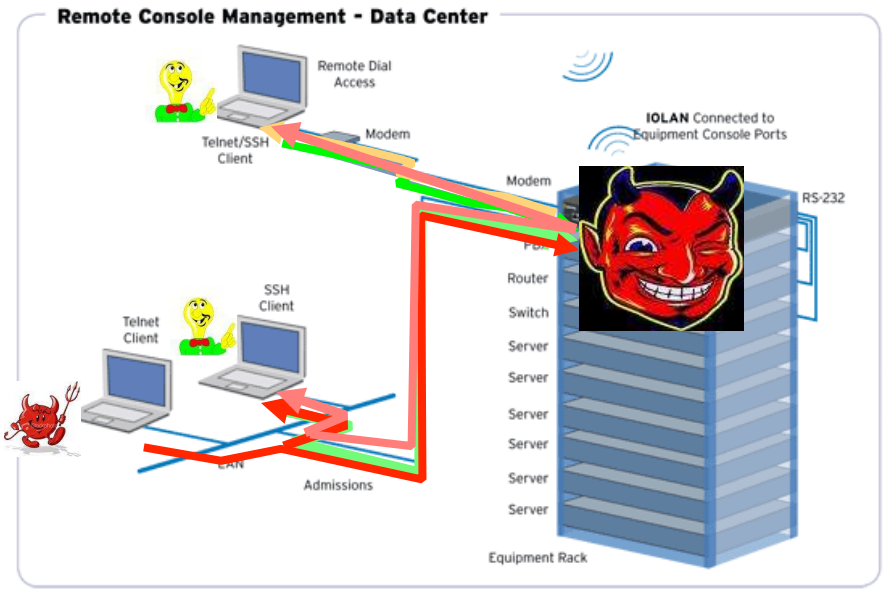
Introduction à la Sécurité

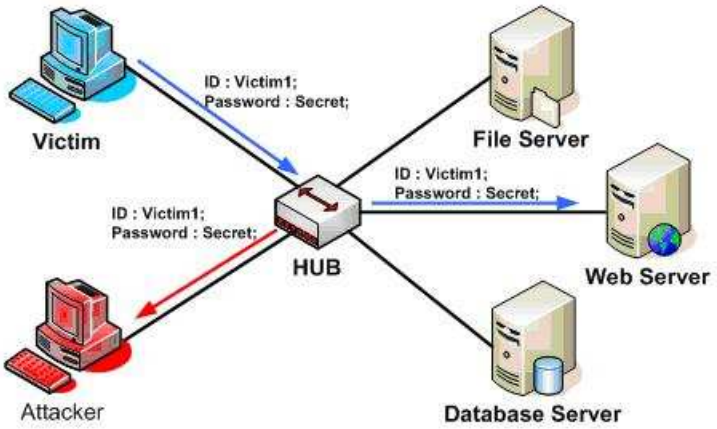
Cours 01

Ahmed Amou El Arby

Qu’est-ce que la sécurité informatique?



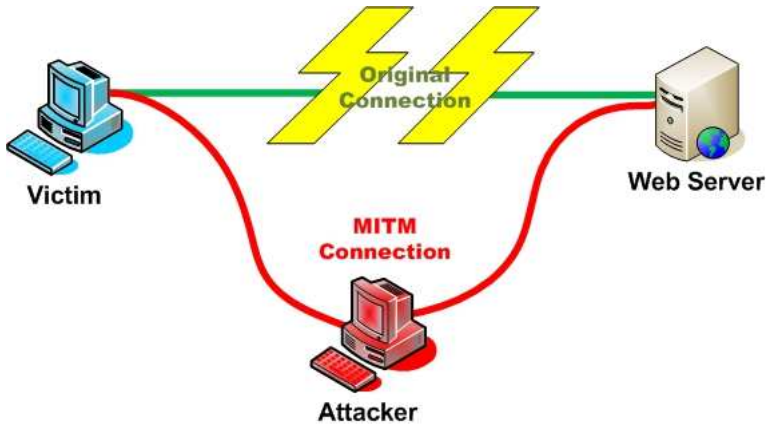
Espionnage de réseau



Interception des paquets en transit sur un réseau

Ceci est facile puisqu'un concentrateur («*hub*») répète tout ce qu'il reçoit à tous.

