CESi exia

ÉCOLE D'INGÉNIEURS INFORMATIQUE

Projet Vergis Corporation

Modification du réseau Vergis Corporation et renforcement de la sécurité informatique.

Chef de projet : CHIAVERINI Marie ;
Responsable : VERGIS Tomas ;
Ingénieur réseau en sécurité : MAZARD Nicolas ;
Ingénieur réseau : BLOCHET Tanguy ;

Table des matières

1 Introduction

Le PDG de Vergis Corporation, veux revoir le réseau de l'entreprise et renforcée la sécurité afin d'éviter tout vol de donnée.

Afin de répondre aux besoins, nous avons réunis une équipe de 3 personnes :

CHIAVERINI Marie : Chef de projet ;

MAZARD Nicolas : Ingénieur réseau en sécurité ;

BLOCHET Tanguy : Ingénieur réseau ;

A la fin de ce projet, tous les étages de tous les bâtiments seront équipés de matériel informatique et l'ensemble des postes seront reliées au réseau filaire de Vergis. L'entreprise peut accéder au site avec un URL à l'intranet en étant à la salle informatique principale. Les employés peuvent également accéder à leurs mails et s'en échanger. Certains service (support / infrastructure / développement) sont autorisés à échanger sur l'ensemble du réseau de l'entreprise, les autres verront leurs accès bloqué. Et enfin, les utilisateurs du réseau peuvent utilisés Internet.

Le rapport contient 3 grandes parties distinctes, en première partie : le cahier des charge ;
En seconde partie : les aspects techniques qui nous ont permis de réaliser le cahier des charges effectué par l'équipe, puis en troisième partie nous parlerons du Wifi et enfin pour la 4ième et dernière partie, nous terminerons sur un Bilan d'équipe, un bilan individuelle de chaque membre de l'équipe et une conclusion.

Première partie

Cahier des charges

Pour répondre aux besoins de la société, nous avons établis un cahier des charges que vous pouvez retrouver ci-dessous :

— Topologie physique ;
— Table d'adressage ;
— politique de sécurité ;
— Maquette ;
— Choix matériel ;
— Devis ;
— Configuration routage ;
— Configuration serveur ;
— Configuration sécurité ;
— Dossier Wifi ;
— Scénario ;

Note : Concernant le dernier point du cahier des charges : Scénario, il s'agit des tests.

Note 1 : Les points abordés seront détaillés par la suite.

1.1 Planning prévisionnel

Vous trouverez ci-dessous le planning prévisionnel de l'équipe.

Planning prévisionnel

Pour la semaine du
01/03/2017 au 08/03/2017

Objectif	01/03/2017 Mercredi	02/03/2017 Jeudi	03/03/2017 vendredi	04/03/2017 Samedi	05/03/2017 Dimanche	06/03/2017 Lundi	07/03/2017 Mardi	08/03/2017 Mercredi
Répartition des tâches								
Topologie physique								
Table d'adressage								
Politique de sécurité								
Maquette								
Choix matériel								
Devis								
Configuration routage								
Configuration serveur								
Configuration sécurité								
Dossier wifi								
Scénario								
Préparation soutenance								
Rapport								
Soutenance								

