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>

4 août 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 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.

Historique

En janvier 2015, Sopra et Steria ont choisi de s'unir dans le groupe Sopra Steria. Ils disposent d'une histoire et d'une culture proches : pionniers des services informatiques, ils se sont bâtis sur une forte culture entrepreneuriale et d'innovation.

Grâce à de très fortes complémentarités des métiers et des géographies, le nouvel ensemble propose l'une des offres les plus complètes du marché, répondant au mieux aux attentes du client.

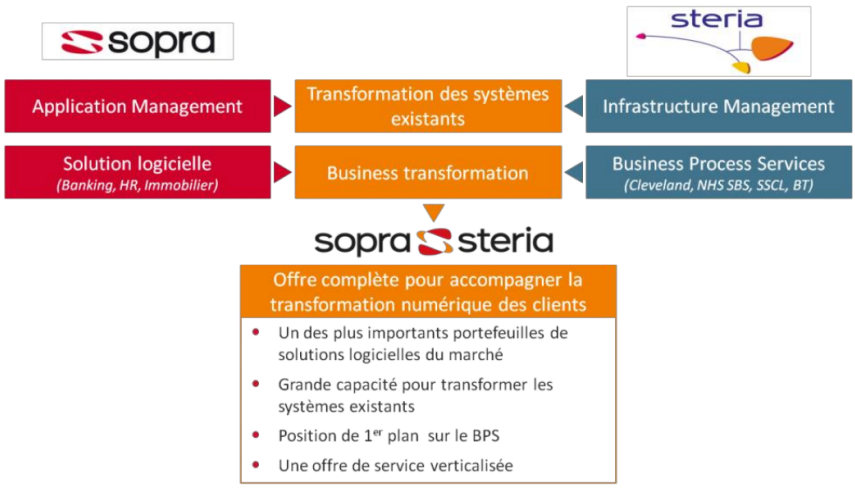

FIGURE 1 – Fusion Sopra & Steria

Sopra Steria est un leader européen de la transformation numérique. Le groupe se positionne dans le top 4 en France et dans le top 10 en Europe des sociétés de services IT (source Gartner).

Avec un CA de près de 3,4 Milliards d'euros (proforma) en 2014, Sopra Steria est localisé dans plus de 20 pays à travers le monde, principalement en

FIGURE 2 – Valorisation

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.

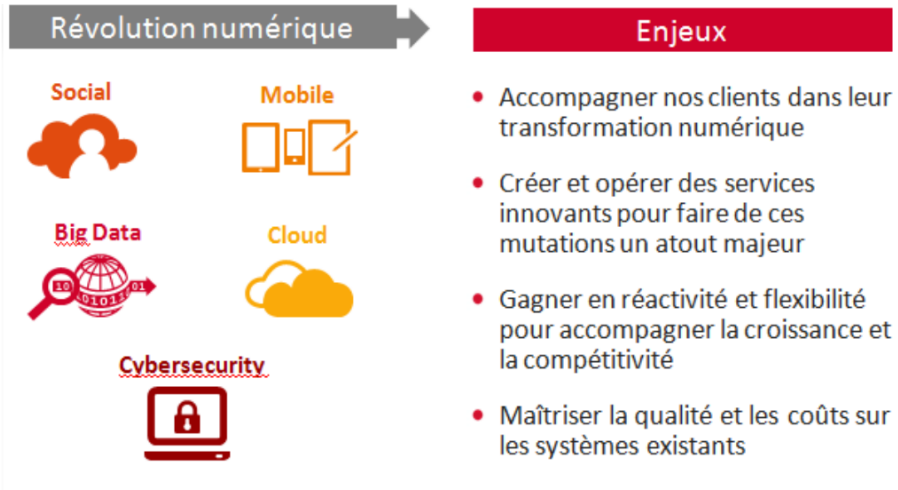

FIGURE 3 – Révolution numérique

Sopra Steria intervient sur l'ensemble des prestations d'accompagnement dans la réalisation de vos projets. Nos savoir-faire forment une chaîne continue de valeur ajoutée, du conseil Métier / SI à la gestion d'infrastructure en passant par l'intégration de système et la gestion d'applications.

