Université de Picardie Jules Verne.

.....

Diplôme d'Etude Superieure Spécialisée

.....

Spécialité : Ingénierie Système et Reseau Informatique

option : compétences complémentaires

Etude et Recherches : Etude individuelle

<u>Thème</u> : La Cybercriminalité

Présenté par **YELEMOU Tiguiane**

Année universitaire 2004/2005

Sommaire

I.Introduction..... 3
I.1.Définition :..... 3
II.Les enjeux de la cybercriminalité..... 4
II.1. L'ampleur de l'usage de l'Internet..... 4
II.2. Les menaces sur les outils critiques de l'Internet : cas du BGP.....6
II.3. La cybercriminalité en chiffres 8
III. Quelques infractions commis sur Internet..... 10
III.1. La pornographie..... 10
III.2. Le phishing.....11
III.3. Problématique de l'accès libre à la connaissance sur la toile..... 12
IV. Des solutions au problème de la cybercriminalité.....15
IV.1. Les solutions techniques..... 15
IV.2. Des mesures politico-juridiques.....20
Conclusion..... 22
Références bibliographiques.....23

I. Introduction

I.1.Définition :

Ces dernières années, les techniques de l'information et les réseaux de communication ont connu une évolution extrêmement rapide. Aujourd'hui, du moins dans les pays occidentaux, Internet est devenu un outil aussi indispensable que courant. Il permet d'appeler des informations à partir de chaque raccordement au réseau et où que l'on soit dans le monde. Toutefois, Internet a aussi un revers de la médaille puisqu'il permet de commettre des infractions de n'importe quel point du globe. Le terme de « cybercriminalité » est un mot générique définissant l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunications en général et plus particulièrement sur les réseaux partageant le protocole TCP-IP, appelés communément l'Internet. La cybercriminalité recouvre deux types d'infractions pénales :

- les infractions directement liées aux technologies de l'information et de la communication (TIC) dans lesquelles l'informatique est l'objet même du délit,
- et les infractions dont la commission est liée ou facilitée par les TIC et pour lesquelles l'informatique n'est qu'un moyen.

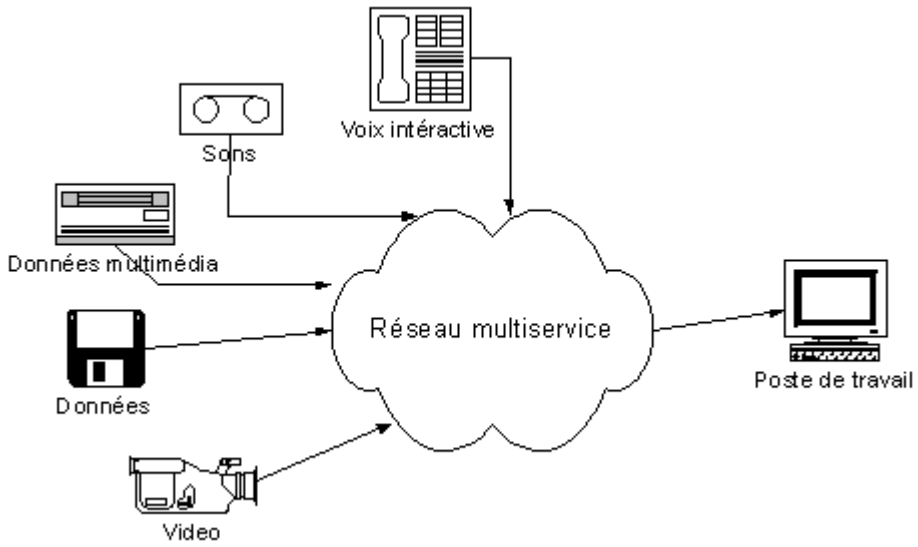
Nous allons dans un premier temps présenter les enjeux de la cybercriminaté, ensuite les differentes formes de crimes commis et enfin nous analyserons les solutions actuelles deployées pour y faire face.

