La sécurité informatique

Charles Dracoulides

le cnam

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Centre Régional Associé Du Havre

MEMOIRE

présenté en vue d'obtenir

le DIPLOME D'INGENIEUR CNAM

SPECIALITE : Informatique

OPTION : Réseaux, Systèmes et Multimédia

par

Charles DRACOULIDES

La sécurité informatique

Soutenu le 7 Mai 2015

JURY

PRESIDENT :	**Monsieur Yann POLLET**	**Professeur**
MEMBRES :	**Monsieur Claude DUVALLET**	**Maître de conférences**
	Monsieur Marc GORKA	**Maître de conférences**
	Monsieur Philippe WENDER	**Ingénieur**
	Monsieur Nicolas LARZUL	**Ingénieur**

Remerciements

Je tiens dans un premier temps à remercier Monsieur Claude DUVALLET, docteur en informatique au CNAM, pour son aide et ses conseils.

Je remercie également la société CRAM qui m'a permis de travailler dans un cadre particulièrement agréable dans lequel j'ai pu évoluer et monter en compétences. Merci également à Patrick LECLERC, directeur du système d'information, pour son accueil au sein de son équipe informatique et pour les projets qu'il m'a permis de réaliser. Une pensée pour mes collègues du service infrastructure avec qui j'ai passé de bons moments.

Je souhaite remercier les prestataires des sociétés Artemys, Frame IP, SFR, Tibco avec lesquels j'ai mené des projets de plus ou moins grande envergure.

Mes dernières pensées iront vers ma famille, à ma femme et à mes parents, qui m'auront soutenu et encouragé jusqu'au bout de ce mémoire.

Liste des abréviations

ACL : Access Control List

AD : Active Directory

AES : Advanced Encryption Standard

API : Application Programming Interface

APSAD : Assemblée plénière des sociétés d'assurances dommage

ATM : Asynchronous Transfer Mode

BAT : Fichier batch

BIOS : Basic Input Output System

BLR : Boucle locale radio

BSD : Berkeley Software Distribution

CA : Chiffre d'Affaire

CCMP : Counter Cipher Mode Protocol

CD : Compact Disc

CISCO ASA : CISCO Adaptive Security Appliances

CNPP : Centre national de prévention et de protection

CO^2 : Dioxyde de Carbone

CPL : courants porteurs en ligne

CRAM : Chauffage rationnel et application moderne

DDOS : Distributed Denial of Service

DES : Data Encryption Standard

DIT : Département Industrie Télésystèmes

DOS : Disk operating system

DSG : Direction des Services Généraux

DSI : Direction des Systèmes Informatiques

EBE : Excédent Brut d'Exploitation

FAI : Fournisseur d'Accès Internet

FBI : Federal Bureau of Investigation

FM : Factory Mutual

FTP : File Transfer Protocol

GPO : Group Policy Object

HTML : HyperText Markup Language

HTTPS : HyperText Transfer Protocol Secure

IDF : Île de France

IEEE : Institute of Electrical and Electronics Engineers

IP : Internet Protocol

IPSEC : Internet Protocol Security

IRC : Internet Relay Chat

ISO : International Organization for Standardization,

ISO 9001 : Base de référence en matière de management de la qualité

ISO 27001 : Spécifie un système de gestion de la sécurité des systèmes d'information

ITIL : Information Technology Infrastructure Library

JRE : Java Runtime Environment

Ko : Kilo octets

LAN : Local Area Network

L2TP : Layer two Tunneling Protocol

MARION : Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux

MASE : Manuel d'Amélioration de la Sécurité des Entreprises

MPLS : Multi protocol Label Switching

MS-CHAP : Microsoft-Challenge-Handshake Authentication Protocol

MS-DOS : Microsoft Disk Operating System

MSN : MicroSoft Network

NAT : Network Address Translation

NOR : Normandie

OS/2 : Système d'exploitation créé par Microsoft et IBM

OSI : Open Systems Interconnection

PC : Personal Computer

PHP : Hypertext Preprocessor

PPTP : Point-to-point tunneling protocol

PSW : Program status word

QDS : Qualité De Service

QOS : Quality Of Service

RDC : Rez-De-Chaussée

RJ45 : Registered Jack 45

RSI : Responsable Système Informatique

SANS : SysAdmin, Audit, Network, Security

SDSL : Symmetric Digital Subscriber Line

SMTP : Simple Mail Transfer Protocol

SQL : Structured Query Language

SRV : Serveurs

SSID : Service Set Identifier

URL : Uniform Resource Locator

USB : Universal Serial Bus

VB6 : Visual Basic

VBA : Visual Basic for Applications

VBS : Visual Basic Script

VLAN : Virtual Local Area Network

VPN : Virtual Private Network

VPN-SSL : Virtual Private Network Secure Sockets Layer

WEP : Wired Equivalent Privacy

WIFI : Wireless Fidelity

WLAN : Wireless Local Area Network

WPA : Wifi Protected Access

X-25 : Protocole de communication normalisé par commutation de paquets en mode point à point offrant de nombreux services

ZIP : Formats de regroupement et de compression de fichier des logiciels WinZip et PKZip

Table des matières

Présentation de l'entreprise CRAM

L'objectif de la CRAM repose sur la maîtrise et la limitation de la consommation d'énergie avec la mise en œuvre de solutions à base d'énergies renouvelables, la conception, la réalisation et l'exploitation des installations. Cela permet de répondre aux grands enjeux économiques, sociaux et environnementaux de ses clients.

De par ses différentes implantations d'agences en Normandie, Ile de France et Picardie, la CRAM se veut proche de ses clients afin de répondre au mieux à leurs attentes.

La CRAM est une entreprise à taille humaine avec un effectif de 300 techniciens et plus de 50 ingénieurs/experts. Les équipes d'experts apportent des conseils aux clients en matière de sûreté et de conformité tout en s'appuyant sur une veille technique permanente. Ils mettent en œuvre des solutions innovantes dans le choix des énergies et des équipements avec comme priorité l'efficacité énergétique durable, possible notamment grâce aux énergies renouvelables.

L'entreprise est certifiée ISO 9001 et MASE (Manuel d'Amélioration de la Sécurité des Entreprises). Tous ses collaborateurs exercent leurs activités selon des méthodes formant un système vivant de Management de la Qualité, de la Sécurité et de l'Environnement.

La société compte plus de 400 collaborateurs au total et réalise un chiffre d'affaires consolidé de 100 millions d'euros. Elle se compose d'une société mère (CRAM SAS) et de plusieurs filiales pour ses activités de réseaux de chaleur et de cogénération.

La CRAM est une société par Actions Simplifiées qui a été fondée au Havre en 1958. Originaire de Normandie, l'entreprise a rapidement étendu son territoire d'activité. Une agence a été créée en Ile de France en 1970, une autre en Picardie en 1971 et un Département Industrie Télésystème a été fondé au Havre en 2005.

Aspect financier de l'entreprise CRAM

Intéressons-nous à quelques chiffres financiers de la société CRAM, le but n'étant pas d'effectuer une analyse financière mais plutôt d'avoir une idée du Chiffre d'Affaires, du résultat net ou encore de la répartition du budget informatique. L'étude financière n'étant pas le but premier, nous ne parlerons pas de l'excédent brut d'exploitation (EBE), de l'équilibre du bilan ou encore des différents chiffres comme l'évolution de l'activité de la société.

La CRAM, qui possède un capital social de 1 million 428 mille euros, a réalisé en 2010 un chiffre d'affaire de 79 millions et 700 k€, soit une baisse de 5,23% par rapport à 2009 où son CA était de 84 millions et 70 k€. Son résultat net est resté quasiment identique avec 4 millions et 212 k€ en 2010 contre 4 millions et 238 k€ en 2009.

La société CRAM est détenue majoritairement par la société DALKIA qui est une filiale de la branche énergie de la société VEOLIA. L'autre partie des parts de la société CRAM sont des actions familiales. La société CRAM a négocié son indépendance de gestion à la cession des parts. Toutefois cet accord reste un accord tacite entre DALKIA et la CRAM qui sont en concurrence au quotidien sur le marché. La société DALKIA a toutefois son mot à dire quand la société CRAM décide d'investir dans un gros projet s'élevant à plusieurs millions d'euros.

Évoquons maintenant plus en détails le fonctionnement du budget informatique, à savoir sa répartition et voyons comment il est formalisé.

Le budget informatique est tout d'abord découpé en deux parties : logiciels et matériels. Il est ensuite redécoupé en fonction de chaque agence (DIT, NOR, SIEGE, IDF).

Pour certaines commandes, une ouverture de chantier est nécessaire, surtout lorsqu'il s'agit d'un gros projet comme le changement des onduleurs de la salle serveur, la commande de plusieurs serveurs, etc. Ces chantiers sont tout de même intégrés au budget mais peuvent être découpés afin d'être éclatés en fonction des années. Par exemple, les onduleurs seront découpés sur 5 ans et chaque année sera donc intégrée 1/5 du prix final du chantier dans le budget annuel.

Management

J'ai régulièrement été amené à manager différents prestataires afin de mettre en place des projets comme celui de la plateforme de supervision. J'ai confié des tâches à mes collègues et je me suis assuré du bon déroulement de ces dernières.

Concernant le projet de sécurisation du système d'information, j'ai embauché une stagiaire en licence de sécurité informatique afin de pouvoir lui confier certains travaux. Etre son tuteur de stage m'a permis de me rendre compte de la complexité d'encadrer une personne n'ayant pas ou très peu d'expérience professionnelle.

Au début, il est difficile de se faire comprendre et d'obtenir ce que l'on souhaite. Il faut en permanence réajuster les priorités de façon à ne pas voir la personne se dissiper sur d'autres sujets que celui originel. Le relationnel reste délicat à gérer mais c'est aussi tout l'intérêt du management…

Introduction

Bien que la sécurité informatique ne soit jamais primordiale pour une société, il faut toutefois être très vigilant car un piratage peut engendrer une très grosse perte financière pour l'entreprise pouvant même aller dans certains cas « extrêmes » au dépôt de bilan de l'entreprise.

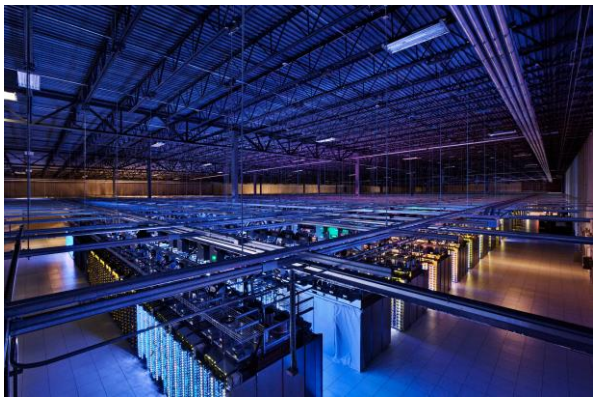
Nous parlerons dans un premier temps de la sécurité physique qui est la base de tout. En effet, pourquoi sécuriser un système d'informations et protéger ses données si un individu quelconque peut connecter son pc au réseau de l'entreprise ou même encore entrer dans la salle serveur ? Nous verrons ainsi les différents types de locaux, les sinistres pouvant survenir, les risques humains, électriques, le câblage réseaux, etc.

La seconde partie traitera de la sécurité réseaux. En effet, quelle utilité peut-il y avoir à sécuriser des machines hébergeant des données si l'échange entre ces dernières ne l'est pas ? Nous détaillerons, dans cette partie, les différents types de réseaux externes ainsi que les équipements et les configurations des réseaux internes.

Dans la troisième partie, nous évoquerons la sécurité des logiciels qui sont bien trop souvent considérés comme sécurisés et sur lesquelles très peu d'attention est portée. Nous étudierons tout d'abord les différentes menaces liées aux logiciels malveillants ainsi que les moyens pour lutter contre ces dernières. Nous nous consacrerons ensuite aux systèmes d'exploitation avec notamment les droits d'accès, l'authentification, les mots de passe, le chiffrement, etc. Nous terminerons par l'évocation de quelques failles et précautions à prendre en développement.

Dans la dernière partie, nous étudierons la sécurité utilisateur qui est la plus complexe à maîtriser. Il est en effet difficile d'imposer quelque chose à des salariés ou encore de les « surveiller ». Cela peut être considéré comme de l'espionnage et provoquer un mécontentement de leur part. Nous commencerons par examiner les risques liés aux utilisateurs puis nous ferons un état des lieux. Pour finir, nous verrons un guide des « bonnes pratiques » et évoquerons brièvement une éventuelle mise en place d'une charte informatique permettant de renforcer la politique de sécurité.

I Sécurité Physique



La sécurité physique est bien trop souvent oubliée. Quel intérêt peut-il y avoir à sécuriser tout un système d'information si n'importe qui peut accéder physiquement aux serveurs et aux postes de travail hébergeant les données ? Pourquoi mettre en œuvre des moyens de redondance dans une salle serveur si celle-ci est sujette à une quelconque intempérie ? Il est donc important de protéger le système d'information des différents risques comme les risques humains, environnementaux, électriques…

Le but d'une sécurité physique aboutie est d'avoir les performances optimales sur la plus longue durée possible par des actions à la fois préventives et protectrices même si cela ne peut empêcher certains sinistres. Il est toutefois important de trouver l'équilibre entre les actions dites préventives et celles dites protectrices puisqu'on ne peut pas toujours prévenir les sinistres mais s'en protéger au mieux.

Nous allons détailler les différents points associés à la sécurité physique et voir quelles précautions, il est nécessaire de prendre ainsi que les choix effectués par la société CRAM dans ces différents domaines.

I.1 Type de local informatique

Afin de protéger le mieux possible les équipements informatiques, il est nécessaire de les isoler dans des salles bien définies. Il est important de séparer les locaux informatiques des locaux où travaillent et circulent les employés. C'est pourquoi, les serveurs et équipements du cœur de réseaux seront placés dans une salle spécifique. Les autres équipements tels que les équipements

réseaux destinés à l'interconnexion des utilisateurs seront eux placés à des endroits stratégiques afin de limiter la longueur des câbles réseaux et la complexité du câblage.

Décrivons plus en détails ces différents types de lieux :

Salle informatique de type "Data Center[1]" :

Elle héberge les serveurs, les calculateurs, la solution de sauvegarde, les baies de stockage... Elle contient également les éléments critiques du réseau (commutateurs[2], routeurs[3]...) ainsi que les points d'accès et équipements servant à connecter la société vers le monde extérieur (central téléphonique, accès Internet...).

Outre l'aspect de la sécurité, une salle contenant des serveurs doit être climatisée puisque les équipements informatiques de cette dernière dégagent beaucoup de chaleur et nécessitent un environnement propre dans lequel il y a le moins de poussière ou résidu possible.

Une salle serveur demande une étude préalable concernant la puissance électrique qu'il faudra calculer en se laissant une marge confortable afin d'éviter toute coupure ou surchauffe des équipements électriques.

L'infrastructure est aussi très importante puisque des armoires remplies de serveurs pèsent relativement lourd. La dalle du bâtiment doit alors supporter cette charge !

---

1 Data Center : Un centre de données est un site physique sur lequel se trouvent regroupés des équipements constituants le système d'informations de l'entreprise (serveurs, baies de stockage, équipements réseaux, etc.).

2 Commutateurs : Un commutateur réseau, ou switch, est un équipement qui relie plusieurs segments (câbles ou fibres) dans un réseau informatique et qui permet de créer des circuits virtuels.

3 Routeurs : Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, au mieux, selon un ensemble de règles.

Salle "connectique" d'étage :

Espace dans lequel sont placés les équipements réseaux permettant l'interconnexion entre les prises réseaux des étages et la salle serveur. Ces espaces contiennent habituellement des panneaux de brassage ainsi que des commutateurs d'étage. Etant donné l'importance de ces équipements, ces locaux sont considérés comme des locaux informatiques et sont donc soumis aux mêmes exigences de conception et de surveillance que les salles informatiques.

Dans le cas de la CRAM, on retrouve les catégories suivantes :

Salle « serveurs » :

C'est l'endroit où se situent tous les serveurs, les équipements réseau et la solution de sauvegarde (coffre dans lequel les bandes de sauvegarde sont placées avant d'être transmises aux différents acteurs extérieurs). Cette salle est climatisée par deux climatiseurs afin d'obtenir une redondance. La température de la salle est surveillée en permanence via un système de supervision identique à celui mis en place sur les chaufferies. Ce système permet le déclenchement d'une intervention et le déplacement d'un technicien de la CRAM dès qu'une température anormale est constatée.

L'accès à la salle serveur est sécurisé par digicode et la porte d'entrée se situe à l'intérieur de la salle d'installation des PC, elle-même fermée à clef.

Salle d'installation :

Salle servant à stocker du matériel en cours d'installation, comme des PC ou des serveurs. Elle est dépourvue de climatisation et ferme à clef.

Baies de brassage :

Baies dans lesquelles sont installés les switchs de distribution du réseau. On les trouve à chaque étage de la société, dans un placard fermant à clef.

I.2 Sinistres

La qualité du bâtiment abritant les données et traitements peut se révéler très importante dans le cas d'intempéries, d'inondations, d'incendies ou même d'intrusions.

On peut distinguer deux grands types de sinistres :

- Les sinistres liés à un incendie pouvant provoquer la destruction partielle ou totale des équipements informatiques et donc engendrer l'indisponibilité de toute une partie de l'architecture. Ils peuvent aussi souvent être accompagnés des dégâts liés à l'eau du fait des tentatives d'extinction...

  Quelques précautions à prendre :

  - Tenir compte du voisinage de la salle informatique.
  - Éviter le stockage à proximité de produits inflammables.
  - Vérifier régulièrement les circuits électriques (proscrire les kyrielles de blocs multiprises).
  - Prévoir des mécanismes d'extinction de feu ne portant pas préjudice aux matériels (gaz).
  - Utiliser des armoires ou coffres forts ignifugés pour le stockage des supports informatiques.

- Les sinistres liés aux dégâts des eaux comme par exemple la rupture d'une conduite, une infiltration, un déclenchement du système anti-incendie ou encore l'obstruction des évacuations d'eaux usagées.

  - Conséquences :

    - Court-circuit.
    - Dangers d'électrocution.
    - Détérioration des équipements.
    - Corrosion des câbles et connecteurs.

- Prévention :

Il convient de choisir judicieusement la localisation de la salle informatique, en évitant les sous-sols (inondations) et les derniers étages (infiltrations). Il est aussi important d'éviter le plus possible la circulation d'eau dans la salle en plaçant le groupe de conditionnement d'air en dehors ou encore en choisissant les chemins de tuyauterie...

Dans le cas où la salle est déjà installée, des parades existent permettant de protéger les équipements. Il est ainsi possible de mettre en place des systèmes de détection de fuites, de surélever les équipements, d'utiliser des tubes hermétiques pour les câblages d'alimentation ou de réseaux. Il est aussi possible de compartimenter le plancher de façon à contenir et à diriger l'eau vers des systèmes d'évacuation.

Etat des lieux de la CRAM :

La salle « serveurs » se situant au troisième étage est de par sa hauteur hors d'atteinte d'éventuelles catastrophes naturelles telles que des inondations.

La salle ainsi que l'étage sont équipés d'extincteurs au CO^2 afin de ne pas dégrader ou rendre inutilisable le matériel dans le cas d'un incendie.

L'arrivée électrique ainsi que les équipements de type onduleur ne sont pas à même le sol afin d'éviter que ces derniers soient touchés lors d'une fuite d'un climatiseur ou tout autre incident de ce type.

Les bandes de sauvegarde se situent dans un coffre-fort afin d'être protégées lors d'un sinistre. La procédure de sauvegarde s'opère dans l'entreprise par un roulement de détention des bandes entre les différents membres du service informatique.

La salle « serveurs » est équipée de deux climatiseurs afin d'assurer une redondance en cas de défaillance de l'une des deux climatisations. Elle est aussi équipée de dispositifs permettant de couper le courant en cas de surcharge ou autre défaut constaté.

Les onduleurs fournissant le courant possèdent une page d'administration permettant de voir les graphiques de consommation électrique, ceci afin d'anticiper une éventuelle montée en charge des équipements. Chaque onduleur a son propre câblage électrique.

Les serveurs sont équipés de deux alimentations afin d'être alimentés par deux onduleurs différents.

De par son activité, la CRAM assure la maintenance de la climatisation et de l'électricité. La salle « serveurs » est sous surveillance 24h/24 et 7j/7. En cas de hausse de la température ou de coupure électrique, une alerte est directement envoyée au système de télésurveillance de la société qui déclenche l'intervention d'un technicien. Ce procédé est le même que celui utilisé pour les clients de la CRAM tels que les chaufferies.

Aucune procédure de sauvegarde pour un usage en mode restreint permettant d'arrêter les serveurs ou équipements non critiques n'a officiellement été diffusée. J'ai toutefois créé et mis à disposition dans la salle « serveurs » une liste sur laquelle figurent les serveurs fondamentaux (AD[4], SQL PROD, FICHIERS, etc.). J'ai aussi défini un ordre de démarrage afin de ne pas démarrer n'importe quel serveur en premier. J'ai également collé des pastilles de couleur sur les serveurs avec des numéros permettant de définir l'ordre de criticité.

I.3 Risques humains

Une personne non autorisée circulant dans les locaux peut provoquer divers incidents (vols, vandalisme, pertes de confidentialité, sabotages, etc.) ayant pour conséquences des pertes de temps, des pertes financières, etc.

---

4 AD : Active Directory est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc.

Il existe différents moyens permettant de prévenir ces incidents comme la mise en place d'un service de détection des déplacements et d'intrusions, un contrôle d'accès (badges, biométrie), une politique d'identification pour les visiteurs, les prestataires, etc.

Il est bien entendu indispensable de contrôler qui entre dans la société puisqu'il peut très bien s'agir du personnel interne, de prestataires, de la société de gardiennage, de nettoyage, etc. De même, dans une salle serveur le contrôle doit être obligatoire et l'accès réservé uniquement aux personnes faisant partie intégrante du service informatique (l'accès peut même être restreint aux personnes de l'équipe infrastructure et non aux développeurs par exemple). Les entrées et sorties de la salle serveur sont une source potentielle de dysfonctionnements volontaires ou involontaires.

Afin d'obtenir une sécurité correcte, il convient d'identifier les zones sensibles pour pouvoir en limiter les accès aux membres du personnel non autorisé et de les informer du caractère sensible de certaines zones dans lesquelles le personnel autorisé intervient. Il est aussi nécessaire de limiter le passage dans des zones intermédiaires et d'interdire l'accès aux zones sensibles (serveurs, réseaux…).

Différentes précautions peuvent être appliquées :

- Sécuriser les zones comportant le matériel le plus sensible ou regrouper ce matériel dans les zones les mieux protégées.

