

Présentation:

- Pascal PETIT
- enseignements:
 - notions de sécurité
 - firewall
 - firewalls libre (netfilter, ipfilter, packetfilter)
- pascal.petit@shayol.org
- tel.: 01 60 87 39 03 (peu fiable)

I Principes de sécurités

- Critères fondamentaux
- domaines d'application de la sécurité
- multiples facettes de la sécurité

Critères fondamentaux

- disponibilité
- intégrité
- confidentialité
- authentification
- non répudiation

Disponibilité

- disponibilité d'une ressource: la ressource est disponible et accessible avec des temps de réponse acceptables
- s'obtient par :
 - dimensionnement approprié et redondance des éléments constitutifs;
 - gestion opérationnelle des ressources et des services
 - exemple: pour un réseau: dimensionnement correct des liens, des matériels actifs et politique de gestion et de routage satisfaisante

Disponibilité (2)

- test de montée en charge
- respect de clause d'engagement de service : indicateurs dédiés à la mesure de la continuité de service
- perte de données
 - sauvegardes
 - procédure de restauration
 - politique de sauvegarde
 - arbitrage entre coût de la sauvegarde et risque d'indisponibilité (ex.: incendie du CL)

Intégrité

- certifier que les données n'ont pas été altérées de façon intentionnelle ou accidentelle
- la modification peut avoir lieu
 - lors du transfert des données (corruption, écoute active)
 - lors du stockage des données
 - lors de leur traitement (bogues des logiciels applicatifs, des OS).
- Implications:
 - légales, plantage des applications et perte d'activité
 - perte d'image

Confidentialité

- protection des données contre une divulgation non autorisée
- 2 moyens techniques complémentaires
 - protéger l'accès aux données
 - les chiffrer
- intégrité et confidentialité ont des contraintes opposées
 - intégrité : multiplier les sauvegardes notamment hors site
 - confidentialité: limiter les lieux de stockage pour faciliter le contrôle d'accès

authentification

- élément clef pour assurer :
 - la confidentialité et l'intégrité des données via un contrôle d'accès: seules les personnes identifiées, authentifiées et habilités à le faire peuvent accéder/modifier les données
 - la non-répudiation et l'imputabilité (preuve d'une transaction, ...)
- Authentification unique (SSO: Single Sign On)
 - l'utilisateur s'authentifie une fois
 - il a accès à toutes les ressources du réseau
 - cf partie technique (keberos, ...)

Critères fondamentaux

- disponibilité
- intégrité
- confidentialité
- authentification
- non répudiation

Identification et authentification

- **identification**: définir l'identité de l'utilisateur
- **authentification**: permet de vérifier l'identité fournie (authentification simple vs authentification forte)
 - via un élément que l'utilisateur connaît (mot de passe, ...)
 - via un élément que l'utilisateur possède (carte à puce, certificat, ...)
 - via biometrie

non répudiation

- **non répudiation** : ne pouvoir nier qu'un événement a eu lieu
- **imputabilité**: on sait qui a réalisé une action
- **traçabilité**: on mémorise des événements imputables
- **auditabilité**: pouvoir réaliser une analyse ultérieure d'un événement. Ex.: en cas d'intrusion.
- moyens: utilisation de journaux
 - de taille limitée
 - éventuellement hors site (intrusion)

Domaine d'application de la sécurité

- sécurité physique
- sécurité de l'exploitation
- sécurité logique
- sécurité applicative
- sécurité des télécommunications

sécurité physique

- maîtrise des systèmes et de l'environnement où ils évoluent
- repose sur :
 - protection des sources énergétique (ex. de redbus)
 - protection de l'environnement (température, sinistre du type incendie, ...=
 - protection des accès physiques
 - sureté de fonctionnement et fiabilité des matériels
 - redondance physique
 - marquage des matériels
 - plan de maintenance préventive (test, ...) et corrective (pièce de rechanges, procédures, ...)

sécurité logique

- mécanisme de contrôle d'accès aux données
- identification/authentification/autorisation
- cryptographie/mots de passe/authentification
- classifier les données pour qualifier leur sensibilité (publique, confidentielle, ...) et les droits d'accès correspondant

sécurité des télécommunications

- offrir une connectivité fiable de bout en bout
- infrastructure réseau sécurisée au niveau:
 - des accès
 - des protocoles de communication
 - des systèmes d'exploitation
 - des équipements (redondance, boucles, ...)
- ex. de pb classiques:
 - la pelleteuse
 - bug sur un matériel actif
 - problème d'interopérabilité entre matériel actifs, logiciels, ...

