La sécurité des réseaux numériques
Introduction

<< Le terme “sécurité” est utilisé dans le but de minimiser la vulnérabilité des biens et ressources.

Un bien peut être représenté par tout ce qui a une valeur.

Une vulnérabilité est n’importe quelle faiblesse qui peut être exploitée pour violer un système ou l’information qu’il contient. Une menace est tout ce qui peut porter atteinte à la sécurité >>

ISO Security Architecture-IS 7498/2

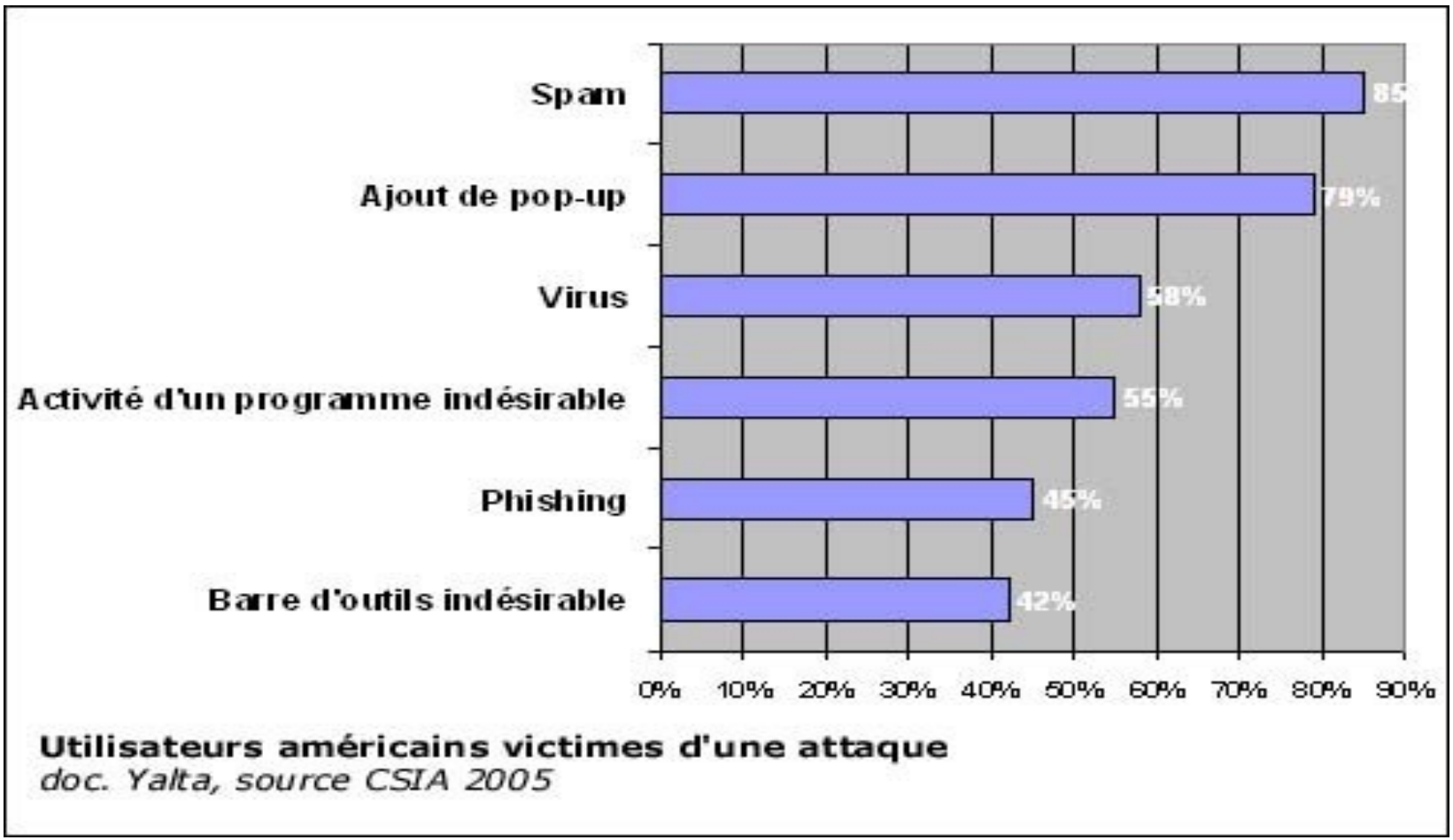
La sécurité

- **La sécurité**
  - ensemble des moyens mis en oeuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles

- **Quelques chiffres**
  - 1 à 3% des systèmes hôtes ont des ouvertures exploitables
  - 88% des systèmes hôtes peuvent être pénétrés par les relations de confiance
  - seules 4% de ces attaques sont détectées et seuls 5% de ces 4% sont rapportés

Attaques sur les postes individuels

- peut précéder l'attaque globale d'une entreprise



Utilisateurs américains victimes d'une attaque

doc. Yalta, source CSIA 2005

Les systèmes sont vulnérables

- La sécurité est chère et +/- difficile à mettre en oeuvre
- La sécurité ne peut être sure à 100%
- La politique de sécurité est complexe et basée sur des jugements humains
- Les systèmes de sécurité sont faits, gérés et configurés par des hommes (errare humanum est !)

