Document présenté à

Farid Alem

Dans le cadre du cours de

Modèle d’affaire et systèmes d’information

**Rapport**

Par

Franz Nkezimana et Cédric Soumpholphakdy

Collège Ahuntsic

6 mai 2014

Actuellement, les affaires dépendent de plus en plus sur des ordinateurs qui ont la capacité de protéger et garder nos informations personnelles. Plusieurs entreprises sont apparues et ils sont spécialistes dans le domaine de la sécurité informatique. Des industries qui veulent protéger leurs données personnelles ont besoin des services d'expert en sécurité informatique.

Leurs taches est de considérer et d’analyses leurs moyens si c'est adéquate ou non et ils doivent créer des solutions pour régler leurs problèmes sur des sécurités informatiques.

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mise en place pour détenir, arranger, et garantir la sécurité des systèmes informatiques. Elle est intrinsèquement liée à la sécurité de l'information et des systèmes d'information.

Voici donc l’historique des sécurités informatiques en autres mots, les origines :

La sécurité de l'informatique a été développée et améliorée pendant plusieurs années à l'aide de l'utilisation des réseaux publiques qui permettent de fournir des informations personnelles.

Un des facteurs qui favorise les sécurités informatiques s'est que l'internet est populaire et cette popularité est un des sources de motivation pour les experts de la sécurité informatique.

L'internet est la source de développement, le plus important du 20 IIème siècle parce que beaucoup de personnes utilisent l'internet pour accéder aux ressources offertes par l'internet. Ces ressources De la recherche et la récupération d'informations à l'utilisation du courrier électronique et des transactions commerciales électroniques.

Par contre, l'internet est base sur des protocoles basés sur la confiance. Le réseau est ouvert à tous les utilisateurs qui sont malveillant et peut être considérer comme un danger pour le système. Plusieurs événements ont contribués à la naissance de la sécurité informatique.

Durant les années 1930 à 1940 :

Les cryptographes polonais conçoivent la machine Enigma en 1918, un appareil électromécanique de cryptage par rotor qui traduit les informations écrites en texte clair en messages cryptés. Ca été conçu pour sécuriser les communications bancaires, l'armée allemande trouve le dispositif des plus utiles pour sécuriser les communications durant la deuxième guerre mondiale.

Alan Turing, un brillant mathématicien, développe alors une méthode pour briser les codes d'Enigma, permettant alors aux forces alliées de développer Colossus, une machine souvent accréditée de la fin de la guerre une année plus tôt.

Année 1960 :

Les étudiants du Massachusetts Institute of Technology (MIT) fondent le Tech Model Railroad Club (TMRC) et commencent à explorer et programmer l'unité centrale PDP-1 du système informatique de l'école. Le groupe finit par utiliser le terme « hacker » (ou pirate) dans le contexte actuel que l'on connaît.

Le Ministère de la Défense américaine (DoD) crée le réseau Advanced Research Projects Agency Network (ARPANet), qui acquiert de la popularité dans les milieux académiques et de recherche, comme un moyen d'échanger électroniquement des données et des informations. Ce dernier ouvre la voie vers la création d'un réseau porteur connu de nos jours sous le nom d'internet.

Ken Thompson développe alors le système d'exploitation UNIX, considéré par beaucoup comme étant le système d'exploitation le plus « susceptible d'être piraté » en raison d'une part, de ses outils pour développeurs et de ses compilateurs très accessibles et d'autre part, de son soutien parmi la communauté des utilisateurs. À peu près à la même époque, Dennis Ritchie met au point le langage de programmation C, indiscutablement le langage de piratage le plus populaire de toute l'histoire informatique.

Année 1970 :

Bolt, Beranek and Newman, une société de développement et de recherche informatique pour le gouvernement et le monde de l'industrie, met au point le protocole Telnet, une extension publique du réseau ARPANet. Ce développement ouvre les portes à l'utilisation par le public de réseaux de données qui étaient autrefois le privilège des entrepreneurs et des chercheurs du monde académique. Il convient néanmoins de préciser que, selon plusieurs chercheurs en matière de sécurité, Telnet est sans doute le protocole le moins sûr pour les réseaux publics.

Steve Jobs et Steve Wozniak fondent Apple Computer et commencent à commercialiser l'ordinateur personnel ou PC (de l'anglais Personal Computer). Le PC devient alors le tremplin pour l'apprentissage par des utilisateurs malintentionnés de l'art de s'introduire dans des systèmes à distance en utilisant du matériel de communication de PC courant tel que des modems analogues ou des logiciels dédiés (war dialers).

Jim Ellis et Tom Truscott créent USENET, un système de type messagerie pour la communication électronique entre des utilisateurs très variés. USENET devient rapidement l'un des forums les plus populaires pour l'échange d'idées en matière d'informatique, de mise en réseau et, évidemment, de craquage (ou cracking).

Année 1980 :

IBM met au point et commercialise des PC basés sur le microprocesseur Intel 8086, une architecture peu coûteuse permettant à l'informatique de passer d'une utilisation purement professionnelle à une utilisation personnelle. Grâce à ce développement, le PC devient un produit ménager de consommation courante non seulement abordable et puissant, mais également simple d'utilisation et contribue par là-même à la prolifération de tel matériel dans l'environnement professionnel et personnel d'utilisateurs malintentionnés.

