

Projet collaboratif de rédaction

Sujet: Internet est-il un lieu sûr ?



*Maceski Cvete
Cossin Tristan
Portier Florian
Fouque Morgan
Gaune Florian*

1. Introduction

2. Histoire et évolution

3. Les dangers

- a. Les virus
- b. Les respects de la vie privée
- c. Les arnaques
- d. Danger des jeux de hasard
- e. Désinformation sur internet

4. Sécurité actuelle et autorités compétentes

- a. ANSSI
- b. Certificats
- c. Cookies
- d. Encryptage
- e. La CNIL

5. Enjeux géopolitiques

6. Conclusion

7. Annexe

Introduction

Internet est un réseau informatique mondial accessible par tout le monde. Mais savons nous exactement ce qu'est Internet et connaissons-nous réellement les risques que nous pouvons encourir en profitant de ce réseau?

Internet est un réseau de réseaux, qui permet l'élaboration d'applications et de services variés tel le courrier électronique, la messagerie instantanée, le pair-to-pair, le World Wide Web, etc...

On commence à parler d'Internet dès 1934, avec Paul Otlet, cependant, il faudra encore quelques années avant de pouvoir voir réellement ce procédé. Ce fut en 1965, que la première connexion informatique à longue distance fut établie, entre le Massachusetts et la Californie. Le courrier électronique quant à lui, ne vit le jour qu'en 1972, grâce à Ray Tomlinson. Ce fut à cette même année que Internet naquit, à partir d'ARPANET, le projet développé depuis 1966.

Internet ne fut ouvert au grand public que dans les années 90.. Pour la France, ce fut en 1994, cependant, son essor s'est vu en 2000. A partir de là se posa la question de la sécurité.

Effectivement, en même temps que l'essor d'Internet, vint également les dangers. Et ces dangers peuvent être divers : les virus, les problèmes liés aux informations confidentielles et personnelles, les arnaques, et bien d'autres.

Malheureusement, encore de nos jours, beaucoup de personnes ne connaissent pas les dangers liés à l'utilisation d'Internet, et encore beaucoup de gens sont victimes de ces dangers.

Dans ce document, nous vous proposons de (re)découvrir l'histoire et l'évolution des dangers sur Internet. Par la suite, nous vous montrerons l'éventail des dangers possibles de l'utilisation d'Internet, suivie par la sécurité et les services qui peuvent nous la garantir. Puis, finalement, nous vous fournirons une vision sur les dangers et les enjeux politiques pouvant être causés par de multiples cyber-attaques.

Histoire et évolution

Au début des années 1980, Internet servait surtout à relier des chercheurs. A cette époque, la circulation des documents ne posait aucun problème de confidentialité et les données traversaient le réseau en clair.

Si au début les protocoles Internet n'ont évolués que pour faire face à l'accroissement du nombre d'utilisateur, l'ouverture du réseau à un usage commercial a modifié les comportements. Comme des informations confidentielles circulent sur les liaisons, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises. Tous cherchant à se protéger contre une utilisation frauduleuse de leur données ou contre des intrusions malveillantes dans les systèmes informatiques.

La tendance actuelle est de mettre en place des protocoles sécurisés qui luttent contre l'usurpation d'identité ou l'espionnage des données privées.

Aujourd'hui dans le domaine de la sécurité des réseaux, il existe plusieurs solutions telles que les routeurs filtrants (pour protéger les réseaux des intrusions extérieures), les protocoles et les applications sécurisées, qui se sont multipliées.

Dans le domaine des protocoles, il existe plusieurs solutions de sécurité telles que le protocole IPSec (IP Security), le protocole SSL/TLS (Socket Secure Layer/Transport Layer Security) et le protocole SSH (Secure Shell).

Actuellement, il ne s'agit plus uniquement de chercher de nouveaux développements afin d'assurer la fiabilité du réseau, ou, d'une manière plus générale, sécuriser son fonctionnement global. Il faut adapter ces solutions aux besoins spécifiques des utilisateurs ainsi qu'à leurs environnements.

Sécurité actuelle et autorités compétentes

1-ANSSI

Service créé par décret le 7 juillet 2009, l' ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) est l'organisme principal dans le domaine de la sécurité des systèmes informatique français.

