Inventaire des menaces sur les systèmes informatiques

Razafy N. R.[1] – Rakotomiraho S.[2] – Randriamaroson R. M.[3]

Laboratoire de Recherche Systèmes Embarqués, Instrumentation et Modélisation des Systèmes et Dispositifs Electroniques
(LR-SE-I-MSDE)
Ecole Doctorale en Sciences et Techniques de l'Ingénierie et de l'Innovation
(ED-STII)

[1]r.razafy@bfm.mg – [2]rakmiraho@gmail.com – [3]rivomahandrisoa@gmail.com

Résume

Cet article présente l'étude sur les menaces sur un système informatique. Les menaces sont les facteurs qui peuvent nuire à la sécurité d'un système d'information. En général, un système d'information a pour but de stocker les informations de gestion ou de fournir des services. L'objectif est de conscientiser les décideurs, les administrateurs et les utilisateurs sur les risques existants. Dans l'étude de la sécurité informatique, il y a un dicton qui dit : « apprendre l'attaque pour mieux se défendre ». L'étude est orientée sur les menaces intentionnelles.

Mots-clés : menaces informatiques, sécurité informatique, piratage, analyse de risque, vulnérabilité, faille de sécurité

Abstract

Threats on computer system are investigated in this paper. Threats are the factors that may affect the safety of an information system. In general, an information system is designed to store the management information or to provide services. In the investigation of computer security, there is a saying: "Learn the attack to self-defend better." The study is oriented on intentional threats. The goal is to make the policy makers, administrate and users aware of existing risks.

Keywords: computer threats, computer security, hacking, risk analysis, vulnerability, security management

1. Introduction

Les menaces informatiques sont les actions ou les évènements, volontaires ou non, pouvant nuire au bon fonctionnement d'un système d'information. La sécurité des systèmes d'information (SI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires mis en place pour conserver, rétablir, et garantir la sécurité du système d'information. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation soient uniquement utilisées dans le cadre prévu. La sécurité informatique est un défi d'ensemble qui concerne une chaine d'éléments : les infrastructures matérielles de traitement ou de communication, les logiciels (systèmes d'exploitation ou applicatifs), les données, le comportement des utilisateurs.

Un SI est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et diffuser de l'information.

2. Analyse des risques

L'analyse des risques est une étude obligatoire pour la mise en place de sécurité. En premier lieu, il faut connaitre les actifs à protéger et leurs propriétaires selon le niveau de criticité. Ayant les valeurs des actifs et les types des actifs, les menaces représentant des risques peuvent être dégagés. A cet étape, les acteurs ayant la motivation pour accéder aux risques peuvent être imaginés avec les moyens y afférents. La protection dépend de la vulnérabilité recensée et de l'attaque à éviter. Ces actions sont dépendantes mais itératives. La figure 2.1 schématise l'analyse de risque selon la méthode OCTAVE v1.1 adapté à la norme ISO 15408 [1].

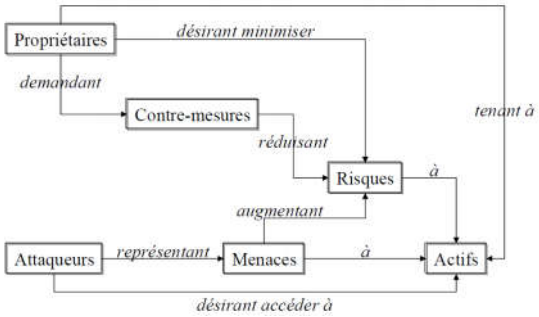

Figure 2.1 : Schéma d'analyse de risque [1]

Les actifs sont l'ensemble des données et des systèmes d'information nécessaires au bon déroulement d'une organisation.

Une menace est la possibilité qu'une vulnérabilité soit exploitée.

La vulnérabilité est le défaut ou la faiblesse d'un système pouvant mener à une faille de sécurité ou à la violation de sa politique de sécurité.

Le risque est l'impact sur la mission de l'organisation, dépendant à la fois de la vraisemblance de la menace (condition) et de son impact sur les actifs et les ressources (conséquence).

Selon les normes, garantir la sécurité se résume à assurer la disponibilité, l'intégrité, la confidentialité et la non-répudiation. Le tableau I représente une récapitulation généralisée de la correspondance avec la motivation d'attaque.

