MEMOIRE

Points à prendre en compte pour la mise en place d'une politique de sécurité en entreprise

LICENCE PROFESSIONNELLE GESTION DES RESEAUX ET SYSTEMES DE TELECOMMUNICATIONS

ANNEE 2006/2007

Jean-Christophe FORTON

UNIVERSITE JOSEPH FOURIER
GRENOBLE 1
SCIENCES.TECHNOLOGIE.SANTÉ

Version : 1.5

SOMMAIRE

1

Introduction

INTRODUCTION

Nous allons aborder, tout au long de ce document, les points à prendre en compte pour mettre en place une politique de sécurité. La politique de sécurité est importante au sein d'une entreprise car elle va permettre de garantir son bon fonctionnement, en analysant les risques auxquels elles s'expose (audit) et en élaborant des contre-mesures venant éviter ces risques.
En sécurité on parle de menace, vulnérabilité, contre-mesure, risque. Avant d'aller plus loin, définissons ces termes.

I) Définitions et contexte

La menace représente l'action de nuire, la vulnérabilité représente le taux d'exposition à une menace et la contre-mesure vient prévenir la menace.
Le risque peut se définir comme une équation de ces trois paramètres :

$$\text{Risque} = \frac{\text{menace} \times \text{vulnérabilité}}{\text{contre-mesure}}$$

Il est important de souligner que la sécurité n'est pas l'affaire d'une personne et que les contre-mesures ne sont pas exclusivement des moyens techniques.
A quoi bon définir une stratégie de mot de passe complexe si les personnes les marquent sur des Post-It collés sur leurs écrans ou sous leurs claviers ?
Il est important de définir des règles à appliquer ainsi qu'une charte informatique résumant toutes les choses interdites, mais la formation et la sensibilisation des personnes utilisant le réseau est très importante. Ces règles à appliquer ne doivent pas être contraignantes, et souvent seule une politique simple, précise et compréhensible est applicable par tout le monde.

Pour sécuriser un système il est primordial de recenser, dans un premier temps, ce qui doit être protégé et son degré de sensibilité. Il faut également identifier les menaces auxquelles il est exposé, pour pouvoir établir une liste d'actions à entreprendre pour le sécuriser.
Pour résumer, la sécurité informatique consiste à vérifier que les logiciels ou données présents au sein d'une entreprise sont utilisés à bon escient et essayera de remplir les cinq objectifs suivants :

- L'intégrité : prévenir la modification des données par des personnes non autorisées,
- la disponibilité : garantir l'accès aux données,
- la confidentialité : prévenir la visualisation des données par des tierces personnes,
- l'authentification : garantir que seules les personnes autorisées ont accès aux données,
- la non répudiation : garantie qu'une transaction ne peut être niée.

Ces cinq objectifs sont remplis aux travers de cinq facettes ou types de sécurité suivants : physique, d'exploitation, logique, applicatives et des télécommunications.

II) Les cinq types de sécurité

La sécurité physique englobe la protection des sources énergétiques, l'environnement d'exploitation, la protection des accès, la sureté de fonctionnement du matériel et les plans de maintenance préventive et corrective.

La sécurité d'exploitation comprend le bon fonctionnement du système, les différents plans de sauvegarde, secours, continuité et test, la gestion du parc informatique, l'analyse des fichiers de logs, la gestion des contrats de maintenance et la séparation des environnements de développement et de production.

La sécurité logique regroupe les mécanismes de sécurité par logiciel, la confidentialité et l'intégrité des données.

La sécurité applicative englobe la robustesse des applications, la sécurité des progiciels, les plans de migrations des applications utilisées en production et les contrats avec les sous-traitants.

La sécurité des télécommunications regroupe la fiabilité et la qualité de la connectivité ainsi que la sécurité de l'infrastructure réseau utilisée.

Nous venons de voir les cinq types de sécurité, nous allons maintenant nous intéresser aux méthodes et moyens qui permettent de les mettre en œuvre.

2

Architecture réseau sécurisée

INTRODUCTION

La sécurité informatique dépend beaucoup de l'architecture réseau qui est employée. Comme nous l'avons vu précédemment, la sécurité d'exploitation suggère une séparation des environnements de production et de développement. Cela est possible grâce a la mise en place de zone démilitarisée.

Les zones démilitarisées permettent en général d'isoler les serveurs des autres machines du réseau. Ces zones isolées sont reliées au reste du réseau par des liens surveillés et souvent filtrés.
Il existe deux principaux types de DMZ : privée et publique.

I) DMZ publique

La DMZ publique sert à isoler des machines accessibles depuis l'Internet. On y retrouve des serveurs de mail, Web, FTP, VPN, etc…
L'objectif est de rendre disponible ces machines sans permettre l'accès au réseau interne depuis l'Internet. Un pare-feu se charge d'effectuer ce blocage en plus de contrôler les connexions qui sont entreprises avec les serveurs.
Voici un exemple de configuration d'une DMZ publique :