II. Les enjeux de la cybercriminalité

II.1. L'ampleur de l'usage de l'Internet

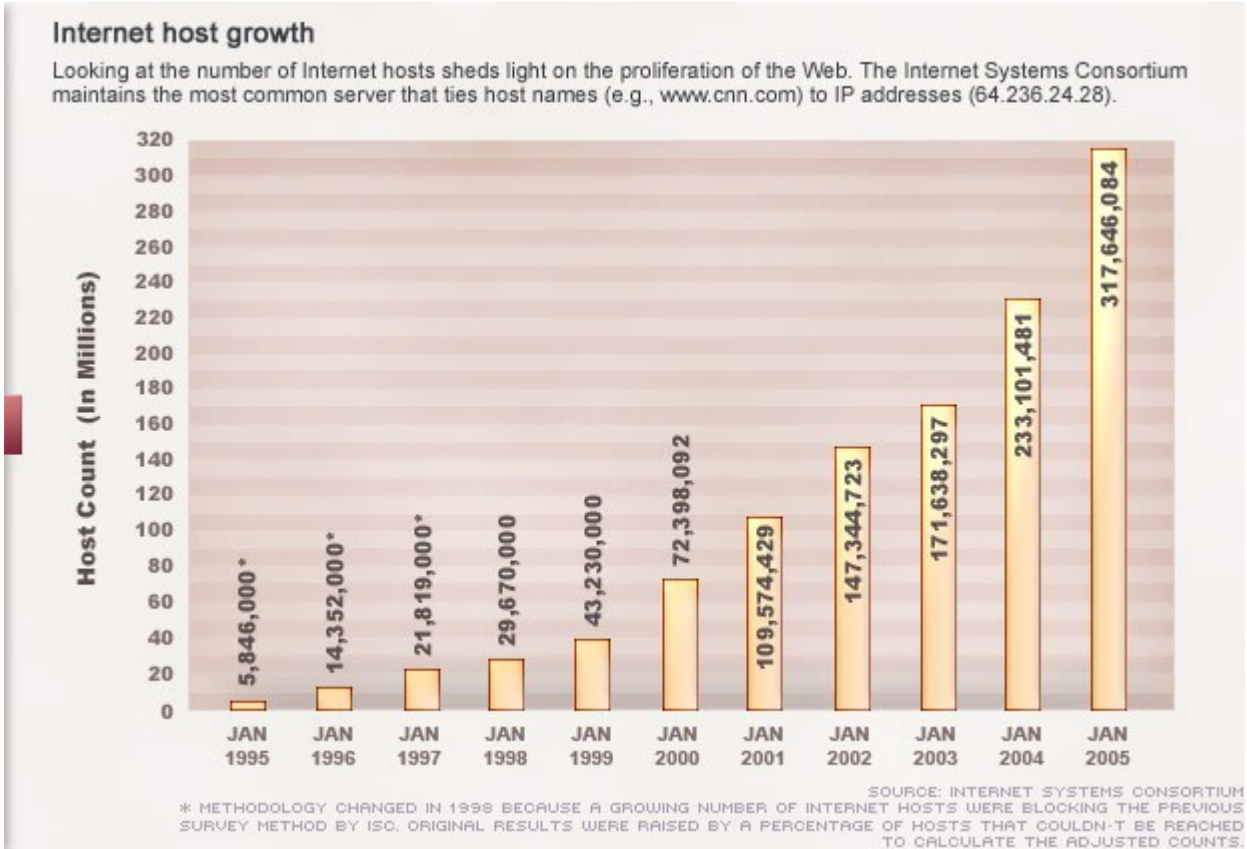
La globalisation des médias et la technologie numérique avec ses implications directes sur l'information et la communication ont généré une nouvelle culture, de nouveaux comportements, de nouveaux modèles et de nouveaux concepts.
Ainsi, la technologie de l'information et de la communication, la société de l'information, la société civile, la fracture numérique, la gouvernance (dans tous ses états), l'Internet, l'Intranet, le virtuel, l'économie basée sur le savoir, la gestion et le management du savoir, la culture électronique (e-gouvernance, e-banking, e-commerce, e-learning, etc.) sont le produit de la jonction entre la révolution numérique et la globalisation des moyens d'information. Beaucoup plus, la convergence entre les télécommunications, l'informatique et l'audiovisuel a elle aussi inauguré une nouvelle ère technologique, celle des fils et des courts-circuits remplacés par des bits et les données et où l'écran a un rôle alternatif en tant que PC ou poste téléviseur. En somme, les communications traditionnellement transmises par les courts-circuits se sont déplacées sur le nouveau protocole Internet et son réseau, ouvrant la voie à la « nouvelle imagerie technologique ».
De nos jours, l'informatique fait partie intégrante de la vie quotidienne. Les ordinateurs sont devenus des outils indispensables qui concernent toutes les activités depuis la gestion et la production des entreprises jusqu'à l'administration de l'Etat.
Mais cette nouvelle technologie a également engendré des formes d'abus et de délinquance spécifiques si bien qu'il a été nécessaire d'instaurer une législation appropriée à cette nouvelle criminalité.
La cybercriminalité comprend à fois des crimes particuliers faisant intervenir des ordinateurs et des réseaux (comme le piratage), et la facilitation de crimes traditionnels grâce à l'utilisation d'ordinateurs (pornographie juvénile, crimes haineux, télémarketing frauduleux via Internet). Outre la cybercriminalité, il y a les « crimes assistés par ordinateur », qui impliquent l'utilisation d'ordinateurs par des

criminels pour les communications et l'entreposage de documents ou de données. Bien que ces dernières activités ne soient pas nécessairement illégales, elles permettent aux autorités d'obtenir de précieux renseignements dans les enquêtes sur des crimes véritables. La technologie informatique présente de nouveaux défis à la politique sociale à propos de questions telles que la vie privée, pour ce qui concerne l'exploration de données et les enquêtes criminelles.