BLOCHET Tanguy

TOUS

MAZARD Nicolas

CHIAVERINI Marie

1.2 Planning effectif

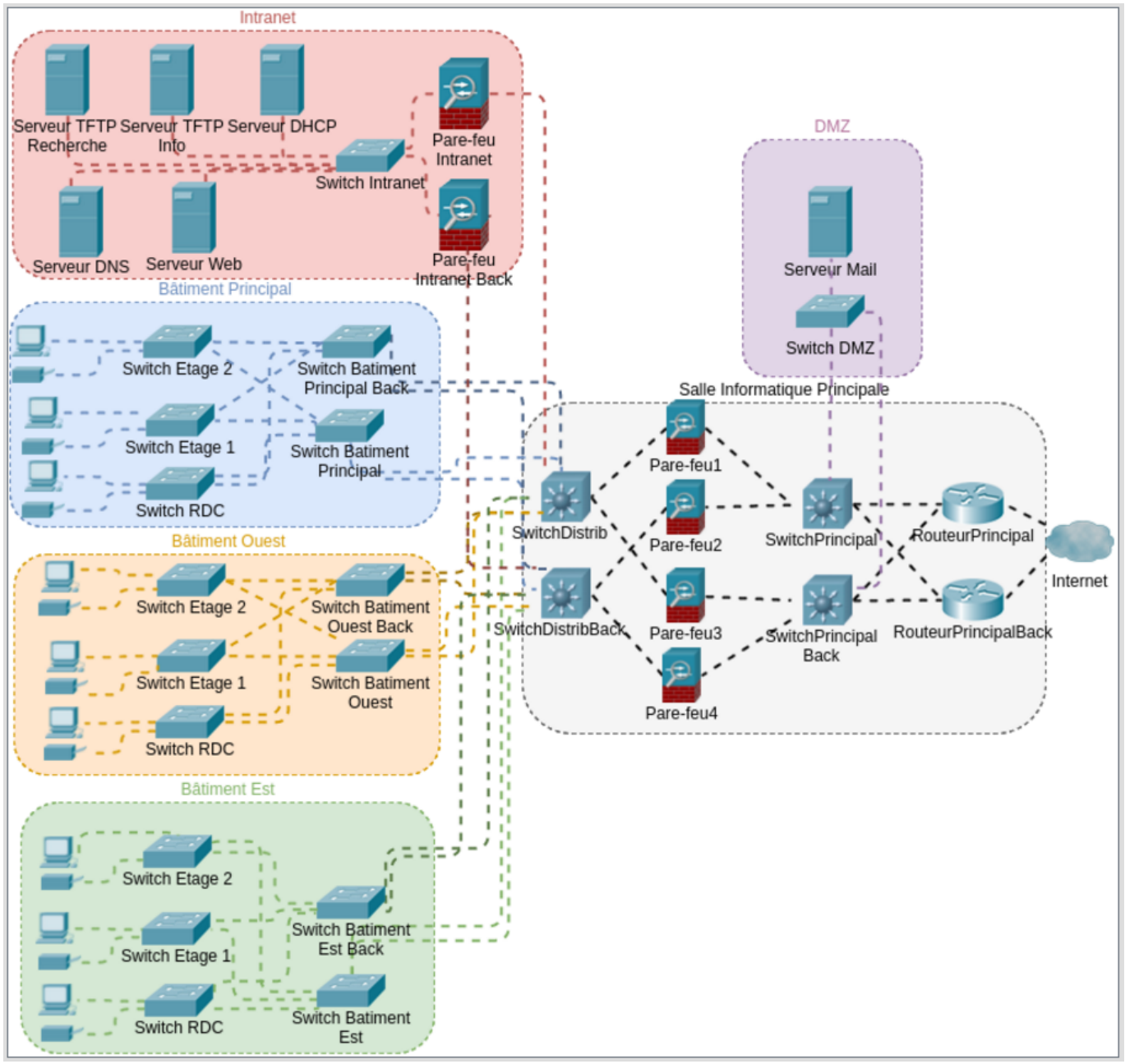
Deuxième partie

Réseau

Cette partie détaillera les aspects techniques du réseau. Il comporte l'architecture du réseau, la table d'adressage, la politique de sécurité et enfin le matériel choisi avec les devis.

2 Architecture du réseau

Le schéma présent ci-dessous représente l'architecture du réseau .



3 Table d'adressage

Le tableau d'adressage va nous permettre de segmenter et d'organiser notre réseau. De plus, il va également nous permettre de configurer nos routeurs.

