

# Audit technique et pentest

---

*Etat de l'art, situation et évolution*



## Mémoire de fin d'étude

*Master Sciences et Technologies,  
Mention Informatique,  
Parcours Cryptologie et Sécurité Informatique.*

### **Auteur**

Rémi Tremblain <remi.tremblain@etu.u-bordeaux.fr>

### **Superviseur**

Pierrick Conord <pierrick.conord@soprasteria.com>

### **Tuteur**

Emmanuel Fleury <fleury@labri.fr>

---

10 juin 2016



### **Déclaration de paternité du document**

Je certifie sur l'honneur que ce document que je soumet pour évaluation afin d'obtenir le diplôme de Master en *Sciences et Technologies, Mention Informatique, Parcours Cryptologie et Sécurité Informatique*, est entièrement issu de mon propre travail, que j'ai porté une attention raisonnable afin de m'assurer que son contenu est original, et qu'il n'enfreint pas, à ma connaissance, les lois relatives à la propriété intellectuelle, ni ne contient de matériel emprunté à d'autres, du moins pas sans qu'il ne soit clairement identifié et cité au sein de mon document.

**Date et Signature**



# Résumé

Le monde de la sécurité informatique est en constante évolution et nous voyons aujourd'hui l'avancement de ce domaine. Ce domaine est considéré comme un point important dans le développement d'une entreprise et sa nécessité n'est aujourd'hui plus à discuter à mesure que le temps passe. En effet, peu importe la taille de l'infrastructure ou les données qu'elle traite, l'entreprise utilise dans la quasi totalité du temps du matériel informatique. Et qui dit matériel informatique dit sécurité informatique. Ceci passe par la mise en place de standard, de règle, de formation ou encore de sensibilisation du personnel mais elle reste souvent source de problème dans les entreprises, l'actualité quotidienne sur le sujet faisant foi.

Domaine de plus en plus important, de plus en plus prisé et reconnu important dans n'importe quelle infrastructure. Forte croissance du nombre de machines et de la demande en sécurité informatique derrière. D'où vient cette nécessité ? Qu'en est-il de maintenant ? Où va-t-on ? le modèle de bug bounty ba bla

Sécurité informatique importante Pas le même besoin qu'avant (Sécurité par le risque)

Nombreux standards maintenant pour répondre aux exigences des sociétés  
Offre et demande

Evolution depuis les années 2000



# Présentation de l'entreprise

Ce travail a été effectué dans le cadre du stage de fin d'étude qui se déroulait sur une période de six mois, au sein de la société Sopra Steria. Les informations qui suivent sont une présentation de la société, de son organisation ainsi que son activité.

## Activité

### A retravailler

Sopra Steria est un leader européen de la transformation numérique. Le groupe se positionne dans le top quatre en France et dans le top dix en Europe des sociétés de services IT (source Gartner). Avec un chiffre d'affaire annuel de 3,6 Milliards d'euros en 2015 et plus de 37 000 collaborateurs Sopra Steria est localisée dans plus de vingt pays à travers le monde, principalement en Europe.

La révolution du numérique est une source d'opportunités pour nos clients dans leur transformation et la fourniture de service de qualité tout en maîtrisant cet écosystème IT ainsi que son coût.

Sopra Steria se définit en quatre points :

- Accompagner nos clients dans leur transformation numérique.
- Créer et opérer des services innovants pour faire de ces mutations un atout majeur.
- Gagner en réactivité et flexibilité pour accompagner la croissance et la compétitivité.
- Maîtriser la qualité et les coûts sur les systèmes existants.