sécurité de l'exploitation

- tout ce qui touche au bon fonctionnement des systèmes
- points clefs
 - plan de sauvegarde,
 - plan de secours
 - plan de continuité
 - plan de test
 - inventaire régulier
 - gestion du parc
 - gestion des configurations et des mises à jour
 - gestion des incidents et suivi jusqu'à leur résolution
 - automatisation, contrôle et suivi de l'exploitation, supervision
 - analyse des journaux
 - gestion de la maintenance
 - environnement de test et de production séparés

sécurité applicative

- fiabilité des logiciels pour assurer la continuité de service et l'absence de corruption des données
- repose sur :
 - méthodologie de développement
 - robustesse des applications
 - contrôles programmés, jeux de tests, procédures de recettes
 - sécurité des progiciels
 - élaboration des contrats (clause d'engagement de responsabilité)
 - validation et audit des programmes
 - qualité et pertinence des données
 - plan d'assurance sécurité (souvent une section du plan d'assurance qualité)
 - indépendance des fournisseurs (logiciel libre, travail en régie, développement local, ...)

Exercice (énoncé)

- dans une petite entreprise, l'ingénieur système a organisé les sauvegardes de la façon suivante :
 - les données sont sur les postes utilisateurs;
 - chaque poste utilisateur est muni d'un graveur de DVD qui contient un DVD RW
 - pour effectuer une sauvegardes, les utilisateurs
 - effacent le DVD-RW
 - créent un fichier .zip
 - le sauvent sur le DVD
- Que pensez-vous de cette procédure ?

Exercice (éléments suggérés par la salle)

- à saisir en direct sur la suggestion des étudiants

facettes de la sécurité

- diriger la sécurité:
 - politique de sécurité
 - un ensemble de mesure techniques éparses ne doit pas se substituer à une gestion cohérente comprenant une évaluation des risques
- aspects juridiques:
 - responsabilité des autres vis à vis de nous (contrat, lois, ...)
 - responsabilité lié au droit des nouvelles technologie (conservation des données, gestion des données personnelles, surveillance, propriété intellectuelle, délit de manquement à la sécurité, ...)

II La stratégie de la sécurité

- évaluer les risques
- démarche sécuritaire
- stratégie de sécurité
- rapport coûts/bénéfices

Exercice (éléments de correction)

- procédure non automatisée, intégralement manuelle reposant sur les utilisateurs
- quid d'un crash pendant la sauvegarde ?
- exhaustivité de la sauvegarde ? , évaluation des risques ?
- quid des tests ?
- quid de la procédure de restauration ?
- surveillance des sauvegardes (journaux)
- sauvegarde hors site ?
- confidentialité des sauvegardes en cas de vol ?
- quid du sav du matériel, procédure en cas de crash ?

facettes de la sécurité (2)

- éthique et formation:
 - charte reconnue par tous
 - les signataires doivent avoir les moyens de l'appliquer
 - actions d'information et de formation
- architecture de la sécurité:
 - dimension techniques et opérationnelles
 - dimension humaine
 - dimension juridique et réglementaire
 - dimension organisationnelle et économique

Evaluer les risques

- but: garantir la pérennité de l'entreprise
- Comment: via une stratégie de sécurité :
 - en se protégeant
 - en organisation la défense
 - en élaborant des plans de réactions aux sinistres

Risque:

- danger plus ou moins prévisible
 - mesurer sa probabilité
 - mesurer les dommages consécutifs
- réagir en
 - réduisant sa probabilité à un niveau acceptable (?)
 - prévoir les mesures à prendre s'il se produit

stratégie de sécurité

- garantir les fondamentaux (intégrité, ...) à l'aide d'outil (coupe-feu, ... et de procédures de gestion)
- démarche globale de l'entreprise (buts, vocabulaire commun, cohérence des outils et procédures déployées, ...)
- portée par la direction de l'entreprise
- compromis entre coût/niveau de sécurité/impact sur le fonctionnement de l'entreprise

IV partie technique

- préliminaire: chiffrement
 - chiffrement symétrique/asymétrique
 - PKI: infrastructure de clefs publiques
 - hachage
- Authentification
- sécurité des infrastructures de communication
- contrôle d'accès réseau
- supervision
- audit et tests d'intrusion
- réaction en cas d'intrusion

Démarche sécuritaire

- étape 1 : mise en place d'une politique de sécurité
 - identifier les valeurs
 - identifier les risques qu'elles courent
 - identifier les moyens et mesures de sécurité à mettre en oeuvre
- étape 2: mise en oeuvre des outils et des procédures
- étape 3: évaluer périodiquement l'adéquation et la cohérence des mesures de sécurité

rapport coût/bénéfice

- perte de productivité
- perte de parts de marché
- pénalité de retard
- perte d'image vis à vis des clients/fournisseurs/...
- coût de gestion des sinistres (assurance, experts, investigation ...)
- frais de justice
- coût de la remise en état