MultiUsage du numérique

L'évolution de l'Internet



II.2. Les menaces sur les outils critiques de l'Internet : cas du BGP

Le BGP (Border gateway Protocole), protocole de routage entre systèmes autonomes , est un outil critique pour le bon fonctionnement de l'Internet *[21]*. Mais il est exposé actuellement aux pirates vu qu'il présente de nombreuses vulnérabilités entre autre le manque d'authentification requise entre pairs BGP et de mécanisme simple pour la vérification de la pertinence des informations trouvées dans les messages *[22]*. Ces deux grandes classes de vulnérabilités sont amplifiées par le fait que BGP ne dispose d'aucune vérification et sécurisation cryptographique du flux TCP : il est dès lors possible d'intercepter, modifier, insérer, rejouer, un flux BGP pour exploiter les deux grandes classes précédentes. Les risques associés à ces vulnérabilités sont nombreux :

- ✓ **Déni de service direct sur le routeur** : tout routeur BGP peut être la cible d'un déni de service classique tel que le SYN flood. Le routeur est alors soit complètement planté, soit très lent. Dans ce cas, il ne peut indiquer en temps voulu à son pair qu'il est toujours en vie (message Keepalive). En cela, le pair considère que le routeur est planté, et purge toutes les routes associées. Une nouvelle session est alors négociée par un des pairs, et l'attaque peut recommencer. La faisabilité d'une telle attaque est haute si le routeur n'est pas particulièrement protégé ou dimensionné, notamment au niveau de sa file d'attente des connexions en cours de négociation.
- ✓ **Réinitialisation (RST) de la session BGP entre les pairs** : la session BGP étant transportée sur un flux TCP classique, on peut envisager la réinitialisation de cette connexion par envoi (spoof) de paquets RST savamment choisis. Il en résulte alors comme précédemment la purge des routes associées au pair, puis la tentative de redémarrage d'une session.
- ✓ **Spooling complet de session** : on crée en aveugle de toutes pièces une session de peering BGP avec une victime, vers laquelle on peut injecter des routes, en enlever,...
- ✓ **Hijacking de sessions existantes** : variation de l'attaque précédente, mais au lieu de créer complètement une session, on réinitialise une session existante

entre deux peers dans laquelle on injecte des paquets de type *update* ou *notify*.

- ✓ **Désagrégation** : en BGP, les préfixes plus spécifiques (c'est à dire plus longs) sont prioritaires. Ainsi, une annonce pour un réseau /24 à l'intérieur d'un /16, et une seule annonce /24 sera gardée pour le préfixe correspondant. Un agresseur peut donc complètement désagréger un grand réseau en envoyant des annonces pour des parties de ce grand réseau. Ces annonces, plus spécifiques vont être prises en compte et le réseau va être complètement partionné en fonction des annonces faites. Le risque associé est principalement un déni de service, mais on peut imaginer qu'un agresseur extrait, d'un réseau important, une petite plage contenant des serveurs sensibles, qu'il fait renvoyer chez lui (voir les attaques suivantes). Notons à propos de la désagrégation l'expérience AS7007 en avril 1997 où un modeste prestataire FLIX[1] *[FEK2004]* a désagrégé pratiquement l'Internet, rendant ainsi le réseau des réseaux inopérant pendant deux heures et fortement perturbé pendant toute la journée. En effet, FLIX a effectué une erreur de configuration sur son routeur, aboutissant à ce qu'il annonce les meilleures routes pour l'Internet entier. Il a annoncé des routes en /24 pour la plupart des blocs CIDR avec pour AS_PATH son propre numéro d'AS. Ces annonces se sont propagées à travers Internet par les sessions eBGP. Par conséquent, le trafic a été détourné vers l'AS 7007 et la taille des tables de routage a considérablement augmenté. Cette augmentation a fait effondrer certains routeurs et a causé des ruptures de service sur les segments de l'Internet.
- ✓ **Injection de routes** : les préfixes annoncés n'étant pas systématiquement vérifiés par le pair, il est possible d'annoncer à son pair un préfixe pour lequel on n'a pas autorité. Couplé avec le principe de priorité des préfixes vu précédemment, un agresseur peut annoncer le préfixe contenant sa victime. Tout le trafic venant de la zone touchée par l'annonce et destiné à la victime

1 FLIX : Florida Internet Exchange, AS 7007

sera routé vers l'agresseur, qui aura tout le plaisir sur la suite (abandon complet donc déni de service, manipulation des données avant réexpédition vers la victime, masquera du serveur,...)