A compléter Introduction de schéma & explication des divers secteurs Focus sur la BU Cyber Sécurité





# Table des matières

## Partie 1. Etat de l'art & aspect théorique

---

<b>1</b>	<b>Etat de l'art</b>	<b>5</b>
1.1	Enigma	5
1.2	Les années 60 & ARPANet	6
1.3	Les années 70	7
1.4	Année 80	7
1.5	Année 90	7
1.6	De nos jours	7
<b>2</b>	<b>Aspect théorique</b>	<b>9</b>

## Partie 2. Situation

---

<b>3</b>	<b>En terme de technique</b>	<b>13</b>
<b>4</b>	<b>En terme juridique</b>	<b>15</b>
<b>5</b>	<b>Constat, ce qu'il faut modifier, pour faire le lien avec la partie d'après</b>	<b>17</b>

## Partie 3. Evolution

---

<b>6</b>	<b>En terme de technique</b>	<b>21</b>
<b>7</b>	<b>Pour le grand public ?</b>	<b>23</b>

## Annexes

---

<b>A</b>	<b>Aux cas où</b>	<b>29</b>
<b>B</b>	<b>Pour la forme</b>	<b>31</b>



# Introduction

Le secteur de la sécurité informatique connaît une croissance importante depuis les années 90, de part son importance dans les entreprises et la démocratisation de l'informatique tout public. On retrouve en effet l'informatique dans toutes ces formes à tout les niveaux de l'industrie, par la gestion d'informations plus ou moins sensible, mais aussi chez les aussi chez les particuliers désireux d'explorer un monde informatique qui évolue très rapidement.

Cependant, une faible proportion des utilisateurs d'éléments informatique (internet, ordinateur, etc) est correctement sensibilisée à la bonne pratique de ces derniers. Et c'est ici le commencement de la réflexion sur lequel ce rapport se porte. En effet, si l'informatique se démocratise, il est important d'en connaître les bonnes pratiques, les enjeux et risques que se développement rapide provoque et plus particulièrement sur l'aspect de la sécurisation informatique dites industrielle.

Nous allons donc aborder ce mémoire de façon chronologique, avec, dans un premier temps, un état de l'art de la sécurisation informatique, en expliquant les prémices de l'informatique et de la sécurisation informatique. Nous discuterons dans cette même partie de l'aspect théorique de la sécurisation informatique comme notamment ce qu'il est nécessaire de sécuriser ou pourquoi sécurisé tels ou tels informations. Dans un second temps, pour aborder plus l'aspect du présent, nous oartirons sur une partie dites techniques en expliquant ce qu'il existe de nos jours en terme d'outils, de prestation ou de modèle pour cadrer et mettre en place une sécurisation informatique appliqué à l'industrie. Nous parlerons aussi du cadre juridique qu'il est nécessaire de mettre en place pour excercer ce genre d'activité. Enfin, pour aborder le furur de la sécurité informatique, nous nous dirigerons vers les modèles qui tendent à emmerger, l'évolution des pratiques ou encore l'ouverture au grand public.

Dans ce mémoire, l'auteur se basera sur sa vision de la sécurité informatique dites industrielle à travers la société Sopra Steria, productrice de service de sécurisation informatique, et de son ouverture au niveau international.



# Première partie

---

## **Etat de l'art & aspect théorique**



## Etat de l'art

Dans cette partie, nous aborderons la question du “Pourquoi”, en expliquant les origines de la sécurité informatique, les idées reçues sur cette discipline aussi nouvelle qu’incomprise et pourquoi elle est aujourd’hui estimée comme un aspect primordial, voir obligatoire, dans le développement d’une entreprise.

Mais si nous devons parler de l’état actuelle de la sécurité informatique, il est important de parler de ses origines, nous nous intéresseront donc dans un premier temps au développement de l’informatique lui même en établissant un état de l’art. Pour cela, nous allons expliquer à travers différents moments clé de l’histoire qui ont permis la naissance et le développement de l’informatique tel que nous le connaissons aujourd’hui.

