Sensibilisation à la sécurité informatique

Jean-Luc Archimbaud

SECURITE SENSIBILISATION

Jean-Luc Archimbaud

CNRS/UREC

jla@urec.fr

http://www.urec.fr/jla

Juin 1997

Cours orienté Unix et IP

PLAN (1)

Exemples d'incidents

La sécurité dans notre monde
- Généralités
- Etude CNRS

Support "logistique"
- Structures en France
- Actions CNRS
- CERTs
- Chartes

Sécurité des réseaux
- Concepts
- Chiffrement
- L'écoute sur Ethernet et le câblage

Caractéristiques de l'Internet, Renater, IP

Sécurité des applications réseaux Unix

PLAN (2)

- Contrôle d'accès
  - Avec les tables de routage dans les stations
  - Avec les tables de routage dans les routeurs
  - Avec des filtres sur un routeur
  - Exemple de structuration de réseau
- Outils
  - crack
  - cops
  - iss et satan
  - tcp_wrapper
  - kerberos
  - boite de chiffrement IP
  - calculettes et S/Key
  - gardes-barrières
- Résumé : où peut on agir ?
- Conseils pour la mise en place d'une politique de sécurité
- Conseils pour les administrateurs de réseaux
- Conseils pour les administrateurs de stations Unix en réseaux

EXEMPLES D'INCIDENTS

GET /ETC/PASSWD

CHOOSE GIRL

/BIN/LOGIN

MOT DE PASSE NVRAM (EEPROM)

TREMPLIN POUR HACKERS

UNE ECOLE DE HACKERS

DIFFUSION DE MESSAGES RACISTES

LA SECURITE DANS NOTRE MONDE : GENERALITES SUR LA SECURITE

Les communications sont vitales pour l'Enseignement et la Recherche

---> la sécurité ne doit pas être un frein systématique

---> ouvrir quand c'est nécessaire

On ne peut pas ignorer la sécurité
Image de marque de l'université ou du labo !

Ca ne rapporte rien mais ça coûte

C'est toujours un compromis

C'est d'abord une affaire de Direction

Elle doit être vue globalement

LA SECURITE DANS NOTRE MONDE : GENERALITES SUR LA SECURITE

La sensibilisation est indispensable

- **Direction (---> responsabiliser)**
- **Utilisateurs**
- **Administrateurs de machines et de réseau**

---> La sécurité est l'affaire de tous

La sécurité c'est 80 % bon sens et 20 % technique

70 % des délits viennent de l'intérieur

Unix est surtout vulnérable à cause de

- **Sa popularité**
- **L'attitude des vendeurs qui livrent un système ouvert**

LA SECURITE DANS NOTRE MONDE : GENERALITES SUR LA SECURITE

En réseau : demande de la compétence et de la disponibilité

Les mécanismes doivent être fiables

Faire ce qu'ils sont sensés faire

--> validation des matériels et des logiciels

Le service doit répondre aux besoins

Ex : le chiffrement est inutile si on a besoin de contrôle d'accès

Il faut regarder le coût / efficacité

---> la confidentialité ou l'intégrité sélective

Facilité d'utilisation et d'apprentissage

Rejet ou contournement si trop contraignant

Ex : mots de passe, accès aux fichiers

Souplesse d'adaptation & portabilité

Evolution, matériel hétérogène

---> normes, standards

LA SECURITE DANS NOTRE MONDE : ETUDE CNRS

Echantillon :

- **3 départements : SPI-SV-IN2P3**
- **11 sites**

Méthode : Melisa et Marion et ...

MARION : méthode d'audit de sécurité

- **600 questions**
- **Risques maximaux**
- **Schéma directeur SSI**

MELISA : méthode d'audit de sécurité

- **Auto-audit**
- **Origine DGA (Direction Générale de l'Armement)**

Buts :

- **En tirer un profil "laboratoire" (peut-être plusieurs)**
- **Découvrir les risques majeurs**

Pour :

- **un schéma directeur de la sécurité**
- **établir des recommandations**
- **engager des actions**
- **mener à bien ce schéma**