II.3. La cybercriminalité en chiffres

19 Janvier 2005 Le Clusif (Club de la sécurité des systèmes d'informations français) a publié jeudi dernier un panorama retraçant l'activité de la cybercriminalité dans le monde au cours de l'année 2004. Une année marquée par une forte croissance des activités à seul but d'enrichissement personnel illustrées par le vol de données, le chantage ou encore l'espionnage industriel.*[22]*

En matière de vols d'informations, le Clusif cite les exemples de l'affaire Microsoft, survenue en février 2004, où l'éditeur retrouve - en libre accès sur Internet - le code source de Windows 2000 SP1 et NT 4.0 Service Pack 3. L'un de ses partenaires sera plus tard identifié comme l'origine de la fuite. Une affaire à mettre en parallèle avec celle qui touche Cisco en mai 2004. Un site russe détaille alors les spécifications du code source de certains routeurs de la société.
Ces vols plus médiatisés que ceux de la Wells Fargo ou de Jolly Technologies peuvent ensuite faire l'objet de commerce en ligne comme le pratique le Source Code Club début juillet ou l'exploitation de failles pour s'introduire sur les réseaux souhaités. Des failles qui, combinées avec la croissance des logiciels espions et des logiciels publicitaires, constituent le second événement marquant de l'année 2004, selon le panorama du Clusif.
L'explosion des codes malveillants capables de "renifler" des informations confidentielles constituent un intérêt double pour les cybercriminels. D'une part, ils peuvent donner lieu à du vol d'informations confidentielles, *phishing* par exemple, et d'autre part, certains laissent une porte ouverte vers le poste de l'internaute afin d'exploiter la machine à l'insu de l'internaute pour une attaque en déni de service par exemple. Le Clusif rappelle qu'il est nécessaire de distinguer les logiciels publicitaires des logiciels espions ou encore des robots et des vers.

Si les premiers prêtent parfois à confusion en raison de leur caractère intrusif, les seconds posent de réels problèmes de confidentialité, les deux derniers programmes étant clairement offensifs. Une menace qui reste ignorée du grand public, d'après le Club professionnel, mais clairement exploitée par les pirates. Ainsi selon l'étude, un réseau de 20 000 proxy se loue 75 euros la semaine et, en échange de 38 euros par mois, il est possible de recevoir une liste des proxy ouverts. Pour accéder à 500 *bots*, le prix peut monter jusqu'à 380 euros.
Dans le domaine du chantage, l'année 2004 aura été marquée par le cas SoftBank. Le fournisseur d'accès Internet japonais doit verser 28 millions de dollars en échange de la non-divulgation des données personnelles de ses clients. Le coût total du dédommagement de ses clients se monte au final à 36 millions de dollars. En mars, c'est au tour de Google d'être victime d'un chantage auprès de son logiciel de publicité. Un pirate se dit être en mesure de détourner le nombre de clics générés et demande 150 000 dollars à la société.

Le panorama se termine par la menace future, celle venue des réseaux sans fil. Avec la convergence des différents environnements mobiles (Bluetooth, Wi-Fi, 3G…), les réseaux sans fil deviennent des proies de plus en plus attirantes pour les cybercriminels.
Le Clusif met ainsi en avant l'augmentation des débits proposés mais aussi des applications et des utilisateurs. Les failles présentes dans les technologies Bluetooth, Wi-Fi et dans les protocoles de voix sur IP donnent aux pirates les moyens de produire les premiers virus mobiles,

III. Quelques infractions commis sur Internet

La cybercriminalité se décline en trois modes différents :

- Les infractions relatives au **contenu** se définissent comme la diffusion intentionnelle par Internet de textes ou d'images illégaux. Les deux infractions principales concernent la diffusion de matériels, d'insultes à caractère raciste, xénophobe ou négationniste, et la pédopornographie.

- L'atteinte à la **propriété intellectuelle** illustrée notamment par la mise en ligne de fichiers musicaux gratuits sans l'accord des auteurs, interprètes ou producteurs.

- Les infractions liées aux **technologies de l'information et de la communication.** Les infractions informatiques sont des atteintes délibérées aux réseaux et bases de données, ou la diffusion de virus ainsi que les trafics relatifs aux mots de passe ou code d'accès. Il peut s'agir également de fraudes aux cartes bancaires et de recueil illégal de données bancaires qui permettent d'accomplir des escroqueries en ligne, ou bien d'interception de correspondances privées utilisant un support informatique.

Nous allons à travers trois analyses illustrer ce phénomène.