- Rendre les accès de maintenance ordinaires (eau, électricité, ascenseurs...) accessibles en dehors des locaux si possible ou au moins en dehors des locaux sécurisés.

- Mettre en place une signalisation conviviale indiquant que l'accès est interdit en précisant par exemple que l'informatique n'est pas un monde à part, que c'est juste un monde à protéger.

- Effectuer une rotation pour des supports de sauvegarde (bandes, cassettes, CD) afin de les sortir de la société.

- Installer des systèmes de contrôle d'accès (systèmes avec badge, cartes, digicodes, etc.).

- Afin de surveiller toute intrusion dans les locaux ou le bâtiment, il est judicieux d'installer un système de surveillance extérieure comme des caméras, détecteurs de présence, etc. Cela permet à la fois d'enregistrer les entrées et les sorties et d'avoir un rôle très dissuasif. Pour que l'enregistrement soit efficace, il doit être continu afin de pouvoir constater une éventuelle effraction.

Risques humains au sein de la CRAM :

La CRAM est équipée d'un contrôle des accès par badges, empêchant toute personne étrangère d'entrer dans la société sans se présenter à l'accueil. Les badges permettent ainsi de définir à quelle porte les gens ont accès. Lors de la mise en place du système de contrôle par badges, j'ai moi-même réalisé un script afin de générer et d'éditer la liste des accès en fonction des groupes « active directory » auxquels les gens appartiennent.

Les locaux informatiques tels que la salle serveur, la salle d'installation ou encore les baies de brassage sont sécurisés comme vu précédemment dans la partie « Type de locaux ».

Un système de vidéo surveillance a également été mis en place. J'ai moi-même configuré le boitier de gestion centrale afin de pouvoir y accéder directement via le réseau. Il suffit ensuite d'installer le logiciel sur les ordinateurs des personnes concernées pour avoir accès aux caméras ainsi qu'aux contenus enregistrés.

I.4 Risques électriques

La qualité de l'alimentation électrique est primordiale puisque des dégâts liés à l'électricité (surtensions, sous-tension, coupures de courant) sont difficilement prévisibles et ont une conséquence sur le matériel informatique non négligeable (pertes de données, pannes d'équipements, etc.). De tels risques ne pouvant être acceptés, il est nécessaire d'avoir un câblage électrique redondant, d'anticiper au mieux la puissance de l'alimentation électrique, de s'assurer que les équipements critiques ont une double alimentation et que les bâtiments sont équipés de systèmes évitant les remontées de foudre, etc. Il est important de s'équiper d'onduleurs de façon à protéger le matériel alimenté par ces derniers afin de garantir une continuité de service correcte.

Les risques électriques concernant la CRAM :

Après avoir connu quelques soucis de coupures électriques dans la salle serveur, cette dernière a entièrement été repensée. J'ai tout d'abord fait intervenir un électricien afin d'analyser l'origine du problème qui provenait d'un déséquilibre au niveau des phases (la salle serveur est alimentée par un réseau triphasé). Ce déséquilibre était dû à une mauvaise répartition des onduleurs. Obtenir une bonne répartition était très difficile puisque chaque armoire comptait environ 3 onduleurs. Ces derniers arrivant en fin de vie (cycle de 5 ans), j'ai donc choisi de les remplacer par deux gros onduleurs mais directement alimentés en triphasé pour répartir parfaitement la charge entre les différentes phases (Annexe 1 – Schéma électrique de la salle serveur du SIEGE).

Lors de mon étude, j'ai aussi soulevé la question de la mise en place d'un groupe électrogène. Après m'être entretenu avec l'électricien, il s'est révélé que ce type d'installation nécessite une maintenance régulière (chaque semaine) avec des démarrages et des tests réguliers.

Le coût annuel d'entretien s'est révélé être « négligeable ». Toutefois, après réflexion et discussion avec le RSI, un tel achat ne serait pas réalisé tout de suite. Les principales contraintes étant le coût d'achat, le manque de place et le passage des câbles avec la nécessité de devoir éventuellement casser le bitume.

I.5 Câblages réseaux

Les liaisons servent à véhiculer l'information entre les éléments actifs du réseau tels que les postes utilisateurs, les équipements réseaux, les serveurs, etc.

Les liaisons peuvent être des éléments internes (câbles, fibre optique, ondes, laser, infrarouges, etc.) Ces liaisons sont présentes dans tous les locaux de l'entreprise (bureaux, entrepôts, couloirs) ce qui les rend faciles d'accès et donc difficiles à sécuriser. De plus, elles sont en perpétuelle évolution.

Il est souhaitable d'éviter que les chemins de câble soient dans des endroits non protégés.

Différents types de menaces sont à constater :

- Coupure accidentelle ou volontaire de câbles (sabotage).

- Branchement « pirate ».
- Interférence (compatibilité électromagnétique des équipements).
- Erreur de manipulation (déconnexion accidentelle).
- Erreur de branchement.
- Dégâts des eaux.
- Perturbation, écoute et rupture des liaisons.
- Radio (électromagnétique), Infrarouge, etc.
- Incendie et propagation de l'incendie.

Le câblage réseau de la CRAM :

Après avoir effectué le tour de la société CRAM, j'ai décidé de supprimer certains câbles qui passaient à l'extérieur des bâtiments, le long d'une haie. D'autres câbles reliant les bâtiments étant passés dans des fourreaux sous le bitume de la société, aucun risque n'est à prévoir. Dans les locaux, le passage des câbles s'effectue dans les faux plafonds (le bâtiment étant sécurisé avec un accès par badge cela réduit les risques).

I.6 Réseaux sans fil

Le réseau sans fil est souvent montré du doigt de par son accessibilité au-delà des locaux puisqu'il n'a pas de délimitation physique. Il est donc nécessaire de placer les bornes WiFi à des endroits stratégiques, de régler leur puissance d'émission afin de réduire et voir même de supprimer les lieux accessibles au public. On peut aussi affiner le signal en changeant le type d'antenne utilisée (omnidirectionnel ou directionnel). Il est impératif qu'aucune personne extérieure ne puisse se connecter au WiFi de l'entreprise et ainsi récupérer des informations pouvant être confidentielles. Sa faible sécurisation oblige aussi à paramétrer les bornes convenablement. Nous verrons ce point par la suite.

Intéressons-nous au réseau WiFi de la CRAM :

Voici un plan représentant la portée des ondes WiFi autour du siege de la société :

Figure 1 - Portée des ondes WiFi autour du siege de la société

Les bornes ont été placées de façon à limiter la propagation des ondes WIFI au secteur de l'entreprise. De plus, elles sont programmées pour se couper à partir de 19H le soir et se rallumer à 7H20 le lendemain matin, limitant ainsi les tentatives d'accès.

I.7 Assurances et normes de conformité

Il devient de plus en plus difficile d'être assuré et correctement indemnisé en l'absence de mise en œuvre d'un niveau élevé de sécurité défini par différentes normes. De nos jours beaucoup de compagnies d'assurance exigent une certification telle que l'APSAD (du CNPP) ou la FM (Factory Mutual). Le recours à un expert est souvent une bonne précaution à prendre afin de vérifier que les installations sont conformes aux contrats souscrits.

La société CRAM fait contrôler ses équipements (extincteurs et autres matériels de sécurité) tous les ans par des organismes spécialisés.

I.8 Les précautions à prendre

Voici quelques précautions :

1. Formaliser l'accueil à l'entreprise. Il suffit souvent à l'intrus d'annoncer qu'il vient d'une société quelconque pour rencontrer un collaborateur et entrer sans aucune vérification.

2. Tout le monde doit être badgé, et pas seulement les visiteurs. À défaut, il suffit à l'intrus de retirer le badge «visiteur » pour *« appartenir »* à l'entreprise et pouvoir s'y déplacer librement.

3. Sensibiliser les collaborateurs de l'entreprise aux intrusions. Ils ne doivent pas hésiter à interroger une personne inconnue croisée dans les locaux, afin de connaître l'objet de sa visite.

4. Formaliser la vidéo surveillance. On peut masquer une caméra longuement sans aucune réaction des employés. Il faut que les procédures de réaction soient bien définies et souvent contrôlées.

5. Surveiller ses déchets. Il arrive de trouver dans des corbeilles des brouillons de bulletins de paie ou des papiers comptables, alors que le coût d'investissement d'un broyeur papier est peu onéreux.

6. Sauvegarde régulière des données informatiques sur d'autres supports physiques que ceux utilisés en production et nécessité de les délocaliser en dehors du site d'exploitation.

7. Aménagement d'un site de secours pour les applications informatiques vitales.

Cette liste de précautions n'aura aucune utilité s'il n'existe aucune documentation à jour et si aucun exercice périodique n'est réalisé. En situation de catastrophe, les humains ne savent faire correctement que ce à quoi ils ont été entraînés.

Il est important de garder en tête que l'ampleur des moyens de protection nécessaires est inversement proportionnelle aux moyens de prévention mis en œuvre…

Comme nous venons de le voir la sécurité physique ne se base pas sur un mais sur plusieurs éléments tous dépendants les uns des autres. En effet, il n'y a aucun intérêt à avoir une salle serveur très bien sécurisée (digicode, vidéosurveillance, …) si les locaux dans lesquels sont installés les switches sont ouverts au public. Il serait même préférable d'investir moins de moyens dans la salle serveur mais de sécuriser l'ensemble des salles informatiques. Cet exemple nous montre l'importance de sécuriser la globalité du système d'informations et non une seule partie. Il faut aussi être vigilant aux périmètres affectés par la sécurité physique car ce dernier n'est pas figé et évolue sans cesse.

II Sécurité des télécommunications

La sécurité des réseaux reste un des points sensibles puisqu'il ne sert à rien d'avoir un système d'information sécurisé si l'échange entre les ressources est visible et accessible par un quelconque individu !

Nous verrons les différents procédés de sécurisation applicables à un réseau externe puis à un réseau local. Dans les deux cas, nous préciserons quels ont été les choix de la CRAM et tenterons d'argumenter au mieux ces derniers.

II.1 Réseau externe

Nous avons vu précédemment dans la présentation de l'entreprise que la CRAM possède plusieurs sites répartis sur le territoire Français. Comme la plupart des entreprises, ces sites se doivent d'être reliés entre eux afin que les différentes ressources puissent communiquer entre elles et être accessibles par tous. Certains employés ont besoin de pouvoir accéder aux ressources du système d'information de l'extérieur, lorsqu'ils sont en déplacement ou que leur secteur d'activité se situe loin d'une agence ou d'un site « antenne ».

Les différents échanges doivent donc impérativement être sécurisés et ce, afin que des gens mal intentionnés ou même des concurrents, ne puissent pas récupérer des informations confidentielles.

La solution la plus sûre dans la théorie serait de relier les sites entre eux par des liaisons dédiées en passant des câbles d'un site à un autre. Cette solution n'est, bien entendu, pas réalisable

dans la pratique puisque son coût serait exorbitant. De plus, pour un nomade devant se connecter aux 4 coins de la France ou du monde cela ne pourrait être envisageable. Le moins onéreux reste l'utilisation des réseaux existants.

Le plus judicieux est donc de se servir du réseau mondial, à savoir Internet. L'inconvénient de ce réseau est que tout le monde y a accès aussi bien à titre professionnel que privé !

Etant donné qu'Internet est en libre accès, il est nécessaire de sécuriser les échanges.

Pour ce faire, l'utilisation du réseau privé virtuel se révèle judicieux, détaillons maintenant ce dernier :

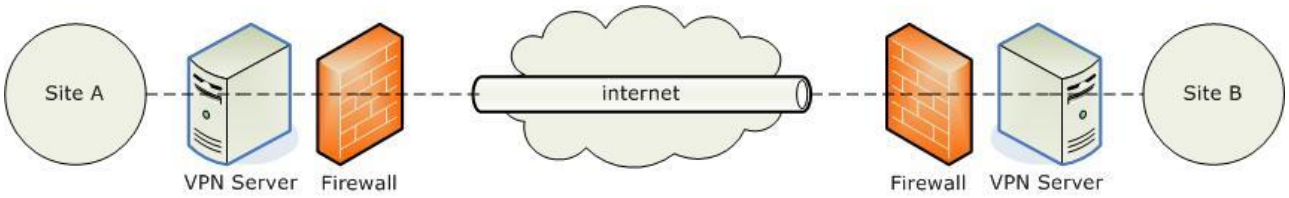


Figure 2 - Principe d'un VPN simple

Plus connu sous le nom de VPN[5], il est apparu avec le «X.25[6]» sur des infrastructures mises en place par les opérateurs. Le X.25 a ensuite été remplacé par le relayage de trames, l'ATM[7] et aujourd'hui le MPLS[8]. Un réseau privé virtuel permet d'étendre le réseau local tout en conservant

---

5 VPN : connexion inter-réseau permettant de relier deux réseaux locaux différents par un protocole de tunnel.

6 X.25 : Le X.25 était un protocole de communication normalisé par commutation de paquets en mode point à point.

7 ATM : traduit en français par « Mode de transfert asynchrone » est un protocole réseau de niveau 2 à commutation de cellules, qui a pour objectif de multiplexer différents flots de données sur un même lien utilisant une technique de multiplexage à répartition dans le temps.

8 MPLS : mécanisme de transport de données basé sur la commutation d'étiquettes ou "labels". La notion d'étiquette provient du fait que les labels sont insérés à l'entrée du réseau MPLS et retirés à sa sortie. Ce protocole permet de fournir un service unifié de transport de données pour les clients en utilisant une technique de commutation de paquets.

son degré de sécurité. Le réseau privé virtuel permet l'interconnexion entre différents réseaux locaux. Cette interconnexion repose sur internet servant de support de transmission ainsi que sur un protocole de « tunnelisation ». Ce protocole, plus connu sous le nom anglais de « tunneling », permet l'encapsulation des données devant être transmises et ce de façon chiffrée afin de satisfaire à la sécurité. Ce réseau, créé artificiellement à l'aide d'internet et d'un protocole de « tunnelisation », est donc appelé « Réseau privé virtuel ».

Le terme privé sert à préciser que seuls les ordinateurs appartenant au réseau local de part et d'autre du VPN peuvent avoir un accès en clair aux données. Le mot « virtuel » précise, lui, le fait que deux réseaux locaux (physiques) sont reliés par une liaison non sécurisée qu'est Internet.

Le principal avantage de la technologie du VPN est son coût réduit par rapport à une liaison physique entre les réseaux locaux dont le prix ne permettrait pas sa réalisation. En effet, le VPN offre une liaison sécurisée où seuls les coûts des équipements ne sont pas négligeables.

Le VPN apporte l'authentification des interlocuteurs, la confidentialité des données avec le chiffrement visant à rendre les données inutilisables par quelqu'un d'autre que le destinataire. Ces éléments sont essentiels dans la transmission des données.

L'inconvénient de la technologie du VPN reste l'utilisation du réseau public (internet) accessible par n'importe quelle personne. Ce qui est donc loin de la qualité de service d'une ligne louée par exemple.

Les principaux protocoles de tunnellisation :

- VPN-SSL

  L'avantage du VPN-SSL est son utilisation via des navigateurs web qui permet de travailler avec un outil familier, ne nécessitant pas de configuration supplémentaire. Cependant, lorsqu'un certificat expire l'utilisateur doit aller manuellement le renouveler. Cela peut poser problème aux utilisateurs novices car sur la majorité des navigateurs web, la consultation des listes de certificats révoqués n'est pas activée par défaut (toute la sécurité de SSL reposant sur ces certificats, ceci pose un grave problème de sécurité). Le client peut aussi télécharger une version modifiée de son navigateur (skins, plugins...), rien ne certifie donc que le navigateur

n'a pas été modifié et que son autorité de certification en soit bien une.

Un autre problème lié à l'utilisation de navigateurs web comme base au VPN est leur spécificité au monde web car par défaut, un navigateur n'interceptera que des communications HTTPS[9] ou éventuellement FTPS[10]. Toutes les communications venant d'autres types d'applications (MS Outlook par exemple) ne sont pas supportées. Ce problème est généralement contourné par l'exécution d'une applet Java[11] dédiée dans le navigateur.

- PPTP[12]

Le protocole PPTP présente l'avantage d'être complètement intégré dans les environnements Windows, ce qui signifie notamment que l'accès au réseau local distant pourra se faire via le système d'authentification de Windows NT : RADIUS[13] incluant sa gestion de droits et de groupes. En revanche, comme beaucoup de produits Microsoft, la sécurité est le point faible du produit.

---

9 HTTPS : L'HyperText Transfer Protocol Secure est la combinaison du HTTP avec une couche de chiffrement comme SSL ou TLS.

10 FTPS : Le File Transfer Protocol Secure est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP, variante du FTP sécurisé avec les protocoles SSL ou TLS.

11 Applet Java : Les applets sont utilisées pour fournir au sein d'applications Web des fonctionnalités interactives qui ne peuvent pas être fournies par le langage HTML.

12 PPTP : est un protocole d'encapsulation PPP sur IP conçu par Microsoft. Il permet de mettre en place des réseaux privés virtuels (VPN) au-dessus d'un réseau public.

13 RADIUS : Un serveur RADIUS dispose d'une base de données comportant les droits utilisateur. Lorsqu'un utilisateur souhaite se connecter à un réseau régi par ce protocole, le NAS (Network Access Server), un intermédiaire entre le réseau et l'utilisateur va interroger le serveur RADIUS et attribuer ses droits à l'utilisateur qui pourra dès lors accéder au réseau.

Ci-dessous quelques exemples :

1. Mauvaise gestion des mots de passe dans les environnements mixtes WINDOWS 95/NT.

2. Faiblesses dans la génération des clés de session (réalisée à partir d'un hachage du mot de passe au lieu d'être entièrement générée au hasard facilitant ainsi les attaques « force brute »).

3. Faiblesses cryptographiques du protocole MsCHAP[14] 1, corrigées dans la version 2 (aucun contrôle n'a été effectué par une entité indépendante).

4. Identification des paquets non implémentés (vulnérabilité aux attaques de type « spoofing »).

- L2TP[15] / IpSec[16]

L'IpSec comporte une plus grande sécurité qui est d'ailleurs plus reconnue que celle utilisée par Microsoft avec le PPTP. D'ailleurs, par défaut le protocole L2TP utilise le protocole IpSec. Cependant, si le serveur distant ne supporte pas le protocole IpSec alors le protocole L2TP pourra utiliser un autre protocole de sécurité. Il est donc indispensable de s'assurer que les équipements d'un VPN L2TP appliquent bien le protocole IpSec.

---

14 MsCHAP : MS-CHAP propose une fonction de hachage propriétaire permettant de stocker un hash intermédiaire du mot de passe sur le serveur. Lorsque la machine distante répond, elle doit préalablement hacher le mot de passe à l'aide de l'algorithme propriétaire.

15 L2TP : Layer 2 Tunneling Protocol signifie protocole de tunnellisation de niveau 2. Il s'agit d'un protocole réseau utilisé pour créer des réseaux privés virtuels.

16 IpSec : L'IpSec est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP.

Les désavantages de l'IpSec :

Il permet seulement d'identifier les machines. Il faut alors prévoir un service d'authentification pour les utilisateurs.

- Offre aucun mécanisme de QoS[17], ce qui limite ses applications (toutes les applications de voix sur IP[18] ou de vidéo sur IP sont impossibles ou seront amenées à être complètement dépendantes des conditions de trafic sur le réseau internet).

- Lourdeur des opérations de cryptage/décryptage (réduit les performances globales des réseaux, et l'achat de périphériques dédiés coûteux devient souvent indispensable).

- MPLS

Les réseaux MPLS représentent aujourd'hui la solution la plus aboutie offrant même de la QoS. La principale contrainte de cette technologie est qu'elle est offerte par les opérateurs eux-mêmes, ce qui pose des problèmes de coûts non négligeables aussi bien pour une petite, que pour une grosse entreprise qui n'auront toutes deux pas les mêmes besoins en bande passante. Cela implique aussi d'être chez un même opérateur pour l'ensemble de son réseau MPLS, ce qui en cas de faillite de la société ou de soucis techniques majeurs, peut se révéler être un véritable handicap…

---

17 QoS : La qualité de service est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau et de garantir de bonnes performances aux applications critiques pour l'organisation.

18 Voix sur IP : La « VoIP » est une technique qui permet de communiquer par la voix, qu'il s'agisse de réseaux privés ou d'Internet. Cette technologie est notamment utilisée pour prendre en charge le service de téléphonie sur IP.

- Comparatif entre le MPLS et l'IpSec

	MPLS	**IpSec**
Étendue	Réduit puisqu'il dépend du fournisseur de service	Large car il repose sur l'accès à Internet
Qualité de service	Des classes permettent d'attribuer des priorités au trafic	L'IpSec se basant sur Internet, la qualité de service ne peut excéder le « best effort »
Coût	Supérieur aux autres réseaux VPN du notamment à la qualité de service	Faible car basé sur le réseau Internet
Sécurité	La sécurité est comparable à celle offerte par les réseaux ATM et Frame Relay[19] existants	Sécurité totale grâce à la combinaison de certificats numériques et de Pki pour l'authentification ainsi qu'à une série d'options de cryptage, triple DES et AES[20] notamment
Applications compatibles	Adapté à tout type d'applications et de logiciels	Inadapté au trafic en temps réel ou à une priorité élevée

19 Frame Relay : Le relayage de trames est un protocole à commutation de paquets situé au niveau de la couche de liaison (niveau 2) du modèle OSI, utilisé pour les échanges intersites (WAN).

20 AES : Advanced Encryption Standard est un algorithme de chiffrement symétrique.

Évolutivité	Grande évolutivité car ne nécessite pas d'interconnexion d'égal à égal entre les sites	Évolution délicate puisque les déploiements exigent une planification soigneuse pour répondre notamment aux problèmes d'interconnexion site à site
Frais de gestion du réseau	Aucun	Traitements supplémentaires pour le cryptage et le décryptage
Vitesse de déploiement	Obligation du fournisseur de déployer un routeur MPLS en bordure de réseau pour permettre l'accès client	Possibilité d'utiliser l'infrastructure du réseau IP existant
Prise en charge par le client	Inutile car le MPLS est une technologie réseau	Logiciels ou matériels client requis

Tableau 1 - Comparatif entre le MPLS et L'IpSec

Réseau externe CRAM :

Les différentes agences et sites de la société sont reliés entre eux par un réseau VPN-MPLS. Concernant les antennes et les sites IP où on ne maîtrise pas la population, des ACL sont mises en place afin de sécuriser les échanges.