4 Réseau général

Numéro	IP	Mask
11 Wifi	192.168.0.0	255.255.252.0
12 Service Rercheche et Developpement	192.168.4.0	255.255.254.0
13 Management	192.168.6.0	255.255.255.0
14 Service informatique	192.168.7.0	255.255.255.192
15 Service informatique developpement	192.168.7.0	255.255.255.224
16 Service informatique support	192.168.7.32	255.255.255.240
17 Service informatique infrastructure	192.168.7.48	255.255.255.240
18 Service direction	192.168.7.64	255.255.255.192
19 Service communication	192.168.7.128	255.255.255.224
20 Service logistique	192.168.7.160	255.255.255.224
21 Service supports clients	192.168.7.192	255.255.255.224
22 DMZ	192.168.7.224	255.255.255.224
23 Intranet	192.168.8.0	255.255.255.224
24 Service RH	192.168.8.32	255.255.255.224
25 Service comptabilité	192.168.8.64	255.255.255.224
26 Service secretariat	192.168.8.96	255.255.255.224
27 Service secretariat direction	192.168.8.128	255.255.255.224
28 Port inactif		

5 Politique de sécurité

La politique de sécurité va permettre d'identifier les risques de sécurité informatique sur le réseau.

L'objectif de cette politique de sécurité consiste à :
— sécurisé les accès aux équipements ;
— à limiter les accès des services à certain équipement ;
— et à la gestion des protocoles ;

Afin de répondre à ces objectifs, il nous faudra acquérir d'un :
— routeur ;
— switch de niveau 2 ;
— switch de niveau 3 ;
— serveur DHCP/DNS, WEB, MAIL, TFTP ;
— Pare-feu (physique et logiciel) ;

5.1 Formation

Pour renforcer la sécurité du réseau, il est important que toute personne suivent une séance de prévention sur les risques informatique. Les types de risques peuvent êtres :
— humains : clique sur des URL inconnus, téléchargement non sécurisé, laisser son ordinateur ouvert ... ;
— ingénierie social : obtenir des informations personnels ;
— l'espionnage industriel : obtenir des informations sur les activités concurrentes ;
— Cracking : détournement de mot de passe, interception d'information (mail, fichier ...) ;
— techniques : lié au matériel, l'environnement ;
— juridiques : non-respect à la signature numérique, vie privé, gestion de document ;
— Virus : ver, wabbit, cheval de troie, logiciel espion ;

L'usage des clés USB et disque amovibles sont interdits. L'utilisation du cloud est conseillé.

5.2 Les accès de chaque services

Aucune communication direct est autorisée entre les services, la communication inter-service s'effectuera par e-mail. Néanmoins, tout les services auront accès à :

— un serveur de mail ;
— internet ;
— intranet.

5.3 Le service Recherche et Développement

Le service Recherche et Développement (R&D) pourra accéder au serveur de fichier qui lui est assigné.

5.4 Le service Informatique

Concernant, le service informatique, il pourra accéder à tout les protocoles. Mais ne pourra pas inter-changer directement entre les différents service informatique (support / infrastructure / développement).

5.5 Protocole autorisé

Ici, vous trouverez une liste des protocoles autorisé sur le réseau :

— TFTP (**seulement pour le service de recherche**)
— HTTP
— HTTPS
— SSH
— POP3
— SMTP
— IMAP
— TCP
— UDP

Tout autre protocole n'étant pas sur la liste est interdit !

6 Configuration des switch de niveau 2

Tout les ports sont fermées et mis sur une VLAN avec aucune permission dessus si celui-ci n'est pas branché.

Le mode VTP est en mode client pour les switchs d'étage et en mode VTP serveur pour le switch de rez-de-chaussée.
Tout les switchs sont configurée en mode Access sauf l'interconnexion entre switchs en mode Trunk.

Aucun port est en mode automatique !

7 Configuration des routeurs

Cette partie est consacré à la configuration des routeurs.
Le nom de domaine pour chaque équipement est : vergis.local.