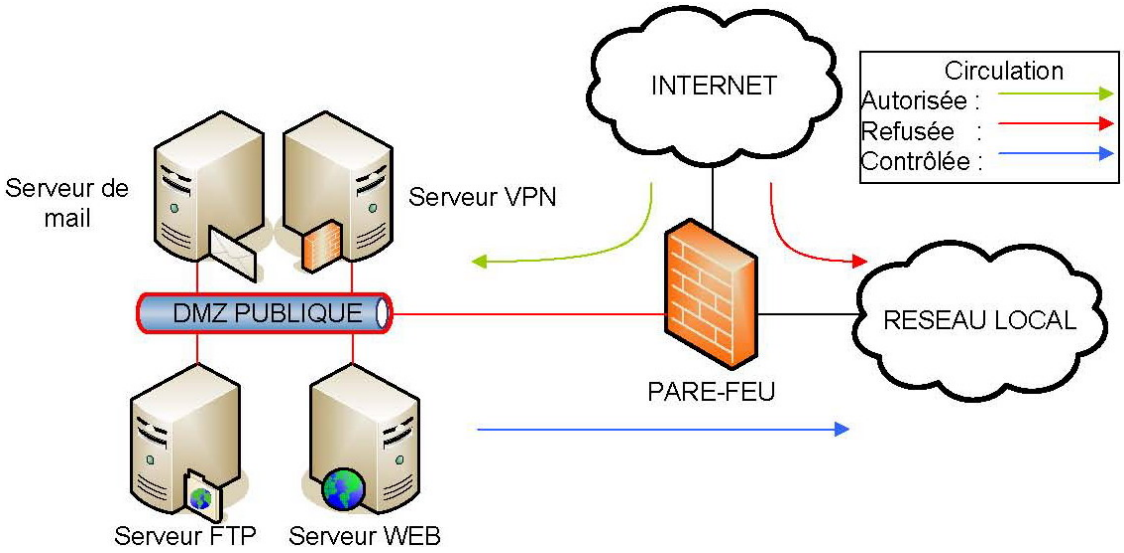

Figure 1.1 : Schéma d'une zone démilitarisée publique

Comme on peut le voir sur le schéma précédent, l'accès de la DMZ publique au réseau local n'est pas complètement interdit mais contrôlé. Prenons comme exemple un serveur Web qui puise des informations dans une base de données. On imagine bien le serveur Web en DMZ publique, mais la base de données qui contient les informations dont on doit garantir l'intégrité, doit être délocalisée dans une zone protégée : la DMZ privée.

II) DMZ privée

La principale fonction de la DMZ privée est de fournir des services, elle peut cependant servir à l'administration du parc informatique. Elle servira, par exemple à fournir un service de résolution de noms (DNS), rendre accessible un partage de fichiers, permettre l'authentification des machines présentes sur le réseau local.
Elle peut fournir aussi des services aux serveurs situés dans la DMZ publique, avec toutefois plus de précaution.

On est en effet, jamais à l'abri d'une attaque pirate sur une machine de la DMZ publique, et fournir un accès total à ces machines constituerait une faille de sécurité. On doit pourtant trouver un compromis et autoriser l'accès, car certains services, comme les bases de données, ne doivent pas se trouver en DMZ publique.
Il y a aussi des services qu'il est préférable de scinder entre DMZ publique et DMZ privée. On peut prendre comme exemple un serveur de mail. Il est plus prudent d'analyser les mails provenant de l'extérieur en DMZ publique, car si l'un deux contenait du code malicieux, il serait exécuté sur le serveur de mail en DMZ publique et ne pourrait nuire au réseau privé. Cependant le cas du serveur de messagerie est épineux et sera abordé plus en détail dans un autre chapitre.
Voici un exemple d'organisation d'une DMZ privée :

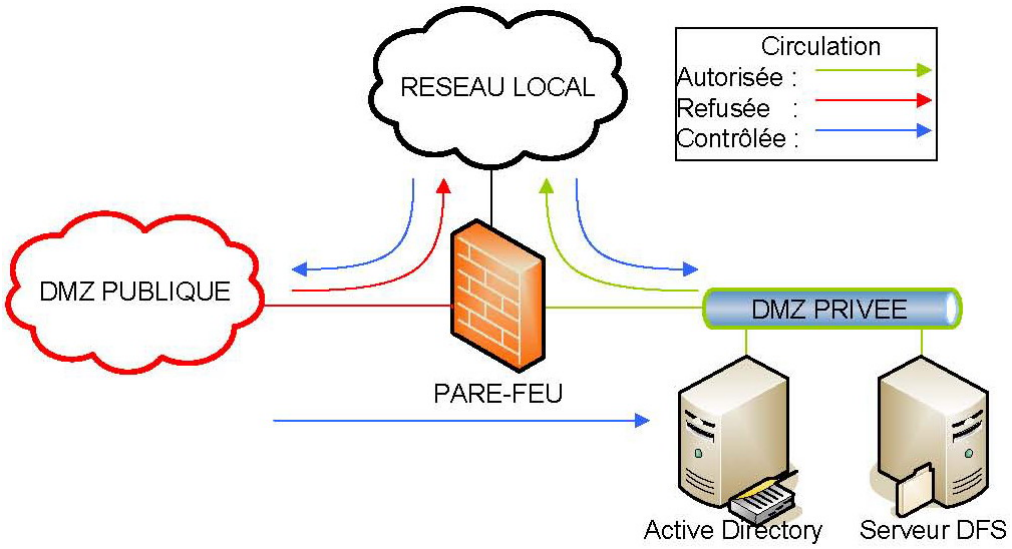

Figure 1.2 : Schéma d'une zone démilitarisée privée

III) Translation d'adresse

La translation d'adresse, sert principalement, à plusieurs ordinateurs possédant des adresses privées de pourvoir accéder à l'Internet en partageant la même adresse publique. Ce mécanisme est assuré par une passerelle qui souvent est intégré aux firewalls ou routeurs. Une des propriétés importantes de la translation d'adresse et qu'elle rend « invisible », du côté Internet, les PC présent sur le réseau privé. En effet, ceux-ci peuvent initier des connexions en direction de l'Internet mais le contraire est impossible. Cela permet de construire un périmètre sécurisé dont la passerelle est la porte.

Nous venons de voir comment les DMZ et le mécanisme de translation d'adresse assuraient une certaine sécurité d'exploitation, penchons nous maintenant sur les matériels utilisés en sécurité.