Son but est d'établir des normes quant à la protection des infrastructures réseaux, notamment ceux de l'Etat, et est chargée de la surveillance constante des flux d'entrées et de la détection dans les meilleurs délais des attaques entrantes.

2-Certificats

Dans un cadre plus privé, les navigateurs internet peuvent afficher une pastille attestant la sûreté d'une plateforme web, communément appelé Certificat de Sécurité, ou Certificat Electronique, délivrable si la plateforme web qui le demande satisfait des exigences sécuritaires et propose une infrastructure qui ne met pas en danger les données de ses utilisateurs.

3-Cookies

Outre l'aspect appétissant de la chose, les Cookies ont été longuement considéré comme la plus grosse fuite d'information possible sur internet. En vous connectant à un site, ou même simplement en le visitant, celui-ci stocke des informations concernant vos habitudes de navigations sur votre machine, et ces données sont réexploitables ultérieurement.

A cause de problèmes récent, la législation française a renforcé la sécurité concernant les Cookies, notamment en obligeant le déploiement d'un module informatif sur les infrastructures webs utilisant ces dits Cookies.

4-Encryptage

Dans un cadre plus global, les systèmes d'encryptage actuels permettent la sécurisation des tubes de circulation des informations, en chiffrant les données passagères avec des clés générées grâce à des algorithmes de cryptage avancés.

D'autres algorithmes permettent de passer un mot de passe de l'état clair à l'état crypté, avec une force de cryptage nécessitant des moyens de décryptage colossaux afin de retrouver le mot de passe de base (sha512+, chiffrement RSA entre 1024 et 2048 bits)

5-LA CNIL

La Commission Nationale de l'Informatique et des Libertés, est un organisme français qui a pour tâche de s'assurer que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle a entre autre un but exécutif, les sites français doivent entre autre répondre au critères dits "informatique et libertés", sans quoi la CNIL peut appliquer des sanctions pécuniaires allant jusqu'à 300.000€, et si appel du Président, toutes sanctions nécessaires peuvent être appliquées.

Les dangers

4.1 Les Virus

De nombreux virus se propagent sur internet, certains ne sont pas en soi dangereux (les répercussions sur l'utilisateur ne dépassant pas un ralentissement de la machine), d'autres en revanche, tel que les trojans, peuvent être beaucoup plus nuisibles. En effet, ils sont destinés à espionner la machine infectée pour y récupérer toutes informations pertinentes (comme les numéros de CB, informations personnelles, etc...).

4.2 Les respect de la vie privée

Ces dernières années ont vu l'explosion de l'utilisation des réseaux sociaux sur internet par le grand public. Malgré les nombreux avantages qu'ils procurent, ils peuvent se révéler dangereux et avoir des répercussions sur la vie de l'utilisateur en dehors d'internet, que ce soit à cause d'un manque d'attention de l'utilisateur (qui publiera des informations sur lui-même à la vue d'un grand nombre de personnes, etc...) ou de conditions d'utilisations floues (revente des informations personnelles à des fins publicitaires, etc...).

4.3 Les arnaques

Internet, grâce au relatif anonymat qu'il procure et à la juridiction floue à laquelle il est soumis, a permis l'émergence d'un grand nombre d'arnaques. Une des plus courantes et des plus efficace est le phishing (dérivé de fishing : pêcher) : un utilisateur mal intentionné (souvent par l'intermédiaire d'un système automatisé) envoie un mail à sa victime en se faisant passer pour une société (une banque par exemple) et lui demandant de fournir des informations sensibles comme un mot de passe, un numéro de CB...

Il est aussi fréquent de recevoir des mails d'un "millionnaire" situé à l'étranger qui se propose de vous reverser une grande quantité d'argent si vous lui envoyez vous-même de l'argent en premier pour l'aider à se sortir d'une situation quelconque ou

pour payer de soi-disant frais de dossiers. La victime ne recevra bien sûr aucun centime de la part du “millionnaire”.

4.4 Dangers des jeux de hasard sur Internet

La prolifération des jeux de hasard et des sites de paris sur Internet n'a fait qu'augmenter le nombre impressionnant de jeunes qui s'adonnent au jeu. C'est devenu chez les adolescents une dépendance plus importante que la cigarette.

