Ministère des Enseignements Secondaire,
Supérieur et de la Recherche Scientifique
---------- (MESSRS) ----------

Université Polytechnique de Bobo-Dioulasso
---------- (UPB) ----------
Ecole Supérieure d'Informatique
(ESI)
http://esi.bf. refer.org
Email: esi@bf.refer. org

BURKINA FASO
Unité – Progrès - Justice

Société Nationale des Postes
------- (SONAPOST) -------
http\\www.sonapost.bf
E-mail : sonapost@sonapost.bf

PROJET DE FIN DE CYCLE

Thème :

ETUDE POUR LE RENFORCEMENT DE LA SECURITE INFORMATIQUE AU SEIN DE LA SOCIETE NATIONALE DES POSTES

Présenté et soutenu par :

M. Aziz Roger OUEDRAOGO

M. Kalifa OUEDRAOGO

Pour l'obtention du diplôme d'Ingénieur de Travaux Informatiques
(Option : Réseaux et Maintenance)

Superviseur:
M. Yassia SAVADOGO
Enseignant à l' ISGE Ouagadougou

Maître de stage :
M. Daniel W. OUEDRAOGO
Administrateur réseau SONAPOST

*Année Académique 2006-2007 ****07 Août-07 Novembre 2007*

Dédicace

Nous dédions ce présent rapport

A grand-mère Azèta OUEDRAOGO pour le courage et l'abnégation qu'elle a toujours su nous enseigné ;

Et

A nos parents respectifs qui nous ont soutenus tout au long de notre formation.

Remerciements

Ce présent document a pu voir le jour grâce à un effort remarquable de la part d'un grand nombre de personnes. Nous leur traduisons ici, nos sincères remerciements et reconnaissances. Il s'agit notamment de :

- La Sainte Trinité pour le don de la vie, de la santé et de la science ;
- M. le Directeur Général et M. le DSI de la Société Nationale des Postes pour nous avoir accueillis au sein de la société;
- L'ensemble du personnel de la Société Nationale des Postes ;
- A M. Daniel W. OUEDRAOGO notre maître de stage pour son soutien et ses conseils ;
- M. Boureima LENGANI administrateur réseau de DPNITIC/UO pour ses conseils;
- M. Ousséini OUEDRAOGO professeur de français et M. Barnabé SYAN professeur d'anglais pour leur orientation ;
- Kadiétou OUEDRAOGO, Rakiéta OUEDRAOGO et Marie OUEDRAOGO nos sœurs chéries pour les prières ;
- Kader OUEDRAOGO, Ousmane OUEDRAOGO, Seydou M. OUEDRAOGO et Roméo OUEDRAOGO nos frères pour leur soutien ;
- Adèle GOUBA, Sonia BOUDA, Maïmouna SIEDEGO, Bertille KERE, Audrey DIOMA, Fanta Camara pour leur amitié ;
- Gautier KINDO, Romuald TIGNAN, Olivier KINDO, Hamidou OUEDRAOGO, M. Nassirou YABRE, M. Mahamadi DABRE, Idrissa OUEDRAOGO pour leur soutien.
- La famille RéMi de la 5ième promotion (RéMI 3 2006-2007) pour leur combativité, leur solidarité et leur sens élevé de l'intégrité.
- Et tous ceux qui ont contribué d'une manière ou d'une autre à la réalisation de ce rapport.

Sigles

BP : Boîte Postale
CCP : Centre des Chèques Postaux
CNE : Caisse Nationale d'Épargne
CLUSIF : CLUb de la Sécurité Informatique Français
CPU: Central Process Unit
DD : Disque Dur
DNS: Domain Name Server
DoS : Denial of Service
EPIC : Établissement Public à caractère Industriel et Commercial.
FTP: File Transfert protocol
HIDS : HostBased Intrusion Detection System
LS : Liaison Spécialisée
LSI : Liaison Spécialisée Internet
LSS : Liaison Spécialisée Simple
MEHARI : MÉthode Harmonisée d'Analyse de RIsques
NIDS: Network Based Intrusion Detection System
SE : Système d'Exploitation
POE : Plan Opérationnel d'Entreprise
POS : Plans Opérationnels de Sécurité
PSI : Politique de sécurité informatique
PSS : Plan Stratégique de Sécurité
PSSI : Politique de Sécurité du Système d'Information
RAM: Random Access Memory
SI : Système d'Information
SONAPOST : La Société Nationale des Postes
UTP: Unsheild twisted pair
VPN: Virtual Private Network
WU : Western Union

INTRODUCTION GENERALE

L'Ecole Supérieure d'Informatique (ESI) est un établissement d'enseignement supérieur et de recherche de l'Université Polytechnique de Bobo-Dioulasso. L'une de ses missions principales est la formation fondamentale et/ou professionnelle dans les domaines de l'informatique.

Créée en 1991, l'ESI forme des ingénieurs de conception informatique, des ingénieurs de travaux informatiques et des étudiants de niveau DEA en informatique. Le cycle des Ingénieurs de Travaux (CITI) offre des formations en Analyse Programmation (AP) et en Réseaux et Maintenance Informatiques (RéMI). La filière RéMI où nous nous sommes inscrits est la dernière à être créée en CITI.

Dans le souci de mieux outiller ses élèves en fin de cycle, l'école les confronte aux réalités et aspects pratiques du métier d'informaticien en alliant à la formation théorique un stage pratique obligatoire de douze (12) semaines. Ce stage pratique vise à garantir une intégration rapide des futurs diplômés dans le milieu professionnel. C'est dans ce cadre que nous avons été accueillis au sein de la SONAPOST à Ouagadougou, du 07 Août au 07 novembre 2007. Le présent rapport marque la fin de notre stage pratique et doit faire l'objet d'une soutenance publique.

Nous structurons notre document en cinq parties qui sont : la présentation de notre centre d'accueil, la gestion de sécurité informatique, l'approche problématique de notre thème d'étude, l'expression des besoins de renforcement de sécurité de la SONAPOST, et enfin une proposition de solutions.

Présentation de la SONAPOST

Chapitre 1 : Présentation de la SONAPOST

La SOCIETE NATIONALE DES POSTES (SONAPOST) est un Etablissement Public à caractère Industriel et Commercial (EPIC). Il est chargé de l'exploitation du service publique des postes ainsi que de la promotion et de la mobilisation de l'épargne.

Elle est engagée dans un projet de croissance dynamique et rentable par l'élaboration d'un plan stratégique de développement. Fidèle à l'idée de progrès social qui présida sa création, la poste aujourd'hui conjugue bien croissance et performance, innovation technologique et satisfaction de la clientèle.

La SONAPOST, premier réseau de contact au Burkina Faso emploie actuellement plus de 813 personnes avec plus de 300 guichets et 77 bureaux de postes à travers le territoire national. Elle administre plus de 367.239 comptes d'épargne avec un niveau de dépôt supérieur à 38 milliards de F CFA. Concernant le segment courrier, plus de 5 millions d'objets de correspondance et 15 000 colis sont transportés par an.

I Objectifs et missions

La Société Nationale des Postes (SONAPOST) a pour objectif, pour son compte ou pour le compte de tiers, au BURKINA FASO :

- d'assurer dans les relations intérieures ou internationales le service publique du courrier dans toutes ses formes ;
- d'assurer directement ou indirectement toute autre activité liée à son objet ;
- d'assurer la mobilisation et la promotion de l'épargne, le règlement des valeurs effets et virements postaux ;

- d'offrir les prestations relatives aux moyens de paiement et de transfert de fonds aux produits de l'épargne et des chèques postaux ;

- d'assurer toute activité financière compatible avec la gestion des services financiers postaux ;

- d'appliquer la législation et la réglementation propre aux postes et les conventions, règlements et arrangements de l'union postale universelle et des unions restreintes dont le BURKINA FASO est membre ;

- de préparer et d'exécuter les plans d'équipement des postes.

II Les domaines d'activités

La SONAPOST, pour répondre à son objectif et s'inscrire dans une politique de développement économique, œuvre dans divers domaines :

II.1 Le domaine du courrier

- *Le courrier officiel* : c'est la collecte, l'acheminement et la distribution du courrier des services de l'Etat sur le territoire national et à l'étranger.
- *Le courrier d'entreprise* : il consiste en un traitement spécifique et privilégié du courrier des entreprises, des institutions et des organisations en raison de l'importance de celui-ci.

- *La boîte postale* : la boîte postale est l'adresse officielle et légale d'une personne physique ou morale et à laquelle son courrier lui est adressé.

- *Le colis postal* : le colis postal constitue le circuit d'approvisionnement, d'achat et de vente par correspondance de la poste.

- *La machine à affranchir* : la machine à affranchir est un mode d'acquittement de la taxe de port très pratique mis à la disposition des particuliers et des personnes morales ayant des quantités importantes de courriers à expédier.

- *Le Post'Eclair* : c'est un service de collecte, de traitement et de distribution rapide à délais garantis des lettres, documents, paquets, cadeaux ... à Ouagadougou et partout au Burkina.

- *Le publipostage* : il consiste à mettre en relation une entreprise et des clients au moyen de messages publicitaires sous pli ou à découvert dont la distribution se fait en boîte postale.

II.2 Le domaine des finances

- *Le mandat* : le mandat Teliman est un système de transfert électronique d'argent qui relie tous les bureaux de poste à travers tout le Burkina Faso.
- *L'épargne* : la Caisse Nationale d'Epargne (CNE) propose le compte local et l'épargne retraite poste.

- *Les chèques postaux* : service spécialisé de la poste, le Centre des Chèques Postaux, en abrégé CCP, est chargé de la gestion des comptes courants.

- *Western Union* : il est utilisé dans tous les bureaux de poste pour envoyer et recevoir de l'argent.

II.3 Le domaine des nouvelles technologies

- *Les cyberpostes* : la SONAPOST offre la connexion à Internet dans plusieurs villes du pays dans ses cybercafés dénommés Cyberpostes.

- *Le Cyberkiosque* : c'est un projet pilote, une borne d'accès à Internet haut débit par liaison satellitaire. L'équipement est composé d'un ordinateur à écran tactile, d'un clavier, d'une souris et d'une webcam incorporés. Il permet de recevoir ou d'émettre un appel audio et vidéo.

III Organisation et fonctionnement

La SONAPOST est organisée en administration centrale, directions régionales, centres spécialisés et en bureaux de poste. Son organigramme est donné en annexe1.

III.1 L'administration centrale

Elle se compose de :

- **La Direction Générale (DG)**

Le Directeur Général est chargé de la direction technique, administrative, commerciale et financière de la société. Il est nommé par décret pris en conseil des ministres sur proposition du ministre de tutelle technique (ministre des postes et télécommunications).

- **Le Secrétariat Général (SG)**

Le Secrétaire Général assiste le Directeur Général dans toutes les questions techniques et d'administration générale. Il assure l'intérim du Directeur Général.

- **Les directions et services rattachés**

Ils ont pour attributions l'organisation, l'animation du réseau de développement et de la gestion des activités et ont en charge les missions d'inspection technique et d'assistance.

- **Les directions techniques**

Elles sont les suivantes :

La Direction du Courrier (DC),
La Direction des Services Financiers (DSF),
La Direction Financière et Comptable (DFC),
La Direction des Ressources Humaines (DRH),
La Direction du Patrimoine et de la Logistique (DPL),
La Direction Commerciale et Marketing (DCM),
La Direction des Systèmes d'Information (DSI).

Nous avons effectué notre stage au sein de la Direction des Systèmes d'Information (DSI). Elle est le centre des ressources informatiques et est composée de trois (03) divisions dont les attributions sont indiquées dans le tableau suivant.

Divisions	Attributions
Division Support et Systèmes (DSS)	- Administration des systèmes informatiques (systèmes, base de données...) ; - mise en place des procédures de sécurité des données, des systèmes et des lieux ; - la mise en place d'une politique de sauvegarde des données ; - l'extension du réseau informatique ; - la formation et l'assistance des utilisateurs ; - la gestion du matériel, etc.
Division Nouvelles Technologies *(DNT)*	- Mise en place de l'infrastructure de base pour l'accès Internet ; - Mise en place de l'intranet/extranet de la société ; - Amélioration de la visibilité de la société relativement aux services offerts ; - le développement des nouveaux produits liés à l'Internet ; - l'administration du réseau.
Division Etude et Développement *(DED)*	- Le déploiement des logiciels ; - La formation des utilisateurs ; - Maintenance des applications ; - Conception et mise à jour du site web de la société.

III.2 Les directions régionales

Les directions régionales sont chargées de l'organisation, de l'animation et de la supervision des structures postales qui leur sont rattachées, ainsi que de la gestion du patrimoine de la société dans leur ressort territorial.

De façon générale, elles sont chargées de la mise en œuvre de la politique de la société définie par la direction générale. Ce sont:

- la Direction Régionale du Centre (DRC) dont le siège est à Ouagadougou ;
- la Direction Régionale de l'Ouest (DRO) qui a pour siège Bobo-Dioulasso ;
- la Direction Régionale de l'Est (DRE) dont Fada N'Gourma est le siège ;
- la Direction Régionale du Nord (DRN) qui a pour siège Ouahigouya.

III.3 Les centres spécialisés

Les centres spécialisés sont des centres dont la vocation est de traiter des opérations spécifiques de contrôle ou d'exploitation ou d'assurer une mission de formation. Ils sont rattachés à une direction technique ou à une direction régionale (mais la plupart reste rattaché à des directions régionales).

III.4 Les bureaux de poste

Les bureaux de poste ont pour vocation le traitement des opérations spécifiques d'exploitation. Ils sont au nombre de 77 avec une moyenne de 4 guichets par bureau.

Gestion de la sécurité des Systèmes Informatiques

Chapitre 2 : Gestion de la sécurité des Systèmes Informatiques

I La sécurité informatique

Aujourd'hui, le monde des affaires est en profonde mutation ; l'économie avait comme source fondamentale de production de richesses l'homme, la terre et le travail. La nouvelle économie est fondée sur l'information ; ainsi, le pouvoir est désormais détenu par celui qui possède et maîtrise l'information, faisant du même coup de celle-ci l'un des biens les plus précieux de ce troisième millénaire.

L'ordinateur avec ses prodigieuses capacités de traitement et de stockage de données constitue dès lors un moyen considérable de connaissance et de puissance. Les systèmes informatiques sont alors devenus de nos jours le cadre privilégié d'hébergement et de forte concentration de cette ressource qu'est l'information qui fait l'objet de convoitise permanente.

La SONAPOST particulièrement abrite des informations sur ses activités, ses clients, ses partenaires. En outre, la plupart des activités est informatisée. La protection de l'information est donc plus qu'une exigence. D'où la nécessité impérieuse de la préserver, de la protéger en un mot de la sécuriser.

I.1 Définition

On désigne par « sécurité », une situation ou un état tranquille qui résulte de l'absence réelle de danger d'ordre matériel ou moral.

En informatique, celle-ci pourrait se traduire comme l'état, la situation où il y a absence de dangers, de menaces ou de risques tant au niveau logiciel que matériel. Elle peut apparaître comme un processus dont le but est de réduire les risques ou la probabilité de subir des dommages.

On entend généralement par sécurité informatique l'ensemble des méthodes (préventives, dissuasives, punitives et conservatoires) utilisées pour maintenir un système informatique dans une **activité normale, durable** et **inaltérée.**

- Par **activité normale**, on signifie que le système doit répondre aux critères qui ont donné lieu à son installation. Il s'agit donc de l'ensemble des services et fonctionnalités que le système d'information est supposé fournir.

- Par **activité durable**, on entend que le système doit perpétuer son activité dans le temps, et ne pas offrir un service dont le fonctionnement est aléatoire.
- Par **activité inaltérable**, on entend que le service fourni doit toujours répondre aux mêmes critères de qualité, tant du point de vue des résultats fournis que de la confidentialité.

On peut aussi définir la sécurité informatique par ses objectifs (ses concepts).

I.2 Les concepts de la sécurité informatique

- **La confidentialité** : C'est la garantie que l'information n'est pas divulguée à des tiers non autorisés (frauduleusement ou non). C'est la possibilité d'accorder un accès sélectif aux informations. Elle doit être assurée au cours de leur collecte, de leur conservation et de leur traitement.

- **La disponibilité :** C'est la garantie de la continuité du service (facteur devenu très important avec le temps). C'est la possibilité d'utiliser les ressources d'information qui existent. Celles-ci doivent être accessibles à ceux qui en ont besoin et inaccessibles aux autres.