3

Matériel utilisé en sécurité

I) Pare-feu

C'est l'outil par excellence utilisé en sécurité. Il permet, de par sa fonction filtrante, de contrôler les échanges entre les différentes zones d'un réseau. Dimensionné pour résister à la plupart des attaques connues, il sert de barrière entre une zone de faible confiance et une zone sensible. Utilisé principalement comme tampon entre l'Internet et le réseau local, il peut servir aussi à protéger un sous ensemble de machines.
Souvent doté de système de remonté d'alertes (SNMP), il assure une sécurité d'exploitation ainsi que logiciel en limitant l'utilisation de failles progiciel.

II) Routeur

Le routeur est l'outil qui permet de faire circuler les informations entre plusieurs réseaux. S'il peut réaliser cet aiguillage, c'est grâce à sa table de routage, que souvent, il gère dynamiquement.
Il existe deux principaux protocoles de routage dynamique : RIP et OSPF. L'avantage du routage dynamique est que le routeur fait lui-même les mises à jour de sa table de routage, mais on peut se demander si ces mises à jour sont bonnes.
En effet, on pourrait imaginer un pirate envoyé des paquets OSPF ou RIP, en se faisant passer pour un autre routeur et ainsi modifier la table de routage des routeurs voisins. Il n'aurait alors aucun mal à récupérer tous les paquets qui transitent sur le réseau.
Un moyen de contrer ce genre d'attaque, est l'authentification des échanges entre routeurs. De la sorte, les routeurs ne mettent à jour leur table de routage en se basant uniquement sur les paquets OSPF provenant de routeurs connus.

III) Passerelle

La passerelle sert à router les paquets entre deux parties d'un réseau. Souvent elle utilise un mécanisme de translation d'adresse (PAT ou NAT). Cette translation est possible grâce à l'utilisation des numéros de ports comme identifiants de transaction. Le seul problème auquel elle peut être confrontée, c'est l'envoi massif de paquet reset sur tous les ports, qui aurait pour effet d'effacer la table des transactions en cours. Ainsi tous les échanges qui transitent par la passerelle sont coupés et cette dernière entre en déni de service.
On pourra installer sur la passerelle une sonde, qui permettra l'analyse du trafic transitant par la passerelle. De plus, la sonde permet de palier au problème de non-répudiation grâce à sa fonction d'écoute, et couplée avec un système de prévention d'intrusion elle permet d'éviter des attaques car elle analyse le contenu des paquets échangés. Nous reviendront sur les sondes plus en avant dans ce document.

IV) Storage Area Network (SAN)

La technologie SAN est utilisée pour le stockage des données. Elle utilise de la fibre optique et permet des débits, à l'heure actuelle de plus de 4 Go/s. L'avantage de cette technologie est qu'elle utilise un langage propriétaire (Fiber Channel) qui n'a rien à voir avec IP, ce qui permet d'éviter les problèmes d'écoute clandestine (eavesdropping).
De plus, ce système fiable permet de solutionner les problèmes de disponibilité, de par ses débits élevés, mais permet également de sécuriser les données.
En effet, les constructeurs fournissent généralement ce type de matériel avec des disques fibre optique qui sont plus fiables et supportent les débits élevés, mais utilise également des baies de disques en raid.

V) Redundant Array of Inexpensive Disks (RAID)

Le RAID que nous allons voir, permet d'assurer une sécurité d'exploitation grâce à la redondance. Il existe deux types de RAID utilisés en sécurité : le RAID 1 et 5.

a. Le RAID 1 ou miroitage de disque

Ce RAID permet de faire de *n* disques un seul disque. Cette redondance apporte une certaine tolérance de panne d'un facteur *n-1*. Si cinq disques sont miroités, quatre disques peuvent défaillir sans qu'il y ait perte de données. On a donc ici une tolérance de panne de quatre disques.
Ce type de RAID reste toutefois onéreux, car la capacité de plusieurs disques n'est pas utilisée.

b. Le RAID 5 ou volumes agrégés par bandes à parité répartie

Le RAID 5 permet de créer un volume agrégé par bande, c'est-à-dire de fusionner l'espace disque de plusieurs entités en un seul bloc. Ce n'est pas tout, à cela on ajoute la parité répartie en inscrivant sur une partie de chaque média le résultat du OU exclusif des autres médias, comme montré ci-dessous :

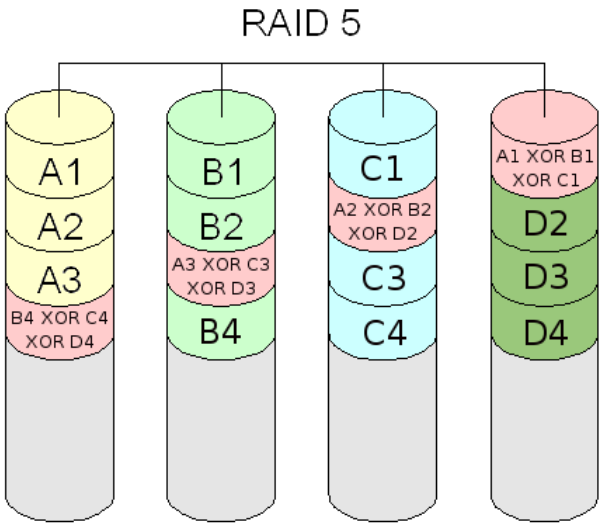

Figure 3.1 : Le mécanisme du RAID 5

Ce type de RAID est moins couteux que le RAID 1, cependant il faut savoir que les performances en écriture sont plus faibles à cause du calcul de parité qui prend du temps, mais en lecture les performances sont *n-1* fois plus grandes. La tolérance de panne est de 1 disque mais des disques dormants (spare) peuvent être ajoutés pour augmenter cette tolérance. Leur rôle est de prendre le relai lorsqu'un disque vient à défaillir.

VI) Onduleurs

Les onduleurs sont des batteries qui permettent de continuer la distribution de courant, pendant une certaine période, après une coupure de courant.
Ils peuvent être redondés ou épaulés par un groupe électrogène, dans ce cas, il peuvent laisser le temps au groupe électrogène de démarrer.