7.1 Mettre en place la configuration basique

Le nom du switch :

```
Router(config)#hostname RouteurPrincipal
```

Le nom de domain :

```
RouteurPrincipal(config)#ip domain-name vergis.local
```

Empécher les recherches sur le réseau

```
RouteurPrincipal(config)#ip domain-lookup
```

Le mot de passe enable :

```
RouteurPrincipal(config)#enable secret ProjetExiaSwitchPrincipal
```

Le mot de passe console :

```
RouteurPrincipal(config)#line con 0
RouteurPrincipal(config-line)#password ProjetExiaSwitchPrincipal
RouteurPrincipal(config-line)#login RouteurPrincipal(config-line)#exit
```

Le mot de passe telnet :

```
RouteurPrincipal(config)#line vty 0 15
RouteurPrincipal(config-line)#password ProjetExiaSwitchPrincipal
RouteurPrincipal(config-line)#login local
RouteurPrincipal(config-line)#transport input ssh
RouteurPrincipal(config-line)#end
```

La bannière :

```
RouteurPrincipal(config)#banner motd #Acces reserve aux personnes autorisees seulement#
```

Le serveur SSH :

```
RouteurPrincipal(config)#crypto key generate rsa
RouteurPrincipal(config)#ip ssh version 2
RouteurPrincipal(config)#ip ssh time-out 60
RouteurPrincipal(config)#ip ssh authentication-retries 3
```

Ajouter un administrateur au SSH

```
RouteurPrincipal(config)#username admin secret password
```

N'oublie pas de sauvegarder :

```
RouteurPrincipal#write
```

7.2 Configuration des sous interfaces

Avant tout manipulation, voir les numéros des VLANS.

commande :

```
RouteurPrincipal(config)#interface [range] {type numero}
RouteurPrincipal(config-if)#ip address {ip} {mask}
RouteurPrincipal(config-if)#encapsulation dot1q
RouteurPrincipal(config-if)#no shutdown
```

N'oublie pas de sauvegarder :

```
RouteurPrincipal#write
```

7.3 Configuration du HSRP

Configuration du premier routeur

```
RouteurPrincipal(config)#interface {type numero}
RouteurPrincipal(config-if)#ip address {ip} {mask}
RouteurPrincipal(config-if)#no shutdown
RouteurPrincipal(config-if)#standby 100 ip {ip}
RouteurPrincipal(config-if)#standby 100 preempt
```

Configuration du second routeur

```
RouteurPrincipalBack(config)#interface{type numero}
RouteurPrincipalBack(config-if)#ip address {ip} {mask}
RouteurPrincipalBack(config-if)#standby 100 ip {ip}
RouteurPrincipalBack(config-if)#standby 100 priority 110
RouteurPrincipalBack(config-if)#standby 100 preempt
RouteurPrincipalBack(config-if)#end
```

7.4 Sécurité dans l'ensemble des équipements

Afin de sécurisé les routeurs, chaque routeur devra afficher un mot avant toute manipulation dans la console.

7.5 Nom du routeur

Chaque routeur possèdera le nom spécifique à sa fonction. Par exemple :

— RAccess1 ;
— RAccess2 ;

7.6 Mot de passe

Le routeur possèdera un mot de passe pour les lignes virtuelles et pour le SSH. Ce mot de passe devra commencer par "ProjetExia" puis suivi du nom du routeur en minuscule.

Attention : Toute configuration modifiée devra être enregistrer dans le startup-config.

8 Configuration des switchs de niveau 3

Les switchs de niveau 3 voient quelques spécifications différents du switch de niveau 2 :

— les ports sont tous en mode trunck ;
— Il faut activer les interfaces connectés et désactiver tous les autres ;
— création des VLAN sur les switchs concernés ;
— enfin, création des liens trunks ;

9 Configuration des ACLs

Les ACL sont définies par des numéros. Le routeur applique les ACL séquentiellement.

— <1-99> IP standard access list : Filtre seulement les adresse ip source ;
— <100-199> IP extended access list : Filtre les adresses IP, protocoles et ports de source et de destination ;
— <200-299> protocole type-code access list : Filtre par protocole ;

10 Configuration des pare-feux

Mettre une notification avertissant l'utilisateur qu'il rentre dans un équipement informatique. Également, mettre en place des mots de passe afin d'assurer une sécurité.

