Network Working Group
Requête pour commentaires:2504
FYI: 34
Catégorie: informationnel

E. Guttman
Sun Microsystems
L. Leong
COLT Internet
G. Malkin
Bay Networks

Février 1999

Guide de l'utilisateur:Sécurité

Statut de ce mémo

Note du traducteur:

Ce document est une traduction non-officielle de la RFC 2054.
L'auteur de cette traduction décline toute responsabilité sur l'utilisation
de ce document et/ou sur d'éventuelles erreurs de traduction.

Concernant les droits du traducteur: le traducteur renonce à ses droits sur
la reproduction de ce document si l'ensemble de ces conditions est respecté:
les reproductions doivent être complètes(contenant cette note),d'un seul
tenant(un seul fichier ou un ensemble de pages physiquement reliées),sans
aucune modification du contenu et réalisées à partir de la dernière version
de ce document disponible ici ou bien en mailant le traducteur et auteurs.

A noter, et l'information est importante, que les licences sont traduites,
procurez-vous la RFC officielle pour les version originales.Vous pourrez trouver
par ailleurs, les copyright originales en fin de document.

Finallement, j'attire votre attention sur la date de parution de cette RFC :Fevrier 1999.
Hors entre la date de parution et la francisation de cette RFC presque quatre années se sont écoulées.
Considérant l'evolution fulgurante du monde infomratique,il convient à mon sens de completer
votre approche de la sécurité informatique, par la l'assimilation de documentation portant un regard plus récent sur le monde de la sécurité informatique.

Dans cette optique,je vous invite à consulter sans modération la rubrique des liens.

Bonne Lecture.

Ce mémoire met à disposition des informations pour la communauté des internautes.Il ne constitue en aucun cas une norme, un standard de l'Internet. La distribution de ce mémoire est gratuite et illimitée.

Avertissement sur les droits d'auteurs.

Extrait :

Le manuel de référence relatif à la sécurité, est le complément de la RFC 2196 « Site Security Handbook (SSH) ». Il est destiné à fournir aux utilisateurs, l'information nécessaire pour maintenir leurs réseaux et leurs systèmes, dans un environnement stable et sécurisé.

Table des matières

Partie Une : Introduction

Ce document donne des directives aux utilisateurs de systèmes informatiques, de réseaux,pour qu'ils puissent assurer la confidentialité de leurs données, de leurs communications privées et sécuriser leurs systèmes et réseaux.

La deuxième partie de ce document concerne les utilisateurs professionnels, des grandes petites
et moyennes entreprises, ainsi que les usagers privés ou les usagers universitaires.

La troisième partie de ce document s'adresse aux utilisateurs qui administrent leur propre ordinateur, à titre privé.

Les administrateurs de systèmes devraient utiliser ce document comme le fondement particulier
d'un guide de l'utilisateur en matière de sécurité.Cependant, ils devraient consulter en premier lieu, le manuel de référence relatif à la sécurité de sites Internet. [RFC2196]

Un glossaire de termes est inclus dans l'appendice, à la fin du document, ce qui permettra aux lecteurs non initiés, de se familiariser avec les termes liés à la sécurité informatique.

1. Lisez-moi

Avant de vous connecter à Internet ou tout autre réseau local, vous devriez vous procurer la « chartre de sécurité » de l'espace multimedia que vous envisagez d'utiliser comme fournisseur d'accés a Internet.

La chartre de sécurité est un rapport conventionnel régissant les règles à respecter par les utilisateurs bénéficiant de la technologie d'un site et de l'ensemble des informations consignées dans le système informatique(L'actif informationel).
En tant qu'utilisateur vous êtes obligé de respecter la chartre crée par l'organisme décideur et les administrateurs de votre site.

Une chartre de sécurité existe afin de protéger le matériel, les logiciels et les données.
Elle justifie les mesures de sécurité en place, ce que les usagers peuvent faire ou non, que faire et qui contacter une fois un problème survenu et plus généralement donner les « règles du jeu » aux usagers.

Ç Les fils ont des oreilles.

Il est beaucoup plus facile d'intercepter des communications à travers des données émanant d'un réseau que de mettre en place une écoute téléphonique. Chaque lien existant entre les ordinateurs est potentiellement peu fiable, tout comme chaque ordinateur à travers lequel transit des données.Toute information qui passe par le réseau peut être interceptée, même si vous vous dîtes que « Personne n'en a rien à faire... »

L'information passant par le réseau peut très bien être lu par un public à qui ces informations sont destinées ou bien par un autre type de public... C'est ce qui peut arriver à un courrier électronique, ou à des informations sensibles accessibles par le biais d'un transfert de fichier(FTP) ou du web.
Referez-vous, SVP aux sections ne tombez pas malade ou les pièges de la messagerie électronique.
Sections spécifiques dédiées à la protection de votre vie privée.

En tant qu'utilisateur votre soucis majeur devrait être,dans un premier temps de protéger votre compte Internet des abus qu'il est possible d'y entreprendre.
Puis,défendre les atteintes portées à votre vie privée.

A moins que,des précautions ne soient prises, chaque fois que vous vous identifiez sur un réseau ou un de ces services, votre mot de passe ou les informations confidentielles peuvent être volées.Ces informations peuvent être utilisées pour accéder illicitement aux systèmes auxquelles vous avez accès.Dans quelques cas les résultats sont évidents :Si quelqu'un obtient l'accès de votre compte bancaire vous devriez trouver moyen de perdre rapidement du cash. Ce qui est moins évident, c'est que les services de nature non financiers peuvent aussi être abusés et ceux de manière très coûteuse.Notez que, vous pouvez être tenu responsable si votre
compte à été utilisé à de fins frauduleuses par quelqu'un d'autre.

Plusieurs services de réseaux demandent à l'usager de s'identifier.
L'usager est invité à fournir son nom d'utilisateur, son mot de passe pour accéder à son compte
Si cette information est transmise sur le réseau sans être crypter, l'information peut être volée et lue par des tiers.

Ce n'est pas un réel problème lorsque vous passez par un service d'accès interne ou la connexion s'effectue via le téléphone et une identification par mot de passe ;un prestataire de service en ligne, tout comme les lignes téléphoniques restent plus difficile à pister qu'une communication Internet.

Le risque est bien présent lorsque vous utilisez des programmes pour vous connecter au-delà du
simple réseau. Beaucoup de programmes populaires utilisés pour se connecter à des services spécifiques(Par ex.. FTP pour le transfert de fichiers),envoient votre nom d'utilisateur, votre mot de passe, et vos données à travers le réseau sans les crypter.
Afin d'éviter l'interception des mots de passe,la précaution la plus communément adoptée, contre l'écoute des mots de passe par les grands établissements ou les sociétés importantes, est d'utiliser le principe :Un mot de passe par connexion.A chaque nouvelle connexion son nouveau mot de passe.

Jusqu'à présent, il était bien trop compliqué et trop cher pour les usagers privés et les petites entreprises d'accéder à un système distant de manière sécurisée..
Toutefois, un nombre croissant de produits l'autorise désormais grâce à la technique du chiffrement(cryptographie), sans pour autant nécessiter un matériel fantaisiste.

Par exemple, Secure Shell[SSH],disponible en version commercial et en version gratuite est disponible sur de nombreuses plateformes.
De nombreux produits basés sur la tecnologie SSH, permettent de chiffrer les données avant quelles ne soient envoyées sur le réseau.

Partie deux: L'utilisateur final, dans un réseau administré centralement.

Les différentes règles établies constituent un résumé de conseils les plus importants, énoncés dans la deuxième partie de ce document.

-Connaissez,votre référant en matière de sécurité.

-Conservez vos mots de passe secrets en toutes circonstances.

-Protégez votre écran de veille par un mot de passe,ou éteignez votre Ordinateur dés que vous quittez votre bureau.

- Ne laissez tout simplement personne accéder physiquement à votre ordinateur et à votre réseau.

Soyez attentifs aux logiciels utilisés, et plus encore des logiciels provenant d'origine inconnue.
Réfléchissez-y à deux fois avant d'installer un logiciel téléchargé....

Ne paniquez pas, consultez votre référant sécurité, si possible, avant de lancer l'alerte.

Rapportez dés que possible les problèmes de sécurité, à votre réferant en matiere de sécurité informatique.

Ç 3.soyez prudent!s

Ç 3.1. Les dangers du téléchargement.

Vous trouverez sur Internet,une multitude de logiciels en plein essor:les gratuiciels ou freewares.
Alors que ce sensationnel développement est l'un des aspects les plus attractifs de l'usage du réseau public, il serait bon d'être prudent.

Des fichiers pourraient se reveler dangereux. Le téléchargement représente le risque le plus important.

Soyez attentifs au stockage de vos fichiers téléchargés, afin que vous puissiez vous souvenir de leur(probablement douteuse)origine.
Ne confondez pas, par exemple un programme téléchargé par un autre, simplement parce qu'il ont
le même nom. C'est une tactique ordinaire, pour inciter les usagers à exécuter des programmes
qui leur semblent familiers, mais qui en réalité sont dangereux.

Les programmes peuvent accéder au réseau sans que vous vous en rendiez compte.
Une chose a garder en tête :Si un ordinateur est connecté, n'importe quel programme à la possibilité d'utiliser le réseau avec ou sans votre accord.

Prenons un exemple :

Vous téléchargez un jeux (par ex un Gamez= un jeu a zero franc), depuis un serveur ftp anonyme
Ce jeu ressmble apparemment à un jeu de type shoot-em-up, mais sans que vous le sachiez, ce jeu transfert tout vos fichiers, un par un,
à travers le réseau sur la machine d'un cracker.

Plusieurs milieux associatifs interdisent explicitement le téléchargement et l'installation de programmes depuis L'Internet.

Ç 3.2. Ne tombez pas malade sur le Web.