4

Sécurité des réseaux sans fil

INTRODUCTION

Les réseaux sans fil nécessitent une attention toute particulière du fait de leur mode de propagation. Ils viennent généralement s'ajouter à un réseau filaire déjà existant, lui octroyant un minimum de flexibilité mais, du même coup, le rendant accessible à des personnes non autorisées. Il est nécessaire de se poser au préalable quelques questions pour pouvoir les déployer en minimisant les risques.

I) Analyse des utilisateurs

Une analyse des utilisateurs doit être menée pour déterminer l'utilisation qui va être faite du réseau. On doit se demander si ces utilisateurs sont de confiances ont non ? S'ils ont besoin d'accéder aux données de l'entreprise ? Si le matériel qu'il utilise pour se connecter au réseau leur appartient ou s'il est sous contrôle de l'entreprise ?
Toutes ces questions permettent de déterminer la manière d'intégrer le réseau sans fil dans l'architecture existante.

II) Intégration des réseaux sans fil

L'intégration du réseau sans fil doit se faire en fonction des services qu'il va fournir. S'il à besoin de fournir des informations de l'entreprise, il doit être relié au réseau interne de l'entreprise. S'il sert juste à fournir une connexion à l'Internet, il doit être isolé du réseau interne. Le réseau sans fil pourrait également servir à relier deux réseaux internes sécurisés grâce à une connexion point à point.
Etudions maintenant l'intégration du réseau sans fil dans le cas ou il est intégré au réseau interne et dans celui ou il ne l'est pas.

a) Intégration au réseau de l'entreprise

Lorsque le réseau sans fil a besoin d'être raccordé, l'utilisation de Vlans est recommandée. Les Vlans reprennent le principe des SSID, en permettant une séparation entre des groupes d'utilisateurs. Ici, le paramètre de séparation va être l'authentification. Si celle-ci réussi, l'utilisateur est reconnu comme une personne de confiance et intègre un Vlan qui lui permettra l'accès aux données de l'entreprise. En revanche, si l'authentification échoue, l'utilisateur ira rejoindre un Vlan « bac à sable » où il sera isolé du reste du réseau filaire.
L'intégration des réseaux sans fil nécessite d'avoir des matériels qui gèrent les Vlans. Du côté filaire on pourra utiliser un Switch manageable ou un router (dans le cas d'une connexion point à point), côté sans fil on utilisera un point d'accès ou un bridge.

Voici un exemple d'intégration dans le cas ou un point d'accès est utilisé :

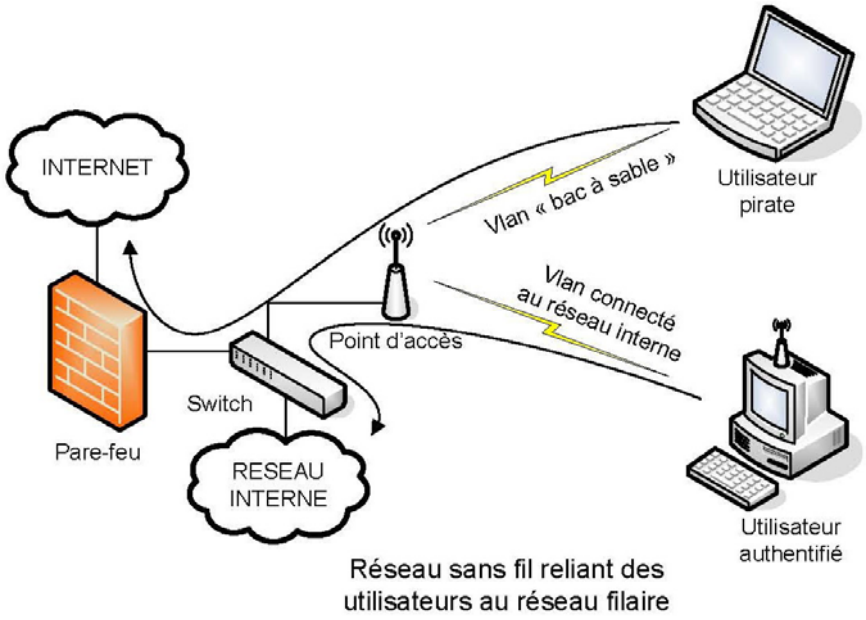

Figure 4.1 : Réseau utilisant un point d'accès

On peut remarquer, dans le schéma ci-dessus, que le pirate (utilisateur non authentifié) a accès à l'Internet. On aurait très bien pu lui interdire toute forme de circulation et l'isoler dans un sous réseau à part.
Observons maintenant la différence avec un réseau utilisant des bridges pour une connexion point à point :

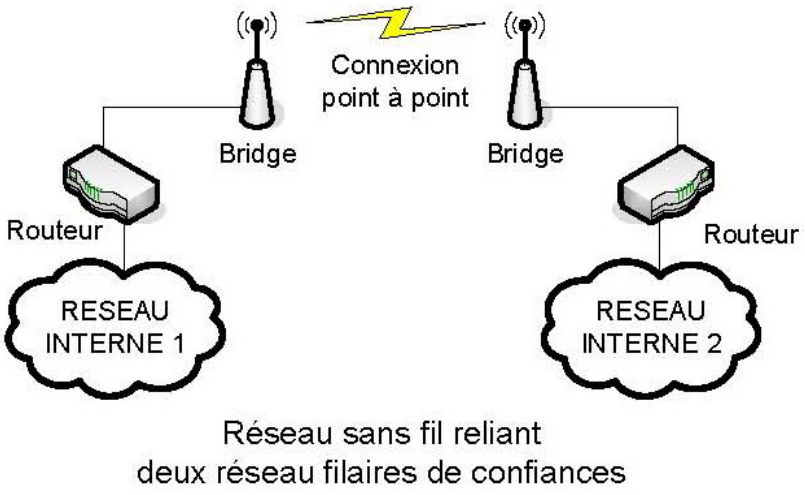

Figure 4.2 : Interconnexion sans fil point à point

Dans le cas ci-dessus, on relie deux bâtiments entre eux, c'est généralement le cas quand une entreprise étend ses locaux de l'autre côté d'une route. Ce sont deux sous réseaux qui font en réalité partie d'un même ensemble.