Le protocole TCP ou Transmission Control Protocol, mis au point par Vint Cerf, se divise en deux parties distinctes. L'IP (ou Internet Protocol) trouve son origine dans cette division et de nos jours, la combinaison des protocoles TCP/IP est désormais la norme pour toute communication Internet.

En raison des progrès effectués dans le domaine du phreaking, ou plus précisément les techniques d'exploration et de piratage du système téléphonique, le magazine 2600 : The Hacker Quarterly voit le jour et lance vers une vaste audience, des discussions sur des thèmes tels que le piratage informatique et les réseaux informatiques.

Après une vague de piratage de neuf jours au cours desquels le « Gang 414 » (baptisé ainsi en référence à l'indicatif du lieu où ses membres habitaient et effectuaient leurs opérations de piratage) s'introduit dans des systèmes d'institutions ultra secrètes, tels qu'un centre de recherche en armement nucléaire ou encore le laboratoire de Los Alamos (Los Alamos National Laboratory), les autorités américaines font une rafle sur leur quartier général.

Legion of Doom et Chaos Computer Club sont deux groupes pionniers en matière de piratage qui commencent alors à exploiter les faiblesses des ordinateurs et des réseaux de données électroniques.

La loi américaine de 1986 sur la répression des fraudes et infractions dans le domaine informatique (Computer Fraud and Abuse Act) est passée par le congrès suite aux exploits de Ian Murphy, alias Captain Zap, qui réussissant à s'introduire dans des ordinateurs de l'armée, vole des informations dans les bases de données de commandes de diverses sociétés et utilise des standards téléphoniques gouvernementaux à accès limités pour effectuer des appels.

Grâce à cette nouvelle loi (Computer Fraud and Abuse Act), la justice est en mesure de condamner Robert Morris, un diplômé universitaire, pour l'introduction du vers portant son nom (Morris Worm) dans plus de 6000 ordinateurs vulnérables reliés à l'internet. Le cas suivant le plus célèbre ayant fait l'objet d'une condamnation en justice est celui de Herbert Zinn, un lycéen qui, après avoir abandonné ses études, s'introduit dans les systèmes informatiques appartenant à AT&T et au ministère de la défense américaine (DoD) et les utilise à des fins malveillantes.

Par crainte que le « ver Morris » puisse être reproduit, l'équipe de réponse aux urgences informatiques (CERT, de l'anglais Computer Emergency Response) est créée afin d'avertir les utilisateurs d'ordinateurs contre les problèmes de sécurité réseau.

Clifford Stoll écrit le livre The Cuckoo's Egg, un récit de l'enquête de l'auteur sur les pirates exploitant son système.

Les années 1990 :

Le réseau ARPANet est dé-commissionné et son trafic transféré sur l'internet.

Linus Torvalds développe le noyau Linux pour une utilisation avec le système d'exploitation GNU ; le développement et l'adoption très répandus de Linux sont en partie dûs à la collaboration des utilisateurs et des développeurs communiquant par le biais de l'internet. En raison de son enracinement dans Unix, Linux est le choix préféré des pirates malintentionnés et des administrateurs qui voient en lui, un moyen utile pour construire des alternatives sécurisées aux serveurs legacy utilisant des systèmes d'exploitation propriétaires (ou Closed Source et donc non-modifiables).

La navigateur Web graphique voit le jour et engendre une croissance exponentielle de la demande pour l'accès public à l'internet.

Vladimir Levin et ses complices transfèrent illégalement des fonds d'un montant d’US $10 millions sur plusieurs comptes en s'introduisant dans la base de données centrale de la CityBank. Levin est plus tard arrêté par Interpol et presque la totalité de l'argent transféré est retrouvée.

Kevin Mitnick est vraisemblablement le plus célèbre de tous les pirates, suite à ses intrusions dans les systèmes de plusieurs grandes sociétés et au vol de toute sorte de données allant des informations personnelles de personnes célèbres à plus de 20.000 numéros de cartes de crédit en passant par des codes sources de logiciels propriétaires. Interpelé et condamné pour infraction par câble, il sert une peine de 5 ans de prison.

Kevin Poulsen et un complice non-identifié truquent les systèmes téléphoniques d'une station de radio afin de gagner des voitures et des prix en espèces. Poulsen qui est déclaré coupable pour des infractions par ordinateurs et câbles, est condamné à 5 ans de prison.

Les histoires de piratage et de « phreaking » (piratage de systèmes téléphoniques) se transformant en légendes, plusieurs pirates potentiels décident de se réunir à une convention annuelle intitulée DefCon afin de fêter le piratage et l'échange d'idées entre passionnés du domaine.

Un étudiant israélien de 19ans est arrêté et condamné pour avoir coordonné plusieurs intrusions dans des systèmes du gouvernement américain pendant la Guerre du Golfe. Selon les sources officielles de l'armée américaine, ces infractions représentent « les attaques les plus organisées et systématiques » des systèmes informatiques du gouvernement dans toute l'histoire du pays.

Le ministre de la justice américaine, Attorney General Janet Reno, en réponse au nombre croissant des brèches de sécurité dans les systèmes du gouvernement fonde le centre de protection de l'infrastructure nationale (ou National Infrastructure Protection Center, NIPC).

Des pirates non-identifiés prennent le contrôle de satellites de communication britanniques et exigent une rançon. Après un certain temps le gouvernement britannique reprend contrôle de ses satellites.

<http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-fr-4/ch-sgs-ov.html>

<http://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information>