III.1. La pornographie

L'exploitation sexuelle des enfants, la pornographie impliquant les enfants et la pédophilie sur Internet revêtent désormais une dimension internationale. Par le satellite, le câble et Internet, ils concernent toutes les couches de la société, touchent tous les continents et menacent des enfants qui devraient être scolarisés pour contribuer au progrès de leur société. *[33]*

Le monde entier est conscient du fait que les enfants victimes d'actes sexuels implicites ou explicites et qui sont filmés - qu'ils soient photographiés ou enregistrés par des caméras numériques - dans un but lucratif et pour une diffusion commerciale, doivent également faire face à l'avenir à un traumatisme psychologique et à un risque

de maladie. On devrait par ailleurs reconnaître que la diffusion répétée maintes fois de ces documents audiovisuels auprès des publics de plusieurs milliers de personnes pérennise le sentiment de culpabilité de ces enfants.
On estime qu'un grand nombre de filles et de garçons livrés à l'esclavage et au tourisme sexuel en Asie et en Afrique finissent victimes du sida (plus d'un million de cas dans la seule Asie). Un très grand nombre d'entre eux sont tentés par le suicide.

A problème international, solution internationale conjuguant les ressources et l'influence de toutes les parties concernées. A aucun moment, en aucun lieu et sous aucun prétexte l'abus sexuel des enfants ne mérite des excuses. Chaque enfant a le droit d'être protégé de la cruauté, de la négligence et de l'exploitation. Chaque enfant est un être humain qui doit être respecté et traité en tant que tel.

En Algérie, selon Younes Grar *[31]*, président de l'Association algérienne des fournisseurs de services internet, ils sont 750 000 utilisateurs à surfer sur le réseau internet à travers les 4 500 cybercafés et à domicile. Cependant, declara-t-il, on est en droit de connaître les caractéristiques socio-démographiques de ces internautes, les sites visités et la langue utilisée, non pour des objectifs inavoués ou mal-intentionnés mais pour savoir la nature et le degré de l'apport de l'Internet dans la formation, l'éducation et l'émancipation des citoyens. En effet, force est de constater que les quelques observations faites au niveau des cybercafés à Alger laissent entendre que les sites liés au sexe semblent prédominer l'opération de surfing. Alors qu'en pratique, le réseau internet est venu pour réhabiliter les valeurs de connaissance et de savoir et devenir un moyen efficace de liberté, de promotion socioculturelle et de développement économique. *[33]*

III.2. Le phishing

Le **phishing** (contraction des mots anglais « *fishing* », en français *pêche*, et « *phreaking* », désignant le *piratage de lignes téléphoniques*), traduit parfois en « **hameçonnage** », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès

d'internautes. *[32]*

La technique du phishing est une technique d'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique mais la « faille humaine » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.

Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.

Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message a généralement peu de sens puisque l'internaute n'est pas client de la banque de laquelle le courrier semble provenir. Mais sur la quantité des messages envoyés il arrive que le destinataire soit effectivement client de la banque.

Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.).

Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte ou bien d'obtenir ultérieurement les données nécessaires en utilisant intelligemment les données personnelles ainsi collectées.

III.3. Problématique de l'accès libre à la connaissance sur la toile

Mettre à disposition des internautes de certaines informations dans le but de faire vite évoluer la science pose souvent le problème de leurs 'usage à des fins criminelles. Le cas actuellement de génome de la grippe espagnole de 1918 est à la une de l'actualité. Il est objet de debats *[23]*. le génome complet du virus responsable de l'épidémie de "*grippe espagnole"* (H1N1) est aujourd'hui accessible sur Interenet. Il est désormais plus facile de créer et produire ce virus à partir des informations publiées qu'il ne le

serait de créer et produire une bombe atomique, pour un résultat qui pourrait être tout autant, voire plus catastrophique. Beaucoup de personnes estiment que l'o*n devrait traiter le séquençage générique de pathologies virales avec autant de précautions que la conception d'armes nucléaires".* .

Jamais Cascio de WorldChanging, dans un billet intitulé "*la sécurité par la connaissance "*, répond point par point à leur inquiétude légitime. Il réaffirme sa confiance dans la plus grande circulation possible des connaissances en étant rassurant sur la dangerosité relative du H1N1 aujourd'hui. Et de rappeler qu'étudier sa nature, - le H1N1 était aussi une grippe aviaire qui avait muté jusqu'à contaminer les êtres humains -, peut nous permettre de mieux comprendre l'évolution du H5N1 qui nous menace. Pour lui, c'est la libre circulation des connaissances disponibles sur le SRAS (Syndrome respiratoire aigu sévère) qui a permis à un réseau de scientifiques de trouver très vite les moyens de limiter son influence. La disponibilité rapide d'information sur le SRAS a eu pour résultat que de nombreux chercheurs à travers le monde ont été capables de mieux comprendre le virus, de développer et tester des traitements d'une manière plus efficace et rapide qu'ils n'auraient pu le faire autrement.

