INTRODUCTION À LA SÉCURITÉ INFORMATIQUE

Confiance et Internet

- Dans la vie courante la plupart des transactions reposent sur une «confiance» acquise par une relation en face à face ou un contact physique
- Dans le cybermonde cette relation de proximité est rompue
- Comment établir une relation de confiance indispensable à la réalisation de transactions à distance entre personnes qui ne se connaissent pas ?

Environnement de l'entreprise

Avant:

- Centralisé
- Échange papiers
- Pas d'accès distant.

Aujourd'hui

- Distribué sur plusieurs sites: siège, filiales, télé-travailleurs, commerciaux, …
- Accès distants,
- Mondialisation des échanges.
- Haut débit

Demain

- 3.000.000.000 de personnes Internautes

Les Risques

Interception de messages

- Prise de connaissance des mots de passe
- Vol d'information
- Perte d'intégrité du système et du réseau

Intrusion des systèmes

- Vol ou compromission des informations
- Destruction des informations
- Virus
- Détournement de biens

Perte d'accessibilité au système ou au réseau

Faux clients, marchands escrocs

Motivations d'un attaquant

Le gain financier

- Récupération de num de cartes bancaires, …

Vengeance

- Site www.aljazeera.netlors de la couverture de la guerre d'irak

Besoin de reconnaissance

- Attaque contre le site du cerist avec un message sur les restrictions d'accès à Internet à Cuba.

Curiosité

- Attaques d'étudiants du MIT sur le premier ordinateur IBM 704 au MIT en 1959.

Recherche d'émotions fortes

Ignorance

- Envoie de mots de passes par email, …

Les programmes malveillants

Un logiciel malveillant (malware en anglais) est un logiciel développé dans le but de nuire à un système informatique.

— le **virus :** programme se dupliquant automatiquement sur le même ordinateur.

Il peut être transmis à un autre ordinateur par l'intermédiaire du courrier électronique ou par l'échange de données ;

— le **ver (*worm*) :** *exploite les communications réseaux d'un ordinateur afin d'assurer sa reproduction sur* d'autres ordinateurs ;

— le **cheval de Troie (*trojan*) :** programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur ;

— la **porte dérobée (*backdoor*)** : permet d'ouvrir d'un accès réseau frauduleux sur un système informatique. Il est ainsi possible d'exploiter à distance la machine ;

Les programmes malveillants

— le **logiciel espion (*spyware)*** : fait de la collecte d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation. Ces informations sont ensuite transmises à un ordinateur tiers ;

— **l'enregistreur de frappe (*keylogger)* :** programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier ; pour intercepter des mots de passe par exemple.

— **l'exploit :** programme permettant d'exploiter une faille de sécurité d'un logiciel ;

— le **rootkit :** ensemble de logiciels permettant généralement d'obtenir les droits d'administrateur sur une machine, d'installer une porte dérobée, de truquer les informations susceptibles de révéler la compromission, et d'effacer les traces laissées par l'opération dans les journaux système.

Les risques humains

Ce sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés.

Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

— la **maladresse :** commettre des erreurs : exécuter un traitement non souhaité, effacer involontairement des données ou des programmes, etc.

— **l'inconscience et l'ignorance** : introduire des programmes malveillants sans le savoir (par exemple lors de la réception de courrier).

De nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils font courir aux systèmes qu'ils utilisent.

Les risques humains

la **malveillance :** *Certains utilisateurs peuvent volontairement mettre en péril le système d'information, en y introduisant en connaissance de cause des virus (en connectant par exemple un ordinateur portable sur un réseau d'entreprise), ou en introduisant volontairement de mauvaises informations dans une base de données.*

l'ingénierie sociale (*social engineering)* est une méthode pour obtenir d'une personne des informations confidentielles, que l'on n'est pas normalement autorisé à obtenir, en vue de les exploiter à d'autres fins

Les risques matériels

— **Incidents liés au logiciel :** Les programmeurs peuvent faire des erreurs de manière individuellement ou collective que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité.