11 Contact

Si vous rencontrez tout problèmes, ou si vous avez des questions, vous pouvez nous contacter :

— Le service informatique : support
Bâtiment principal, au Rez de chaussé.

12 Choix du matériels

Le choix du matériel s'est porté sur des éléments de la gamme Cisco pour les avantages qu'elle propose ; la fiabilité des équipements, la garantie de ces équipements, des configurations communes entre les équipements ainsi que des protocoles communs, un support client compétent, ainsi qu'une communauté active et puissante. Chaque matériel choisi ci dessous prends en compte le protocole SSH.

12.1 Switchs

12.1.1 Cisco Small Business SG250-26

FIGURE 1 – Switch Cisco Small Business SG250 à 26 ports

Ce sont les switchs de niveau 2 pour connecter les utilisateurs finaux des rez-de-chaussée des 3 bâtiments, ainsi que ceux d'entrée de bâtiment qui connectent les switchs finaux aux switchs de distribution. Ces switchs rackables de niveau 2 propose 24 ports 10/100/1000 Mbits pour un prix très abordable de 241,63€HT l'unité.

12.1.2 Cisco Small Business SF250-48

FIGURE 2 – Switch 48 ports SF250

Ce sont les switchs qui desserviront les utilisateurs finaux dans les étages supérieurs des 3 bâtiments, ils disposent de 48 ports afin de pouvoir connecter tous les utilisateurs de ces étages. Les ports Gigabits ne sont pas nécessaires sur ces switchs, un débit 100 Mégabits est largement suffisant pour les utilisateurs finaux.

12.1.3 Cisco Small Business SG500X-24

Ces switchs seront les switchs de distribution principaux et de secours en cas de panne. Ils proposent des interfaces Gigabits, qui mettent à disposition des taux de transfert adéquat pour des switchs de distribution. Ce sont des switchs de niveau 3,

FIGURE 3 – Switch

afin de décharger les routeurs qui n'auront pas à s'occupper du routage inter-VLAN entre l'intranet, la DMZ et les utilisateurs finaux.

12.2 Routeurs

12.2.1 Routeur Cisco 2901

FIGURE 4 – Router Cisco 2901 modulable

Pour le routeur il fallait un routeur disposant de port gigabits Ethernet et port RS-232. Il fallait un routeur comportant un pare-feu intégré, et qui soit puissant. Le routeur Cisco 2901 répond à tout ces critères et de plus il est modulable, il peut comporter jusqu'à 4 modules, pouvant ajouter des ports Ethernet, fibre ou série dans le cas où le réseau évoluerait.

12.2.2 2-Port Serial WAN interface Card HWIC-2T

FIGURE 5 – Module interface 2 ports série

Pour se connecter au WAN il faut disposer de ports série, ce routeur permet d'ajouter des modules tel que le HWIC-2T pour ajouter deux ports séries.

12.3 Bornes Wifi

12.3.1 Cisco Aironet 2802E-E

Ces points d'accès Wifi sont très performants, ils intègrent les vitesses du Wifi AC Wave 2 qui permet de mettre en place la technologie MU-MIMO qui permet à plusieurs utilisateurs de communiquer simultanéement avec la borne. Cette borne comporte 4

FIGURE 6 – Borne d'accès wifi Cisco Aironet 2802E-E

antennes en réception et 4 en émission, de quoi quadrupler le débit. C'est une borne dual band 2,4 Ghz et 5Ghz pour un meilleur débit un un encombrement moindre.

12.4 Pare-feu

12.4.1 Cisco ASA 5506

FIGURE 7 – Pare-feu Cisco ASA 5506

Ce pare-feu de nouvelle génération (NGFW) présentent de nombreuses fonctionnalités de protection avancées, un débit maximum de 250 Mbps et 8 ports Gigabit Ethernet.

13 Devis

Ici se trouve le devis des matériaux qu'on emploiera pour l'entreprise.