Chiffrement: robustesse

- cryptanalyse: analyser une information chiffrée pour la déchiffrer (dont des méthodes en force brute, ...)
- algo public
- la sécurité repose sur :
 - la non divulgation de la clef
 - la robustesse de l'algorithme
 - la taille de la clef (gare aux comparaisons entre algo différents)
 - l'utilisation de clefs différentes pour chiffrer des messages différents limite la quantité d'information à la disposition de l'attaquant

chiffrement: taille des clefs

- attaques en force brute: tenter une partie importante de l'espace des clefs
- temps dépend du nombre de clefs possibles et donc de la taille de la clef:
 - 10 bits : 1024 clefs possibles
 - 56 bits: $2^{56} \approx 7 \cdot 10^{16}$
 - dépendance exponentielle en fonction de la taille de la clef: 1 bit de plus = 2 fois plus de temps
- la taille critique dépend de l'algo (et de sa vitesse, de ses faiblesses, ...)

algorithmes classiques

- symétriques:
 - DES (1976): standard américain (1977), clef de 56 bits sur des blocs de 64 bits. dépassé de nos jours.
 - triple DES (1978): variante via une triple application de DES permettant d'avoir des clefs entre 128 et 192 bits sur des blocs de 64 bits.
 - RC2, RC4, RC5 (1994) et RC6:
 - IDEA (1992): clef 128 bits sur des blocs de 64 bits
 - blowfish: clef 32 à 448 bits sur des blocs de 64 bits. Algo très analysé, considéré comme solide. utilisation libre.
 - AES (1998): clefs 128, 192 ou 256 bits sur blocs de 128 bits. standard américain. utilisation libre.

durée de vie des clefs

- dépend de sa taille
- dépend de son taux d'utilisation
- dépend du contexte d'utilisation
- hiérarchie de clef (clef maîtresse, clef de session par ex.)
- révocation de clef
- une utilisation intensive du chiffrement nécessite la mise en place d'une IGC (infrastructure de gestion de clef ou PKI – Public Key Infrastructure en anglais)

algorithme de chiffrement

- chiffrement symétrique/asymétrique
 - symétrique:
 - les algo classiques sont rapides
 - la même clef sert au chiffrement et au déchiffrement
 - souvent utilisé via une clef de session
 - clef de session: transmise via algo asymétrique (on parle d'enveloppe digitale)
 - session: chiffrée par un algo symétrique et la clef transmise
 - asymétrique:
 - les algo classiques sont lents
 - couple de clef publique/clef privée
 - clef publique: peut être connue de tous
 - clef privée: tenue cachées
 - ce qui est chiffré avec l'une ne peut être déchiffré qu'avec l'autre

algorithmes classiques

- asymétriques:
 - RSA s'appuyant sur la factorisation de nombres premiers
 - Diffie-Hellman et El Gamal s'appuyant sur le calcul des logarithmiques discrets
 - des algorithmes nouveaux s'appuyant sur les courbes elliptiques

hachage/ empreinte

- principe:
 - une fonction non réversible H:
 - connaissant $H(x)$, il est très difficile de trouver y tel que $H(y)=H(x)$
 - telle que deux empreintes différentes correspondent forcément à deux textes différents
 - la probabilité d'avoir deux empreintes identiques est très faible

hachage: applications

- authentification des utilisateurs:
 - on stocke la version hachée du mot de passe
 - un grain de sel permet d'éviter que deux personnes qui ont le même mot de passe aient la même empreinte
- copie optimisée de fichiers
- vérification de l'intégrité de fichiers

signature d'un message

- On considère l'algorithme de signature suivant :
 - chiffrer avec sa clef privée un message m contenant le texte « je m'appelle toto »
 - joindre le courrier en clair à ce message chiffré et l'envoyer au destinataire
 - le destinataire peut lire le courrier et déchiffrer la signature avec la clef publique de toto.
- citez les failles de cet algorithme
- proposez des solutions pour les combler

PKI: Public Key Infrastructure (IGC: Infrastructure de Gestion de Clefs)

- Problème:
 - comment être sûr qu'une clef publique est valide et est bien la clef publique d'une personne donnée ?
- Solutions:
 - PGP: confiance transitive : WeB Of Trust
 - Certification par un tiers de confiance : IGC

Hachage: algo classiques

- MD4 (mdp windows NT & Co)
- MD5 (mdp unix): empreinte de 128 bits, considéré comme faible (collisions)
- sha-1: empreintes de 160 bits (solidité mise en doute actuellement)
- sha-2: empreintes de 256, 384 ou 512 bits au choix
- utilisation d'un algo de chiffrement: le mot de passe est transformé en clef pour chiffrer un texte connu. ex. connu: DES modifié itéré 25 fois pour les mots de passe unix.