Pour les nomades et les clients, un réseau VPN-SSL a été mis en place leur permettant de se connecter depuis l'extérieur. Un portail est accessible depuis Internet afin qu'ils puissent utiliser les différents services fournis par la société. Le portail est celui fourni par les boîtiers CISCO ASA

(deux boîtiers ont été installés afin d'obtenir une redondance), le tout connecté à Internet par l'intermédiaire d'une ligne Altitude Telecom en BLR[21] et d'un secours en SDSL.

II.2 Réseau Local

Le réseau local de la société est un réseau de confiance puisque les personnes se connectant à ce dernier sont des salariés de la société. Toutefois, ne maîtrisant pas toujours la population et de par la taille du site, il faut rester vigilant. Nous sommes en droit de remettre en question l'intégrité des salariés ainsi que leurs intentions, peut-on vraiment leur faire confiance ? De même, des prestataires sont souvent amenés à se connecter au réseau de la société avec des ordinateurs et des intentions non définies. Peuvent-ils récupérer des données sensibles via le réseau local ?

Il y a différentes façons de sécuriser les communications au sein d'un réseau Local, nous allons voir les principaux points et effectuer un état des lieux de la société CRAM.

II.2.1 Les équipements réseau

Intéressons-nous d'abord aux équipements réseaux dont il est primordial de bien connaître le rôle et les fonctions de chacun puisqu'ils ont tous une utilité différente.

II.2.1.1 Hub (diffusion à tout le monde)

Le principe d'un HUB est de retransmettre à tout le monde les informations, ce qui au niveau de la sécurité n'est pas du tout recommandé. Une personne mal intentionnée pourrait alors se servir de ces informations pour accéder à des systèmes sécurisés.

Tous les HUB ont été retirés de la société CRAM y compris ceux dans les bureaux servant à connecter deux postes entre eux.

---

21 BLR : La boucle locale radio est l'ensemble des technologies permettant à un particulier ou une entreprise d'être relié à son opérateur (téléphonie fixe, Internet, télévision...) via les ondes radio.

II.2.1.2 Switch (diffusion à une personne précise)

L'avantage principal du Switch par rapport au HUB est d'adresser à la bonne personne les informations, ce qui est recommandé au niveau de la sécurité d'une part, mais aussi au niveau des performances réseau puisque cela évite d'envoyer des informations dans le vide.

Le réseau de la société CRAM est distribué avec des switchs (1 Gbits/s pour la rocade et 100 Mb/bits pour la diffusion dans les étages).

II.2.1.3 Borne Wifi

Le WiFi est depuis le début critiqué et mis de côté car il n'est pas un exemple dans le domaine de la sécurité. La problématique de ce dernier réside dans le fait qu'il n'y ait pas besoin de se raccorder physiquement à un équipement pour se connecter. Ce point est un réel problème puisque n'importe qui peut accéder à l'équipement et ce malgré le fait qu'il soit dans des locaux sécurisés avec digicode et autre. Avec le Wifi, la couche de sécurité physique se trouve supprimée, bien qu'elle se révèle très importante dans une société.

La sécurité physique concernant le WiFi a été évoquée dans la première partie (I.6).

II.2.1.4 Module CPL[22]

Bien que cette technologie soit très récente, j'ai tenu à l'intégrer afin de voir ses avantages et inconvénients au sein de l'entreprise. En effet, au niveau personnel, cette technologie a un intérêt car très peu de foyers possèdent un câblage en RJ45, alors qu'une entreprise a de manière globale tous ses locaux câblés avec des prises RJ45 permettant d'avoir un réseau Ethernet.

Dans le cas d'une « antenne », cela peut être intéressant pour la CRAM puisque qu'il s'agit souvent d'anciennes maisons ou d'anciens bâtiments publics n'étant pas équipés de câblage RJ45.

---

22 CPL : La communication par courants porteurs en ligne permet de construire un réseau informatique sur le réseau électrique d'une habitation ou d'un bureau, voire d'un quartier ou groupe de bureaux.

II.2.1.5 Pare-Feu physique

Il existe deux types de pare-feu, un pare-feu dit de « logiciel » (nous le verrons par la suite dans la partie « sécurité logicielle ») s'installant directement sur les postes utilisateurs et l'autre pare-feu dit « physique » se présentant soit sous la forme de boîtiers (Appliance[23]), soit d'un ordinateur ou d'un serveur, tous deux comportant une couche logicielle.

Un pare-feu physique permet de protéger un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (internet par exemple). Un pare-feu filtre les paquets de données échangées avec le réseau. Il s'agit ainsi d'une passerelle filtrante comportant au minimum deux interfaces réseau (celle vers le réseau à protéger et celle vers le réseau externe). Il est possible d'installer un système pare-feu sur n'importe quelle machine et avec n'importe quel système, à partir du moment où la machine est suffisamment puissante pour traiter l'ensemble du trafic, que le système est sécurisé et qu'aucun autre service que celui du filtrage de paquets ne fonctionne sur la machine.

La CRAM ne possède plus de pare-feu en interne. Nous avons opté pour un pare-feu directement hébergé chez notre fournisseur d'accès. Après avoir possédé ce type d'équipement, nous avons fait le choix de l'externaliser car ce genre de boîtier est efficace à condition qu'il soit régulièrement administré et maintenu à jour. De plus, il est nécessaire d'investir dans du bon matériel largement dimensionné car cela devient vite un goulot d'étranglement du réseau surtout lorsqu'on active différentes fonctions telles que l'anti-spam[24]…

---

23 Appliance : le serveur appliance est un serveur dédié à une seule tâche. Peu évolutif, il est souvent équipé de Linux et « plug and play ».

24 Spam : Le spam, pourriel ou polluriel est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

II.2.2 La Configuration des équipements réseaux

II.2.2.1 Switch

II.2.2.1.1 Administration

Pour renforcer la sécurité, il a été nécessaire d'administrer les switch de la CRAM afin que n'importe qui ne puisse pas en prendre le contrôle et en détourner l'usage pour ses besoins personnels. Le blocage des ports non utilisés (shutdown) n'a pas été mis en place car lorsqu'une prise n'est pas utilisée, elle n'est pas brassée dans la baie et cette dernière ferme à clef.

II.2.2.1.2 Supervision

La supervision fonctionnant sous Nagios (Open Source) permet de savoir si un des équipements est défaillant, ou encore si quelqu'un a mis hors tension ce dernier ou essaie d'effectuer des opérations non autorisées sur l'équipement. Lorsque la plateforme détecte une anomalie, une alerte est générée et un mail est envoyé automatiquement avec le nom de l'équipement concerné.

II.2.2.1.3 Sécurisation

La sécurisation peut s'effectuer à l'aide de VLAN[25] permettant ainsi de rendre étanches les différentes machines reliées au switch et donc d'éviter des propagations de virus ou un accès sans limite au réseau de la société. Afin de pouvoir mettre en place des VLAN il est nécessaire d'avoir des switches dit de niveau 3 (L3), c'est pourquoi j'ai prévu dans le futur budget de remplacement des équipements l'achat de ces derniers permettant la mise en œuvre d'une telle infrastructure. La mise en place de VLAN au sein de la CRAM permettra d'isoler le réseau des serveurs de celui des utilisateurs et d'isoler aussi les différents services de la CRAM entre eux.

---

25 VLAN : Un réseau local virtuel, communément appelé VLAN (pour Virtual LAN), est un réseau informatique logique indépendant. De nombreux VLAN peuvent coexister sur un même commutateur réseau.

II.2.2.2 Borne Wifi

Nous avons vu précédemment le WiFi dans les parties « Sécurité Physique » et dans « Les équipements réseaux », nous allons maintenant nous intéresser aux paramétrages de cet équipement.

Il existe différentes normes ainsi que différents modes pour les bornes WiFi. Détaillons ces deux points :

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2 Mbit/s (WiFi est un nom commercial, et c'est par abus de langage que l'on parle de « normes » WiFi). Des révisions ont été apportées à la norme originale afin d'améliorer le débit (c'est le cas des normes 802.11a, 802.11b, 802.11g et 802.11n, appelées normes 802.11 physiques) ou de spécifier des détails de sécurité ou d'interopérabilité.

Il existe 4 modes différents :

Le mode infrastructure : c'est un mode de fonctionnement qui permet de connecter entre eux les ordinateurs équipés d'une carte WiFi via un ou plusieurs points d'accès qui agissent comme des concentrateurs (exemple : répéteur ou commutateur en réseau Ethernet). Autrefois, ce mode était essentiellement utilisé en entreprise. Dans ce cas, la mise en place d'un tel réseau oblige de poser à intervalles réguliers des bornes Point d'accès dans la zone qui doit être couverte par le réseau. Les bornes, ainsi que les machines, doivent être configurées avec le même nom de réseau (SSID[26]) afin de pouvoir communiquer. L'avantage de ce mode, en entreprise, est de garantir un passage obligé par le point d'accès. Il est donc possible de vérifier qui accède au réseau. Actuellement les FAI, les boutiques spécialisées et les grandes surfaces fournissent aux particuliers des routeurs sans fil qui fonctionnent en mode infrastructure et sont faciles à configurer.

Le mode « Ad Hoc » : ce mode permet de connecter directement les ordinateurs équipés d'une carte WiFi, sans utiliser un matériel tiers comme un point d'accès. Ce mode est idéal pour

---

26 SSID : Le SSID est le nom d'un réseau sans fil selon la norme IEEE 802.11. En mode infrastructure, le SSID sert à identifier le Hotspot tandis qu'en mode Ad Hoc, il permet d'identifier la connexion.

interconnecter rapidement des machines entre elles sans matériel supplémentaire (exemple : échange de fichiers entre portables dans un train, dans la rue, au café…). La mise en place d'un tel réseau nécessite de configurer les machines en mode Ad Hoc (au lieu du mode Infrastructure), de sélectionner un canal (fréquence), de définir un nom de réseau (SSID) communs à tous et si nécessaire une clé de chiffrement. L'avantage de ce mode est de s'affranchir de matériels tiers, c'est-à-dire de pouvoir fonctionner en l'absence de points d'accès. Des protocoles de routage dynamiques rendent envisageable l'utilisation de réseaux maillés autonomes dans lesquels la portée ne se limite pas à ses voisins (tous les participants jouent le rôle du routeur).

Le mode pont « bridge » : Un point d'accès en mode pont sert à connecter un ou plusieurs points d'accès entre eux pour étendre un réseau filaire, par exemple entre deux bâtiments. La connexion se fait au niveau de la couche 2 OSI. Un point d'accès doit fonctionner en mode racine « root bridge » (généralement celui qui distribue l'accès Internet) et les autres s'y connectent en mode « bridge » pour ensuite retransmettre la connexion sur leur interface Ethernet. Chacun de ces points d'accès peut éventuellement être configuré en mode pont avec connexion de clients. Ce mode permet de faire un pont tout en accueillant des clients comme dans le mode Infrastructure.

Le mode répéteur « range-extender » : Un point d'accès en mode répéteur permet de répéter un signal WiFi plus loin (par exemple pour atteindre un fond de couloir en L). Contrairement au mode pont, l'interface Ethernet reste inactive. Chaque « saut » supplémentaire augmente cependant le temps de latence de la connexion. Un répéteur a également tendance à diminuer le débit de la connexion. En effet, son antenne doit recevoir un signal et le retransmettre par la même interface, ce qui en théorie divise le débit par deux.

Les bornes WiFi de l'entreprise CRAM fonctionnent en mode infrastructure.

II.2.2.1.1 Administration

Tout comme pour les switches, il est nécessaire d'administrer les équipements réseaux afin que n'importe qui ne puisse pas en prendre le contrôle.

II.2.2.1.2 Supervision

Comme vu précédemment pour les switches, les bornes WiFi sont supervisées, ce qui est indispensable puisqu'elles sont souvent placées dans des endroits « normalement sécurisés » et souvent isolés.

II.2.2.2 Sécurisation

La sécurisation peut être non seulement effectuée avec une clef WEP, WPA, WPA2 mais aussi par filtrage d'adresses MAC.

Voyons plus en détails ces deux types de sécurité :

II.2.2.2.1 Sécurisation par clef

Wired Equivalent Privacy (WEP) :

2001 : Publication d'une analyse permettant de révéler qu'une attaque passive permet de retrouver la clé WEP après une écoute clandestine du réseau pendant quelques heures. Des outils automatisés ont été publiés, ce qui rend maintenant possible la réalisation de ce type d'attaque avec un ordinateur personnel et des logiciels gratuits.

2003 : Série d'imperfections détectées dans le WEP dont deux faiblesses générales :

- le WEP est optionnel, de nombreuses installations ne l'ont donc jamais activé.
- le WEP n'inclut pas un protocole de gestion des clés, le mécanisme repose sur une unique clé partagée entre tous les utilisateurs.

2005 : Le FBI procède à la démonstration de la possibilité de pénétrer en 3 minutes un réseau protégé par du WEP et ce en utilisant des outils disponibles publiquement (par exemple grâce au logiciel « Aircrack-ng » disponible sous Linux et Windows).

2006 : Il est maintenant possible de pénétrer les réseaux protégés par une clé WEP en quelques secondes seulement ! Il faut pour cela tirer parti de la fragmentation des paquets pour accélérer le cassage de la clé. Les détails de cette technique sont expliqués dans l'article en anglais "A final nail in WEP's Coffin" (Un dernier clou dans le cercueil du WEP).

WiFi Protected Access (WPA et WPA2) :

Pour pallier aux nombreuses faiblesses détectées dans le WEP, le WPA fut créé en 2000, permettant ainsi de sécuriser les réseaux sans fils de type WiFi. Il a été conçu pour fonctionner avec toutes les cartes WiFi après mise à jour de leur micro-logiciel, mais pas obligatoirement avec la première génération des points d'accès WiFi.

Le WPA2, son successeur, prend en charge le mécanisme CCMP, lequel s'appuie sur AES. Le protocole CCMP est considéré comme complètement sécurisé. En mai 2004, le NIST (National Institute of Standards and Technology) l'a approuvé. Il est pris en charge depuis 2005 par Windows XP et sur tous les Macintosh comportant une carte « AirPort Extreme ».

Les WPA et WPA2 fournissent une bonne sécurité à condition de respecter les deux points suivants :

- l'utilisateur doit activer WPA ou WPA2 en remplacement du WEP qui reste le choix de chiffrement par défaut sur la plupart des équipements.
- lorsque le mode « WPA personnel » (WPA-Personal) est utilisé, une phrase secrète (plus longue que les classiques mots de passe de 6 à 8 caractères habituels) est nécessaire afin d'assurer une sécurité complète.

Depuis l'adoption du standard 802.11i (WPA2), on peut raisonnablement parler d'accès réseaux sans-fils sécurisé. Cependant, en l'absence de WPA2, il est possible d'utiliser un tunnel chiffré (VPN) comme vu précédemment afin de se raccorder au réseau de son entreprise sans risque d'écoute ou de modification.

II.2.2.2.2 Sécurisation par filtrage d'adresse MAC

Le filtrage par adresse MAC permet de contrôler l'accès au réseau informatique en se basant sur l'adresse MAC physique de la carte connectée au réseau. Une adresse MAC physique est une adresse unique qui est assignée à chaque carte réseau, commutateur (switch), routeur, caméra IP, etc. L'adresse MAC n'étant pas conservée après le passage par un routeur, cette technique n'est valable qu'au sein d'un réseau local.

Il faut toutefois être vigilant car contrairement aux idées reçues, l'usurpation d'adresse MAC est très facile à réaliser. Il existe une technique appelée le « MAC Spoofing » qui consiste à usurper l'adresse MAC d'une machine autorisée. (Ne pas confondre avec l'« ARP Spoofing[27] » qui consiste à détourner un flux vers une nouvelle adresse MAC.)

Il est aussi important de distinguer l'adresse MAC physique de l'adresse MAC logicielle. Une adresse physique est difficile à modifier, mais celle-ci sert uniquement d'adresse MAC par défaut pour établir les connexions réseaux. C'est en réalité le système d'exploitation qui choisit l'adresse MAC avec laquelle il désire communiquer. Par exemple, sous Windows le changement de l'adresse MAC se fait en modifiant manuellement une clé de registre ou voir également dans les propriétés avancées de la carte réseau (uniquement avec certains pilotes).

Une bonne politique de sécurité ne doit donc pas reposer uniquement sur l'adresse MAC.

Le type de clef de sécurité utilisé par la CRAM est le WPA2. Le filtrage d'adresse MAC a été désactivé car la gestion des adresses MAC prendrait trop de temps (ajout et suppression d'adresse MAC pour les prestataires, les nouveaux ordinateurs portables, les smartphones, etc.). La diffusion du SSID a été désactivée, ce qui n'empêchera pas une personne experte de trouver le réseau WiFi mais réduira les tentatives de connexion par un utilisateur lambda.

II.2.2.3 Routeur

Dans une entreprise, les routeurs appartiennent la plupart du temps au FAI et sont donc configurés par ces derniers. Toutefois, il est intéressant de voir quelques éléments de configuration pouvant renforcer la sécurité.

---

27 ARP Spoofing : appelé aussi ARP poisoning, est une technique utilisée en informatique pour attaquer tout réseau local utilisant le protocole de résolution d'adresse ARP, les cas les plus répandus étant les réseaux Ethernet et Wi-Fi. Cette technique peut permettre à l'attaquant de détourner des flux de communication transitant sur un réseau local commuté, lui permettant de les écouter, de les corrompre, mais aussi d'usurper une adresse IP ou de bloquer du trafic. En détournant le flux, l'attaquant peut ainsi voir les données qui transitent en clair entre les deux machines.

II.2.2.3.1 Access Control List (ACL)

Les access control list permettent d'appliquer des filtres sur les interfaces et d'indiquer au routeur les paquets qu'il doit accepter et ceux qu'il doit refuser.

Les ACL sont lus par le routeur de manière séquentielle. C'est la première instruction rencontrée par le paquet en question qui fait foi, et les instructions suivantes ne sont pas utilisées.

Attention, il est très important qu'une ACL non finie se termine toujours par « *deny any* » afin de refuser tous les paquets qui ne répondent à aucune règle de l'ACL et ainsi couvrir tous les cas possibles.

Il existe deux types d'ACL, les standards et les étendues. L'ACL standard ne prend en compte que l'adresse IP source alors qu'une ACL étendue prend en compte plus de critères, comme l'IP destination et les ports utilisés.

Les ACL au sein de la CRAM sont positionnées sur les routeurs du fournisseur d'accès ce qui permet d'empêcher les connexions non autorisées provenant des sites distants (antenne, site IP) où nous ne maîtrisons pas toujours les utilisateurs (locaux fréquentés par des pompiers et autres). Les ACL mises en place sont de type étendu puisque le filtrage se fait par rapport à l'adresse IP et le port de connexion de la ressource.

II.2.2.3.2 Qualité de service

La qualité de service (QdS) ou Quality of service (QoS) est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau et de garantir de bonnes performances aux applications critiques pour la société. La qualité de service permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par rapport aux applications qui par exemple suivent les protocoles utilisés.

En fonction du type de service envisagé, la qualité pourra résider dans le débit (téléchargement ou diffusion vidéo), le délai (pour les applications interactives ou la téléphonie), la disponibilité (accès à un service partagé) ou encore le taux de pertes de paquets (pertes sans influence pour de la voix ou de la vidéo, mais critiques pour le téléchargement).

Une QdS a été mise en place à la CRAM sur les routeurs du fournisseur d'accès permettant ainsi de prioriser les flux des applications les plus critiques dans la société tels que les échanges SQL. Cette fonctionnalité permet aussi lorsque la bande passante est saturée d'éviter de rendre indisponibles des applications critiques pour la société.

II.2.2.3.2 Network address translation (NAT)

Un routeur implémentant du NAT permet de changer le plan d'adressage interne et d'utiliser des adresses non uniques (utilisées ailleurs dans le monde) et non routables sur Internet. On parle aussi d'adresses *publiques* (uniques au monde) et *privées* (uniques seulement dans le réseau privé). Un des buts du NAT est de rendre les adresses privées invisibles depuis Internet. Il est alors possible d'assigner que quelques adresses à l'ensemble des adresses externes du NAT, sachant que les imprimantes par exemple n'ont pas besoin de communiquer avec l'extérieur de façon permanente (donc leurs adresses n'ont pas besoin d'être traduites).

Le NAT apporte un bénéfice en termes de sécurité puisque les adresses internes se retrouvent dissimulées. La sécurité des équipements derrière un NAT n'est cependant pas supérieure à celle qu'un pare-feu à états peut fournir. Ce dernier comporte tout de même une complexité additionnelle sur le fonctionnement des applications, notamment pour des applications du réseau pouvant avoir quelques difficultés à fonctionner.

J'ai utilisé le NAT au sein de la CRAM afin de pouvoir se connecter et prendre la main sur les ordinateurs des sites distants. J'ai dû installer un routeur en plus de celui fourni par notre fournisseur d'accès sur chaque site distant afin d'avoir la main sur l'équipement (ce qui n'était pas possible avec l'équipement du fournisseur d'accès). J'ai donc configuré un sous-réseau avec un adressage différent de celui fourni par le routeur du FAI. J'ai ensuite associé des ports à des adresses IP « locales » permettant ainsi de se connecter à distance sur la machine souhaitée en indiquant l'adresse IP du routeur du FAI suivie du port correspondant à la machine locale à laquelle on souhaite accéder. Ce sous-réseau permet aussi d'autoriser les ordinateurs du sous-réseau à sortir ou non sur internet et à se connecter uniquement aux ressources que l'on définit.

La sécurité des télécommunications consiste à protéger les échanges entre les ressources puisqu'il n'y a aucun intérêt à vouloir sécuriser des locaux si les liaisons entre ces derniers ne le

sont pas ! Nous avons détaillé les différents types de technologies permettant une bonne sécurisation des réseaux externes dont les équipements sont dans la majorité des cas gérés par les fournisseurs d'accès. Contrairement aux réseaux externes, les réseaux locaux sont bien plus complexes à protéger puisque l'ensemble des équipements doit être choisi, configuré et supervisé convenablement. En effet, il est inutile, d'investir dans des équipements coûteux s'ils ne sont pas configurés correctement. De même, pour obtenir un réseau sûr, il est indispensable qu'il soit surveillé par des personnes compétentes. La sécurité des télécommunications peut donc se révéler coûteuse pour l'entreprise, mais indispensable si cette dernière ne souhaite pas subir des pertes de données et donc d'argent.

III Sécurité Logique

Les vulnérabilités logicielles peuvent mettre en danger les processus métier et les données clés d'une société. Il est nécessaire de mettre en œuvre des stratégies de sécurité logicielle pour toutes les applications appelées à jouer un rôle important en termes de confidentialité, d´intégrité ou de disponibilité. De nombreux systèmes censés contrôler la sécurité du réseau partent du principe que la couche logicielle est sécurisée, au lieu de protéger réellement le système contre les vulnérabilités logicielles.