- **L'Intégrité** : C'est la garantie que l'information n'est pas altérée aussi bien à la source que pendant le transfert.

- **La non répudiation :** C'est la garantie qu'aucune transaction ne peut être niée.

- **L'Identification/Authentification (I & A)** : consiste à garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

I.3 Les différents types d'attaques

Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Les attaques peuvent à première vue être classées en deux (02) grandes catégories :

I.3.1 Classification des attaques suivant leur forme

I.3.1.1 les attaques passives

Elles consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible. On peut citer en exemple :

- l'écoute sur le média de transmission par branchement sur ligne ou par capture de signaux hertziens ;
- l'analyse de trafic, en vue de découvrir l'existence d'une communication entre deux sites ;
- l'utilisation de canaux cachés par usage des brèches (ports) de protocoles de protection ;
- le cheval de Troie,...

I.3.1.2 les attaques actives

Ces types d'attaques consistent à modifier des données ou des messages, à s'introduire dans des équipements réseaux ou à perturber le bon fonctionnement de ce réseau.

Exemples :

- l'interception et la modification de messages ;
- l'effacement de la donnée ou sa non disponibilité ;
- les mascarades ou déguisements (intrusion, se faire passer pour quelqu'un d'autre...) ;
- la génération ou l'absorption de trafic afin d'empêcher un service.

I.3.2 Classification des attaques suivant leurs objectifs

Pour mettre en exergue les motivations et les objectifs des différentes attaques des systèmes informatiques on peut les regrouper en quatre (4) grands groupes.

I.3.2.1 Les attaques d'accès

Ce sont des tentatives d'accès à l'information par une entité non autorisée. Ce type attaque peut survenir à l'endroit où se trouve l'information mais également pendant la transmission. Les attaques d'accès prennent différentes formes selon que l'information est stockée sur un support ou en transit sur le réseau. Elles concernent la confidentialité de l'information. L'accès peut être obtenu en volant physiquement les supports de stockage ou en interceptant l'information en transit sur le réseau.

I.3.2.2 Les attaques de modification

Elles consistent à tenter de modifier le contenu de l'information en supprimant ou en ajoutant de l'information au contenu déjà existant. Elles concernent l'intégrité des données.

I.3.2.3 Les attaques par déni de service

Ce sont des types d'attaques qui rendent impossible l'utilisation des ressources par les utilisateurs légitimes. L'objectif du DoS (Denial of Service) est de nuire. Le DoS concerne la disponibilité de l'information.

On en distingue différents types:

Le DoS aux données : le DoS aux données rend les données indisponibles en les modifiant ou en les supprimant.

Le DoS aux applications : il consiste à rendre les applications non exploitables.

Le DoS aux systèmes : il consiste à rendre le système non utilisable. Les applications et données sont immobilisées du même coup.

Le DoS aux communications : Il isole le système et le rend inaccessible.

I.3.2.4 Les attaques de répudiation

Ce sont des attaques contre la responsabilité. Elles consistent à donner de fausses informations dans le but est de nier un évènement ou une transaction et généralement en se faisant passer pour quelqu'un d'autre.

I.4 Les contre-mesures

La contre mesure est l'art de piloter les éléments du réseau ou de la machine cible, afin d'éviter à une attaque, de se propager ou de perdurer. Les contre-mesures sont fonction des types d'attaques. Le tableau ci-dessous spécifie les contre-mesures adaptées à chaque type d'attaque.

Types d'attaques	Concepts de sécurité concernés	Exemples d'attaques	Exemples de solutions
Les attaques d'accès	Confidentialité ; I&A	Spoofing, Sniffing, Spywares, Keylogger	Mots de Passe, carte à puce, authentification par empreintes digitales ou analyse rétinienne, protection des supports de stockage et des câbles réseaux.
Les attaques de modification	Confidentialité, Intégrité et I&A	Modification de salaire par un employé, solde de l'épargne,...	Mots de Passe, carte à puce, authentification par empreintes digitales ou analyse rétinienne.
Les attaques par déni de services	Confidentialité, disponibilité	Virus, vers, chevaux de Troie ; Smurf, ping de la mort ; Canular ; Coupure de câble, piquage sur media de transmission.	Antivirus ; Pare-feu matériel ou logiciel ; Anti-Spam ; Restriction logicielle ; Stratégies des droits des utilisateurs ; Audit des comptes utilisateurs ; Protection physique des medias de transmission, Chiffrement.
Les attaques de répudiation	I&A ; Non répudiation	Masquerade IP, négation d'une transaction électronique, détournement de session de chat.	Utilisation de protocoles sécurisés de transactions électroniques (SET, HTTPS), chiffrement, signatures numériques, certification.

II Notion de politique de sécurité informatique

II.1 Définition

Une politique de sécurité informatique (PSI) est l'ensemble des modèles d'organisation, des procédures et des bonnes pratiques techniques permettant

d'assurer la sécurité informatique. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité informatique.

La PSI constitue le principal document de référence en matière de sécurité informatique de l'organisme. Elle en est un élément fondateur définissant les objectifs à atteindre et les moyens accordés pour y parvenir. Elle n'est pas à confondre à la Politique de Sécurité du Système d'Information (PSSI) car il est indéniable que le système d'information ne se résume pas au système informatique.

Pour garantir la sécurité, une politique de sécurité informatique est généralement organisée autour de trois (3) axes majeurs : la sécurité physique des installations, la sécurité logique du système informatique et la sensibilisation des utilisateurs aux contraintes de sécurité.

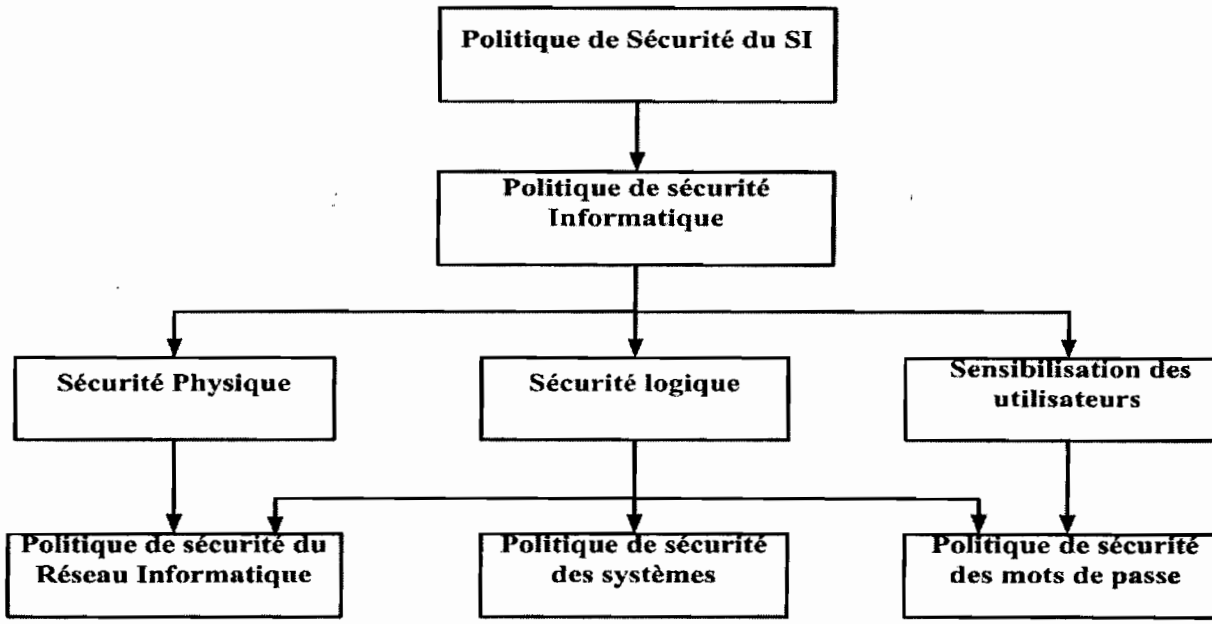


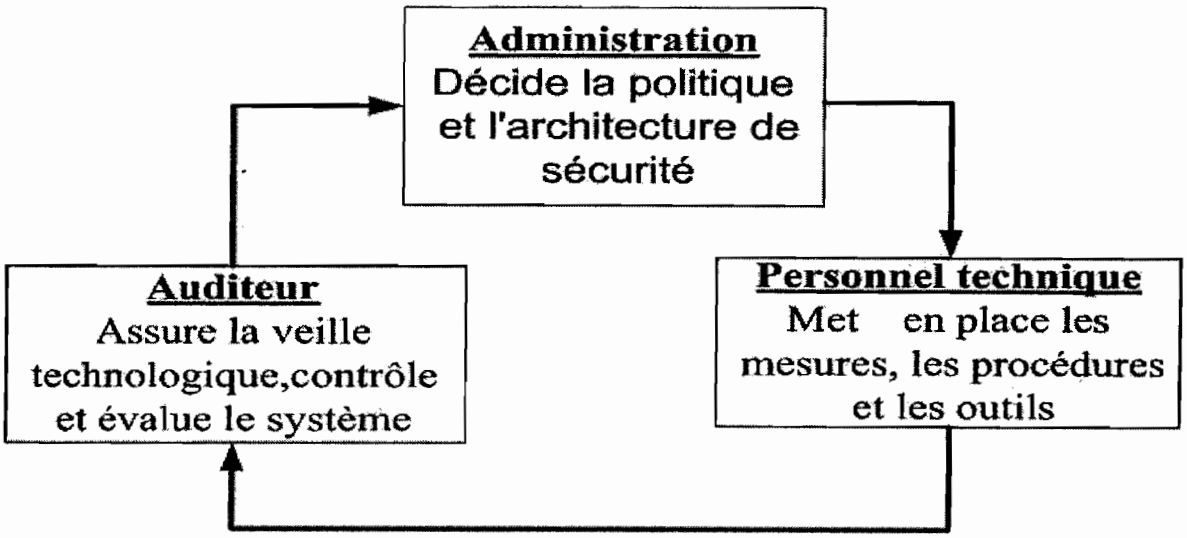
Illustration des axes majeurs de la politique de sécurité

II.2 Les acteurs dans la mise en œuvre d'une politique de sécurité

La mise en œuvre d'une politique de sécurité n'est pas une tâche qui incombe à l'administrateur seul. Elle implique les personnes suivantes :

- L'Administration : les premiers responsables, le personnel juridique ;
- Le personnel technique ;
- L'auditeur du système informatique.

Le schéma ci-après indique la responsabilité de chacun des acteurs.



Les principaux acteurs et leur rôle dans la mise en œuvre d'une politique de sécurité

II.3 Les étapes de la mise en œuvre d'une politique de sécurité

Le processus de mise en place de la sécurité dans un système informatique comprend les étapes suivantes :

II.3.1 Identification des besoins en sécurité

Cette première étape se subdivise en trois parties d'inventaire qui sont :

- **Inventaire des ressources informatiques** : il s'agit ici de faire l'inventaire des ressources informatiques matériels (appareils de traitement de données et dispositifs informatiques) et logiques (les systèmes d'exploitation, les programmes, la documentation des applications réseaux, etc.). Il prend en compte le bâtiment qui abrite le système.

- **Inventaire des dangers qui pèsent sur le système** : Cette étape consiste à identifier les différentes catégories de dangers qui menacent les ressources informatiques, à élaborer une liste des incidents qui pourraient survenir et à déterminer la fréquence de chacun de ces dangers.

- **Inventaire des vulnérabilités** : Il s'agit ici d'identifier les failles du système liées aussi bien au personnel (mots de passe faciles à déterminer ou personnel non sensibilisé) qu'aux équipements matériels et logiques (absence de pare-feux, failles d'implémentation de protocoles).

II.3.2 la rédaction des règles de sécurité à appliquer

A ce niveau, il faut faire ressortir les principes de base à respecter, définir les autorisations d'accès aux ressources, la formation et la sensibilisation du personnel de l'entreprise.

II.3.3 La Mise en œuvre des mesures de sécurité

Il s'agit ici de mettre en place une protection efficace contre les risques identifiés (sécurité du milieu, des machines, des données, du réseau, gestion de la sécurité ...) en utilisant les outils adaptés.

II.4 Les méthodes de vérification et de renforcement

II.4.1 L'Audit de sécurité

Un audit de sécurité permet de mettre en évidence les faiblesses de la mise en œuvre d'une politique de sécurité. Le problème peut venir de la politique elle-même : mal conçue ou inadaptée aux besoins de l'entreprise, ou bien d'erreurs quant à sa mise en application.

Des audits sont nécessaires suite à la mise en place initiale d'une politique de sécurité, puis régulièrement pour s'assurer que les mesures de sécurité sont mises à niveau et que les usages restent conformes aux procédures.

Les activités du réseau doivent être auditées afin que l'administrateur puisse s'assurer que les utilisateurs possèdent uniquement les droits qui leur ont été octroyés. Aussi les audits permettront de vérifier si le système n'a pas été attaqué ou si une attaque a réussi ou pas. Il est donc nécessaire d'auditer tous les évènements survenus sur le système.

II.4.2 Tests d'intrusion

Ils consistent à éprouver les moyens de protection du système d'information en essayant de s'introduire dans le système en situation réelle. On distingue généralement deux méthodes :

La méthode de la boite noire : elle consiste à essayer d'infiltrer le réseau sans aucune connaissance du système.

La méthode de la boite blanche : elle consiste à tenter de s'introduire dans le réseau en ayant une connaissance du système.

II.4.3 Les systèmes de détection d'intrusions

Il existe des systèmes de détection d'intrusions appelés IDS (Intrusion Detection System) chargés de surveiller le réseau et de déclencher une alerte lorsqu'une requête est suspecte ou non conforme à la politique de sécurité.

Il existe trois grandes familles distinctes d'IDS :

- Les NIDS (*Network Based Intrusion Detection System*), qui surveillent l'état de la sécurité au niveau du réseau.
- Les HIDS (*HostBased Intrusion Detection System*), qui surveillent l'état de la sécurité au niveau des hôtes.
- Les IDS hybrides, qui utilisent les NIDS et HIDS pour avoir des alertes plus pertinentes.

Exemples d'IDS: Snort, DarkSpy, FCheck, Bro, Osiris, Prelude...

II.5 Les outils d'analyse de risques

II.5.1 Introduction

La sécurité du système d'information d'une entreprise est un requis important pour la poursuite de ses activités. Qu'il s'agisse de la dégradation de son image de marque, du vol de ses secrets de fabrication ou de la perte de ses données clients, une catastrophe informatique a toujours des conséquences désastreuses.

Organiser cette sécurité n'est pas chose facile. C'est pourquoi il existe des méthodes reconnues pour aider les responsables informatiques à mettre en place une bonne politique de sécurité et à procéder à des audits permettant d'en vérifier l'efficacité.

II.5.2 Exemples d'outils d'analyse de risque

II.5.2.1 *EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)*

Elle a été créée par la DCSSI[1] du Ministère de la Défense (France). Elle est destinée avant tout aux administrations françaises et aux entreprises. Elle permet d'identifier les risques d'un SI et de proposer une politique de sécurité adaptée aux besoins de l'entreprise ou de l'administration.

La méthode EBIOS se compose de 4 guides (*Introduction*, *Démarche*, *Techniques*, *Outillages*) et d'un logiciel permettant de simplifier l'application de la méthodologie explicitée dans ces guides. Le logiciel libre et gratuit permet de simplifier l'application de la méthode et d'automatiser la création des documents de synthèse.

Les cinq (05) étapes de la méthode EBIOS sont :

1. étude du contexte

[1] Direction Centrale de la Sécurité des Systèmes d'Information

2. expression des besoins de sécurité
3. étude des menaces
4. identification des objectifs de sécurité
5. détermination des exigences de sécurité

II.5.2.2 *Melisa (Méthode d'évaluation de la vulnérabilité résiduelle des systèmes d'information)*

Melisa fut inventée par Albert Harari au sein de la Direction Générale de l'Armement en France.

Melisa est une méthode assez lourde basée sur un thésaurus de questions. Elle a vocation à être utilisée par de grandes entreprises.

II.5.2.3 *MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux)*

Marion a été développée par le CLUSIF dans les années 1980. C'est une méthode d'audit de la sécurité d'une entreprise, elle ne permet pas de mettre en œuvre une politique de sécurité en tant que telle. A base d'un questionnaire, elle donne une évaluation chiffrée du risque informatique.

Elle utilise vingt sept (27) indicateurs classés en six (06) thématiques. Chaque indicateur se voit attribuer une note entre 0 (insécurité) et 4 (excellent), la valeur 3 indiquant une sécurité correcte.

