Chapitre 8 : sécurité des systèmes

Exemple de sociétés hackées :

- Target (USA) : 40 millions de numéros de cartes bleues
- HomeDepot : 60 millions de numéros de CB
- Sony : 70 millions de données utilisateurs
- Valve : 35 millions (cryptées)
- …
- Cyberattaques contre les états
  - → 2010 : Japon vs Corée du Sud
  - → 2013 : Singapour
  - → 2014 : Russie Crimée Ukraine
  - → …
- Espionnage d'état et industriel (hack mails démocrates)

I. Vulnérabilité des systèmes et usage abusif

Précédemment, les données sur les personnes étaient stockées dans des dossiers physiques dans des bâtiments protégés.

Aujourd'hui, ces données sont numériques donc facilement :

- Duplicables : copiée/collée
- Partageables : sur un serveur
- Véhiculables : je mets la donnée sur une clé USB, je peux l'envoyer par mail

Les systèmes sont interconnectés : risques d'accès non autorisés, d'usage abusif ou de fraude.

Un système interagit avec d'autres systèmes.
Un système compromis et c'est l'ensemble des systèmes qui est compromis.

La vulnérabilité peut venir :

- Du logiciel
- Du réseau
- De l'humain : principale faille informatique
- Des partenaires : FRN, clients et toutes entités avec lesquelles l'E interagit
- Des mises à jour constantes des systèmes
- Des mauvaises manipulations
- Des pannes de courant entraînant une chute de service
- Des catastrophes naturelles (inondations, incendies…)

Problème de l'externalisation :

- Des données sensibles sont envoyées à l'étranger (sécurité de leur système ?)
- Ces données peuvent être interceptées
- L'externalisation de développement d'application pose le problème des « backdoor ».

Internet démultiplie les problèmes de sécurité :

- Les ordinateurs sont connectés en permanence

- Les emails sont souvent la source du virus/malware
- Problème de « phishing » = hameçonnage

Problèmes des connexions sans fil (Wi-Fi, Bluetooth…) :
- Les bandes de fréquence radio sont facilement interceptables
- Des antennes Wi-Fi peuvent fonctionner sur plusieurs centaines des mètres
- Certaines normes (WEP) sont crackables en quelques minutes
- La norme WPA est aussi attaquable grâce à un dictionnaire

Programmes malveillants :
- Virus = programme qui se multiplie à l'aide d'un programme hôte. Il le modifie pour ses besoins.
- Ver (Worm) = se multiplie sans l'aide de programme. Utilise les failles de sécurité pour se reproduire.
- Cheval de Troie : logiciel d'apparence légitime qui exécute des actions à l'issu de l'utilisateur (partage de fichiers, accès secret au système…). Il ne se multiplie pas.

Sources d'infection par virus/ver :
- Pièces jointes de mail
- Téléchargement sur internet
- Navigation web
- Récemment, naissance des virus pour appareils mobiles

Conséquences infection :
- Des millions d'ordinateurs « zombifiés »
- Des dizaines de milliards d'€ dépenses pour lutter contre les malwares pour réparer les dégâts

II. Dimensions juridiques de la sécurité

- Marché mondial de la sécurisation des SI : centaines de milliards de dollars, par an, en croissance constante (en 2018)
- Exigences juridiques : contraint les E à protéger l'intégrité de l'information afin de fournir des informations financières exactes
- La loi impose aux E d'assurer la confidentialité et l'exactitude des données

Lors d'une poursuite, une E devra répondre à une demande d'accès à l'information :
- Il faut donc une politique efficace de conservation des documents électroniques ne serait-ce que pour des questions juridiques.

Exigences judiciaires potentielles :
- Récupérer des données dans un ordinateur en tant que preuve
- Trouver l'information pertinente pour la fournir au tribunal

III. Etablissement du contrôle des SI

Nature des principales menaces :
- Accidents (foudre, inondation, perte de service : perte connexion internet…)
- Erreurs (saisie, transmission…)
- Malveillance : action d'origine humaine
  - → Vol de données, sabotage, attaques logiques, divulgation d'informations…

La politique de sécurité doit être :
- Simple et compréhensible
- Adoptable par un personnel préalablement sensibilisé, voire formé
- Aisément réalisable
- Facile en termes de maintenance

La politique de sécurité comprend 4 composantes :
- Politique de contrôle des accès
- Politique de protection
- Politique de réaction : protocole à mettre en place ?
- Politique de suivi : qu'est-ce qu'on va mettre en place pour faire audit/contrôle et où on peut s'améliorer ?