One Time passwd: une application amusante des algo d'empreintes

- Exercice.
- dans une version ultérieure de ce document

IGC: définition

- IGC: ensemble de moyens matériels, de logiciels, de composants cryptographiques mis en oeuvre par des personnes, combinés par des politiques, des pratiques, des procédures requises qui permettent de :
 - créer
 - gérer
 - conserver
 - distribuer
 - révoquerdes certificats basés sur la cryptographie asymétrique

éléments obligatoires d'une IGC

- 3 éléments obligatoires :
 - autorité de certification
 - autorité d'enregistrement
 - service de publication

• autorité de certification (CA ou Certification Authority en anglais)

- autorité de confiance reconnue par une communauté d'utilisateurs
- délivre et gère des certificats de clefs publiques
- maintient une liste des certificats révoqués (LCR en français, CRL en anglais)
- les certificats sont conformes à la norme X.509
- génère les certificats à clef publique et garantit l'intégrité et la véracité des informations qu'ils contiennent en les signant avec sa clef privée

• Autorité d'enregistrement (RA: Registry Authority)

- intermédiaire entre l'utilisateur et l'autorité de certification.
- l'utilisateur s'adresse à elle
- en application de la politique de certification, elle vérifie les données de l'utilisateur :
 - identité
 - correspondance clef privée/publique
 - ...
- transmet les informations validées à l'AC

• Service de publication

- met à la disposition de la communauté les certificats générés par l'AC
- publie aussi la liste des certificats révoqués

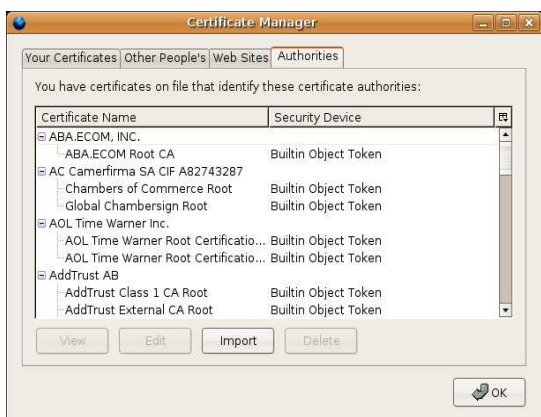
• Composants optionnels de l'IGC

- autorité d'horodatage (AH ou Timestamping Authority)
 - date des données qui lui sont transmises
 - Le Protocole D'horodatage (ou Time-Stamp Protocol) : rfc 3161
- service de séquestre:
 - stocke de façon sûre des clefs privées
 - pour permettre le déchiffrement des données en cas de perte
 - ne doit pas concerner les clefs de signature

• Certificat

- contient entre autre
 - l'identité de son propriétaire (personne, machine, ...)
 - sa clef publique signé par une AC
 - période de validité
 - type d'utilisation de la clef (champ optionnel)
 - ...

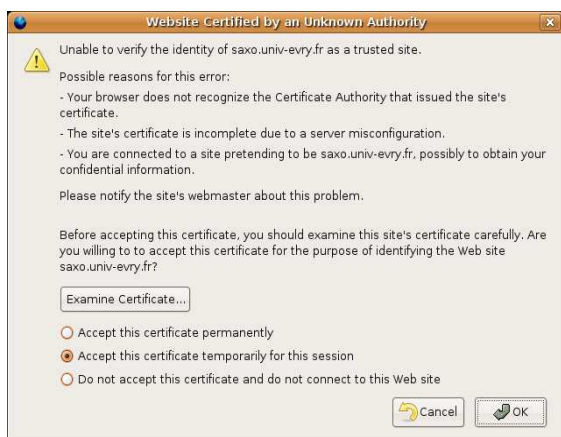
• Exemple: navigateur WeB



• Exemple: navigateur WeB:

- un client se connecte sur le site WeB de l'entreprise
- il obtient les références de l'AC et le certificat
- il vérifie le certificat
- il génère une clef de session qu'il transmet chiffrée au serveur de l'entreprise
- la session est maintenant chiffrée

• Exemple: Pb certification



• Exemple: certificat



Bibliographie:

- « méthodes de cassage des mots de passe » par D. Ducamp, 2005-2006, <http://www.ossir.org/resist/supports/cr/20060530/mdp-RESIST-2006-05.pdf>
- MISC No 13, mai-juin 2004: « PKI »
- « Sécurité informatique et réseaux » de S. Ghernaoui-Hélie, Dunod 2006

Authentification: aspects techniques

- protocoles
 - mot de passes jetables (« One Time Password: OTP »)
 - kerberos
 - « Secure Remote Password » (SRP)
- outils et protocoles associés
 - annuaires
 - NIS (et NFS)
 - LDAP
 - RADIUS

sécurité des infrastructures de télécommunication

- protocole IP
- intranet: sécurité contre les risques internes
- internet: sécurité contre les risques externes
- confidentialité

exemple d'attaque: dhcp

- neutraliser un serveur dhcp
- le remplacer
- devenir routeur (mim)
- serveur dns (phishing)