Vous vous exposez à de grands risques, lorsque votre navigateur télécharge des fichiers depuis
le web.
Voir les dangers du télechargement.
Votre navigateur permet à chaque fichier d'être retracé depuis l'Internet.
Les navigateurs téléchargent des fichiers, même quand cela n'est pas nécessaire.

Ainsi,le risque mis en avant par le téléchargement de fichiers

peut être présent, même si vous ne sortez pas activement(de votre réseau)et ne gardez pas franchement ces fichiers.
Tout les fichiers que vous avez chargé depuis le réseau doivent être considérés potentiellement dangereux(même les fichiers présents dans le cache du navigateur).Ne les installez pas par erreur, alors qu'il pourrait s'agir de programmes malveillant.(Souvenez vous, les programmes sont également des fichiers.) Vous pourriez croire avoir téléchargé un fichier texte, alors qu'en réalité il s'agit d'un cheval de Troie,d'un script,etc.)

Les navigateurs Internet peuvent planifier le téléchargement et l'exécution de programmes en votre nom, soit de manière automatique ou après une intervention manuelle.Vous pouvez désactiver ces caractéristiques. Si vous les laissez actives, assurez-vous de bien en avoir compris les conséquences.
Vous devriez lire le guide de sécurité, qui accompagne la documentation de votre navigateur Internet, tout comme la chartre de sécurité de votre société.
Il faut être conscient que les programmes téléchargés peuvent être dangereux
à exécuter sur votre machine.
Pour plus de détails, voir « De quel programme s'agit'il ? ? de toute façon... ».

Les pages Web contiennent souvent des formulaires. Soyez attentifs au fait que tout comme les
Mails, des données envoyées depuis un navigateur Internet vers un serveur Web ne sont pas sécurisées.
Plusieurs méthodes ont été crées pour empêcher ceci, plus particulièrement le protocole SSL (Protocole permettant la transmission sécurisée de formulaires dans le Web, notamment lors des
transactions commerciales en ligne, nécessitant l'utilisation d'une carte de crédit.).
Cet outil est livré avec la plupart des navigateurs Internet.Il Chiffre les données envoyées entre le navigateur Internet de l'usager, et le serveur Web, afin que personne ne puisse les lire en route.

Il est possible qu'une page web vous semble authentique, alors qu'en réalité, elle n'est qu'une contrefaçon. Il est facile de copier l'apparence d'une page web originale, et tout aussi possible de ‘bouleverser' le protocole du réseau qui communique avec le serveur désiré. Ceci dans le but de rediriger le navigateur Internet vers un imposteur.

Cette menace peut être écartée, en utilisant SSL, qui vérifie l'authenticité d'une page Web. Quand une page ‘sécurisée' à été téléchargée, la ‘protection' ou le ‘verrouillage' du navigateur Internet vous le signalera.
Il est bon de vérifier deux fois ce qui va suivre :Visionnez les certificats, associés aux pages web auxquelles vous avez accès. Chaque Navigateur Internet à une manière différente de
procéder. Les certificats établiront une liste de leurs propriétaires, et des personnes à l'origine de leur diffusion.
S'ils semblent dignes de confiance, vous n'aurez probablement pas de problème.

Ç3.3 Les pièges de la messagerie

Tous les tracas ordinaires d'une entreprise s'appliquent aux messages électroniques, que vous auriez pu recevoir par n'importe quel autre moyen.
Par exemple, l'expéditeur peut très bien être ou ne pas être celui ou celle qu'il prétend incarner.
Si vous n'utilisez pas un logiciel de sécurité pour analyser vos mails, il vous sera très difficile de déterminer de manière certaine qui a envoyé le message. Ce qui signifie que le courrier électronique n'est pas un outil approprié pour mener à bien différent types d'affaires
Il est très facile de falsifier le nom de l'expéditeur d'un mail, afin de tromper le destinataire, persuadé de communiquer avec son véritable expéditeur.

Il conviendrait d'aborder un autre problème lié à la sécurité, lorsque vous utilisez votre messagerie électronique :La confidentialité...

Vos mails transitent, à travers l'Internet, d'un ordinateur à un autre.
Comme les messages se déplacent entre les ordinateurs,(et de ce fait, ils s'arrêtent dans la boite aux lettres de l'utilisateur en attendant d'être lu)ils peuvent éventuellement être consultés par d'autres individus.

Pour cette raison il est bon d'y réfléchir à deux fois avant d'envoyer des informations confidentielles ou extrêmement personnelles par messagerie électronique.
Vous ne devez jamais envoyer vote numéro de carte de crédit ou d'autres données sensibles par mail non chiffré.

Referez vous à la section Les fils ont des oreilles

Pour venir à bout de ce problème, des petits programmes relatifs à la confidentialité sont disponibles(il permmettent par exemple de gerer les cookies ou encore d'installer des filtres.)
Quelques-uns uns d'entre eux sont directement intégrés à votre logiciel de messagerie.

S'il existe un service fort apprécié par les usagers, il s'agit bien du transfert de leur courrier électronique.Toutefois cette pratique devrait être employée avec prudence.Imaginez le
scénario suivant :

Un usager possède un compte privé chez un fournisseur d'accès Internet,et souhaiterai y recevoir tous ses courriers d'ordre professionnel.
Il paramètre donc son compte, afin que sa messagerie professionnelle transfert son courrier sur son compte privé. Tout le courrier qu'il recevra
sur son lieu de travail, transitera par l'Internet, jusqu'a atteindre le compte privé.
Pendant tout ce trajet le courrier peut être lu.
Un message électronique, sensible,envoyé au bureau,peut être reniflé par la surveillance du traffic(Les logiciels de surveillance de trafic (ONGuard Internet Manager en est un exemple) permettent de visualiser en direct un site consulté par un employé et d'en bloquer l'accès immédiatement. Ils permettent aussi de constituer une liste des sites qui ont déjà été consultés, de créer un fichier de sites indésirables et d'en interdire l'accès automatiquement)
Et ce à chacune des nombreuses interruptions effecutées par votre message lors de son acheminement.

Veuillez noter, que le courrier éléctronique recu au bureau,n'est donc pas forcemment

confidentiel.Verifiez ce point avec votre employeur,qui a la possibilité (dans certains cas)de, legalement lire vos courriers éléctroniques et de les utiliser.
Le statut légal du courrier éléctronique depend directement du poids de la loi relative à la vie privée,spécifique à chaque pays.

De nombreux logiciels de messagerie,permettent de joindre des fichiers aux couriers.Les fichiers joints provenant de votre messagerie sont des fichiers comme n'importe quels autres fichiers.quelque soit le chemins emprunté par un fichier,si il mene vers un ordinateur,il est peut-être dangereux.Si la pièce jointe est tout simplement un fichier texte,pas de probléme. Mais il se pourrait que se soit bien plus qu'un simple fichier texte.Si le fichier attaché est lui même un programme ou un script executable,une extreme précaution devrait être prise avant
de l'executer.Voir la section intitulée « Les dangers du téléchargement »

3.4 les mots de passe

Les mots de passe peuvent être facilement devinés par un intrus,à moins que des précautions ne
soient prises.
Vos mots de passe doivent contenir un mélange de chiffres,de lettres majuscules et miniscules,
ainsi que de ponctuation.
Evitez les vrais mots,quelque soit le language,la combinaison de ces mots.Ne parlons même pas
des numéros de plaque d'immatriculation et numero de permis.
Le meilleur mot de passe est une fausse suite .(par ex un acronyme d'une phrase que vous n'oublierez pas) telle que "2B*Rnot2B" (evidemment n'utlisez pas ce mot de passe !)

Resistez à la tentation de noter votre mot de passe.Si vous le faites,gardez le avec vous jusqu'a ce que vous le reteniez,puis detruisez le ! Ne JAMAIS laissez votre mot de passe inscrit sur un terminal informatique ou sur un tableau.Vous n'inscriveriez pas votre code pin sur la carte d'une caisse enregistreuse n'est ce pas ? Vous devez posseder un mot de passe pour chaque compte,ou du moins autant que vous puissiez en retenir.Surtout qu'il est conseillé de les changer periodiquement.

Vous ne devriez egalement JAMAIS sauvegarder vos mots de passe dans les procedures de scripts et d'identifications.Ils pourraient être utilisés par une personne ayant accès à votre machine.

Soyez sur de vous etre réellement identifié et connecté depuis votre systéme.

La simple apparition d'une fenêtre d'identifiant de connexion, vous demandant votre nom d'utilisateur et votre mot de passe,ne signifie pas forcemment que vous allez accedez au service requis.Evitez les fenêtres d'identifiant de connexions inhabituelles,et reportez immediatement ces anomalies à votre referant en sécurité.Si vous remarquez quelque chose d'etrange lors de votre connexion,changez votre mot de passe.

A moins que des précautions aient été prises,comme le chiffrement(ou le cryptage) quand votre mot de passe est envoyé sur le réseau,vous devriez dans la mesure du possibe,utiliser un mot de passe different lors de chaque connexion sur un syteme,situé au dela de votre reseau(Certaines applications effectuent ce travail à votre place).
Voyez le chapitre les fils ont des oreilles,pour plus d'informations sur les risques liés à l'activation d'un systéme à distance.

3.5 Les virus et autres maladies

Les virus sont essentiellement des éléments indésirables vehiculés par des logiciels et capables de trouver leur propre chemin vers des ordinateurs sains.Ce que le virus fait une fois que l'hôte est infecté ?Cela varie selon differents facteurs.Pour quelles actions à été programmé le virus ?Quelle partie du systéme de votre ordinateur est attaqué ?