Activité

L'ensemble de l'expertise de Sopra Steria est regroupé au sein de la filiale Solutions & Cyber dans une BU CyberSécurité sous la responsabilité d'Ilhame CHOUKRANI.

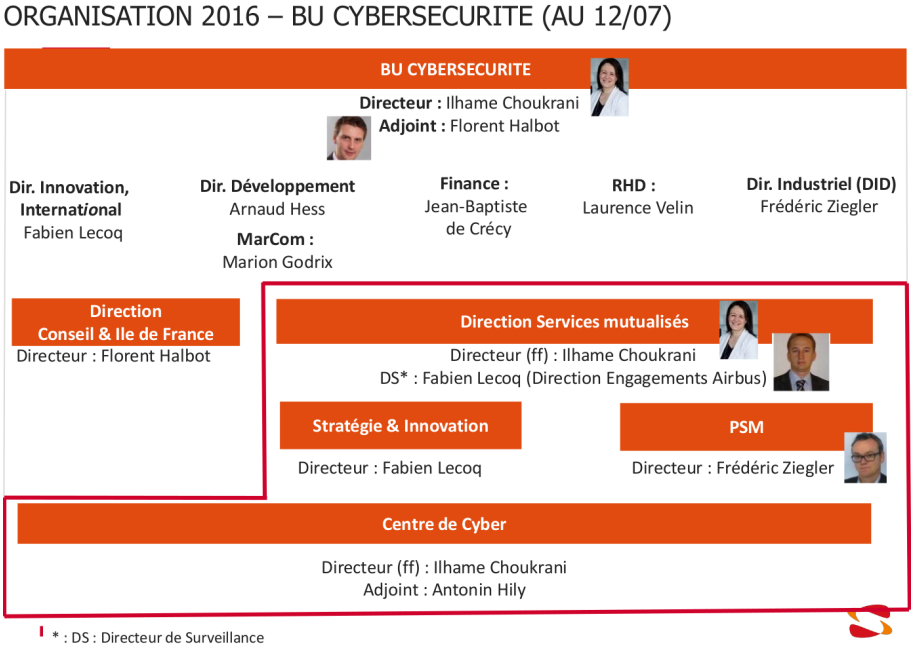

FIGURE 4 – Organigrame

Cette Business Unit compte :
— Plus de 200 consultants, experts SSI en France ;
— 3 Centres de CyberSécurité (France, UK et Singapour) ;
— Un budget R&D d'environ 3,3% du CA Sécurité.
Carte d'identité de la BU CyberSécurité et chiffres clés dans le monde :

FIGURE 5 – Carte d'identité

Table des matières

Introduction

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

Cependant, une faible proportion des utilisateurs d'éléments informatiques (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 ce développent rapide provoque et plus particulièrement sur l'aspect de la sécurisation informatique dite 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 sécuriser tel ou tel information. Dans un second temps, pour aborder plus un aspect actuel de la sécurité, nous partirons sur une partie dite technique en expliquant ce qu'il existe de nos jours en termes d'outils, de prestation ou de modèle pour cadrer et mettre en place une sécurisation informatique appliquée 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 dite 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, voire obligatoire, dans le développement d'une entreprise.
Mais si nous devons parler de l'état actuel de la sécurité informatique, il est important de parler de ses origines, nous nous intéresserons 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.

1.1 Enigma

Impossible de parler de sécurité informatique sans parler de cette invention faite par des cryptographes polonais en 1918 : Enigma . À l'origine, ce dispositif électromécanique de chiffrement par rotor fut inventé pour sécuriser les communications bancaires, mais l'armée allemande en trouve une utilité tout autre en s'en servant pour sécuriser ses communications durant la seconde guerre mondiale. Mais le plus important dans cette invention fut été la réponse faite par les alliées, avec l'aide d'Alan Turing [1] avec la création de la machine Colossus [2] pour briser les codes provenant d'Enigma. 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, au moment du commencement de l'industrialisation des ordinateurs grand public. Mais cette période apporte son lot d'avancement en matière de sécurité informatique et nous allons comprendre pourquoi avec quelques faits historique marquants.