Aujourd'hui, le marché souterrain est bien ancré et mature. Monnayer des données volées n'a jamais été aussi 'accessible'. Autrement dit, les pirates qui veulent des données n'hésitent plus à investir du temps, de l'énergie et de l'argent pour élaborer des stratégies d'attaques visant des cibles très précises.

III.1 Logiciel malveillant

Un logiciel malveillant (malware en anglais) dont le nom est la contraction de « malicious » (malveillant) et de « software » (logiciel) désigne un programme qui a pour seul but de nuire à un système informatique et qui agit sans le consentement de l'utilisateur. Il est important de faire la distinction entre les malwares[28] et les virus. Les malwares englobent en réalité différentes catégories comme les virus, les vers, les chevaux de Troie ainsi que d'autres menaces. Les virus ont

28 Malwares : Un logiciel malveillant est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté. De nos jours, le terme virus est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les malwares englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces.

été la catégorie la plus répandue durant plusieurs années jusqu'à l'arrivée du cheval de Troie en 2005.

Les logiciels malveillants sont classés en fonction de leur mécanisme de fonctionnement. On distingue 3 types de mécanisme différents, à savoir :

- Le mécanisme de propagation : un ver qui se propage sur un réseau informatique en exploitant une faille applicative ou humaine.
- Le mécanisme de déclenchement : une bombe logique comme celle surnommée « vendredi 13 » se déclenchant lorsqu'un évènement survient.
- La charge utile : le virus « Tchernobyl » qui tente de supprimer des parties importantes du BIOS bloquant ainsi le démarrage de l'ordinateur infecté.

La différence entre les classes n'étant pas toujours évidente à définir, la classification ne peut donc pas être parfaite. Toutefois, cette classification est aujourd'hui la classification standard et la plus couramment adoptée dans les milieux internationaux de la sécurité informatique.

Une autre méthode de classification, proposée par J.Rutkowska, distingue les malwares en fonction de leur mode de corruption du noyau du système d'exploitation : les malwares ne touchant pas au noyau (applications, micro logiciel), ceux corrompant des éléments fixes comme du code, ceux corrompant des éléments dynamiques tels que des données et la catégorie de malwares se plaçant au-dessus du noyau (hyperviseurs).

Avant d'entamer la partie suivante, regardons le résumé des logiciels malveillants et leurs menaces :

Virus	de boot – de fichier – macrovirus – de script
Vers	de réseau – de courrier électronique – Internet - IRC[29]
Chevaux de troie	Porte dérobée – dropper – notificateur – logiciel espion
Autres menaces	Exploit – publiciel – rogue – composeur – enregistreur de frappe – rootkit – canular - pharming

Tableau 2 - Logiciels malveillants et leurs menaces

III.1.1 Les différentes menaces

Il est aujourd'hui difficile de différencier les types de menaces puisqu'un malware est souvent composé de plusieurs types de malwares différents. En effet, un ver peut par exemple intégrer des fonctions propres au cheval de Troie. Cette partie est très théorique, mais toutefois importante afin de prendre conscience des différentes menaces existantes et d'avoir une vue d'ensemble des failles ou méthodes utilisées.

III.1.1.1 Les virus classiques

Les virus sont créés afin de se répliquer et de se propager sur d'autres ordinateurs en s'insérant dans des documents, programmes, etc. Il existe différents types de virus : les virus de secteur d'amorçage, de fichier, de macro et de script. Certains d'entre eux intègrent des rootkits (le but d'un rootkit est d'obtenir et de pérenniser un accès à un ordinateur le plus furtivement possible). Ces derniers peuvent se révéler particulièrement dangereux et endommager de manière plus ou moins importante les machines infectées.

Un virus se répand à l'aide des réseaux informatiques, des cédéroms, des clefs USB, etc.

---

29 IRC : Internet Relay Chat est un protocole de communication textuelle sur Internet. Il sert à la communication instantanée principalement sous la forme de discussions en groupe par l'intermédiaire de canaux de discussions, mais peut aussi être utilisé pour de la communication de un à un. Il peut par ailleurs être utilisé pour faire du transfert de fichiers.

Il est important de distinguer les virus des vers qui sont eux, des programmes capables de se propager et de se dupliquer par leurs propres moyens mais sans contamination de programmes. Il faut bien distinguer les virus des logiciels malveillants et ne pas utiliser le mot virus pour décrire toute forme de logiciel malveillant.

La majorité des virus est créée pour s'attaquer à l'environnement Windows (système d'exploitation le plus répandu sur la planète). Toutefois il existe aussi des virus pour les systèmes d'exploitation de type Unix/Linux/Apple, mais ils se font rares et aucune épidémie ne peut être comparable à celles des virus Windows. Il existe tout de même des systèmes moins touchés comme FreeBSD axant son développement sur la sécurité, Netware ou encore OS/2 bien trop rares pour apporter une quelconque notoriété à un développeur de virus.

De fausses alertes sont souvent propagées via courriel amenant parfois des utilisateurs novices à détruire des éléments du système d'exploitation complètement sains et encombrant par la même occasion les systèmes de messageries !

Il peut être intéressant d'identifier quelques types de virus :

- Les virus de fichier : il est dans la plupart des cas écrit en assembleur et s'intègre dans un programme normal. Il va ensuite être activé à chaque fois que l'utilisateur exécute le programme « infecté ». Une fois activé, le virus va aller s'intégrer dans d'autres programmes exécutables.

  Les virus de fichier peuvent être répartis en plusieurs catégories, ceux qui infectent les fichiers exécutables comme nous avons vu auparavant, ceux qui créent ou dupliquent des fichiers (virus compagnons), ceux qui créent leur propre copie dans divers répertoires ou encore ceux qui utilisent les caractéristiques des systèmes de fichiers (virus de fichiers système).

  Les virus de fichiers peuvent aussi contenir une « charge utile » qui permettra l'exécution d'une action qui sera déclenchée plus tard ou lors d'un évènement particulier. Cette action peut se révéler critique avec la détérioration de certaines fonctions du système d'exploitation, la détérioration de certains fichiers ou encore la destruction complète de toutes les données de l'ordinateur. Un virus peut aussi être

anodin et ne provoquer que l'envoi de messages. On qualifie de « bombe logique » un virus supprimant des fichiers et représentant une menace pour le système.

- Le virus boot : Il s'installe dans un des secteurs de boot d'un périphérique de démarrage comme un disque dur, une disquette, etc. Il remplace le programme de démarrage (bootloader) en le copiant à un autre endroit. Dans le cas où le disque ne possède pas de programme de démarrage, le virus crée le sien mais ne va en aucun cas modifier un programme comme pourrait le faire un virus classique. En remplaçant un programme de démarrage, il agit comme un virus « prepender » (qui s'insère au début). Ce type de virus était beaucoup présent dans les années 1990 lorsque les disquettes étaient utilisées. Il est techniquement possible d'en programmer pour les CD, les mémoires USB, mais aucun n'a été recensé aujourd'hui.

- Le macrovirus : Beaucoup de logiciels de comptabilité, d'édition, de traitement de textes et autres utilisent des macros servant à automatiser les tâches répétitives. Ce sont, la plupart du temps, des macros relativement complexes contenant une multitude de commandes. Ce type de virus est programmé en langage macro et se propage en exploitant les caractéristiques du langage de programmation des macros. Il infecte par conséquent tous les programmes intégrant ces macros.

  On peut prendre l'exemple d'un macrovirus utilisant Visual Basic for Application (VBA) de Microsoft qui permet notamment de créer des macros pour s'attaquer uniquement à la suite « Microsoft Office » (Word, Excel, …). Le « normal.dot » peut alors se trouver infecté provoquant ainsi à chaque lancement de Word l'exécution du virus !

- Les virus script : les virus de script peuvent être assimilés à des virus de fichier. Ils sont dans la plupart des cas programmés en VBS, JavaScript, Bat, PHP, etc. Ils agissent en infectant d'autres scripts tels que les fichiers de commande, type service Windows ainsi que Linux. Ils peuvent aussi faire partie d'un virus à plusieurs composants. Ils sont, dans certains cas, capables d'infecter d'autres formats tels que le HTML, si toutefois ce format permet l'exécution de scripts.

Si on prend le cas des virus de type batch apparus à l'époque où MS-DOS était en vogue, ce sont des virus « primitifs » mais pour autant capables de se reproduire et d'infecter d'autres fichiers batch. Bien qu'ils soient lents et qu'ils aient un pouvoir infectant très limité, certains programmeurs ont été jusqu'à créer des virus batch cryptés et polymorphes, ce qui pour l'époque était une véritable prouesse technique tant le langage batch est simple et primitif.

Les virus-vers sont des virus classiques avec un programme hôte qui s'apparente aux vers (en anglais « worm ») sur les points suivants :

- Leur mode de propagation est lié au réseau.
- Leur action est discrète et non-destructrice pour les utilisateurs de la machine infectée.
- Ils poursuivent des objectifs larges, tels que l'attaque par DoS (*Denial of Service*) d'un serveur par des milliers de machines infectées se connectant simultanément.

III.1.1.2 Les vers de réseau

Un ver n'a nullement besoin d'un programme hôte pour se reproduire puisqu'il se sert des différentes ressources de l'ordinateur sur lequel il est hébergé afin d'assurer sa propre reproduction. Ils sont en effet capables d'envoyer une copie d'eux même à d'autres machines. On peut aussi les classer selon leur technique de propagation :

- Les vers de courrier électronique.
- Internet.
- IRC.
- Les vers réseaux.
- Les partages de fichiers.

La reproduction n'est pas l'unique objectif du ver. Il se veut aussi malfaisant par les actions suivantes :

- Il espionne l'ordinateur sur lequel il se trouve.
- Il offre une porte dérobée à d'éventuels pirates informatiques.
- Il détruit les données sur l'ordinateur infecté.
- Il envoi des requêtes vers un serveur internet dans le but de provoquer un déni de service.
- Ainsi que d'autres dégâts.

Son activité provoque bien souvent des effets secondaires pouvant aller du ralentissement de la machine infectée ou du réseau jusqu'au « plantage » de services ou du système d'exploitation de la machine infectée.

Les vers peuvent être programmés en C, C++, Delphi, assembleur ou tout autre langage de programmation. Il existe aussi des vers écrits sous forme de scripts pouvant être intégrés dans un courriel ou sur une page HTML. L'activation de ces vers se fait par une action de l'utilisateur qui croit accéder à des informations lui étant destinées.

Dans la plupart des cas, les vers utilisent des failles de logiciels afin de se propager. Ces failles sont habituellement corrigées par les éditeurs de logiciels dès que les vers apparaissent. Il est, de ce fait, nécessaire de maintenir à jour les logiciels afin de réduire la probabilité d'infection par des vers informatiques.

Certains vers ont connu une expansion fulgurante comme par exemple le ver « I Love You » qui a d'ailleurs fait beaucoup parler de lui.

III.1.1.3 Les chevaux de Troie

Les chevaux de Troie (Trojan horse), d'apparence inoffensifs, sont conçus afin d'exécuter des actions à l'insu de l'utilisateur. Ils utilisent en général les droits de leur environnement afin de diffuser, détourner ou détruire des données. Ils permettent aussi l'ouverture d'une porte dérobée

permettant ainsi à un pirate informatique de prendre la main à distance et par la même occasion de contrôler l'ordinateur infecté. Ils sont programmés de façon à être installés de manière invisible dans le but de corrompre l'ordinateur hôte.

La différence entre les virus et les vers, est que ces derniers ne se répliquent pas.

Pour qu'une machine soit infectée, il faut en général qu'un fichier contaminé soit ouvert. Ce fichier peut se présenter sous la forme d'un jeu (test QI, jeu à but lucratif) ou sous la forme d'une amélioration d'un logiciel (MSN, Safari, Photoshop, etc.). Les mises à jour sont alors proposées par courriel. Il est important de savoir qu'une entreprise de micro-informatique ne proposera jamais de mise à jour de ses programmes pas courriel.

Les différents symptômes d'une infection peuvent être :

- Une activité anormale du modem, de la carte réseau ou encore du disque dur (lorsqu'il n'y a pas d'activité de la part de l'utilisateur, des données sont chargées).
- Une réaction curieuse de la souris.
- Une ouverture non demandée de certains programmes.
- Des plantages répétés.

Afin de supprimer ce genre de programme malveillant, on peut utiliser un antivirus, un pare-feu ou encore un anti-malware. Il peut aussi être nécessaire de démarrer en mode sans échec, voir même sur un autre système d'exploitation.

On peut classer les chevaux de Troie par rapport aux actions qu'ils exécutent sur les machines attaquées.

Voyons maintenant les différents types de chevaux de Troie :

III.1.1.3.1 Les chevaux de Troie génériques

Ces chevaux de Troie endommagent les ordinateurs des victimes, menacent l'intégrité des données et peuvent aussi nuire au fonctionnement de l'ordinateur.

III.1.1.3.2 Les portes dérobées

Ces chevaux de Troie sont reconnus pour être les plus dangereux et les plus répandus à l'heure actuelle. Ils s'apparentent à un logiciel d'administration comme celui utilisé par les administrateurs système. Ce type d'outil permet donc de prendre le contrôle à distance d'un ordinateur infecté via un LAN ou INTERNET. La seule différence avec les outils d'administration licite réside dans le fait que les portes dérobées s'installent et s'exécutent sans le consentement de l'utilisateur.

La porte dérobée installée surveille le système local à l'insu de l'utilisateur et n'apparait pas forcément dans le journal des applications actives. Parmi les différentes fonctions d'une porte dérobée, on peut citer :

- Le redémarrage de la machine.
- L'affichage de messages.
- L'envoi ainsi que la réception de fichiers.
- Le lancement et la suppression de fichiers ou de données.

Cela permet donc aux auteurs des « virus » de détecter et de télécharger des informations confidentielles. Ils peuvent aussi exécuter du code malicieux, intégrer des ordinateurs dans des réseaux bot, etc. La porte dérobée regroupe la majorité des autres types de chevaux de Troie en un seul. Il existe certaines variantes agissant comme des vers à l'exception que leur propagation ne se fait pas de manière permanente, mais uniquement lorsque le « maître » en donne l'ordre par l'intermédiaire d'une commande.

III.1.1.3.3 Les chevaux de Troie PSW

L'objectif de ces chevaux de Troie est de voler les mots de passe système, le plus souvent en recherchant des fichiers système pouvant contenir des informations confidentielles. On retrouve par exemple les mots de passe, les numéros de téléphone d'accès à internet, etc. Ce ne sont pas les seules données volées puisque les détails du système (système d'exploitation, mémoire, espace disque), les adresses IP, les détails d'enregistrement ou encore les mots de passe pour les jeux en

ligne le sont aussi. Les différentes informations collectées sont envoyées à une adresse électronique (celle du « maître » ou utilisateur du programme illicite) elle-même codée dans le cheval de Troie.

III.1.1.3.4 Les chevaux de Troie cliqueurs

Ils permettent de rediriger les ordinateurs infectés vers des sites Web ou d'autres ressources spécifiques, en envoyant des commandes au navigateur ou en remplaçant les fichiers système dans lesquels sont stockées les URL « standard » (fichier Hôte dans Windows).

L'objectif étant dans la plupart des cas :

- d'augmenter le nombre de visites sur un site particulier (publicitaire par exemple).
- d'organiser une attaque d'un service sur un serveur ou d'un site spécifique en utilisant la méthode du déni de service.
- de conduire l'ordinateur victime vers une ressource infectée où il sera attaqué avec d'autres programmes malveillants (Chevaux de Troie, Virus…).

III.1.1.3.5 Les chevaux de Troie téléchargeurs

Ce type de cheval de Troie va commencer par télécharger des programmes malveillants ou des logiciels publicitaires. Il va ensuite utiliser une liste codée dans le cheval de Troie, soit depuis un site web spécifique ou depuis une ressource internet quelconque. Il peut ensuite les installer immédiatement comme ultérieurement sur l'ordinateur de la victime. Toutes ces actions, se faisant bien évidemment sans le consentement de l'utilisateur.

III.1.1.3.6 Les chevaux de Troie droppers

Ils rendent possible l'installation d'autres programmes malveillants à l'insu de l'utilisateur. Ils installent leur charge utile à l'intérieur d'un fichier d'archive ou même au sein du système d'exploitation. Le programme malveillant est déposé dans un endroit spécifié sur le disque local où il va ensuite être exécuté.

Ci-dessous la structure des droppers :

Fichier principal contient la charge utile du dropper
Fichier 1 première charge utile **Fichier 2** deuxième charge utile
... autant de fichiers que l'auteur souhaite

Tableau 3 - Structure des droppers

La charge utile renferme la plupart du temps des chevaux de Troie et au moins un canular (jeux, images, blague, etc.). Le canular a pour seul objectif de masquer la partie dangereuse de la charge utile en faisant croire à l'utilisateur que le dropper est inoffensif. L'installation et l'exécution des fichiers de la charge utile (ou bombe logique) s'effectuent par l'intermédiaire d'un code contenu dans le dropper.

Les pirates informatiques utilisent ce genre de programme afin d'installer de façon masquée d'autres chevaux de Troie ou virus et de « jouer un tour » aux logiciels antivirus qui ne sont pas en mesure d'analyser tous les composants.

III.1.1.3.7 Chevaux de Troie proxy[30]

Ils offrent un accès anonyme à internet en se servant de l'ordinateur infecté comme d'un serveur proxy. Ce type de cheval de Troie est notamment très recherché par les spammeurs par exemple pour la diffusion massive de messages électroniques. Ils sont très souvent inclus dans les virus, ce qui permet aux auteurs de ces derniers de pouvoir vendre le réseau de machines infectées aux spammeurs.

III.1.1.3.8 Chevaux de Troie espions

Ils permettent d'enregistrer l'activité de l'utilisateur et de la transmettre à un maître. Ces chevaux de Troie recueillent les informations en enregistrant la frappe du clavier (KeyLogger), et en capturant l'écran, les journaux des applications actives ainsi toutes autres actions des utilisateurs. Ils sont dans la plupart des cas utilisés afin de dérober des informations à caractère financier et ainsi d'alimenter les fraudes en ligne.

III.1.1.3.9 Chevaux de Troie notificateurs

Leur but est d'enregistrer le maximum d'informations sur la machine infectée comme l'adresse IP de la machine, les numéros de ports ouverts, les adresses de courrier électronique, etc. Toutes ces informations recueillies sont ensuite envoyées par mail ou par un autre type de support. Les notificateurs sont souvent repris dans les ensembles de chevaux de Troie afin de permettent au maître de savoir si l'installation s'est bien déroulée sur l'ordinateur de la victime.

III.1.1.3.10 Bombes d'archive

Elles sont représentées sous la forme de fichiers archivés, codés dans le but de saboter l'utilitaire de décompression lorsque ce dernier essaie d'ouvrir le fichier infecté. Une fois la « bombe » déclenchée, cela provoquera le ralentissement ou le plantage de la machine infectée. Le

---

30 Proxy : Un proxy, parfois appelé mandataire, est un composant logiciel qui se place entre deux autres pour faciliter ou surveiller leurs échanges. Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet.

disque de la machine peut aussi se retrouver noyé par des données inutiles. Ce type de chevaux de Troie est particulièrement dangereux lorsque les données sont traitées au départ comme cela peut être le cas sur un serveur, ce qui peut provoquer son plantage.

Trois types de bombes existent :

- Celle à en-tête incorrecte dans l'archive ou comportant des données corrompues qui peuvent entraîner le plantage de l'utilitaire de décompressions lorsque l'archive est ouverte et décompressée.
- Celle, dite de données répétées, représentée sous la forme d'un fichier lourd qui contient des données de petite taille se répétant. Un fichier de 5Mo sera ramené à une taille de 200Ko en cas de compression au format RAR[31] et de 480Ko au format ZIP[32]).
- Celle de séries de fichiers identiques au sein de l'archive sans que cela n'ait de répercussions sur la taille de l'archive elle-même (On peut compacter 10100 fichiers identiques dans un fichier de type RAR de 30Ko ou dans un fichier de type ZIP de 230Ko).

III.1.1.4 Les autres logiciels malveillants

De nombreuses autres menaces existent mais elles ne sont pas forcément dangereuses en soit puisqu'elles ne mettent pas directement en péril les ordinateurs. Elles servent tout de même à créer des virus, chevaux de Troie ou encore à réaliser des activités illégales telles que les attaques par déni de service (DoS) ou encore à pénétrer au sein d'ordinateurs d'autres personnes (Outils DoS et DDoS, Outils d'attaque et exploits, inondeurs,…).

---

31 RAR : RAR est un format de fichier permettant la compression de données. Ce format a été inventé par le russe Eugene Roshal (Roshal ARchive).

32 ZIP : ZIP est un format de fichier permettant l'archivage et la compression de données sans perte de qualité. On peut donc le comparer à la combinaison de tar (archivage) et gzip (compression) dans le cadre d'une archive compressée .tgz.

Dressons une liste de ces différentes menaces :

III.1.1.4.1 Outils DoS et DDoS

Ces outils visent les serveurs Web en envoyant une multitude de requêtes à l'un d'entre eux. Cette méthode cause l'arrêt du serveur si ce dernier n'est pas soutenu par d'autres ressources additionnelles. On pourra alors qualifier de déni de service cet arrêt provoqué par l'ensemble des requêtes. C'est donc pour cette raison que ce type d'attaque s'appelle « attaque par déni de service » (DoS). On peut aussi retrouver ce type de procédure DoS dans la charge utile de certains vers.

Contrairement au programme DoS qui mène des attaquent à partir d'un seul ordinateur avec l'autorisation de l'utilisateur, les attaques par déni de service distribué (DDoS) utilisent, quant à elles, un grand nombre d'ordinateurs infectés à l'insu ou sans l'autorisation de leurs propriétaires. Les programmes de type DDoS peuvent être téléchargés sur les ordinateurs de la victime par divers moyens. Une fois téléchargés, ils lancent l'ordre d'attaquer, soit lorsque leur maître leur en donne l'ordre, soit en fonction d'une date de reprise située dans le code.

III.1.1.4.2 Outils d'attaque et exploits

Les outils d'attaque permettent de pénétrer à l'aide des portes dérobées sur des ordinateurs distants et d'en faire des zombies en téléchargeant d'autres programmes malveillants sur les machines infectées.

Les exploits utilisent eux, les vulnérabilités des applications et des systèmes d'exploitation dans le but d'obtenir un résultat identique.

III.1.1.4.3 Inondeurs

Ils permettent d'inonder les canaux de données en utilisant des paquets de données et des messages électroniques inutiles.

