supervision de la sécurité

- aspects juridiques
- organisation
- collecte d'information

Supervision: aspects juridiques

- un exposé précis sort du cadre de cet enseignement (=> nous ne ferons que des constatations générales)
- superviser l'activité du réseau implique de conserver, analyser des données personnelles (adresse ip, journaux d'un proxy WEB, ...)
- le recoupement des traces collectées permet une surveillance des personnels

Problèmes et solutions

- Problèmes :
  - ne pas tomber dans l'excès de surveillance;
  - la collecte des données personnelles et la cybersurveillance sont encadrés par la loi
  - la jurisprudence impose de journaliser les accès vers internet
- Solutions:
  - le personnel doit être prévenu à l'avance (charte informatique, information spécifique)
  - faire valider l'adéquation du dispositif avec la réglementation
  - qualifier les données de façon à réglementer l'accès aux journaux et autres données de supervision (contenant des données personnelles)

jurisprudence, position de la cnil

- un administrateur système
  - doit garantir la continuité de service et la sécurité des systèmes et des réseaux
  - dans ce cadre, il peut avoir à manipuler des données personnelles
- exploitation des données de supervision
  - uniquement à des fins liées au bon fonctionnement du réseau et des systèmes
  - aucune autre utilisation n'est tolérée, même sur ordre hiérarchique
  - l'administrateur système n'a pas à rendre compte à sa hiérarchie de ce qu'il découvre dans les données privées qu'il manipule

Aspect juridique: un exemple concret

- Le cas décrit ci-dessous a été décrit en cours.
- cf http://www.juriscom.net/txt/jurisfr/prv/tcorrparis20001102.htm

Organisation

- supervision : coûteux notamment en temps humain
- des pratiques standardisées: voir par exemple ITIL (IT Infrastructure Library : ensemble de bonne pratiques)

Collecte d'information

- mode de collecte : synchrone vs asynchrone
- mécanisme de tranport
  - garantir: intégrité, authentification et confidentialité
  - respecter la politique de sécurité et notamment le sens des flux, la politique de gestion de mots de passe, ...
- performances
  - performance de la collecte qui ne doit pas perdre d'information
  - impact de la collecte sur les performances des systèmes et du réseau
- fiabilité du stockage

Collecte: exemples

- savoir discerner les événements utiles dans un flot d'évènements
- journaliser les évènements pertinents pour éviter le raz de marée

Collecte : exemples

- Exemples d'évènements individuellement pertinents
  - modification de fichiers systèmes (configuration, exécutables, dll, ...)
  - ouverture de session hors heures ouvrables, échecs d'ouverture de session
  - création de comptes utilisateur
  - arrêt/redémarrage d'un service, reboot d'un équipement

Collecte: exemples

- Les outils de détection d'intrusion (IDS) génèrent un nombre important d'évènements
  - -> approche statistique: si on passe de 10 évènements par minutes à 100/mn, il faut regarder de plus près
  - lien avec un scanner de vulnérabilité (une attaque sur un système dont on sait qu'il présente la faille vs idem sur un système sans la faille)
- trafic réseau:
  - détection de anomalie de trafic (pic, type, horaires, ports, ...)
  - insertion de trafic, attaques classiques

validation de la sécurité: audit et tests d'intrusion

- dans une version ultérieure de ce document.

réagir face à une intrusion

- intrusion
- intrusion: en quoi suis-je concerné ?
- formation, response team
- détecter l'intrusion
- CERT, kesako ?
- faire cesser l'intrusion
- permettre l'analyse de la cause et de la source de l'intrusion
- garantir la continuité de service

intrusion

- un intrus pénètre dans un système d'information :
  - en exploitant une erreur de configuration
  - en exploitant une ou des vulnérabilités logicielles
  - via des informations (mot de passe, ...) récupérés sur un autre système compromis,
  - par « social engineering »
  - ...

Intrusion

- ayant pris le control à distance des systèmes vulnérable, l'attaquant pourra :
  - consulter et falsifier des données confidentielles (courriers, mot de passe, rapports, No CB, ...)
  - installer des programmes lui permettant de revenir simplement (backdoor)
  - attaquer d'autres machines internes : rebond interne
  - attaquer des machines d'autres sites depuis ces machines: rebond externe
  - porter atteinte à l'image de l'organisation attaquée (en défigurant son site WeB, ...)

intrusion: en quoi suis-je concerné ?

- réponse irresponsable: « je n'ai pas de données précieuses donc je ne suis pas concerné »
- responsabilité
  - en cas d'utilisation par l'intrus pour attaquer d'autres sites (rebond, ddos, spam, ...)
  - pour mettre en ligne des serveurs de warez, irc, ...
- continuité de service
- vol/destructions de données, défiguration de site WeB, ...
- perte d'image

