RECOMMANDATION

SECURITE INTRANET

Octobre 1998

Commission Réseaux et Systèmes Ouverts

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANCAIS
30, Rue Pierre Sémard – 75009 Paris
Tel : 01 53 25 08 80 - Fax : 01 53 25 08 88

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Bernard	**CAUBERE**	**CLUSIR Rhône Alpes**
Philippe	**CONVERSIN**	**Dassault Electronique**
Michèle	**COPITET**	
Jean-François	**GONEL**	**AFP**
Thomas	**HUTIN**	**ENST**
Franck	**PAPAVOINE**	**GIE Sesam Vitale**
Lazaro	**PEJSACHOWICZ**	**Bull**
Paul	**RICHY**	**France Telecom**
Mohamed	**SALAH**	**ENST**
Hervé	**SCHAUER**	**Hervé Schauer Consultants**

TABLE DES MATIERES

1. INTRODUCTION

1.1 Préambule

Ce document s'adresse aux RSSI des entreprises ou à des responsables informatiques ou des responsables d'applications. Les concepts véhiculés exigent une connaissance préalable des grandes fonctionnalités des télécommunications, plus précisément des protocoles et services offerts par INTERNET.

Ce document ne prétend pas être exhaustif. Il présente de façon pragmatique et concrète les principales et plus fréquentes vulnérabilités d'un INTRANET ainsi que les moyens les plus usités pour y remédier. Son but est également de monter qu'un INTRANET, malgré son caractère intra-entreprise, doit faire l'objet d'un conception, d'une organisation et d'une administrations sérieuses et réfléchies.

1.2 Définition

*Un IN**TRA**NET est un réseau informatique interne utilisé au sein d' un organisme et utilisant les services et caractéristiques de l'IN**TER**NET.*

Les services INTERNET pris en compte dans notre étude incluent les applicatifs suivants :

1. messagerie (SMTP),
2. serveur WEB (HTTP),
3. connexion à distance (TELNET),
4. transfert de fichiers (FTP),

forum de discussion, newsgroup (NNTP).

1.3 Motivations

A ce titre, il met à la disposition des utilisateurs internes les ressources d'information de l'organisme auquel ils appartiennent selon leurs rôles et prérogatives.

Les motivations à la généralisation des INTRANET sont généralement :

1. l'économie considérable par rapport aux autres techniques de réseau,
2. la facilité de déploiement,
3. le recours aux standards les plus largement diffusés actuellement et permettant de résoudre les problèmes d'hétérogénéité en facilitant la communication,
4. l'ouverture vers l'**EXTRA**NET,
5. l'ouverture vers l'**INTER**NET,

6. un phénomène de masse dépassant un simple effet de mode.

1.4 Mise en œuvre

En terme de sécurité, un organisme préparant son INTRANET aura donc à concilier objectivement les héritages spécifiques et antagonistes, chacun avec ses forces et ses faiblesses, des réseaux internes privés traditionnels et des réseaux IP ouverts.

Les réseaux internes traditionnels étaient caractérisés par :

- une administration structurée,
- un environnement de confiance.

Du monde INTERNET, les réseaux INTRANET héritent des aspects suivants :

- technologie IP ouverte,
- population considérable d'internautes susceptibles d'intervenir,
- vulnérabilité de l'ouverture aux accès externes potentiellement hostiles,
- environnement socio-économique de suspicion.

Dans ce type d'environnement, comme pour tous les autres, les règles caractérisant la sécurité des systèmes d'information doivent être mises en œuvre. Afin de protéger le système d'information contre les menaces, il est nécessaire d'établir une démarche préliminaire d'analyse des risques basée sur la valeur de cette information. Ensuite il convient d'adopter des solutions techniques adaptées associées à des procédures, impliquant l'entreprise sur le long terme, permettant de contrôler l'efficacité de ces mesures et les attaques effectuées inévitablement dès que cette valeur de l'information est importante.

Il est donc nécessaire de rappeler que la technique seule n'est pas suffisante et peut au contraire apporter une illusion de sécurité si aucun contrôle ne lui est associé.

Il ne faut pas oublier non plus, les parades nécessaires à tout réseau interne d'entreprise quel qu'en soit le contexte, par exemple une politique d'anti-virus doit être prise en compte dans un INTRANET.