Tableau I : correspondance entre objectifs de sécurité et menace

Objectif	Menace
Disponibilité	Panne matériel Accès physique Attaque par saturation
Intégrité	Attaque de modification
Confidentialité	Attaque d'accès Espionnage et vol d'information
La non-répudiation	Attaque de répudiation

Deux autres méthodes peuvent être aussi utilisées, qui sont la méthode EBIOS (Expression des Besoins et Identification des Objectifs de sécurité) et la méthode MEHARI (MEthode Harmonisée d'Analyse de Risques).

La méthode EBIOS est une méthode établie par DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) pour identifier les besoin de sécurité d'un système d'information. La DCSSI la présente comme un outil d'arbitrage au sein des directions générales. Elle est du

niveau d'un détail proche de la norme ISO 13335 [2]. Les quatre étapes proposent par cette méthode sont l'étude du contexte, expression des besoins, étude des risques et l'identification des objectifs de sécurité.

La méthode MAHARI est proposée par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français). Elle permet l'évaluation des risques mais également le contrôle et la gestion de la sécurité de l'entreprise sur court, moyen, et long terme indépendamment de la répartition géographique du système d'information. Elle s'articule sur trois plans, qui sont le PSS (Plan Stratégique de Sécurité), le POS (Plan Opérationnels de Sécurité) et le POE (Plan Opérationnel d'Entreprise). Elle est plus proche des logiques de la norme ISO 17799 [2].

3. Détermination de la raison de la menace et de la faille de sécurité

En se référant au schéma d'analyse de risque en utilisant la méthodologie OCTAVE, la détermination de la raison de la menace consiste à « désirant accéder à actif ». Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables [3]. Les principales motivations sont :

- obtenir un accès au système,
- consulter et/ou voler des informations (données bancaires, secrets industriels, propriétés intellectuelles, etc.),
- glaner des informations personnelles sur un utilisateur,
- s'informer sur l'organisation d'une entreprise en balayant le réseau,
- troubler ou nuire le bon fonctionnement d'un service,
- utiliser le système d'un tiers comme « rebond » pour une attaque,
- obtenir de contrôle sur le système.

Le pirate fait la correspondance entre le comportement de l' « être humain » et les configurations techniques pour avoir les défauts de sécurité. Il se met à la place des administrateurs et des utilisateurs pour pouvoir faire le recensement des failles et les points de vulnérabilité d'un système. Pour arriver au but, une reconnaissance et l'établissement de la cartographie du système cible constituent la première étape. Mais il existe aussi des attaques généralisées qui sont diffusées sans connaître les cibles, comme le cas des virus.

Les menaces informatiques peuvent venir aussi bien de l'intérieur que de l'extérieur. Pour recenser les risques, l'administrateur de sécurité devra avoir une vision de l'intérieur et de l'extérieur. Mais dans tous les cas, les menaces sont l'exploitation de la vulnérabilité. En général, la vulnérabilité vient de la négligence d'un être humain. L'installation et la configuration d'un logiciel ou d'un équipement par défaut sont les plus fréquentes. La reconnaissance effectuée par les pirates commence toujours par le test des mots de passe par défaut, les ports par défaut, les services ayant des failles. Pour le cas de la sécurité des données, les malintentionnés exploitent les données sur les supports de sauvegarde et les données de production migrées dans les environnements test pour éviter de laisser des traces.

Le maillon faible d'un système d'information peut être un utilisateur, une application ou un équipement. Ayant un contrôle ou une seule action sur l'un de ces composants, un pirate peut avoir le contrôle total d'un système entier. Une

attaque de grande envergure est une succession d'action : reconnaissance, établissement de la cartographie du système cible, obtention d'accès, augmentation de privilège, exécution de l'action voulue, et suppression de trace.

4. Le facteur humain

Le mode de vie de l'homme et d'une entreprise a été grandement changé avec l'évolution technologique du traitement d'information et de la télécommunication. L'utilisation de l'informatique devient inévitable dans tous les domaines. Face à cette évolution technologique la sécurité et la protection des biens sous format numérique sont primordiales ainsi que les offres de services.