Certains virus agissent comme de veritables bombes à retardement,qui s'activent uniquement lorsque certaines conditions sont réunies,comme par exemple, l'arrivée à une date butoire.
D'autres virus restent cachés dans le systéme jusqu'à ce qu'un programme contaminé soit activé.
Il en existe bien d'autres,actifs en permanence et qui exploitent chaque opportunité pour vous faire des misères.Un virus astucieux peut egalement modifier la configuration de votre systéme puis se cacher.
Soyez attentifs au type de logiciels que vous installez sur votre machine.Utilisez uniquement des logiciels de « sources fiables »,si possible.
Consultez votre chartre sécurité avant d'installer un logiciel.Afin d'eviter
des problèmes de maintenance et de sécurtité,certains sites donnent acces aux logiciel, uniquement aux administrateurs systèmes.

Les réseaux locaux utilisent leurs propres outils et menent leur propre politique de sécurité, afin de remedier aux menaces que representent les virus.Consultez votre charte sécurité,ou referez vous à votre administrateur système, pour savoir quelle atitude adopter face a cette menace.

Il serait judicieux de réferer à votre administrateur système toute anomalie détectée par vos outils de protection(parefeu,antivirus,etc).Vous devriez le stipuler à l'administrateur systeme de votre site ,ainsi qu'à la personne qui vous a contaminé.Dans ces situations il est important

de rester calme.Les virus semment la confusion et vous font plus perdre de temps qu'ils ne causent de dommages préjudiciables.
Avant l'annonce fracassante d'un Virus,assurez vous à l'aide d'un antivirus que vous êtes réellment infecté,et si possible en presence d'un personnel technique competent.

Les chevaux de troie et les vers sont souvent répertoriés dans la categorie des virus.Nous evoquerons le cas des cheveaux de troie dans la section intitulée « quel est ce programme,de tout manière.. »
Pour les themes de cette section,les vers seront considéres à part entière comme une categorie de virus.

3.6 Les modems

Vous devez êtes vigilant lorsque vous ajoutez des fonctionalités materiels sur votre ordinateur,et plus patriculièrement lorsque ce materiel permet de transporter des données .
Assurez-vous d'avoir une autorisation avant d'installer ce type de materiel sur un ordinateur connecté à un resau local.
Les modems representent un risque serieux en matiere de sécurité.
De nombreux réseaux sont protegés par un ensemble de prédispositions techniques(parefeu,routeur,passerelle)déstinées à lutter contre les attaques frontales issues du réseau public.
Si votre ordinateur est relié à ce type de réseau,faîtes bien attention lorsque vous utilisez votre modem.
Il est assez envisageable d'utiliser un modem pour avoir accés à un reseau distant tout en étant connecté depuis un réseau securisé.
Votre ordinateur peut, dans ce cas, se reveler être une veritable faille pour les défenses de votre réseau...Des utilisateurs non autorisés,pourraient dans ce cas, avoir accés au réseau de votre entreprise depuis votre machine !

Soyez vigilant :Si votre modem reste actif, alors que votre machine est configurée pour autoriser les connexions vers et depuis d'autres ordinateurs (c'est le cas par exemple lorsque vous utilisez sous Windows des applications telles que Hyperterminal,et l'acces réseau à distance.),assurez vous d'avoir mis en oeuvre toutes les options de sécurité requises.

Nombreux sont les modems reglés par défaut,pour répondre aux appels arrivants.

Si vous en avez pas l'utilité,il est conseillé de désactiver cette option.

Certains logiciels, requierent ce type d'accès à distance, pour pouvoir par exemple récuperer des infos sur un serveur nécesaires à son fonctionnement.

Pour ce type de service, n'autoriser l'accès à votre machine depuis une ligne téléphonique,qu'une fois toutes les options de sécurité disponibles activés.

Notez que'empecher l'affichage des numeros(de telephone) ne vous protegerea pas d'une personne,susceptible de créer une brèche sur votre machine et d'y acceder depuis la ligne téléphonique du modem.

3.7 Ne me quittez pas...

Ne laissez pas un terminal informatique ou un ordinateur connecté sur un compte,en votre absence.

Quand cela est possible,utilisez l'ecran de veille,protegé par un mot de passe.Vous pouvez le parametrer pour qu'il se declenche,aprés un certain temps d'inactivité de votre machine.

Les sinistres tels qu'une personne cherchant à effacer votre travail peuvent arriver plus souvent que vous ne le pensez.
Si vous restez connecté,une personne peut sa saisir de votre poste faire quelques bêtises pour lesquelles vous seriez tenu responsable.
Par exemple, imaginez dans quel embarras vous pourriez être, si un courrier éléctronique obscène était envoyé au président de votre société en votre nom,ou que votre compte soit utilisé pour transferer en toute illegalité un contenu à cactère pornographique.

Toute personne susceptible d'acceder physiquement à votre machine, peut à coup sur y occasioner des dégats.Cependant, assurez vous de bien connaître les personnes ayant accés à votre machine. Si vous ne pouvez pas sécuriser physiquement votre machine,il est sage de chiffrer les fichiers que vous conservez sur votre disque dur.Si possible,il est aussi raisonnable de fermer la porte de bureau donnant acces à votre ordinateur.

3.8 Protections de fichiers

Les fichiers et les repertoires partagés sur,les réseaux locaux,et tout les autres systèmes bénéficiant du partage de ressources,requiert attention et maintenance.

Il existe deux types de systemes :

-Les fichiers partagés.

Les fichiers partagés peuvent être soient accessibles par tous,ou faire partie d'un groupe d'utilisateurs restreints.Chaque système procède de manière differente.Apprenez à maitriser les contrôles d'accés aux ressources partagées,et à implementer de tels controles sans vous tromper.

Fichiers protegés.

Ils comportent les fichiers auxquelles vous seule devriez avoir accès,mais qui sont aussi disponibles pour les personnes possedant les droits de l'administrateur réseau.Prenons pour exemple,les fichiers associés à la remise d'un E-mail.Vous ne voudriez pas qu'un autre utilisateur lise vos Email,et bien assurez vous que ces fichiers possedent les droit d'utilisations requis.

3.9 Tout chiffrer.

De plus, il existe des fichiers d'ordre privés.Il se peut que vous deteniez des fichiers auxquels vous seul devez avoir accès.Dans ce cas,il est prudent de chiffrer vos fichiers.
Grâce à cette méthode,même si votre réseau est une véritable passoire,ou que votre administrateur système se prend pour M. Hyde,vos informations confidentielles ne seront plus accéssibles.
Le chiffrement est egalement trés important si vous partagez des ressources.
Par exemple votre ordinateur personnel, peut être utilisé par des camarades ,qui preferent assurer la confidentialité de leur Email et toutes autres informations de nature financière.Le chiffrement vous permet d'associer partage de ressources,et utilisation privée.

Avant de chiffrer vos fichiers,consultez la chartre sécurité qui régit votre accès au réseau.Certains pays,et certains employeurs interdisent formellement le stockage ou le transfert de fichiers chiffrés.

A tire d'information,je vous invite à consulter cette adressse :

http://www.univ-tlse1.fr/DESS-DSI/DSI/Articles/a97/a97_crypto.htm
ou encore :
http://www.internet-juridique.net/

Faîtes attention aux clés ou aux mots de passe que vous employez pour chiffrer vos fichiers.Mettre en lieu sur vos mots de passe et clés de chiffrage,ne vous aidera pas seulement à les tenir à l'ecart des curieux ,mais cela vous permettrra également de les sécuriser.

Bien entendu si vous perdez ces clés et mots de passe,il vous sera imposible de déchiffrer vos données.
Il est donc prudent de conserver plus d'une copie de ces clés. Il peut également être judicieux d'avoir recours à «un tiers de confiance» si votre entreprise utilise la chiffrement.

(Selon la legislation francaise en vigueur,la cryptologie n'est libre que si les clés utilisées pour coder le message sont gérées par des " tiers de confiance ", ou avec une autorisation du Premier Ministre. Ces " tiers de confiance ", assujettis au secret professionnel et situés sur le territoire français, devront être préalablement agréés par le Premier Ministre.)

Cela peut éviter quelques désagrements:imaginez que la seule personne de votre entreprise connaissant ces clés,décide de quitter votre societé,ou soit frapper par un éclair...

Alors que l'on peut se procurer aisemment de nombreux logiciels de cryptographie,on peut constater que la qualité varie radicalement.

PGP(qui passe pour la solution logicielle assurant « une confidentialité accrue ») par exemple,offre de grandes possibiltés en matière de chiffrement.(Allez visiter ce site. http://www.openpgp.fr.st/) .La plupart des logiciels ordinaires,vous permettent de chiffrer vos données,mais l'assimilation de la cryptographie dans ce cas,sera assez faible.
Il ne faut pas vous laissez intimider par le carcatère complexe des logiciels de cryptographie.De nombreux logiciels simples d'utilisation sont disponibles.

3.10 Détruire tout le reste

Vous seriez surpris de voir ce qui peut être jeter dans les corbeilles à papier: Notes de réunions,vieux plannings,annuaire télephonique interne,la liste des logiciels utilisés par votre entreprise,des notes en rapport avec vos client, et même des études de marché.
Tout ceci s'avererait trés utile pour,des agents recruteurs,vos concurents et même pour un journaliste zelé à la recherche d'un scoop.
La menace que représente la fouille des poubelles est sérieuse,prenez la au serieux ! !
Passez au broyeur tous les documents potentiellment utilisables avant de les jeter.
Dans la même optique,lorsque vous effacez un fichier depuis votre poste de travail ,les données ne sont en aucun cas supprimées.
La seule solution consiste à reformater votre disque dur.
(NB:De nombreuses entreprises preferent tout simplement détruire physiquement,leurs disques durs.En effet,certains logiciels permettent de restituer les données d'un disuqe dur reformaté ;ca prend bcp de temps mais ca fonctionne bel et bien.)