Néanmoins certains risques sont plus intimement liés à la notion d'INTRANET dans la mesure où il induit, avec le groupware et le workflow, une destructuration des organisations et des sources d'information de l'entreprise. Aussi est il très important avant toute mise en oeuvre d'un INTRANET que l'entreprise fasse une étude préalable précise de communication, d'organisation voire de management.

(**NOTA:** Par extension et pour simplifier, le terme RISQUE a été employé dans la suite du document. Pour être complètement puriste, il est certain que nous étudions les VULNERABILITES intrinsèques de l'INTRANET dans ce document, les risques associés dépendant du contexte de chaque entreprise.)

2. LA PUBLICATION ET LA DIFFUSION D'INFORMATION

Les services pris en compte dans ce chapitre sont: HTTP et FTP.

2.1 Introduction

2.1.1 Pour HTTP

Dans cette partie on s'intéresse aux aspects sécurité liés à la publication de l'information et à sa distribution sur le réseau interne : l'INTRANET.

Le problème de la sécurité de l'INTRANET est, à plus d'un titre, similaire au problème de la sécurité sur l'INTERNET.

L'INTRANET et l'INTERNET s'appuient tous les deux sur le concept Client-Serveur. D'un coté, on a les applications clientes (butineurs), et de l'autre côté des serveurs de fichiers (Serveur de pages HTML, serveurs de messageries...).

Contrairement à une idée largement répandue, HTTP n'est pas simplement un afficheur de pages HTML, mais il est également capable de transférer d'autres formats via le browser, qui s'enregistrent néanmoins sur les différents postes, sans les afficher. De plus sur les postes clients, les accès au WEB (en INTRANET et en INTERNET) sont à la base d'enregistrements de nombreux fichiers qui peuvent vite saturer le disque dur et d'autre part laisser de nombreuses traces.

Comme généralement en sécurité, la formation et sensibilisation des utilisateurs pour accéder à l'information par le Web est une solution efficace pour pallier une majorité des risques induits.

2.1.2 Pour FTP

Concernant les risques et parades possibles se référer au document " Sécuriser UNIX ", CLUSIF 1997.

2.2 Les risques associés

2.2.1 Sur les postes clients

2.2.1.1 Les codes mobiles

Ils son représentés essentiellement par les modules de JAVA, ACTIVEX, PLUGINS....

Souvent, on ne connaît pas exactement les actions sous-jacentes activées par ces codes mobiles (tout particulièrement en Active X), ce qui peut entraîner des actions illicites (e.g. dans un workflow pour une gestion de production: un code est programmé pour permettre une approbation non autorisée par un utilisateur non habilité).

2.2.1.2 Les COOKIES

L'intérêt des cookies pour l'utilisateur est qu'elles permettent la gestion d'un contexte qui est ensuite reporté dans l'applicatif. Les cookies pallient le fait que HTTP n'est pas un protocole contextuel. Les cookies ont donc le grand avantage de dispenser d'un stockage sur le serveur de chaque contexte.

En revanche, ils contiennent souvent les login et mots de passe du poste client, et même si ils ne peuvent pas être lus par un autre serveur que celui qui les a envoyés au client, il faut se méfier des interactions avec Active X, dont la finalité n'est jamais limpide. En particulier, on peut très bien imaginer le plantage du navigateur d'un client à distance.

Par ailleurs, les cookies constituent un moyen de récupérer de l'information par la connaissance des actions de l'utilisateur. En particulier si le poste client est utilisé par plusieurs utilisateurs, chaque cookie posé par un serveur constitue une trace qui reste sur le disque dur.

2.2.1.3 Les liens OU raccourcis

Si on répond positivement à la demande de lien ou de raccourci sur certaines pages via INTERNET Explorer, une icone se crée automatiquement sur le poste qui permet ensuite l'accès direct à cette page. En fait, on ne sait pas à l'avance ce qui se passe réellement, ni comment supprimer par la suite cette icône.

2.2.1.4 Le NetCasting (ou technologie PUSH)

Le client s'inscrit auprès d'un serveur. Ce dernier lui envoie des informations de manière régulière ou non, le client reçoit de l'information à la manière d'un récepteur de télévision. Par conséquent, le client n'a pas la maîtrise du contenu des informations envoyées et celles ci peuvent très bien être des mises à jour de versions d'applications. Il est donc très important pour le client, de connaître la fiabilité et le niveau de confiance à placer dans le serveur.