Un des points importants de l'évolution de l'informatique se passe avec un groupe d'étudiants du MIT (Massachusetts Institute of Technology) qui, vers 1959, fonde le Tech Model Railroad Club (TMRC) afin d'obtenir l'accès a ce que l'on appellera aujourd'hui le premier ordinateur industriel : le PDP-1. À 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 tous 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 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 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 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 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'évènements majeur dans le développement de l'informatique, de par le jargon mis en place et très largement utilisé de 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 importantes pour la démocratisation de l'informatique pour le grand public en palliant aux problèmes d'accès au réseau de données 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 données 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 dialers). 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 utilisateurs très variés. USENET, crée par Jim Ellis et Tom Truscott, devient rapidement l'un des forums les plus populaire pour l'échange d'idées en matière de tout 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 nécessité 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 Années 80

Dans les années 80, IBM [5] fait une avancée en matière d'équipement informatique en produisant des ordinateurs basés 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, notamment avec les deux groupes pionniers 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 électroniques : Legion of Doom et Chaos Computer Club. Mais un constat rapide est dressé : la loi n'est pas suffisamment 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 réussissa l'exploit de s'introduire dans les ordinateurs de l'armée pour voler des informations des bases de données de commandes de diverses sociétés et utiliser des standards téléphoniques gouvernementaux à accès limités pour effectuer des appels personnels. Cette avancement en matière de juridiction met donc l'accent sur la dangerosité de l'informatique et sur la nécessité de cadrer ce qui s'en rapporte et donc, par conséquence de la nécessité 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 modernes de par 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 intéressante 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 décommissions 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 nettement avec Kevin Mitnick, considéré comme le plus célèbre de tous 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 numéros 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 créateur Robert Morris, un diplômé universitaire qui infectât pas moins de 6000 machines relié à l'internet.

1.6 De nos jours

Entre les années 1990 et 2000, le nombre 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 controversé, comme avec des ressources sur le darknet [8] ou les forums de discussions décentralisés. Cependant, avec toutes ces activités, 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 d'US $13,2 milliards

On voit donc bien avec ce développement historique de l'informatique et de ses besoins en matière de sécurité informatique, notamment 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 particulières 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 négligence humaine.
La question légitime qu'il serait bon de se poser serait de savoir ce que l'on doit sécuriser. Ce à quoi 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 par la multitude d'information disponible, la complexité de la tâche et de la mise en place, 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 lambda.
De nos jours, la mise en place de sécurité informatique passe par un raisonnement et un travail sur l'utilisateur et ce afin qu'elle soit le plus efficace possible. Elle ne doit pas être trop intrusive (pop-up, demande d'autorisation, UAC [1], etc), trop envahissante ou trop compliqué pour que son utilisation soit la plus intuitive possible et faire en sorte qu'elle soit naturelle par l'utilisateur.

Un autre problème est qu'avant les années 2000, la sécurisation par le risque était très peu mise en oeuvre : on sécurisait les endroits où l'on était attaqué. On pourrait appeler ça une sécurisation par "le dégât", étant donné que l'attaque a déjà eu lieu. On y oppose à cette forme de sécurisation, la sécurisation par le risque. Elle s'effectue par la réalisation des analyses de risques et en sécurisant les éléments essentiels, les "organes vitaux" du système.

Nous allons donc voir dans la partie suivante ce dont on dispose pour réaliser la mise en place de toute la sécurité informatique, des outils mais aussi des méthodologies à notre disposition pour être actif et efficient.