III.1.1.4.4 Constructeurs et VirTools

Les constructeurs sont utilisés par les auteurs de virus afin de créer de nouveaux programmes malveillants et des chevaux de Troie. Certains constructeurs sont dotés d'une interface utilisateur qui permet de sélectionner le type de virus, les objets à attaquer, les options de cryptage,

la protection contre les débogueurs et les désassembleurs, etc. Les constructeurs moins complexes n'ont pas d'interface et sont construits au travers d'un fichier configuration.

Les virTools regroupent tous les utilitaires afin de faciliter la création des virus. Ils servent également à analyser les virus afin de voir comment ils pourraient être utilisés dans une attaque.

III.1.1.4.5 Crypteurs de fichiers et polycrypteurs

Ce type d'outils permet de crypter les codes malicieux afin qu'ils ne puissent pas être décelés par des antivirus.

III.1.1.4.6 Nukers

Le but de ce type d'utilitaires est de générer des erreurs fatales en exploitant les vulnérabilités des applications et des systèmes d'exploitation. Les pirates informatiques les utilisent afin d'entraîner le plantage des machines attaquées.

III.1.1.5 Les programmes en rapport avec les logiciels malveillants

C'est une catégorie difficile à définir puisqu'elle regroupe des applications licites pouvant être utilisées par un pirate afin de pénétrer un ordinateur. Ces programmes qui ne sont pas, à l'origine conçus afin d'être malveillants, sont parfois utilisés à des fins illégales et/ou compromettantes.

III.1.1.5.1 Dialers

Ces programmes ne nuisent pas aux machines sur lesquelles ils sont installés. Toutefois, s'ils ne sont pas détectés et supprimés, ils peuvent avoir de sérieuses conséquences financières. Les propriétaires de sites Web utilisent ces programmes afin que les machines infectées se connectent à des sites dont la visite est payante. Dans la majorité des cas, il s'agit de sites pornographiques. Même si l'ordinateur en lui-même n'est pas endommagé, la lourde facture téléphonique générée fait que ces produits ne sont pas du tout les bienvenus sur les ordinateurs et dans les réseaux.

Il existe deux catégories de dialers : les dialers chevaux de Troie et les dialers malicieux. Les numéroteurs chevaux de Troie sont installés à l'insu de l'utilisateur et établissent automatiquement des connexions vers des sites payants. Les numéroteurs dangereux, quant à eux, avertissent

l'utilisateur des appels qui seront effectués et du coût de ceux-ci. Ils peuvent être désinstallés en suivant la procédure standard. Ce deuxième groupe pourrait être qualifié de malveillant vu que l'installation se réalise sans le consentement de l'utilisateur, mais celui-ci a toutefois l'occasion de décider des actions à prendre.

III.1.1.5.2 Téléchargeurs

Même les utilitaires de téléchargement licites peuvent être dangereux car ils sont programmés pour fonctionner en arrière-plan, sans intervention directe de l'utilisateur. Un pirate informatique peut facilement remplacer les liens d'un site sain par ceux d'un site infecté, ce qui signifie que le programme malveillant est téléchargé sur l'ordinateur de la victime à son insu.

III.1.1.5.3 Serveurs FTP

Ils peuvent être utilisés pour obtenir un accès à distance à certains fichiers. Une fois qu'un pirate aura installé une telle application sur un ordinateur, il pourra télécharger n'importe quel fichier de la victime et suivre l'activité de l'ordinateur infecté.

III.1.1.5.4 Serveurs proxy

À l'origine, ces utilitaires furent développés pour protéger les réseaux internes en séparant les adresses internes des utilisateurs externes. Toutefois, les pirates informatiques les utilisent également pour se connecter anonymement à Internet : l'adresse du serveur proxy remplace l'adresse du pirate informatique.

III.1.1.5.5 Serveurs Telnet

Ces utilitaires ont été développés pour pouvoir accéder à distance aux ressources d'autres machines. Les pirates informatiques les utilisent pour obtenir un accès total à la machine de la victime.

III.1.1.5.6 Serveurs Web

Les serveurs Web sont des utilitaires qui permettent d'accéder à des pages Internet situées dans une zone définie du système de fichiers. Les pirates informatiques s'en servent pour obtenir un accès total au système de fichiers de la machine attaquée.

III.1.1.5.7 Clients IRC

Ces utilitaires donnent accès aux canaux IRC. Il existe de nombreux clients IRC, surtout mIRC qui intègre de puissants langages de script pour automatiser le client IRC. Ces fonctions peuvent être exploitées pour programmer des chevaux de Troie et des vers IRC. Lorsqu'il installe un cheval de Troie IRC sur la machine de sa victime, le pirate informatique installe également subrepticement un client IRC.

III.1.1.5.8 Moniteur

Il s'agit d'utilitaires licites qui surveillent l'activité de l'ordinateur et de l'utilisateur. Il existe des versions commerciales de ces utilitaires. Ses données sont, soit enregistrées sur le disque dur, soit envoyées à une adresse électronique définie. Les programmes de surveillance diffèrent des chevaux de Troie espions en ce sens, qu'ils ne dissimulent pas leur présence dans le système et qu'il est possible de les désinstaller.

III.1.1.5.9 PSWTool

Ces utilitaires rétablissent les mots de passe perdus. Ils affichent à l'écran les renseignements relatifs au mot de passe ou les enregistrent sur le disque. Lorsqu'ils sont utilisés lors d'attaques informatiques, ils renvoient les renseignements au pirate.

III.1.1.5.10 Remote Admin

Ces outils d'administration à distance donnent aux pirates un contrôle total sur la machine de la victime.

III.1.1.5.11 Décortiqueurs

Ces programmes ne sont pas des virus ou des chevaux de Troie, mais bien des programmes que les pirates utilisent pour déverrouiller certains logiciels. En général, ils ne représentent aucun danger pour les logiciels installés et se contentent de supprimer la clé des logiciels protégés.

III.1.1.5.12 RootKit

Les RootKit permettent de camoufler la présence de certains objets (clé de registre, fichiers, procédés) au sein du système. Un RootKit n'étant pas en soi une menace, il sera classé dans la même catégorie que le malware qu'il dissimule. Si par exemple, il camoufle un Trojan, alors il sera considéré comme un Trojan.

III.1.1.5.13 Mauvaises blagues et canulars

Ce groupe contient les programmes qui ne causent pas de dégâts directs à la machine infectée. Ils se contentent de lancer de fausses alertes sur les dégâts qui ont été ou qui seront causés. Par exemple, ces messages avertissent les utilisateurs que les disques ont été formatés, qu'un virus a été découvert ou que les symptômes d'une infection ont été décelés. La seule limite est en quelque sorte le prétendu sens de l'humour de l'auteur du virus.

III.1.1.6 SPAM

Nous pouvons décrire le SPAM comme étant un email anonyme, indésirable et qui est envoyé en masse.

Détaillons un peu plus les termes de cette définition :

- Anonyme : envoyé depuis des adresses volées à l'insu de son utilisateur afin de masquer le véritable expéditeur.
- Indésirable : Si l'utilisateur souhaite ou non-recevoir ce type d'emails.
- Mailing de masse : Les spammeurs ne gagnent de l'argent que grâce aux quelques réponses reçues. Pour que le spam soit rentable, il faut donc envoyer le mail initial en masse.

Le mot « publicité » n'est pas employé afin de définir le spam puisque de nombreux spam ne sont pas de la publicité. En effet, en plus de vanter des produits et des services, le spam peut aussi appartenir à des catégories comme les messages politiques, les appels à la charité, les arnaques financières, les chaînes de courriels ainsi que les faux spam destinés à distribuer des logiciels malveillants.

III.1.2 Moyens de lutter contre les logiciels malveillants

Il existe plusieurs outils permettant de lutter contre les logiciels malveillants. Ces différents outils permettent de détecter leur présence et de les nettoyer. Toutefois, il est important de rester à l'écoute des utilisateurs qui pourront signaler un fonctionnement anormal de leur poste informatique si ce dernier a été infecté par un logiciel malveillant.

III.1.2.1 Antivirus

La détection se fait selon deux principes :

- **une analyse par signatures** qui permet de détecter les virus connus à condition que les définitions de virus soient régulièrement mises à jour.
- **une analyse heuristique** qui permet de détecter avec des résultats variables les virus inconnus à partir de leur logique de programmation et le cas échéant de leur comportement à l'exécution.

La plupart des antivirus fonctionnent selon deux modes :

- **un scanner** qui permet à l'utilisateur de lancer une analyse d'un disque ou d'un fichier lorsqu'il le souhaite ("on demand").
- **un moniteur** qui surveille le système en temps réel ("on access") et empêche l'utilisateur d'ouvrir un fichier infecté.

Certains antivirus analysent seulement "à la demande" (ex. : antivirus en ligne) ou disposant que d'un moniteur (ex. : antivirus génériques).

Un antivirus peut aussi balayer le contenu de la mémoire de l'ordinateur, examiner les courriels, agir en amont de la machine en scrutant les échanges de fichiers avec l'extérieur, aussi bien en flux montant que descendant.

Après avoir installé un nouveau serveur antivirus virtuel sous hyper-v[33] (de façon à obtenir une haute disponibilité) avec le système d'exploitation Windows 2008 R2 64 bit (pour installer une version 64 bit de l'antivirus Trend micro permettant le scan des nouvelles machines sous Windows 7), je vérifie quotidiennement que l'antivirus Client et Serveur aient bien les dernières mises à jour du moteur de scan et de la base antivirale. Il existe des antivirus plus performants que celui choisi par la CRAM mais le gros avantage de ce dernier est la gestion centralisée du parc informatique, des clients et des serveurs.

III.1.2.2 Anti-spyware

Un anti-spyware permet de supprimer les logiciels espions du PC en analysant les fichiers mais aussi les clés de registre de Windows, les cookies "espions" et stopper les spywares en cours d'exécution.

Il est possible qu'un logiciel sain cache un spyware indispensable à son fonctionnement. La suppression de cet espion peut empêcher le programme de fonctionner. Un bon anti-spyware sauvegarde ses actions afin de pouvoir revenir en arrière et permettre de décider de supporter ou non l'espion.

Un pare-feu est un logiciel antispyware naturel dans la mesure où il peut bloquer ses transmissions d'informations privées vers l'extérieur. En effet, la première fois que le spyware cherchera à communiquer avec l'extérieur, le pare-feu demandera s'il faut autoriser cette connexion ou non. Une fois la réponse négative enregistrée en tant que règle, le pare-feu l'empêchera de communiquer des informations privées à l'extérieur. Ceci est valable si le spyware ne cherche pas à camoufler ses connexions dans d'autres flux autorisés par le pare-feu.

---

33 Hyper-V : Hyper-V, plus connu sous le nom de Windows Server Virtualization, est un système de virtualisation basé sur un hyperviseur 64 bits de la version de Windows Server 2008.

En complément d'un logiciel antispyware, il est important de mettre à jour régulièrement son système d'exploitation et son navigateur car les spywares s'installent en exploitant les failles de sécurité.

Il faut éviter les sources de fichiers et les sites Web dits «underground» car ils sont plus dangereux que la moyenne des sources. Il s'agit des sites Web pornographiques, de warez, des fichiers téléchargés de source inconnue, etc. Il peut être judicieux de bloquer certains sites web au sein de l'entreprise et de laisser l'accès à internet seulement aux personnes qui en ont l'utilité.

Aucun anti-spyware n'a actuellement été mis en place au sein de la CRAM.

III.1.2.3 Anti-malware

Ces logiciels anti-troyens, rootkits et hijackers complètent un antivirus. Ils renforcent la prévention ou complètent une suppression de malware.

Les anti-malware peuvent fournir une protection en temps réel contre l'installation de logiciels malveillants sur un ordinateur (même fonctionnement que la protection antivirus avec en plus une analyse de toutes les données réseaux entrantes et un blocage des menaces qu'il rencontre). Ce type de logiciels anti-malware scanne aussi le contenu de la base de registre Windows, les fichiers du système d'exploitation et les programmes installés sur un ordinateur.

Aucun anti-malware n'est installé sur les ordinateurs de la CRAM sauf dans le cas de soupçon ou nous installons Malwarebytes' Anti-Malware.

III.1.2.4 Anti-spam

La plupart des messageries proposent un filtre anti-spam qui qualifie automatiquement des emails comme spam et les déplace dans un dossier dédié pour ne plus encombrer le dossier de réception.

Il existe aussi les listes noires dans lesquelles on peut ajouter des adresses email (prenom.nom@domaine.com), des groupes d'adresses (nom@domaine.com) ou un domaine entier (domaine.com), pour bloquer les expéditeurs et ne plus recevoir d'email de leur part.

Certains fournisseurs peuvent aussi proposer une personnalisation du filtre dans lequel on ajoute certains mots ou expressions présents dans le titre ou le corps de l'email.

À l'inverse, il existe aussi des listes blanches d'adresses email dans lesquelles on saisit des adresses qui ne sont alors pas envoyées vers le dossier SPAM même si l'anti-spam l'a considérée comme telle.

Un de nos clients ne recevait plus nos emails. Après vérification, je me suis aperçu en testant notre domaine CRAM (http://mxtoolbox.com/) qu'il avait été blacklisté. Une machine infectée qui envoyait du spam en était la cause ! J'ai donc demandé à notre fournisseur d'accès que notre serveur de messagerie soit le seul à pouvoir envoyer du SMTP[34]. J'ai dû ensuite demander la suppression du blacklistage de notre domaine. Pour que cette demande soit acceptée, il a fallu en préciser la cause et expliquer le ou les moyens mis en œuvre pour éviter que cela ne se reproduise.

Un module anti-spam est installé sur notre serveur de messagerie interne fonctionnant sous lotus notes.

III.1.2.5 Pare-feu logiciel

Un pare-feu protège des intrusions car il filtre les communications entrantes depuis Internet vers la machine et dans l'autre sens en ne répondant pas aux demandes de présence intempestives. Un pare-feu logiciel est qualifié de pare-feu personnel car il est chargé sur un ordinateur individuel.

---

34 SMTP : Le Simple Mail Transfer Protocol (littéralement « Protocole simple de transfert de courriers »), généralement abrégé SMTP, est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.

En filtrant les communications entrantes, un pare-feu protège des menaces suivantes :

- une application communicante ayant ouvert un port sur l'ordinateur pouvant servir aussi à une intrusion (en exploitant à distance une faille de sécurité).
- le système d'exploitation qui est composé d'une multitude de logiciels communicants, c'est-à-dire une multitude de ports potentiellement ouverts.
- une tentative de déconnexion à distance.
- une connexion avec un troyen préalablement installé sur la machine (pour une intrusion ou une prise de contrôle à distance de votre ordinateur).

Les applications Internet communiquent automatiquement vers l'extérieur pour :

- améliorer la qualité du service (par exemple savoir si une nouvelle version du logiciel est disponible).
- récupérer un bandeau publicitaire (adware) : seul moyen de financer une application gratuite.
- envoyer les informations privées à leur serveur (spyware).
- envoyer les mots de passe (troyen).

Un pare-feu personnel permet de détecter ces communications et permet de les autoriser ou de les interdire.

Les pare-feu possèdent aussi un mode discret "stealth" qui empêche l'ordinateur de répondre (comme s'il était hors ligne). Ce mode permet ainsi de réduire la possibilité d'intrusion, en plus de la tentative elle-même.

Un pare-feu logiciel est aussi capable de détecter si un programme a été modifié. Certains malwares injectent leur code dans un programme habituellement autorisé à communiquer (par exemple Internet Explorer). Le pare-feu va alors détecter un changement dans la communication de ce programme et demander à l'utilisateur s'il l'autorise toujours ou non.

Le gain de sécurité apporté par la mise en place d'un tel pare-feu est très intéressant. En revanche, un tel dispositif de sécurité est bien trop complexe pour des personnes novices à moins d'utiliser un profil avec des règles définies à l'avance. De plus, pour être efficace, il est indispensable de prendre en compte tout nouveau programme, ce qui demande trop de temps. Aucun pare-feu « logiciel » n'est mis en place à la CRAM sur les postes utilisateurs. J'ai, en revanche, configuré le pare-feu Windows sur les serveurs en utilisant les GPO[35], ce qui permet de centraliser à un seul endroit la gestion des règles. J'ai configuré le pare-feu via les GPO de telle sorte qu'il soit toujours possible en local d'éditer les règles du pare-feu sur le serveur, ce pour un besoin spécifique.

III.2 Systèmes d'exploitation

Pour un système d'exploitation donné, il est important d'avoir des moyens et des procédures de protection des objets que le système permet de manipuler. Les éléments à protéger peuvent être des fichiers, des périphériques, des processus, des espaces mémoire créés, etc.

Cette protection permet d'empêcher qu'un utilisateur puisse altérer un fichier qui ne lui appartient pas et dont le propriétaire ne lui en a pas donné l'autorisation. Il permet aussi d'empêcher qu'un processus, en cours d'exécution, ne modifie une zone mémoire attribuée à un autre processus sans son autorisation.

Nous pouvons enfin dire que la protection d'un objet informatique se résume aux éléments suivants :

- Un objet (processus, fichier, segment mémoire) a un propriétaire identifié, généralement l'utilisateur qui l'a créé.

---

35 GPO : Les stratégies de groupe (Group Policy Object en anglais) sont des fonctions de gestion centralisées de la famille Microsoft Windows. Elles permettent la gestion des ordinateurs et des utilisateurs dans un environnement Active Directory. Les stratégies de groupe font partie de la famille des technologies IntelliMirror, qui incluent la gestion des ordinateurs déconnectés, la gestion des utilisateurs itinérants ou la gestion de la redirection des dossiers ainsi que la gestion des fichiers en mode déconnecté.

- Le propriétaire d'un objet peut avoir conféré à lui-même et à d'autres utilisateurs des droits d'accès à cet objet (lecture, écriture, exécution,…).

- À chaque objet, est donc associée une liste de contrôle d'accès (ACL) qui énumère les utilisateurs autorisés et leurs droits.

III.2.1 Droits d'accès

Le droit d'accès est nécessaire à un utilisateur pour accéder à des données protégées ou à des ressources.

En fonction du contexte, le droit d'accès peut s'étendre au sens de l'organisation des accès au système d'information, au sens de la sécurité des systèmes d'information, ou bien au sens juridique.

Dans le système d'information d'une entreprise, à chaque fichier est associée une liste de permissions qui détermine ce que chaque utilisateur a le droit de faire sur le fichier.

Au sein de la société CRAM, les droits d'accès sont définis en fonction des services auxquels les personnes appartiennent et sont alloués uniquement sur demande écrite de leur responsable.

La gestion des droits devenant souvent très complexe, la société a investi dans un logiciel (« script logic ») permettant de lister les droits utilisateurs mis en place sur les répertoires.

III.2.2 Authentification

Pour un système informatique, elle consiste à vérifier l'identité d'une entité (personne, ordinateur...), pour autoriser l'accès de cette entité à des ressources tels que des systèmes, réseaux, applications, etc.

Un protocole d'authentification peut appartenir à différentes familles :

- L'authentification simple qui ne repose que sur un seul élément ou « facteur » (le mot de passe utilisateur).

- L'authentification forte reposant sur deux facteurs ou plus.
- L'authentification unique permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder par exemple à plusieurs applications informatiques.

L'authentification peut se baser sur différentes techniques comme un mot de passe préalablement établi, une vérification biométrique (voix, empreintes digitales, iris, …), etc.

Chaque utilisateur possède un compte « machine » lui permettant de s'identifier sur le réseau de la CRAM. Chacun de ces comptes est nommé de la même façon : la première lettre du prénom ou les deux premières d'un prénom composé suivi de son nom. Chaque compte est donc nominatif et propre à chacun.

III.2.3 Audit de sécurité (Identification)

L'identification est rendu possible grâce à l'audit de sécurité. En effet, si par exemple, quelqu'un supprime un fichier sur un serveur, cette suppression est tracée. Le nom du compte étant associé à cette suppression est alors enregistré, ce qui permet de retrouver la personne à l'origine de cette action.

La mise en place de l'audit se fait uniquement sur certaines actions, sinon les logs seront illisibles et de trop grosses tailles. De plus, les performances du système s'en trouveront affectées. Il est aussi possible d'auditer les échecs de tentatives de connexion pour lutter contre l'usurpation d'identité.

Le système d'audit a un inconvénient puisqu'il peut renseigner sur le compte qui était utilisé lors d'une opération, mais on ne peut pas avoir la certitude que le compte était utilisé par son propriétaire.

L'identification allant de pair avec l'authentification, nous sommes, par exemple, capables d'identifier qui fait quoi sur les serveurs de fichiers de la société.

III.2.4 Mot de passe

Aucune politique de mot de passe n'est actuellement appliquée. Chaque utilisateur est donc libre de laisser son mot de passe par défaut ou de le changer à sa guise. Il faudra donc à l'avenir

prévoir et mettre en place une stratégie de mot de passe. Comme nous le verrons dans la prochaine partie (sécurité utilisateurs), j'ai diffusé un guide au sein de la société dans le but de sensibiliser les utilisateurs et de leur faire prendre conscience des risques qu'ils encourent lorsqu'ils laissent un mot de passe par défaut ou qu'ils le divulguent à leurs collègues.

III.2.5 Liste d'accès (Permission)

Une liste d'accès est en quelque sorte une liste d'utilisateurs et de groupes ayant des permissions d'accès à un objet. Chacun des objets comporte une ACL qui lui est propre. Les propriétaires des objets peuvent par exemple via le gestionnaire de fichiers, ajouter ou supprimer des utilisateurs ou des groupes et ainsi gérer les permissions.

III.2.6 Chiffrement

Le chiffrement, permet de rendre impossible la compréhension d'un document à toute personne n'ayant pas la clé de déchiffrement.

La sécurité d'un système de chiffrement repose d'avantage sur le secret de la clé de chiffrement que sur l'algorithme en lui-même.

Aucun chiffrement n'est utilisé au sein de la société CRAM, car la grande majorité des utilisateurs ayant des ordinateurs de bureau cela n'aurait aucun intérêt.

III.3 Développement

La sécurité dans les développements est généralement « plutôt bien traitée » chez de grands éditeurs ou certaines SSII mais reste plutôt « oubliée » pour les développements « in house ». Durant la programmation, il est important de prendre en compte la sécurité informatique à tous les moments de la conception et de la réalisation à l'utilisation d'un programme.

Un logiciel sécurisé doit garantir la confidentialité des informations qu'il contient, l'intégrité des données ou encore la performance et la disponibilité requise.

