Audit technique et pentest

Etat de l'art, situation et évolution

université de BORDEAUX

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>

9 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 mone 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 necessité n'est aujourd'hui plus à discuter à mesure que le temps passe. En effet, peut 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 qu'elle infrastructure Forte croissance du nombre de machine et de la demande en sécurité informatique derriere D'où vient cette necessité ? 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 standard 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 soéciétés de services IT (source Gartner).
Avec un chiffre d'affaire annuel de 3,6 Milliards d'euros en 2015 et plus de 37 000 colaboraters Sopra steria est localisée dans plus de vingts pays à travers le monde, principalement en Europe.

La révolution du numérique est une source d'opportunités pour nos clients dans leur transformtion et la fourniture de service de qualité tout en maitrisant cet écosystème IT ainsi que son coût.
Sopra Steria se définit en quatres 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 coissance et la compétitivité.
- Maîtriser la qualité et les coûts sur les systèmes existants.

A completer Introduction de shéma & explication des divers secteurs Focus sur la BU Cyber Sécurité

Table des matières

Introduction

Le secteur de la sécurité informatique connait une croissance importante depuis les années 90, de part son importance dans les entreprises et la démoncratisation 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.

Cepandant, 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 reflexion sur lequel ce rapport ce porte. En effet, si l'informatique se démocratise, il est important d'en connaitre 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 sécuritsation 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 nottament ce qu'il est necessaire de sécuriré 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 préstation 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 necessaire 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

CHAPITRE 1

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 estimé 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 et d'établir 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 la sécurité informatique et de l'information.

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 [1] avec la création de la machine Colossus [2] 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.

1.2 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 mais aussi par son jargon. Et c'est en 1949 que des étudiants du MIT fondent le Tech Model Railroad Club afin d'obtenir l'accès a ce que l'on appelle aujourd'hui le premier ordinateur industrielle : le PDP-1. A travers leur club ils ont effet commencer à etudier, explorer et coder sur cette unité centrale et mettent aux jours

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.

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

1.3 Les années 70

Protocole Telnet par Bolt, Beranek et Newman. Ouverture grand public > autrefois fermé aux entreprise

Steje Jobs et Wozniak : Apple Computer > accès grand public a du matériel de hacking

Jim Ellis et Tom Truscott : USENET (forum)

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

CHAPITRE 2

Aspect théorique

A revoir, pas tès clair, partie utile ?
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

CHAPITRE 6

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

ANNEXE B

Pour la forme

Bibliographie

[1] Jean Dupont and Patrick Durand. *Titre du LIVRE*. Flammarion, 2014.

[2] Prenom1 Nom1, Prenom2a Prenom2b Nom2, and Prenom3 Nom3. Titre de l'article. *Conférence Internationale sur la sécurité dans le Monde*, 2013.

Index