Sécurité des systèmes

Introduction

Deux définitions au terme "sécurité" au sens informatique:

- Pérennisation du fonctionnement d'un système informatique pour qu'il assure les services attendus de lui
- Contrôle de l'utilisation d'un système informatique vis à vis d'utilisateurs autorisés ou non:
  - Confidentialité des données
  - Autorisations discrétionnaires
  - Protection
  - Audit
  - ...

RETOUR

Pérennité

Dispositifs matériels

- Salles informatiques dédiées
- Climatisation
- Onduleur
- Dans les ordinateurs
  - Alimentations redondantes
  - Ventilateurs changeables à chaud
  - Disques "hot plug"
  - Ajout/changement de mémoire
  - Ajout/changement de processeur
  - Disques durs en RAID (Redondant Array of Independant Disks)
    - Si un disque disparait, les autres permettent de reconstituer les informations qu'il contenait
      - Mirroring
      - Stripping avec parité
- Mirroring de systèmes: Une machine de remplacement est prête à prendre la relève en cas de problème
- Réseau redondant: Doublage (ou +) des connexions réseau

Mises à jour système et applications

- Pas de programme informatique sans bugs
- Mise à disposition de correctifs (patchs) par les éditeurs
    - Systèmes d'exploitation
    - Pilotes logiciels (drivers) de périphériques
        - cartes graphiques
        - cartes réseau
        - cartes mères
        - ...
    - Applications
- Service fréquemment gratuit, possiblement payant par abonnement
- Installation automatisable
- WindowsUpdate pour les systèmes d'exploitation Microsoft Windows
- MicrosoftUpdate pour l'ensemble des produits Windows
- Différents utilitaires suivant les distributions Linux

Politique de sauvegarde

- Un crash disque ou un crash système toujours possible
  -> Impossibilité d'exécution du système
  -> Impossibilité d'accès aux données
- Utilisation d'une sauvegarde préalablement réalisée
    - Système
    - Données
- Automatisation des sauvegardes
- Stockage des supports de sauvegarde dans un lieu sécurisé

Politique de sécurité

Aspects matériels

- Contrôle de l'accès physique aux ordinateurs
    - Salle machine sécurisée et fermée
    - Ordinateurs portables enfermés
    - Postes clients non portables fixés
    - Données cryptées
    - Lecteur de carte à puce pour l'authentification

    - Lecteur d'empreinte digitale pour l'authentification
    - ...
- Contrôle (interdiction) des dispositifs de sauvegarde amovibles pour éviter le vol de données
    - Clés USB
    - Disques durs externes
    - Graveurs de CD, de DVD
    - ...
- Contrôle de l'accès au réseau
    - Éviter les réseaux sans fil
    - Si pas possible d'éviter les réseaux sans fil, activer les options de sécurité les + fortes
    - Éviter les réseaux CPL
    - Si pas possible d'éviter les réseaux CPL, activer les options de sécurité les + fortes
    - Éviter les infrastructures à réseau filaire où il suffit de se "brancher" physiquement pour être connecté au réseau
    - ...

Aspects logiciels

- Contrôle discrétionnaire
    - Soumettre à authentification toute action sur un système pour obtention d'une autorisation:
        - Ouverture de session de travail
        - Accès aux fichiers
        - Accès au réseau
        - Exécution des applications
        - Exécution de commandes "système"
        - ...
    - Moyen d'authentification
        - Compte d'utilisateur + mot de passe
        - Carte à puce
        - Empreintes digitales
        - ...
- Cryptage des données, cryptage des communications
    - Technique classique de cryptage: Le cryptage à clé publique

Le tiers devant assurer le décryptage crée un couple clé privée-clé publique.
Il communique la clé publique au tiers devant crypter des informations.
Celui-ci réalise le cryptage de son message et transmet le résultat.
Les informations cryptées ne pourront être décryptées que par le créateur du couple de clés car seule la clé privée permet de décrypter ce qui a été crypté par la clé publique correspondante.

- S'assurer que les données sensibles sont stockées sous forme cryptée sur mémoire de masse
- S'assurer que les communications sur le réseau sont cryptées
  - Utilisation de protocoles spécifiques
    - https
    - ...

- Authentification mutuelle du client et du serveur

- Protection des données personnelles
  - Qui sait véritablement ce que font les logiciels?
  - Protection des données privées sur Internet
    - Cookies
    - Google
    - Facebook
    - ...
  - Problématique particulière au téléphone portable
    - Suivi GPS
    - Transmission d'informations
    - ...