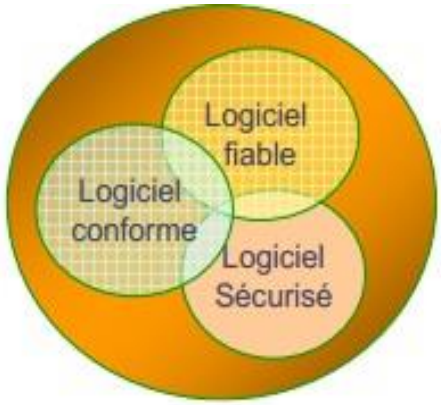


Figure 3 – Qualité du développement

D'après le SANS (SysAdmin, Audit, Network, Security) Institute, 80% des anomalies ont fréquemment trois origines :

- L'acceptation de saisie utilisateurs sans phase de contrôle et de validation (Injection SQL, cross site scripting).

- L'autorisation des données placées dans une zone tampon a excédé la taille du tampon (Saturation de tampon et possibilité d'exécuter du code dans l'espace libre).

- La mauvaise gestion des entiers (Attaques visant les contrôles ActiveX ou JRE Java).

Il peut être judicieux d'effectuer les tests suivants :

- Tester le code source pour vérifier que la construction du code est conforme aux règles de programmation du langage utilisé.

- Test fonctionnel afin de détecter les erreurs qui ne se déclenchent que lors de l'exécution (interfaces utilisateur, API, etc.).

- Tests de performances par exemple sur des applications web, intranet, etc.

Les langages de développement utilisés par la CRAM sont les suivants :

Langages utilisés	
VB6	.Net
VBScript	C#
JavaScript	

Tableau 4 - Liste des langages de développement utilisés par la CRAM

La CRAM doit être vigilante vis-à-vis de ses applications puisqu'elle les développe elle-même et est donc par conséquent plus sujette à des bugs pouvant remettre en cause l'intégrité des données.

L'authentification des utilisateurs sur les applications se fait via le compte Active Directory. Cela permet de créer des groupes ayant accès à telle ou telle application et d'y placer ou non les utilisateurs.

Les données des applications sont stockées dans des bases de données « SQL server » hébergés sur des serveurs spécifiques.

Après avoir vu différentes menaces logiciels, on s'aperçoit que leur diversité est très importante et qu'il est difficile de toutes les lister. L'installation d'un antivirus est, aux yeux de la plupart des personnes, indispensable, mais peu connaissent les firewalls, les anti-malware et autres moyens de protection… Le choix d'un antivirus est très important puisqu'il n'est pas forcément adapté aux besoins. Dans le cas d'une entreprise, nous allons plutôt opter pour un antivirus permettant de protéger l'ensemble du parc informatique même si celui-ci est moins performant qu'un autre. En effet, la centralisation de l'affichage des menaces sur une console centrale permet aux administrateurs d'être alertés en temps réel des menaces et d'éviter ainsi toute propagation sur

le parc informatique. De même, les notions de liste d'accès, de droits ou encore de cryptages empêchent certains logiciels malveillants d'obtenir des informations ou de les exploiter. Il est aussi très important de rester vigilant lors des développements d'applications « in house » et de respecter certaines règles…

IV Sécurité des utilisateurs

La sensibilisation des utilisateurs aux problèmes de sécurité est primordiale. Mettre en place des règles de sécurité, des stratégies de mots de passe ne sert à rien si ces derniers n'ont pas pris conscience du réel impact de la sécurité. Avant d'effectuer des recommandations ou de mettre en place des procédures, il est nécessaire d'effectuer un audit de sécurité utilisateur puis de rédiger un guide dit de « bonnes pratiques ». Pour « verrouiller » ce périmètre, il est souhaitable de créer une charte informatique afin de mettre en place des limites aux utilisateurs.

Le comportement d'un utilisateur étant imprévisible, nous allons dans un premier temps définir quels sont les risques. Nous examinerons ensuite de plus près le comportement des utilisateurs, ainsi que l'utilisation qu'ils font de l'outil informatique. Nous réaliserons un questionnaire qui servira d'audit utilisateur. Ce dernier permettra de se focaliser sur les principaux points critiques et orientera le guide des bonnes pratiques ainsi que la charte informatique. Pour finir, nous verrons comment réduire ces risques et les prévenir.

Un chapitre aurait pu être consacré aux différents types de démarches comme la démarche MARION[36] ou ITIL[37]. Bien que ces démarches aient été visualisées afin d'orienter les travaux, elles

36 MARION : La méthode d'analyse de risques informatiques orientée par niveau (Marion) est une méthode d'audit, proposée depuis 1983 par le CLUSIF, visant à évaluer le niveau de sécurité informatique d'une entreprise. L'objectif est double, il permet de situer l'entreprise auditée par rapport à un niveau jugé correct et d'identifier les menaces ainsi que les vulnérabilités à contrer.

ne pourront être appliquées à la CRAM. En effet, la CRAM reste une société avec une culture d'entreprise relativement ancienne et complexe dans laquelle il est nécessaire d'y adapter chaque élément de la sécurité. Cela est aussi valable pour le questionnaire d'audit que pour la charte informatique ainsi que tout autre élément de sécurisation réduisant les droits et les libertés des différents utilisateurs.

IV.1 Risques humains

IV.1.1 La maladresse

Tous les humains commettent des erreurs. Il leur arrive plus ou moins fréquemment d'exécuter un traitement non souhaité, d'effacer involontairement des données ou des programmes, etc.

IV.1.2 L'inconscience et l'ignorance

La plupart des utilisateurs sont inconscients ou ignorent les risques qu'ils font encourir aux systèmes qu'ils utilisent. Ils introduisent souvent des programmes malveillants sans le savoir. Des manipulations inconsidérées (autant avec des logiciels que physiquement) sont aussi relativement fréquentes.

IV.1.3 La malveillance

Rares sont les personnes pouvant prétexter l'ignorance des risques informatiques, tant les média ont pu parler des différents problèmes de virus et de ver ces dernières années (même s'ils ont tendance à se tromper sur les causes et les problèmes). Certains utilisateurs peuvent pour diverses raisons mettre volontairement en péril le système d'information en y introduisant des virus ou de mauvaises informations dans une base de données. Un informaticien peut ajouter délibérément des fonctions cachées lui permettant de détourner à son profit de l'information ou de l'argent.

---

37 ITIL : (Information Technology Infrastructure Library pour « Bibliothèque pour l'infrastructure des technologies de l'information ») ITIL est un ensemble d'ouvrages recensant les bonnes pratiques (« best practices ») du management du système d'information.

IV.1.4 L'ingénierie sociale

L'ingénierie sociale (*social engineering*) est une méthode permettant d'obtenir d'une personne des informations confidentielles dans le but de les exploiter à d'autres fins (publicitaires...). La technique consiste, par exemple, à se faire passer pour un administrateur réseau et à demander des informations personnelles (nom de connexion, mot de passe) en prétextant un problème quelconque (réseau, logiciel). Ces informations peuvent très bien être demandées par téléphone, par courriel, etc.

IV.1.5 L'espionnage

L'espionnage industriel permet d'obtenir des informations sur des activités concurrentes, des procédés de fabrications, des projets en cours, des futurs produits, des politiques de prix, des clients, des prospects, etc.

IV.1.6 Le détournement de mot de passe

Un administrateur système ou réseau peut très bien modifier les mots de passe d'administration afin de prendre le contrôle d'un système ou d'un réseau. On peut citer l'histoire de Terry CHILDS, un ancien administrateur réseau du système informatique de la ville de San Francisco, qui a été condamné pour avoir modifié tous les mots de passe des équipements du réseau de la ville. Ce dernier, en désaccord avec sa direction, avait changé les mots de passe d'accès au réseau sans les divulguer, bloquant ainsi le WLAN[38]. Bien qu'il ne soit pas l'architecte du réseau, il est le seul à avoir construit et configuré les équipements réseau. Cet exemple montre l'importance du facteur humain dans la sécurité informatique et la nécessité de ne pas avoir qu'une seule personne responsable de la totalité d'un système.

---

38 WLAN : Un réseau sans fil (wireless network en anglais) est un réseau informatique ou numérisé qui connecte différents postes ou systèmes entre eux par ondes radio. Il peut être associé à un réseau de télécommunications pour réaliser des interconnexions entre nœuds.

Maintenant que nous avons vu les différents risques pouvant être liés aux utilisateurs, cela va nous permettre de mieux orienter notre audit de sécurité et plus particulièrement le questionnaire que nous évoquerons dans la partie suivante.

IV.2 État des lieux

IV.2.1 Réalisation de l'audit

Le meilleur moyen d'effectuer un état des lieux est de réaliser un audit. Ce dernier permettra de connaître les habitudes et les méthodes de fonctionnement des utilisateurs. Nous pourrons voir si ces derniers changent ou non régulièrement leur mot de passe, si des personnes dans leur entourage connaissent leurs identifiants permettant d'accéder au système d'information, etc.

En annexe, se trouve le questionnaire réalisé qui a permis d'effectuer l'audit utilisateur (Annexe 2 – Questionnaire utilisateurs).

Voyons maintenant plus en détails les différents points de ce questionnaire :

L'objectif principal de ce questionnaire est de couvrir l'ensemble des domaines afin d'avoir une vue représentative des menaces dont l'utilisateur peut être victime.

Afin d'avoir des réponses, les plus proches possibles de la réalité lors du questionnaire, il est important de préciser aux personnes interrogées que celui-ci est anonyme. De cette manière, les gens ne masquent pas certaines habitudes par crainte de sanction.

Il est important d'être vigilant quant à la formulation des questions afin de ne pas braquer les utilisateurs. Cela permettra d'avoir un audit qui reflètera le mieux possible l'état actuel de la sécurité au niveau des utilisateurs.

Les questions doivent être claires, précises et courtes puisqu'elles s'adressent, la plupart du temps, à des utilisateurs novices dans le domaine de l'informatique.

Nous allons maintenant voir et analyser les résultats de ce questionnaire.

IV.2.2 Résultat de l'audit

IV.2.2.1 Les mots de passe

Les utilisateurs ont-ils déjà changé une fois leur mot de passe ?

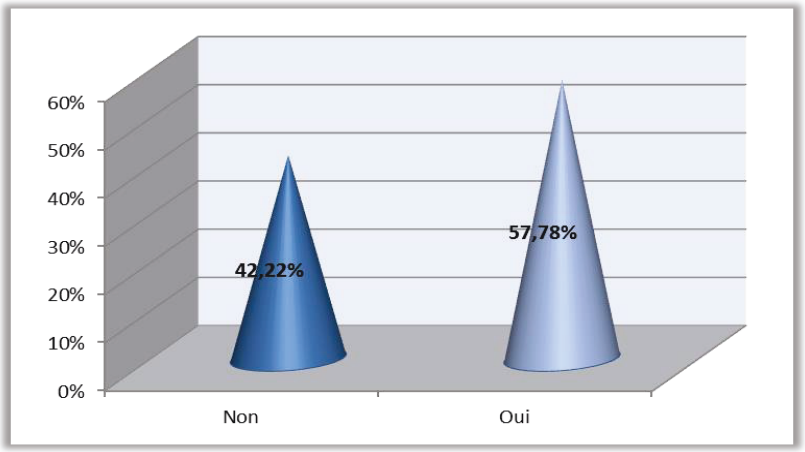


Figure 4 - Sondage utilisateurs - Changement de mot de passe

Comme nous pouvons le voir ci-dessus, une bonne majorité des utilisateurs n'a pas changé son mot de passe depuis son arrivée et a donc laissé celui par défaut attribué aux nouveaux arrivants ! Ce point est très critique du point de vue de la sécurité puisque n'importe quelle personne de la société peut se faire passer pour quelqu'un d'autre et avoir accès à des documents confidentiels !

Voyons maintenant combien de personnes, parmi celles ayant changé au moins une fois leur mot de passe, ont pris l'habitude de le renouveler régulièrement durant l'année :

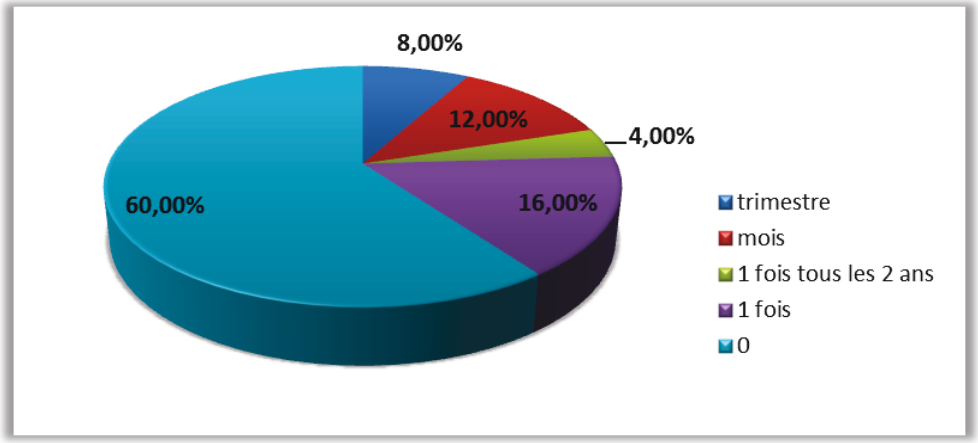


Figure 5 - Sondage utilisateurs - Renouvellement du mot de passe

Cette figure nous démontre que peu d'utilisateurs ont l'habitude de changer leur mot de passe régulièrement. En effet, seuls 20% d'entre eux le change au minimum une fois par trimestre, ce qui parait être la fréquence idéale.

Poussons un peu plus loin notre analyse et attachons-nous à la complexité et à la longueur des mots de passe. En effet, changer son mot de passe est important, mais si ce dernier ne comporte que deux caractères, alors cela n'est pas plus sécurisant que d'avoir toujours un même mot de passe plus complexe.

Ci-dessous la représentation de la longueur des mots de passe du personnel de la CRAM :

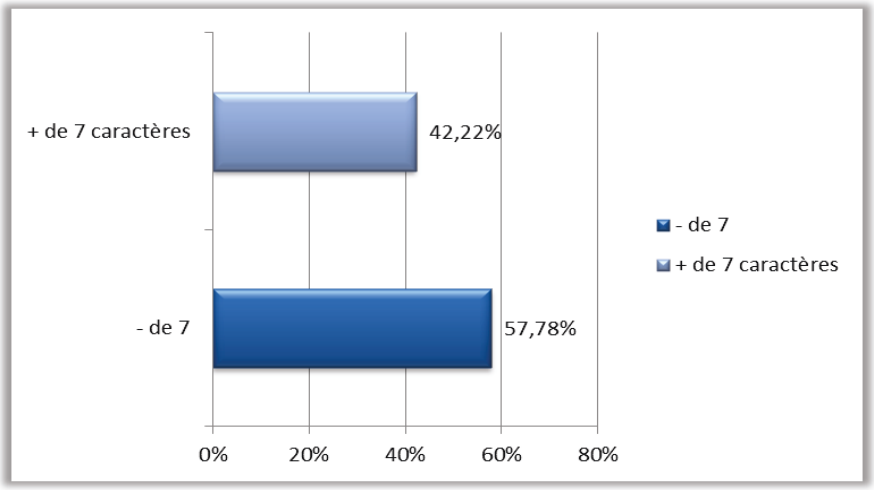


Figure 6 - Sondage utilisateurs - Longueur des mots de passe

Voyons maintenant la longueur des mots de passe en fonction de la complexité de ces derniers :

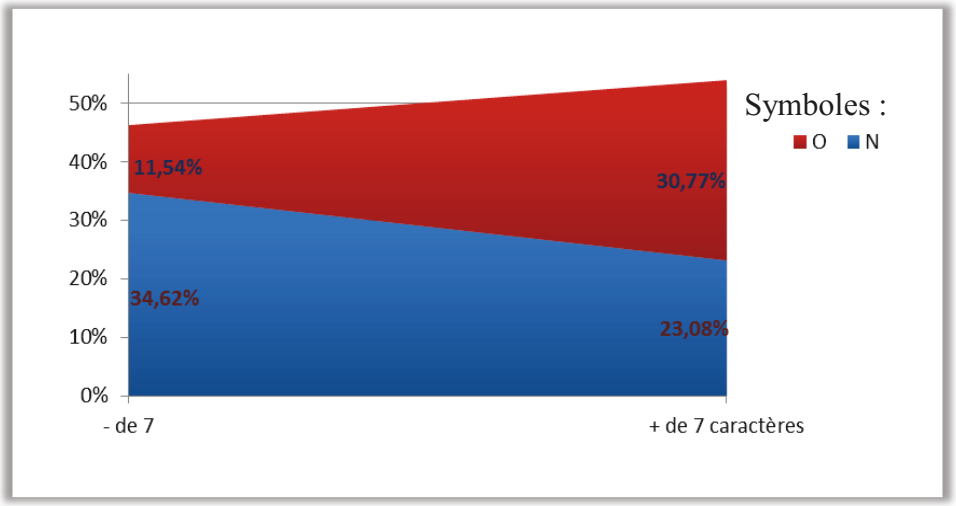


Figure 7 - Sondage utilisateurs - Complexité des mots de passe

Les mots de passe sont, pour l'ensemble des personnes, trop courts et pas assez complexes. Voyons brièvement quel est le temps nécessaire pour résoudre différents types de mots de passe.

Prenons l'exemple d'un mot de passe d'une **longueur de 8 caractères :**

Type de mots de passes	Nombre de caractères	Nombre de possibilités	Temps de résolution
Caractères spéciaux	95	6634204312890625	33 ans
Lettres et nombres	62	218340105584896	1 an
Lettre seulement	52	53459728531456	96 jours
Lettres minuscules avec une majuscule	26	1670616516608	3 jours
Lettres minuscules seulement	26	208827064576	9h

Tableau 5 - Temps de résolution d'un mot de passe

Voyons qui connait les mots de passe du personnel de la CRAM :

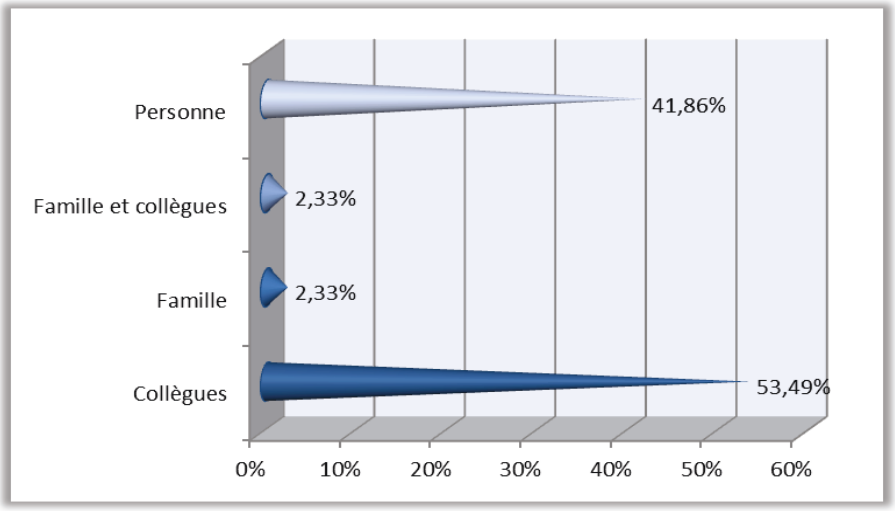


Figure 8 - Sondage utilisateurs - Connaissance des mots de passe

Comme nous pouvons le constater, 41.86% des employés n'ont jamais donné leur mot de passe et environ la même proportion l'a uniquement communiqué à ses collègues.

Ces résultats montrent que la sécurité au niveau des mots de passe est plus que préoccupante et qu'il est indispensable de mettre en œuvre une stratégie de mots de passe rapidement.

Il pourrait, par exemple, être judicieux de configurer une GPO afin d'obliger les utilisateurs à avoir des mots de passe plus complexes et à les changer régulièrement. Il ne faut pas trop durcir cette règle, car sinon les utilisateurs risquent de noter leur mot de passe sur des post-it aux alentours de leur PC.

Toutefois, on peut noter certains cas particuliers. Sur l'ordinateur du standard téléphonique, plusieurs personnes travaillent avec la même session, car le logiciel de celui-ci doit fonctionner en permanence. Certaines personnes ont, par exemple, donné leur mot de passe à leur supérieur lors de leur départ en vacances et ne l'ont pas changé à leur retour.

IV.2.2.2 Verrouillage de la session

Nous allons maintenant nous intéresser au verrouillage du poste utilisateur. Les utilisateurs laissent-ils leur session ouverte lorsqu'ils s'absentent ?

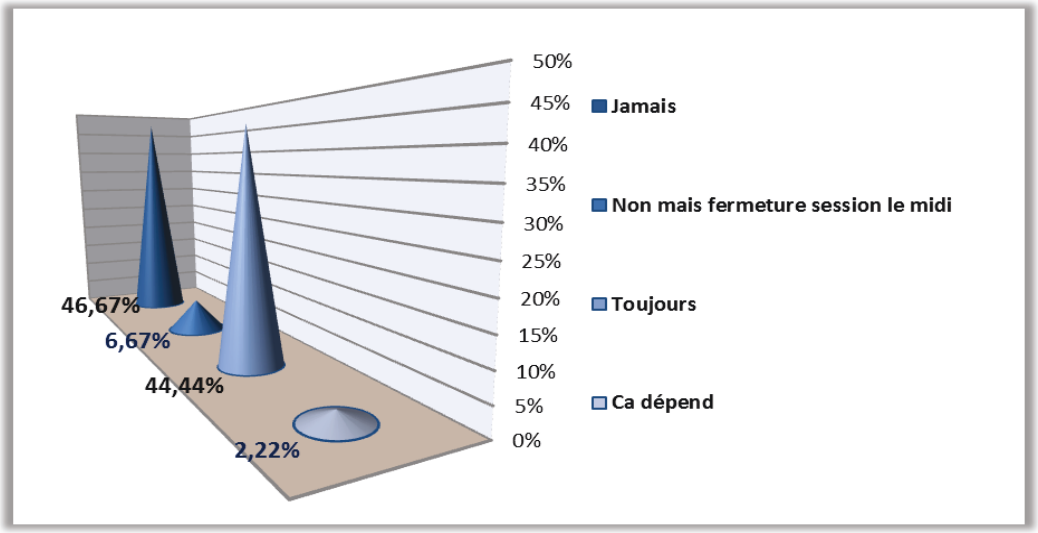


Figure 9 - Sondage utilisateurs - Verrouillage de la session

Beaucoup d'utilisateurs ne verrouillent pas leur session donc il serait judicieux de mettre en place une GPO avec un verrouillage de session, et ce de manière automatique. Attention toutefois, à laisser un délai relativement long aux utilisateurs si jamais ils sont au téléphone par exemple… Bien que par défaut les PC soient en fermeture de session lors de la sortie de la veille, cela ne suffit pas forcément.