Contrôler l'accès au réseau (NAC)

- interdire l'accès au réseau interne des postes non autorisés
- but: éviter des attaques/vol d'informations d'un visiteur agissant de l'intérieur (filaire, WiFi)
- divers méthodes :
 - sécurité physique (accès aux locaux)
 - brassage à la demande
 - filtrage par adresses MAC ou IP
 - portail captif
 - analyse distante des postes
 - 802.1X

IP V4

- aucun mécanisme de sécurité
- aucun mécanisme d'authentification
- pas de gestion de la qualité de service
- aucun mécanisme pour la confidentialité
- le protocole contient des éléments facilement exploitables (désactivés de nos jours)
- conséquences:
 - sécurité géré au niveau application (ssh, https, ...)
 - vpn ,ipsec

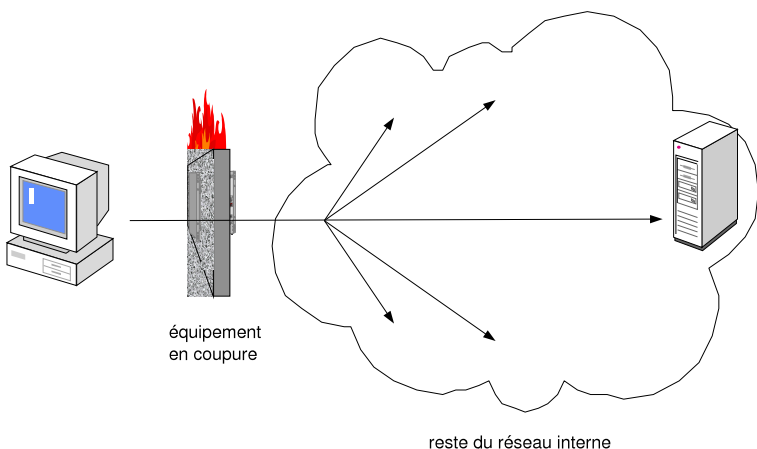
Intranet: risques

- bon dimensionnement et bonne gestion du réseau interne de l'entreprise
- idem pour les serveurs hébergeant les applications
- contrôler l'accès aux données
- contrôler l'accès physique au réseau
- protéger les serveurs des attaques
- une clef: cloisonnement et contrôle d'accès
 - VLAN, 802.1X
 - coupe feu

NAC: brassage à la demande

- brassage et activation de ports à la demande
 - éviter les prises libres utilisables
 - coûteux en ressources humaines
 - protection très faible : ne peut rien contre l'utilisation d'une prise utilisée
- contrôle des adresses MAC:
 - affectation d'adresses MAC par ports :
 - le port est coupé si le matériel qui est branché n'a pas l'adresse MAC déclarée
 - fastidieux à gérer :saisie des données, déblocage des ports bloqués par erreur
 - gestion globale des adresse MAC sur l'entreprise
 - facilement contournable (MAC écrite sur les postes, faciles à changer)

•NAC: équipement en coupure



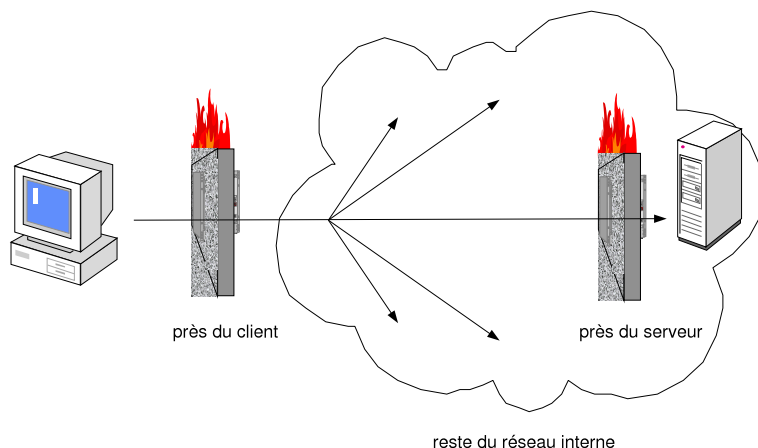
•NAC: positionnement de l'équipement en coupure

- positionnement de l'équipement en coupure:
 - seul ce qui est après l'équipement est protégé
 - ce qui est avant est exposé
 - positionnement proche du client:
 - pour réguler un accès au réseau de l'entreprise
 - de nombreux type de flux vont devoir être autorisés
 - positionnement proche du serveur :
 - pour réguler l'accès à un unique type d'applications
 - permet de filtrer de façon fine le trafic (on sait plus précisément de quoi devra être constitué le trafic)