Peu importe à quel point un système de sécurité est sophistiqué et complexe, il y aura toujours un être humain pour contrôler ce système. Dans son environnement de travail journalier, l'humain doit faire des choix et prendre des décisions qui peuvent avoir des conséquences importantes pour la sécurité de l'entreprise. Si l'humain est l'élément central de toute organisation, il représente également l'élément le plus vulnérable, car il est à la fois la cause de nombreux incidents et la partie maîtresse dans la protection de l'information. Faisant partie à la fois de la solution et du problème, il est essentiel de s'attarder sur son comportement et de comprendre pourquoi il est vulnérable [4].

4.1 Ingénierie sociale

L'ingénierie sociale, qui est l'art d'utiliser la tromperie et le mensonge pour arriver à ses fins, exploite précisément ce maillon faible de la chaîne de sécurité. Ce procédé consiste à entrer en contact avec un utilisateur du réseau, en se faisant passer en général pour quelqu'un d'autre, afin d'obtenir les informations voulues même un mot de passe. Avec la même méthode, une faille de sécurité peut être créée en envoyant un cheval de Troie à certains utilisateurs de réseau. Il suffit qu'un des utilisateurs exécute la pièce jointe pour qu'un accès au réseau interne soit donné à l'agresseur extérieur. L'être humain est classé parmi le maillon le plus faible de sécurité.

4.2 Irresponsabilité

Certains utilisateurs et administrateurs ont une naïveté et ont une ignorance du problème de sécurité. Ils ne sont pas conscients de l'importance de l'information en leur possession. En laissant par exemple leur mot de passe sur un bout de papier collé sur l'écran, les autres utilisateurs peuvent en profiter en puisant des informations aux quelles ils n'ont pas le droit d'accéder. De même pour les administrateurs qui stockent les mots de passe dans un fichier excel portant le nom « motdepasse.xls » dans un ordinateur non sécurisé.

Les environnements de test, les sauvegardes et les corbeilles sont aussi l'endroit où les malfaiteurs ont l'habitude de fouiller. Ces endroits n'héritent plus des politiques de sécurité dans les environnements de production. Copier les données de la production vers l'endroit test sans faire attention est une grave erreur.

4.3 Exploitation de privilège

Ayant le droit d'accès à des informations, un utilisateur peut l'exploiter pour soustraire et divulguer des informations. Des personnes peu scrupuleuses peuvent

profiter des failles d'une organisation pour piller des informations personnelles et violer des données confidentielles, pour leur propre bénéfice ou pour le compte d'un crime organisé [5]. Un employé ayant une autorisation valide et ayant connaissance de la vulnérabilité du système peut attaquer facilement l'ensemble du système. Généralement ces attaques sont des attaques venant de l'interne du réseau et ils sont difficilement détectables par rapport aux attaques externes.

5. Accès physique

Dans ce cas l'attaquant a un accès aux locaux ou éventuellement aux machines. En ayant un contact direct sur le système, l'intrus peut agir directement sur les matériels. Deux cas d'attaques peuvent être effectués : vandaliser les équipements ou installer un matériel ou logiciel pour pouvoir soustraire des informations.

5.1 Vandalisme

Le vandalisme consiste à faire des actions de détérioration des équipements. L'objectif est d'arrêter un ou des équipements pour nuire au bon fonctionnement du système. Au cas où les accès aux équipements sont protégés par des mots de passe, la méthode brutale est d'enlever les câbles d'alimentation ou de couper tout simplement l'électricité. En plus de l'arrêt de service, l'extension manuelle des serveurs peut engendrer une panne du système ou d'une application et une panne de disque dur.

5.2 Vols

Etant à l'intérieur de l'entreprise, l'intrus peut connecter son portable pour accéder à l'ensemble du réseau. Après il peut faire des analyses des paquets sur le réseau ou installer des logiciels malveillants. Ayant un agent installé à l'intérieur de l'entreprise, le pirate peut accéder facilement au réseau. D'autre cas plus barbare consiste à voler carrément les ordinateurs, les serveurs ou les supports de stockage de données.

6. Les attaques d'accès

Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information [6]. Pour avoir les informations, les attaqueurs ont deux façons d'arriver à leur fin, soit en forçant l'accès, soit en analysant les informations qu'ils arrivent à capturer.