2.2.2 Sur les serveurs

Un certain nombre de risques sont, en fait, directement liés **au contexte** du serveur. On peut noter les exemples suivants:

- la machine hôte n'est pas dédiée et les applications qui cohabitent peuvent affecter la sécurité du serveur.
- la configuration de la machine hôte est inadéquate....

Il est donc très important de faire une étude préalable d'architecture, voire de dédier les serveurs aux seuls services INTRANET utilisés. Il est également important de ne pas mélanger le serveur WEB institutionnel qui est accessible par l'INTERNET et le serveur WEB INTRANET qui ne comporte que des accès aux applications internes.

2.2.2.1 Modules CGI-BIN associés au serveur HTTP

Les CGI-BIN représentent une technique très utilisée pour interfacer le serveur HTTP avec des applications différentes de manière à rendre le site WEB plus interactif...

Les risques principaux associés à cette technique sont:

- le détournement par la commande exec " ..... ",
- le débordement de pile .

2.2.2.2 Autres types de risques

Plus généralement, on peut noter d'autres types de risques dont les plus fréquents peuvent être:

- les risques liés à **la substitution** du serveur (détournement du site, de la première page ou de certains documents critiques), lorsque le serveur n'a pas de fonction d'identification par rapport au client. Une des méthodes employée consiste à court circuiter le DNS interne,
- les risques liés à la **compromission** des systèmes de sécurité propres aux serveurs ou aux application associées,
- les risques liés à un **déni de service** suite à un bombardement de trames (ce risque devient d'ailleurs de plus en plus fréquent et facile à effectuer dans un contexte INTERNET).

2.3 Les solutions associées

2.3.1 Sur les postes clients

2.3.1.1 Les codes mobiles

Une solution efficace mais radicale est d'interdire l'utilisation des codes mobiles pour la totalité du réseau (ACTIVEX, PLUGINS). On risque alors, de limiter toutes les possibilités d'affichage de la page concernée. On peut laisser aussi leur utilisation à la discrétion des utilisateurs (applets java), mais les messages intempestifs de confirmation sont souvent lassants.

Pour JAVA, on peut utiliser des applets certifiées. Pour les besoins de l'entreprise, on peut aussi certifier les applets au niveau de l'entreprise après avoir vérifié leur innocuité.

Comparativement aux composants de ActiveX, les applets java ont une action limitée (et donc un impact limité) grâce à l'effet " bac à sable " qui constitue une sorte de cloisonnement intrinsèque.

Pour Active X : on peut exiger que la signature s'exécute au niveau du serveur et non au niveau du browser.

2.3.1.2 Les cookies

Il faut savoir que seul le serveur qui a fourni des informations par le biais de cookies sur les postes clients est en mesure de les exploiter ultérieurement.

Néanmoins, il faut contrôler le niveau d'information demandée et se méfier des demandes d'email ou d'informations nominatives sans but vraiment précis.

On peut aussi configurer le butineur pour laisser à la discrétion de l'utilisateur l'autorisation des cookies au cas par cas, mais de nouveau, cela devient vite fastidieux pour l'utilisateur.

On peut aussi filtrer les cookies ou les interdire en amont (au niveau du firewall, de la passerelle ....) en ayant cloisonné auparavant son applicatif ou son réseau.

Une autre option consiste à nettoyer périodiquement les fichiers qui contiennent des cookies en ouvrant le répertoire " cookie " avec un éditeur standard puis à en vérifier le contenu et à supprimer, si besoin, les cookies. Cette démarche a l'avantage de permettre la vérification des serveurs qui utilisent des cookies et qui positionnent leur contenu en clair ou non.

2.3.2 Sur les serveurs

2.3.2.1 Les CGI-BIN

La meilleure parade est de faire attention au codage des applications CGI, de vérifier le code importé, suivre certaines règles lors de l'implémentation d'une application en interne. Se référer à des organismes tels que les CERT (CA96) qui fournissent des avis et recommandations très pertinents.