1. User Access Control de Miscrosoft

Deuxième partie

Situation technique

CHAPITRE 3

Prémices

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 existe 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 défensive [2]) doit être cadré pour ne pas nuire à l'audité, ce qui serait contre-productif. On verra également la valeur ajouté des certifications et des normes ISO qui fleurissent actuellement et leurs effets sur les prestations que les entreprises peuvent proposer et pourquoi elles deviennent de plus en plus nécessaire.

En terme de technique, nous allons voir ce qu'il existe en terme d'outillage pour réaliser les audits techniques (et ses variantes) et plus particulièrement les tests d'intrusions et les méthodologies qui y sont liées.
Mais commençons par distinguer tests d'intrusion et audit de sécurité, car il s'agit de deux notions qui peuvent paraître similaires au premier abord mais dont les cadres respectifs ne correspondent pas forcément et dont il est important de faire une différence. Un audit de sécurité est plus large qu'un test d'intrusion, lors d'un audit de sécurité, nous allons vérifier la sécurité organisationnelle, le PRA/PCA (Plan de Reprise et Plan de Continuité d'Activité), DLP (Data Loss Prevention), la conformité par rapport aux exigences d'une norme (exemple : PCI DSS) ou un référentiel, et également procéder à une correspondance orale avec les membres du SI [3], DSI [4], RSSI [5] et membres de

1. Pentest
2. Audit technique
3. Système d'Information
4. Directeur des Systèmes d'Information
5. Responsable de la sécurité des systèmes d'information

l'équipe technique , à un audit des configurations des services, serveurs, composants réseaux, etc., également l'audit de code pour les applications utilisées, déployées, voir développées en interne par l'entreprise cliente, et enfin effectuer une analyse des risques (EBIOS, MEHARI, MARION).

Parmi les référentiels souvent utilisés pour l'audit de sécurité, on retrouve la norme ISO 27 000 / ISO 27 001, le référentiel général de sécurité de l'ANSSI, le référentiel COBIT et dans d'autres contextes, les normes de type SOX, PCI-DSS, etc. Nous verrons cela plus précisément dans une partie dédiée prochainement.

CHAPITRE 4

Audit de sécurité

Nous allons donc parler plus précisément de l'Audit de sécurité dans cette partie. 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'objectif d'un audit de sécurité est de recenser les points forts mais aussi les points faibles (ou vulnérabilités) du système audité. A la suite de ce recensement, l'auditeur dresse une série de recommandations pour résoudre les points faibles trouvés. On réalise conjointement une analyse de risque afin de rendre l'audit le plus complet possible. L'audit se déroule en fonction d'un référentiel, dont voici les principaux points :

— La politique de sécurité du système d'information (PSSI) : Il s'agit d'un plan d'action afin de maintenir un niveau de sécurité donné.
— La base documentaire du SI.
— La réglementations propre à l'entreprise, comme notamment la nécessite de chiffrer les périphériques de stockage.
— Les textes de loi.
— Les documents de référence dans le domane de la sécurité informatique.

Nous avons vu dans la partie précédente ce qui nous avait amené à repenser notre façon de sécuriser nos systèmes d'informations et la mise en place d'audit de sécurité peut être une méthode pour prévenir des risques. Ce couteau suisse de la sécurité informatique peut être utilisé pour différent aspect :

— Réagir à une attaque, en analysant le vecteur d'attaque, la cible, etc.
— Se faire une idée de ce que l'auditeur possède en terme de sécurité.
— Tester la mise en place effective de la politique de sécurité du système d'information.
— Ter un nouvel équipement et son intégration dans le réseau de l'audité.
— Evaluer l'évolution de la sécurité, mais cela implique la réalisation d'audit périodique.

Mans dans tous les cas, il a pour but de vérifier la sécurité et pour cela, il fournit en résultat un rapport d'audit. Celui-ci est constitué de la liste exhaustive des vulnérabilités recensées par l'auditeur sur le système analysé. Il contient également une liste de recommandations permettant de supprimer les vulnérabilités trouvées.