Thématiques des indicateurs de la méthode Marion :

- sécurité organisationnelle
- sécurité physique
- continuité
- organisation informatique
- sécurité logique et exploitation
- sécurité des applications

La méthode se déroule en 4 phases :

La phase de **préparation** permet de définir les objectifs de sécurité à atteindre ainsi que le champ d'action de l'audit et le découpage fonctionnel du système informatique à adopter pour simplifier la réalisation de l'étude.

L'**audit des vulnérabilités** consiste à répondre aux questionnaires. Ces réponses données vont permettre de recenser les risques du système informatique et les contraintes de l'entreprise. A l'issue de cet audit, sont construits une *rosace* et un diagramme différentiel représentant respectivement la note attribuée à chacun des indicateurs et les facteurs de risques particulièrement importants.

L'**analyse des risques** permet de classer les risques selon leur criticité (en classes : Risques Majeurs et Risques Simples). Elle procède au découpage fonctionnel du SI pour une analyse détaillée des menaces, de leurs impacts respectifs et de leur probabilité.

Le **plan d'action** propose les solutions à mettre en œuvre pour élever la valeur des indicateurs à la valeur 3 (niveau de sécurité satisfaisant) *de l'audit des vulnérabilités* en vue d'atteindre les objectifs fixés *en préparation*. Le coût de la mise à niveau est évalué et les tâches à réaliser pour y parvenir sont ordonnancées.

MARION a été abandonnée en 1998 au profit de la méthode Méhari. Cette dernière va plus loin en proposant la création complète de la politique de sécurité.

II.5.2.4 *MEHARI (MÉthode Harmonisée d'Analyse de RIsques)*

Méhari a été développée par le CLUSIF depuis 1995. Elle est dérivée des méthodes Melisa et Marion. Existant en langue française et en anglais, elle est utilisée par de nombreuses entreprises publiques ainsi que par le secteur privé.

Le logiciel RISICARE développé par la société BUC SA est un outil de gestion des risques basé sur la méthode Méhari.

La démarche générale de Méhari consiste en l'analyse des enjeux de sécurité et en la classification préalable des entités du système informatique en fonction de

trois critères de sécurité de base (confidentialité, intégrité, disponibilité). Ces enjeux expriment les dysfonctionnements ayant un impact direct sur l'activité de l'entreprise. Puis, des audits identifient les vulnérabilités du système informatique. Et enfin, l'analyse des risques proprement dite est réalisée.

Schéma général de la méthode Méhari

Méhari s'articule autour de 3 types de livrables qui sont :

- **Le Plan Stratégique de Sécurité** (PSS) fixe les objectifs de sécurité ainsi que les métriques permettant de les mesurer. C'est à ce stade que le niveau de gravité des risques encourus par l'entreprise est évalué. Il définit la politique de sécurité ainsi que la charte d'utilisation du système informatique pour ses utilisateurs.

- **Les Plans Opérationnels de Sécurité** (POS), définissent pour chaque site les mesures de sécurité qui doivent être mises en œuvre. Pour cela, ils élaborent des scénarii de compromission et auditent les services du système informatique. Sur la base de cet audit, une évaluation de chaque risque (probabilité, impact) est réalisée permettant par la suite d'exprimer les besoins de sécurité, et par la même occasion les mesures de protections nécessaires. Enfin, une planification de la mise à niveau de la sécurité du système informatique est faite.

- **Le Plan Opérationnel d'Entreprise** (POE) assure le suivi de la sécurité par l'élaboration d'indicateurs sur les risques identifiés et le choix des scénarii de catastrophes contre lesquels il faut se prémunir.

Méhari apporte une démarche centrée sur les besoins de continuité d'activités de l'entreprise et fournit des livrables types aidés d'un guide de

méthodologie. Les audits qu'elle propose permettent la création de plans d'actions concrets. Cette méthode permet donc de construire une politique de sécurité destinée à pallier les vulnérabilités constatées lors des audits du *Plans Opérationnels de Sécurité* et d'atteindre le niveau de sécurité correspondant aux objectifs fixés dans le *Plan Stratégique de Sécurité*.

II.5.3 Conclusion

Il existe de nombreuses méthodes d'analyse de risques, certaines simples d'utilisation, avec parfois des outils logiciels en simplifiant l'utilisation. D'autres méthodes sont réservées à de grands comptes du fait de leur complexité et des ressources humaines impliquées. Il faut donc choisir la méthode qui s'applique le mieux à votre entreprise ou organisme publique.

Approche du thème d'étude

Chapitre 3 : Approche du thème d'étude

I Problématique

Les nouvelles technologies de l'information et de la communication (NTIC) sont désormais indissociables de la vie de nombreuses sociétés. Les enjeux qui y sont associés sont considérables, au point qu'une légère négligence peut paralyser l'ensemble des activités de l'organisation. Pour le cas de la SONAPOST qui fait l'objet de notre étude, un capital de plus 38 milliards de F CFA est à protéger et montre qu'il est nécessaire et impérieux de se prémunir d'une sécurité robuste conséquente.

C'est fort de cette idée et conscients qu'aucun système ne peut être sécurisé à 100% que nous nous sommes investis pour ce thème intitulé : **«ETUDE POUR LE RENFORCEMENT DE LA SECURITE INFORMATIQUE AU SEIN DE LA SONAPOST»**.

Nous pensons par ce thème, contribuer à la consolidation des dispositions mises en œuvre pour restreindre les menaces et les dangers pesant sur les ressources informatiques de la SONAPOST. En effet réduire les risques encourus par l'organisme ou l'entreprise du fait de son SI est le but premier recherché par la sécurité informatique qui va constituer essentiellement l'objectif de notre étude.

II Objectif de notre étude

L'étude que nous devons mener consiste à :

-Analyser le réseau de la SONAPOST afin d'identifier les faiblesses, les risques et les vulnérabilités du système,

- Proposer des pistes de solutions efficaces et adéquates afin de remédier aux problèmes éventuels identifiés,

-Evaluer les coûts de la mise en œuvre de ces solutions proposées.

A cette fin, il nous est nécessaire d'établir une démarche à suivre pour mieux explorer tous les aspects sécuritaires possibles du réseau.

III Démarche à suivre

Pour notre étude nous pouvons nous baser sur l'une ou l'autre des méthodes d'analyse de risques décrites ci-dessus. Mais signalons qu'elles sont toutes, un ensemble de documentations, de questionnaires et d'outils dont nous n'en avons pas la totale possession. Cependant nous allons nous appuyer sur les principes d'évaluation de risques de la méthode MEHARI. Ainsi nous évaluerons le niveau de sécurité de la SONAPOST dans l'esprit d'approche de cette méthode (non pas en suivant tous les axes qu'elle a définis. Ce choix s'explique surtout par ces trois principales raisons :

1. MEHARI est conçue pour permettre une approche cellulaire qui permet de s'adapter à la taille et à la complexité de l'entreprise ou organisme. Cette méthode est donc appropriée à la SONAPOST qui regroupe plusieurs services d'activités plus ou moins semblables et dont le réseau informatique est de type MAN (Metropolitan Area Network).

2. Le choix des mesures de sécurité est directement corrélé aux faiblesses de sécurité de l'entreprise grâce à une analyse du niveau de vulnérabilité.

3. De plus MEHARI est aujourd'hui l'une des méthodes les plus efficaces et la plus utilisée dans l'analyse de risques informatiques.

Expression des besoins de renforcement de la sécurité informatique

Chapitre 4 : Expression des besoins de renforcement de la sécurité Informatique

I Etude de l'existant

Introduction

L'étude de l'existant est une partie essentielle de notre travail. En effet nos analyses, remarques et éventuelles suggestions de renforcement ne peuvent qu'être basées sur cette partie « existant ». Il nous faut donc connaître parfaitement le réseau car le niveau de sécurité d'un système se réduit au niveau de sécurité de son maillon le plus faible.

I.1 Présentation de l'existant

I.1.1 *Présentation géographique du réseau*

Le réseau informatique de la SONAPOST est reparti à travers le territoire national. Il est composé de plusieurs réseaux Ethernet. Il compte précisément vingt (20) sites dont neuf (9) à Ouagadougou et onze (11) en provinces.

I.1.2 *Les différents sites du réseau*

Nous pouvons classer les sites en deux groupes : Les sites de Ouagadougou (composés du siège et de 8 sites voisins de la même ville) et les sites distants (regroupant l'ensemble des sites situés dans les autres provinces).

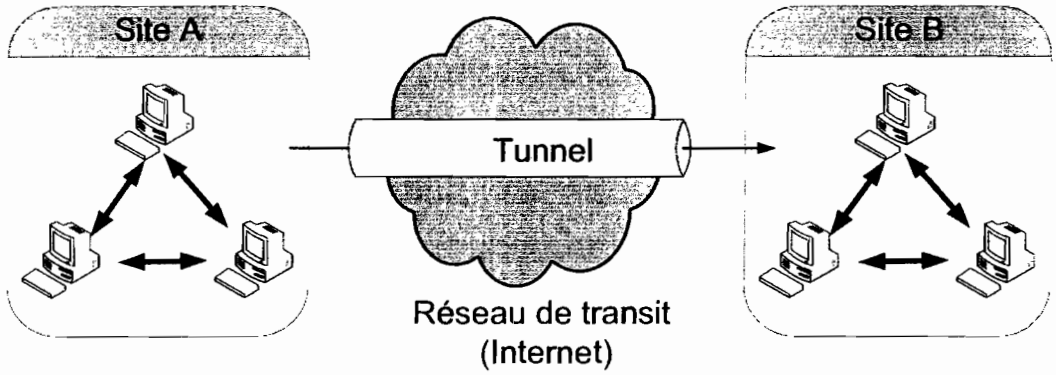
Sites voisins du siège (8)	Sites Distants (11)
Ouaga-Aéroport, Ouaga-Zogona Ouaga-Building-Lamizana, Ouaga-Dassasgho, Ouaga-Nimnin, Ouaga-Goughin, Ouaga-Patte-d'oie, Ouaga -1200 logements.	Bobo-RS, Bobo-Hamdalaye, Bobo -Nieneta Banfora, Fada-N'gourma, Garango, Koudougou, Koupela, Ouahigouya Tenkodogo, Yako.

I.1.3 *Interconnexion des différents sites*

La SONAPOST utilise des Liaisons Spécialisées (avec ou sans connexion Internet) pour interconnecter l'ensemble de ses sites au siège. Au total nous avons vingt et une (22) Liaisons Spécialisées (LS) dont douze (15) avec connexion à Internet (LSI) et neuf (7) sans connexion encore appelées Liaisons Spécialisées simples (LSS).

Un réseau VPN (Virtual Private Network) est implémenté pour permettre aux sites utilisant des LSI de se connecter au site siège. Pour cela un serveur VPN est installé au siège. Le VPN est utilisé pour relier au moins deux sites entre eux. Il est donc particulièrement utile pour la SONAPOST qui est une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Dans le cas de la SONAPOST des données très sensibles sont amenées à transiter sur le VPN (base de données clients, informations financières de Western Union ou de la CNE...). Des techniques de cryptographie avec des algorithmes, sont mises en œuvre pour vérifier que les données n'ont pas été altérées et sont restées confidentielles. Ils assurent une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. Ainsi les utilisateurs des sites utilisant les LSI accèdent aux ressources du réseau interne de façon sécurisée. Le serveur VPN est implémenté sous IPcop.

Voici une illustration schématique d'un VPN.



Dans le tableau suivant nous résumons, en fonction du type de connexion l'ensemble des sites et les débits correspondants.

LSI			LSS	
Sites		**Débit (Kbits/s)**	**Sites**	**Débit (Kbits/s)**
Siège	Internet	512	Ouaga-Patte-d'oie	128
	Cyber	256		
	Colis Postaux	64	Ouaga-1200 Lgts	64
Ouahigouya		256		
Banfora		128	Ouaga-Aéroport	128
Fada-N'gourma		128		
Tenkodogo		128	Koudougou	64
Koupela		128		
Garango		64	Ouaga-Building Lamizana	128
Bobo-RS		256		
Bobo Hamdalaye		128	Ouaga-Goughin	64
Bobo Nieneta		128		
Dassasgho		128	Ouaga-Zogona	128
Nemnin		256		
Yako		128		

❖ Schéma récapitulatif du réseau de la SONAPOST

Des descriptions précédentes, nous pouvons à présent, faire une synthèse schématique du réseau de la SONAPOST réparti dans près d'une dizaine de provinces.

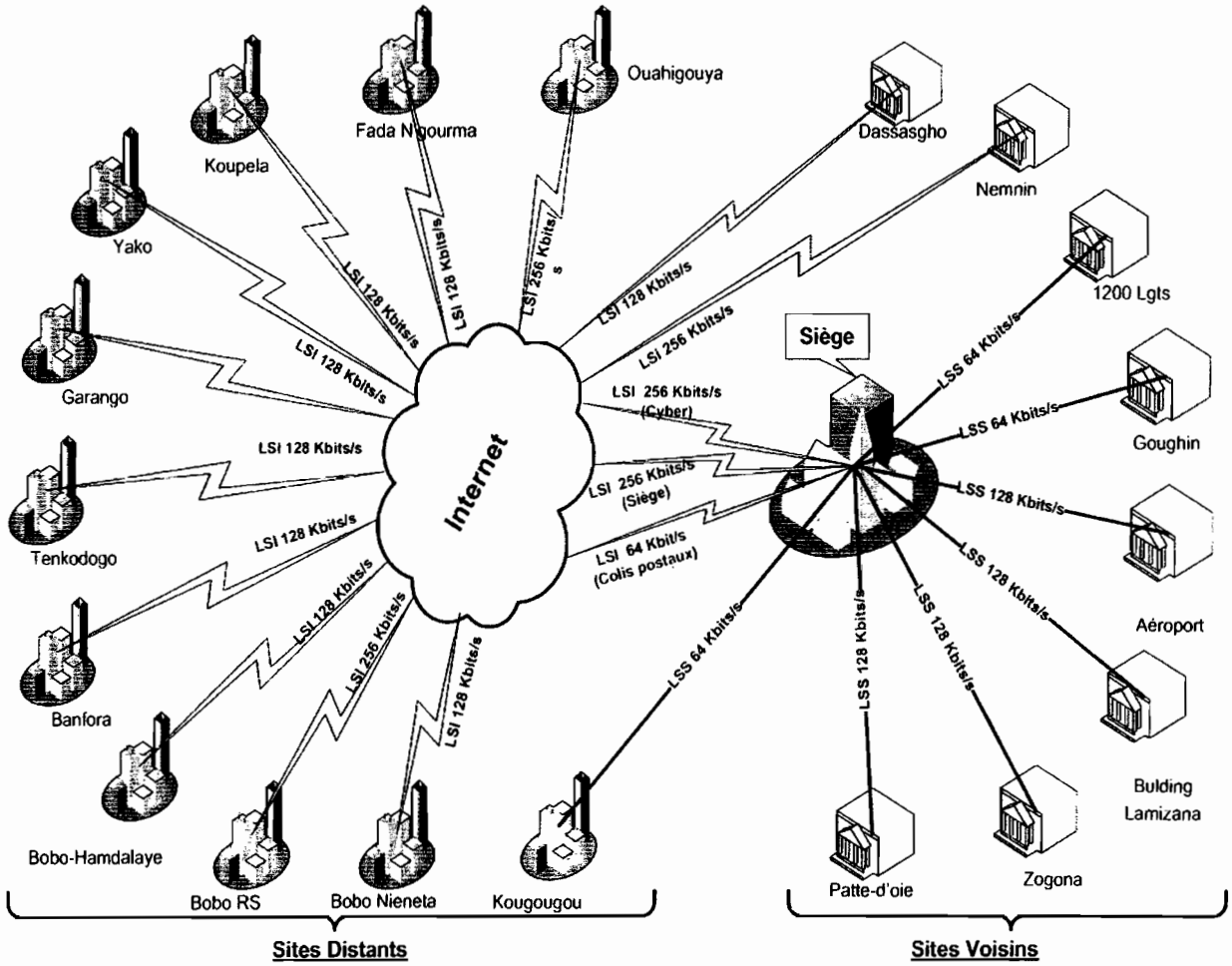


Schéma récapitulatif du réseau de la SONAPOST

I.2 Inventaire matériel et logiciel du réseau

Nous avons pu effectuer l'inventaire des équipements et logiciels utilisés au siège en approchant les différents administrateurs (réseau et système). Pour les sites voisins et distants, la récolte des informations sur l'existant s'est faite par

appels téléphoniques aux différents administrateurs réseaux avec l'aide de l'administrateur général au siège.