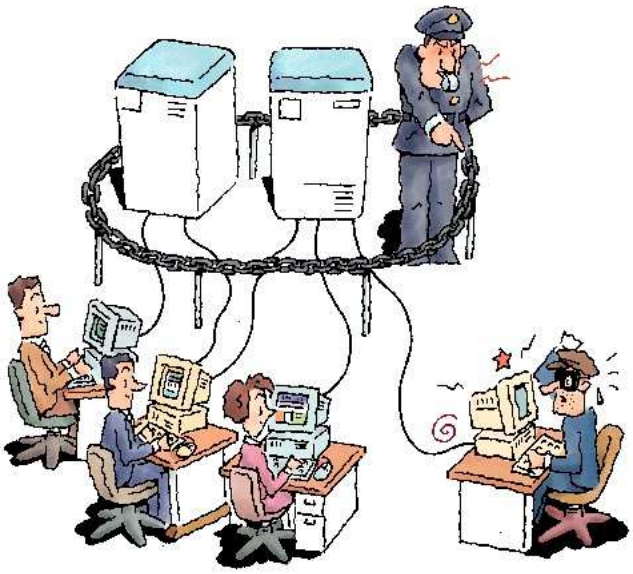
Attaque de l’homme du milieu



Attaque où l’adversaire fait intrusion sur le canal de communication entre deux noeuds terminaux du réseau :

- Injecte des faux messages et
- Intercepte l’information transmise.

Le but de la sécurité informatique



Cyber Attacks Hit 75% of Enterprises in 2009

Symantec's latest report has more unsettling news for IT security administrators.

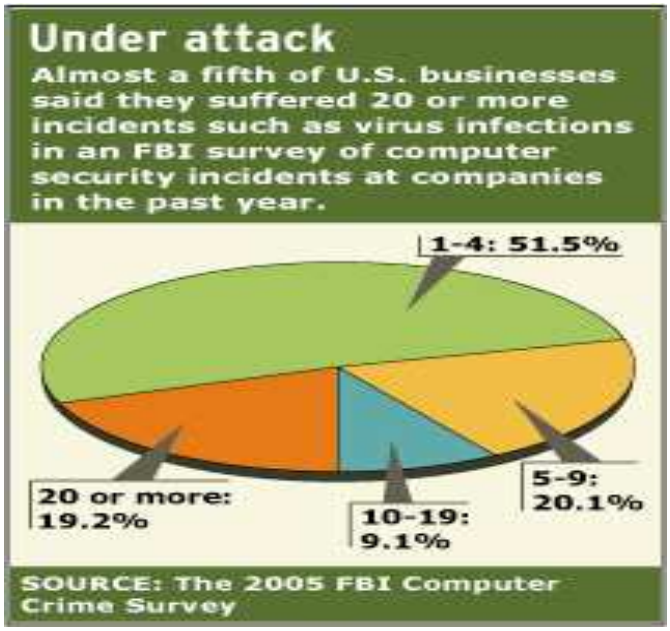
February 24, 2010
By Kerry Barrett: *More stories by this author*:

If there's still any doubt about it, security vendor Symantec's latest data makes it perfectly clear: Hackers have enterprises firmly in their cross-hairs.

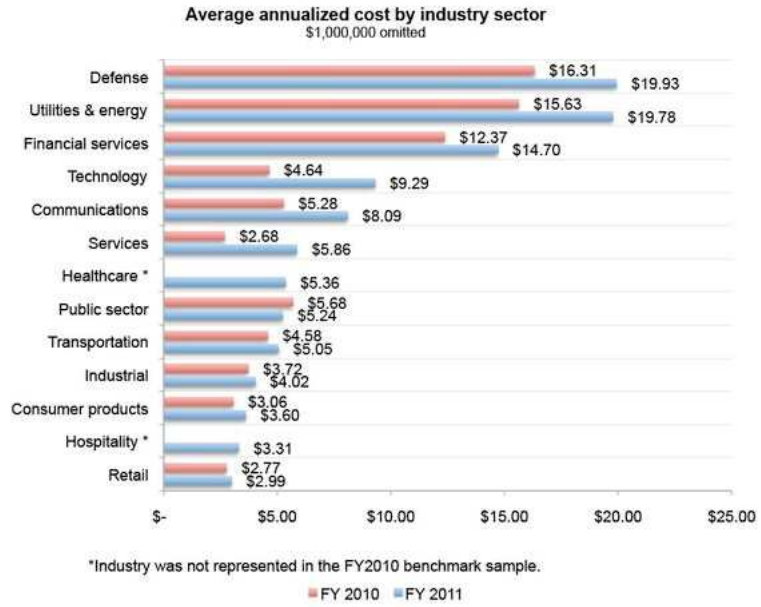
The company's new State of Enterprise Security gives new, alarming indications that not only are malicious hackers, identity thieves, and malware authors eying high-value targets, enterprise IT security administrators' efforts to fight back are being hamstrung by budgets and staffing.

Not surprisingly, enterprises are finding it tough to cope, and Symantec puts a very hefty price tag on the cost of all of those breaches. eSecurity Planet has the story.