3.11 De quel programme s'agit il ?,de toute facon ?

Les programmes utilisés ces dérnières années,sont devenus de plus en plus complexes.Ces programmes bénéficient souvent d'extension, qui peuvent se réveler « dangereux ».
Ces exetensions rendent les applications plus puissante,plus souple et personalisable.Ils ouvrent aussi la porte à toutes sortes de risques.

-Certaines applications peuvent bénéficier raccord,d'extensions(les plug-in).
Ne soyez pas dupes,ce n'est pas parce que vous avez une totale confiance en un logiciel qu'il ne faut pas se méfier d'un plug -in qui viendrait ajouter de nouvelles fonctionnalités à votre programme.

Par exemple,certains sites webs vous suggèrent de téléchrager le plug-in approprié,afin de visualiser au mieux une page ou une partie du contenu de cette page.

Eleménts à prendre en considération : Quel est ce plug-in ? ?
Qui l'a écris ? Y' a t'il un danger, à l'integrer à mon navigateur ? ?

Certains fichiers sont appellés « documents composites ». Cela signifie que vous aurez besoin d'utiliser non pas un programme pour visualiser ou éditer ce document,mais de plusieurs programmes.

« NB :Un document composite est, en fait, un document cible considéré par rapport à son contenu. Cela peut être:un document créé par un logiciel de traitement de texte qui contient un graphique créé par un tableur; une page Web;un message électronique auquel on a joint un fichier; etc. »

Pour l'usager, le document apparaît comme un seul et même document.On rencontre également ce type de documents sous differentes appelations« document composé », « document mixte » ou « document hétérogène ».
Une nouvelle fois, mefiez vous lorsque vous téléchargez ce type de documents.Même s'ils s'utilisent avec des logiciels populaires,n'en croyait pas pour autant que le document associé soit fiable.
Supposons que vous recevez un message éléctronique,lisibe uniquement avec une extension spécifique.Ce composant peut être un programme dangereux,qui s'empressera d'effacer votre disque dur !

certains programmes sont téléchargés automatiquement lorsque vous accedez à une page web.Bien qu'il existe des protections pour utiliser ce type de programme en toute sécurité,des failles de sécurité ont été decouvertes par le passé.
Pour cette raison,les réseaux locaux nécessitent la désactivation de certaines fonctionnalités spécifiques à votre navigateur.

4. La Paranoia est une bonne chose

Beaucoup de gens ne le réalisent pas ,mais le social engineering
« NB :(Le « Social engineering », encore appelé en français « subversion psychologique » est une pratique consistant à abuser de la confiance d'une ou de plusieurs personnes,dans le but $principal de récupérer des informations confidentielles.) »
est une methode employée par de nombreuses personnes pour accéder au systéme de votre ordinateur.

Généralement, les personnes victimes d'intrusions sytéme, ont le sentiment que ces intrusions sont liées à une vulnerabilité technique qui aurait été exploitée par les intrus.
Les gens pensent aussi que les intrusions systémes sont purement techniques.
Toutefois,en réalité la « subversion psychologique » joue un rôle trés important,et aide grandemment les attaquants,à déjouer les protections que vous avez mis en place.

-Ce qui a tendance à demontrer qu'il s'agit souvent d'un tremplin trés facile d'acces,vers les sytémes protegés,surtout si les attaquants n'ont absolument aucun accés au système.
Dans ce contexte,le social engineering peut être definis ainsi :il consiste à gagner la confiance d'utilisateurs légitimes jusqu'a en abuser,afin qu'ils révelent les secrets de leur sytème,ou qu'ils les aident involontairement à accéder à leur sytème.

-Grâce au social enginneering,un attaquant obtient des informations et/ou une assistance qui pourrait l'aider à déjouer facilement les protections mises en place.Utiliser adroitement,le social engineering peut vous sembler autenthique,même si ce n'est en réalité qu'une vaste supercherie.

-La plupart du temps,les attaquants emploient la méthode télephonique.
Cette méthode leurs permet de conserver l'anonymat et se revele être beaucoup plus simple d'utilisation.Il leurs suffit juste de se faire passer pour un particulier quelconque, puis une fois les informations obtenues,ils disparaissent et ont en géneral de tres fortes chances de ne plus pouvoir être retrouvés.

Il existe diffèrentes méthodes de social engineering.Vous trouverez ci-desous quelques-unes de plus utilisées :

Un pirate peut prétendre être un utilisateur légitime qui ne connaît pas ce type de systéme,ou qui tout simplment débute en imformatique.Le pirate se rapproche alors de l'administrateur systéme et des autres utilisateurs en réclamant de l'aide.
Le pirate prétend avoir perdu son mot de passe ou bien encore,qu'il lui est tout simplement impossibile de se connecter au systéme,alors qu'il doit pouvoir s'y connecter urgemment.
Les pirates sont aussi connus pour se faire passer pour des VIP d'une entreprise,vociférant leurs requêtes à l'administrateur.
Dans une telle situation,l'administrateur(ou ce peut-être un usager)peut se sentir menacé par l'appel d'une telle autorité,et repond aux attentes du Pirate.

Les pirates employant la méthode téléphonique peuvent ne jamais avoir vu votre écran,auparavant.Dans ce cas,leur astuce consiste à rester dans le vague ,ne pas rentrer dans les détails,et d'inciter l'utilisateur à divulguer un maximum d'informations sur leur système.
Le pirate peut avoir recours à une voix féminine perdue et désesperée,pour faire croire à l'utilisateur qu'il porte secours à une damoiselle en détresse.Trés souvent,cela incite les utilisateurs à se découvrir. L'utilisateur revèle parfois ces secrets,quand il n'est plus sur ces gardes.

Un pirate peut aussi profiter des appels à l'aide d'utilisateurs rencontrants un probléme d'ordre technique.Offrir son aide à l'utilisateur,et un bon moyen de gagner sa confiance.Un utilisateur

frustré, confronté à ce type de problèmes sera plus que content lorsqu'une personne lui proposera son aide.
Le pirate se fait passer pour un administrateur systéme ou un technicien de maintenance.Ce pirate obtiendra la plupart du temps des informations non négligables,parce que l'utilisateur croit qu'il est bon de réveler ces secrets à des techniciens.

Le passage par des pages webs peut faire courir de gros risques au pirate,dans le sens ou il ne lui sera pas aisé de se dérober rapidement.Mais en contrepartie,le risque encouru pourrait s'averer fructueux ,si le pirate obtient tout les droits sur le systéme d'un usager naïf.

-Quelquefois,un attaquant peut avoir accés à un système sans posseder au préalable les secrets de systèmes ou des acces des terminaux.
Tout comme on ne doit pas transporter les bagages d'une autre personne pour passer la douane,aucun utilisateur ne devrait prendre les commandes à la place d'un autre.
Mefiez vous des pirates qui incite les utilisateurs a inserer des commandes qu'il ne comprennent pas et qui pourraient endommager le système.
Ces pirates exploiteront les bugs et failles des logiciels systemes même sans acces direct à votre systeme.les commandes précedemment inserées par l'utilisateur peuvent non seulement endommager le systeme mais aussi ouvrir un acces sur votre propre compte ou créer un brèche qui permettra au pirate d'acceder plus tard au systeme.si vous n'êtes pas sur des commandes que l'on vous a incité à inserer, ne suivez tout simplement pas les instructions.Vous ne savez jamais a quoi et ou cela vous menera.

Pour vous prémunir de devenir une victime du "social enginnering"(la subversion psychologique),une importante chose a garder à l'esprit est que vos mots de passe doivent rester secret.Un mot de passe de votre compte personnel devrait n'etre connu que de vous.Les administrateurs systemes qui ont besoin d'intervenir sur votre poste n' a pas besoin de votre mot de passe.En tant qu'administrateur ,les privileges qui leur sont attribués leur permettent d'intervenir sans que n'ayez à reveler votre mot de passe.Un administrateur ne devrait pas vous demander votre mot de passe.

Les utilisateurs devraient n'utiliser leur ciompte qu'a des fins personnels.Les comptes ne devraient pas être partagés,pas même temporairement avec l'administrateur systeme ou un terchnicien de maintenance .La plupart des travaux de mainteance requiert des privileges spéciaux que ne possedent pas l'utilisateur.Les administrateurs systemes possedent leur propre compte pour travailler et ne n'ont nullment besoin d'acceder à un compte utilisateur.

Les techniciens de maintenane qui se rendent sur place deraient être accompagnés par l'administrateur local du site(qui lui devrait être connu de vous).Si le site de l'administrateur ne vous est pas connu, ou si le technicien vient seul, il est raisonnable de passer un coup de fil à l'administrateur de votre site ,pour verifier que le technicien doit effectivement intervenir.Pourtant ,beaucoup de gens ne le feraient pas , car il passeraient pour des paranoiaques ou parce que il est toujours embarassant de montrer que l'on n'a pas confiance envers les visiteurs.

A moins d'être sur que la personne à laquelle on s'adresse est bien la même personne,aucune information confidentielle ne devrait être devoilée à de tels individus.
Parfois les pirates,peuvent être assez habile pour prendre la voix d'une personne que vous connaissez au téléphone.Il est toujours judicieux de vérifier à deux reprises l'identité d'une personne.si vous en êtes incapable l'action la plus raisonnable consiste à ne rien reveler de secret.Si vous êtes administrateur système il devrait y avoir une procedure type à suivre pour l'atrribution de mots de passe aux usagers.Si vous êtes un utilisateur lambda il n'y a aucune raison que vous divulguiez vos infos confidentielles à quelqu'un d'autre.Certaines entreprises assignent un compte commun pour plusieurs usagers.Si vous vous trouvez dans cette situation ,assurez vous de connaître chaque utilisateur afin de pouvoir être en mesure de verifier ulterieurement son identité

Partie Trois: L'utilisateur final administrant un ordinateur relié au réseau

L'usager à son domicile ou l'usager qui administre son propre ordinateur à de nombreuses obligations similaires à l'utilisateur final.