*Développement chronologique à revoir, plus raconté*

### 1.1 Enigma

Impossible de parler de sécurité informatique sans parler de cette invention faites par des cryptographes polobais en 1918 : Enigma . A l’origine, ce dispositif electromécanique de cryptage par rotor fut inventé pour sécuriser les communications bancaires, mais l’armée allemande en trouve une utilité tout autres en s’en servant pour sécuriser ses communications durant la seconde guerre mondiale. Mais le plus important dans cette invention fut été la réponse faites par les alliées, avec l’aide d’Alan Turing<sup>1</sup> avec la création de la machine Colossus<sup>2</sup> pour briser les codes provenant d’Enignma. On accrédite d’ailleurs la fin de la guerre d’une année plus tôt à cette machine.

On voit donc à partir de cette date, l’apparition de ce que l’on pourrait appeler le premier ordinateur, ouvrant ainsi la porte à l’informatique moderne.

---

1. Mathématicien et cryptologue britannique né en 1912 et mort en 1954, auteur de travaux qui fondent scientifiquement l’informatique

2. Premier calculateur électronique fondé sur le système binaire

## 1.2 Les années 60 & ARPANet

On se place désormais dans les années 60 et sur le commencement de l'industrialisation des ordinateurs grand public. Mais cette période apporte son lot en matière d'avancement de la sécurité informatique et nous allons comprendre pourquoi avec quelques faits historiques marquants.

Un des points importants de l'évolution de l'informatique ce passe avec un groupe d'étudiants du MIT qui, vers 1959, fondent le Tech Model Railroad Club (TMRC) afin d'obtenir l'accès à ce que l'on appellera aujourd'hui le premier ordinateur industrielle : le PDP-1. A travers leur club ils commencèrent à étudier, explorer et coder sur cette unité centrale et mettent au point le premier jeu vidéo sur micro-ordinateur : Spacewar. Mais ce n'est pas le plus important fait relayé à ce club, en effet on lui attribua la naissance du terme "hack" et de tout ses dérivés, mais aussi tout un jargon qui fait maintenant partie du Jargon File<sup>3</sup>.

Le fait le plus marquant dans l'évolution de l'informatique se passe en 1969 avec un projet mené le Ministère de la Défense américaine (DoD) : le réseau Advanced Research Projects Agency Network (ARPANet). Ce projet permetta de relier quatre universités américaines à travers les États-Unis grâce à un concept de transfert de paquets, qui deviendra par la suite la base du transfert de données sur internet. L'intérêt de cette avancée se situait sur le fait que les communications étaient basées sur la communication par circuits électroniques, telle que celle utilisée par le réseau téléphone, où un circuit dédié est activé lors de la communication avec le poste du réseau. Mais avec le réseau développé par la DARPA, on met en avant une communication plus robuste et capable d'être établie sur de plus grande distance. Il a été en effet développé dans le but de continuer à fonctionner malgré une attaque nucléaire massive de la part de l'Union soviétique (contexte de la guerre froide) et permettant à un paquet émis d'adapter son chemin en fonction de l'état du réseau (changement de nœud, etc).

Enfin, on ne peut parler des années 60 sans parler du développement d'UNIX par Ken Thompson, 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.

On peut donc penser que cet époque apporte son lot d'événement majeur dans le développement de l'informatique, de part le jargon mis en place et très largement utilisé de nos jours, mais aussi par l'environnement UNIX qui a vu le jour et le langage de programmation le plus utilisé aujourd'hui. Mais le plus gros impact de cette décennie reste la mise en place du réseau ARPANet, ancêtre de l'internet, mais qui se positionne comme étant un moyen d'échanger des données sur un réseau et ce, sans se préoccuper de la distance. Il

---

3. Glossaire spécialisé dans l'argot des programmeurs



restera cependant limité aux universités et professionnel dans ses premières versions.