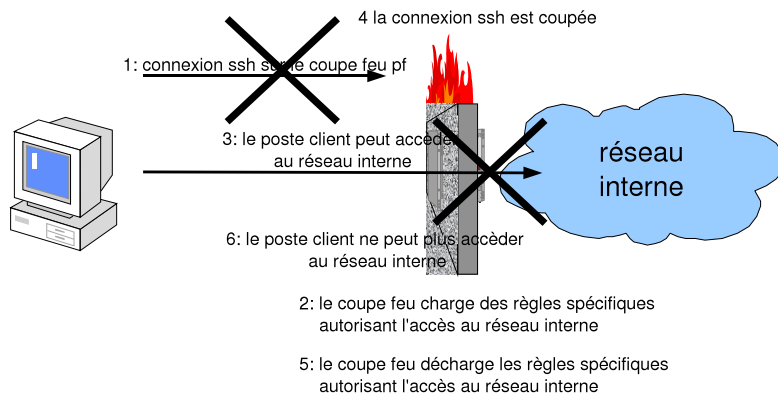
•NAC: Contrôle via un équipement en coupure

- l'accès réseau n'est autorisé qu'après authentification sur un équipement en coupure
 - par une connexion directe sur l'équipement (http, ssh, telnet, ...). Exemple: authpf (OpenBSD, PacketFilter)
 - par une redirection automatique : proxy transparent et portail captif
- succès de l'authentification => chargement de règles de filtrage, de VLAN spécifiques
- méthode « moderne » facilitant une gestion centralisée

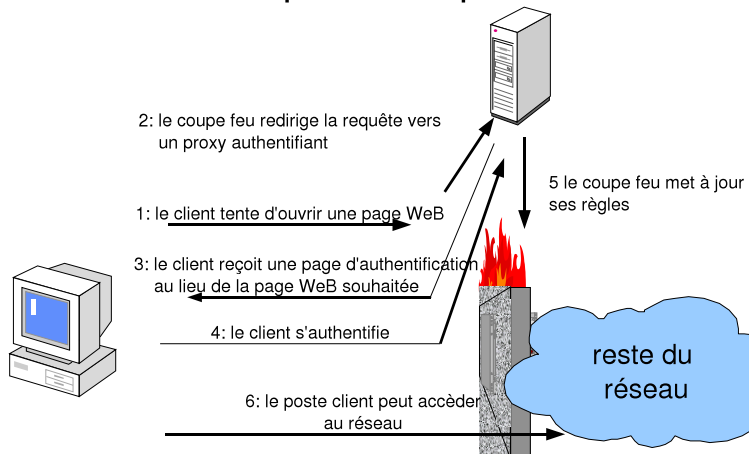
•NAC: positionnement de l'équipement en coupure



•NAC: authPF



•NAC: portail captif WeB



•NAC: Contrôle par un équipement en coupure niv. 3

- Pb: possibilité d'usurpation d'IP, MAC, ... pour emprunter les droits d'une connexion active
 - authentification périodique pour valider la présence du client authentifié
 - portail WeB:
 - la page d'authentification se recharge périodiquement
 - si la page est fermée ou ne se recharge pas, l'accès est coupé au bout d'un temps paramétrable
 - ou utilisation d'un protocole en mode connecté (connexion coupée => perte de l'accès)
 - authpf: coupure de la connexion ssh => coupure immédiate de l'accès (penser à paramétrer le timeout ssh)

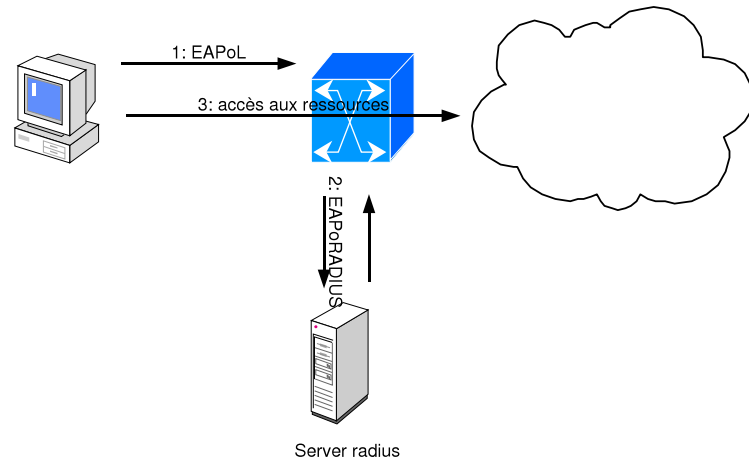
802.1X: contrôle niveau 2

- 3 éléments entrent en jeu :
 - le client (« supplicant ») qui souhaite un accès au réseau
 - le point de contrôle (« authenticator ») à l'entrée du réseau local (commutateur, borne WiFi en général)
 - le serveur d'authentification (« authentication server ») radius