Ci-dessous vous trouverez des conseils supplémentaires concernant la troisième partie.

- Lisez les manuels pour apprendre comment enclencher les dispositifs de sécurité,puis activez les.

- Prenez en considération le degré de confidentialité nécéssaire pour vos E-Mail.Avez vous investis dans un logiciel garantissant les atteintes à votre vie privée?

- Préparez vous au pire à l'avance.

- Restez informez des menaces les plus récentes.

5. Créez votre propre chartre sécurité.

Vous devriez decider dans un premier temps quels risques sont acceptables,puis mettez vous à la tache.Il est également raisonnable de revoir vos décisions à intervalles regulières,et quand cela s'avere nécessaire.
Il peut être sage de tout simplement empecher le téléchargement de logiciels provenant d'une origine inconnue ,vers une machine stockant des données d'entreprisesY,ou d'autres données précieuses ou potentiellement dommageables si les informations sont perdus ou volés.

Si le systeme est à vocation commune,disons recréatifs,correspondance,et quelques compte privés,peut être vous essaierez vous au téléchargement de logiciels.Vous prendrez

inévitablement des risques en acquiérant des éléments qui ne sont pas exactement ce qu'ils semblent être.

Il peut être valable d'installer des logiciels garantissant votre vie privée sur une machien disposant de multiples comptes utilisateurs partagés. De cette manière,un camarade de chambre n'aura pas accés à vos données personnelles.

6. Les ennuis arrivent

Si vous remarquez que vos fichiers ont été modifiés ou corompu d'une facon ou d'une autre et que votre compte à été utilisé sans votre consentement vous devriez en avertir votre référent sécurité immédiatement.Lorsque vous ne connaissez pas votre référent sécurité,tentez d'appeller l'assistance technique de votre fournisseur d'accés internet.

6.1 Comment se préparer au pire à l'avance.

- Lisez attentivement toute documentation . asurez vous que tout soit sur lorsque les services tournent sur votre machine.Si les services réseau sont activés,assurez vous qu'ils soient convenablement configurés(définissez toutes les permissions de maniere à inerdire tout connexion anonyme ou en tant que guest).Progressivement,de nombreux programmes disposent de fonctionnalités réseau,implementés au sein du logiciel.Apprenez à les configurer convenablement et de maniee fiable afin d'en tirer profit.

- Sauvegardez les données des usagers.C'est toujours primordial.Ls sauvegardes sont pensées de maniere à assurer la récuperation des données si votre disque dur plante ou si vous effacez par megarde un fichier.Les sauvegardes sont tout aussi importantes au cas ou vous seriez victime d'incidents liés à la sécurité.Une des plus vicieuses et malheureuse menace est causée par les virus informatiques et les cheveaux de Troie qui effacent le contenu de votre disque dur.

- Munissez vous d'outils d'audit et d'antivirus.Apprenez à vous en servir et à les installer avant de les utiliser sur un réseau public.Beaucoup d'outuils liés à la sécurité requierent qu'ils tournent sur un système sain,afin que la comparaison puisse être effectuée entre l'état présent et l'état d'origine de la machine.

-Mettez à jour regulièrement vos logiciels réseau.Quand une nouvelle version du programme, est dipsonible, il est prudent de mettre à niveau.Les vulnerabilités seront pour la plupart

réparées.Plus vous attendrez pour les mises à jour, plus vous vous exposez au risque que les vulnerabilités de votre produit soit connues et exploitées par des pirates.Restez à jour !!

- sachez qui contacter si vous vous douter de quelquechose.

Votre fournisseur d'acces Internet à t'il un referent sécurité ou une assistance technique? Renseignez vous avant que les pannes surviennent ,ainsi vous ne retournerez pas les problemes dans tout les sens afin de savoir d'ou provient cette panne.Gardez le contact à la fois en ligne et hors connexion.

Il existe trois manières d'éviter les problèmes avec les virus.

1. Ne soyez pas confus.

Dans la mesure du possible, soyez attentifs au type de logiciels installé sur votre système.Si vous n'êtes pas conscient ou pas sur de l'origine du programme, il est préférable de ne pas le lancer.Procurez vous le logiciels depuis des sources fiables.N'executez pas de programmes et ne rebootez pas sur de vieilles disquettes,(à moins que vous ne les ayez formaté)tout particulierement si les vieilles disquettes qui ont été utilisées pour importer des logiciels maisons proviennent d'un salon de démonstration commercial ou de tout autre provennance potentiellement peu fiables.

A peur prés tous les risques de se faire infecter par un virus peuvent être éradiqués,si vous portez une attention particuliére aux types de fichiers stockés sur votre ordinateur.Voir"les dangers du téléchargement" pour plus de détails.

2. Scannez reguliérement.

Faites réviser votre système régulierement.Il existe d'excellent antivirus et outils d'audit pour la plupart des plateformes existantes .Servez vous en,et si possible,parametrez les pour qu'ils s'executent automatiquement et periodiquement.Installez aussi les mises à jour de ces outils et tenez vous informé des nouvelles menaces de Virus.

3. Remarquez l'inhabituel.

Il n'est pas vrai qu'une diffèrence que vous ne puissiez cerner ne constitue pas une difference du tout, mais c'est une bonne manière d'apprehender le sujet.

Vous devriez être habitué au fonctionnement de votre systéme.Si il se produit des changements inexplicables(par example des fichiers que saviez existants ont disparu ,ou d'étranges nouveaux fichiers sont apparus et l'espace disque commence à saturer), vous devriez verfier si un virus est présent sur votre systéme.

Vous devriez prendre un peu de temps pour vous familiarisez avec votre antivirus .Servez vous de la fonction de mise à jour automatique(si la mise n'excede pas les trois mois).Il est trés important de tester votre ordinateur si vous vous êtes servis de logiciels de partage ou d'orgine douteuse, ou si quelqu'un s'est servis du lecteur de disquette pour transferer des fichiers, et plus encore.

6.2 Comment réagir si vous pressentez des problèmes

si vous préssentez que votre ordinateur personnel,à un virus ou qu'un malicieux virus s'execute,ou que votre syteme à été visité,l'action la plus appropriée est tout d'abord de déconnecter le systeme de tout les réseaux.Si posiible,ayez recours à l'antivirus ou à un outil d'audit.

Vérfier les fichiers systèmes corrompus,altérés ou habilement remplacés est un travail tres pénible à réaliser manuellement.Heureusement il existe de nombreux outils d'audits pour les systemes orientés UNIX.Si le logiciel est téléchargé depuis le réseau,il est raisonnable de lancer une analyse antivirus ou l'outil d'audit regulierement.

Il devient clair que votre système personnel a été attaqué,il est temmps de le nettoyer.Idéalement,un systéme devrait être reinstallé aprés avoir subis des dommages.

Ce qui se traduit par le formatage de votre disque dur(donc effacer toutes les données présentes).Ensuite, installez le systéme d'exploitation et les logiciels additionnels requis.Il est préferable d'installer le systeme d'exploitation et les logicels supplémenatires depuis une disquette ou un CD-ROM,plutôt que de les installer à partir d'une sauvegarde.

Pourquoi privilegier les supports d'origine plutôt que la sauvegarde stockée sur un disque dur ? ? Simplement parce qu'il est envisageable que cette sauvegarde ait été piraté par le passé,et par conséquent,cette sauvegarde système contient deja des programmes abimés ou vérolés.La restauration d'un système est une chose vraimment pénible,mais qui en vaaut la peine.N'oubliez pas de réinstallez toutes les mises à jour de la sécurité que vous aviez éffectué avant d'avoir eu ce problème de sécurité.Obtenez ces mises à jour depuis une source fiable et certifiée.

6.3 Le courrier éléctronique

Tachez d'être prudent avec les courriers éléctroniques sauvegardés.Les copie de messages recus ou envoyées(ou même,n'importe quel fichier),stockées sur le serveur de votre fournissuer d'accès Internet,peuvent se réveler vulnérables.Le risque est qu'une personne puisse ‘forcer' s'infiltrer sur votre compte ,et lire vos messages.Conservez vos messages éléctroniques,tout comme les fichiers sensibles,sur votre ordinateur personel.

7.Seul,chez vous

Un système personel peut être penetré depuis l'Internet,si l'usager est imprudent.Les fichiers systèmes d'un utilisateur privé peuvent être volés,endommagés ou même detruits.Intrinsèquement si la stabilté du système est compromise,il est encore possible d'y accéder plus tard.Cette section met en avant quelques points délicats(problemes)et vous donne les conseils nécessaires pour les utilisateurs privés sur Internet.

7.1 Mefiez vous des Démons(Deamons).

Un systéme privé utilisant PPP (Point-to-Point Protocole) : Type du serveur auquel la connexion internet accède. Protocole standard pour la plupart des serveurs y compris les serveurs Internet et les serveurs NetWare ;Si vous voulez tout savoir sur ce protocole visitez ce site http://www.labouret.net/ppp/).pour se connecter directemment à l'Internet est de plus en plus courant.Ces systèmes représentent un des plus grand risque de sécurité lorsqu'ils ont recours à des programmes appellés « les services ».Si vous lancez des « services »,vous mettez en effet votre ordinateur à disposition des autres,pour tout le réseau.Ces « services » comprennent.