Devis

Intelligence Artificielle

Date : 3/2/2017

N° FACTURE 1

Date d'expiration : 3/8/2017

À Vergis

Vergis corporation

5 rue tauron city

Tauron City

02.78.85.12.15

Réf client 4586

Vendeur	Tâche	Méthode d'expédition	Conditions de livraison	Date de livraison	Modalités de paiement	Échéance
LDLC.PRO	Matériel informatique	Chronopost Express	Aucune	10/03/2017	Paiement à la réception	15/03/2017
Senetic.fr	Matériel informatique	UPS Express	Aucune	10/03/2017	Paiement à la réception	15/03/2017

Qté	N°article	Description	Prix unitaire HT	TVA	Total HT
11	SG250-26-K9-EU	Switch Gigabit Ethernet 26 ports Cisco Small Business SG250-26 allie idéalement de nombreuses fonctionnalités pour un réseau efficace et mieux connecté.	241,63€	20%	2 657,93€
2	CISCO2901/K9	Routeur externe, modulaire, format 1 U, ram 512 Mo, mémoire flash 256 Mo, Gigabit Ethernet, Montable sur rack.	1 047,75 €	20%	2095,50€
1	HWIC-2T=	Module carte 2ports 1RS-232.	367,51€	20%	367,51€
6	SF250-48-K9-EU	Avec les commutateurs intelligents Cisco 250, vous pouvez bénéficier de performances et d'une sécurité optimales.	274,96€	20%	1 649,76€

6	ASA5506-SEC-BUN-K9	Les pare-feu Cisco de nouvelle génération (NGFW) présentent des fonctionnalités de protection avancées contre les programmes malveillants ainsi que des IPS de nouvelle génération (NGIPS).	929,96€	20%	5 579,76€
10	AIR-AP2802E-E-K9	Borne Wifi Cisco AIRONETqui intègre les dernières vitesses de Wifi AC Wave 2 et paramètres de sécurité avancée.	591,63€	20%	5 916,30€
4	SG500X-24-K9-G5	Commutateurs administrables empilables Ethernet, qui offre toutes les capacités avancées pour assumer un réseau exigeant.	899,96€	20%	3 599,84€
				Sous-total	21 866,60€
				Taxes ventes	20%
				Total	**26 239,92€**

Devis prépaé par : BLOCHET Tanguy_____

Ceci est un devis des biens nommés, soumis aux conditions indiquées ci-dessous : Payer par la société, livraison en toute discrétion et en toute sécurité, en cas de perte de matériel, la somme doit être remboursée.)

Pour accepter ce devis, signez ici et renvoyez-le : _____

Merci de votre commande !

Vergis 5 rue tauron city Tauron City Téléphone [02.78.85.12.15] Télécopie

Troisième partie

Wifi

Voyant votre entreprise équipé de borne wifi, il est important d'être informé des problèmes de celle-ci.

14 Wi-Fi

Tout d'abord, il faut savoir que la Wi-Fi est une technologie sans fil utilisée pour se connecter à un réseau internet. L'avantage de ce type de connexion est de s'affranchir du câble qui peut s'avérer souvent problématique.

Elle utilise la norme IEEE 802.11, c'est un standard international décrivant les caractéristiques d'un réseau local sans Wi-Fi.

Néanmoins le Wi-fi possède aussi des désavantages, comme des coupures ou bien une connectivité lente. Ceci peut être du au matériel qui bloque les ondes. Il est alors conseillé d'être connecté en Ethernet afin d'obtenir une meilleure connectivité !

15 Règlementation

En souscrivant à une offre de service d'accès Internet auprès d'un FAI (Fournisseur d'Accès Internet), vous devez savoir que ce dernier enregistre tout le trafic effectué depuis votre connexion, et ce pour des raisons légales liées à la sécurité !

Attention, en cas de fraude, la responsabilité sera reporter sur le client, c'est à dire vous ! En effet, le fournisseur d'accès internet ne peut pas différencier les utilisateurs qui utilise la connexion internet.

