires
4. Effectuer des sauvegardes régulières
5. Sécuriser l'accès Wi-Fi de votre entreprise
6. Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur
7. Protéger ses données lors de ses déplacements
8. Être prudent lors de l'utilisation de sa messagerie
9. Télécharger ses programmes sur les sites officiels des éditeurs
10. Être vigilant lors d'un paiement sur Internet
11. Séparer les usages personnels des usages professionnels
12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Veille technologique, quelques pistes

Quelques éléments de base :

- Club de la sécurité de l'information français (CLUSIF) : publications
- L'ANSSI : site officiel
- Liste de nouvelles récentes éditée par Kapersky : lien
- Base de données des failles et attaques récentes : lien
- Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques : dernières failles signalées