6.1 L'écoute du réseau (sniffing)

Un analyseur de réseau ou sniffer est un dispositif permettant de capturer les informations transitant sur le réseau [7]. Dans un réseau non commuté, les données sont envoyées à toutes les machines du réseau. Un logiciel sniffer peut intercepter tous les paquets qui circulent sur le réseau même ceux qui ne sont pas destinés pour le poste travail hébergeant le logiciel. Par exemple, lors d'une connexion « telnet » le mot de passe de l'utilisateur va transiter en clair sur le réseau. Après, le pirate peut se connecter facilement au serveur. De même le logiciel peut analyser les sessions de transfert de fichier en cours ainsi que les échanges de courrier électronique.

6.2 Le cheval de Troie et porte dérobée (backdoor)

Le cheval de Troie est un sous-programme caché dans un autre programme. Ce nom vient de la légende grecque de la prise de Troie à l'aide d'un cheval en bois rempli de soldats qui attaquèrent la ville une fois à l'intérieur. En général, le but d'un cheval de Troie est de créer une porte dérobée pour que le pirate puisse ensuite accéder à l'intérieur de l'ordinateur victime.

A travers un programme illégal, le pirate a accès à l'ordinateur et soustrait les informations qu'il souhaite. Pour cela, il laisse donc des portes dérobées qui lui permettront de reprendre facilement le contrôle du système informatique. De même si l'utilisateur change de mots de passe ou ajoute un nouveau module de sécurité, l'accès est encore ouvert tant que le programme est encore en exécution.

6.3 L'ARP poisoning

L'objectif de l'attaque consiste à s'interposer entre deux machines du réseau et à transmettre à chacun un paquet falsifié indiquant l'adresse physique de l'autre machine à changer, l'adresse ARP (Adress Routing Protocole) fournie étant celle de l'attaquant. De cette manière, à chaque fois qu'un des deux machines souhaite communiquer avec la machine distante, les paquets seront envoyés à l'attaquant de manière transparente à la machine destinatrice.

Ayant tous les paquets à sa possession, le pirate peut soustraire les informations qu'il veut, comme les données sensibles, les mots de passe et les informations concernant l'organisation de l'entreprise.

6.4 Balayage des ports

Un scanner de vulnérabilité est un utilitaire permettant de réaliser un audit de sécurité d'un réseau en effectuant un balayage de ports ouverts sur une machine donnée ou sur le réseau tout entier. La technique se fait à partir des requêtes permettant de déterminer les services fonctionnant sur un hôte distant. Le but est d'avoir les listes des ports ouverts et les ports actifs. En analysant de façon plus fine la structure des paquets TCP/IP reçus, les scanners peuvent arriver à déterminer le système d'exploitation ainsi que les versions des applications associées à chaque port. Les éléments recueillis serviront plus tard pour accéder à la machine ou l'équipement cible.

6.5 Le craquage de mot de passe

En connaissant l'application cible, le pirate va essayer d'accéder au système avec les utilisateurs d'administration standard (administrateur, admin, root, …). Le craquage consiste à faire de nombreuses tentatives jusqu'à trouver le bon mot de passe. Deux méthodes pouvant être utilisées ont l'utilisation de dictionnaire et la méthode brute [6].

L'utilisation de dictionnaire consiste à utiliser une base de données de mot de passe. La base de données contient les mots de passe courants avec les variantes possibles (à l'envers, avec un chiffre, …). Par contre, la méthode brute prend toutes les combinaisons possible de mots de passe dans l'ordre jusqu'à trouver le bon. Mais avant d'utiliser ces deux méthodes, l'agresseur essaie en premier lieu les mots de passe autour de la vie de l'entreprise ou de celle de l'utilisateur comme la date de naissance, nom d'enfant, nom de l'entreprise.

7. Les attaques par saturation (déni de service*)*

Les attaques par saturation sont des attaques informatiques qui consistent à envoyer des milliers de requêtes pour paralyser ou bloquer un service offert par un système. L'objectif est de rendre indisponibles les données ou les services pour les utilisateurs. Aucune notion de récupération ni de modification n'est prise en compte ici [8].

Les attaques par déni de service est un fléau pouvant toucher tout serveur et tout site internet. Généralement, elles exploitent les failles liées à l'implantation d'un protocole du modelé TCP/IP. La difficulté est de détecter les attaques venant de l'intérieur du réseau, là où les serveurs sont exposés directement aux agresseurs sans passer par aucun firewall.