LA SECURITE DANS NOTRE MONDE : RECOMMANDATIONS ETUDE CNRS

Désignation d'un responsable de la sécurité

Sensibilisation des personnels

Sauvegardes régulières

Bonne gestion de mots de passe

Amélioration de l'administration des stations

Protection des éléments de communication

Fermeture à clé des portes

Organisation et contrôle des personnels non permanents

Respect des réglementations

- **Trop de copies de logiciels**
- **Peu de déclarations à la CNIL**

Amélioration de la qualité des développements

STRUCTURES

Haut fonctionnaire de défense ENSRIP :

M. Pioche

Universités

Un correspondant / Université ou Ecole
Nombre d'établissements : 130
Coordination CRU

CNRS

Fonctionnaire de défense : M. Schreiber

RSSI : Michel Dreyfus

CM "Sécurité informatique (réseaux)" 1/2 temps

Correspondant / DR

Correspondant technique / "gros labo"

Accord tacite de réciprocité" CNRS et Ens Sup

RENATER

Charte RENATER

CERT-RENATER

Un correspondant sécurité par organisme

Isabelle Morel

FRANCE

BCRCI

CNIL

DST

SCSSI

Aide en cas d'incident de sécurité

Diffusion électronique -> correspondants techniques

---> CERT-CNRS

Diffusion fax -> correspondants DR

Cours - sensibilisation

Bulletin d'information ---> Dir Labo
Cours sécurité Unix en réseaux
Journées de sensibilisation avec le SCSSI
Rubrique "Sécurité" dans le Microbulletin

ftp.urec.fr, gopher.urec.fr, www.urec.fr

Recommandations papiers

Tests de certains produits

Groupe sécurité SOSI

LES CERTS

Computer Emergency Response Teams

Sert une communauté

FIRST : regroupe les CERTs

Organise les moyens de défense et de réaction

Diffusion d'information

- ## Recommandations
- ## Corrections de trous de sécurité (informatique et réseau)

Mise en relation des responsables sécurité

Petite cellule

Experts

Pression sur les constructeurs . . .

Ne remplace pas la police

CHARTES

"de bon usage" ou "de sécurité"

Sensibilisation-responsabilisation des personnels

Par université ou laboratoire

Exemples : ftp.urec.fr:pub/securite/Chartes

Contenu

- Utilisation des Systèmes d'Information
- Qui est responsable de quoi
- Ce qu'il ne faut pas faire
- Recommandations (choix du mot de passe, ...)
- Rappel des lois et des peines encourues

Signée par tous (même les utilisateurs de passage)

Peut-être courte

Pas de valeur juridique

CONCEPTS SECURITE RESEAUX

CONFIDENTIALITE

Message compris uniquement par le destinataire
Mécanisme : chiffrement

INTEGRITE

Message reçu identique à celui émis
Mécanisme : scellement - signature

CONTROLE D'ACCES

Uniquement les émetteurs autorisés peuvent envoyer des messages
Toutes les couches et étapes
Filtrage - ACL

NON RÉPUDIATION

Sur l'émetteur
Sur le destinataire
Mécanisme : notarisation

AUTHENTIFICATION

- Certificat d'identité
- Couplée avec identification
- Dans les 2 sens
  - Appelant (individu) ---> Appelé (application)
  - Appelé (application) ---> Appelant (individu)
- Problème de l'unicité de l'identification
- Problème de l'Autorité

Authentification d'un utilisateur : mécanismes

- Ce qu'il sait - Ce qu'il est - Ce qu'il possède
- Mot de passe
  - Pour accéder à quoi ?
  - Problème réseau : où est il stocké ?
- Avec un matériel spécifique
  - Caractéristique physique de l'utilisateur
- Objet que détient l'utilisateur
  - Carte à puce
  - Authentifieur - Calculette
- Problèmes
  - Coût - Normalisation - Accès universel
- Exemple sur un réseau : KERBEROS

CONCEPTS SECURITE RESEAUX

DISPONIBILITE

Matériels et logiciels doivent fonctionner
Maillage des liaisons, duplication des équipements

TRACES

Journalisation
Etre au courant d'un problème, comprendre et éviter la réédition
Problème du dépouillement
Problème du volume de données

ALARMES

AUDIT

Quel est le niveau de sécurité de ma machine, de mon réseau, de mon site ?