- Attaques
  - But: Acquérir des droits sur un système
    - Y obtenir une connexion de travail
      - Par accès à la console
      - Par accès via connexion réseau
    - Y exécuter des programmes
    - Y acquérir des droits supérieurs à ses droits normaux -> Droits d'administration
    - Y camoufler ses activités

- Activités:
  - Copier des données
    - Vol
    - Intelligence économique
    - ...
  - Pervertir des données
  - Distraire des ressources de leur destination
    - Serveur de spams
    - Serveur de fichiers pirates
    - ...
  - Empêcher le système de fonctionner nominalement
    - Déni de service
  - Effacer ses traces (éventuellement par destruction du système) avant de se déconnecter
  - ...
- Le cas particulier des sites Web:
  - Défacement
  - Hébergement d'"autre chose"
  - ...

- Moyens: Exploiter les caractéristiques des systèmes informatiques et leurs failles
  - Techniques
    - Craquage de mot de passe par force brute
    - Craquage de mot de passe par dictionnaire
    - Écoute des communications sur le réseau (Sniffing)
    - Usurpation d'identité (Spoofing)
    - Cheval de Troie (Trojan horse)
    - Key logger
    - Vers
    - Déni de service
      - Flooding
      - Mail bombing
      - SMS bombing
    - Dépassement de tampon (Buffer overflow)
    - Bombe logique
    - Site Web d'hameçonnage

        - Infection par consultation d'un site Web
        - ...
    - Humains
        - Ingéniérie sociale
        - Corruption
        - Extorsion
        - Vol
        - ...
- S'en prémunir
    - Mettre à jour ses systèmes: Supprimer les failles connues
    - Ne laisser en fonctionnement sur une machine que les programmes qui doivent l'être: Fermer les portes inconnues
    - Soumettre toute utilisation d'une ressource informatique à une authentification: Ne pas autoriser n'importe qui à mettre un pied dans l'embrasure de la porte
    - Politique de mot de passe
        - Forcer l'utilisation de mots de passe complexes: Rendre difficile le craquage des mots de passe
        - Forcer le changement régulier des mots de passe: Éviter qu'un mot de passe corrompu ne soit utilisable trop longtemps
        - Interdire les mots de passe identiques lors des changements
        - Mots de passe à usage unique
    - Sensibiliser les utilisateurs banalisés aux problèmes de sécurité: Faire que chacun se sente investi
    - Mettre en place des processus d'audit local des serveurs et des postes clients: Détecter les fonctionnements locaux anormaux
    - Surveiller le trafic réseau: Détecter les fonctionnements réseaux anormaux
    - Mettre en place un pare-feu (firewall): Empêcher le trafic réseau non explicitement autorisé, bloquer le trafic anormal
    - Mettre en place des zones démilitarisées:

Placer les machines sensibles dans des réseaux isolés auxquels l'accès est réalisé par l'intermédiaire d'un nombre limité de machines inter-médiatrices fortement surveillées
- Configurer les systèmes pour qu'ils refusent l'installation de tout composant complémentaire
  - Logiciel sur les ordinateurs
  - "Application" sur les mobiles
  - Module complémentaire sur les navigateurs
  - ...
- Se tenir informé pour réagir rapidement lorsqu'une nouvelle menace apparaît: Être pro-actif
  - CERT (Computer Emergency Response Team)
  - CLUSIF(CLUb de la Securité de l'Information Français)
  - Sites Web des éditeurs de logiciel anti-virus
  - ...

- Logiciels malveillants (malware)
  - Définition: Tout logiciel installé à l'insu de l'administrateur et des utilisateurs et exploitant l'ordinateur à des fins malveillantes
  - Spyware (Logiciel espion)
    - Programme informatique analysant l'activité de la machine à l'écoute d'informations confidentielles à communiquer à un tiers importun
      - Login - mot de passe lors d'une authentification
      - Numéro de carte bleue - nom du propriétaire - date de validité - cryptogramme visuel lors d'un paiement sur Internet
      - ...
    - Installé subrepticement au cours d'activités

de consultation sur Internet
        - Installé subrepticement lors de l'installation d'un autre logiciel
        - S'en prémunir:
            - Logiciel anti-spyware
            - Configurer son navigateur pour qu'il refuse l'installation automatique de programmes
    - Tracking cookies
        - Fichiers de trace des activités sur Internet

- Virus
    - Programme informatique capable de se reproduire d'une machine sur une autre machine et donc de se diffuser très rapidement par réaction en chaîne
    - Buts des concepteurs:
        - Réaliser une attaque en bonne et due forme
        - Prouver l'existence d'une faille de sécurité
        - Prouver que l'on sait faire
        - ...
    - Types:
        - Virus de boot
        - Virus d'autorun
        - Ver
        - Hoax
        - ...
    - S'en prémunir:
        - Anti-virus
            - Poste client
            - Serveur
                - Messagerie
                - Fichiers
                - Proxie
                - ...
        - Désactiver l'autorun sur les périphériques amovibles (clés USB, disques USB, ...)
        - Ne jamais exécuter directement un programme exécutable reçu par émail. Se méfier des pièces jointes.
        - Se méfier de tout mail qui demande de

communiquer une information à tous les correspondants de votre carnet d'adresses
        - Se méfier de tout mail demandant la communication d'informations personnelles et/ou confidentielle
        - Être attentif à toute modification du fonctionnement de la machine: Limiter et enrayer l'infection quand c'est encore possible
        - ...

