REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA
FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

DEPARTEMENT D'INFORMATIQUE

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique

Filière : Informatique

Spécialité : Technologie de l'Information et de Communication

Par: DAHIA Youcef

SUJET

Sécurisation des applications web

Soutenu publiquement le : / /2016 devant le jury composé de :

.....	Université de M'sila	Président
Mr. BENAZI Makhlouf	Université de M'sila	Rapporteur
.....	Université de M'sila	Examinateur
.....	Université de M'sila	Examinateur

Promotion : 2015 /2016

Table des matières

Introduction générale

L'émergence du web et la dynamique que connaît l'industrie informatique ont impacté notre vie, et nous ont rendu dépendant l'utilisation de ces technologies pour effectuer toute sorte de transaction.

A présent tout peut se faire en ligne : achat électronique, réseaux sociaux, transaction bancaire... etc.

Cette évolution constante et révolutionnaire de l'utilisation des nouvelles technologies de l'information et de la communication a affecté tous les domaines, et a résulté des menaces pouvant nuire à la vie privé et aux données personnelles ainsi qu'aux données confidentielles des personnes ou entreprises.

Pour ces raisons, l'aspect sécurité a été mis en avant. Il représente à présent un actif crucial pour l'entreprise, qui doit assurer un cadre sécurisé aussi bien pour elle que pour ses utilisateurs.

Les experts de la sécurité informatique affirment que le risque zéro ne peut être atteint, Néanmoins les bonnes pratiques sont de vigueur, et peuvent le réduire considérablement.

Le contexte hostile du monde de l'internet, l'apparition constante des menaces, ainsi que la complexité des applications web qui va de pair avec l'émergence des nouvelles technologies, nous mettons face à des problématiques récurrentes qui sont:

Comment sécuriser une application web?
Comment maintenir la sécurité d'une application web?
Quelles sont les démarches à entreprendre pour la sécurisation d'une application web?

C'est dans ce contexte que s'inscrit ce travail dont l'objectif est double. Premièrement d'effectuer une étude approfondie sur la sécurité informatique en général et la sécurité sur la toile en particulier ainsi que les menaces auxquelles les entreprises doivent faire face.

Deuxièmement, il s'agit de mettre en pratique les connaissances acquises, afin de sécuriser l'application web, ce besoin fera l'objet de notre mémoire.

A cet effet, nous allons aborder dans cette étude l'aspect sécurité des applications web et les bonnes pratiques à prendre en considération dans une architecture sécurisée et à haute disponibilité.

Dans la partie pratique nous allons définir une architecture type en se basant sur les bonnes pratiques de la sécurisation des applications web et mettre en place les outils indispensables qui feront l'objet d'une barrière frontale afin d'assurer la sécurité à quatre niveaux:

- La limitation des accès à travers la mise en place et la configuration d'un pare feu Open source Endian firewall.
- La sécurisation de l'accès au site web à travers l'implémentation et la configuration d'un proxy reverse Open source SQUID.
- Le contrôle des paquets entrants et sortants à travers une solution de détection d'intrusion Open source Snort.

Notre mémoire est organisé comme suit:

Le chapitre 1 propose une étude sur les fondements de la sécurité informatique dans sa globalité et les outils de sécurité les plus répondus et leurs fonctionnements.

Le chapitre 2 nous présentons un aperçu sur le mécanisme et les concepts de base des applications web, nous exposons brièvement les vulnérabilités et menaces les plus répondues, et nous abordons les bonnes pratiques à prendre en considération pour la sécurisation des applications web.

Le chapitre 3 présente l'analyse conceptuelle dans laquelle nous exposons une étude de l'existant et les objectifs estompés, et nous utilisons une annotation pour la modélisation de l'architecture que nous allons implémenter et enfin nous énumérons les outils choisis tout en argumentant notre choix.

Le Chapitre 4 est un aperçu de toutes les étapes effectuées dans l'implémentation de l'architecture et la mise en production des outils sur les quels notre choix a porté.

Conclusion générale

L'étude menée tout au long de notre mémoire avait pour objectif de répondre aux problématiques suivantes:

Comment sécuriser une application web?

Comment maintenir la sécurité d'une application web?

Quelles sont les démarches à entreprendre pour la sécurisation d'une application web?

Pour apporter les éléments de réponse nécessaires à ces problématiques, nous avons décortiqué l'aspect de la sécurité informatique dans sa globalité et la sécurité des application web en particulier en prenant en compte l'évolution permanente des technologies de l'information qui va de pair avec la multiplication des menaces auxquelles nous devons faire face.

L'étude théorique a été suivie par une analyse conceptuelle qui nous a permis d'identifier les besoins et de modéliser l'architecture projetée.

Compte tenu de l'importance de l'aspect sécuritaire des applications web, nous avons utilisé les outils fondamentaux de sécurité et appliqué les bonnes pratiques dans une architecture proposée.