I.2.1 Les différents OS et logiciels utilisés

Les différents systèmes d'exploitation et logiciels utilisés sont :

Système d'Exploitation	Logiciels
Windows 98 SE, Windows 2000, Windows 2000 et 2003 Server Standard et Entreprise, Red Hat, Sun Solaris, Unix Sco.	Office 2000 et 2003, SAGE 1000 Antivirus AVG, Client CCP, CNE, BP, etc.

I.2.2 Les équipements d'interconnexion utilisés

Dans l'ensemble, on a pour les différents sites, un routeur pour l'interconnexion au siège, des concentrateurs ou des commutateurs pour la gestion interne des ordinateurs du réseau local. Le tableau ci-dessous donne les différents types d'équipements utilisés dans le réseau de la SONAPOST.

Routeurs	Switchs
Cisco 805	D-LINK DES 3226S 10/100/1000 Base T
Cisco 1000	D-LINK DES 1024S 10/100/1000 Base Sx ;
Cisco 1005	
Cisco 1600	CISCO Catalyst 2950 10/100/1000 Base T, Sx et Fx ;
Cisco 1841	
Cisco 1720	Dell Power connect 30-48 ;
Cisco 2600	
	NWay 10/100 Base T

Pour protéger l'ouverture du réseau sur Internet, des firewalls sont mis en place. En effet pour les sites utilisant la LSI, des firewalls sont placés à l'entrée de chaque réseau local tandis que ceux utilisant la LSS passent par le firewall principal du siège.

I.2.3 *Les serveurs et leurs caractéristiques*

❖ Les serveurs d'administration du réseau

Ces serveurs dits d'administration du réseau ont pour rôle la protection globale du réseau contre les intrusions ainsi que la gestion des droits d'accès au réseau et éventuellement facilitent les tâches de gestion du réseau. Ils assurent également l'établissement de la connexion virtuelle et la sauvegarde des données. Ils sont au nombre de six (06). Le détail de chacun d'eux est donné dans le tableau suivant.

Serveurs	Marque	Caractérist. matérielles	OS
Firewall + VPN	Compaq EVO	RAM : 160 MO DD : 80 GO CPU : 3 GHZ	IPCOP
Internet (Web, DNS, messagerie)	Compact ML 350	RAM : 1Go DD : 3x18Go CPU: 3.2Ghz	Red Hat 8.0
Contrôleur principal de domaine et serveur	HP Proliant ML 370	RAM : 1Go	2003 Serveur Entreprise
Contrôleur secondaire de domaine	HP Proliant ML 370	RAM : 1Go DD : 4 x 72Go	Windows 2003 Serveur standard
antivirus AVG	-	-	-
Sauvegarde	HP Proliant ML 370	-	-

❖ Les serveurs applicatifs

Nous appelons serveurs applicatifs ceux qui sont directement liés à la gestion automatisée des activités de la SONAPOST. Ce sont :

International Financial System (IFS): Héberge l'application IFS utilisée dans les transactions électroniques.

CCP (Centre de Chèques Postaux): Héberge l'application de comptabilité CCP.

BP (Boite Postale) : Gère les payements et les résiliations des clients de Boîte Postale ;

BD Orale : Hébergement de la base de données du service Boîte Postale

RAS WU : Gère les transferts Western Union ;

Développement Oracle (Serveur test) : Permet d'interpréter des scripts et de les traduire en requêtes SQL afin d'interroger le serveur de base de données Oracle.

CNE (Centre Nationale d'Epargne) : Gère les comptes CNE.

Le tableau ci-après donne l'ensemble des caractéristiques de ces serveurs.

Serveurs	Marque	Caractéristiques matérielles	OS
IFS	HP Proliant ML 370	RAM: 1Go DD: 2 x 36Go CPU: 3Ghz	Windows 2000 Serveur
CCP	Compact Proliant 5500	-	Unix SCO Open Serveur 5
BP	Dell power Edge 1600SC	-	Red Hat 8.0
BD Orale	Sun Entreprise 250	DD : 80Go	Sun Solaris
WU	Compact Deskpro ML 370 P3	RAM : 256MO DD : 10Go CPU: 730Mhz	Windows 2003 Serveur Sp1
Développement Oracle	Compact EVO 0310	RAM : 512Mo DD : 80Go CPU:1.79Ghz	Windows XP Pro SP1
CNE	HP Proliant ML 350 G2	DD : 3x18Go (RAID 5)	Unix Sco 5.0

Les serveurs de gestion des activités

I.2.4 Le réseau électrique

Au siège l'ensemble des prises pour le réseau informatique est alimenté par un courant ondulé. Cette ondulation électrique est gérée par trois onduleurs centraux dont les caractéristiques sont consignées dans le tableau suivant.

EQUIPEMENT	PUISSANCE	EMPLACEMENT
Onduleur MGE UPS System Galaxy 3000	30 KVA	Bâtiment RP/CCP (en salle serveur)
Onduleur Category 5 kystone panel chlorique Power protection synthesis twin	15 KVA	Bâtiment CMS
Onduleur UPS EAVON	15KVA	Bâtiment CNE

Des onduleurs de faibles puissances délivrent une alimentation ondulée pour quelques postes de travail du réseau qui n'ont pas de prises à courant ondulé.

En plus deux groupes électrogènes servent de relais en cas de coupure prolongée du courant.

I.2.5 Tableau récapitulatif de l'inventaire matériel de l'existant du réseau

Le tableau ci-dessous, présente le nombre total des équipements utilisés.

Equipements	Routeurs	Hub	Switchs	Serveurs	PC	Onduleurs centraux	Groupes électrogènes
Nombre	24	4	42	12	345	3	2

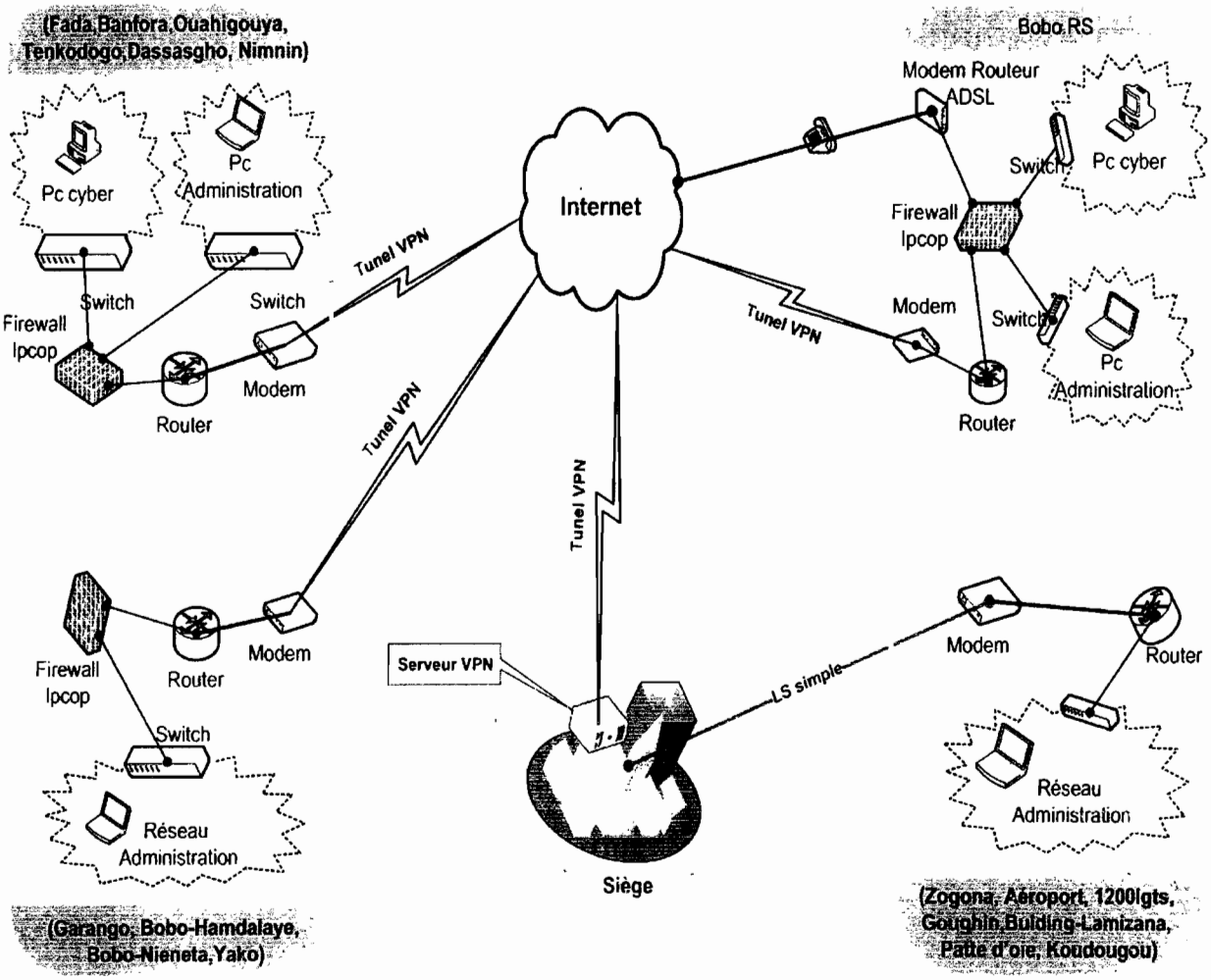
I.3 L'adressage du réseau

La répartition du réseau de la SONAPOST est d'abord faite par son agencement géographique. Une segmentation logique vient faciliter

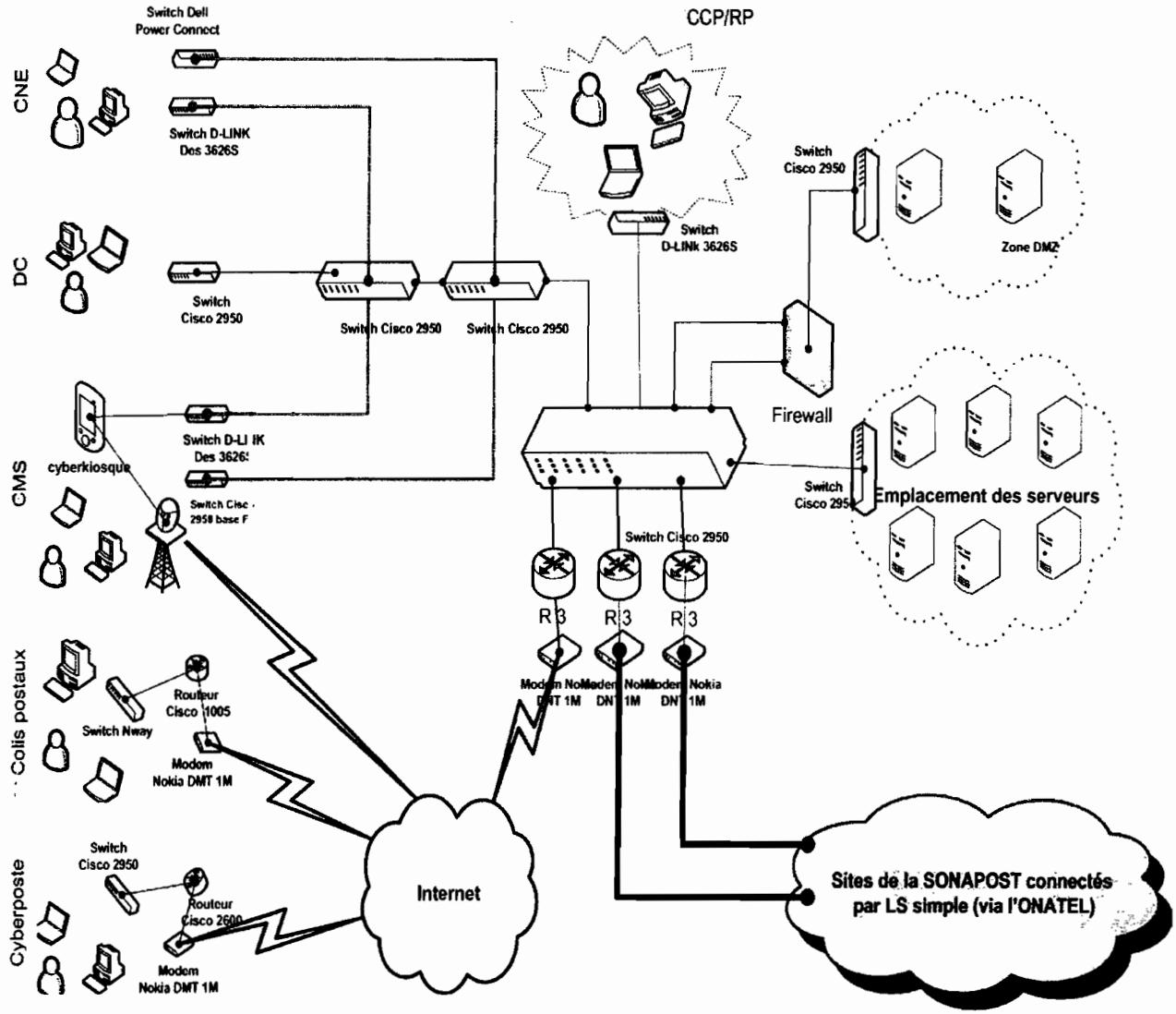
l'administration de ce vaste ensemble interconnecté. Cette division logique est aussi un plus pour la sécurité car elle permet un meilleur contrôle du trafic réseau. Chaque site géographique représente un réseau. Les classes d'adresse A, B et C sont toutes utilisées dans le réseau.

I.4 Topologie physique du réseau

La connaissance de l'existant est un requis important pour notre étude. Ainsi après avoir recensé les équipements d'interconnexion et leur emplacement nous avons élaboré les deux schémas suivants qui mettent en exergue la topologie actuelle du réseau.



Topologie physique du réseau (Sites voisins et Sites distants)



Topologie physique du réseau (Siège)

Conclusion

L'inventaire de l'existant nous a permis de concevoir la topologie du réseau. Cette illustration nous fourni une connaissance générale du réseau. Mais une analyse minutieuse suivie d'une critique rigoureuse nous donnera une meilleure perception de cet ensemble interconnecté.

II Etude critique du réseau de la SONAPOST

Introduction

Notre travail, consiste essentiellement, à évaluer le réseau informatique en vue de détecter les faiblesses d'ordre sécuritaire et proposer des voies et moyens de perfectionnement. Cette étude passe donc par une analyse minutieuse du réseau aussi bien coté physique que logiciel. Ainsi il nous faut maintenant, après avoir recensé l'existant du parc informatique de la SONAPOST, passer à une phase de critique logique et conséquente. Le réseau de la SONAPOST s'étend sur toute l'étendue du territoire national. Nous précisons donc que l'essentiel de la critique physique sera basé sur les sites de Ouagadougou principalement du siège où nous avons effectué notre stage de fin de cycle.

II.1 Quelques aspects positifs du système informatique

Avant de relever les vulnérabilités et autres faiblesses du système informatique de la SONAPOST, nous résumons dans les deux tableaux ci-dessous, quelques atouts de ce système. Ces aspects positifs nous donnent une meilleure illustration du système et nous permettront d'optimiser dans les moyens à mettre en œuvre pour son renforcement.

II.1.1 Les aspects positifs au niveau physique

Nous résumons dans ce tableau des aspects positifs sécuritaires du point de vue physique :

Aspects	Description
Système de surveillance et accès au local de la DSI	Présence de Camera à toutes les entrées ; Fermeture à clé des portes après chaque entrée et sortie;
Délocalisation du serveur CNE	Le serveur CNE est détaché.
Installation électrique	Prise de terre ; Onduleurs centraux alimentant les prises informatiques ; Groupes électrogènes assurant le relais en cas de coupure d'électricité.
Topologie du réseau	Topologie étoile (Ethernet commutée). Cette centralisation facilite la tâche d'administration. Les câbles utilisés sont essentiellement la paire torsadée UTP et FTP et la fibre optique. Le piquage d'informations sur ces médias est très difficile. Les câbles sont enfermés dans des goulottes.
Equipements d'interconnexion	Les routeurs Cisco 2600 et les switchs Cisco Catalyst 2950 configurables sont de bonne performance.
Liaison d'interconnexion des sites	Les sites directement reliés au siège par la LS simple ont une connexion permanente et disposent une large bande passante.