- Audit (accounting)
    - Définition: Fonctionnalité d'enregistrement des activités réalisées sur un ordinateur ou un réseau
    - Activités "auditables" sur une machine
        - Ouverture/fermetures de session de travail
        - Accès aux fichiers
        - Accès au réseau
        - Utilisation des droits
        - Accès aux imprimantes
        - Utilisation des applications
        - ...
    - Activités auditables sur un réseau
        - Trafic depuis une machine particulière
        - Trafic vers une machine particulière
        - Trafic sur un protocole particulier
        - Pics de trafic
        - ...

Aspects humains

80% des problèmes proviennent de l'intérieur

- Mauvaises pratiques
- Utilisation de logiciels non sécurisés autorisés ou non
    - Messagerie instantanée
    - Skype
    - ...
- Malveillance
- Concurrences
- Jalousies
- Attaques délibérées

- Activités privées
  - Peer to peer
  - Téléchargements illégaux
  - Réseaux sociaux
  - ...
- ...

Aspects légaux

- Attaques répréhensibles au sens de la loi
  - De 3 mois à 3 ans de prison, peine éventuellement assortie du sursis
  - De 30000 à 300000€ d'amende
  - Dommages et intérêts
- HADOPI
- CNIL
- Mise en place de l'état de l'art en matière de protection
- Information auprès de la population des utilisateurs relative aux containtes propres au système informatique qu'ils utilisent

Cibles principales

- Virus: Microsoft Windows
  - Machines les plus répandues
  - Attaque contre Microsoft
- Attaques: Microsoft Windows
  - Machines les plus répandues
  - Attaque contre Microsoft
- Attaques: Linux
  - Failles d'Unix
  - Système bien connu car ouvert
- Attaques: Sites Web dynamique
  - PHP
- Attaques: Contre le propriétaire du système
  - Entreprises
    - Immobilisation de l'infrastructure informatique
    - Espionnage industriel, intelligence économique
    - Vol d'informations personnelles

        - Vol de numéros de carte bancaire
        - Chantage
        - ...
    - Organismes gouvernementaux
        - Ministère de la défense
        - Ministère de l'intérieur
        - Ministère des finances
        - Centres de recherche
        - ...
    - Organisations non gouvernementales nationales et internationales
        - Greenpeace
        - Amnesty International
        - Reporter sans frontière
        - Charlie-Hebdo
        - ...

Avenir

- Quid des terminaux mobiles de type smartphone ou tablette?
- Cyber-guerre entre entreprises
- Cyber-guerre entre gouvernements
    - Israël <-> Iran
    - ...
- ...

Authentification mutuelle des intervenants par chiffrement asymétrique

- Objectif envoyer des données chiffrées à Alice en lui garantissant qu'il en est l'expéditeur.
    1. Bob crée une paire de clés asymétriques: Il conserve la clé privée et diffuse librement la clé publique (notamment à Alice).
    2. Alice crée une paire de clés asymétriques: Elle conserve la clé privée et diffuse librement la clé publique (notamment à Bob).
    3. Bob effectue un condensât de son message « en clair » puis chiffre ce condensât avec sa propre clé privée.
    4. Bob chiffre son message avec la clé publique d'Alice.

5. Bob envoie le message chiffré accompagné du condensât chiffré.
6. Alice reçoit le message chiffré de Bob, accompagné du condensât.
7. Alice déchiffre le message avec sa propre clé privée. À ce stade le message est lisible mais elle ne peut pas être certaine que Bob en est l'expéditeur.
8. Alice déchiffre le condensât avec la clé publique de Bob. Alice utilise la même fonction de hachage sur le texte en clair et compare avec le condensât déchiffré de Bob. Si les deux condensateurs correspondent, alors Alice peut avoir la certitude que Bob est l'expéditeur. Dans le cas contraire, on peut présumer qu'une personne malveillante a tenté d'envoyer un message à Alice en se faisant passer pour Bob!

- Utilisé en https

RETOUR