Les principales contributions se résument comme suit:

- L'application du processus de sécurité des système informatique en se basant sur le modèle PDCA afin de faire ressortir les étapes à suivre;
- Concevoir une architecture sécurisée qui concorde avec précision avec le niveau de sécurité attendu;
- Concocter les outils adéquats et fiables et les utiliser et configurer comme étant une barrière de sécurité frontale;
- Mettre en relief l'aspect prévention à travers la mise en œuvre des outils nécessaires à la prévention d'intrusion;

Toutefois, nous pouvons envisager différentes perspectives afin de maintenir le niveau de sécurité, à titre d'exemple nous citons:

- Mise en place d'outil pour tester la vulnérabilité du site web.
- La mise en place d'un tunnel VPN.

Pour finir, nous devons signaler que notre mémoire, comme tout travail de recherche, n'est pas libre de quelques lacunes et limites. Celles-ci sont principalement dues aux raisons suivantes:

- Courte durée.

- Ressources matérielles et logicielles limitées pour l'implémentation de l'environnement de test;

Bibliographie et webographie

[1] et [2] Professeur REMAEKERS Jean. «Cours de sécurité informatique» .Université de Namur. Belgique.2012.

[3] Site officiel du moteur de recherche Wikipedia.« Organisation Internationale de Normalisation ».http://fr.wikipedia.org/wiki/Organisation_internationale_de_normalisation.

[4] Site officiel de l'Organisation Internationale de Normalisation. http://www.iso.org

[5] Site du dictionnaire informatique. http://dictionnaire.phpmyvisites.net

[6] par Alban Jacquemin et Adrien Mercier . Les firewalls[pdf].

[7] Robert S. Mueller, RSA Cyber Security Conférence (1/03/2012) : http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmartingterrorists-hackers-and-spies

[8] Site official du Web Application Security Consortium WASC. http://www.webappsec.org/

[9] WASC. «Web Application Security Consortium: Threat Classification».http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

[10] Site officiel du OWASP , Top 10 List : https://www.owasp.org/index.php/Top_10_2013-Top_10

[11] Site officiel du moteur de Recherche Wikipedia. «Défense en profondeur ». https://fr.wikipedia.org/wiki/D%C3%A9fense_en_profondeur .

[12] Forum des développeurs et IT pro. « UML2 - de l'apprentissage à la pratique »http://laurent-aubibert.developpez.com/Cours-UML/

[13] Site officiel d'Endian Firewall http://www.endian.com

[14] Guide de configuration Netfilter-iptables REFERENCE: OPPIDA/DOC/2009/AUA/534/1.4.

[15] Site officiel de SourceFire. « SNORT » http://www.sourcefire.com/fr/technologies-open-source

[16] Site officiel du blog informatique et des nouvelles technologies EASEOhttp://blog.easeo.fr/aides-howto/00site-internet/reverse-proxy-httphttps-avec-squid-3-sous-debian

ملخص :

إن عدد الهجمات ضد الشركات تنمو بشكل متزايد، مما يسبب خسائر كبيرة، وبالتالي فإن الحاجة لأمن المعلومات للشركات يصبح ذات أهمية بالغة .

لقد طورت عدة سياسات وأدوات لتزويد آليات الدفاع الفعال من بينها جدار الحماية، نظام كشف/منع التسلل، الوسيط، الهدف منها هو تحديد وتبادل كل ما يمر عبر الشبكة من الداخل والخارج والسماح بالمرور للمخولين فقط .

في مشروعنا هذا قمنا باقتراح مخطط حماية بسيط وفعال والذي يتكون من ثلاث وحدات: جدار الحماية، نظام كشف/منع التسلل، الوسيط ، هاته الوحدات تعمل معا لضمان السياسة الأمنية .

الكلمات المفتاحية : جدار الحماية ، تصفية ، تطبيق الويب ، السياسة الأمنية .

Abstract:

The number of attacks against companies are growing which can cause significant losses, thus the need of IT security becomes so important.

Several policies and tools have been developed to provide effective defense mechanisms which include firewalls, Intrusion détection/prévention system (IDS/IPS), reverse proxy, their goal is to filter all traffic exchanged with the outside network and allow only authorized traffic.

In our project we proposed a simple and effective architecture for securing web applications which consists of three modules : Endian Firewall, IDS /IPS, reverse proxy. Those modules work together to ensure our security policy.

Key-Words: Firewall, filter, web application, security policy.

Résume :

Le nombre d'attaques contre les entreprises ne cessent d'augmenter ce qui peut entrainer des pertes conséquentes, ainsi, le besoin des entreprises en sécurité informatique devient de plus en plus important.

Plusieurs politiques et des outils ont été développés pour fournir des mécanismes de défense efficaces parmi lesquels on trouve les pare-feux, Système de détection/prévention d'intrusion (IDS/IPS), reverse proxy, leur but étant de filtrer tout le trafic échangé avec le réseau extérieur et de ne laisser passer que le trafic autorisé.

Dans notre projet on a proposé une architecture simple et efficace pour la sécurisation des applications web qui se compose de trois modules : Endian Firewall, IDS /IPS, reverse proxy, ses ensemble outils peut assurer la politique de sécurité.

Mots clés : Pare feu, filtrer, application web, politique de sécurité.