II.1.2 Les aspects positifs au niveau logique

Nous résumons dans ce tableau des aspects positifs sécuritaires du point de vue logique :

Aspect	Description
Poste de travail administratif	Identification par nom d'utilisateur et authentification par mot de passe.
Serveur de Sauvegarde	Un serveur assure la sauvegarde des données.
Sécurité réseau	❖ Des Firewalls protègent le réseau contre les éventuelles intrusions venant de l'extérieur (Internet). ❖ Un réseau VPN est implémenté pour permettre un partage sécurisé des ressources. ❖ Chaque site constitue un réseau. Ceci renforce la sécurité par la limitation et le contrôle des accès hôtes. ❖ Serveur DNS permet la résolution des noms dans le réseau.
Les contrôleurs de domaine (principal et secondaire)	Ils permettent une gestion centralisée et facile des comptes et des utilisateurs. Le contrôleur secondaire est un miroir du premier dont l'objectif est d'assurer le relais en cas de panne ou de dysfonctionnement sur le contrôleur principal. Il est implémenté au sein de la SONAPOST avec 2003 Serveur.
Plate-forme	Le système d'exploitation Windows XP est utilisé dans la majorité des cas. Ce système même s'il est vulnérable reste toujours fiable et facile à utiliser.
Serveur Antivirus AVG	Un Serveur d'antivirus permet la mise à jour antivirus des postes du réseau.

II.2 Recherche et analyse des dysfonctionnements

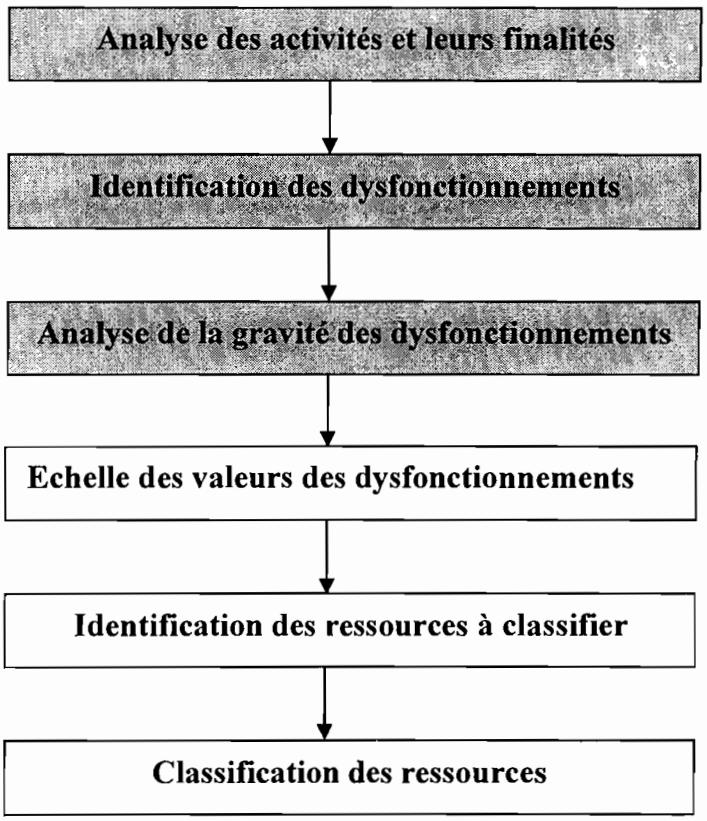
II.2.1 Démarche à suivre

Il y a un consensus assez général pour dire que l'objectif de la sécurité est de minimiser les risques encourus par l'entreprise ou l'organisme du fait de son système d'information. En d'autres termes la sécurité doit permettre de rendre le

risque acceptable. Un risque inacceptable c'est «la conjonction de vulnérabilité fortes et d'enjeux critiques. »

(Enjeux critiques + vulnérabilités fortes = Risques inacceptables.)

Pour l'identification des vulnérabilités et menaces pesant sur le système informatique de la SONAPOST, nous allons suivre le principe de base de la démarche Méhari dans le processus de l'analyse des enjeux. Cette démarche consiste à procéder à une analyse des activités, d'en déduire les dysfonctionnements puis les évaluer pour enfin effectuer une classification des ressources du système selon le schéma ci-dessous :



Principe de la démarche Méhari

NB : Les trois dernières étapes (**Echelle des valeurs des dysfonctionnements, Identification des ressources à classifier, Classification des ressources**) sont des documents de référence d'aide à la décision pour les responsables des systèmes informatiques. Elles interviennent surtout lors de la rédaction du document final de la politique de sécurité qui n'est pas exactement l'objet de notre étude. Par conséquent nous n'aborderons pas ces axes dans ce présent rapport.

II.2.2 Analyse des activités et de leurs finalités

La connaissance des activités menées par l'entreprise donne une idée générale qui, circonscrite, nous permet de référencer les ressources à protéger et d'identifier dans le cas de la sécurité, les intérêts qui pourraient motiver d'éventuels attaquants. Elle permet également d'identifier les habitudes et les comportements du personnel de l'entreprise.

Elle se dégage surtout lors de la collecte d'informations sur les domaines d'activité de l'entreprise et par observation des situations de travail. C'est une des bases de la critique.

Il convient de signaler que cet axe a déjà été développé dans la première partie « **Présentation de la SONAPOST** » de notre rapport et ressortira inévitablement au niveau de l'identification des dysfonctionnements.

II.2.3 Identification et analyse de gravité des dysfonctionnements

Il n'est pas sérieusement envisageable de s'occuper de la sécurité d'une entreprise sans se poser la question de l'état des vulnérabilités de cette entreprise devant les risques divers que sont les accidents, les erreurs humaines ou les malveillances. Les vulnérabilités d'une entreprise sont les points par lesquels elle (l'entreprise) peut être attaquée. En ce sens, analyser les dysfonctionnements revient à faire un diagnostic de l'état de la sécurité.

Dans MEHARI, quatre (4) niveaux de gravité ou de criticité sont distingués et permettent de se référer à une échelle de gravité. Ces quatre niveaux sont :

Niveau 4 (Vital) : Le dysfonctionnement redouté est extrêmement grave et met en danger l'existence même ou la survie de l'entité ou de l'une de ses activités majeures.

Niveau 3 (Très grave) : Il s'agit là des dysfonctionnements très graves au niveau de l'entité sans que son avenir soit compromis.

Niveau 2 (Important) : Il regroupe les dysfonctionnements ayant un impact notable au niveau des opérations de l'entreprise, de ses résultats ou de son image tout en restant globalement supportables.

Niveau 1 (Non significatif) : Les dommages encourus n'ont pratiquement pas d'impact sur les résultats des activités de la société ni sur son image.

Nous listons ici les vulnérabilités, les fragilités et les menaces qui pèsent sur le réseau informatique de la SONAPOST. Notre identification de ces faiblesses se fait par niveau croissant de criticité.

II.2.3.1 Niveau 1 : Dysfonctionnements non significatifs

- **Les vulnérabilités de la plate-forme Windows**

La quasi-totalité des postes tourne sur Windows (98, 2000, XP, 2000 et 2003 Serveur, etc.). Seuls quelques serveurs fonctionnent sous Unix et Linux. Windows est connu pour sa simplicité d'utilisation mais reste et demeure un système fermé et très faillible.

- **La faiblesse des performances des équipements utilisés**

Même si certains matériels informatiques sont performants, la SONAPOST abrite toujours en son sein des équipements dépassés au regard des applications utilisées. C'est le cas des hubs qui posent des problèmes de sécurité du fait qu'ils propagent les informations sur tous les ports, des machines telles que les Pentiums 1 et 2 qui sont utilisés dans le réseau. Leur remplacement permettra d'améliorer la qualité de service et les temps d'accès.

Il y a ici aussi le cas du serveur de messagerie. Il a de faibles caractéristiques et n'offre ce service de messagerie qu'aux premiers responsables de la société.

- **La mise à jour des systèmes**

Aussi bien du coté des serveurs que des postes utilisateurs, les mises à jour des systèmes ne sont pas toujours effectives. Cela rend les systèmes plus vulnérables.

➢ **Adressage du réseau**

Actuellement le réseau de la SONAPOST est adressé de façon statique. Cet adressage ne facilite pas la tâche d'administration surtout en tenant compte de l'évolutivité du réseau.

➢ **Manque d'agents de surveillance**

Bien qu'il y ait un système de vidéo surveillance, il est déplorable de constater qu'il n'existe pas d'agents chargés de sa gestion. Ce service reste disponible et donc sous exploité.

II.2.3.2 Niveau 2 : Dysfonctionnements très graves

➢ **Manque de serveurs de relais**

De nombreux serveurs participent à la gestion des activités de la SONAPOST. Toutefois il n'existe aucune image de ces serveurs, dont certains sont capitaux (Serveur VPN, CNE, CCP, BP, WU,...) pour continuer le service en cas de panne physique de serveur.

➢ **La topologie du réseau : les liaisons d'interconnexion**

Le réseau de la SONAPOST dépend totalement de l'ONATEL SA fournisseur d'accès national. En plus le débit qu'offre une connexion par VPN n'est pas contrôlable du fait qu'il s'adosse sur l'Internet (Le LAN s'adosse sur le WAN pour donner du VPN). De même les LS utilisées ne sont pas à l'abri des pirates qui peuvent se glisser sur les lignes de communication afin d'intercepter des données.

Il est temps que la SONAPOST dispose d'un réseau autonome sécurisé (interconnexion des différents sites par VSAT, BLR, WIMMAX,...) qui lui permettra d'être plus concurrente.

- **Absence de Système de détection d'intrusions et de système d'alertes**

Aucun système de détection ni de surveillance réseau n'est mis en place pour permettre aux administrateurs d'être avertis en cas de problème dans le réseau. Ces systèmes doivent être prévus dans la politique de sécurité pour faciliter la tâche des administrateurs.

- **Manque d'anti-Spywares**

Il n'y a pas de serveur anti-Spywares dans le réseau. Cette lacune ne permet pas de contrer l'action des logiciels espions.

- **Absence d'antivirus et d'anti-Spam sur le serveur de messagerie**

Le service de messagerie est implémenté sous Red Hat 8.0. Mais il n'y a aucun antivirus ni d'anti-Spam installé sur ce serveur. Certes les virus n'auront généralement pas d'actions sous Linux mais un logiciel de contrôle viral est nécessaire pour protéger les clients accédant à ce serveur et qui tournent sous Windows. De même un anti-Spam limiterait l'action du courrier intempestif.

- **Faiblesses liées à l'antivirus AVG**

AVG est l'antivirus utilisé à la SONAPOST. Cependant cet antivirus est connu pour les faiblesses suivantes :

- Incapacité à détruire quelques Trojans;
- Analyse plus longue (3 ou 4heures pour tout le disque) ;
- Ralentissement du système.
- Certains tests sur les navigateurs ne sont pas faits en temps réel

Il serait donc préférable de changer d'antivirus.

- **Gestion des utilisateurs**

Installation des logiciels par des utilisateurs

Aucune politique de sécurité n'est mise en place pour empêcher les utilisateurs d'installer des programmes douteux de leur propre initiative. Ceci est

une négligence grave du fait qu'un système est plus faillible de l'intérieur. Cette inattention peut être la porte d'entrée de nombreux logiciels espions et autres virus.

Utilisation des périphériques d'entrée

Les utilisateurs peuvent infecter leur poste et au delà tout le réseau par l'utilisation des médias amovibles, des CD, des DVD et autres supports de stockage.

Politique de mot de passe

Il n'y a pas une politique clairement définie pour les mots de passe (longueur, fréquence de changement,...). En effet le mot de passe de l'administrateur comme celui des utilisateurs doit être de qualité.

- **Absence d'une charte d'utilisation du matériel informatique**

La charte permet de responsabiliser davantage l'ensemble du personnel de l'entreprise et en particulier les utilisateurs du réseau et de l'outil informatique en général. Il est donc fondamental de former le personnel dans ce sens afin qu'il puisse garder en bon état le patrimoine informatique de l'entreprise. La SONAPOST manque de ce document qui est un maillon important.

- **Absence d'une politique de sécurité informatique**

Certes, des mesures de sécurité sont mises en place mais il n'existe pas de document décrivant clairement et de façon concise les stratégies et les plans de sécurité adoptés par la SONAPOST. Une politique de sécurité permettra de garantir la disponibilité, l'intégrité et la confidentialité des données, des applications et du système informatique en général. Ce document devrait présenter les risques et les solutions à apporter dans certains cas d'attaques du système informatique. Il facilite l'administration et la restauration du système informatique en cas de problème.

- **Maintenance du parc informatique**

La maintenance préventive des ordinateurs et autres périphériques n'est pas clairement définie. Elle est effectuée généralement de façon curative.

De plus la localisation de la salle de maintenance (au deuxième niveau du bâtiment RP/CCP) n'est pas assurant pour un bon transport du matériel défectueux à maintenir.

II.2.3.3 Niveau 3 : Dysfonctionnements à conséquences dramatiques

- **Emplacement du serveur de sauvegarde**

Le serveur de sauvegarde se trouve dans la même salle que les autres serveurs. Un incendie dans cette salle par exemple ne l'épargnerait pas. Il est donc indispensable de le délocaliser.

- **Accès et gestion de la salle serveur**

Accès physique : La salle serveur est située dans le bâtiment CCP/RP. Elle dispose de deux portes dont l'une s'ouvre sur une allée pour passagers et se fermant à clé simple tandis que l'autre se trouve à l'intérieur du secrétariat et dispose en plus de la clé, d'un code d'identification. Mais cette dernière porte est en panne et reste ouverte pendant les heures de travail. Ce fait constitue un danger pour les serveurs même si la porte du secrétariat se ferme.

Gestion : La salle est fréquentée par de nombreuses personnes. Outre les administrateurs des serveurs, le personnel de la DSI (Personnel de maintenance, secrétaires, agent de liaison) y accède car un téléphone mis à leur disposition s'y trouve. Seuls les administrateurs doivent être autorisés à accéder à cette salle.

De plus, plusieurs administrateurs au total six (06) sont chargés de gérer différents serveurs qui se trouvent être tous dans la même petite salle. Une relation de confiance existe certes, mais des chantages, des attaques internes et des malveillances peuvent survenir surtout que certains boîtiers des serveurs ne sont pas verrouillés. Même une simple inadvertance pourrait provoquer un accident car la salle est contiguë et accessible à des personnes non autorisées.

II.2.3.4 Niveau 4 : Dysfonctionnements fatals

➢ **Le regroupement des serveurs dans une même salle**

Exceptés le serveur CNE et le serveur d'antivirus, l'ensemble des serveurs du réseau de la SONAPOST (12 au total) se retrouve dans la même ville (Ouagadougou), dans le même site (au siège), dans le même bâtiment (Bâtiment CCP/RP) et de surcroît dans la même salle (au niveau de la DSI). Il est inéluctable qu'un incendie, une catastrophe de moindre envergure (dans la salle serveur ou dans le bâtiment) paralyserait complètement tout le réseau national de la SONAPOST. Au regard des enjeux ceci est un risque inacceptable que court notre chère société des postes. Il est nécessaire et impérieux qu'une solution appropriée soit vite déployée.

➢ **Absence de firewall au service des colis postaux**

Aucun firewall ne protège les ordinateurs du service colis postaux. Leur accès Internet leur permet de se connecter au serveur IPS (International Postal Système) qui se trouve en France. Ce serveur assure le suivi et la localisation des objets postés. Une intrusion sévère immobiliserait les activités de ce service. Le manque du pare-feu est une faille grave car il constitue un élément capital dans la sécurité des réseaux.

Conclusion

Le réseau de la SONAPOST regorge d'atouts majeurs. Mais force est de constater que ce vaste ensemble interconnecté (le réseau) est sous exploité. Beaucoup de faiblesses et de failles sécuritaires plus ou moins graves existent et sont à résoudre pour une mise en valeur optimale du réseau informatique.

Proposition de solutions

Chapitre 5 : Proposition de solutions

Introduction

Cette partie est un axe fondamental de notre étude. Elle fait une synthèse des imperfections sécuritaires et regroupe un ensemble de solutions et mesures appropriées relatif à ces insuffisances précédemment mises en exergue.