The telephone survey conducted in January contacted 2,100 businesses and government agencies in 27 countries and found that 100 percent of them had experienced cyber losses of some type in the past year. Seventy-five percent of organizations said they were hit by a cyber attack in the past year and 36 percent of those rate the attacks as either "somewhat" or "highly effective."


Under attack
Almost a fifth of U.S. businesses said they suffered 20 or more incidents such as virus infections in an FBI survey of computer security incidents at companies in the past year.
1-4: 51.5%
5-9: 20.1%
10-19: 9.1%
20 or more: 19.2%
SOURCE: The 2005 FBI Computer Crime Survey

Le coût des attaques augmente dans pratiquement tous les secteurs :



Concepts utiles

Confidentialité : Nous voulons des systèmes où l'information n'est accessible qu'aux utilisateurs à qui les messages sont destinés.

Plusieurs techniques permettent d'obtenir la confidentialité. Les méthodes de la cryptographie donnent des solutions pratiques pour satisfaire cet objectif.

Conformité : Nous voulons des systèmes qui assurent les destinataires d'un message de son origine et de son intégrité.

Comme pour la confidentialité, l'authenticité peut être garantie par des méthodes cryptographiques.

Accessibilité : Nous voulons des systèmes qui fonctionnent comme ils se doivent. Les données produites doivent être accessibles aux utilisateurs légitimes.

Nous ne voulons pas dire la fiabilité et la conformité des programmes ici. Plutôt, qu'arrive-t-il en cas de panne de courant pendant l'exécution d'une requête?

Les politiques de sécurité

Dans la pratique, nous avons besoin d'une description des objectifs de sécurité qu'un système nécessite (c.-à-d. politique de sécurité) :

Doit être beaucoup plus précise que de parler d'authenticité et de confidentialité.

Il est primordial d'établir les objectifs avant d'envisager les méthodes…

Dans un modèle abstrait, une politique peut ressembler à l'identification des états considérés comme vulnérables (à éviter) et sécuritaires.

Lorsqu'un système fait appel aux humains comme participants actifs alors les politiques sont souvent beaucoup moins précises parce qu'elles sont dictées dans le langage habituel. Le problème est qu'elles laissent ainsi place à interprétation.

Les politiques de sécurité (II)

Une politique de sécurité est une façon de définir les événements que l'on veut éviter dans le fonctionnement d'un système.

Ce qu'est une politique de sécurité est différent d'un auteur à l'autre. Elle peut dans certains cas contenir des stratégies dont le but est de garantir que les objectifs sont satisfaits.

Un énoncé politique et non une politique!

Une politique:

Cette politique vise à assurer que nos machines ne soient pas sujettes aux attaques de virus informatiques. Chaque machine doit utiliser un logiciel antivirus. Une seule personne doit être responsable de chaque machine. Elle doit vérifier que les logiciels antivirus sont mis à jour.

Une non-politique:

Cette compagnie prend la sécurité très au sérieux. Les attaques par virus informatiques sont très dangereuses. Nous ferons tout pour les éviter!

Modéliser les attaques

N'importe quel système peut être attaqué :

par des utilisateurs honnêtes mais négligents,

par des utilisateurs malhonnêtes,

par des intrus qui prennent le contrôle de machines, ou

par la nature (p.ex. une panne de courant)…

Repousser toutes ces attaques est habituellement impossible. Sinon, c'est souvent inabordable et inefficace.

Nous devons donc nous en tenir à un modèle définissant les attaques contre lesquelles nous voulons nous prémunir.

Les mécanismes de sécurité

Modèle d'adversaires

Politique de sécurité

mécanismes de sécurité

Sécurité du système?

Dans ce cours, nous prendrons le direction inverse!

Les mécanismes

Politique

Seuls les médecins sont autorisés à accéder aux dossiers des patients.

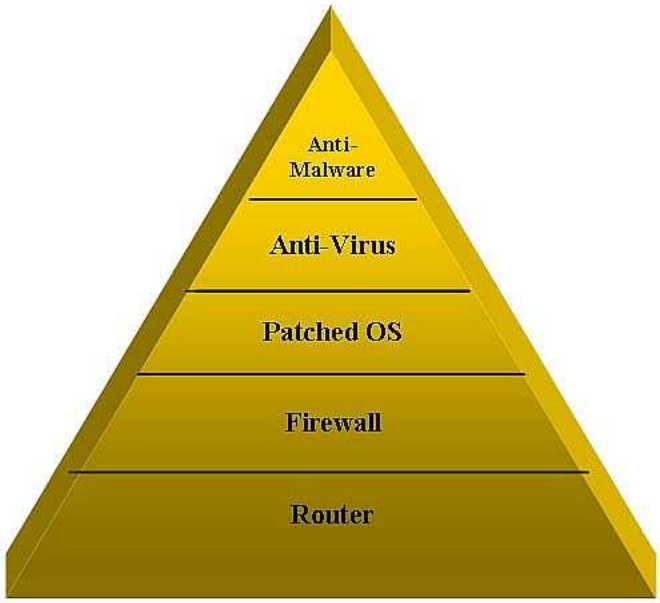
Modèle d'adversaire

Les intrusions à partir de terminaux doivent être éliminées.