Lorsqu'un déni de service est provoqué par plusieurs machines, on parle alors de « déni de service distribué » ou « DDOS » (Distributed Denial of Service). Dans ce cas, le logiciel malveillant est installé dans plusieurs ordinateurs ou utilise les autres ordinateurs pour renvoyer les requêtes tout simplement [3].

7.1 Le flooding et le débordement de tampon

Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille jusqu'à ce que cette dernière n'arrive plus à les traiter et qu'elle se déconnecte du réseau. Suite à un débordement, la machine peut aussi se bloquer, redémarrer, ou écrire sur le code en mémoire.

7.2 TCP-SYN flooding

Le TCP-SYN flooding est une variante de flooding qui s'appuie sur une faille du protocole TCP. Le principe est d'envoyer un grand nombre de demande de connexions au serveur (SYN : SYNchronisation) à partir de plusieurs machines. Le serveur va retourner va répondre avec le paquet SYN-ACK (ACK : ACKnowledgement) et attendre en retour une réponse ACK qui n'arrivera jamais. A la saturation de la queue permettant de stocker les connections en attente de fin d'ouverture, la machine n'acceptera plus aucune nouvelle demande.

7.3 Le smurf

Le smurf est une attaque utilisant le ping et les serveurs de broadcast. La première étape consiste à falsifier l'adresse IP pour se faire passer pour la machine cible. On envoie après un ping sur un serveur de broadcast. Le serveur le fera suivre à toutes les machines qui sont connectées, qui vont renvoyer chacun un « ponq » au serveur qui le fera suivre à la machine cible. Celle-ci sera inondée sous les paquets et finira par se déconnecter.

8. Les attaques de répudiation

La répudiation est une attaque contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un évènement ou une transaction se soit réellement passé.

8.1 L'IP spoofing

L'IP spoofing n'est pas une attaque en tant que tel mais une méthode pour dissiper l'identité. La méthode est de faire passer une action en falsifiant l'adresse IP. La source se communique avec la machine cible comme une machine de confiance. Il existe deux types d'IP spoofing qui sont le Non Blind Spoofing et (NBS) le Blind Spoofing (BS) [8].

Le NBS consiste à utiliser la technique du spoofing pour s'interférer dans une connexion dont les paquets traversent un sous-réseau auquel le pirate a accès. La technique du BS nécessite une toute autre configuration. Dans ce cas, l'attaquant ne capture pas les paquets émis par la machine cible. L'attaquant doit pouvoir prédire les paquets qui seront envoyés par la station qu'il désire attaquer.

8.2 L'attaque par rebond

L'attaque par rebond est une méthode pour cacher l'identité et faire passer l'attaque par une autre machine. L'objectif est de masquer les traces permettant de remonter jusqu'à la machine source. Le pirate garde toujours à l'esprit le risque de se faire repérer et privilégie habituellement les attaques par rebond. Les conséquences d'une telle attaque ne se limite pas tout simplement à un ordinateur cible mais aussi à l'entreprise. Etant un système de transit des diffusions de courrier, le nom de domaine de l'entreprise peut être refusé par tous les autres dispositifs de sécurité et s'ajoute dans la blacklist.

9. Les attaques de modification

Une attaque de type « modification » consiste, pour un attaquant à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information. La première étape est d'avoir un accès ; puis d'exécuter des modifications. Les applications et les données sont susceptibles de modification. Ce type d'attaque est difficile à détecter s'il vient de l'interne du réseau, et se fait par le biais de « virus ».

Le virus est un programme parfois caché dans un autre programme capable de se propager dans un réseau. Un virus est un programme informatique qui, à l'insu de l'utilisateur, exerce une action nuisible à son environnement [8]. Il a pour but de nuire au système d'exploitation ou à une des applications, en changeant les données ou le programme même. Par exemple, un virus est capable de modifier le « registre » est de changer l'appel d'un exécutable par un autre. Mais le plus dangereux est aussi d'effacer les données du disque dur.

10. L'espionnage et vol d'information

L'espionnage consiste à effectuer des intrusions puis soustraire des informations. Dans ce cas d'attaque, il n'y a pas de destruction ou de modification. Le but n'est pas de nuire au bon fonctionnement du système mais de recueillir tout simplement des informations.

