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>

16 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 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

Partie 1. Etat de l'art & aspect théorique

1 Etat de l'art **5**
- 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 8
- 1.6 De nos jours 9

2 Aspect théorique **11**

Partie 2. Situation

3 En terme de technique **15**
- 3.1 Audit de sécurité 15
- 3.2 Pentest 15
- 3.3 Limitation - lien avec le juridique 15

4 En terme juridique **17**

5 Constat, ce qu'il faut modifier, pour faire le lien avec la partie d'après **19**

Partie 3. Evolution

6 En terme de technique **23**

7 Pour le grand public ? **25**

Annexes

A Aux cas où **31**

B Pour la forme **33**

Bibliographie **35**

Index **37**

Introduction

Le secteur de la sécurité informatique connait 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 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 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 sécurité ou pourquoi sécurisé tels ou tels informations. Dans un second temps, pour aborder plus l'aspect du présent, nous partirons 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 exercer ce genre d'activité. Enfin, pour aborder le futur de la sécurité informatique, nous nous dirigerons vers les modèles qui tendent à immerger, 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, 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 polonais en 1918 : Enigma . A l'origine, ce dispositif électromécanique 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. 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 historique marquant.

Un des points important 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 a 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 attribuera la naissance du terme "hack" et de tout ses dérivés, mais aussi tout un jargon qui fait maintenant partie du Jargon File [3].

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 permettra de relier quatre université américaine 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 avancé se situait sur le fait que les communications étaient basées sur la communication par circuits électronique, 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 établi 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 noeud, 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'évènement majeur dans le développement de l'informatique, de part le jargon mise en place et très largement utilisé des nos jours, mais aussi par l'environnement UNIX qui a vu le jours 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 ARAPNet, 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 res-

3. Glossaire spécialisé dans l'argot des programmeurs

tera 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 [4] 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 dédies (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 systèmes informatiques.
On peut aussi noter l'apparition d'un système de messagerie pour la communication électronique entre des utilistateurs très variés. USENET, crée par Jim Ellis et Tom Truscott, devient rapidement l'un des forums les plus popplulaire pour l'échange d'idées en matière de toute et n'importe quoi, mais principalement d'informatique, de mise en réseau et bien évidemment, de craquage.
C'est dans cette période là que la nécessite de sécurité informatique commence à se faire ressentir, 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 et que ce domaine reste assez nouveau.

1.4 Année 80

Dans les années 80, IBM [5] fait une avancée en matière d'équipement informatique en produisant des ordinateurs basé sur le microprocesseur Intel 8086. Ce processeur de faible coût permet à l'informatique de passer d'une utilisation purement professionnelle à une utilisation personnelle, et cela permet à l'ordinateur de devenir un produit ménager de consommation courante. Ce changement de situation permet de rendre le PC plus abordable, puissant mais aussi plus simple d'utilisation et contribue à une prolifération de ce matériel dans l'environnement professionnel et personnel, et par conséquence dans celui d'utilisateurs malintentionnés.

Mais avec ce développement soudain de l'informatique et de ses mauvaises pratiques, le monde fait face à une recrudescence de des délits informatiques, nottament avec les deux groupes pionners en matière de piratage

4. TErminal NETwork ou TELecommunication NETwork, ou encore TELetype NETwork
5. Expliqué le sigle

informatique qui commencent à se faire remarquer dans leur exploitation des faiblesses des ordinateurs et des réseaux de données éléctroniques : Legion of Doom et Chaos Computer Club. Mais un constat rapide est dressé : la loi n'est pas suffisament armée pour faire face à cette nouvelle tendance. Ce n'est qu'en 1986 que le congrès américain vote une loi sur la répression des fraudes et des infractions dans le domaine informatique [6] à la suite des exploits de Ian Murphy, plus connu sous le nom de Captain Zap, qui reussissa l'exploit de s'introduire dans les oridnateurs de l'armée pour voler des informations des bases de données de commandes de diverses sociétés et utiliser des standards téléphoniques gouvernemantaux à accès limités pour effectuer des appels personnels. Cette avancement en matière de juridiction met donc l'accent sur la dangereusité de l'informatique et sur la nécessité de cadrer ce qui s'en rapporte et donc, par conséquence de la nécéssité de la sécurité informatique.

Transition à travailler

Suite à l'augmentation des menaces informatiques, et par crainte que le « ver Morris » [7] 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.

On voit donc apparaitre dans les années 80 les réponses aux problèmes informatiques moderne de part les institutions qui émergent mais aussi par la réglementation qui s'impose pour faire face aux nouvelles menaces.

1.5 Année 90

La période des années 90 est la plus intéréssante pour le développement de notre mémoire. C'est celle-ci qui marque les plus grandes avancées dans le domaine de l'informatique et de sa sécurité. Commençons avec le fait plus marquant de cette période avec la décomission de l'ARPANet et le transfert de son trafic vers le World Wide Web tel que nous le connaissons aujourd'hui. C'est avec ce transfert que le premier navigateur Web graphique voit le jour : WordlWideWeb. Cette innovation engendrant une croissance exponentielle de la demande pour l'accès public à l'internet. Avec cette explosion de l'internet, les délits se multiplient, comme nottement avec KEvin Mitnick, considéré comme le plus célèbre de tout les pirates, pour s'être introduit dans les systèmes de plusieurs grandes sociétés et avoir volé toute sorte de données allant des informations personnelles de personnes célèbres à plus de 20.000 numéris de cartes de crédit en passant par l'extraction de code source de logiciels propriétaires
C'est par la même occasion que 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).