Les jeunes qui maîtrisent bien les nouvelles technologies se tournent de plus en plus vers les sites Internet de jeux de hasard parce qu'ils sont faciles d'accès, pratiques et anonymes. Les jeunes n'ont pas à chercher longtemps pour trouver des jeux de hasard en ligne. Les casinos inondent Internet de leur publicité, qui apparaissent sur des sites populaires auprès des adolescents et même des enfants. Beaucoup de jeunes parient sur des événements sportifs dans des sites qui classent ensuite leurs résultats par rangs et offrent des prix aux meilleurs joueurs. Ils ne sont pas considérés comme de « vrais » sites de paris parce que leurs participants ne jouent pas pour de l'argent. Il reste que c'est un apprentissage du jeu et que beaucoup de ces sites ont des liens vers de « vrais » casinos

4.5 Désinformations sur internet

Il devient assez facile de propager des informations scientifiques non vérifiées ou encore validées mais dans un contexte de présentation délibérément orienté afin de faire passer une propagande politique.

Les enjeux géopolitiques

Internet n'a rien d'un monde virtuel. Il est devenu un enjeu primordiale pour nos gouvernements. Comment protéger les données personnelles de ses citoyens, comment protéger les secrets industriels de ses entreprises. Comment lutter contre des menaces floues, dont l'origine est souvent inconnu ou incertaine à l'heure ou internet est devenu d'une si grande importance pour tous ses acteurs ?

Sous l'espace virtuel que l'on voit quand on parle d'internet, il y a une réalité, celle des infrastructures qui le font exister. Les réseaux, les serveurs, les câbles sous-marins, les data centers etc.. Qui les construit, qui les contrôle, qui exploite et comment ? Leur répartition à la surface du globe est un enjeu pour nos gouvernements.

Alors qui contrôle internet ? Les Etats-Unis ont créé en 1998 l'ICANN qui gère la régulation d'internet. C'est une société Californienne à but non lucratif. Sa mission est de gérer l'attribution de nom de domaine. Les décisions de l'ICANN s'imposent à tous les Etats. Mais cet organisme est souvent remis en question notamment à cause de ses très étroites relations avec les Etats-Unis.

La Chine qui exerce un contrôle presque totale sur l'accès à Internet de ses citoyens, est de plus en plus soupçonné de recruter, former ou engager des pirates informatique. Ces pirates informatiques ont pour but de dérober des informations aux entreprises privées sur des secrets industrielle ou diverses autres données pouvant être utiles. De même, les Etats ne sont pas épargnés par ses attaques qui visent leurs secrets les mieux gardés.

La Chine n'est sûrement pas le seul pays à réaliser ce genre d'actions. La provenance des ses attaques restant presque totalement incertaine, il est difficile d'engager des sanctions contre les Pays ou les groupes les réalisant.

De plus en plus de pays se dotent d'une force d'intervention pour se défendre contre les diverses attaques dont ils sont les cibles ou même pour en attaquer d'autres.

Conclusion

Malgré l'évolution constante de sa sécurité, autant sur le plan technologique que sur le plan institutionnel, internet reste un lieu aux multiples risques. En particulier pour les personnes non averties des dangers de ce dernier.

La sécurité sur Internet est devenu un enjeu majeur pour les Etats qui se doivent d'assurer leur propre protection ainsi que celle de leurs citoyens.

Annexe

Pour ce travail, nous avons opté pour une division des tâches. Ainsi, L'introduction fut rédigé par Gaune Florian, la partie de l'histoire et de l'évolution fut apportée par Cossin Tristan. Les dangers nous furent expliqués, par Cvete Maceski, la sécurité mise au grand jour par Fouque Morgan. Et finalement, les enjeux géopolitiques furent introduits par Monsieur Portier Florian. La conclusion, quant à elle, fut rédigé par toute l'équipe.

Nos problèmes se sont surtout focalisés sur la division et la répartition du sujet. De plus, des petits soucis au niveau de la compréhension grammaticale de certaines phrases nous a value quelques petits ralentissements.

Le groupe