-Le serveur FTP
-Le serveur Web

Il y a en général deux types de programme qui opérent sur L'Internet:
Les clients(comme votre navigateur Internet et vos logiciels de messagerie)et les serveurs(comme les serveurs Web ou les serveurs de messagerie).
La plupart des logiciels qui tournent sur des systèmes privés appartiennent à la categorie des ‘clients';mais de plus en plus des logiciels ‘serveurs' sont diponibles pour les plateformes traditionnellement‘clients'.
Les logiciels ‘serveurs' qui tournent en arrière plan sont dénommés en tant que DAEMONS.Beaucoup de ces serveurs Daemons ont des noms qui s'achevent par un « d » comme par exemple « inetd »(Internet Daemon) ou « talkd »(talk daemon).Une fois configurés,ces programmes attendent la requête d'un client pour un service spécifique sur le réseau.

Il y a quatre chose importante à garder à l'esprit,tant que le implications de la sécurité et l'execution de services sur votre orfinateur personnel seront concernés.

Tout d'abord,le plus important :si un serveur n'est pas convenablement parametré,il reste trés vulnérable aux attaques du réseau.Il est vital ,si vous lancez des ‘services',d'être à l'aise,avec sa propre configuration.Ce qui n'est pas toujours évident,et qui requiert de la pratique ou des compétences techniques.

Tous les logiciels comportent des failles,et ces failles exploitées malicieusement,peuvent servir à detruire la sécurité d'une machine.Si vous faîtes tourner un serveur sur votre ordinateur,restez vigilant.Cela requiert du travail :Il faut garder le contact avec le fournisseur du logiciel,afin d'obtenir les mises à jour et les patchs de sécurité.il est vivement recommandé se tenir infomrer des principaux problèmes de sécurité,notemment par le biais des forums traitant de ce sujet.Voir la [RFC 2196] pour obtenir une liste des références.

Si des failles sont mises à jour sur votre serveur,cela implique que vous cessiez d'utiliser votre serveur,ou que vous appliquiez les patchs et correctifs de sécurité le plus tôt possible.

D'une manière empirique,plus vos logiciels sont dépassés et plus vous aurez de chances d'être vulnérable aux attaques connus.Il ne s'agit pas de ne faire confiance qu' aux marques les plus en vogue.La plupart du temps,découvrir des vulnérabilités sur votre serveur ,même les plus évidente,peut prendre du temps.

- Quelques serveurs,démarrent,sans avertissement.Certains navigateurs Internet et des clients Telnet lancent automatiquement les serveurs FTP,si ils ne sont pas formellement configurés pour rejeter ces connnexions.Si ces serveurs ne sont pas eux-memes parametrés de manière optimale,l'ensemble des fichiers sytèmes,pourraient se retrouver à disposition sur Internet.

En général tout logiciel est capable de lancer un serveur réseau daemon.Pour l'envisager de la manière la plus fiable qu'il soit,il est bon de bien connaître le logiciel utilisé.Lisez le manuel et si une question se pose,appelez l'entreprise ou envoyez un mail à l'auteur du logiciel libre ,pour déterminer si vous employez vraimment un service en utilisant ce produit.

Un usager privé qui lance un service de connexion à distance,depuis son propre ordinateur se confronte à de serieux risques.
Ce service permet à l'utilisateur de se connecter depuis son ordinateur personnel à d'autres ordinateurs sur Internet,ce qui peut se réveler assez pratique.Mais le danger est qu'une personne observe secretement la session d'identification et soit capable de se faire passer pour vous,et qui sait ce qu'il fera ensuite.Voyez la section ‘les fils ont des oreilles'qui suggere les prédispositions à prendre concernant l'ouverture de session à distance.

Si possible,activez toutes les options «fichiers de verfification» de votre logiciel serveur,qui se rapporte à la sécurité.Vous aurez besoin de revenir sur ces fichiers de vérification régulierement afin d'en tirer pleinement partie.Vous devriez être aussi conscient que ces fichiers grossisent rapidement en taille,veillez donc à ce qu'il ne remplissent pas votre disque dur !

7.2 changez de lieu de travail.

Les ouvertures de sessions à distance permettent à un utilisateur privilegié d'avoir un accès physique à un système distant,tout en bénéficiant du confort de son domicile.
De plus en plus d'entreprises offrent à leur employés la possibilité de travailler depuis leur domicile,tout en ayant accès à leur compte et ordinateur de bureau , tout ceci grâce aux liaisons commutées.

Comme evoqué dans dans la section "les fils ont des oreilles" les connections Internet peuvent être interceptées.Si vous vous evertuez à utiliser un service de connexion à distance,assurez vous que cette connexion dispose des technologies de sécurité adéquates.Si c'est le cas utilisez les.

Les connexions peuvent donc être sécurisées à l'aide de technologie comme le mot de passe à usage unique,ou secure shell(ou encore le protocole securisé :Secure Socket layer(SSL).Le mot de passe à usage unique à l'avantage d'être inutilisabe si il est volé,alors que le protocole sécurisé «secure shell» chiffre les données envoyées par le biais de la connection.Referez vous à la section « Ne tombez pas malade sur le Web »,pour plus de précisions sur SSL.Les services sécurisés,doivent aussi être présents sur la machine à laquelle vous accédez à distance

7.3 Protegez vous.

Administrez son ordinateur personnel signifie que vous allez devoir choisir le logiciel serveur adapté à vos besoins.Les logiciels de cryptage constituent une protection pour les données.Si vous conservez des chiffres d'affaires ou d'autres données sensibles sur votre ordinateur,le chiffrement vous aidera à les préserver de toutes indiscretions.Par exemple,si vous lancez un service du réseau depuis votre ordinateur personnel,et que vous ne configurez pas correctement les restrictions des usagers sur des repertoires privés,un utilisateur distant(autorisé ou non)peut accéder aux fichiers de vos répertoires privés.Par contre si ces fichiers sont chiffrés,l'usager distant ne pourra rien en faire.Par ailleurs,avec tout les differents apsects de cryptage tournant sur chaque système,les clés de cryptage et les mots de passe doivent absolument être conserver en lieu sur !

7.4 Liens

Voici une liste de liens non exhaustive ajoutée par mes soins(le traducteur).

Ce lien est un très bon complément à la lecture de cette RFC :

A lire D'urgence ! ! http://www.bugbrother.com/security.tao.ca/index.html
http://www.bugbrother.com/
http://www.cru.fr/securite/
http://www.cnrs.fr/Infosecu/Revue.html
http://www.securite.org/index2.html

8. Note finale.

Ce document constitue pour le lecteur une introduction,ou les détails ne sont que sommairement abordés.Les solutions relatives à la sécurité sont rapidement dépassées,bien que de nombreux efforts soient consentis pour maintenir le debat d'actualité;les exemples donnés peuvent trés bien être denué de sens dans l'avenir,au rythme auquel évolue l'Internet et l'industrie de l'imformatique.

A une epoque ou les individus évoquent de plus en plus prudemment le coût du confort,pour sécuriser leur domicile,dans un monde en perpetuelle évolution,les utilisateurs d'ordinateurs reliés à un réseau ne devraient pas ignorer la sécurité.Cela peut être trés génant,mais il est toujours préférable d'etre assuré,plutôt que peiné.

APPENDICE :Glossaire et terme de sécurité.

Note du traducteur: Ce glossaire est déstiné avant tout aux novices.C'est pourquoi,je me suis permis de completer
certaines définitions parfois peu explicites.

Appendice: Glossaire de termes de sécurité

Conditios génétrales d'utilisation

Acceptable Use Policy (AUP)

Il s'agit d'un ensemble de règles et de directives qui spécifient de mainière plus ou moins détaillée les attentes en terme de droits d'utilisation des systémes ou des réseaux.

Compte

voir compte informatique.

Identifiants Anonymous et Guest

Services accesibles sans aucune forme d'identification.Ce qui est la pupart du temps le cas ,avec le protocole, qui autorise les accés anonymes(il est d'usage pour ce type de Serveur FTP autorisant l'accés anonyme de s'identifier en tant que Anonymous et d'inserer son mail en guise de mot de passe,ainsi l'acces au serveur FTP vous est autorisé).D'autres systémes mettent à disposition des usagers un compte spécial nommé "Guest"(litteralament 'invité'),pemettant d'acceder auxservices de maniere restreinte.

Outils d'audits.

Outils servant à analyser les systemes réseau ou d'ordinateurs,afin de déterminer le niveau de sécurité ou la fonctionnalité de l'ensemble des services fournis.COPS (Computer Oracle Password and Security analyzer) et SATAN (Security Administrator's Tool for Analyzing Networks)en sont deux exemples tres populaires.Un lien qui vous en dira un peu plus sur l'audit informatique actuel.

http://www.institut.capgemini.fr/seminaires/ADT.html

Authentication ou Identification

Authentication se refere à un Processus permettant de vérifier l'identité déclarée d'une personne ou de toute autre entité.Ce mecanisme d'identification nécessite un nom d'utilisateur et un mot de passe comme preuve de l'identité de l'usager.

Réseau administré centralement

Réseau de systémes qui à la responsabilité d'un unique groupe d'administrateurs qui ne sont pas repartis mais qui travaillent centrallement pour prendre soin du réseau.

Certifiats

Les Certificats sont des données qui sont utilisées pour vérifier les sigantures numériques. Un certificat n'est digne de confiance que si l'entreprise l'utilisant en est l'auteur.un certificat sert verifier un article particulier signé, tel qu'un courrier éléctronique ou une page Web. La signature numérique,l'article et le certificat sont tous élaborés à l'aide de programmes mathématiques.On peut deduire , si la signature est valide, que "Selon l'entreprise qui est à l'origine de ce certificat, le signataire était (un nom)".

Systeme propre

Un ordinateur qui à été installé récemment avec son système d'exploitation et ses logiciels acquis depuis une distribution média reconnue. Comme souvent, des logiciels et de nouvelles configurations sont apportées à un ordinateur,il devient de plus en plus difficile de déterminer si l'ordinateur est propre ou à été compromis par des virus et des cheveaux de troie, ou encore une mauvaise configuration réduisant sensiblement la sécurité du système.