6. Computer Fraud and Abuse act
7. En référence à son créateurRobert Morris, un diplômé universitaire qui infectat pas moins de 6000 machines relié à l'internet.

1.6 De nos jours

Entre les années 1990 et 2000, le nombres d'ordinateurs est passé d'un million à plus de 370 millions, la barre du milliard de sites web a même été franchie en 2014. L'accès à l'informatique et internet s'est vu banaliser, au même titre que l'accès à du contenu de nature contreversé, comme avec des ressources sur le darknet [8] ou les forums de discussions décentralisés. Cependant, avec toutes cette activité, le nombre d'incident augmente et 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. 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 US$13,2 milliards

On voit donc bien avec ce développelement historique de l'informatique et de ses besoins en matière de sécurité informatique, nottament pour les industries, pour qui la sécurité fait désormais partie des dépenses non seulement quantifiables, mais justifiables incluses dans tout budget. 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.

8. Réseau privé virtuel anonymisé

CHAPITRE 2

Aspect théorique

La sécurité de l'information et de la sécurité informatique en général est soumise à des contraintes particulière car elle s'appuie essentiellement sur la bonne coopération de l'utilisateur. Car de nos jours, 90% des problèmes de sécurité informatique sont dût à une négligeance humaine.
La question légitime qu'il serait bon de se poser serait de savoir ce que l'on doit sécurisé, à laquelle on pourrait répondre "tout". Mais la sur-sécurisation reste un problème dans le sens où elle est beaucoup trop compliqué à mettre en place de part la compléxité de la tâche, l'intrusivité et la bienveillance de l'utilisateur. Car la sécurité informatique n'est pas réservé à une élite formaté dans le domaine, elle passe avant tout par l'utilisateur.

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

La sécurité informatique est aujourd'hui quelque chose de très important dans le développement d'une entreprise, comme nous l'avons vu dans la partie précédente. Nous allons voir dans cette partie ce qu'il éxiste en terme d'outils et de prestation dans le monde de la sécurité informatique, en se penchant d'avantage sur la mise en oeuvre de test d'intrusion (ou pentest) et sa valeur vis à vis d'un audit de sécurité standard. Nous ferons le lien entre la partie précédente pour voir et constater si l'on est ou pas en mesure de répondre aux menaces en matière d'informatique. Nous verrons aussi par la suite tout ce qui touche au cadre légale et juridique, car, les différentes forme de sécurité (offensive [1] et défensiveAudit technique) doit être cadré pour ne pas nuir à l'audité, ce qui serait contre-productif. On verra également la valeur ajouté des certifications et des normes ISO qui fleurissent actullement et leurs effets sur les prestations que les entreprises peuvent proposer et pourquoi elles deviennent de plus en plus nécessaire.

1. Pentest

CHAPITRE 3

En terme de technique

En terme de technique, nous allons voir ce qu'il existe en terme d'outillage pour réaliser les audits techniques (et tous ses variantes) et les tests d'intrusions, mais aussi la méthodologie qui y est liée.

3.1 Audit de sécurité

L'audit de sécurité d'un système d'information (SI) est une vue à un instant T de tout ou partie du SI, permettant de comparer l'état du SI à un référentiel.

L'audit répertorie les points forts, et surtout les points faibles (vulnérabilités) de tout ou partie du système. L'auditeur dresse également une série de recommandations pour supprimer les vulnérabilités découvertes. L'audit est généralement réalisé conjointement à une analyse de risques, et par rapport au référentiel. Le référentiel est généralement constitué de :

la politique de sécurité du système d'information (PSSI) la base documentaire du SI réglementations propre à l'entreprise textes de loi documents de référence dans le domaine de la sécurité informatique

3.2 Pentest

Les tests d'intrusion sont une pratique d'audit technique. On peut diviser les tests d'intrusion en trois catégories principales : les tests boîte blanche, les tests boîte grise et les tests dits boîte noire.

3.3 Limitation - lien avec le juridique

Routine rapport conseil

Différence entre audit et pentest

Audit : Conforme (mais vulnérable ?) différente forme d'audit

Pentest : On casse tout Différent outils à disposition (scanneur, automatisation de rapport, travail à la mano)

CHAPITRE 4

En terme juridique

Certif, iso Audit Pentest Encadrement -> scope

CHAPITRE 5

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

Décalage On fournit un travail mais cen 'est pas forcément suivi par tout le monde

Troisième partie

Evolution

CHAPITRE 6

En terme de technique

Bug bounty, Uberisation du modèle -> court circuit -> Twitter a corrigé plsu de 360 failles critiques Prestation moins chère, on fournit des pages, plus du service Iso, certification

CHAPITRE 7

Pour le grand public ?

Nombreuses presations Ouverture

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

Alain Turing, 5

Colossus, 5

Enigma, 5

Résumé, v

Spaceware, 6