— **Incidents liés à l'environnement :** les machines électroniques et les réseaux de communication sont sensibles aux variations de température ou d'humidité (tout particulièrement en cas d'incendie ou d'inondation) ainsi qu'aux champs électriques et magnétiques.

Il est possible qu'un ordinateur tombe en panne de manière définitive ou intermittente à cause de conditions climatiques inhabituelles ou par l'influence d'installations électriques notamment industrielles (et parfois celle des ordinateurs eux-mêmes !).

Les risques matériels

Ils sont liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels. Ces incidents sont plus ou moins fréquents selon le soin apporté lors de la fabrication et l'application de procédures de tests effectuées avant que les ordinateurs et les programmes ne soient mis en service.

Certaines de ces pannes ont des causes indirectes, voire très indirectes, donc **difficiles à prévoir.**

— **Incidents liés au matériel** : la plupart des composants électroniques, produits en grandes séries, peuvent comporter des défauts. Ils finissent un jour ou l'autre par tomber en panne.

Certaines de ces pannes sont assez difficiles à déceler car intermittentes ou rares. Parfois, elles relèvent d'une erreur de conception (*une des toutes premières générations du processeur Pentium d'Intel pouvait produire, dans certaines circonstances, des erreurs de calcul) ;*

Les risques et menaces de la messagerie électronique

— le **pourriel (*spam*) :** un courrier électronique non sollicité, la plupart du temps de la publicité. Ils encombrent le réseau, et font perdre du temps à leurs destinataires ;

— **l'hameçonnage (*phishing*)** : un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles ;

— le **canular informatique (*hoax*) :** un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes.

Ils encombrent le réseau, et font perdre du temps à leurs destinataires.

Les risques et menaces sur le réseau

— les **écoutes (*sniffing*)** : *technique permettant de récupérer toutes les informations transitant sur un* réseau (on utilise pour cela un logiciel sniffer). Elle est généralement utilisée pour récupérer les mots de passe des applications et pour identifier les machines qui communiquent sur le réseau.

— **l'usurpation d'identité (*spoofing*) :** *technique consistant à prendre l'identité d'une autre personne ou* d'une autre machine. Elle est généralement utilisée pour récupérer des informations sensibles, que l'on ne pourrait pas avoir autrement.

— le **déni de service (*denial of service*)** : *technique visant à provoquer des interruptions de service, et* ainsi d'empêcher le bon fonctionnement d'un système. Il peut y avoir des tentatives d'extorsion de fond : menacer de stopper l'activité d'une entreprise.

Pertes phénoménales !!!

74% des pertes financières sont dûent aux:

- attaques de virus (plus de 15 millions de dollars de perte)
- accès non autorisés aux systèmes d'information (plus de 10 millions de dollars de perte)
- vols d'équipement mobile (plus de 6 millions de dollars)
- vols de la propriété intellectuelle (plus de 6 millions de dollars)

52% des organisations sondées ont déclaré avoir été attaqué en(2006) :

- 24% d'entre elles ont reporté plus de 6 attaques
- 48% ont reporté 1 à 5 attaques

Conséquences !

34% des organisations allouent pas moins de 5% du budget informatique à la sécurité informatique

- En 2006, les compagnies de revenues inférieurs à 10 millions de dollars ont dépensé en moyenne 1349 dollars par employé pour la sécurité informatique-
- un rehaussement de 210% par rapport à l'année 2005

plus de 80% des institutions conduisent un audit de sécurité informatique

la majorité des institutions jugent la formation en sécurité informatique comme importante et stratégique

- 61% de ces organisations refusent de sous-traiter leurs fonctions de sécurité informatique

Services de sécurité

Authentification

- Permet de vérifier l'identité revendiquée par une entité, ou l'origine d'un message, ou d'une donnée
- Le terme authentification recouvre plusieurs interprétations

Confidentialité

- Permet de se protéger contre la consultation abusive des données par des entités tierces indésirables

Contrôle d'intégrité

- Permet de vérifier qu'une données n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement)

Contrôle d'accès

- Permet de vérifier que toute entité n'accède qu'aux services et informations pour lesquelles elle est autorisée

Non répudiation

- Permet de se protéger contre la contestation d'envoi et de réception de données lors d'une communication