Caisco estime que la publication du génome de la grippe de 1918 "*est beaucoup plus utile pour ceux qui essaient de nous défendre des pandémies que pour la poignée de ceux qui pourraient essayer de nous attaquer"* . Il va plus loin : "*L'accès ouvert et global aux informations fondamentales sur les virus et les pathologies ne nous met pas en danger, mais renforce notre pouvoir. Parce que les scientifiques ont séquencé et publié le génome de la grippe de 1918, les efforts pour comprendre les mécanismes donneront aux chercheurs un point de départ indispensable pour trouver des traitement et combattre la pandémie à venir."*

Le débat ne repose pas sur l'opposition entre propriété et ouverture, entre libre accès et copyright comme on le voit souvent, mais dépasse le cadre caricatural de la propriété pour interroger l'accès à la connaissance, sa sécurité et sa pérennité. Il pose surtout la question du rôle qu'entretien le secret et la non-information sur la connaissance.

Il manque peut-être à la démonstration convaincante de Jamais Caisco, la preuve irréfutable que la santé publique est mieux garantie par la divulgation du génome que le contraire. L'occasion d'apporter cette preuve sera peut-être donnée par les conséquences et avancées scientifiques que cette publication va permettre en terme de délais de recherche et d'accès par des biologistes du monde entier.

IV. Des solutions au problème de la cybercriminalité

Garantir la sécurité des utilisateurs d'Internet est un élément essentiel dans la protection des droits des personnes, notamment le droit au respect de la vie privée, et dans la croissance du commerce électronique. Par conséquent, le secteur industriel et les pouvoirs publics ont tous les deux besoin de localiser et d'identifier les personnes qui exploitent les réseaux de la technologie d'information à des fins délictueuses. Nous présenterons quelques solutions techniques et des mesures prises par les pouvoirs publics.

IV.1. Les solutions techniques

Du protocole de routage interdomaines BGP

Les alternatives à BGP sont pour l'instant trop complexes à déployer. L'espoir est actuellement porté sur Secure-BGP, actuellement en phase de maturation technologique. S-BGP authentifie les peers et sécurise le flux par un canal Ipsec *[LYN 2003]*. D'autre part, chaque annonce est autorisée par un mécanisme de certification type PKI, dont les autorités pressenties sont des organismes de gestion des blocs d'adresses : ARIN, APNIC, RIPE, Afrinic.

S-BGP n'étant pas encore utilisable en situation réelle, la sécurisation se résume à l'application des fameuses BCP (Best Common Pratices)[2] *[41]*:

- forcer l'authentification MD5 des peers
- filtrer les annonces venant de ses clients, pour vérifier qu'ils annoncent bien les préfixes leur ayant été assignés
- filtrer les annonces sortant de chez soit, pour vérifier que seules les classes possédées sont attribuées
- filtrer les annonces venant d'autres AS, pour vérifier si possible qu'elles correspondent bien aux peers, et sinon qu'elles ne contiennent pas de blocs non assignés
- ....

2BCP : Best Common Pratices

Les firewalls

Le firewall est l'un des moyens les plus fréquents de se protéger : c'est une passerelle entre le réseau de l'entreprise et Internet. C'est un point de filtrage et de contrôle de l'activité de ces réseaux. C'est le firewall qui est chargé d'interdire ou d'autoriser les flux d'informations en entrée ou en sortie. L'objectif du firewall est de protéger le réseau interne de l'entreprise des accès non autorisés provenant de l'extérieur ainsi que de garantir un certain niveau de sécurité entre le réseau internet et les machines extérieures à celui-ci (typiquement dans le cadre d'un VPN, virtual private network).

Concrètement, un firewall est souvent une machine, un serveur avec un logiciel qui fait le pont entre ces deux réseaux (internet - internet ou deux réseaux internes avec des niveaux de sécurité différents). Le logiciel est chargé du filtrage des packets en fonction de leurs caractéristiques : type, source, destination. En outre, le firewall permet également un contrôle au niveau applicatif ce qui permet de bloquer le recours à certains outils non autorisés.

Le chiffrement (cryptage des données)

Le but premier du chiffrement a été bien entendu la garantie de la confidentialité des informations transmises par l'armée et le gouvernement. Avec le développement des réseaux et de l'informatique non militaire, le cryptage s'est fortement répandu. Les enjeux se sont aussi faits plus pressants avec le développement du commerce-électronique qui impliquait la garantie de la sécurité des transactions et notamment de la préservation de la confidentialité des numéros de cartes bancaires. Le chiffrement est très utilisé entre les banques, les entreprises, les organismes financiers et même les particuliers.

Le principe du chiffrement est le suivant : l'idée c'est de tranformer l'information de manière à ce qu'elle ne soit pas compréhensible par une personne non destinataire. Ainsi l'information peut transiter par des canaux publics sans que la confidentialité de la transmission ne soit remise en cause. Il existe plusieurs méthodes de chiffrage :

- Le chiffrement symétrique

La source et la destination de l'information diposent de clé de chiffrement à utiliser avant la transmission de l'information. C'est cette même clé qui va servir à crypter et à décrypter le message.