Maintenant que nous avons observé l'intégration des réseaux sans fil intégré au réseau d'entreprise, étudions ceux qui ne le sont pas.

b) Réseau sans fil non relié

Dans le cas d'un réseau sans fil n'ont relié au réseau interne de l'entreprise, offrant seulement une connexion à l'Internet comme les Hotsopts, on choisira une architecture proche de celle utilisant le point d'accès vu ci-dessus. Les clients se connectent au point d'accès avec ou sans authentification, cela dépend si un système de tarification est mit en place, le point d'accès étant directement relier à l'Internet par le biais d'un routeur.

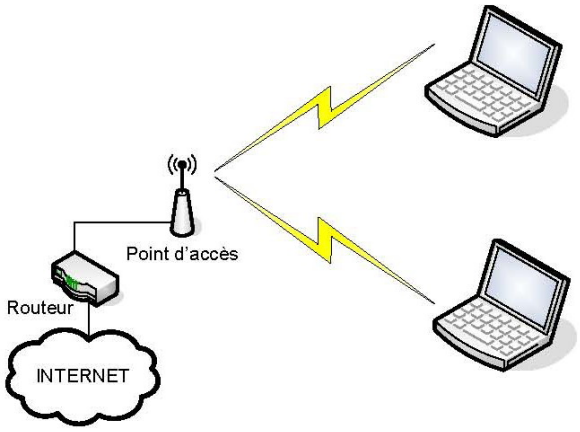

Figure 4.2 : Réseau relié directement à l'Internet

Maintenant que nous avons vu les différentes façons d'intégrer un réseau sans fil, attardons nous sur les moyens d'authentifier les utilisateurs.

III) Authentification

L'authentification est très importante dans les réseaux sans fil, car elle permet de s'assurer que seuls les utilisateurs approuvés sont connectés. Elle peut avoir lieu de plusieurs façons, en utilisant un serveur d'authentification (RADIUS), en configurant le filtrage d'adresse MAC sur le point d'accès, en utilisant une phrase (PSK).

Le filtrage par adresse MAC est à éviter, car ce dernier peut être facilement déjoué. Il suffit à un pirate d'écouter le réseau est de repérer les adresses autorisées, il n'a plus alors qu'à modifier son adresse MAC : cette technique s'appelle le spoofing.

Une manière de s'authentifier de façon sécurisée est d'utiliser un serveur d'authentification, voire, si peu d'utilisateurs ont besoin de se connecter, une phrase secrète.
L'avantage du serveur d'authentification est qu'il peut être couplé à une base de données contenant les comptes des utilisateurs approuvés. De plus, l'authentification est beaucoup plus forte avec le serveur, car celui-ci peut utiliser un certificat pour créer un tunnel crypté avec l'utilisateur (PEAP). Une fois le tunnel créé, une simple authentification par login / mot de passe est possible. C'est la solution qui est majoritairement déployée car elle ne nécessite aucune configuration particulière sur le poste client.
Une solution plus lourde, qui nécessite l'installation d'un certificat sur le poste client, est possible (EAP-TLS). On peut voir un inconvénient à ce genre d'authentification, c'est qu'elle ne nécessite que la présence du certificat. On pourrait imaginer qu'un pirate vole un portable contenant le certificat, il pourrait alors se connecter sans problème au réseau sans fil.
C'est pourquoi on privilégiera cette dernière solution, pour la connexion de postes fixes plutôt que de portables.

IV) Cryptage de la liaison radio

Le cryptage de la liaison est tout aussi important que l'authentification car il permet de garantir l'intégrité ainsi que la confidentialité des échanges.
Il existe plusieurs méthodes de chiffrements, certaines sont dépassées, d'autres plus récentes, sont assez robustes.

a) Wired Equivalent Privacy

Commençons par parler du cryptage WEP. Il est clair que cette méthode de chiffrement, utilisée seule, est complètement obsolète. La seule raison valable de l'utiliser est pour des raisons de compatibilité avec du vieux matériel. Même avec une rotation de clé fréquente, le cryptage WEP est à proscrire.

b) WEP (128 bit) + TKIP = WPA

Le WEP a connu une seconde jeunesse, lorsque l'IEEE à développer le chiffrement TKIP (Temporal Key Integrity Protocol) dans le cadre de la norme 802.11i. L'avantage de ce chiffrement est qu'il ne requiert pas le changement du matériel qui est compatible avec la WEP. Avec l'arrivé du chiffrement TKIP, la sécurité des réseaux sans fil devient une réalité et le WPA s'impose comme la référence en matière de cryptage.

c) Advanced Encryption Standard

L'AES a été élu en 2003, protocole de chiffrement assez fort pour crypter des données de niveau « TOP SECRET », selon la NSA. Ce protocole est venu remplacer le vieillissant DES, Data Encryption Standard, élaboré par la NSA même en 1976. L'AES est un algorithme symétrique qui n'a pour le moment pas été encore cassé.
Je me permets d'émettre quelques réservations quant à l'utilisation de cet algorithme en wifi, car pour le moment, à chaque fois que je l'ai essayé, la qualité de la liaison radio a baissé, que ce soit sur du matériel D-Link ou Cisco, l'expérience a été négative. Dans le meilleur des cas le débit diminuait, dans le pire la liaison radio ne fonctionnait plus.

d) Connexion VPN

On n'y pense pas souvent, mais la connexion VPN peut être un bon moyen de crypter une connexion wifi et cela sans se soucier des équipements radio utilisés. En effet, le cryptage se fait au niveau de la couche trois entre les deux extrémités distantes. Cela peut être un avantage si le matériel est ancien et ne gère que le cryptage WEP, sinon c'est assez contraignant d'avoir à lancer une connexion VPN pour se connecter à un réseau sans fil. Cela nécessite l'installation de logiciels supplémentaires, souvent propriétaires, sur les postes clients et par conséquent cette solution est lourde à déployer sur beaucoup de machines.