Acteurs d'une politique de sécurité :
- Responsable sécurité des SI
  - → Vérifie que les ressources sont en cohérence avec la politique de sécurité
  - → Remonte les informations à la direction
  - → Conseille sur les stratégies de sécurité
  - → Fait une veille sur les règlementations en matière de propriété intellectuelle, protection des données, cybercriminalité…
- Responsable des ressources humaines
  - → Contrôle les nouveaux salariés
  - → Sensibilise les salariés aux problématiques de sécurité
  - → Fait signer une déclaration de secret professionnel
- Chefs de service
  - → Informe le responsable sécurité des besoins des collaborateurs
- Utilisateurs
  - → Doivent respecter les règles et les procédures
  - → Ne doivent pas divulguer les informations confidentielles

Maintien de la continuité des affaires :
- Systèmes à tolérance de pannes
- Systèmes à haute disponibilité
  - → Serveurs redondants
  - → Equilibrage de charge
  - → Ecriture miroir

Externalisation de la sécurité :
- Sécuriser un SI est couteux
- Cela demande des compétences très spécifiques
- Une société peut choisir d'externaliser pour

→ Surveiller son réseau
→ Effectuer des tests de vulnérabilité
→ Proposer une infrastructure de secours

IV. Outils et technologies pour la sécurisation des SI

Objectifs de la sécurité informatique :

- Disponibilité
- Intégrité
- Confidentialité
- Respect de réglementation

Contrôle de l'accès :

- Bloquer l'accès aux personnes non autorisées (en interne et externe)
- Pour bénéficier d'un accès, il faut être autorisé et être authentifié (= vérification de l'identité par mot de passe)
- L'authentification par mot de passe pose beaucoup de problèmes (outils, partage, mot d passe à sécurité faible, même mot de passe pour plusieurs services…)

Possibilité d'authentification biométrique :

- S'appuie sur les mensurations ou traits de comportement
- Empreintes digitales, visage, empreinte rétienne
- Couteux et pas assez faible
- Problème de vie privée…

Pare-feu :

- Bloque l'accès
- Combinaison matériel et logiciel qui contrôlent les flux de données qui entre et sort d'un réseau
- Situé entre réseau interne et réseau public

Systèmes de détection d'intrusion :

- En plus du pare-feu
- Surveillance du trafic en continu
- Détecte des comportements suspects
  → Accès suspect sur des fichiers critiques
  → Utilisation de protocoles suspects

Antivirus :

- Sur toutes les machines et sur les serveurs
- Vérifie les disques durs et les systèmes (comportements suspects ?)
- Vérifie les disques externes (clé USB…)
- Détecte les zones infectées et les nettoie
- Doit être continuellement mis à jour

Sécurité des réseaux sans fil

- Utiliser WPA à la place de WEP
- Crypter toutes les transactions (https…)
- Utiliser certificats et signatures électroniques

Considérez que tout ce que vous faites en ligne sera public.
Ne considérez pas les paramètres de vie privée et l'utilisation de mots de passe comme des remparts au point précédent.
Quand vous renseignez des informations, considérez que vous donnez le contexte associé.
Considérez que la liste de vos achats par CV sera un jour publique.
Les données ne disparaissent pas, même quand vous les supprimez.

V. Politiques de sauvegardes

Définie en fonction du volume de données et de la durée de conservation.
Il faut définir :

- Les périmètres à sauvegarder (services, matériels, sites, utilisateurs…)
- Les types de données sauvegardées (fichiers utilisateurs, fichiers serveurs, documents…)
- La fréquence de sauvegarde et la périodicité de rotation des sauvegardes

Il faut définir :

- Les supports de sauvegarde
- Les liens et moyens de stockage des sauvegardes (lieux différents, sauvegarde déportée, armoire ignifugée…)

Exemple de procédure de sauvegarde :

- Sauvegarde journalière doublée et utilisée toutes les 2 semaines
- Sauvegarde mensuelle conservée 1 an
- Sauvegarde annuelle archivée définitivement

Plusieurs méthodes de sauvegarde :

- Complète
- Différentielle

Ne pas oublier de tester régulièrement toutes les sauvegardes et de les restaurer !