2.3.2.2 La substitution du serveur HTTP

Pour éviter que par malveillance on substitue un serveur compromis au serveur WEB, une parade consiste à utiliser le protocole HTTPS ou SSL , ce qui oblige le serveur à utiliser ses certificats pour s'authentifier. Il va de soi que les certificats doivent être délivrés par une autorité à laquelle toutes les parties font confiance.

Une règle générale pour minimiser l'impact des risques cités précédemment est de cloisonner finement les systèmes applicatifs aussi bien le serveur que les applications qui gravitent autour, ainsi que les codes mobiles. De plus il est vivement conseillé d'utiliser les procédures de sécurité répertoriées et associées aux protocoles utilisés dans l'INTRANET (voir rapports du CLUSIF sur UNIX sécurisé, et NT sécurisé)

2.3.2.3 La compromission et le déni de service

Afin d'éviter la compromission, une authentification et traces des actions effectuées sur les systèmes de sécurité et applications s'avèrent naturellement indispensables.

Pour le déni de service, il est important de bloquer l'arrivage des trames pour le service considéré en cas de trafic anormal. Cette action est facilement effectuée avec l'utilisation d'un firewall.

Sinon, pour éviter des dénis de service spécifiques à l'expéditeur d'un message (si l'expéditeur réfute avoir émis un message), les mécanismes de signature électronique peuvent s'avérer intéressants.

3. LES ACCES INTERACTIFS AUX APPLICATIONS

Les services pris en compte dans ce chapitre sont: TELNET et les applications type “ web enabled ”

3.1 Introduction

TELNET a été la première application interactive (client/serveur) s’appuyant sur l’architecture TCP/IP. La simplicité de configuration et d’administration de cette suite de protocoles en favorise la sélection pour réaliser des réseaux INTRANET, ceci s’ajoutant à la possibilité, au moins conceptuelle, d’établir des connexions aisées vers l’INTERNET avec les mêmes applications. De plus ces applications sont souvent disponibles à peu de frais, sur la quasi totalité des plates-formes et couvrent de manière satisfaisante un très grand nombre de besoins.

L’exemple de Telnet permet de saisir les risques associés aux informations situées sur un serveur concernant leur intégrité et leur confidentialité: absence ou faiblesse de l’authentification de l’utilisateur sur le poste client, absence de contrôle des droits d’accès, mais aussi pour le client: absence d’authentification mutuelle et pour l’information elle même : écoute ou modification en ligne.

Concernant les applications “ **web enabled** ”, il s’agit d’accéder à des applications via HTTP pour permettre une ergonomie web classique. Il existe, par conséquent, plusieurs interfaces (ex web serveur d’Oracle...) entre un serveur HTTP et un certain nombre d’autres serveurs applicatifs qui peuvent être compromis si le serveur web fait lui-même l’objet d’attaques ou, à l’inverse il faut être prudent sur le fait qu’un utilisateur ne passe pas outre le serveur HTTP pour se connecter directement sur un serveur applicatif. Ces accès interactifs correspondent donc, à l’environnement classique des applications de production de l’entreprise et il convient, de toute façon, de leur appliquer les règles habituelles de sécurité des systèmes d’information.

3.2 Les risques associés

3.2.1 Sur les postes clients

En général, le problème est que l’on a à partir d’un service INTRANET, une action sur les applications. Par conséquent tous les éléments actifs “ sauvages ” peuvent agir sur les stations clientes. Il est donc important de bien contrôler les configurations des postes clients.

3.2.2 Sur les serveurs

Les risques concernent la violation de l’intégrité et de la confidentialité des données ainsi que les attaques mettant en jeu la disponibilité des serveurs.

En effet, par rapport à des applicatifs classiques, l’accès à une application via HTTP génère un trafic bien plus important en raison des icônes, images, animations qui sont ajoutées pour l’ergonomie, le tout peut entraîner des dénis de service.

D’autre part, la mise en place d’un INTRANET remet en cause la méthode classique d’authentification uniquement auprès “ du ” serveur de production ; dans un environnement

distribué, cette nécessité risque d'imposer des authentifications répétées auprès de chacun des services si l'on n'adopte pas des solutions dites de " Single-Sign-On " (S.S.O.) surtout pour les applications n'établissant pas de contexte de connexion.