- le chiffrement asymétrique

Là, il existe deux types de clés : une clé publique qui est à la disposition de tous et qui permet de crypter le message et une clé privée qui seule permet de déchiffrer le message. L'avantage principal de ce type de cryptage est qu'elle évite l'échange de clé même par des canaux publics hautement sécurisés.

A noter que le chiffrement est considéré comme une arme de guerre. En France le chiffrement est autorisé depuis 1999 si la longueur des clés ne dépasse pas 128 bits. Il faut une déclaration préalable auprès des autorités concernées pour toute utilisation de clés de cryptage entre 40 et 128 bits.

SSL (protocole le plus répandu dans la sécurisation des transactions)

SSL signifie Secure Socket Layer et a été créé par Netscape. Sa popularité provient de sa grande facilité de mise en oeuvre et d'utilisation. Il se matérialise par l'apparition d'une petite clé dans le navigateur. Cette clé brisée devient entière si la transaction est sécurisée avec le SSL.

Le SSL est donc un protocole d'échange d'information qui permet de garantir confidentialité, intégrité des échanges ainsi que l'authentification des parties. Le fondement de ce protocole est l'algorithme de chiffrement à clé publique RSA (de Rivest-Shamir-Adleman, ses créateurs). Deux paires de clés - une pour le verrouillage et l'autre pour le déverrouillage - à 40 bits sont utilisées.

SET

Protocole spécialement créé par Visa et MasterCard pour sécuriser les transactions en ligne, son champs d'action se restreint au seul chiffrement des données bancaires alors que SSL permet aussi que crypter images et texte.

Entre en ligne de compte dans le processus de sécurisation trois éléments qui sont le client, le vendeur et la banque du vendeur. Les certificats du client et du vendeurs sont communiqués par leurs établissement bancaire respectif avant que la transaction soit réalisée. Avec ce type de transaction, le vendeur n'entre jamais en connaissance du numéro de carte bleue , une personne malintentionnée ne peut donc pas non plus faire un usage frauduleux de ce numéro.

La détection d'intrusion via un NIDS (Network Intrusion Detection System)

La détection d'intrustion (IDS) complète souvent un Firewall. Elle permet une surveillance en temps réel des réseaux par une écoute permanente couplée à une réponse adaptée en fonction des anomalies. La où le Firewall se contente d'accepter ou de refuser les requêtes, un système de détection des intrusion permet la mise en oeuvre de mesure approriées comme la déconnecton immédiate des intrus, le lancement de programmes ad-hoc ou l'alerte des administrateurs du réseau en cas d'attaque.

L'authentification

Les systèmes d'information sont de plus en plus ouverts vers l'extérieur du fait de l'interconnexion enter les sites à distance, les postes nomades et le réseau principal de l'entreprise. C'est la raison pour laquelle l'identification est devenu un enjeu crucial en terme de sécurité. L'authentification est une procédure qui permet d'autoriser chaque utilisateur, un ordinateur l'accès à un type d'information

Il existe de nombreuses techniques d'authentification parmi lesquelles on trouve :

- Les mots de passe
- Les mots de passe uniques : ils ne serves que pour une requête et sont invalidés juste après.
- Les cartes à puces :le principal intérêt de la carte à puce c'est que l'utilisateur doit la posséder physiquement pour l'utiliser et souvent la compléter par des données que seul l'utilisateur connaît (code par exemple)
- Les super carte à puces : ce sont des cartes à puce de dernière génération qui comportent un clavier, un écran et une source d'énergie autonome. Ce type de cartes ne nécessite pas de terminal ou de réseau pour fonctioonner.
- Les caractéristiques biométriques : empreintes digitales, volaes, signatures
- Le chiffrement : la possession d'une clef de chiffrage

Le filtrage de contenu

L'idée est de contrôler les échanges d'information au sein de l'entreprise et aussi par rapport à l'extérieur. Parmi les pratiques à proscrire on trouve l'utilisation non professionnelle de la messagerie, le non respect de la confidentialité, le spamming (mail non solicité), le spoofing (usurpation d'identité pour le mail), la transmission de virus...

Protection des postes nomades

Les risques concernant les postes nomades sont de plus en plus élevés. Non seulement les données contenues dans ces postes peuvent être sensibles mais si ces postes sont détournés, ils peuvent servir de point d'entrée dans le système informatique de l'entreprise. Les réponses à ces préoccupations sont le recour à un VPN, virtual private network qui consiste à un cryptage point à point, une utilisation stricte des procédures d'authentification ou encore l'utilisation de solution de chiffrement et de protection au démarrage.

La PKI ou Public Key Infrastructure

Cette infrastructure regroupe tous les éléments requis par une autorité de certification afin de permettre l'émission des certificats à un ensemble d'individus ou de réseaux ainsi que l'administration de ces certificats. Un certificat identifie deux entités distantes qui souhaitent communiquer ensemble.