Notre analyse des dysfonctionnements nous permet de faire la synthèse suivante des problèmes rencontrés dans le réseau de SONAPOST :

- certaines des mesures de sécurité actuelles du réseau sont défaillantes,
- l'infrastructure du réseau est sous exploité,
- la sensibilisation et la responsabilisation des utilisateurs ne sont pas effectives,
- la protection du personnel et des biens n'est pas assurée,
- aucun plan d'administration du réseau n'est élaboré,
- aucun plan de continuité n'a encore été conçu,
- le personnel technique est insuffisant,
- le système de sauvegarde et de reprise après sinistre est défaillant,
- le matériel technique est insuffisant.

Nos solutions de renforcement de la sécurité informatique au sein de la SONAPOST se résument essentiellement en trois points où les problèmes cités trouveront leurs solutions :

1. **Politique de sécurité**
2. **Projet de charte d'utilisation**
3. **Mesures d'accompagnement**

I Politique de sécurité

Nous proposons ici les grandes lignes de la politique de sécurité à mettre en place. Il faut souligner que sa rédaction complète en un document final reste à élaborer. En effet, elle nécessite des rencontres avec les premiers responsables et

est faite de concert avec un juriste. Au regard de ces contraintes et du manque de certaines ressources (Documentions complètes de Méhari et temps), nous nous axons sur la partie technique du document.

I.1 Politique de sauvegarde réseau avec l'outil libre AMANDA

I.1.1 Présentation de AMANDA

AMANDA (Advanced Maryland Automated Network Disk Archiver) est un outil de sauvegarde réseau développé par l'université du Maryland. Il est basé sur une logique maître-esclave. Le maître possède le périphérique de sauvegarde et donne des ordres aux esclaves pour qu'ils sauvegardent les disques. Il récupère ces sauvegardes et il les copie sur le périphérique de sauvegarde.

Le serveur doit posséder un gros disque et un lecteur de bande ainsi qu'une bonne connectivité réseau. Le disque sert de disque tampon durant la sauvegarde et stocke également des index des différentes sauvegardes.

Les esclaves sont une variété de machines UNIX sur lesquelles on peut compiler la partie client d'AMANDA. Actuellement seules les machines UNIX sont "nativement" supportées. Des possibilités d'utiliser Samba pour sauvegarder des machines "Windowsiennes" sont possibles.

Pour chaque partition sauvegardée AMANDA offre la possibilité de générer un index des fichiers sauvegardés. Ainsi la récupération des fichiers sur les bandes en est grandement simplifiée.

On peut également installer des serveurs de bandes annexes qui seront utilisés lors de la récupération des fichiers. Ainsi on peut récupérer en parallèle des fichiers de différentes sauvegardes.

I.1.2 Les points forts d'AMANDA

L'outil libre Amanda :

- ❖ est basé sur les standards de logiciels de sauvegarde (Unix dump, restore et Gnu tar).
- ❖ sauvegarde plusieurs machines en parallèle sur un disque tampon, écrit les sauvegardes terminées une par une sur la bande aussi rapidement que l'on puisse écrire un fichier sur une bande. Par exemple, une bande DAT de 12 Go avec une vitesse d'écriture de 1Mo/s pour le lecteur sera remplie en 3 heures.
- ❖ implémente une gestion de bande simple: On ne risque pas d'effacer une mauvaise bande par erreur.
- ❖ inclue le support pour une sécurité Kerberos[2] 4 ainsi que des sauvegardes encryptées.
- ❖ indique les bandes dont on a besoin et trouve la bonne image de sauvegarde sur la bande lors de la récupération des fichiers.
- ❖ produit un rapport incluant toutes les erreurs et l'envoie aux opérateurs de la sauvegarde.
- ❖ ajuste automatiquement l'ordonnancement des sauvegardes et le niveau des sauvegardes tout en restant dans le cadre prédéfini. Il n'est plus nécessaire de jongler avec l'organisation des sauvegardes lorsque l'on rajoute de nouveaux disques.
- ❖ inclue un programme de vérification de la configuration sur le serveur ainsi que sur les clients et envoie éventuellement les résultats par courrier électronique.
- ❖ utilise la compression sur les clients ou sur le serveur.
- ❖ possède beaucoup d'autres options.

I.1.3 Définition de la politique de sauvegarde

➧ *Les données du réseau à sauvegarder*

Au regard de l'enjeu important que représentent les serveurs applicatifs (ceux qui sont directement liés à la gestion automatisée des activités) du réseau de la

[2] Système basé sur le chiffrement pour authentifier des utilisateurs et des connexions réseaux. Il utilise un système de tickets au lieu de mots de passe en texte clair.

SONAPOST, il parait nécessaire d'effectuer la sauvegarde de tous ces serveurs afin d'en assurer l'intégrité et une haute disponibilité. Rappelons que la disponibilité et l'intégrité sont des objectifs fondamentaux de la sécurité. De principe de base, un serveur doit être toujours disponible au besoin.

Les données à sauvegarder seront donc essentiellement constituées de :

- bases de données financières (IFS, CCP, CNE) et de gestion de payement et résiliation (Boite Postale) ;
- informations administratives (fichiers de comptabilité, comptes rendus, contrats, exposés et planning des services techniques, correspondances des partenaires, etc.).

Procédures de sauvegarde

Les différents types de sauvegarde qui existent sont :

Sauvegarde complète : C'est une méthode de type « annule » et « remplace ». On écrase le contenu de sauvegarde par la nouvelle information. Méthode très sûre mais longue si le volume est important.

Sauvegarde différentielle : C'est une méthode qui sauvegarde toutes les informations qui ont été modifiées depuis la dernière sauvegarde complète.

Sauvegarde incrémentale : C'est une méthode qui ne sauvegarde que les informations qui ont été modifiées depuis la dernière sauvegarde enregistrée sur le support.

Sauvegarde mixte : C'est une combinaison des trois méthodes précitées.

Pour le cas présent de la SONAPOST nous allons faire une sauvegarde mixte :

- une sauvegarde journalière incrémentale à 17h 45mn ;
- une sauvegarde complète trimestrielle ;
- à chaque mise à jour sur un poste de travail ou un serveur, une image disque du poste ou du serveur est réalisée par l'administrateur.

Cette technique de combinaison nous permettra d'économiser du temps et de l'espace.

- ***Conservation des bandes***

Mettre les bandes de sauvegarde journalière dans une armoire (à l'épreuve du feu si possible) après chaque sauvegarde et s'assurer de bien la refermer.

Il faut conserver les supports mensuels et annuels en dehors du site des serveurs, dans une localisation la plus éloignée possible de leur source, dans un coffre-fort blindé ignifugé. Le lieu de conservation doit être tenu secret et décidé avec le premier responsable du Système d'Information.

Sous aucun prétexte l'administrateur chargé des sauvegardes ne doit laisser les sauvegardes dans la salle des serveurs ou à la portée de personnes non autorisées.

Chaque bande doit être référencée (date et autres) de façon unique. On doit y retrouver nécessairement le type et la période de sauvegarde.

Des sauvegardes spécifiques peuvent être réalisées en parallèle pour d'autres données sensibles dont la sauvegarde est indispensable et jugée nécessaire par l'administrateur et conservées suivant les obligations prescrites dans la présente politique.

- ***Test et vérification des sauvegardes***

Il faut tester la bonne récupération des données afin de s'assurer du bon fonctionnement des sauvegardes.

Egalement il faut contrôler régulièrement (chaque mois) le journal des sauvegardes afin de vérifier qu'aucune anomalie n'ait perturbé le bon fonctionnement des sauvegardes (erreurs d'application, mauvais supports ou supports saturés par exemple).

L'administrateur chargé des sauvegardes a l'obligation de veiller à la mise à jour du plan des sauvegardes. Toute nouvelle donnée sensible de l'entreprise doit être sauvegardée.

- ***Restauration***

Le processus de récupération des données à partir des copies de sauvegarde permet de redémarrer une chaîne applicative après un sinistre ou tout autre événement ayant interrompu l'activité (perte de données, altération, corruption complète ou partielle de données, etc.). Plus les applications ont un caractère critique, plus la restauration doit être rapide et surtout offrir toutes les garanties de cohérence des données au regard de la logique applicative.

Avec AMANDA les bandes nécessaires à une restauration sont indiquées. L'administrateur doit veiller à connaître l'emplacement de toutes les bandes et à fournir rapidement celles demandées.

I.1.4 Installation et configuration

Voir annexe 2.

I.2 Politique de mot de passe

L'accès au compte d'un seul employé d'une entreprise peut compromettre la sécurité globale de toute l'organisation. Ainsi, toute entreprise souhaitant garantir un niveau de sécurité optimal se doit de mettre en place une réelle politique de sécurité en matière de mots de passe.

Une politique des mots de passe est une suite de règles destinées à améliorer la sécurité, en encourageant les utilisateurs à recourir à des mots de passe relativement complexes et en les utilisant correctement.

I.2.1 Création de mots de passe

Un bon mot de passe est un mot de passe fort, qui sera donc difficile à retrouver même à l'aide d'outils automatisés mais facile à retenir. Pour ce faire, il

existe des moyens mnémotechniques pour fabriquer et retenir des mots de passe forts.

I.2.1.1 *Méthode phonétique*

Cette méthode consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple la phrase « *J'ai acheté huit cd pour cent euros cet après midi* » deviendra **ght8CD%E7am**.

I.2.1.2 *Méthode des premières lettres*

Cette méthode consiste à garder les premières lettres d'une phrase (citation, paroles de chanson...) en veillant à ne pas utiliser que des minuscules. Par exemple, la citation « **un tiens vaut mieux que deux tu *l'auras*** » donnera **1tvmQ2tl'A.**

I.2.2 Caractéristiques des mots de passe

- **Longueur :** de 6 à 8 caractères minimum.
- **Les caractères employés :** L'utilisation des minuscules et des majuscules et l'insertion de chiffres et de caractères spéciaux permettent une meilleure résistance en cas de tentative d'accès avec divers mots de passe.
- **Validité** : Pour lutter contre les programmes utilisant la *force brute*[3], les mots de passes ne devraient faire partie ni d'un dictionnaire, ni de noms propres, ni de dates valides et ni de données personnelles telles qu'un numéro de compte.
- **Période de validité** : L'administrateur doit imposer le changement de mots de passe périodiquement (tous les 180 jours).

I.2.3 Les règles d'utilisation

Une politique de mots de passe doit s'accompagner de bonnes habitudes d'utilisation :

[3] Méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.

- ne jamais partager un compte utilisateur;
- ne jamais utiliser le même mot de passe pour différents accès;
- ne jamais donner son mot de passe, même aux personnes chargées de la sécurité;
- ne jamais écrire sur papier son mot de passe;
- ne jamais communiquer son mot de passe par téléphone, mail ou messagerie instantanée;
- s'assurer de la déconnexion avant de quitter un poste;
- changer le mot de passe au moindre soupçon de compromission.

I.2.4 Audit de mots de passe

Il peut représenter la première étape d'une campagne de sensibilisation. Celle-ci aura pour but de démontrer l'importance de faire preuve de rigueur. L'administrateur pourra dans le cadre de la sensibilisation, procéder à du cracking[4] de mot de passe en temps réel pour faire la démonstration de la rapidité du procédé lorsque les consignes ne sont pas appliquées.

Cet audit doit être réalisé au moins une fois l'an.

I.3 Remplacement des firewalls IPcop par des firewalls matériels Cisco PIX

I.3.1 Description de la technologie Cisco PIX

Les firewalls Cisco PIX sont des équipements spécialement conçus pour la sécurité. Ils mettent à la disposition des entreprises une large gamme de services intégrés de sécurité et de réseau, notamment :

- des services évolués de pare-feux sensibles aux applications (pare-feux applicatifs);
- l'une des meilleures sécurités VoIP (Voix sur IP) et multimédia du marché;
- une tolérance aux pannes reconnue parmi les meilleures de l'industrie,

[4] Fait de déjouer les protections mises en place dans un système.

- une connectivité VPN IPSec robuste pour les accès distants de postes nomades ou interconnexions site à site.

Grâce à de nouvelles fonctionnalités VPN des pare-feux Cisco PIX, l'entreprise peut connecter par Internet, de façon économique et en toute sécurité, ses réseaux et ses utilisateurs mobiles depuis le monde entier.

Les solutions supportées, sont des VPN de site à site utilisant les normes VPN IKE (Internet Key Exchange) et IPSec (IP Security) jusqu'aux fonctionnalités innovantes d'accès à distance de Cisco. Leur fonctionnalité Easy VPN contrairement aux solutions VPN traditionnelles, permet de bâtir une architecture de VPN à accès distant dont l'évolutivité, la rentabilité et la simplicité d'utilisation éliminent les frais d'exploitation liés à la gestion des configurations des équipements distants. Cisco Easy VPN apporte d'autres services comme le contrôle de l'état de la sécurité sur les clients VPN et les mises à jour logicielles automatiques des clients VPN Cisco, afin de fournir un accès à distance sécurisé et facile à gérer vers les réseaux d'entreprise.

Les pare-feux Cisco PIX cryptent les données à l'aide des normes DES (Data Encryption Standard) 56 bits, 3DES (Triple DES) 168 bits ou AES (Advanced Encryption Standard) jusqu'à 256 bits.

Les fonctionnalités des pare-feux Cisco PIX sont très nombreuses et présentent de grands avantages pour les entreprises.

I.3.2 Avantages dans le réseau de la SONAPOST

L'utilisation de ces pare-feux dans le réseau de la SONAPOST donnera les avantages suivants:

- ❖ Une simplicité des interconnexions des sites et également de leur gestion avec la solution VPN robuste IPSec;
- ❖ Une surveillance de l'activité de tout le réseau fiable et en temps réel: les fonctions de surveillance (notamment un tableau de bord et une visionneuse syslog en temps réel) fournissent, d'un seul coup d'œil, des informations vitales sur la santé des unités et du réseau comme sur les évènements.
- ❖ Possibilité de création, sur un même serveur dédié Cisco PIX, de multiples contextes de sécurité (pare-feux virtuels) disposant chacun de son propre

ensemble de politique de sécurité, de ses interfaces logiques et de ses domaines administratifs. Ainsi on pourra définir pour chaque site de la SONAPOST utilisant les LSS un pare-feu virtuel avec des paramètres de sécurité personnalisés et adaptés.

- Donne à l'administrateur un meilleur contrôle de l'utilisation des ressources définissant à quel moment certaines listes de contrôle (ensemble de paramètres de sécurité) sont actives, avec des intervalles de temps personnalisables en fonction des différentes listes. On pourra par exemple interdire l'accès au serveur CCP et CNE à partir d'une certaine heure de la journée.
- L'administrateur peut à distance, configurer, surveiller et dépanner ses pare-feux Cisco PIX par l'intermédiaire de l'interface de commande en ligne (CLI). L'accès sécurisé à la CLI s'effectue de plusieurs manières, notamment par le protocole SSH (Secure Shell) version 2 et Telnet sur IPSec ou par un port console.
- Création simple d'un grand nombre de VLAN (Virtual Local Area Network);
- Garantit une meilleure protection du réseau que celle actuellement réalisée avec IPcop.
- Bien d'autres avantages sécuritaires et économiques.