L'administration permanente des authentifiants et des droits de chaque personne doit être mise en œuvre de manière systématique et auditable par l'autorité responsable de la sécurité. Les solutions adoptées doivent pouvoir s'adapter à la présence de " domaines " de confiance, nécessaires dès que l'entreprise atteint une taille importante et/ou couvre un large espace géographique.

Des moyens suffisants doivent être mis en place pour assurer un suivi permanent de la bonne mise en œuvre de la politique de sécurité. De plus cette politique doit être cohérente et adaptée au niveau de risque reconnu par l'entreprise pour chaque serveur et chaque base de données.

En effet, il ne faut pas oublier qu'un serveur HTTP peut avoir des liens, par relais applicatifs Web, sur maints serveurs donc il ne suffit pas de contrôler, pour un utilisateur, sa seule autorisation ou non à HTTP. Souvent, par ces relais, on établit un menu applicatif relatif au droit de l'utilisateur, suite à une demande d'une URL point d'entrée unique . Il faut se méfier du fait que chaque choix du menu correspond souvent à une url " cachée " a priori mais qui peut être accédée par un utilisateur non habilité qui en demandera l'accès direct par HTTP.

Par ailleurs, il est important d'assurer une bonne cohésion entre les autorisations HTTP et URL et Telnet afin qu'un utilisateur ne se connecte pas directement à un serveur auquel il n'a pas accès via le serveur HTTP et les relais applicatifs.

3.3 Les solutions associées

3.3.1 Sur les postes clients

Pour assurer l'authentification réciproque du serveur vers le client, on peut utiliser aujourd'hui des certificats mais il n'y a pas encore de mise en place complète, à ce jour, d' organismes certificateurs fiables sauf à l'être soi-même dans sa société.

Les attaques postes-clients désormais classiques par des virus importés dans des fichiers, sont suivies par des attaques provenant de codes importés dans des applets Java ou ActiveX dont il est très difficile de contrôler l'origine sauf si ils sont signés.

L'analyse de ces codes doit être effectuée dans des proxies mais l'état actuel rend ce contrôle illusoire. Une autre technique, qui commence à émerger, consisterait à exécuter ces applets sur une machine spécialisée et cloisonnée qui exécute puis rapatrient le résultat sur le client.

Il est à noter que les spécifications de Java version JDK 1.2 devraient apporter la possibilité de gérer des profils d'applets mais au risque d'une charge très importante pour les responsables de la sécurité.

Il est rappelé qu'un cloisonnement entre les organisations de l'entreprise conserve son importance ainsi qu'une cohérence des profils des droits des utilisateurs, cela renouvelle la nécessité d'organiser en parallèle une administration suivie de ces droits.

Par ailleurs, on ne sait jamais si une application est fiable ou non, seules des règles de qualité des développements et de maintenance permettent d'en maîtriser l'ensemble.

3.3.2 Sur les serveurs

Un suivi des droits des utilisateurs et de leur délégation permet de mieux assurer les contrôles d'accès aux serveurs et des échanges de ces droits de serveurs à serveurs.

Se reporter aux avis du CERT sur le niveau de fiabilité et les failles des applicatifs (ex. listener http)

4. LA MESSAGERIE ELECTRONIQUE

Le service pris en compte est SMTP.

4.1 Introduction

Nous allons étudier comme dans les paragraphes précédents les risques au niveau des clients (User Agent) et des serveurs (Mail Transfert Agent) puis les solutions permettant de lutter contre ces risques.

La messagerie est typiquement le service où il existe le plus d'interconnexions avec INTERNET et par conséquent, où l'on hérite le plus des problèmes liés à l'INTERNET.

4.2 Les risques associés

4.2.1 Sur les postes clients

Le principal problème rencontré par tous les utilisateurs est bien évidemment le problème des **virus**. S'il est acquis que des virus peuvent se trouver dans les fichiers attachés, existe-t-il un risque à l'ouverture d'un mail avec le client de messagerie (Viewer) ? Il semblerait que oui dans la plupart des cas. Les clients de messagerie qui peuvent lire les messages au format HTML (fournis avec Outlook par ex.) sont certainement vulnérables aux scripts qui pourraient s'y trouver (Javascript, VBscript).