802.1X:

- le port du commutateur ne laisse passer vers le commutateur que les trames EAPoL (EAP encapsulé dans de l'ethernet)
- le commutateur encapsule la requête EAP dans un paquet EAPoRADIUS
- sécurité: pas de communication directe entre client et serveur d'authentification

•NAC: 802.1X, contrôle au niveau 2



802.1X: cinématique

- le client transmet des informations d'authentification et sa posture de sécurité (éléments de conformité)
- le point d'accès valide ces informations avec le serveur radius qui lui retourne éventuellement des éléments de configuration (VLAN , ...)
- en fonction de la réponse obtenue, l'accès est autorisé dans les conditions précisées dans la réponse (notamment le VLAN du client) ou interdit

802.1X: points de mise en oeuvre

- continuité de service: point clef: le serveur radius
- support 802.1X par les équipements réseau, par les postes clients
- impact du choix de la méthode d'authentification EAP:
 - authentification de la machine/de l'utilisateur (quid de l'accès réseau pendant le boot)
 - type d'authentification (certificat, OTP, ...)

802.1X: points de mise en oeuvre

- gestion de périphériques passifs (imprimantes, ...)
- impact sur la facilité d'administration du parc (WakeUpOnLan, ...)
- sécurité de la zone de quarantaine
 - vis à vis du reste du réseau
 - à l'intérieur de la zone (interdire les connexions entre postes)

Divers types de coupes-feux

- terme recouvrant des réalités variées :
 - filtre de paquet
 - coupe feu à état
 - mandataire (proxy applicatif)
 - coupe feu personnel
- agissant à des niveaux variés:
 - couche liaison
 - couche réseau/transport
 - couche application

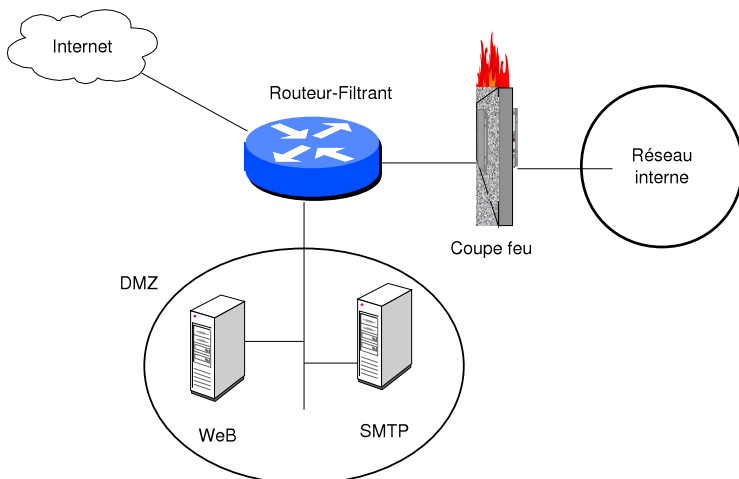
Coupe Feu: généralités

- termes équivalents : parefeu, coupefeu, garde barrière (US: firewall)
- élément d'une politique de sécurité :
 - Buts possibles:
 - protéger les postes internes des attaques, cloisonnement
 - interdire la fuite des données de l'entreprise (cas d'un espion en interne)
 - contrôler les accès réseau des programmes présents sur un poste de travail (firewall perso)
 - Moyens:
 - filtrer/interdire le trafic non autorisé/dangereux,
 - laisser passer le trafic légitime
 - modifier les paquets (NAT, REDIRECT, mandataire transparent, ...)

coupe feu pour sécurité périmétrique

- sécurité périmétrique
- indispensable mais insuffisante contre les ennemis de l'intérieur:
 - WeB, mail, portable ramenés à la maison puis dans l'entreprise, vpn, ...
 - ces accès directs aux postes clients nécessitent des mesures spécifiques pas forcément compatibles avec les demandes des utilisateurs:
 - mandataire WeB avec antivirus & Co
 - relais smtp entrant avec antivirus
 - politique de sécurité stricte sur les portables, sous-réseau dédié en interne, ...