Tous les cryptages vus précédemment donnent cependant un faux sentiment de sécurité. En effet, s'ils sont utilisés sur des postes clients non sécurisés à l'aide de pare-feu, un pirate pourrait s'introduire sur un poste authentifié et ainsi rebondir dans le tunnel crypté.

Maintenant que nous avons étudié l'intégration, les moyens d'authentification et de cryptage utilisés dans les réseaux sans fil, intéressons nous à la sécurisation des services.

5

Sécurisation des services

INTRODICTION

La sécurisation des services comprend leur bon fonctionnement, mais également que seules les personnes autorisées y ont accès. Il n'est peut-être pas grave qu'une personne accède à un service DNS, mais qu'en est-il si elle a accès à un service DFS, elle sera certainement tentée de lire des informations, voire de les modifier.
Ce chapitre se propose donc de lister quelques points à vérifier sur les différents services.

I) Messagerie

Le serveur de mail est assez délicat à sécuriser du fait qu'il permet une communication directe avec des personnes externes à l'entreprise. Il est possible, par le biais de pièces jointes, de faire circuler du code malicieux qui s'exécutera alors sur le réseau interne.
On peut palier à se genre de problème en scindant le service mail en deux serveurs : un présent en DMZ publique, l'autre en DMZ privée. Les mails qui arrivent de l'extérieur sont reçus par le serveur présent en DMZ publique qui les analyse. Si les mails sont exempts de tout code malicieux, alors ils sont forwarder au serveur présent en DMZ privée. On pourrait imaginer en DMZ publique, en plus de l'analyse antivirus, une analyse anti-spam qui met à jour une blacklist des domaines spammeur.

Pour envoyer du courrier vers l'extérieur, c'est le mécanisme inverse. Le serveur interne envois son mail au serveur présent en DMZ publique qui, après analyse, l'envoie aux différents destinataires.

L'autre problème des serveurs de mail est qu'ils ont une option relai, qui leur permet de relayer du mail, quelque soit sa provenance. Cette option est utilisée par les spammeur pour envoyer du spam par l'intermédiaire d'un autre domaine que le leur. Cela leur permet de ne pas se faire blacklister car c'est le serveur relai qui va l'être. Il faut donc bien vérifier que l'option relai est désactivée, surtout sur les serveurs présents en DMZ publique.

II) Fichier / FTP

Pas de faille de sécurité à proprement parler à part une bonne configuration des partages.
Il ne faut pas oublier de mettre des quotas pour l'espace disque, cela évite que les utilisateurs accumulent des giga octets de données et cela les forcent à faire le tri. De plus il faut bien contrôler les droits de chacun, afin d'éviter des accès non autorisés.

Pour ce qui est du serveur FTP, s'il est présent en DMZ publique, il faut bien contrôler ses droit en écriture. En effet, celui-ci pourrait servir d'espace de stockage en ligne pour toute sorte de contenu pirate.

III) DNS

Le DNS permet de transformer un nom en une adresse IP et c'est pourquoi il faut sécuriser ses mises à jour. Quelqu'un de mal intentionné pourrait lui envoyer de fausses informations et ainsi détourner un flux sans problème. S'il est en mode itératif cela ne pose pas de problèmes, car il va interroger les serveurs racine, cela s'applique seulement s'il est redirecteur. Il faut que le serveur vers lequel il redirige soit de confiance.
Une bonne configuration est de scinder le service DNS en deux serveurs : un serveur itératif en DMZ publique et un redirecteur en DMZ privée. Au début le serveur redirecteur va questionner souvent le serveur itératif mais à la fin il ne va pas se construire une base

de nom fiable. De plus le serveur en DMZ publique permet de faire de la résolution inverse pour les personnes qui désirent se connecter à des machines internes.

IV) DHCP

Le service DHCP permet de fournir une configuration IP aux clients qui le demandent. Ce protocole, de par sa compatibilité avec son ancêtre BOOTP, n'est pas très sécurisé et envoie tout en broadcast. C'est pourquoi les attaques par déni de service sont très simples et vont paralyser le réseau en épuisant le stock d'adresses IP disponibles. Pour comprendre dans les détails la composition de l'attaque, vous pouvez aller voir en annexe, le lien vers un document PDF qui explique chaque détail de l'attaque et se termine par la mise en place d'un serveur DHCP pirate.
Une des parades qui a été trouvée par la NSA, est la méthode 80/20. Cette méthode consiste à avoir deux serveurs DHCP, un qui détient 80% des adresses disponibles sur le réseau et l'autre qui n'en détient que 20%. Cela permet de ne faire entrer en déni de service qu'un seul des serveurs DHCP (voir document de la NSA en annexe).

V) Active Directory

Active Directory est un annuaire qui permet de fournir une authentification par login / mot de passe. L'objectif, lorsqu'un tel serveur est installé sur le réseau, est d'essayer de centraliser tous les comptes sur un même serveur. Cela évite de se compliquer la tâche à dupliquer les comptes et lorsqu'une mise à jour est faite elle n'est faite qu'à un seul endroit. Je pense notamment à la suppression du compte d'un employé qui a été licencié. Si son compte est retiré de l'annuaire mais qu'il est toujours présent dans les comptes VPN du firewall, celui-ci pourra toujours se connecter sur le réseau de l'entreprise.