En plus du risque de virus, de macro-virus dans les pièces jointes et la nature de ces pièces jointes, la **taille des pièces jointes** peut poser des problèmes d'utilisation abusive de ressources voire de saturation, ou de fuites importantes d'information.

On retrouve une utilisation illégitime des ressources informatiques de l'entreprise dans **les chaînes de message**. Les **rumeurs** circulant sur INTERNET gaspillent aussi les ressources de l'entreprise.

Il ne faut pas se fier à l'adresse de l'émetteur du mail puisque son usurpation est rendue possible en dialoguant directement avec le démon SMTP par exemple.

Les informations présentes dans l'entête SMTP révèlent des informations sur le système d'information de l'entreprise (logiciels serveurs de messagerie, noms et adresses IP de ces serveurs). Attention, ces informations font partie du protocole SMTP; les enlever pourrait conduire à des dysfonctionnements (atteinte sur la disponibilité).

Les **automates** associés au client de messagerie, notamment les réponses automatiques et les listes de renvoi, peuvent conduire à des boucles et faire effondrer le système de messagerie de l'entreprise.

Le protocole **POP3** n'est plus à l'état de l'art de la sécurité informatique aujourd'hui. L'authentification repose sur un simple mot de passe statique et l'utilisateur n'a pas de traces des dernières connexions (infructueuses ou non).

Enfin, le **SPAM** consiste à saturer les boites aux lettres de messages publicitaires de toutes natures, de messages de type chaînes, qui ne sont pas demandés par le destinataire de ces messages.

4.2.2 Sur les serveurs

Les attaques par déni de service existent sur les serveurs de messagerie; elles sont plus faciles à réaliser lorsque le serveur est couplé à un antivirus (envoyer des messages comprenant de nombreuses signatures de virus).

Les **messages publicitaires** ("junk e-mail") posent aussi le problème de la bonne utilisation des ressources de l'entreprise (humaines et informatiques).

Au niveau de la confidentialité on déplore la toute puissance de **l'administrateur qui peut lire tous les messages**.

Si la plupart des versions de sendmail utilisées pour la messagerie électronique sont upgradées régulièrement, les serveurs hébergeant des anciens applicatifs possèdent eux **des anciennes versions buggées de sendmail**. Si le service SMTP tourne sur un de ces serveurs, cela constitue une porte d'entrée possible.

Pour les grandes entreprises le problème **d'utilisateurs homonymes** peut se poser. Quelles adresses email leur donner? Le problème est d'autant plus gênant lorsque l'une des personnes est antérieure à l'autre dans l'entreprise et possède déjà une adresse mail bien connue de ses interlocuteurs.

4.3 Les solutions associées

4.3.1 Sur les postes clients

Un **antivirus couplé au client de messagerie** est une solution complémentaire à un antivirus couplé au serveur de messagerie. Il est d'ailleurs préférable que les logiciels antivirus proviennent d'éditeurs différents.

Pour les problèmes de chaînes de mails et de tailles des pièces jointes les solutions seront davantage organisationnelles que techniques.

Pour lutter contre l'usurpation d'identité, les **solutions de signatures numériques s'appuyant sur des certificats** sont des parades efficaces. Le serveur de messagerie peut donner des probabilités de risques en recherchant l'origine des messages (à quel domaine DNS appartient le serveur de messagerie qui vient d'envoyer ce message, est ce qu'il correspond à l'adresse mail de l'émetteur?).

Il faudra regarder du côté organisationnel pour trouver une solution aux problèmes liés aux automates.

Concernant POP3, il est meilleur aujourd'hui d'utiliser IMAP4.

Pour éviter la pratique du SPAM, il convient de " configurer " sa messagerie de manière à ne pas accepter le relayage de messages et n'autoriser que le " send " classique; de refuser tous messages en provenance de " Spamer " authentifié, par l'établissement d'une liste rouge par exemple; ou encore, par l'analyse du contenu (voir aussi la configuration de SENDMAIL dans le web de " isoc.asso.fr "). D'ailleurs, La jurisprudence dans certains états des USA condamne la pratique du " Spamer ".

4.3.2 Sur les serveurs

Pour lutter contre les attaques par déni de service on protégera les piles IP des serveurs de messagerie en filtrant les mauvais datagrammes IP. On cherchera aussi à limiter les impacts de telles attaques.

