الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

RAPPORT DU PROJET DE FIN D'ÉTUDES

Pour l'obtention du diplôme de

Poste Graduation Spécialisée en Sécurité Informatique

Sécurisation d'un réseau informatique d'une entreprise

Réalisé par :

KRABA ABDERRAOUF

BELHACINI CHAWKI

Devant le Jury :

Président :

M. AMRANE Abdassalam

Examinateurs :

M. DJEDJIG NABIL

M. KHEMISSA HAMZA

L'Encadreur

Mr AMIRA Abdelouhab

Co-encadreur

Mr MEKANNE Salem

Promotion : 2017 /2018

ملخص

الأمن المعلوماتي هو قضية رئيسية في التقنيات الرقمية الحديثة. مع تطور الإنترنت وفكرة مشاركة المعلومات بشكل عام، أصبحت الاحتياجات الأمنية ذات أهمية متزايدة.

ينطوي تطوير تطبيقات الإنترنت، مثل التجارة الإلكترونية أو التطبيقات الطبية أو مؤتمرات الفيديو، على احتياجات جديدة مثل تحديد الجهات المتواصلة وسلامة الرسائل المتبادلة بينها وسرية معاملاتها وتوثيقها، سواء كانت بيانات طبية أو ضريبية أو مصرفية، فإن الحاجة إلى الأمان ضرورية من أجل جعل النظام أكثر مصداقية مع احترام كل من احتياجات المستخدمين والتطبيقات. ومع ذلك، فإن هذا الأمن له ثمن: وهو إقامة الثقة بين الأطراف المتصلة حيث تنشأ الثقة بين المستخدمين عبر تأمين المعاملات، باستخدام التشفير والتوقيع الإلكتروني والشهادات الالكترونية على سبيل المثال.

نحاول خلال العمل المقدم في هذه الأطروحة اقتراح دليل لأمان شبكة الكمبيوتر الخاصة بشركة ما، مع التطرق إلى جميع الجوانب المختلفة للأمن المعلوماتي من أجل تقديم بنية شبكة مؤمنة

Abstract

Security is a major issue of modern digital technologies. With the development of the Internet and the notion of sharing in general, security needs are becoming increasingly important.

The development of Internet applications such as e-commerce, medical applications or videoconferencing, involves new needs such as the identification of communicating entities, the integrity of the messages exchanged, the confidentiality of the transaction, the authentication of entities, the anonymity of the owner of the certificate, the authorization of the rights, the power of attorney, etc.

Whether it is medical, tax or banking data, the need for security is essential in order to make the system more credible while respecting both the needs of users and applications. This security nevertheless has a price : that of establishing trust between communication partners. The trust of the users goes through the securing of the transactions, by using for example the encryption, the electronic signature and the certificates.

The work presented in this thesis, consists in the proposal of a guide of security of the computer network of a company, it touches all the different aspects of the security in order to offer a secure network architecture

Résumé

La sécurité est un enjeu majeur des technologies numériques modernes. Avec le développement de l'Internet et de la notion du partage en général, les besoins en sécurité sont de plus en plus importants.

Le développement d'applications Internet telles que le commerce électronique, les applications médicales ou la vidéoconférence, implique de nouveaux besoins comme, l'identification des entités communicantes, l'intégrité des messages échangés, la confidentialité de la transaction, l'authentification des entités, l'anonymat du propriétaire du certificat, l'habilitation des droits, la procuration, etc..

Qu'il s'agisse de données médicales, fiscales ou bancaires, le besoin en sécurité est essentiel afin de crédibiliser le système, tout en respectant à la fois les besoins des utilisateurs et des applications. Cette sécurité a néanmoins un prix : celui de l'établissement de la confiance entre les partenaires en communication. La confiance des utilisateurs passe par la sécurisation des transactions, en utilisant par exemple le chiffrement, la signature électronique et les certificats.

Le travail présenté dans ce mémoire, consiste en la proposition d'un guide de sécurité du réseau informatique d'une entreprise, il touche un peu partout les différents volets de la sécurité afin d'offrir un architecture réseau sécurisé.