Nous allons voir les différentes pratiques qui existent et qui sont généralement utilisées pour arriver à produire un audit de sécurité :

— **Interviews** : Les interviews sont réalisées sur toutes les personnes ayant un rôle dans la mise en place ou l'utilisation de la sécurité informatique sur SI. On y retrouve généralement le DSI, le ou les RSSI, les différents administrateurs, les utilisateurs du système d'informations peut importer leur rôle dans l'entreprise, ainsi que tout autre rôle ayant un lien avec la sécurité.
Un des aspects importants sur le rôle de l'auditeur lors des interviews est faire preuve de diplomatie afin de pas faire sentir à l'audité le moindre jugement du fait qu'il est interrogé sur son travail, ce qui pourrait fausser les résultats et rendre l'audit moins pertinent.

— **Test d'intrusion** : Les tests d'intrusions sont une partie importante des audits techniques. Ils permettent de vérifier un système de sécurité d'une manière très perspicace puisque que l'auditeur se positionne en tant qu'un attaquant afin de vérifier le plus précisément possible l'état de la sécurité informatique du système d'information.
Mais tout ceci sera expliqué dans une partie dédié aux tests d'intrusions, du fait qu'il y ai eu une plus grande activité dessus lors du stage.

— **Relevé de configuration** : Dans cette partie, il s'agit d'analyser, le plus pertinemment possible, les composants du système d'information. On se focalisera tout particulièrement sur les configurations utilisées. A la suite de cette observation, la liste des vulnérabilités est dégagée en comparant le résultat à des configurations réputées sécurisées et à des ensembles de failles connues. Beaucoup d'aspects peuvent être contrôlés durant un relevé de configuration, allant de l'architecture du SI aux applications, en passant par les hôtes (clients et serveurs).

— **Audit de code** : Lors d'un audit de code, le but est de comprendre le code source, pour en analyser la sécurité et déceler les éventuels problèmes qui peuvent exister, comme les dépassements de tampon ou les bugs de format pour un programme, ou encore les vulnérabilités menant à des failles XSS [1] ou des injections SQL.
L'audit de code étant fastidieuse dans certain cas (gros projet, architecture compliqué, etc.), l'utilisation d'outils d'analyse de code, comme RATS [2], permet de "dégrossir" le travail, mais cela reste un traitement automatique, un oeil humain reste nécessaire pour ne pas passer à côté

1. Cross-site Scripting : Faille de sécurité typiquement présente sur les applications web, elle permet à un attaquant d'injecter du code du côté du client dans des pages web visibles par d'autre personne.
2. Rought Auditing Tool for Security

de problèmes flagrants.

— **Fuzzing** : Dans le cas où l'application est dites en "boite noire" (pas d'accès au code directement), on utilise une analyse de code qui vise à analyser le comportement d'une application en fonction des données, plus ou moins aléatoires, que l'on injecte en entrée.

Nous avons donc recensé un large choix d'outils pour réaliser à bien un audit de configuration, donc certain spécialement centré sur l'humain puisqu'il reste la partie la plus incertaine du système de sécurité.

CHAPITRE 5

Pentest

Cette partie se verra être plus détaillé techniquement, étant l'activité sur laquelle l'auteur s'est concentré sur le stage. Elle utilisera des données anonymisées dont l'auteur du rapport à participé à l'élaboration. Il sera fait ici une explication des outils et méthodes utilisées pour expliquer le test d'intrusion, ou pentest.

Comme nous l'avons vu précédemment, les tests d'intrusion sont une pratique courante des audits techniques. 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. Leur différenciation se situe dans les informations dont on dispose au départ du pentest.

Nous allons donc voir plus précisément les nuances entre les différents type de tests, les pratiques mais aussi les outils utilisés.

5.1 Boîte noire, dans la peau d'un pirate

Dans le contexte Boîte noir (ou Black Box), le pentester se met réellement dans la peau d'un attaquant externe et commence son test d'intrusion en ayant le moins d'information possible sur sa cible (sa cible étant alors l'entreprise ayant demandé un pentest). En effet, lorsqu'un asseyant débute son attaque, il ne dispose pas (ou rarement) de la cartographie complète du SI, de la liste des serveurs avec leurs IP, etc. Le contexte Black Box vise donc à trouver et à démontrer la présence d'un plan d'action exploitable par une personne externe permettant de prendre le contrôle du système d'information ou de mettre la main sur certaines informations.