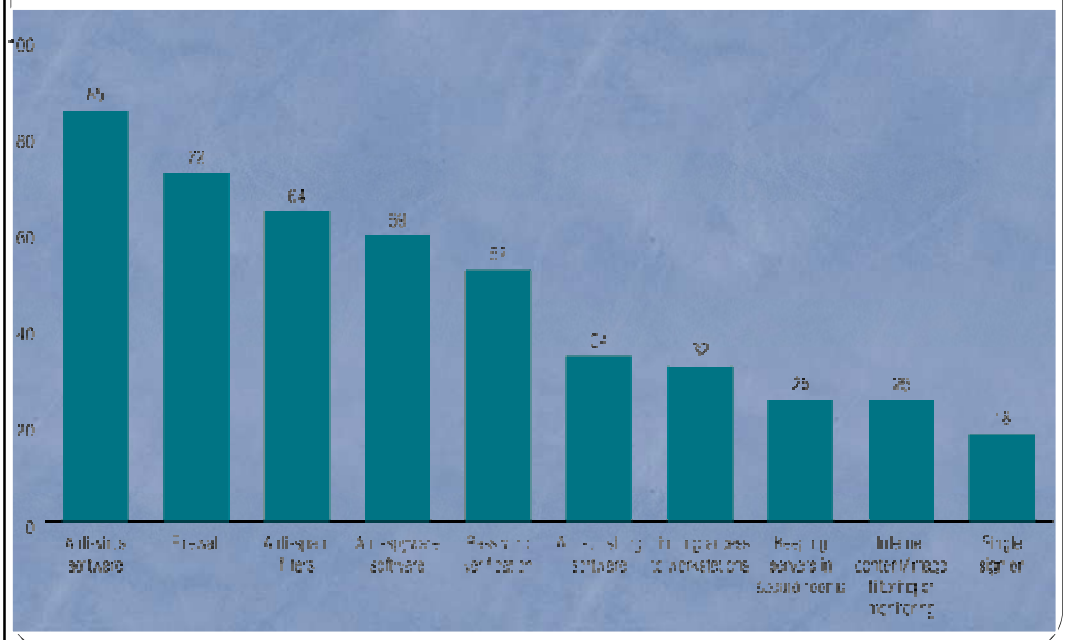
Les mécanismes de sécurité devront probablement contenir :

- Une base de données chiffrée contenant les dossiers médicaux
- Un accès par mot de passe assurant que seuls les médecins autorisent le système à fournir les données en clair.

Quelques mécanismes



La sécurité dans l'industrie



Établir la sécurité

Supposons que nous avons une politique de sécurité bien établie, un modèle d'adversaire précis, et que nous avons utilisé des mécanismes de sécurité pour satisfaire nos politiques :

> Est-ce que le système résultant est sécuritaire? Peut-il être attaqué avec succès?

Cette question est la plus importante en sécurité informatique, mais aussi la plus difficile.

Dans bien des situations, les réponses sont meilleures que « Ç'a l'air correct ça! », mais n'arrivent pas à donner une conclusion définitive. Pourquoi?

Établir la sécurité (II)

Pour prouver la sécurité d'un système, nous devons avoir un modèle mathématique nous permettant de prouver des théorèmes pour établir que le système n'atteint jamais un état vulnérable.

Ces modèles doivent composer avec tous les adversaires inclus dans le modèle d'adversaire.

Ceci peut causer des problèmes :

Le modèle d'adversaire est d'une trop grande généralité pour la représentation de toutes les menaces. Il devient alors très difficile de prouver quoi que ce soit. Le problème peut même devenir indécidable.

Le modèle d'adversaire est trop restrictif pour que toutes les menaces soient écartées. Un adversaire pourrait alors passer entre les mailles.

Établir la sécurité (III)

Tout ceci est bien malheureux mais nous devons adopter un point de vue pratique ici :

La sécurité est nécessaire.

Même si la théorie est incomplète, ceci ne veut pas dire qu'il ne faut rien faire.

Même si la théorie est incomplète, ceci ne veut pas dire qu'elle est inutile. Nous pouvons par exemple nous assurer qu'un certain nombre de menaces sont exclues et nous concentrer sur l'analyse des autres.