Sommaire

REMERCIEMENTS 3

ملخص 4

ABSTRACT 5

RESUME 6

SOMMAIRE 7

LISTES DES FIGURES 11

LISTES DES TABLEAUX 12

BIBLIOGRAPHIE 13

INTRODUCTION GENERALE 14

I. CHAPITRE 1 :INTRODUCTION A LA SECURITE INFORMATIQUE. 17

A. Introduction : 18

B. Aperçu Sur La Sécurité Informatique de l'entreprise : 19

B.1. La Sécurité Réseau d'Entreprise : 19

C. Risque de la sécurité dans l'entreprise : 20

C.1. Risques Humains : 20

C.2. Risques systèmes : 21

D. Concept de base de la sécurité informatique : 22

D.1. Menaces, risques et vulnérabilités : 22

D.2. Concepts de base de la sécurité d'information 22

a. Définitions : 22

b. La tirade CIA : 24

B. Les domaines de la sécurité informatique : 26

C. Conclusion : 30

II. Chapitre 2 :Les Différents Volets De La Protection Du Réseau D'entreprise. 31

A. Introduction 32

B. Sécurité physique et environnementale : 34

a. La sécurité physique de l'environnement : 34

b. La sécurisation des zones serveurs (Salles serveurs) : 35

c. Solution contre les risques liés à la sécurité physique : 36

d. La sécurisation des équipements : 37

e. Outils/moyens de défense/protection : 38

C. Sécurité réseau : 40
C.1. Administration : 40
a. Réseau d'administration dédié (Vlan d'administration) : 40
b. Port physique dédié (port de management) : 40
c. Accès à l'administration du commutateur : 41
d. Protocole d'administration : 41
e. Limitation de l'accès à l'interface d'administration : 41
f. Gestion des comptes utilisateur : 42
g. Supervision SNMP : 42
h. Synchronisation horaire : 43
i. Journalisation 43
C.2. Contrôle d'accès : 44
a. Le contrôle d'accès local : 44
b. Le contrôle d'accès distant : 45
c. RADIUS : 45
d. TACACS+ : 45
e. Politique de sécurité des mots de passe : 45
f. Bannière de connexion : 46
C.3. VLAN : 46
a. Protocole VTP : 46
b. Configuration des VLAN : 46
c. Protocol DTP : 47
d. VLAN de quarantaine : 48
e. VLAN par défaut et VLAN natif : 48
C.4. Sécurisation des ports : 49
a. Sécurisation des ports de switch : 49
b. Mesures et outils/moyens de défense/protection : 49
C.5. Mécanismes liés à la disponibilité : 50
a. DHCP snooping et IP Source Guard: 50
b. Inspection ARP : 52
c. Spanning Tree: 52
d. Storm control : 53
C.6. Routage : 54
C.7. Firewall : 54
a. Définition et rôle : 54
b. Filtrage de paquets : 54
c. Statefull Inspection : 55
d. Pare-feu applicatif : 55
e. Next Generation Firewall (NGFW) : 55
f. Mesures et Outils/moyens de défense/protection : 56
g. Mesures et Outils/moyens de défense/protection : 56
C.8. Le système de détection d'intrusion IDS et IPS : 57
a. Les IDS : 57
b. NIDS: 57
c. HIDS : 57
d. IDS basé sur la signature : 57
e. IDS basé sur les anomalies : 57
f. IDS passif : 58
g. IDS réactif : 58
h. Mesure et Outils/moyens de défense/protection : 59
C.9. Réseaux privés virtuels (VPN) : 59
a. DMVPN :Dynamic Multipoint VPN 60
b. Les modèles de déploiement : 61
c. Les bénéfices du DMVPN 61

D. Sécurité des postes de de travail : 63
D.1. Antivirus : 63
a. Mesures et Outils/moyens de défense/protection : 64
b. Mesures organisationnelles : 64
c. Mesures techniques 65
d. Mesures et Outils/moyens de défense/protection : 66
D.2. Les correctifs – (les Patchs) : 66
a. Mesures et Outils/moyens de défense/protection : 67
D.3. Active Directory (AD) 68
D.4. Mot de passe 69
a. Vulnérabilités fréquentes : 71
b. Conseils supplémentaires : 72
c. Mesures et Outils/moyens de défense/protection : 73

E. Sécurité des serveurs (web, mail, etc.) : 73
E.1. Certification électronique : 73
a. Le certificat SSL à validation de domaine (DV) : 74
b. Le certificat SSL à validation d'organisation (OV) : 74
c. Le certificat SSL à validation étendue (EV) : 74
d. Mesures et Outils/moyens de défense/protection : 75
E.2. Sauvegarde des données : 76
a. Périphériques de sauvegarde 76
b. Types de sauvegardes basées sur l'emplacement : 77
c. Recommandation : 77
L'objectif principal est d'être en veille, car dans tous les cas de sinistre, il réplique et sauvegarde les données. 78
E.3. Virtualisation : 78
a. Principe : 78
b. Virtualisation et la sécurité : 78
E.4. La surveillance des systèmes (monitoring) : 79

F. Sécurité des applications : 80
F.1. Authentification 80
a. Authentification en utilisant quelque chose que vous connaissez : 80
b. Authentification par quelque chose que vous possédez : 80
c. Authentification par quelque chose que vous êtes : 80
d. Authentification par quelque chose que vous savez faire : 80
e. Authentification multi-facteurs : 81
F.2. Cryptage et chiffrement : 81
a. Le SSL (Secure Socket Layer) / TLS (Transport Layer Security) : 81
b. En pratique, le SSL devrait être utilisé dans les cas suivants : 82
c. Mesures et Outils/moyens de défense/protection : 82
F.3. Signatures électroniques : 83
a. Mesures et Outils/moyens de défense/protection : 83
F.4. Mise à jour des applications : 84
a. Mise à jour des logiciels : 84
b. Mise à jour des systèmes d'exploitation : 84
Outil pour le scan des vulnérabilités : 85
a. Nessus : (http://www.nessus.org.): 85

G. Conclusion : 86

III. Experementation **..... 87**

A. Introduction : 88

B. L'architecture réseau de l'entreprise cible : 88

B. Environnement matériel de travail : 89
B.1. Pc de travail : 89
B.2. Environnement logiciel de travail et outils : 89
B.3. Logiciels : 89
a. PfSense 89
B.4. Architecture : 90
a. Schémas logiques : 90
b. Schémas EVE-NG 90

C. Implémentation : 91
C.1. Sécurité Réseau: 91
a. Adressage Réseau LAN : 91
b. Réseau WAN : 92
c. Adresses Fix : 92
C.2. Application du guide : 93
a. Les VLANS : 93
b. Configuration SSH : 94
c. Configuration STP (Spanning tree) : 94
d. Sécurisation des ports de switch : 95
e. Sécurisation des serveurs DHCP : 96
f. Gestion des authentifications : 97
g. Configuration du routage : 98
h. Configuration VPN : 99
i. Administration : 100
C.3. Les Serveurs : 101

D. Conclusion : 103

E. Annexe: 104

PERSPECTIVE 106

F. 108

G. Glossaire : 109