Client

Tout dépend du point de vue, un client peut être un ordinateur dont se sert un utilisateur final afin d'accéder à un service hébergé sur un autre ordinateur appellé 'Serveur'.
Le 'Client' peut aussi faire référence à un programme ou à une partie du système utilisé par l'usager-final pour accéder à un programme ou à un service fournis par un autre programe.(Par exemple, un navigateur Innternet est un client qui acceéde aux pages misent à disposition par un serveur Web).

Document composite

Un document composite est un fichier contenant ('un ensemble de)des données.Les fichiers sont composés de multiples
parties:un document pur, un document chiffré, un document numérique signé, ou des documents compressés.
Ces fichiers composés de differentes parties de documents sont connus comme 'documents composites' et peuvent requerir
un multitude de programmes nécessaires à leur interpretation et manipulation.Ils peuvent être utilisés sans connaissances spécfiques de l'utilisateur.

A propos des documents composites on peut egalement trouver cette définition:
Déf. :
Document contenant des données de nature différente (texte, graphique, image, son, voix, etc.) qui ont été créées par plusieurs applications et qui
peuvent être soit incorporées dans le document, soit liées au document en question, auquel cas elles sont mises à jour automatiquement à l'intérieur du document,
en même temps qu'elles le sont dans le document source.

Note(s) :
Un document composite est, en fait, un document cible (« destination document ») considéré par rapport à son contenu. Cela peut être : un document créé par un logiciel de
traitement de texte qui contient un graphique créé par un tableur; une page Web; un message électronique auquel on a joint un fichier; etc. Pour l'utilisateur final, le document apparaît comme un seul et même document.
On rencontre parfois « document composé », « document mixte » ou « document hétérogène » comme équivalents de « compound document », mais l'expression consacrée est « document composite ».

Compte(informatique)

Ce terme décrit l'autorisation nécéssaire permettant d'accéder à un systéme informatique ou à un réseau.
Chaque utilisateur-final possède un compte, qui consiste le plus vraisemblablement en une combinaison d'un nom d'utilisateur et d'un mot de passe,ou d'une toute autre preuve que l'usager est bien la personne assignée à ce compte.

Configuration de services réseau.

Une partie des taches de l'adminstrateur qui consiste à spécifier les conditions et détails des services réseau, qui dirigent le déploiement des services .Concernant un serveur Web,ce deploiement implique les attributions des droits d'acés utilisateurs (detreminer quels pages webs seront accesibles pour une categorie d'utilisateur donnée), et le type d'informations retenues pour les futurs remaniement du serveur.

Cookies

Enregistrement d'infomrations dans les cookies s'effectuent lors de vos visites sur les sites webs et sront utilisées lors de votre prochain passage par le serveur.le serveur peut recevoir les infomrations de cookies provenant d'autres sites webs,ce qui bien entendu constitue une atteinte à votre vie privée .

Cracker

Ce terme est utilisé pour décrire ,les agresseurs, les intrus et autres sales mecs ,qui ne respectent pas les règleset essaient de contourner les dispositifs de sécurité et /ou s'en prendre aux particuliers ou entreprises.

NB:la notion de cracker se révelant parfois ambigue voici une définition plus complete pechée dans un dictionnaire.

Déf. :cracker=pirate informatique

Criminel informatique qui exploite les failles dans une procédure d'accès pour casser un système informatique, qui viole l'intégrité de ce système en dérobant, altérant ou détruisant de l'information, ou qui copie frauduleusement des logiciels.

Note(s) :
Le piratage informatique peut prendre trois formes :
a) copie frauduleuse de logiciels;
b) pénétration des réseaux et banques de données;
c) introduction d'antiprogrammes pour contaminer les systèmes.

Le cyberpirate est un pirate informatique qui se manifeste et effectue ses attaques malveillantes essentiellement dans Internet.
L'utilisation en anglais du terme hacker dans le sens de « pirate informatique » prête à confusion.
En effet, même si, sous l'influence de la presse, hacker a été et est encore utilisé comme équivalent de cracker, il désigne avant tout le bidouilleur qui, lui, n'est pas un criminel informatique.
Les termes anglais hacker et cracker, fréquemment utilisés en français dans le sens de « pirate », peuvent aisément être remplacés par pirate informatique.

Daemons (inetd, talkd, etc.)

Il s'agit de processus qui tournent sur un système informatique pour mettre à disposition des services
d'autres systèmes informatiques.Généralement les "Daemons sont considérés comme des "serveurs".

Decrypting

Il s'agit du processus qui consiste à decrypter un fichier ou un message chiffré pour en restituer les données originales(afin evidemment de les utiliser).

Compte par défaut

Certains systemes et logiciels serveurs sont livrés préconfigurés .
Ces comptes peuvent être livrés parametrés avec un mot de passe et un nom d'utilisateur définis à l'avance pour permettre un acces complet et pratique à tous utilisateurs lors de la connexion initiale. Il est toutefois conseillé de désactiver le compte par défaut, ou de changer les identifiants de connexion dans un soucis de minimiser les problèmes de securité de votre systéme.

Numéroteur téléphonique.

Un moyen qui permet d'acceder à un systeme distant ou à un réseau via un réseau de télcommunications téléphoniques.L'ordinateur utilise un modem pour composer un appel téléphonique vers un autre modem,qui en contrepartie fournis l'acces internet. Voir egalement PPP

Signature éléctronique(ou certificats éléctroniques).

Une signature éléctronique est crée par un programme informatique de mathématiques.Il ne s'agit pas d'une signature écrite, ni d'une représentation infographique de celle ci.La signature est comme une cachet de cire, qui pour être produite requiert un tampon particulier; cette signature est généralement attachée à un email ou un fichier.L'origine du message ou du fichier peut être verifié par la signature numerique(à l'aide d'un outils particulier).

Logiciels téléchargés

Il s'agit d'ensembles de logiciels recuperés depuis l'Internet (en utilisant, par exemple le protocole FTY).

Télécharger

L'acte de récuperer des fichiers depuis un serveur sur le réseau.

Progiciel de messagerie.

Pour communiquer par messagerie éléctronique, l'utilisateur final utilise habituellement un client email qui fournit l'interface utilisateur pour créer, envoyer, récuperer et lire des messages éléctroniques.Differents logiciels de méssagerie fournissent le même ensemble de fonctions basiques, mais disposent de differentes interfaces utilisateurs et peut être de fonctions spéciales.Des packs de messagerie proposent le chiffrement et la possibilité de signature numérique.

Logiciels de sécurité pour la messagerie.

Logiciels qui proposent les signatures numériques et le chiffrement(et déchiffrement)pour activer la protection des messages et documents prioritaires pour l'envoi vers un réseau potentiellement nonsécurisé.PGP est un exemple de ce type de logiciels.

Cryptage/decryptage(ou chiggrage/dechiffrage)

Il s'agit d'un procédé mathemathique qui brouille les données afin d'en assurer la confidentialité.

Logiciel de chiffrement.

logiciel qui fournis pour les utilisateurs finaux les fonctionalités requises pour le cryptage et décryptage de messages et fichiers.PGP en est un exempler.

Utilisateur-Final

Un(humain) individus qui utilise les systemes informatiques et les réseaux.(En gros vous !!)

Fichiers (programmes, données, texte et bien plus encore).
Les fichiers comportent les données des utilisateurs,mais aussi les programmes, les systèmes d'exploitation et les données de configuration systeme.

Fichiers serveurs.(fichiers d'echanges????)

Un système informatique qui propose un moyen de partage et de travail sur les fichiers systèmes stockés, entre les usagers ,avec acces à ces fichiers sur le reseau.

Transfert de fichiers.

Le processus de transfert de fichiers entre deux ordinateurs sur un réseau, utilisant un protocole tel que FTP ou HTTP.

Correctifs , Patchs et leurs installations.

Les distributeurs en réponse à la découverte de vulnérabilités compromettant la sécurité de leur systéme propose un ensemble de fichiers qui doivnet être installés sur le terminal informatique.Ces fichiers 'corrigent' ou 'patchent' le systeme d'exploitation ou le logiciel pour éliminer les vulnérabiltés liées à la sécurité.

FTP (File Transfer Protocol)

un protocole qui autorise le transfert de fichiers entre un client FTP et un serveur FTP.

Groupe d'utilsateurs

Les logiciels de sécurité informatique permettent souvent le paramétrage de permissions pour des groupes (d'utilisateurs),à l'opposé des usagers individuels.

Assistance technique

Un support technique qui peut être appellé pour obtenir de l'aide lors de difficultés avec un ordinateur ou lors de problemes de communication.

Internet

Un collectifs de réseaux interconnectés qui utilise un ensemble de protocoles communs appellés pile TCP/IP ,qui active les communications entre les ordinateurs connectés.

Tiers de confiance," Key Escrow"

Clés qui sont utilisés pour crypter et decrypter les fichiers.La clé fiduciaire est utilisée pour stocker les clés qui seront utilisés par une tierce partie afin d'acceder aux données à l'interieur du fichier chiffré.

Clé utilsés pour crypter et decrypter des fichiers

Pour utiliser le cryptage, un utilisateur final doit fournir quelques secrets, sous forme de données plus communement appelées cléfs

Connexion, connexion a un systéme.

Il s'agit d'une action conduite par l'usager lorsqu'il s'identifie sur son systeme.

Boite dialogue de connexion.

Les caractères qui sont affichés quand on s'identifie en vue d'une connexion pour demander à l'usager son nom et mot de passe.

Connexion

Si un utilisateur s'est convenablement authentifié sur un systéme, et béneficie alors d'un accés legitime il est consideré comme connecté.

Connexion

Les logiciels systemes et serveurs disposent souvent d'une fonction permettant de recenser les evenements.Ces evenements peuvent être configurés afin d'être inscris dans un fichier connu en tant que fichier log. Le fichier log peut etre consulté ulterieurement et permettre d'identifier les dysfonctionnments du systéme et les failles de sécurité.