Aspects juridiques d'une intrusion

- dans une version ultérieure de ce document
- à prendre en compte :
  - s'il doit y avoir dépôt de plainte, les traces prouvant les choses doivent être inattaquables. Pb: elles proviennent des équipements du plaignant (vous !).
  - la destruction de preuves est répréhensible : l'une des premières action doit être de faire une copie secteur à secteur des disques du système concerné
  - votre responsabilité peut être en jeu si l'intrus attaque d'autres sites depuis le votre

formation, response team

- garantir une réaction de qualité en cas de détection d'intrusion nécessite
  - une politique de sécurité qui définit
    - les actions préventives notamment en matière de conservation d'information
    - les actions de terrain à mener en cas d'intrusion permettant d'éviter des erreurs irrémédiables
  - une formation/information des personnels informatique
  - une entité centrale (Response Team) à même de conseiller, accompagner les personnels de terrain

détecter une intrusion

- la honte (+problèmes juridiques): être prévenu par une autre entité qu'il y a eu une intrusion sur son propre parc
- La détection suppose des mesures préventives génériques (bonnes pratiques du métier, voir transparent suivant)
- des mesures locales « non standard » sont un plus car elles peuvent prendre au dépourvu un attaquant pas trop malin ou son rootkit

mesures à prendre pour détecter l'intrusion

- mesures à prendre à l'avance:
  - des journaux non falsifiables et analysés
  - régulièrement: centralisation via syslog, snmp
  - des horloges synchronisées
  - des mécanismes de détection automatiques (IDS, tripwire, ...)
  - surveillance des systèmes et du trafic réseau
  - prise d'empreinte des fichiers du système
    - de façon à pouvoir détecter les fichiers corrompus
    - stockées hors ligne ou sur support en lecture seule
  - un kit d'outil et des fiches de procédures pour l'intervention après intrusion
  - pot de miel: attention, juridiquement et techniquement délicat.

CERT®, CSIRT: Historique

- 1988: R. Morris crée un vers utilisant sendmail qui échappe à son contrôle.
- suite à l'inefficacité des réactions et du manque de coordination: création du premier CERT
- création de nombreux CSIRT
- 1989: WANK (War Against Nuclear Killer) montre le manque d'efficacité de ces CSIRT qui ne se font pas confiance
- 1990: création du FIRST (Forum for Incident Response Security Team): communication entre CSIRT en termes de prévention, réaction et recherche.

CERT®/CSIRT

- CSIRT: Computer Security Incident Response Team (CERT® est un terme déposé)
- CERT®: Computer Emergency Response Team. Le CERT® est le premier CSIRT.
- FIRST (Forum for Incident Response Security Team)

Rôles d'un CSIRT

- centralisation des demandes d'assistance suite aux incidents de sécurité (attaques)
  - réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;
- traitement des alertes et réaction aux attaques informatiques :
  - analyse technique, échange d'informations avec d'autres CERTs,
  - contribution à des études techniques spécifiques ;

Rôles d'un CSIRT

- établissement et maintenance d'une base de donnée des vulnérabilités ;
- prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au moins leurs conséquences ;
- coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet CERTs nationaux et internationaux.

CSIRT Français

- Quelques CSIRT français :
  - le CERTA dédié au secteur de l'administration française ;
  - le Cert-IST est le CSIRT dédié au secteur de l'Industrie, des Services et du Tertiaire (IST);
  - le CERT-RENATER est le CERT dédié à la communauté des membres du GIP RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche).

Comment réagir à une intrusion

- mesures immédiates à prendre
  - problèmes:
    - soit perdre perdre les informations volatiles en cas d'arrêt brutal du système
    - soit risquer une réaction de l'intrus en cas d'analyse préalable sans arrêter
    - juridiquement, provoquer la destruction de preuves est répréhensible
  - dans tous les cas, prévenir le RSSI de l'entreprise, le CERT ad hoc
  - ne pas se faire justice soit-même, contacter le CERT® concerné et suivre ses conseils

politique 1

- on joue la sécurité
- pour éviter toute destruction de données et toute attaque sur des sites distants
- pour éviter toute destruction de preuve et toute modification du disque dur local
- au détriment de la récupération des traces volatiles

- On arrête tout de façon à empêcher l'intrus de réagir et d'agir
  - déconnecter l'équipement concerné du réseau
  - arrêter le système (éventuellement brutalement)
  - analyse post mortem

Politique 2

  - on prend des risques (destruction de données, attaque d'autres sites, destruction de preuves, ...)
  - pour maximiser le nombre d'éléments récupérés
- on laisse le système compromis tourner pour récupérer des traces de son fonctionnement
  - analyse réseau
  - récupération des données volatiles et analyse du système compromis en marche (hors du cadre de cet enseignement, voire article revue MISC No 9)
  - copie des données hors ligne
  - déconnexion et arrêt du système
  - analyse post mortem

analyse postmortem

- sauver les traces sur un support hors ligne :
  - faire une copie physique du disque
    - indispensable juridiquement
    - la copie secteur à secteur préserve les zones non utilisées du disque et la mémoire virtuelle
  - sauver les journaux de l'équipement et des autres éléments du réseau (qui ont forcément interagit avec l'équipement/le pirate)

rétablir le service

- réinstaller l'équipement concerné
- changer tous les mots de passe, clefs, ...
- restaurer les données d'après une sauvegarde non compromise
- passer tous les correctifs de sécurité
- combler la faille exploitée par l'intrus (ce qui suppose de l'avoir détectée)

Bibliographie

- documents du CERTA (http://www.certa.ssi.gouv.fr/)
- MISC No 9: que faire après une intrusion
- « sécurité informatique: principes et méthodes » de L. Bloch et C. Wolfhugel, Eyrolles.

Bibliographie

- MISC 27, sept-oct. 2006 : « la méthode EBIOS: présentation et perspective d'utilisation pour la certification ISO 27001 »
- MISC 27, sept-oct. 2006 : « Contrôler l'accès aux réseaux et la conformité des équipements »
- MISC 2; avri-mi-juin 2002: « architecture d'un réseau sécurisé »
- MISC 2; avri-mi-juin 2002: « protection de l'infrastructure d'un réseau IP: couche liaison de données »