Un autre détail à prendre en compte, c'est la définition du mot de passe administrateur. Certaines personnes ne définissent pas de mot de passe administrateur pour, tout simplement, ne pas être dérangées lors de l'ouverture de session. Cela représente une faille important, surtout si la personne possède beaucoup de droits sur le réseau.

VI) Security Configuration Wizard

Le SCW est un assistant qui permet de centraliser la gestion de la sécurité sur une machine qui utilise Windows 2003 Server. Cet assistant va analyser les rôles du serveur sur lequel il s'exécute pour ensuite modifier la configuration des services ainsi que la base de registre qu'il modifiera en conséquence. L'exécution de cet assistant est plus que recommandé par Microsoft dans son ouvrage *Windows Server 2003 Security Guide*.

6

Sécurisation des clients

I) Contrôle des logiciels installés

Quand on parle de sécurité, on est obligé de parler de contrôle des postes clients. C'est souvent ces derniers qui sont sujets aux attaques. Que ce soit des virus circulant sur disquettes ou clé USB, ou même des chevaux de Troie qui s'installent par le biais d'applications douteuses, les postes clients restent la cible privilégié des pirates.
On a déjà vu des postes clients émettre du spam suite à l'installation d'un logiciel récupéré sur Internet, et dans ce cas c'est souvent la responsabilité de l'administrateur qui est mise en cause.
En effet, que faire si le serveur de mail de l'entreprise est blacklister suite à l'installation d'un logiciel vérolé, qui est responsable ? Est-ce l'administrateur réseau ou le client qui à installé le logiciel ?
Dans ce cas, le fait d'être blacklister n'est encore pas trop grave, mais imaginons que plusieurs postes aient installé le programme vérolé et qu'ils deviennent des zombies. Ces postes se mettraient alors à attaquer le site Web d'une banque et dans ce cas le préjudice causé serait plus important.
On voit que la sécurité n'est pas l'affaire d'une personne mais bien un travail de sensibilisation. On ne peut décemment pas interdire toute installation de logiciel, il ne faut pas étouffer l'utilisateur, mais on ne peut pas le laisser infecter tout le réseau, c'est pourquoi l'administrateur doit déployer une série de logiciels de sécurité sur tous les postes clients.

II) Installation des logiciels de sécurité

On peut dénombrer trois types de logiciels de sécurité : les antivirus, les antis spam, les firewalls.

d) Les antivirus

Les antivirus permettent de contrer les infections virales. Pour être efficaces, ils doivent être mis à jour régulièrement avec les dernières définitions de virus. Des antivirus « version entreprise » sont intéressants pour le déploiement de masse et il existe deux solutions.
La première est la solution *msi*, celle que Norton a choisi. L'administrateur doit simplement créer une stratégie de groupe dans laquelle il spécifie l'installation de l'antivirus. Toutes les machines installeront l'antivirus au prochain démarrage.
La deuxième solution est l'installation web. L'utilisateur se rend sur un site Web, installé généralement sur la même machine que l'antivirus, et n'a plus qu'à se laisser guider par l'assistant en ligne. Cette deuxième méthode requiert souvent l'acceptation de contrôle ActiveX qui peut dérouter l'utilisateur inexpérimenté.
Les antivirus « entreprise » possèdent une console d'administration depuis laquelle il est possible de lancer les mises à jours sur les postes clients, obtenir des statistiques sur les postes les plus infectés, et l'avantage de se système est que la mise à jour depuis l'Internet n'est réalisée qu'une seule fois par le serveur.

e) Les antis spam

Les antis spam préviennent l'introduction de codes malicieux sur la machine. Ils servent également lors de la navigation Internet en bloquant des pages qui exécuteraient des programmes douteux. Ils viennent en supplément de l'antivirus, pour étoffer la protection du poste client.

f) Les firewalls

Les firewalls sur les postes clients ne servent pas ou peu à bloquer les attaques qui arrivent de l'Internet, car celles-ci sont déjà arrêtées par le pare-feu présent en tête de réseau, mais servent à empêcher les clients d'avoir des comportements inhabituels. Comme par exemple envoyer des mails directement vers l'Internet sans passer par le serveur de mail de l'entreprise (spam). On voit souvent le pare-feu comme une barrière qui nous protégerait de l'Internet, mais il sert aussi à filtrer nos échanges avec l'Internet. Des logs peuvent être mis en place, grâce au pare-feu, puis consulté pour vérifier qu'aucun comportement inhabituel n'est arrivé sur le réseau.

7

Logiciels, protocoles et services utilisés en sécurité

I) Contrôle des clients et des serveurs

a) Nagios

Nagios permet un contrôle sur l'ensemble du parc de serveurs. En plus de tester la connexion aux différents serveurs, il contrôle que les services s'exécutent bien sur les machines. Il permet également de visualiser le trafic réseau qui se déroule sur un lien, précis. Pour finir, il peut être paramétré pour envoyer des mails selon des d'alertes prédéfinies.

b) OCS Inventory NG

OCS Inventory NG permet, quant à lui, de contrôler les postes clients de manière simplifiée. Une fois installé sur un poste client, il permet la visualisation de la configuration de cette machine. Des programmes installés sur le système en passant par les mises à jour de sécurité (service pack) ainsi que la version du système d'exploitation et même la configuration hardware, OCS Inventory NG permet un contrôle assez poussé du client. Une autre fonctionnalité intéressante de ce programme, il permet la gestion des licences.