Des listes de contrôle d'accès (ACL) au niveau des serveurs de messagerie évitent que des messages publicitaires arrivent au niveau des clients.

Sur les machines qui ne font pas partie du système de messagerie de l'entreprise, on ne démarrera pas les services de messagerie.

Concernant les anciennes versions de sendmail: il est recommandé de suivre les avis du CERT pour connaître les failles et installer les patchs correspondantes.

Concernant la confidentialité et l'intégrité (dans ce cas, le chiffrement doit être compris dans le sens signature ou scellement) des messages: tous les problèmes peuvent être résolus par l'application du chiffrement mais ceci nécessite la mise en place d'une organisation interne de gestion des clés. En contrepartie, il faut faire attention au fait que le chiffrement des messages peut présenter un risque de prolifération de virus, les anti-virus ne déchiffrant pas les messages.

Aussi en palliatif, le cloisonnement physique de l'INTRANET, les contrôles d'accès stricts et l'audit permettent de limiter les attaques en confidentialité et intégrité.

Pour l'homonymie, dans de grandes organisations, la gestion des annuaires (LDAP) s'intègre dans la gestion du personnel (flux de personnel, codification des noms,...), et peut être un moyen efficace de gestion des emails.

5. LE TRAVAIL COOPERATIF ENTRE NEWSGROUP ET GROUPWARE

5.1 Introduction

Dans ce chapitre nous allons évoquer les risques et solutions à mettre en place pour des organisations utilisant les notions de newsgroup et groupware.

Les **newsgroup** sont souvent appelées forums de discussion. Cela donne le moyen à un utilisateur de s'abonner à une liste publique de discussions de son choix pour laquelle il recevra tous les commentaires des autres abonnés de la liste et pour laquelle il pourra lui même, émettre des avis. **C'est le service NNTP qui est utilisé**.

Le **groupware** est un ensemble de produits qui permettent le travail coopératif ou encore, workflow, i.e. la gestion de processus entre divers acteurs (e.g. le travail coopératif d'un processus de gestion de commandes pourra être mis en place avec du groupware).

5.2 Les risques associés

5.2.1 Pour les newsgroup:

En INTRANET pur, les risques sont peu nombreux. En revanche, dès qu'il y a accès avec INTERNET, on retrouve les risques identiques à ceux de HTTP puisque les groupes de news publics renvoient sur le web. En effet, souvent des pages HTML sont introduites dans les news, qui redirigent sur le web en activant le butineur.

Par ailleurs, un risque important mais non technique à prendre en compte revient aux utilisateurs qui divulguent des informations sur leur entreprise sans en avoir réellement conscience (ce problème est d'ailleurs identique avec le mail)

5.2.2 Pour le groupware

Actuellement c'est le produit LOTUS Notes le plus répandu, mais en NT5, EXCHANGE aura une interface avec agenda et annuaire. Ce sont des systèmes assez complexes à mettre en place qui doivent faire l'objet d'une étude d'organisation et d'implémentation spécifique.

5.3 Les solutions associées

5.3.1 Pour les newsgroup:

Contrôler en interne le serveur de news ; sur un plan sécuritaire, séparer le serveur de news INTERNET de celui de l'INTRANET quand il y a la possibilité d'avoir deux serveurs.

En définitive il n'existe pas de risque majeur, mais cependant des précautions sont à prendre dans l'hypothèse de deux serveurs distincts (INTRANET et INTERNET). Filtrer l'entrée des news, selon les besoins des services. Authentifier la journalisation (s'assurer de la bonne information des usagers au sujet de cette surveillance des news et de leur consultation). Il est donc recommandé de journaliser les entrées/sorties de toutes les utilisations de l'INTERNET au sein de la société.

Autre recommandation, développer l'usage de groupe fermé de news avec authentification en SSL, en dépit d'une mise en œuvre délicate due aux certificats.

Concernant les utilisateurs, on ne saurait, comme d'habitude que conseiller des sessions de sensibilisation ainsi que des chartes de recommandation pour travailler avec ces nouveaux services.

5.3.2 Pour le groupware

Se référer aux avis du CERT (web: www.cert.org) concernant les bugs de Notes (assez bien documentés pour ce produit), et aux documentations systèmes des constructeurs ou des éditeurs.

