Sécurité des systèmes d'information

Concepts fondamentaux

Nathanaël Cottin

contact@ncottin.net
http://www.ncottin.net

version 0.0.2 – 2011

Facteurs

- Omniprésence des données numériques
- Transactions commerciales
- Partenaires commerciaux

Types d'agresseurs, motivations

- Plaisantins : curiosité
- Compétiteurs : notoriété
- Vandales : vengeance
- Espions : cupidité
- Autre : ignorance

Principales fraudes et menaces

- Usurpation d'identité
- Authentification
- Déni de service
- Menaces dérivées :
  - Fishing (hameçonnage) : détournement d'informations
  - Spoofing d'IP (usurpation d'adressse IP) : modification de l'IP de l'émetteur
  - Sniffing réseau

Types de sécurité

- Sécurité physique (matérielle)
- Sécurité logique
- Sécurité des communications
- Facteur humain

Éléments à sécuriser

- Infrastructures (déni de service)
- Réseaux et protocoles de communication
- Postes de travail (logiciels malveillants)
- Employés...

Objectifs

- Intégrité : garantie de non falsification des données
- Confidentialité : contrôle de l'accès aux données sensibles
- Disponibilité : garantie d'accès au SI
- Non-répudiation : impossibilité de négation d'une transaction (initiateur et destinataire)
- Authentification : accès aux ressources uniquement par les entités autorisées

Étude du risque

Risque exprimé par :

$$R = \frac{M \times V}{CM}$$

Avec :

- R : risque
- M : menaces (actions nuisibles)
- V : vulnérabilités (failles potentielles)
- CM : contre-mesures (prévention des menaces)

Types de sécurité

- Sécurité par l'obscurité
- Sécurité par hôte individuel
- Sécurisation des accès réseau

⇒ Politique de sécurité

Contenu

Procédures :

- D'alerte
- De sauvegarde
- De restauration et reprise

⇒ Prévention : limiter l'impact des menaces
⇒ Réaction :

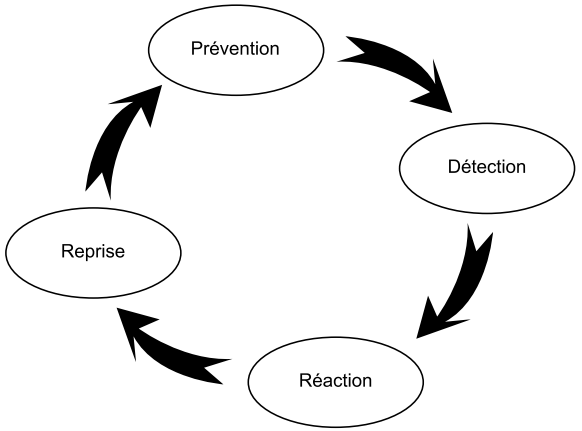
- Réduire les délais de traitement
- Favoriser la continuité d'activité

Mise en place

- Audit de l'existant
- Vulnérabilités et failles potentielles
- Propositions de solutions

⇒ Besoin d'organisation de l'entreprise
⇒ Prévoyance et (in)formation

Cycle de mise en œuvre



Points abordés

- Trames réseau : IDS, pare-feu, ...
- Protocoles réseau : TLS, ...
- Cryptographie

⇒ Sécurité logique
⇒ Sécurité des comunications

Identification

Identification

Désignation d'un individu au sein d'une population par une association personne – information unique

⇒ Connaître l'identité d'un utilisateur
⇒ L'identification n'authentifie pas un utilisateur pour l'accès à une demande particulière (autorisation)

Authentification

Authentification

Vérification de la validité d'une information pour un individu identifié. Ne requiert pas nécessairement l'unicité

⇒ Vérifier l'identité d'un utilisateur
⇒ Exemple : login / mot de passe de connexion d'un compte partagé n'identifie pas l'utilisateur

Autorisation

Autorisation

Validation des droits d'accès d'un utilisateur authentifié lui permettant d'accéder à des ressources et/ou traitements

⇒ Exemples : exécution d'un service distant, gestion d'un sémaphore sur une ressource critique

Moyens de preuve d'identité

- Ce que l'on sait : mot de passe
- Ce que l'on détient : clé secrète, objet physique (dongle)
- Ce que l'on est : biométrie
- Ce que l'on sait faire : signature

Attaque par rejeu ("replay")

A FAIRE...

Usurpation d'adressse IP ("IP spoofing")

A FAIRE...