II) Remontée d'alerte et logs

a) SNMP

Simple Network Management Protocol, permet la gestion des équipements réseau, mais également la remontée d'alertes. Ce protocole est supporté par tous les routeurs, switchs, point d'accès et firewalls utilisés en entreprise.
L'administrateur, en utilisant des logiciels comme Kiwi Syslog Daemon ou encore Monitor Magic, peut stocker tous ces logs dans une base de données.
Le plus dur sera de paramétrer l'équipement pour qu'il n'envoie pas de logs à tout va.

b) Snort

Snort est une sonde que j'ai utilisé en projet. Elle permet en plus de garder une trace de l'activité réseau comme le SNMP, de prendre des décisions par le biais de scénarii. Ces scénarii peuvent avoir comme paramètres l'activité processeur, l'occupation mémoire, une activité réseau particulière, etc...
La sonde est généralement installée sur un ordinateur exposé à des attaques ou bien sur un ordinateur qui assume le rôle de routeur. Dans ce dernier cas, elle pourra enregistrer l'activité réseau pour prouver a postériori qu'une transaction s'est bien déroulée (non répudiation).

III) Authentification des personnes et des matériels

a) Remote Authentication Dial-In User Service (Radius)

Le serveur Radius permet l'authentification des personnes ainsi que des machines. Il peut être couplé avec une base de données de type annuaire comme Active Directory ou LDAP mais également avec une base de données comme MySQL. Il permet, en plus de l'authentification, de faire de la comptabilité (accounting). On peut ainsi savoir qui s'est connecté, où et pendant combien de temps.
Le serveur radius reçoit les requêtes des matériels qui sont enregistrés comme clients radius et seulement ceux-ci. Cela permet de contrer l'installation de matériels non autorisés comme les point d'accès voyous.

b) TACAS +

Le TACAS + est la version du protocole Radius de chez Cisco. Elle permet de gérer, comme le radius, la fonction d'authentification et de comptabilité. La seul différence qu'il existe entre TACAS et Radius et que le premier utilise TCP, alors que le second utilise UDP. En revanche, là où Radius gère des méthodes d'authentifications EAP complexes comme le TLS ou PEAP, TACAS ne gère que l'authentification par empreinte md5 (login / mot de passe). On préférera l'authentification Radius à celle TACAS.

8

Reprise sur désastre

INTRODUCTION

La reprise sur désastre est délicate, que ce soit après une catastrophe naturelle, ou après un virus. Dans les deux cas l'entreprise doit retrouver ses données pour reprendre une activité. Nous allons étudier divers moyens qui permettent d'arriver à une reprise d'activité rapide (2 à 3 jours).

I) Réplication site distant

La réplication sur site distant permet un redémarrage d'activité instantanée car les donnes sont constamment actualisées et le site distant contient généralement les même machines que sur le site principal. Ce type de réplication coûte très cher et nécessite la pose de fibre optique entre les deux sites. De plus, comme les sites doivent être éloignés de plusieurs kilomètres, les frais de génie civil sont souvent prohibitifs.
Nous allons nous intéresser à d'autres moyens qui permettent également la reprise sur désastre.

II) Ghost

Le logiciel Ghost, régulièrement utilisé en TP, permet de sauvegarder une configuration fonctionnelle d'une machine. Ce type de sauvegarde peut être effectué avant le changement de version d'un logiciel. La restauration est très rapide et se fait généralement en moins de cinq minutes.

III) Robot de sauvegarde

Les robots de sauvegarde permettent la sauvegarde des données de l'entreprise sur bandes. Les bandes, qui ont généralement une capacité de 400 Go, peuvent ensuite être exportées sur un site distant.

IV) Analyse post-mortem

L'analyse post-mortem n'a de sens que si l'origine du désastre est un virus. Il est nécessaire, après ce genre de désastre, de mener une enquête pour déterminer l'origine du dysfonctionnement qui à permis l'intrusion du virus.

9

Annexes

Ces annexes sont organisées par thèmes, les thèmes pouvant être des protocoles, nom de programmes, service, etc…

I) Webographie

SNORT : www.snort.org (Site de Snort sous Linux)

WINSNORT : www.winsnort.com (Site de Snort sous Windows)

DHCP : http://masterim.univ-lyon1.fr/assodessim/modules/archives/downloads/rapportDHCP.pdf (Document résumant les failles du protocole DHCP)

Sur tous les sujets, le site http://www.commentcamarche.net/, permet de se faire une idée sur ce que l'on cherche.

II) Bibliographie

Windows 2003 Serveur :

- *Windows Server 2003 Security Guide Version 2.0*
  Ecrit par Microsoft au department:
  Microsoft Solutions for Security and Compliance
- *Windows Server 2003. Entraînez-vous à planifier et optimiser une infrastructure réseau*
  Aux éditions ENI
- *Windows Server 2003 en 2 Volumes. Maîtrisez Active Directory*
  Aux éditions ENI
- *Active Directory. Sous Windows Server 2003 DNS, OUs, délégations … Stratégies de groupe*
  Aux éditions ENI

Windows XP :

- *Guide to Securing Microsoft Windows XP*
  Ecrit par la *NSA* au department:
  Operational Network Evaluations Division of the Systems and Network Attack Center (SNAC)
- Windows XP Security Guide
  Ecrit par Microsoft au département:
  Microsoft Solutions for Security and Compliance

Wifi :

- *Wifi déploiement et sécurité. la QoS et le WPA, 2e édition*
  Aux éditions DUNOD
- *802.11 Réseaux sans fil. La référence, 2e édition*
  Aux éditions O'REILLY

VPN :

- *Les VPN. Principes, conception et déploiement des réseaux privés virtuels, 2e édition*
  Aux éditions DUNOD

DNS :

- *DNS. Concepts, architecture et administration sous Windows Server 2003*
  Aux éditions ENI

Snort :

- *Sécurité réseau avec Snort et les IDS*
  Aux éditions O'REILLY

Linux :

- Administration système et réseau
  Aux éditions DUNOD

Réseaux en général :

- Réseaux 4e édition d'Andrew Tanenbaum
  Aux éditions PEARSON EDUCATION