6. REMARQUES GENERALES SUR LE DNS

Il est important, dès que l'on gère un INTRANET, d'avoir un serveur DNS privé dans son réseau interne qui comporte les adresses et les noms de domaine internes et d'avoir un DNS public, de préférence, en Demilitarized Zone (DMZ) qui comportera les adresses et noms de domaine accessibles de l'extérieur. D'ailleurs la plupart du temps, la seule adresse connue de l'extérieur est celle du firewall qui permet de masquer les adresses internes et qui effectue également, le relai vers le serveur de DNS interne.

Par ailleurs, les DNS public et secondaire peuvent être hébergés chez un opérateur si ce dernier garantit formellement la gestion de la sécurité de ce service.

7. REMARQUES SUR L'OUVERTURE DE L'INTRANET AVEC L'INTERNET ET L'EXTRANET

Les entreprises créent très rarement des INTRANET complètement isolés et internes. Ces technologies sont le plus souvent employées pour établir des liens et des moyens de communication communs avec l'extérieur donc pour s'interconnecter avec INTERNET. Dans ce cas, il faut naturellement bien isoler le réseau sûr INTRANET du réseau INTERNET par des solutions techniques de type firewall associées à des anti-virus qui proposent, de plus, l'analyse de contenus de pages HTML, de fichiers transmis par FTP et de pièces jointes dans les mails. Il est également important d'utiliser des moyens de masquage ou de translation d'adresses souvent inclus dans le firewall, pour qu'aucune adresse interne ne soit révélée à l'extérieur.

Les INTRANET sont généralement constitués de réseaux locaux reliés entre eux par des liens situés hors de l'entreprise constitués de liaisons louées, ou de lignes commutées publiques, ou encore de lignes partagées avec d'autres entreprises (réseaux à commutation de paquets, de trames ou même l'INTERNET): on parle alors d'**EXTRANET**.

Chaque type de liaison, interne comme externe, doit être examiné en fonction de la sensibilité de l'information qui y est véhiculée. Des solutions idoines de protection des données doivent alors être mises en œuvre.

Par exemple les authentifiants (mots de passe, etc.) ne doivent pas circuler en clair dès que l'on veut éviter une écoute et un emploi non autorisé de ceux-ci.

De plus les sessions doivent être protégées, si nécessaire, contre les écoutes et les intrusions actives (interruption, substitution de correspondant, rejeu d'un échange,..). Cela est effectué par des contrôles de séquence, des réauthentifications périodiques, et éventuellement la mise en œuvre de moyens de chiffrement pour assurer l'intégrité, la confidentialité et l'authenticité des opérations les plus critiques.

L'emploi de serveurs d'accès distants, souvent placés en DMZ d'un firewall, s'avère intéressant pour contrôler des liaisons via RTC pour les postes nomades.

Chaque environnement (interne comme externe à l'entreprise) peut exiger l'emploi de tel ou tel moyens cités en relation avec la " valeur " des données échangées pour l'entreprise. Il faudra veiller particulièrement à détecter la présence possible de liaisons non autorisées (PC ou serveurs reliés à INTERNET ou à des partenaires). Des firewalls (administrés eux aussi) sont recommandés entre les zones à niveaux de confiance différents.

Un moyen efficace de contrôler des informations à haut niveau de confidentialité ou stratégiques consistent à employer la technique de tunnel chiffré (VPN), qui permet de créer virtuellement un réseau privé sur des réseaux externes en utilisant le chiffrement. Il faut dans ce cas, être au courant de la législation de chaque pays en matière de cryptologie, et...l'appliquer !

8. CONCLUSION

Pour conclure, il faut néanmoins noter que concrètement, on se heurte souvent dans l'entreprise, au niveau des systèmes clients, à des accès indifférenciés aux 3 types de réseau (INTERNET, INTRANET, Extranet), et qu'il est nécessaire de traiter le problème dans sa globalité. La nature des risques est à peu près similaire dans les 3 cas, mais leur impact est différent.

Une définition claire de la politique de sécurité en amont de toute implantation technique est une fois de plus, la meilleure démarche à adopter pour pérenniser l'existant et préserver l'avenir de son INTRANET.