Exemple d'un déroulement de pentest en boîte noire

Nous allons nous placer dans le contexte d'un pentest en boîte noire, afin d'expliquer de manière complète la procédure et les outils utilisés et prendre comme appuie un client type demandant cette prestation. Le client en question, l'entreprise BlackBox, a demandé comme prestation de réaliser un pentest sur vingt-quatre URL de son parc, sans donner d'informations quant aux

identifiants ou à la structure du réseau.

En commençant avec très peu d'informations, le pentester doit donc chercher depuis l'extérieur comment s'introduire dans le système cible, il adopte alors la méthodologie et le comportement qu'aurait un pirate réel. Dans cette configuration-là, le pentester va d'abord opérer ce que l'on appelle une reconnaissance de la victime via un procédé de "social engineering", afin de récupérer un maximum d'information sur la victime. Ici, internet est une source d'informations très appréciable du fait de la facilité d'accès des informations, mais il existe des logiciels spécialisés dans la récolte d'information comme l'excellent Maltego. Dans le cas de notre client, cette investigation n'était pas utile, du fait du nombre d'URL à tester et du laps de temps attribué. Nous avons donc réalisé une prestation de pentest flash, qui consistait à utiliser des outils qui opéraient des traitements automatisés sur les URL, afin de se concentrer sur une analyse plus fine, notamment sur des points qui semblaient plus sensible.

TODO : listing matériel, capture décran anonymisé

5.2 Boîte blanche, dans la peau d'un technicien

Ici, c'est exactement l'inverse. Le pentesteur travail en proche collaboration avec le DSI, le RSSI et l'équipe technique du système d'information. Le but est alors d'obtenir 100% des informations sur le système d'information et d'accompagner la DSI/RSSI dans la détection de vulnérabilité. Un des avantages du mode Boîte blanche (ou White Box) est que l'on peut alors détecter des failles de sécurité de façon plus large et que le mode Black Box n'aurait pas permis de déceler, car en se trouvant à l'intérieur du réseau à tester, le testeur aura plus de facilité à trouver ces failles car il connaît non seulement le système, mais il peut avoir accès directement aux ressources dont il a besoin. De plus, le mode White Box s'intègre plus facilement dans le cycle de vie du SI, parfois à chaque stade de son évolution.

Le testeur peut être en possession de nombreuses informations. Parmi elles, les plus courantes sont :

— Schémas d'architecture ;
— Compte utilisateur permettant de s'authentifier ;
— Code source de l'application ;

5.3 Boite grise, entre bon et mauvais hackeur

En général, lors de tests d'intrusion en mode boîte grise, le testeur dispose uniquement d'un couple identifiant - mot de passe. Ceci lui permet notamment de passer l'étape d'authentification.

L'objectif de ce type de test est d'évaluer le niveau de sécurité vis-à-vis d'un "utilisateur normal".

CHAPITRE 6

Limitation - lien avec le juridique

TRANSITION Parmi les référentiels souvent utilisés pour l'audit de sécurité, on retrouve la norme ISO 27 000 / ISO 27 001, le référentiel général de sécurité de l'ANSSI, le référentiel COBIT et dans d'autres contextes, les normes de type SOX, PCI-DSS, etc.

Certification à revoir

Différent outils à disposition (scanneur, automatisation de rapport, travail à la mano)

CHAPITRE 7

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 8

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 9

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] Statistique sur les infractions. `http://www.cert.org/stats/`, 2003.

[2] Impact des trois virus les plus virulents. `http://www.newsfactor.com/perl/story/16407.html`, 2012.

[3] Découverte de faille majeurs. `http://www.cert.org`, 2014.

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

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

Index