Architecture classique:



Architecture classique:

- machine bastion:
 - machine directement exposée aux attaques
 - ex.: machine ayant une adresse ip publique, serveur smtp entrant, serveur WeB, ...
- dmz
 - zone intermédiaire entre le réseau interne et le réseau externe non maîtrisé
 - contient des machines bastion
 - isole des machines publiques du réseau interne

Architecture classique

- But :
 - limiter/interdire l'accès direct de/vers l'extérieur aux postes/serveurs internes
 - réserver l'accès de/vers l'extérieur à des machines ciblées, surveillées et configurées en conséquence avec la plus petite surface d'attaque possible : les machines bastion
- Limitations:
 - supprime les accès réseau directs
 - mais pas les entrées de contenu malicieux via WeB ou mail (virus & Co)

défense en profondeur

- défense globale et dynamique, coordonnant plusieurs lignes de défense couvrant toute la profondeur du système d'information
- traduction: ceinture et bretelles
 - la sécurité périmétrique seule ne suffit pas
 - l'hétérogénéité des systèmes permet d'éviter la faille qui troue tout (à opposer aux problèmes de compétence des équipes système qui incitent à homogénéiser)
- pour plus d'informations:
<http://www.ssi.gouv.fr/fr/confiance/documents/Methodes/mementodep-v1.1.pdf>

Architecture classique

- quoiqu'insuffisantes, ces architectures avec protection périmétrique ont quand même quasiment fait disparaître les attaques directes
- Elles peuvent être complétées par d'autres mécanismes que nous allons voir maintenant
- A noter que l'amélioration de la qualité de systèmes d'exploitation a largement fait baisser les problèmes d'exploitation directes à distance (cf http://hack.lu/images/4/45/Renaud_Hack_Lu.pdf)

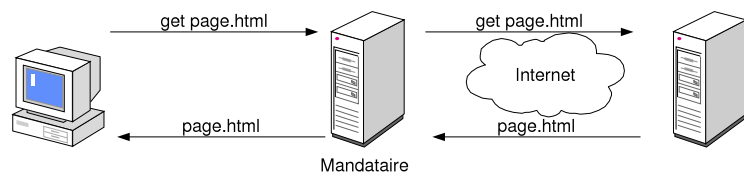
Surface d'attaque

- diminuer la surface d'attaque: les attaques ont souvent lieu par l'exploitation de faille de logiciels
- => limiter les services accessibles sur une machine
 - en désactivant les services inutiles
 - en répartissant les services sur plusieurs machines
- Exemple historique: windows 2000 installé avec le serveur WeB IIS installé et actif

défense en profondeur

- exemples de mesure y participant
 - routeur filtrant ou firewall d'entrée de marque A
 - dmz, firewall d'entrée de l'intranet de marque B
 - blindage des OS, firewall local sur les serveur
 - cloisonnement de l'intranet
 - système de détection d'intrusion
 - antivirus sur les mandataires WeB, smtp entrant
 - antivirus, firewall personnel sur les postes de travail
 - ...

Mandataire (proxy)

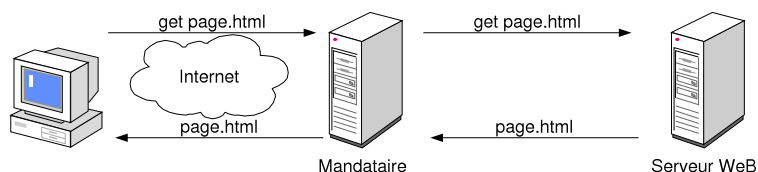


- le mandataire peut effectuer
 - un travail de nettoyage sur les données reçues (antivirus, ...)
 - un filtrage ou un nettoyage sur les données transmises
 - une journalisation des requêtes
 - une demande d'authentification des utilisateurs

Mandataire (proxy)

- permet à un client des connexions indirectes à des serveurs externes
- fonctionnement
 - le client transmet sa requête au mandataire
 - le mandataire interroge le serveur distant
 - le mandataire transmet la réponse au client
- Avantages :
 - travail au niveau application
 - permet du filtrage en entrée (antivirus, ...) et en sortie (interdire certaines requêtes)
 - permet journalisation des requêtes, authentification.
- Cas courants: WeB, SMTP entrant/sortant

Reverse proxy



- le reverse proxy :
 - peut protéger un OS un peu faible des accès directs
 - peut effectuer un filtrage ou un nettoyage sur les requêtes transmises pour palier la faiblesse d'un logiciel serveur WeB
 - peut demander une authentification

proxy variés :

- proxy transparent:
 - proxy couplé avec un firewall qui détourne les requêtes vers le proxy sans que le client le sache
- proxy http / https
 - https est chiffré
 - les proxies https déchiffrent et rechiffrent les données au vol (gare aux problèmes légaux)

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

Organisation

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

Collecte: exemples

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

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>

Collecte d'information

- mode de collecte : synchrone vs asynchrone
- mécanisme de transport
 - 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

- 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

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: 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

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

- 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, ...)

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

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

- 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)

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

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.

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.

Comment réagir à une intrusion

- mesures immédiates à prendre
 - problèmes:
 - soit 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 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

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).

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

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