Vous trouverez-ci dessous une liste des obligations légales liées aux opérateurs Wi-Fi :

— L'accès Internet Wi-Fi ouvert au public, vous devez être détenteur d'une licence opérateur délivrée par l'ARCEP(Autorité de Régulation des Communications et des Postes) permettant d'exploiter les fréquences Wi-Fi 2.4 Ghz.

— Vous devez mettre en place les moyens permettant d'identifier techniquement et d'authentifier tous les utilisateurs qui fréquentent et se connectent sur vos hotspots.

— Vous devez enregistrer tout le trafic effectué sur Internet par tous les utilisateurs se connectant depuis vos hotspots et conserver ces données pendant une période d'un an (nécessite le déploiement et la configuration d'un serveur de logs chez un hébergeur). Vous devez être capable de fournir ces informations sur commission rogatoire ou réquisition judiciaire.

— Vous devez déclarer le système d'authentficiation et de logs de vos hotspots à la CNIL (Commission Nationale de l'Informatique et des Libertés).

— Vous devez déployer et configurer un serveur de mail ANTISPAMS afin d'éviter les envois de SPAMS depuis vos hotspots.

— Vous devez veillez à pouvoir interdire le téléchargement illégal depuis vos hotspots.
— Vous devez vous maintenir informé et appliquer toutes nouvelles obligations légales concernant les opérateurs, dès la parution du decret d'application.

16 Risques et danger

16.1 Confidentialité

L'accès sans fil aux réseaux locaux demande l'élaboration d'une politique de sécurité dans les entreprises et chez les particuliers.

En effet, un pirate informatique peut entrer dans le réseau privé d'une entreprise afin de dérober toute information utile.
C'est pourquoi, dans le but d'améliorer la confidentialité, des méthodes sont proposés, comme le Wi-Fi Protected Access (WPA) ou plus récemment le WPA2.

Un des risques qui peut se poser pour le détenteur d'un point d'accès est sa responsabilité lorsque celui-ci est utilisé pour réaliser des des actions illégales comme le partage illégal de copies protégées par le droit d'auteur, problème qui se pose principalement lorsque le point d'accès n'est pas sécurisé.

D'autres méthodes de sécurisation existent, comme l'installation d'un serveur Radius qui est chargé de gérer les accès par nom d'utilisateur et mot de passe.

16.2 Humain

Des scientifiques ont testés les ondes Wi-Fi afin de connaitre l'impact de celle-ci sur la santé de l'homme.

Plusieurs organismes ont eu comme résultat que les effets des radio-fréquences n'ont aucun impact sur la santé si les limites des ondes est respectée ! Par ailleurs, l'organisme ajoute que pour minimiser l'exposition aux radiofréquences il suffit de les éloigner des lieux où une personne se tient pendant de longues périodes. Quelques dizaines de centimètres suffisent à diminuer nettement le niveau d'exposition, préciserais La **Fondation Santé et Radiofréquences**.

Cependant, l'organisation mondiale de la santé (OMS) a conclut en 2006 que l'exposition prolongée aux ondes du Wi-fi ne présentait aucun risque pour la santé, mais elle est depuis revenue sur cette position en ajoutant que le Wi-Fi dans la liste des éléments cancérogènes du groupe 2B (possiblement cancérigène pour l'homme) en mai 2011.

Il est recommandé de désactiver le Wi-Fi de sa box autant que possible.

17 Conclusion

Il existe encore peu de tests scientifique à ce jour montrant l'impact des ondes Wi-Fi sur la santé et sur l'environnement.
Néanmoins, tant que l'homme fait attention et modère l'usage de la Wi-Fi ou de toute autre radiofréquences, ça ne devrait pas poser de problème pour la santé. Ceci est notre opinion.

Quatrième partie

Bilan

18 Bilan d'équipe

19 Bilan individuelle

19.1 CHIAVERINI Marie

19.2 MAZARD Nicolas

19.3 BLOCHET Tanguy

20 Conclusion