IV.2. Des mesures politico-juridiques

Vu la dimension planétaire de l'Internet, la sécurité du réseau et la confiance qu'il devrait inspirer sont des éléments qui nécessitent une action concertée à l'échelle mondiale. Les délits liés à l'informatique sont commis dans le cyberespace et ne sont pas cantonnés aux frontières d'un État. Ils peuvent en principe être perpétrés à partir de n'importe où et à l'encontre de n'importe quel utilisateur d'ordinateur dans le monde. Par ailleurs, il est clair que les activités traditionnellement illicites ne deviennent pas licites dès lors qu'elles se pratiquent via ou avec le concours de l'Internet.

Ceci dit, en matière de cybercriminalité, la protection des droits de l'individu peut poser des problèmes complexes, comme par exemple la détermination de la juridiction compétente, de la législation applicable et de son application transfrontalière. De plus, il n'existe pas de statistiques fiables rendant compte de l'ampleur réelle du phénomène de la cybercriminalité, alors que le nombre d'activités illicites pourrait augmenter à mesure de l'accroissement de l'utilisation des ordinateurs et des réseaux. Il est indispensable de rassembler des informations fiables sur l'ampleur de la cybercriminalité. Il est possible d'agir sur la prévention des activités criminelles en améliorant la sécurité des infrastructures d'information et en donnant aux autorités en charge de la répression des moyens d'action appropriés, tout en respectant intégralement les droits fondamentaux de la personne.

Avec la première Convention internationale de lutte contre la cybercriminalité, les pays membres du Conseil de l'Europe et leurs partenaires (Etats-Unis, Canada, Japon,

Afrique du sud) se sont engagés sur la voie d'une régulation juridique et éthique d'un domaine jusqu'alors abandonné, pour le meilleur comme pour le pire, aux seules règles du marché.

La convention, adoptée formellement par les Ministres des Affaires étrangères le 8 novembre 2001, a été ouverte à la signature des Etats le 23 novembre 2001 à Budapest. La Lituanie a ratifié la Convention sur la cybercriminalité le 18 mars 2004. Cette ratification, qui était la cinquième, a entraîné l'entrée en vigueur de la convention le 1er juillet 2004.

Un Protocole additionnel à la Convention sur la cybercriminalité, demandant aux Etats de considérer comme criminelle la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques, a été adopté le 7 novembre 2002 par le Comité des Ministres. Ses deux objectifs majeurs sont d'harmoniser le droit pénal et d'améliorer la coopération internationale afin de mieux lutter contre le racisme et la xénophobie sur l'Internet. Ce protocole a été ouvert à la signature à la session d'hiver de l'Assemblée parlementaire du Conseil de l'Europe de janvier 2003 et a été immédiatement signé par la France.

Conclusion

Le caractère décentralisé et en réseau d'Internet exige des solutions nouvelles et innovantes pour garantir qu'Internet soit un moyen de communication et de commerce sûr. Toute solution efficace passe par l'établissement de bonnes relations de travail entre le secteur industriel et les pouvoirs publics, reposant sur le respect et une meilleure compréhension des besoins et des capacités de chacun. Elle exige également de la vigilance pour protéger les droits des personnes, les libertés civiles et la confidentialité des communications licites. Enfin, les solutions adoptées au niveau mondial doivent être flexibles et s'adapter aisément aux mutations technologiques rapides.

Références bibliographiques

[11]http://www.alternatives.ca/article577.html

[21] RFC 1771

[22] http://www.itrmanager.com/46423-clusif,publie,etude,securite,messagerie.html

[22] Nicolas Dubée, « BGP et DNS: attaques sur les protocoles critiques de l'Internet », Secway / BD Consultants, Mai 2003.

[31] http://www.algerie-dz.com/article1160.html

[32]http://www.securityinfo.ch/phising.html

[33] http://www.info.fundp.ac.be/~mapi/brochure-fr.html

[41] Ines Feki, Mohamed Achemlal & Ahmed Serhrouchni, « Risques de sécurité liés au protocole de routage inter domaines BGP », France Télécom, ENST Paris; 2004.

Table des matières

I.Introduction..... 3
I.1.Définition :..... 3
II.Les enjeux de la cybercriminalité..... 4
II.1. L'ampleur de l'usage de l'Internet..... 4
II.2. Les menaces sur les outils critiques de l'Internet : cas du BGP.....6
II.3. La cybercriminalité en chiffres 8
III. Quelques infractions commis sur Internet..... 10
III.1. La pornographie..... 10
III.2. Le phishing.....11
III.3. Problématique de l'accès libre à la connaissance sur la toile..... 12
IV. Des solutions au problème de la cybercriminalité.....15
IV.1. Les solutions techniques..... 15
IV.2. Des mesures politico-juridiques.....20
Conclusion..... 22
Références bibliographiques.....23