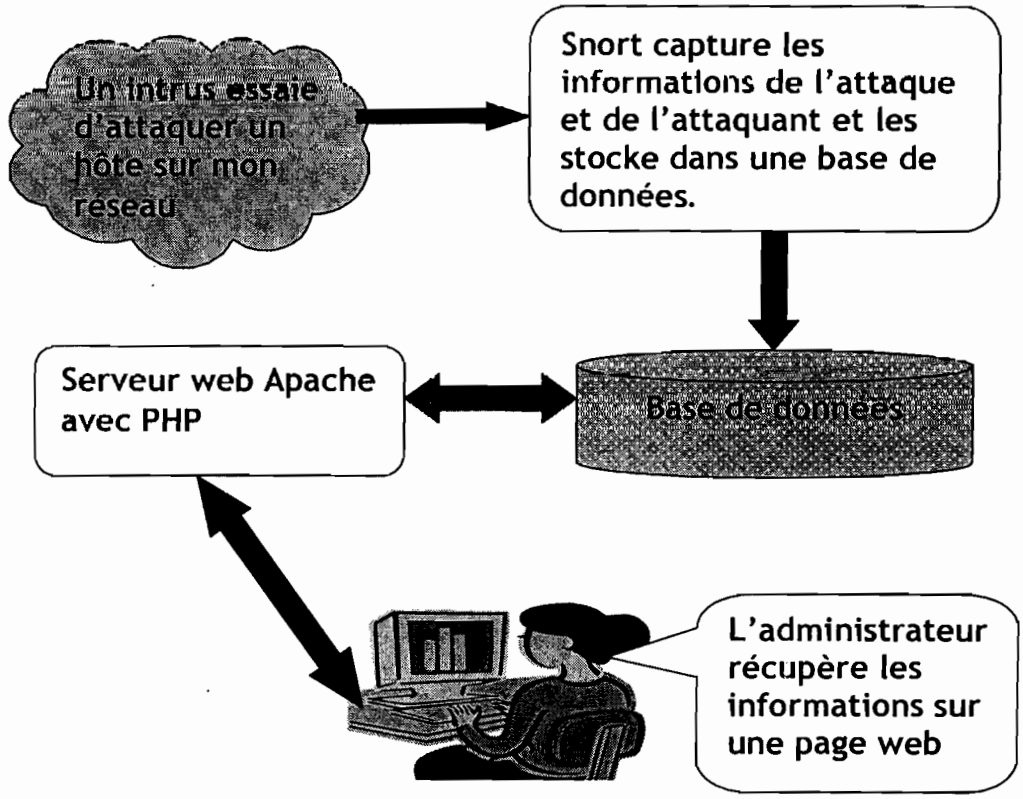
I.4 Implémentation du système de détection d'intrusion SNORT

- **Présentation de SNORT**

Snort est un système de détection d'intrusion (IDS) libre sous licence GPL. C'est un sniffer de réseau. Il est capable d'effectuer en temps réel des analyses du trafic et de logger les paquets sur un réseau IP. Il peut effectuer des analyses de protocoles, recherche/correspondance de contenus et peut être utilisé pour détecter une grande variété d'attaques et de sondes. Cependant, comme tout logiciel, Snort n'est pas infaillible et demande une mise à jour régulière. Snort peut également être utilisé avec d'autres projets open sources

tels que SnortSnarf, ACID, Sguil et BASE[5] afin de fournir une représentation visuelle des données concernant les éventuelles intrusions.

❖ **Fonctionnement de Snort**



I.5 Redondance de serveurs avec le système clustering

Le terme anglais cluster signifie littéralement "grappe". Il s'agit de regrouper des ressources informatiques par l'intermédiaire d'un réseau.

Les technologies de mise en cluster permettent à plusieurs serveurs de travailler à l'unisson et d'offrir l'apparence d'un environnement informatique unique. En effet, on fait interagir plusieurs serveurs distincts comme une seule entité, afin de cumuler leur puissance de calcul, et faire en sorte que l'indisponibilité d'un équipement n'entraîne pas l'indisponibilité de l'ensemble (l'architecture est alors dite« tolérante aux pannes »). D'un point de vue technique, chaque serveur exécute son propre système d'exploitation, mais ils

[5] *Basic Analysis and Security Engine*

opèrent ensemble comme s'ils ne formaient qu'un. Dans les clusters, un nœud désigne un serveur. Une baie (ensemble de disques partagés entre les nœuds) sert généralement à la centralisation du stockage.

Ainsi, d'un cluster minimaliste à 2 machines jusqu'à des infrastructures pouvant compter plusieurs dizaines de serveurs, on dispose d'une solution évolutive, économique, performante et sécurisée, permettant aux entreprises de se concentrer sur le développement de leur activité.

❖ **Avantage du Clustering**

Tolérance aux pannes : La tolérance des pannes signifie que, si un nœud ne fonctionne plus, un autre peut immédiatement prendre le relais en veillant à ce que les utilisateurs soient dérangés le moins possible.

Basculement : C'est le processus par lequel la charge d'un nœud est automatiquement transférée à un autre nœud.

Restauration automatique : C'est le processus par lequel la charge est retransférée au nœud défaillant une fois qu'il fonctionne de nouveau.

❖ **Organisation des clusters de serveurs**

Dans le cas de la SONAPOST, le système de clustering s'impose au regard de l'importance des applications.

Les systèmes d'exploitation des serveurs sont essentiellement Windows 2003, Linux (Debian) et Sun OS.

Pour la redondance des serveurs de la SONAPOST, nous proposons deux clusters. Un premier qui regroupera les serveurs tournant sous Windows et un second qui rassemblera ceux qui fonctionnent avec le système UNIX.

❖ **Les systèmes pour le Clustering**

Cluster Windows: Windows server data center.

Cluster UNIX: Mosix.

I.6 Autres mesures de sécurité

Les vulnérabilités de la plate-forme Windows : Pour pallier aux problèmes liés au système Windows nous optons pour un basculement progressif vers une plate-forme Linux qui bien qu'ouvert reste plus robuste que Windows et présente moins d'intérêt vis-à-vis des pirates (du moins pour l'instant). Dans ce cas il faudra faire développer les différentes applications de gestion des activités sous Linux ou utiliser des progiciels similaires libres et assurer la formation des utilisateurs. Nous proposons concrètement la version 2006 de la distribution Mandriva pour les raisons suivantes :

- interface utilisateur assez proche de Windows, simple d'utilisation,
- faible coût pour son installation car il n'y a pas d'achat de licence,
- nécessitera seulement une formation des utilisateurs du nouveau système,
- les systèmes Linux sont moins vulnérables que Windows.

Mais il est possible de garder les systèmes Microsoft et :

- payer les licences pour toutes les machines,
- effectuer régulièrement les mises à jour,
- protéger efficacement les systèmes avec des antivirus,
- acquérir légalement les logiciels.

La mise à jour des systèmes : Effectuer une mise à jour régulière des différents systèmes (serveurs et clients) afin de les maintenir dans de bonnes performances.

Le serveur de messagerie : Pour pouvoir étendre ce service nous proposons l'achat d'un disque dur de 120Go et une RAM de 256Mo. De plus nous proposons pour des raisons de sécurité le changement de son SE RedHat par Debian. En effet RedHat n'est plus à nos jours entretenue c'est-à-dire n'est plus mis à jour.

Pour la protection contre les spams et les virus nous proposons de :

Filtrer les virus avec ClamAV

Filtrer les spams avec SpamAssassin

NB : ClamAV et SpamAssassin sont des solutions libres

Adressage du réseau : Implémenter un adressage dynamique (DHCP) avec

Le regroupement des serveurs dans une même salle : Pour la délocalisation des serveurs nous proposons de mettre :

- le serveur relais VPN à Koudougou,
- le serveur de sauvegarde à Ouahigouya,
- les serveurs WU, IFS et d'administration du réseau (firewall, DNS, Messagerie, Contrôleurs de domaine, ...) au Siège,
- les serveurs de BP, de BD Oracle, de Développement Oracle et de CCP à Dassasgho ;
- Antivirus et CNE au siège (à leur endroit actuel).

Absence de firewall au service des colis postaux : La meilleure solution est d'intégrer ce réseau au principal et utiliser le firewall au siège dans l'optique d'une extension future.

Mais de façon palliative, il faut urgemment placer un firewall. Nous proposons l'utilisation de Kerio Personal Firewall v2.0 fonctionnant sous Windows.

II Projet de Charte d'utilisation

AVANT PROPOS

Ce projet de charte a été élaboré à la suite de notre étude de renforcement de la sécurité informatique au sein de la SONAPOST. Il a été motivé principalement par l'ampleur des dysfonctionnements relevés dans la partie critique de notre travail et liés à l'absence d'une charte d'utilisation et surtout par la solution sécuritaire qu'il représente dans une société.

En effet ce présent document est élaboré dans le but d'inspirer et d'aider la SONAPOST à préciser de manière contractuelle les conditions d'utilisation par le personnel des ressources informatiques et des services liés aux technologies de l'information et de la communication. Cette charte s'inscrit dans un objectif de sensibilisation et de responsabilisation. Elle vise à promouvoir des comportements de vigilance et de sécurité et à renforcer la prévention d'actes illicites en amenant les utilisateurs à constamment s'interroger sur la légitimité de leurs actes.

Son contenu doit être adapté pour une meilleure utilisation raisonnée et maîtrisée des ressources et des TIC, au fur et à mesure de l'évolution de la société, de la technologie et de ses usages, de la législation et de la jurisprudence des tribunaux.

Charte de d'utilisation des moyens informatiques et du réseau de la Société Nationale des Postes du Burkina Faso

ENTRE :
La Société Nationale des Postes du Burkina Faso (SONAPOST),
Ci-après dénommé "la Société "
D'UNE PART,
ET
Tout employé de la SONAPOST et toute personne susceptible d'utiliser les ressources matérielles et logicielles informatiques, les réseaux ou toute autre infrastructure de la SONAPOST
Ci-après dénommé l'"Utilisateur "
D'AUTRE PART.

La présente charte a pour objet de formaliser les règles de déontologie et de sécurité que les Utilisateurs s'engagent à respecter en contrepartie de la mise à disposition des ressources informatiques de la Société.

1. Domaine d'application

Les règles et obligations énoncées ci-dessous s'appliquent à tout Utilisateur des matériels, systèmes, logiciels et réseaux informatiques de la Société.

Est déclaré Utilisateur, toute personne qui fait usage des ressources informatiques de la Société. L'Utilisateur est responsable, en tout lieu, de l'usage qu'il fait des ressources informatiques.

L'administrateur est une personne compétente en matière informatique et de réseaux, à qui a été attribuée la fonction de gestion de tout ou une partie de la

Général si le comportement d'un Utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

Les informations permettant de se connecter au système d'information (messagerie, compte Utilisateur, ...) sont strictement personnelles. Chaque Utilisateur est responsable de l'utilisation qui en est faite. Nul n'est autorisé à utiliser les informations personnelles d'autrui.

La connexion au réseau de tout ordinateur propre à un département ou un service, doit se faire sous contrôle d'un administrateur. Ce dernier doit s'assurer que les règles de sécurité sont bien respectées.

2.2 Droits et devoirs de l'Utilisateur

La sécurité des moyens informatiques mis à la disposition impose à l'Utilisateur :

- De respecter les consignes de sécurité et notamment les règles relatives à la définition et aux changements de mots de passe. Ce mot de passe ne doit correspondre ni à un mot, ni à un nom propre et ce, dans quelque langue que ce soit, et doit être gardé secret. Il doit comporter au minimum 6 caractères, choisis parmi des lettres de l'alphabet, des chiffres et des caractères de ponctuation

- De respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre Utilisateur, ni chercher à connaître ces informations ;

- De garder strictement confidentiels ses mots de passe et ne pas les dévoiler à un tiers.

- Si pour des raisons exceptionnelles et ponctuelles, un Utilisateur se trouvait dans l'obligation de communiquer son mot de passe, il devra procéder, dès qu'il en a la possibilité, au changement de mot de passe ou en

demander la modification à l'administrateur. Le bénéficiaire de la communication du mot de passe ne peut le communiquer à son tour à un tiers, ni l'utiliser en dehors de la circonstance exceptionnelle à l'origine de la communication.

- De verrouiller son poste de travail en cas d'absence et/ou d'utiliser les économiseurs d'écran avec mot de passe afin de préserver l'accès à son poste de travail ;

- D'avertir les administrateurs de tout dysfonctionnement constaté ;

- De ne pas installer, télécharger ou utiliser sur les matériels informatiques un logiciel et/ou un progiciel sans qu'une licence d'utilisation appropriée n'ait été souscrite par la Société;

- De s'interdire d'accéder ou tenter d'accéder à des ressources informatiques pour lesquelles l'Utilisateur ne bénéficie pas d'une habilitation expresse ; l'Utilisateur doit limiter ses accès aux seules ressources pour lesquelles il est expressément habilité à l'exclusion de toute autre, même si cet accès est techniquement possible ;

- D'avoir une obligation de confidentialité et de discrétion à l'égard des informations et documents électroniques à caractère confidentiel disponibles dans le système d'information ;
- D'utiliser les ressources et les moyens informatiques prioritairement à des fins liées à leurs activités et/ou à leurs formations professionnelles au sein de la Société.

- De respecter l'architecture réseau de la Société et de ne pas modifier sa configuration (connexion d'équipement réseau sur les prises murales) sauf accord préalable de l'administrateur réseau.
- A la fin de la journée, l'Utilisateur doit sortir du système et mettre les ordinateurs hors tension avant de partir. Les ordinateurs contenant des

fichiers ou informations sensibles doivent être codés et enfermés à clé dans les bureaux ou sécurisés de manière adéquate de toute autre façon.

- Si un système informatique présente des anomalies, le service d'assistance technique doit en être informé immédiatement. Une anomalie peut être l'indice d'une infection par un virus ou d'un autre problème de sécurité.

2.3 Droits et devoirs des administrateurs

Les administrateurs ont le devoir d'assurer un bon fonctionnement des réseaux et des moyens informatiques. Ils ont le droit de prendre toutes dispositions nécessaires pour assumer cette responsabilité tout en respectant la déontologie professionnelle.

En particulier sur incident, les administrateurs peuvent être amenés avec l'autorisation du responsable de service, de département ou de division à examiner le contenu de fichiers ou boîtes aux lettres, de façon à obtenir suffisamment d'informations pour pallier les incidents de fonctionnement ou s'il y a lieu, de pouvoir déterminer si un Utilisateur ne respecte pas la politique d'utilisation des ressources informatiques de la Société décrite dans ce document. Les administrateurs ont l'obligation de préserver la confidentialité des informations privées qu'ils sont amenés à connaître dans ce cadre.

Les administrateurs sont autorisés, en cas de difficultés majeures, à prendre des mesures provisoires et conservatoires ou à arrêter des services réseaux.

Tout message transportant un virus sera détruit par les outils de sécurité informatique sans que le destinataire et/ou l'émetteur puisse être informé.

Les Utilisateurs peuvent demander l'aide des administrateurs pour faire respecter leurs droits.

2.4 Mesures de contrôle de la sécurité

Le système d'information ainsi que l'ensemble des moyens de communication peuvent faire l'objet de surveillance et de contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus.

Le vol ou le détournement d'un matériel informatique (ordinateur, périphériques, CD etc.) doit être signalé aussi rapidement que possible au supérieur hiérarchique en fournissant le nom de l'Utilisateur directement concerné, la marque, le modèle, le type de l'ordinateur, son mode d'utilisation, la nature des informations contenues, la valeur, la date du vol, une copie de la déclaration à la police (le cas échéant) ainsi que toutes autres informations pertinentes relatives au vol ou au détournement.

2.5 Sécurité du poste de travail

Un ordinateur propre à l'administration centrale, aux directions régionales, aux centres spécialisés ou aux bureaux de poste, entre sur le réseau de la Société sous contrôle d'un administrateur. Durant la vie du poste, l'Utilisateur doit mettre en place un ou plusieurs dispositifs afin d'en assurer son intégrité.

Les administrateurs devront procéder à la mise à jour régulière des logiciels et/ou progiciels assurant la sécurité du système d'information et notamment des antivirus.

En cas de doute sur l'intégrité d'un poste de travail, l'administrateur peut le déconnecter. Le poste sera rebranché lorsque le chargé du réseau estimera qu'il ne portera pas atteinte à l'intégrité et à la sécurité du système d'information.

3. Usages des services Internet (Web, messagerie, forum, Chat)

La quantité et la facilité de circulation des informations et des contenus sur Internet ne doivent pas faire oublier la nécessité de respecter

la législation. L'Internet, les réseaux et les services de communication numérique ne sont pas des zones de non-droit. En effet :

L'Utilisateur doit faire usage des services Internet dans le seul cadre de ses activités, de sa formation professionnelle, dans le respect des principes généraux ainsi que dans le respect de la législation en vigueur.

Le téléchargement de fichiers, notamment de sons et d'images, depuis le réseau Internet est autorisé, dans le respect des droits de la propriété intellectuelle, mais doit correspondre à l'activité de l'Utilisateur dans la Société.

Les messages électroniques permettent d'échanger des informations à vocation professionnelle liées à l'activité directe de la Société. En toutes circonstances, les Utilisateurs doivent adopter un comportement loyal et digne et s'imposer le respect des lois et notamment celles relatives aux publications à caractère raciste, diffamatoire, injurieux et pornographique.

L'Utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques.

4. Propriété intellectuelle

L'utilisation des moyens informatiques implique le respect des droits de propriété intellectuelle de la Société Nationale des Postes du Burkina, de l'Union Postale Universelle, de ses partenaires et plus généralement de tout tiers titulaire de tels droits.