Un système ne peut pas être sûr à 100%

- Il est impossible de garantir la sécurité totale
- Même un système fiable peut être attaqué par des personnes abusant de leurs droits
- Plus les mécanismes de sécurité sont stricts, moins ils sont efficaces
- On peut s'attaquer aux systèmes de sécurité eux-mêmes…

Méthodes utilisées pour les attaques

- La négligence interne des utilisateurs vis à vis des droits et des autorisations d'accès
- Se faire passer pour un ingénieur pour obtenir des infos comme le mot de passe
- Beaucoup de mot de passe sont vulnérables à une attaque systématique
- Les clefs de cryptographie trop courtes peuvent être cassées

Méthodes utilisées pour les attaques

- L'attaquant se met à l'écoute sur le réseau et obtient des informations
- IP spoofing : changer son adresse IP et passer pour quelqu'un de confiance
- Injecter du code dans la cible comme des virus ou un cheval de Troie
- Exploitation des faiblesses des systèmes d'exploitation, des protocoles ou des applications

Outils des attaquants

- Programmes et scripts de tests de vulnérabilité et d'erreurs de configuration
- Injection de code pour obtenir l'accès à la machine de la victime (ex : cheval de Troie)
- Echange de techniques d'attaques par forums et publications
- Utilisation massive de ressources pour détruire des clefs par exemple
- Utilisation d'outils pour se rendre anonyme et invisible sur le réseau
- ……..

Méthodes d'attaques

- **Cheval de Troie**
  - petit programme malveillant d’apparence anodine (jeu, petit utilitaire...) permettant de prendre le contrôle à distance de la machine
  - peut causer des dégâts comme un virus classique

Méthodes d'attaques

- **Backdoor (porte arrière)**
  - entrer dans un programme par un point plus ou moins secret (ex : sécurité pour débloquer un code d’accès perdu)

Méthodes d'attaques

- **Sniffing**
  - écouter une ligne de transmission pour récupérer des données à la volée (ex : pour se procurer des mots de passe)

Méthodes d'attaques

- **Spoofing**
  - technique d’intrusion par envoi de messages semblant provenir d'une adresse IP connue par le firewall (adresse interne existante autorisée)

Méthodes d'attaques

- **Phishing (hameçonnage, filoutage)**
  - Technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

Méthodes d'attaques

- **Phishing (hameçonnage, filoutage)**
  - La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration, etc.) afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

Méthodes d'attaques

- **Attaque par rebond**
  - menée via un autre ordinateur qui se trouve involontairement complice

Méthodes d'attaques

- **Attaque par le milieu**
  - se placer entre deux ordinateurs en communication et se fait passer pour un afin d'obtenir le mot de passe de l'autre

Méthodes d'attaques

- **Déni de service**
  - attaque cherchant à rendre un ordinateur hors service en le submergeant de trafic inutile

Virus

- **Malware**
  - Programmes destinés à causer des dégâts sur les systèmes d'information : vers, virus, chevaux de Troie...
  - .....

Virus

Types de virus

- virus : programme pirate, capable de se propager et de se reproduire
- virus polymorphe : virus qui modifie automatiquement ses principales caractéristiques (nom, taille...) pour échapper à la détection des antivirus
- .....

Virus

Types de virus

- rétro-virus : virus dont la première action est de stopper l'antivirus ou le firewall (très difficiles à supprimer)
- ….

- …..

Virus

- **Types de virus**
  - bot : transforme un PC en machine esclave (exécuter des commandes pour son maître, rechercher les mots de passe, mettre en place un serveur FTP ou SMTP, arrêter les systèmes de protection, ...)
  - .....

Virus

- **Types de virus**
  - ver (worm) : se propage aux autres correspondants listés dans la liste des contacts par l'intermédiaire des messageries (sous la forme de pièce jointe)
  - keyloggers : enregistre les frappes claviers
  - .....

Prévention des attaques

Indispensable

- disposer d'une bonne sauvegarde de toutes ses données
- faire un audit des portes inutilement ouvertes (modems installés à demeure, logiciels de transmissions permanents…)
- lorsqu'ils existent, vérifier que les comptes d'administration ont des mots de passe sécurisés
- supprimer les comptes utilisateurs non utilisés (notamment à la suite de chaque départ)
- désactiver les services non utilisés sur les machines

Prévention des attaques

- **Souhaitable:1/2**
  - Mettre à jour systèmes et logiciels (serveurs et serveurs Web principalement) à l'aide des patchs de sécurité officiels fournis pour fermer les brèches logicielles découverte

Prévention des attaques

- **Souhaitable:2/2**
  - installer un FireWall qui sert d'intermédiaire lors des transmissions et bloque ainsi les attaques directes
  - structurer les réseaux en zones étanches par activité et sensibilité (VLAN).

Principales technologies de défense

- **Authentification**
  - vérifier la véracité des utilisateurs, du réseau et des documents
- **Cryptographie**
  - pour la confidentialité des informations et la signature électronique

MERCI