Le guide des bonnes pratiques permettra de sensibiliser les utilisateurs sur les « dangers » qu'ils encourent en laissant leur session ouverte. Grâce à ce guide, nous pourrons espérer un changement dans leur attitude. Les chiffres restent tout de même encourageants, puisque la moitié du personnel verrouille sa session si elle s'absente plus de 10 minutes de son ordinateur.

IV.2.2.3 Travail à domicile

Intéressons-nous maintenant au travail à domicile. En effet, celui-ci n'a pas de rapport direct avec la société, mais reste tout de même une source d'ennuis. Beaucoup de gens travaillent sur des documents professionnels chez eux et procèdent à des échanges entre leur ordinateur personnel et celui de la société. Ce point se révèle donc relativement critique puisque si leur ordinateur personnel ne contient aucun antivirus ou moyens de protection, alors leur ordinateur professionnel est susceptible d'être infecté.

Bien que cela ne soit pas dans la politique de la société, voyons le pourcentage de personnes travaillant chez eux sur des documents professionnels :

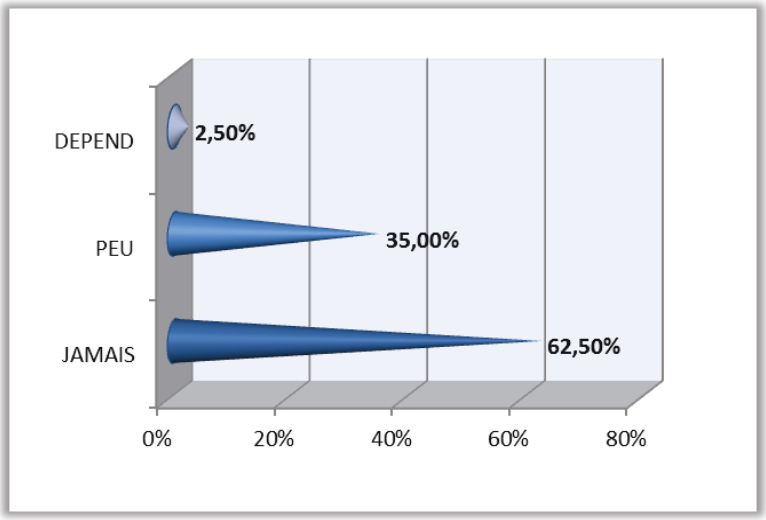


Figure 10 - Sondage utilisateurs - Travail à domicile

Une bonne partie des employés travaille pour la société à leur domicile, que ce soit sur des documents CRAM, pour effectuer des recherches ou encore pour se tenir informée des nouvelles lois en vigueur.

En voyant ces résultats, on constate qu'il est judicieux de s'intéresser aux moyens de transport des données utilisés entre la société et le domicile.

Les clés USB :

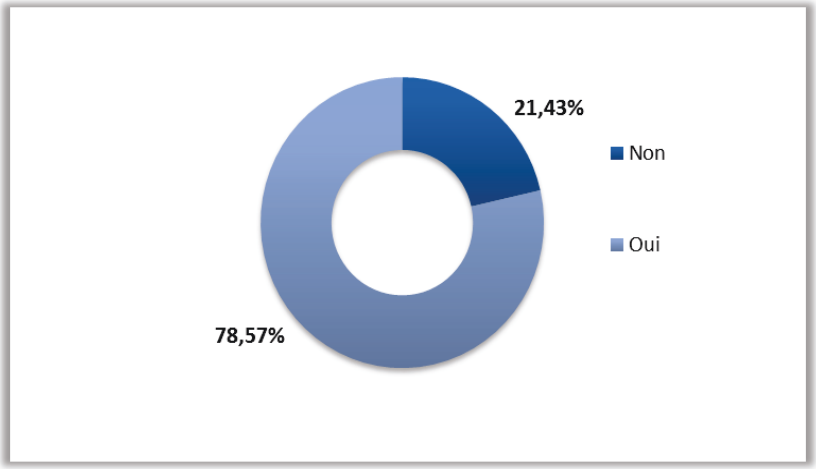


Figure 11 - Sondage utilisateurs – Transport des données - Clés USB

Les courriels :

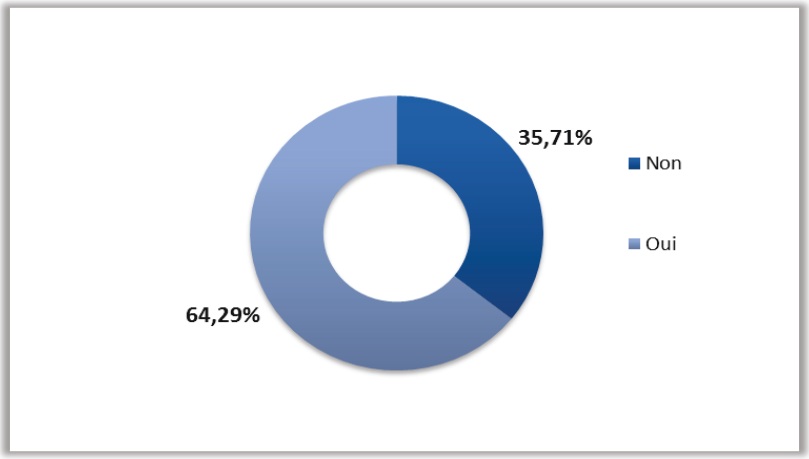


Figure 12 - Sondage utilisateurs – Transport des données - Courriels

La majorité des utilisateurs se servent de clés USB ainsi que de leurs courriels pour transférer leurs données, ceci nous pousse donc à nous intéresser à ces deux types de technologie par la suite.

IV.2.2.4 Périphériques

L'utilisation de périphériques pose souvent problème. En effet, il est impossible d'être sûr des données contenues sur ces derniers. Le personnel utilise-t-il des périphériques ?

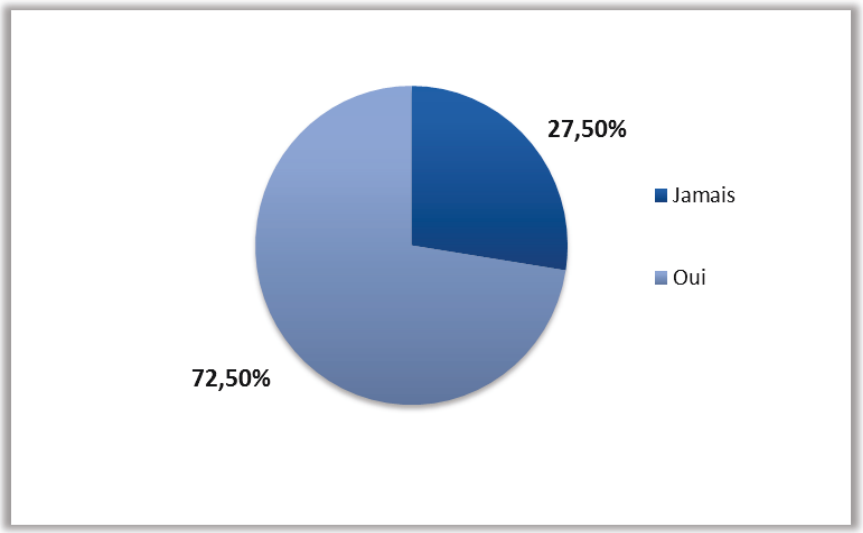


Figure 13 - Sondage utilisateurs – Utilisation des périphériques

Comme nous pouvons le constater sur le graphique ci-dessus, la majorité du personnel de la société utilise des périphériques, cela peut aller des clés USB aux appareils photo en passant par des téléphones portables.

Le nombre de périphériques utilisés sur les postes va croître dans l'avenir avec l'arrivée des iPhone pour le personnel de la société.

Etant donné le nombre de personnes utilisant des périphériques dans la société, il est indispensable d'avoir un antivirus vérifiant chaque périphérique connecté. Cette fonctionnalité est activée dans le paramétrage de l'antivirus de la CRAM ce qui est un bon point.

IV.2.2.5 Messagerie

D'après cet audit, la totalité du personnel regarde l'expéditeur et le contenu du courriel avant d'ouvrir les pièces jointes ce qui est une bonne attitude puisqu'elle évite beaucoup de virus et autres pièces jointes infectées.

Quelques personnes souhaitent savoir comment sécuriser les échanges par courriels entre leur domicile et leur bureau. Comme vous le verrez par la suite, cette notion a été intégrée dans le guide des bonnes pratiques à titre informatif. Dans le cas où les personnes voudraient l'utiliser, ils devront alors contacter le service informatique.

Dans un but de sécurité optimale, il pourrait être judicieux de mettre en place une utilisation des signatures numériques automatiques.

IV.2.2.6 Imprimantes

Le temps pendant lequel les documents restent à l'imprimante peut se révéler problématique puisque ces derniers peuvent contenir des informations à caractère confidentiel. Les directeurs d'agence possèdent une imprimante personnelle afin de ne pas rencontrer ce genre de problématiques. En effet, même en allant chercher immédiatement ces documents, cela peut demander 30 secondes ou plus en fonction de l'endroit où se situe le copieur.

Durée pendant laquelle un document reste sur l'imprimante :

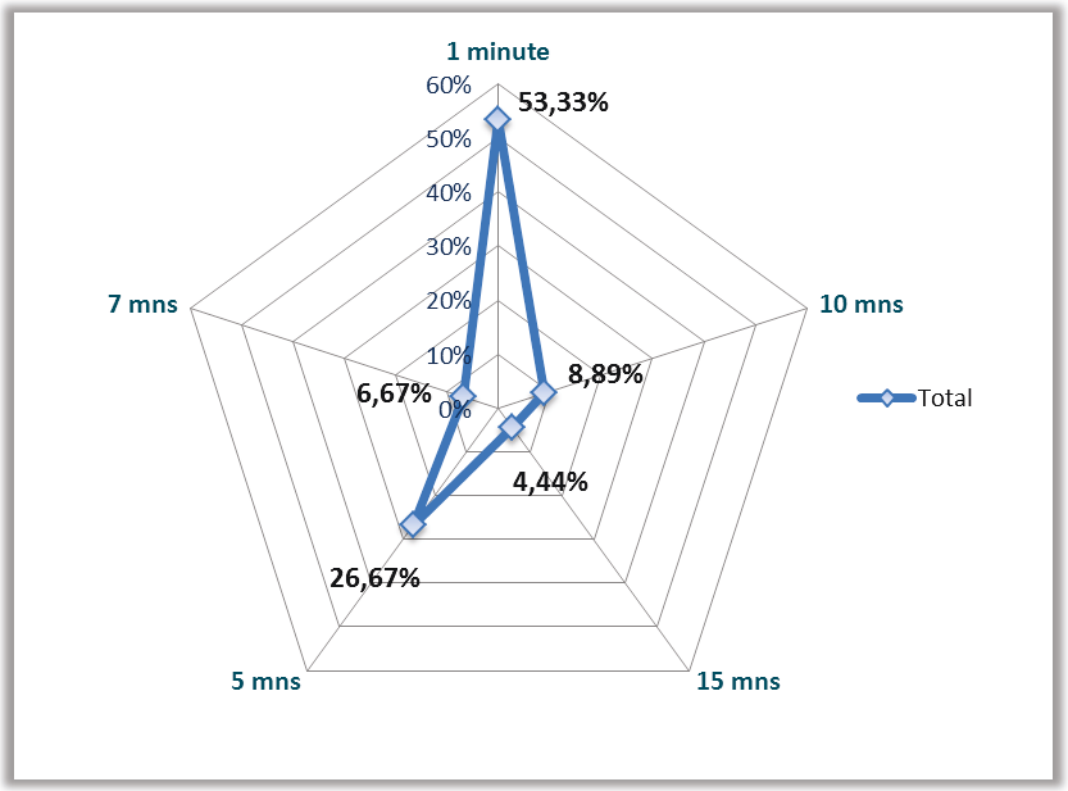


Figure 14 - Sondage utilisateurs – Imprimantes

Nous constatons qu'en moyenne les documents sont récupérés dans un laps de temps de 4 minutes.

IV.2.2.7 Sécurité physique

Les boissons :

Des boissons, à proximité du poste informatique, peuvent rendre ce dernier inutilisable, il est donc important de sensibiliser les utilisateurs à propos de ce sujet.

Voyons les résultats obtenus :

	Pourcentage de personnes qui boivent à proximité de leur PC
Non	20.93%
Oui	79.07%

Tableau 6 - Sondage utilisateurs – Boissons à proximité du poste de travail

Comme les chiffres nous l'indiquent, la majorité du personnel de la CRAM boit à proximité de son poste de travail que ce soit avec des bouteilles ou des tasses. Il sera donc judicieux de rappeler ce risque dans le guide des bonnes pratiques afin de sensibiliser les utilisateurs.

Inconnu étranger à la société :

Si une personne étrangère à la société se promène dans les couloirs, quel est le pourcentage de personnes qui va aller vers cet individu ?

	Pourcentage de personnes qui va vers une personne
Non	13,9%
Lui parle	86.05%

Tableau 7 - Sondage utilisateurs – Personne étrangère

La plupart des salariés ne laissent donc pas une personne seule errer dans les couloirs.

IV.3 Sensibilisation des utilisateurs

Afin de sensibiliser les utilisateurs sans pour autant employer la méthode forte, un guide de bonnes pratiques a été réalisé. Ce dernier se devait d'être le plus simple possible et comporter des

illustrations afin que les utilisateurs puissent au premier coup d'œil connaître les précautions à prendre.

Pour chaque point, les conséquences engendrées sont expliquées afin de faire prendre conscience aux utilisateurs de l'importance de leurs actes de tous les jours sur le système d'information.

Le guide de bonnes pratiques se trouve en annexe (Annexe 3 – Guide Des Bonnes Pratiques Informatiques).

Ce guide a été diffusé par email puisque dans l'audit utilisateur le choix préféré des utilisateurs s'est révélé être la diffusion par mail.

IV.4 Politique de sécurité utilisateur

La politique de sécurité permet de définir la protection du système d'information de l'entreprise. Elle se compose d'un ensemble comportant des directives, des procédures, des codes de conduite, des règles organisationnelles et techniques. Par conséquent, elle implique la mise en œuvre d'une sécurité adaptée aux usages, économiquement viable et conforme à la législation.

Une politique doit être formalisée dans l'entreprise sous forme d'un document devant comporter un recueil des pratiques régissant la manière de gérer, de protéger et de transmettre les informations critiques ou sensibles appartenant à l'entreprise. La documentation sur la norme ISO 27001 et sa suite est l'ouvrage de référence permettant d'aider à la réalisation de ce référentiel.

Le principal objectif de la sécurité informatique étant de sauvegarder la pérennité de l'entreprise, c'est pourquoi la politique de sécurité mise en œuvre doit s'inspirer des besoins réels précédemment définis à partir des évaluations des actifs, des menaces et des vulnérabilités. La politique de sécurité impose une complémentarité entre les procédures, les outils mis en œuvre et les personnes impliquées.

Mise en place de cette politique :

Pour mettre en place une réglementation plus stricte et fixer des limites aux utilisateurs, il s'est avéré nécessaire de rédiger une charte informatique faisant partie intégrante de la réglementation intérieure de l'entreprise. Cette charte informatique est sensible puisqu'elle oblige

d'être en accord avec la législation et les lois afin de ne pas porter atteinte à la liberté et à la vie privée des salariés.

Cette charte informatique n'a pas été réalisée, car la direction ne souhaite pas obliger les utilisateurs à signer une charte de ce type et préfère les laisser « libres » sans leur imposer de contraintes.

Il ne serait alors donc pas judicieux de passer du temps à réaliser ce type de charte demandant beaucoup de temps, notamment au point de vue juridique, et de ne pas la voir être appliquée par la suite…

Comme nous venons de le voir, la sécurité utilisateur représente une partie très importante dans la sécurisation du système d'informations qu'il ne faut pas négliger. L'utilisateur peut, à lui seul, représenter une menace en effectuant volontairement ou involontairement des manipulations néfastes. Avant d'entamer toute action permettant de renforcer cette sécurité, il est nécessaire d'effectuer un audit afin de relever les points critiques sur lesquels travailler en premier. Suite à cet audit, il peut être judicieux de réaliser un guide des bonnes pratiques permettant ainsi d'informer l'utilisateur sur les risques encourus, tel que de renverser son café sur son poste de travail, de ne pas récupérer tout de suite ses impressions ou encore d'échanger des données avec son ordinateur personnel pouvant être vérolé. Bien plus que des bonnes pratiques, ce guide permet d'alerter les utilisateurs et de les rendre plus vigilants si quelqu'un leur demande leur mot de passe ou encore si une personne inconnue rôde dans les couloirs…

Conclusion

Après avoir vu l'ensemble du périmètre de la sécurisation d'un système d'information, nous pouvons nous rendre compte à quel point il est important de ne pas se concentrer uniquement sur une partie mais plutôt d'essayer d'avoir une vision plus globale. Il peut être parfois frustrant de ne pas sécuriser de manière optimum une partie, mais il faut mieux sécuriser l'ensemble du périmètre et obtenir ainsi un niveau de protection homogène.

Pour tester le réel degré de sécurité d'une infrastructure informatique et savoir rapidement quelles actions correctives mener et à quel coût, il s'avère judicieux d'effectuer un audit de sécurité par une société extérieure qui aura un point de vue plus « critique ». Cela représente, certes, un coût mais ce dernier se révèle nécessaire. Une fois les points du premier audit corrigés, il s'avèrerait judicieux d'en effectuer un nouveau afin de valider les améliorations apportées.

La sécurité au sein d'une entreprise passe souvent en second plan puisque cela ne représente pas un gain direct d'argent. Toutefois, il est important de rappeler régulièrement à la direction de l'entreprise les risques encourus. Ces risques sont souvent ignorés et pas évalués comme ils devraient l'être. L'investissement est difficile à justifier tant qu'une perte d'argent liée à un problème de sécurité n'a pas eu lieu, mais il faut impérativement sensibiliser les personnes pour prévenir ces derniers.

De par la rapidité de l'évolution et de la croissance informatique, il est important de garder une bonne communication entre la direction des systèmes informatiques (DSI) et la direction des services généraux (DSG). En effet, les moyens mis en œuvre pour assurer la sécurité, ainsi que le dimensionnement des moyens de protection doivent sans cesse être mis à jour au fil du temps. Un décalage peut s'installer et exposer la société à des risques importants d'incidents et d'arrêts d'exploitation. Aujourd'hui plus de 95 % des entreprises sont dépendantes de leur informatique.

Bibliographie

Ouvrages imprimés

Titre du livre : Sécurité informatique
Auteurs : L. Bloch et C. Wolfhugel
Edition : EYROLLES
Année de parution : Mai 2009

Titre du livre : La sécurité informatique
Auteur : Jean-François CARPENTIER
Edition : Editions ENI
Année de parution : Avril 2009

Ouvrage en ligne

Partie : **II.2 Réseau Interne**
Titre de l'ouvrage : Sécurité physique des éléments d'un réseau local
Auteur ou Organisme : CLUSIF
Disponible sur : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/SecPhysReseauLocal.pdf
Date de consultation : 29/01/2011

Partie : **II.2 Réseau Interne**
Titre de l'ouvrage : La Sécurité informatique
Auteur ou Organisme : Yves LESCOP
Disponible sur : http://ylescop.free.fr/mrim/cours/securite.pdf
Date de consultation : 29/01/2011

Partie : **II.2 Réseau Interne**
Titre de l'ouvrage : Sécurité Informatique – Attaques Informatique
Auteur ou Organisme : Jean-Olivier GERPHAGNON
Disponible sur : http://www.rederio.br/downloads/pdf/nt00700.pdf
Date de consultation : 30/01/2011

Partie : **II.2 Réseau Interne**

Titre de l'ouvrage : Administration d'un réseau local

Auteur ou Organisme : P. Pinault

Disponible sur : http://www.disk91.com/cours/unix/admin_base.pdf

Date de consultation : 30/01/2011

Partie : **Partie III. Sécurité logiciel**

Titre de l'ouvrage : Sécurité des logiciels

Auteur ou Organisme : CNRS Info

Disponible sur : www.cnrs.fr/Cnrspresse/math2000/pdf/Maths22.pdf

Date de consultation : 05/02/2011

Partie : **Partie III. Sécurité logiciel**

Titre de l'ouvrage : Protection et sécurité dans les systèmes d'exploitation

Auteur ou Organisme : Mourad LOUKAM

Disponible sur : http://www.loukam.net/SE_Master_Chapitre4.pdf

Date de consultation : 05/02/2011

Partie : **Partie III. Sécurité logiciel**

Titre de l'ouvrage : Sécurité dans les développements d'applications

Auteur ou Organisme : Eric DERONZIER

Disponible sur :

http://www.ysosecure.com/images/stories/Documents/Plan%20pr%C3%A9sentation%20Maintien%20de%20la%20S%C3%A9curit%C3%A9.pdf

Date de consultation : 06/02/2011

Schéma web

Partie : **II.1 Réseau Externe**

Titre de la page : Réseau privé virtuel

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

URL : http://upload.wikimedia.org/wikipedia/commons/thumb/0/0f/VPN_site-to-site.jpg/600px-VPN_site-to-site.jpg

Date de consultation : 15/01/2011

Illustrations

URL : http://orialis.fr/wp-content/themes/orialis2/sliderfile/images/finances-gestion.jpg

URL : http://www.planete-plus-intelligente.lemonde.fr/partners/ibm/cacheDirectory/HTMLcontributions/img/management.jpg

URL : http://www.google.com/about/datacenters/gallery/#/

URL : http://www.itespresso.fr/wp-content/uploads/2011/10/chiffrement-%C2%A9-Yong-Hian-Lim-Fotolia.com_.jpg

URL : http://www.opalean.com/wp-content/uploads/2011/10/S%C3%A9curit%C3%A9.jpg

Sites web

Partie : **I. Sécurité physique**

Titre de la page : Sécurité : Eviter aussi les risques physique !

Auteur ou Organisme : Acheteurs Info

Titre de la page d'accueil : Le guide l'acheteur – Votre plate-forme d'informations, pour faciliter vos démarches professionnelles !