### 1.3 Les années 70

Les années 70 quant à elles, sont importante pour la démocratisation de l'informatique pour le grand public en palliant aux problème d'accès au réseau de donnée ARPANet. En effet, la société Bolt, Beranek et Newman, met au point le protocole de communication Telnet<sup>4</sup> comme étant une extension publique du réseau ARPANet, cassant ainsi le privilège des entrepreneurs et des chercheurs du monde académique quant à son accès. Ce protocole ouvre donc la voie à l'utilisation du réseau de donnée pour le grand public. Mais cependant, l'accès au matériel informatique nécessaire pour l'accès au réseau reste compliqué. Et c'est sur ce point que Steve Jobs et Steve Wozniak créent Apple Computer et mettent au point et commercialisent l'ordinateur personnel ou PC (de l'anglais Personal Computer). Le PC devient alors un accélérateur dans 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 que des modems analogues ou des logiciels dédiés (war dielers). Comme la sécurité telle que nous la connaissons actuellement n'existait pas, il était d'autant plus facile de trouver et d'exploiter des vulnérabilités sur les sytèmes informatiques.

C'est dans cette période là que la nécessité de sécurité informatique commence à se faire désirer, puisque l'accès à l'information commence à être de plus en plus facile et de plus en plus dangereuse étant donné que les standards de contrôle ne sont pas encore mis en place.

### 1.4 Année 80

IBM et Intel 8086 > utilisation personnel Protocol TCP 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

### 1.5 Année 90

Fin de l'ARPANet et création du WWW La navigateur Web graphique voit le jour et engendre une croissance exponentielle de la demande pour l'accès public à l'interne 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).

### 1.6 De nos jours

Tous les jours, environ 225 cas majeurs de brèches de sécurité sont rapportés au Centre de Coordination du CERT à l'université de Carnegie Mellon

---

4. TErминаl NETwork ou TELecomunication NETwork, ou encore TELetype NETwork

En 2003, le nombre d'infractions rapporté au CERT est monté à 137.529, par rapport à 82.094 en 2002 et par rapport à 52.658 en 2001 L'impact économique au niveau mondial des trois virus Internet les plus dangereux ayant surgi au cours des trois dernières années a atteint un montant total de US13, 2*milliards*

La sécurité informatique fait désormais partie des dépenses non seulement quantifiables, mais justifiables incluses dans tout budget IT. Les sociétés nécessitant de l'intégrité et la haute disponibilité de données recourent aux capacités des administrateurs système, développeurs et ingénieurs pour assurer la fiabilité de leurs systèmes, services et informations 24 heures sur 24, 7 jours sur 7. La possibilité de devenir la victime d'attaques coordonnées, d'utilisateurs ou de processus malveillants représente une véritable menace au succès d'une société.

## CHAPITRE 2

# Aspect théorique

Qu'est ce que l'on doit sécurisé? Trop de sécurité tue la sécurité -> trop  
emcombrant pour l'utilisateur L'user va chercher à bypass les systèmes  
Sécurisation des systèmes critiques Sécurisation en fonction de ce qui existe



## Deuxième partie

---

### **Situation**

Qu'est ce que l'on fait maintenant

## CHAPITRE 3

# En terme de technique

Routine rapport conseil

Différence entre audit et pentest

Audit : Conforme (mais vulnérable ?) Pentest : On casse tout





## CHAPITRE 4

# En terme juridique

Pentest Encadrement



## CHAPITRE 5

# **Constat, ce qu'il faut modifier, pour faire le lien avec la partie d'après**

Décalage bla bla bla



## Troisième partie

---

### **Evolution**





## En terme de technique

Bug bounty, Uberisation du modèle Prestation moins chère, on fournit des pages, plus du service Iso, certification





## CHAPITRE 7

# Pour le grand public ?

Nombreuses presations



# Conclusion

La sécurité informatique c'est cool C'est super nouveau, soumis a plein de changement Plein de logiciel libre (mentalité du monde du piratage informatique)



## **Annexes**



ANNEXE **A**

**Aux cas où**





## **Pour la forme**