10.1 L'homme au milieu

Le pirate essaie de prendre le contrôle des équipements réseaux pour pouvoir capter les échanges de données au sein du réseau. La technique exploite les failles de protocole réseau. En général, le pirate utilise le DHCP (Dynamic Host

Configuration Protocol), ARP (Adress Routing Protocole), ICMP (Internet Control Message Protocol), proxy http (Hypertext Transfer Protocol) et DNS (Domain Name System).

10.2 L'espiogiciels (spyware)

Le spyware ne nuit pas bon fonctionnement du système mais plutôt au respect de la vie privée. Le but est d'installer des logiciels pouvant remonter des informations vers les éditeurs. Par exemple, le Real Networks envoie certaines informations vers l'éditeur à chaque insertion de CD. Les logiciels gratuits (freeware) cachent souvent un tel type d'application.

10.3 Le cookie

Le cookie est une chaine de caractère qu'un serveur dépose sur le disque dur, via le navigateur, afin d'accélérer les prochaines visites, mais aussi d'envoyer des informations vers le serveur. Lorsque le serveur WEB propose un cookie, les utilisateurs ignorent ce terme et valident l'installation. Il sert à stocker les informations sur l'utilisateur et les préférences de l'utilisateur. Ces informations vont être renvoyées au serveur en vue de création de base de données contenant les renseignements sur les utilisateurs.

10.4 Le phishing

Le phishing ou « hameçonnage » une méthode frauduleuse pour récupérer des informations (généralement bancaires) auprès des internautes. Il se base sur l'ingénierie sociale en exploitant la faille humaine. Le principe est d'envoyer un semblant de courrier électronique venant d'un tiers de confiance. Le courrier contient un lien hypertexte qui est un formulaire. En remplissant le formulaire, les informations vont être collectées et stockées dans le serveur du pirate. Pour les envois massifs vers des adresses électroniques collectées au hasard, les messages sont parfois peu parlants pour les utilisateurs.

10.5 Hoax (rumeur)

Un hoax est une rumeur envoyée par mail. Ces rumeurs comportent souvent des problèmes de sécurité soit disant découverts par des services officiels ou célèbres. En ayant une confiance au mail sans en vérifier l'authenticité, l'utilisateur renvoie des informations confidentielles.

10.6 Exploitation de vulnérabilité des serveurs WEB

Pour véhiculer les informations sur internet, le HTTP et le HTTPS sont les protocoles utilisés. Les pages de présentation sont stockées dans un serveur web, par contre les données peuvent être stockées dans d'autre serveur. L'attaque d'un serveur web consiste à détecter via les informations qui transitent durant la consultation du site les failles du serveur web. Le but de l'agresseur est d'essayer de remonter vers le serveur de base de données pour pouvoir soustraire les informations. Plusieurs techniques existent comme les attaques par injection (SQL Structured Query Language, OS Operating System, LDAP Lightweight Directory Access Protocol, ...), l'exploitation

d'authentification et gestion de session mal conçue, et l'exploitation de faille des composants vulnérables.

11. Conclusion

« Se protéger » contre les menaces informatiques est un défi quotidien pour les détenteurs de données numériques et les fournisseurs de services. En suivant l'évolution technologique, les risques de s'exposer face à des attaques se multiplient de plus en plus. Ce travail a permis de faire un recensement des menaces par type. Les attaques ne sont pas isolées mais peuvent être exécutées en cascade. Il suffit d'une simple action et une seule faille pour conduire à déjouer toutes les mesures de sécurité implantées. La conséquence d'une ignorance peut être grave et irréversible.

12. Références

[1] Jean-Marc ROBERT, *« Analyse de risque OCTAVE V1.1 »*, 2013

[2] La Revue, *« Rappel sur les normes et méthodes en matière de sécurité des systèmes d'information »*, 2007

[3] Brault, *« Les menaces informatiques »,* 2008

[4] David CASTONGUAY, Centre International de Criminologie Comparée (CICC), Université de Montréal, *« Pirater l'humain »*, 2009

[5] IBM, *« Sécurité et protection de données sensibles »,* 2006

[6] Stéphane GILL, *« Type d'attaque »*, 2003

[6] Fabrice HARROUET, Ecole Nationale d'Ingénieurs de Brest, *« Ecoute du réseau et usurpation d'identité »*

[7] Jean-Olivier GERPHAGNON, *« Attaques informatique »*

[8] Cyrille DURET, *« Les attaques Internet et les moyens de s'en protéger »,* 2002