Chacun doit :

- utiliser les logiciels dans les conditions des licences souscrites ;

- ne pas reproduire, copier, diffuser, modifier et utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

5. Rappel et respect des lois

Il est rappelé que toute personne utilisant les ressources informatiques de la Société est soumise à la législation burkinabé en particulier dans le domaine de la sécurité informatique.
(Voir département juridique pour spécification particulière et conformité de la présente charte)

6. Sanctions

Les exemples suivants, non exhaustifs, sont ceux d'une utilisation non autorisée et/ou inappropriée des ressources informatiques de la Société qui peuvent exposer un Utilisateur à une mesure disciplinaire pouvant aller jusqu'à la résiliation de son contrat de travail :

1. Téléchargement, impression, création, affichage, transmission, envoi, expédition ou transfert de toute autre façon d'éléments ou de communications, non professionnels, inappropriés, constituant une infraction, une intimidation ou un harcèlement ; et accès à ces éléments ou communications, sur le plan interne ou externe, notamment lorsqu'il s'agit d'éléments qui sont en contradiction avec les règles de la propriété intellectuelle , de la protection de la vie privée ou du secret professionnel.

2. Accès aux ressources informatiques de la Société ou informations d'un autre Utilisateur sans son consentement exprès.

3. Utilisation des ressources informatiques de la Société pour accomplir un acte qui est en contradiction avec les politiques de la Société ou constituant une violation de celles-ci.

4. Copie ou utilisation de logiciels en violation d'un contrat de licence.

5. Envoi ou réception, par le biais des ressources informatiques de la Société, d'éléments protégés par des droits de reproduction, de secrets commerciaux,

d'informations confidentielles, exclusives ou financières ou d'éléments similaires sans autorisation appropriée.

7. Divulgation d'informations confidentielles sur des employés, la Société, ses affaires commerciales ou ses clients.

Le non-respect des règles définies dans la présente Charte pourra entraîner la suppression immédiate du droit d'accès de l'Utilisateur à tout ou une partie du Système d'Information sur décision du Directeur Général ainsi que, le cas échéant, des sanctions disciplinaires et /ou des poursuites judiciaires, civiles ou pénales.

Ce texte est à soumettre à l'appréciation du Conseil d'Administration de la Société Nationale des Postes (SONAPOST) du Burkina Faso

III Mesures d'accompagnement

Nous suggérons ici quelques conseils et bonnes pratiques en appui aux solutions que nous avons élaborées précédemment.

III.1 Pour l'administration : Création du poste de Responsable Sécurité Système d'Information (RSSI)

La croissance des problèmes liés à la sécurité nécessite un réel pilotage de ce domaine au niveau de l'entreprise. A cause de la complexité des systèmes informatiques, la protection des applications et celle des données deviennent une préoccupation majeure des entreprises. Ceci nécessite des spécialistes de la sécurité. Le métier de RSSI permet aux entreprises de cristalliser les exigences de sécurité et de manager les plans d'action.

Les RSSI doivent être capables d'identifier les indicateurs les plus pertinents à présenter, comment et avec quels mots, quelle terminologie. L'objectif est de sensibiliser la direction sur la nature de certains risques afin qu'elle puisse réagir de manière proactive.

Définition de la mission de RSSI suivant le CIGREF[6] (nomenclature 2002)

- Le RSSI est généralement rattaché à la direction informatique ;
- Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte ;
- Il peut intervenir directement sur tout ou une partie des systèmes informatiques et de télécommunications de son entité ;
- Il effectue un travail de *veille technologique*[7] et réglementaire sur son domaine et propose des évolutions qu'il juge nécessaires pour garantir la sécurité logique et physique du système d'information dans son ensemble ;
- Il est l'interface reconnue des exploitants et des chefs de projets mais aussi des experts et des intervenants extérieurs pour les problématiques de sécurité de tout ou partie du SI ;
- savoir comment le Système d'Information peut participer à la création de valeurs et s'aligner avec la stratégie de l'entreprise.
- Profil : Ingénieur ou équivalent bac + 4 ou 5 en informatique.
- Expérience : 10 à 15 ans d'expérience, dont une première expérience minimale dans le domaine de la sécurité

Évolution des missions du RSSI liées à la maturité de l'entreprise face à la sécurité de l'information

Elle s'articule sur quatre points :

- Quand le poste de RSSI n'existe pas dans une entreprise, la fonction de sécurité de l'information est assurée par la DSI sur un plan uniquement technique et souvent au coup par coup (mise en œuvre d'Antivirus, pare-feu pour site Web, etc.). C'est le cas actuel de la SONAPOST.

- Dès la prise de conscience, la fonction de RSSI est créée. Sa première mission va être de développer une Politique de Sécurité de l'Information en s'appuyant sur des normes et méthodes.

[6] Club Informatique des GRandes Entreprises Françaises
[7] Etude permanente portant sur les évolutions technologiques d'un marché

- En période de développement, le RSSI va devoir diffuser cette culture sécurité et avoir une mission de diffusion de ce savoir et savoir-faire dans l'ensemble des entités de l'entreprise.

- Enfin, à la maturité de l'entreprise, qui correspond à l'époque où la culture sécurité s'est diffusée dans l'entreprise (comme la culture qualité), le RSSI sera impliqué dans la stratégie de l'entreprise et participera notamment à l'élaboration du schéma directeur.

NB : Il convient de souligner que l'ensemble de notre étude est une partie du travail incombant au RSSI.

III.2 Pour l'administrateur du réseau

L'administrateur du réseau doit :

- lire régulièrement le journal d'évènement ;
- prévoir deux comptes administrateurs, l'un avec tous les droits et l'autre avec des droits limités pour les tâches courantes ;
- renommer le compte administrateur sur toutes les machines et mettre un mot de passe;
- supprimer les comptes des utilisateurs qui ont quitté l'entreprise ;
- supprimer ou invalider le compte invité sur les postes Windows;
- donner aux utilisateurs des règles de sécurité concernant l'ouverture des fichiers joints (*.EXE, *.DOC, *.BAT, ...) ;
- Se tenir informé des nouvelles technologies émergentes ;
- informer les utilisateurs des droits dont on peut doter les fichiers ;
- Sensibiliser les utilisateurs sur les problèmes de sécurité ;
- Former les utilisateurs sur l'utilisation de l'ordinateur.

III.3 Pour les utilisateurs :

Les utilisateurs devront :

- Respecter la charte d'utilisation ;
- Ne pas hésiter à contacter l'administrateur en cas de problème ;
- Suivre les règles de sécurités données par l'administrateur.

Remarque : Le réseau de la SONAPOST est en pleine évolution. En effet il faut souligner qu'à la fin de notre stage des réaménagements qui sont en cours embrassent une de nos solutions à savoir le remplacement des firewalls IPCop par des firewalls matériels Cisco PIX.

A la place des Cisco PIX se sont des Nokia IP260 Base System qui seront déployés dans les différents sites.

Il y a également le remplacement des certains routeurs par des routeurs Cisco 1841 et certains des switchs par des switchs de marque Linksys plus performants.

IV Evaluation des coûts

Achat de matériels

Désignation	Quantité	Coût/unité	Coût total
Licence antivirus kaspersky 6.0 pro(pour 100 postes)	01	1 820 000	1 820 000
Disque Dur 120Go	01	120 000	120 000
RAM 256 Mo	01	25 000	25 000
Coffre fort 1m²	01	1 416 000	1 416 000
Total1 HTT (Sans les coûts du clustering)			**3 381 000**

Coûts de l'étude et de la mise en œuvre

Travaux	Temps Nécessaire (jours)	Coût /jour	Coût total
Formation des utilisateurs à l'utilisation de Linux (400 personnes)	10	150 000	1 500 000
Etude complémentaire pour la rédaction de la politique de sécurité	10	25 000	250 000
Mise en place de la politique de sécurité (avec mission en province)	20	150 000	3 000 000
Coût HTVA			4 750 000

Total provisoire

Achat de matériels	3 381 000
Etude et mise en œuvre	4 750 000
Coût HTVA	8 131 000
TVA 18%	1 463 580
Total TTC	9 564 580

NB : Pour le Clustering nous avons soumis une demande d'estimation de couts à la société DataSys. Nous n'avons pas encore la facture pro forma. Nous suggérons à la SONAPOST de lancer un appel d'offre pour la mise en place du clustering.

CONCLUSION GENERALE

A la lumière de notre étude il apparaît clairement que les stratégies sécuritaires actuelles de la SONAPOST restent insuffisantes aussi bien du côté physique que du côté logique. Du reste, nous nous sommes appliqués à une recherche de solutions possibles ayant abouti à un choix conséquent et adéquat pour un renforcement de sécurité informatique élargie.

Le stage pratique en fin de cycle dans notre école est une occasion offerte aux étudiants, futurs ingénieurs de Travaux informatiques, de s'imprégner au mieux des réalités de la vie professionnelle. A la SONAPOST, nous pensons avoir atteint cet objectif à un niveau très acceptable et satisfaisant. Nous avons appris en trois mois la responsabilité qui revient à un informaticien et la lourde tâche d'assurer la sécurité d'un système informatique. Nous repartons avec un sentiment de non achèvement de notre travail. Ainsi souhaiterions-nous qu'une étude complémentaire soit faite sur la sécurité applicative et sur l'optimisation de l'interconnexion des différents sites du réseau.

RECOMMANDATIONS ET SUGGESTIONS

A la SONAPOST :

Au regard de la réticence générale des responsables des sociétés quant à la l'investissement dans la sécurité, nous invitons la direction à activer son engagement pour la sécurité de son système d'information. Certes, la sécurité ne permet pas de gagner de l'argent mais elle permet d'éviter d'en perdre.

Reconnaissant l'apport réel et bénéfique de notre stage au sein de la SONAPOST, nous exhortons les premiers responsables à toujours soutenir notre école en acceptant chaque année ses étudiants en quête de connaissances pratiques et professionnelles.

A l'ESI :

Nos premiers pas dans le milieu professionnel nous ont révélé quelques insuffisances dont la résolution consolidera les bases de la formation dispensée aux étudiants. Ainsi proposons nous de :

- Introduire un cours sur les systèmes d'information en REMI : aspects conception et sécurisation.
- Développer des projets en filière REMI. On pourra entre autres accentuer les recherches sur les techniques de:
  - Redondance et basculement de serveurs.
  - Câblage et protection de réseau,
  - Sauvegarde de donnée,
  - ...
- S'impliquer dans la recherche de stages pour les étudiants
- Assurer la prise en charge financière des stagiaires pendant la période de stage.

Annexes

```
        group                   = amanda
        groups                  = yes
        server                  = /usr/local/libexec/amandad
    }

service amandaidx
    {
        protocol                = tcp
        socket_type             = stream
        wait                    = no
        user                    = amanda
        group                   = amanda
        groups                  = yes
        server                  = /usr/local/libexec/amindexd
    }

service amidxtape
    {
        protocol                = tcp
        socket_type             = stream
        wait                    = no
        user                    = amanda
        group                   = amanda
        groups                  = yes
        server                  = /usr/local/libexec/amidxtaped
    }
```

Xinetd a besoin de connaître quel port il doit écouter et vers quel programme renvoyer la requête.

Pour cela il faut renseigner le fichier "/etc/services"

```
amanda          10080/udp
kamanda         10081/udp
kamanda         10081/tcp
amandaidx       10082/tcp
amidxtape       10083/tcp
```

Ensuite il faut relancer Xinetd avec la commande

```
bash-2.05b$ killall -HUP xinetd
```

II. Installation du Client

II. 1 Installation

Même procédure que pour le serveur, nous créons un utilisateur amanda et nous installons Amanda. Vous pouvez remarquer que nous passons l'option "-without-server" au script configure afin d'installer une version plus minimale.

```
bash-2.05b$                                groupadd                                amanda
bash-2.05b$ useradd -g amanda -G disk -s /bin/false amanda

bash-2.05b$ tar zxvf amanda-x.y.z.tar.gz
bash-2.05b$ cd amanda-x.y.z
bash-2.05b$ ./configure \
> --with-user=amanda \
> --with-group=amanda \
> --with-config=/etc/amanda \
> --with-gnutar=`which tar` \
> --with-amandahosts \
> ----with-portrange=50000,50100 \
> --without-server
bash-2.05b$ make
bash-2.05b$ make check
bash-2.05b$ make install
```

II. 2 Configuration de amandahosts

Tout comme pour la partie serveur, nous allons entrer dans le fichier amandahosts le nom du serveur et celui de l'utilisateur qui sera autorisé à se connecter au client pour faire une sauvegarde.

```
# machine                    utilisateur
backup-server    Amanda
```

II.3 Lancer Amanda

Amanda va etre lancé via Xinetd. Pour cela il faut modifier les fichiers xinetd.conf et services comme pour le serveur.

```
# Fichier xinetd.conf
service amanda
    {
        protocol              = udp
        socket_type             = dgram
        wait                  = yes
        user                  = amanda
        group                  = amanda
```

```
    groups              = yes
    server              = /usr/local/libexec/amandad
}

# Fichier /etc/services
amanda          10080/udp
kamanda         10081/udp
kamanda         10081/tcp
amandaidx       10082/tcp
amidxtape       10083/tcp
```

Ensuite il faut relancer xinetd avec la commande

```
bash-2.05b$ killall -HUP xinetd
```

III. Démarrer une sauvegarde

III.1 Vérification

A chaque nouveau disque, il faudra lui donner un nom. Ce nom servira pour retrouver facilement sur quel disque se trouve telle ou telle sauvegarde.

```
bash-2.05b$ su amanda -c "amlabel serveur Serveur-001"
```

Ensuite nous allons tester notre configuration. Ce test doit être effectué à chaque fois que l'on ajoute un client à une configuration.

```
bash-2.05b$ su amanda -c "amcheck serveur"
```

III.2 Programmer les sauvegardes

Nous allons éditer la crontab de l'utilisateur amanda, afin de lancer une sauvegarde une fois par jour a 2:05 AM.

```
bash-2.05b$ su amanda -c "crontab -e"
05 02 * * * /usr/local/sbin/amdump serveur
bash-2.05b$ su amanda -c "crontab -l"
```

IV. Faire une restauration

La restauration devra se faire depuis une machine cliente

Nous allons faire un exemple. Imaginons que nous voulions restaurer le fichier "/www/labo-linux.org/index.php" et le dossier "/www/labo-linux.org/images/"

Premièrement il faut se placer dans le dossier racine de la sauvegarde soit "/www"

```
bash-2.05b$ cd /www
```

Ensuite on lance la commande amrecover avec le nom de la sauvegarde

```
bash-2.05b$ amrecover -c serveur
```

Une fois connecté, on va renseigner le nom du client, la date de la sauvegarde et la racine de la sauvergarde

```
sethost web-server
setdate 2004-08-23
setdisk /www
```

Puis grâce à la commande "add", nous allons spécifier le fichier et le dossier à restaurer

```
cd /www/labo-linux.org
add index.php
add images/
```

La commande "extract restaurera les fichiers et dossiers sélectionnés.

```
extract
```

Annexe 3 : Fiche de maintenance

Fiche de maintenance Une fiche par équipement		N° d'identification de la fiche :
Numéro d'inventaire de l'équipement		Date :
Type d'équipement		
Type de problème (à cocher)	Matériel	Logiciel
Description du problème		
Couverture par la garantie (à cocher)	Oui	Non
Description de la réparation		
Réparation effectuée par		
Commentaires		

« L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique.»

[Albert Einstein]

Mais

« LE MOYEN D'ETRE SAUF, C'EST DE NE PAS SE CROIRE EN SECURITE.»

[Thomas Fuller]

BIBLIOGRAPHIE

- **Ouvrages ou livres :**

  - Tableau dc bord de la sécurité 2ième édition (cedric Liorens, Laurent Levier, Denis Levier) Groupe Eyrolles 2003, 2006,
  - MéhariTM V3 Guide de l'analyse des risques (octobre 2004)
  - MéhariTM V3 Principes et mécanismes (octobre 2004)
  - Guy PUJOLLE: Les réseaux Edition 2003 ;

- **Sites Web :**

http:\\www.sonapost.bf/ ;
http:\\www.securité.org/ ;
http:\\www.commentcamarche.net/ ;
http:\\www.linux-France.org/ ;
http:\\www.secuser.com/ ;
http:\\www.supinfo.fr/ ;
http:\\www.alaide.com/ ;
http:\\www.eerezo.com/ ;
http:\\www.microsoft.com/ ;
http:\\www.clusif.asso.fr/ ;
http:\\www.wikipedia.com/ ;
http:\\www.framesoft.net/ ;
http:\\www.generation-nt.com/ ;
http:\\www.mirror.open-xchange.org/ ;
http:\\www.info-appliquée.com/ ;
http:\\www.safenet_inc.com/ ;
http:\\www.ybet.be/ ;
http:\\www.free-av.com/.

Table des matières