Masquerade (see Remote Log In)

L'acte d'une personne qui pretend être une autre personne afin d'obtenir un accès à un compte utilisateur constitue une 'masquerade'.Ce peut être accomplis en fournissant un faux nom, ou en volant les mots de passe d'une autre personne et en se connectant sur le compte de cette même personne.

Network File System (NFS, Partage de fichiers sur PC, etc.)

NFS est une application et une suite de protocole qui met à disposition une méthode de partage de fichiers entre les clients et les seveurs .Il existe d'autres protocoles qui disposent de fichiers d'accés sur le réseau.Ils fournissent des fonctionalités similaires mais n'interagissent pas entre eux

Fonctionalités réseaux des logiciels.

Quelques logiciels possèdent des caracteristiques qui leur permettent de récuperer des fichiers partagés depuis le réseau.Il ne semble pas toujours évident que des logiciels disposent de fonctionnalités orientées réseaux.

Services Réseaux

Services qui ne sont pas fournis sur l'ordibnateur local qu'utilise l'usager mais sur un serveur situé sur le réseau..

Mot de passse à usage unique:One-Time Passwords (OTP)

Au lieu d'utiliser le même mot de passe encore et toujours, un mot de passe different est attribué sur chaque sous sequence de connexion.

Passphrase

Un passphrase est un long mot de passe .Il est souvent composé de plusieurs mots et symboles qui le rende plus difificile à deviner.

Ecran de veille protegé par un mot de passe

Un écran de veille bouche l'affichage habituel d'un moniteur.Un écran de veille protegé par mot de passe peut seulement être désactivé si le mot de passe de l'usager est inseré.Ce qui empeche un systeme connecté d'être abusé et de caché le travail effectués des visiteurs.

Patch

Voir "correctifs, Patchs et leur installation"

Permissions

un autre mot pour le contrôle d'accés qui est utilisé pour controler les accés aux fichiers et autres ressources.

PGP (Pretty Good Privacy)(Assez Bonne confidentialité)

PGP est une application qui fournit les outils pour chiffrer et signer numériquement les fichiers sur les terminaux informatiques. Il s'avère particulièrement utile pour chiffrer et/ou signer numeriquement les fichiers et messages avant de les envoyer par Email.

Les modules Plug-in

Composants logiciels qui s'integrent aux autres logiciels(comme par exemple les navigateurs Internet)pour proposer de nouvelles fonctionalités.

Le referent securité

En cas de failles de sécurité ou de problèmes, de nombreuses organisations disposent d'un réferent qui peut alerter les autres et prendre les mesures appropriées.

PPP (Point to Point Protocol)

PPP est la mécanisme par lequel la plupart des utilisateurs établissnet leur connection réseau entre leur PC et leur fournissuer d'acces Internet.une fois connecté, le Pc est capable de transmettre et de recevoir des données depuis n'importe quel autre systeme sur le réseau.

Programes liés à la confidentialité.(Privacy Programms)

Un autre terme concernant les logiciels de chiffrement qui mettent en avant leur utilité pour assurer la confidentialité et par consequent la vie privée de l'utilisateur final qui l'utilise.

Logiciel d'accés à distance Remote Access Software

Ce logiciel permet à un ordinateur d'utiliser un modem pour se connecter à un autre système(hyperterminal sous WIN98).Il autorise également un ordinateur à mettre en attente les appels vers un modem (Cet ordinateur dispose du service d'acces distant).Les logiciels d'acces distant peuvent tres bien disposer d'acces vers un oridnateurunique ou un réseau unique.

Connexion distante

Si un utilisateur final utilise une connexion distante pour s'identifier sur un système cette acte est consideré comme une connexion distante.

Security Features

Il s'agit de carcateristiques qui fournissent des protections ou permetteent aux usagers ou administrateurs de tester la sécurité de leur systeme , par exemple a l'aide d'audit.

Chartre sécurité.

une chartre de sécurtité est écrite par les organistations pour piloter la politique de securité,sous la forme de "à faire" "à ne pas faire".Ces directives et régles sont valables pour les usagers sans contradiction avec la notion de sécurité physique,de securité des données,et de la sécurité des informations ainsi que de son contenu(EX:les règles établissent que les sites à caractère sexuel ne devraient pas être visités, et que les droits d'auteur devraient être honorés lorsque vous télécharger des logiciels,etc)..

Serveur

Un serveur est un système, ou un ensemble de processus sur un ordinateur fournissant des services à des clients a travers les réseaux.

Compte partagé

Un compte commun est celui qui est partagé par un groupe d'utilisateurs, à l'opposé d'un compte normal qui est disponible pour simplement un usager.
Ci ce compte est utilisé à tort , il est trés dificile voir impossible de savoir quel usager en est reponsable.

Permissions de partage .

La plupart des ordinateurs permettent aux utilisateurs de partager de fichiers sur le réseau.Ces systémes mettent à disposition un méchanisme pour les usagers destiné à controler qui à le droit de lire ou d'editer les fichiers.

Site

Cela depend du contexte dans lequel ce terme est utilisé, il peut être attribué a un groupe de terminaux informatiques regroupés dans un même endroit geographique, une organisation

juridique, ou une adresse du réseau.Un site se refere typiquement à un réseau d'une administration commune.

SSH (Secure Shell)

SSH fournit un protocole entre le client et le serveur,permettant une connexion distante sécurisée.

SSL (Secure Sockets Layer)

Ce protocole propose des services de securité pour d'une part sécuriser les protocoles utilisés sur le réseau.SSL est couramment utilisé par des navigateurs web pour chiffrer les données envoyées et téléchragées depuis un serveur.

Administrateutrs systèmes.

L'individu qui assure le bon fonctionnement du système et qui possède les privilèges d'administrateurs.Afin d'eviter les erreurs commises les sessions de connexion administrateur devraient se limiter au minimum.

Priviléges d'administrateurs systémes.

Le travail des administrateurs systémes implique qu'ils disposent de plus de droits ,de permissions exceptionelles sur les fichiers systéme.

Fichiers systémes.

Un ensemble de fichiers sur un système qui n'appartiennent pas aux usagers,qui pilote les fonctionalités du systéme.Les fichiers systèmes ont un impact trés important sur la sécurité informatique..

Telnet

Un protocole qui permet une connexion distante à un autre oridnateur sur le réseau.

Terminal

un mécanisme muet(orienté texte) qui est connecté à un ordinateur ,et qui permet aux utilisateurs et administeurs d'acceder à ce même ordinateur

Terms of Service (TOS)

Voir "Acceptable Use Policy (AUP)".

Menace

La possibilté qu'une vulnerabilité puisse être exploitée et compromettre la sécurité des sytémes sur le réseau.Même si une vulnerabilté n'est pas connu,cela représente un menace en soi.

les cheveaux de troie

Un programme qui comporte en lui un processus permettant au createur du programme d'acceder au systeme et de l'utlilser.

Virus

Un programme qui se propage et se multiplie sur les systémes informatiques,et contenant en soi (secretement et perfidement) un autre programme.Un virus peut être transmis sur un terminal informatique par differents moyens.

Antivirus

Logiciel qui detecte et detruit dans la mesure du possible les virus presents sur les terminaux informatique.Cet outil alerte egalement l'utilisateur.

Vulnerabilités

Une vulnérabilité est la présence d'une faiblesse, dans la conception, ou d'une erreur d'implemmentation qui peut conduire à un fatal et indésirable dysfonctionement qui compromet la sécurité du systéme, du réseau, de ces applications et des protcoles concernés.

Cache du navigateur internet

Il s'agit d'un fichier système qui est utilisé pour stocker des pages web et les fichiers relatifs.Il peut être utiliser pour récharger réafficher les dernieres pages web ou fichiers visitées plutôt que de les recharger a chque fois que vous vous connectez au réseau.

Web Browser Capabilities(competences du navigateur web)

L'ensemble de fonctiopnnalités qu'un navigateur web est en mesure d'offir pour l'usager.Cela tient compte egalement de l'ensemble des plug-ins livrés avec.

Serveur Web

Un programme serveur qui propose un accés aux pages web.Des serveurs web proposent des accés à d'autres services,telles que les bases de données,et les repertoires.

Vers

Un programme informatique qui se propage et se multiplie.Les vers à l'opposé des virus sont concus pours se multiplier et se propager dans les environnements réseaux.

Remerciements

Le manuel de référence sur la sécurité à été realisé grâce à l'effort conjoint du groupe de travail du manuel de réference en matiere de sécurité informatique de l'IETF.
Il y a également d'autres personnes qui ont contribués de manière considérable à l'élaboration de ce document.---Simson Garfinkle et Eric Luiijf ont fournis des informations trés importantes pour ce document.La contribution de Klaus-Peter Kossakowski à été également trés appreciée pour le glossaire.

References

[GLOSSARY] Malkin, G., Ed., "Internet User's Glossary", FYI 18, RFC 1983 August 1996.

[RFC2196] Fraser, B., Ed., "Site Security Handbook", FYI 8, RFC 2196 September 1997.

Egard pour la sécurité.

ce document traite des atitudes à adopter pour accroître et préserver la sécurité de leur systéme.

Authors' Addresses

Erik Guttman
Sun Microsystems
Bahnstr. 2
74915 Waibstadt
Germany

Phone: +49 7263 911701
EMail: erik.guttman@sun.com

Lorna Leong
COLT Internet
250 City Road
City Forum, London
England

Phone: +44 171 390 3900
EMail: lorna@colt.net

Gary Malkin
Bay Networks
8 Federal Street
Billerca, MA 01821
USA

Phone: +1 508 916 4237
EMail: gmalkin@baynetworks.com

Full Copyright Statement