Disponible sur : http://www.acheteursinfo.com/actualites_securite.html

Date de consultation : 08/01/2011

Partie : **I. Sécurité physique**

Titre de la page : Protéger ses infrastructures : la sécurité physique requiert des spécialistes

Auteur ou Organisme : Jérôme SAIZ – 01net

Titre de la page d'accueil : Actualités informatique

Disponible sur : http://www.01net.com/article/175234.html

Date de consultation : 08/01/2011

Partie : **I. Sécurité physique**

Titre de la page : Fiches de prévention des risques matériels

Auteur ou Organisme : Guide Informatique

Titre de la page d'accueil : Les actualités guide informatique

Disponible sur : http://www.guideinformatique.com/fiche-prevention_des_risques_materiels-437.htm

Date de consultation : 08/01/2011

Partie : **I. Sécurité physique**

Titre de la page : Dossier sur la sécurité physique

Auteur ou Organisme : Guide Informatique

Titre de la page d'accueil : Les actualités guide informatique

Disponible sur : http://www.guideinformatique.com/dossier-locaux_securite_physique-24.htm

Date de consultation : 09/01/2011

Partie : **II.1 Réseau Externe**

Titre de la page : Understanding VPN SSL

Auteur ou Organisme : Bhaven HARIA

Titre de la page d'accueil : Information Security Intelligence

Disponible sur : http://palisade.plynt.com/issues/2006Jul/ssl-vpn/

Date de consultation : 15/01/2011

Partie : **II.1 Réseau Externe**

Titre de la page : Réseau privé virtuel

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel

Date de consultation : 15/01/2011

Partie : **II.1 Réseau Externe**

Titre de la page : Réseaux privés virtuels - Vpn

Auteurs ou Organisme : Xavier LASSERRE, Thomas KLEIN et Sébastien FONTAINE

Titre de la page d'accueil : Le site de partage des connaissances du monde TCPIP

Disponible sur : http://www.frameip.com/vpn/

Date de consultation : 15/01/2011

Partie : **II.1 Réseau Externe**

Titre de la page : Réseau informatique

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/R%C3%A9seau_informatique

Date de consultation : 15/01/2011

Partie : **II.1 Réseau Externe**

Titre de la page : Intranet

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Intranet

Date de consultation : 16/01/2011

Partie : **II.2 Réseau Interne**

Titre de la page : La sécurité réseau interne

Auteur ou Organisme : Pink PACHIDERM – LINUX magazine France n°11

Titre de la page d'accueil : La sécurité réseau interne

Disponible sur : http://okki666.free.fr/docmaster/articles/linux047.htm

Date de consultation : 16/01/2011

Partie : **II.2 Réseau Interne**

Titre de la page : Wifi – Cours d'introduction

Auteur ou Organisme : Comment ça marche

Titre de la page d'accueil : Actualités informatique

Disponible sur : http://www.commentcamarche.net/faq/3020-wifi-cours-d-introduction

Date de consultation : 16/01/2011

Partie : **II.2 Réseau Interne**

Titre de la page : Wi-Fi

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Wi-Fi

Date de consultation : 16/01/2011

Partie : **II.2 Réseau Interne**

Titre de la page : Wired Equivalent Privacy

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Wired_Equivalent_Privacy

Date de consultation : 29/01/2011

Partie : **II.2 Réseau Interne**

Titre de la page : Wi-Fi Protected Access

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access

Date de consultation : 29/01/2011

Partie : **II.2 Réseau Interne**

Titre de la page : Filtrage par adresse MAC

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Filtrage_par_adresse_MAC

Date de consultation : 29/01/2011

Partie : **II.2 Réseau Interne**

Titre de la page : Qualité de service

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Qualit%C3%A9_de_service

Date de consultation : 29/01/2011

Partie : **II.2 Réseau Interne**

Titre de la page : ACL : Résumé théorique

Auteur ou Organisme : Cisco goffinet

Titre de la page d'accueil : Technologies des réseaux

Disponible sur : http://cisco.goffinet.org/s2/acl_resume/

Date de consultation : 30/01/2011

Partie : **II.2 Réseau Interne**

Titre de la page : Les Access Control List (ACL) : Qu'est-ce que c'est et comment s'en servir pour le filtrage réseau

Auteur ou Organisme : AidoWeb

Titre de la page d'accueil : Aide et Forum Informatique

Disponible sur : http://www.aidoweb.com/tutoriaux/les-access-control-list-acl-qu-c-comment-s-servir-filtrage-reseau-623

Date de consultation : 30/01/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Sécuriser son ordinateur et connaître les menaces

Auteur ou Organisme : Malekal's Site

Titre de la page d'accueil : Site entraide informatique

Disponible sur : http://www.malekal.com/2010/11/12/securiser-son-ordinateur-et-connaitre-les-menaces-2/

Date de consultation : 05/02/2011

Partie : **III. Sécurité logiciel**

Titre de la page : La sécurité logique

Auteur ou Organisme : Guide Informatique

Titre de la page d'accueil : Les actualités guide informatique

Disponible sur : http://www.guideinformatique.com/dossier-securite_logique_virus_et_intrusions-7.htm

Date de consultation : 05/02/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Logiciels de sécurité

Auteur ou Organisme : Guide Informatique

Titre de la page d'accueil : Sécurité internet

Disponible sur : http://eservice.free.fr/logiciel-securite.html

Date de consultation : 11/02/2012

Partie : **III. Sécurité logiciel**

Titre de la page : Logiciel malveillant

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Logiciel_malveillant

Date de consultation : 06/02/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Virus informatique

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Virus_informatique

Date de consultation : 06/02/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Machine zombie

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Machine_zombie

Date de consultation : 12/02/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Logiciel antivirus

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://fr.wikipedia.org/wiki/Logiciel_antivirus

Date de consultation : 12/02/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Malware

Auteur ou Organisme : Wikipédia

Titre de la page d'accueil : L'encyclopédie libre

Disponible sur : http://en.wikipedia.org/wiki/Malware

Date de consultation : 19/02/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Antivirus

Auteur ou Organisme : Clashinfo

Titre de la page d'accueil : Communauté informatique

Disponible sur : http://www.clashinfo.com/dico/definition-a/art92-antivirus.html

Date de consultation : 19/02/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Sécurité et protection des systèmes d'exploitation

Auteur ou Organisme : Benoît PAILLET

Titre de la page d'accueil : L'institut d'électronique et d'informatique Gaspard-Monge

Disponible sur : http://www-igm.univ-mlv.fr/~dr/XPOSE/Securite/

Date de consultation : 19/02/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Sécurité / Législation

Auteur ou Organisme : Comment ça marche

Titre de la page d'accueil : Actualités informatique

Disponible sur : http://www.commentcamarche.net/contents/security/

Date de consultation : 05/03/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Virus classiques

Auteur ou Organisme : Viruslist

Titre de la page d'accueil : Encyclopédie virus

Disponible sur : http://www.viruslist.com/fr/virusesdescribed?chapter=161595136

Date de consultation : 05/03/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Descriptions des Programmes Malicieux

Auteur ou Organisme : Viruslist

Titre de la page d'accueil : Encyclopédie virus

Disponible sur : http://www.viruslist.com/fr/virusesdescribed

Date de consultation : 05/03/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Exposé sur les virus informatiques

Auteur ou Organisme : V.D

Titre de la page d'accueil : TECFA Education & Technologies

Disponible sur : http://tecfa.unige.ch/staf/staf-j/diego/staf14/ex8/virus.html

Date de consultation : 05/03/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Anti-Spyware : Supprimer les Logiciels Espions et s'en Protéger

Auteur ou Organisme : eservice

Titre de la page d'accueil : Sécurité internet

Disponible sur : http://eservice.free.fr/lo-anti-spyware.html#sousleresume

Date de consultation : 05/03/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Arsenal Anti-Spam : Filtre, Logiciel ou Service Web Antispam

Auteur ou Organisme : eservice

Titre de la page d'accueil : Sécurité internet

Disponible sur : http://eservice.free.fr/lo-anti-spam.html#sousleresume

Date de consultation : 12/03/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Cours VB.Net - Diverses sortes de programmation

Auteur ou Organisme : Developpez

Titre de la page d'accueil : Club des professionnels de l'informatique

Disponible sur : http://plasserre.developpez.com/cours/vb-net/?page=bonnes-pratiques1#LXVI-A-6

Date de consultation : 12/03/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Instructions de codage sécurisé

Auteur ou Organisme : MSDN

Titre de la page d'accueil : Microsoft

Disponible sur : http://msdn.microsoft.com/fr-fr/library/8a3x2b7f.aspx

Date de consultation : 12/03/2011

Partie : **III. Sécurité logiciel**

Titre de la page : Instructions de codage sécurisé

Auteur ou Organisme : MSDN

Titre de la page d'accueil : Microsoft

Disponible sur : http://msdn.microsoft.com/fr-fr/library/8a3x2b7f.aspx

Date de consultation : 12/03/2011

Partie : **Partie IV. Sécurité Utilisateur**

Titre de la page : Démarche ITIL

Auteur ou Organisme : Energit

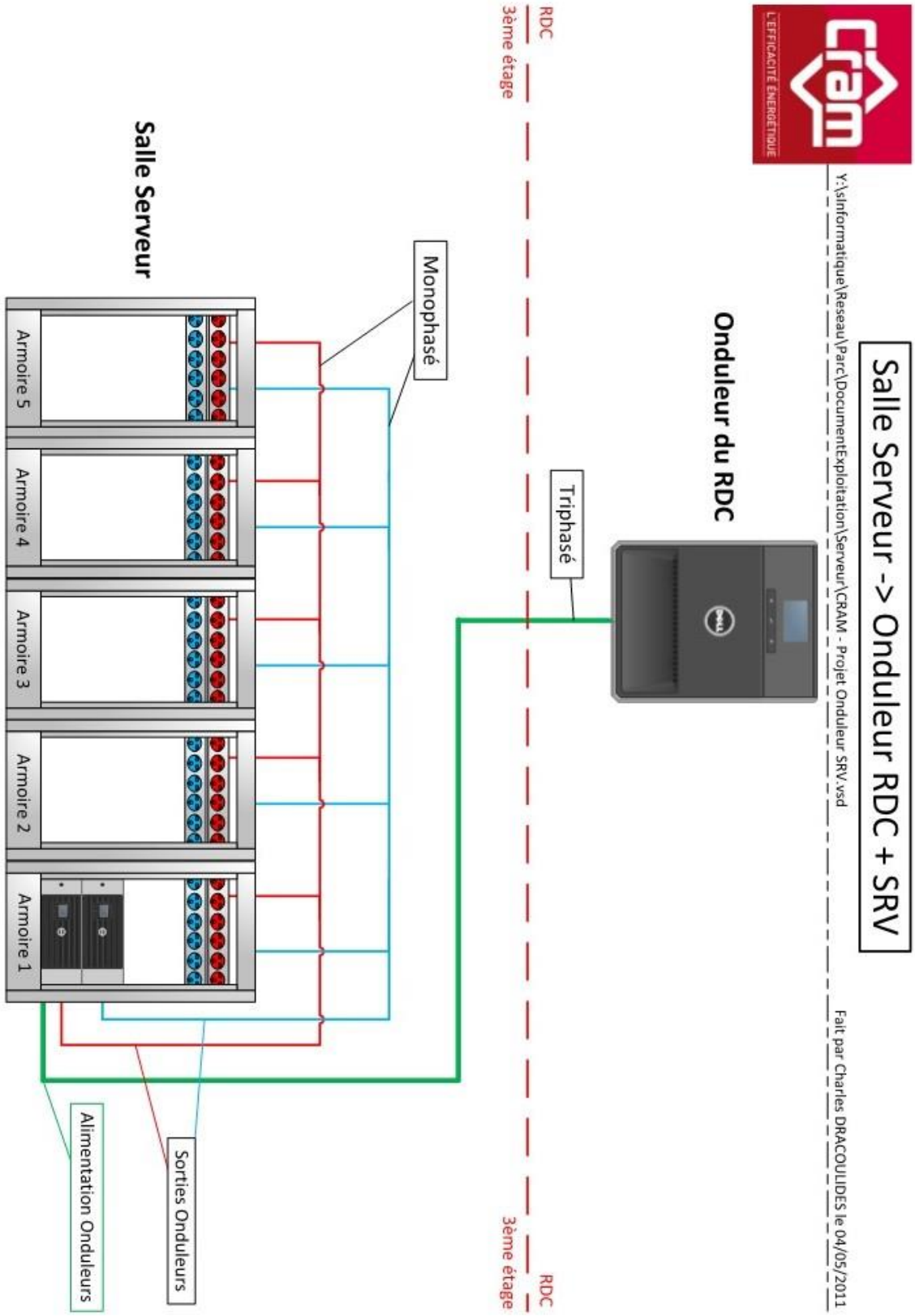
Titre de la page d'accueil : Votre référent Green for IT & IT for Green

Disponible sur : http://energit.fr/document.php?idCateg=8&id=7&PHPSESSID=21a634a44a4636aed33178d0536d8ddf

Date de consultation : 02/04/2011

Table des annexes

Annexe 1 – Schéma électrique de la salle serveur du siège de l'entreprise



Annexe 2 – Questionnaire utilisateurs

Questionnaire pour la mise en place d'une politique de sécurité

Ce questionnaire est anonyme, il servira à réaliser des statistiques.

1. **Utilisation des outils**

   a. **Messagerie**

   Regardez-vous toujours l'expéditeur et le contenu du message avant d'ouvrir une pièce jointe ?

   ◘ Oui ◘ Non

   b. **Imprimantes**

   Allez-vous chercher immédiatement vos documents aux copieurs, imprimantes ?

   ◘ Oui ◘ Non

   Si non :

   Dans quel laps de temps en moyenne allez-vous les chercher ?

   ◘ 5 min
   ◘ 10 min
   ◘ 15 min ou plus

   c. **Absence**

   Verrouillez-vous votre session si vous allez être absent pour une durée de plus de 15 min ? (à chaque fois que vous quittez votre poste des yeux | le faites-vous quand vous quittez votre poste pendant plus de 10 min ?)

   ◘ Oui ◘ Non

   d. **Sites visités**

   Les sites que vous visitez sont-ils populaires et connus ?

   ◘ Oui ◘ Non

   Quel type d'informations recherchez-vous le plus souvent sur internet ?

   ……

   e. **Téléchargement**

   Connaissez-vous toujours la provenance de vos téléchargements (documents, pièces jointes, logiciels) ?

   ◘ Oui ◘ Non

f. Multimédia

Utilisez-vous des téléphones, clés USB, disque dur externe ou autre périphérique sur votre station de travail ?

◘ Oui ◘ Non

Envoyez-vous des mails via votre adresse de messagerie personnelle à la CRAM ?

◘ Oui ◘ Non

Si oui, est-ce dans un usage professionnel ?

◘ Oui ◘ Non

2. Mots de passe

Avez-vous déjà changé votre mot de passe ?

◘ Oui ◘ Non

a. Fiabilité

Votre mot de passe comporte-t-il au moins 7 caractères ?

◘ Oui ◘ Non

Comporte-t-il également des symboles et des lettres majuscules ?

◘ Oui ◘ Non

Est-il facile à trouver (nom de votre enfant, animal de compagnie, etc.) ?

◘ Oui ◘ Non

b. Fréquence du changement

A quelle fréquence changez-vous votre mot de passe ?

◘ 1 fois par trimestre ◘ 1 fois par mois ◘ 1 fois par an ◘ Jamais

c. Confidentialité

Avez-vous marqué votre mot de passe aux alentours de votre station de travail ?

◘ Oui ◘ Non

Qui dans votre entourage connait votre mot de passe ?

◘ Famille
◘ Collègues
◘ Personne

3. Travail à domicile

Travaillez-vous souvent en dehors de l'entreprise sur des sujets de la CRAM en utilisant l'outil informatique ?

- ◘ Oui : à quelle fréquence ?.....
- ◘ Non

Si oui,

Utilisez-vous des clés USB, des CD pour échanger vos fichiers ?

◘ Oui ◘ Non

Ces supports contiennent-ils que des informations professionnelles ?

◘ Oui ◘ Non

Utilisez-vous votre adresse mail personnelle pour échanger des fichiers avec la CRAM ?

◘ Oui ◘ Non

4. Sécurité physique

Buvez-vous souvent à proximité de votre poste de travail ?

◘ Oui ◘ Non

Parlez-vous aux personnes qui semblent perdues ou qui cherchent quelqu'un?

◘ Oui ◘ Non

Si une personne appelle et vous demande des données que faites-vous ?

- ◘ Demande de présentation ◘ Vous ne lui donnez pas
- ◘ Vous donnez les informations à un membre du service concerné que vous connaissez

5. Types d'informations

Préféreriez-vous être informé de la politique de sécurité par :

- ◘ Mails
- ◘ Formation
- ◘ Guide pratique

6. Propositions

Si vous avez des remarques ou des propositions à faire :

……
……
……
……

Le service Informatique

Annexe 3 – Guide Des Bonnes Pratiques Informatiques

Guide Des Bonnes Pratiques Informatiques

Quels risques encourez-vous ?

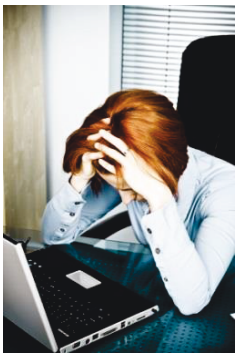
- La perte de documents électroniques

Des logiciels tels que les virus peuvent supprimer une partie ou la totalité de vos documents sauvegardés sur votre poste.

- Le vol d'informations

Plus connu sous le nom d'espionnage industriel, cette technique permet à des concurrents de récupérer des informations cruciales telles que des appels d'offre, des contrats, prospects, etc.

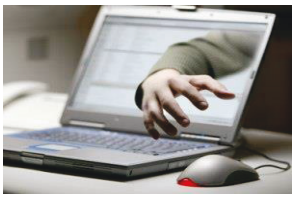
- Utilisation impossible de votre poste



Une personne mal intentionnée peut très bien prendre le contrôle de votre poste et faire en sorte que ce dernier devienne inutilisable.

Vous pouvez aussi rendre inutilisable votre ordinateur si par inadvertance vous renversez votre boisson dessus.

- Utilisation frauduleuse de votre machine



Une personne connaissant vos identifiants peut, par exemple, se servir de votre compte pour télécharger des

programmes malveillants ou des fichiers infectés ou envoyer des mails à votre nom, ouvrir vos documents enregistrés sur le réseau, etc.

Pour votre enrichissement personnel

- Pourquoi font-ils cela ?

- Cupidité
- Vengeance/rancune contre une société concurrente ou son ancien employeur
- Défis intellectuels & abus

Les personnes malveillantes arrivent à attaquer des ordinateurs, des banques, des sociétés, des universités via votre poste et en cumulant la puissance de l'ensemble des PC qu'ils ont infectés.

- Leurs techniques

❖ Les virus

Logiciel s'attachant aux documents électroniques pouvant par la suite être mis sur des disques, des clés USB dont le but est souvent offensif. Un virus a dans tous les cas besoin d'une intervention humaine pour se propager.

❖ Les vers

Contrairement aux virus, les vers se propagent de manière autonome. Ils peuvent être envoyés via des téléphones mobiles par l'intermédiaire du Bluetooth sous forme d'un message ou d'un fichier vidéo.

❖ Les spams ou phishing

C'est un courrier électronique envoyé à un grand nombre de personnes sans leur accord préalable. La personne mal intentionnée peut falsifier des courriers électroniques et des sites internet.

Le SPAM est utilisé pour obtenir, à l'insu de l'internaute, des coordonnées bancaires, des informations d'identification d'un site de vente en ligne, etc.

❖ Les trappes (Porte dérobée dans un système informatique.)

Il s'agit en général d'un programme caché ou d'un composant électronique rendant le système de protection d'un ordinateur inefficace lorsque lui sont envoyées certaines commandes (uniquement connues des hackers).

❖ Les chevaux de Troie (ou backdoors)

Programme bénin (jeux, documents…) que nous nommerons « A » cachant un autre programme nommé « B » qui lui est malveillant.

Lorsque le programme « A » est exécuté alors le programme « B » s'exécute en arrière-plan et ouvre ainsi une « porte » dans votre ordinateur afin de permettre l'exécution de code malveillant.

❖ Les logiciels espions (spywares)

Ces logiciels collectent des informations de votre PC et les envoient (à votre insu) à une personne malveillante, il en existe deux types :

- **Les adwares** sont des logiciels d'affichage de publicités dont les trois but principaux sont de :
  - gagner de l'argent (via les publicités)
  - ralentir votre PC (ouverture permanente de fenêtres publicitaires)
  - générer une perte de temps (obligation de fermer toutes les fenêtres à la main)

Exemple d'écran infesté par un adware

- **Les malwares** sont plus dangereux puisqu'ils collectent les mots de passe et les informations sensibles.

On retrouve essentiellement ces logiciels espions sur internet dans des fichiers d'installations de logiciels. Ils peuvent aussi être installés sur votre PC après leur piratage, si la personne malveillante trouve une faille dans votre ordinateur.

❖ Les logiciels de brute force

Afin de trouver le mot de passe de votre messagerie ou de votre ordinateur, ce logiciel essaye toutes les combinaisons possibles, avec différents alphabets (minuscules, minuscules et MAJUSCULES, caractères spéciaux…).

Comment se protéger ?

-Verrouiller sa session

- Verrouiller votre session est une bonne sécurité pour protéger vos informations.

  Il suffit de faire les combinaisons de touches suivantes :
  - Windows + ℓ
  - Ctrl + Alt + Sup puis déverrouiller et saisir votre mot

- Changer son mot de passe

- Le changer au moins 2 fois par an pour plus de sécurité
- 8 caractères est la longueur minimale pour qu'un mot de passe soit plus difficile à casser
- Vous devrez intégrer des symboles : ?/§ !;ù*µ%$£ pour que votre mot de passe soit plus dur à casser par les 'pirates'

Temps moyen d'un « pirate » pour trouver votre mot de passe de 8 caractères selon l'écriture choisie

Alphabets possibles	Nombre de possibilités	Temps de découverte de votre mot de passe
Caractères spéciaux	95 caractères	33 ans
Lettres et nombres	62 caractères	1 an
Lettres	52 caractères	96 jours
Minuscules avec 1 majuscule	26 & 1 lettre spéciale	3 jours
Minuscules	26 caractères	9h

orange : bon **orange clair : moyen** **blanc : mauvais**

- Clés USB de la CRAM

- Disponible en prêt au service informatique
- Toujours tenir votre ordinateur personnel à jour pour éviter les virus sur les clés USB de la CRAM (utiliser un antivirus et des logiciels comme des anti-spams et/ou des anti-malwares (la suite Microsoft Security Essential par exemple)).
- **Si vous trouvez une clef USB, donnez-la au service informatique, elle peut être contaminée par des virus !**

- L'imprimante

Aller directement aux copieurs & aux imprimantes afin d'éviter de laisser les documents (confidentiels ou non) à la vue de tous

- L'ingénierie sociale

Technique ayant pour but d'extirper des informations à des personnes sans qu'elles ne s'en rendent compte via les moyens suivant :

- *Par téléphone*
- *Par lettre*
- *En contact direct*

Si une personne inconnue vous appelle en vous disant qu'elle fait partie de la CRAM et qu'elle souhaiterait connaître votre date de naissance, ou tout autre donnée confidentielle à votre sujet, NE LUI COMMUNIQUEZ PAS !

Merci d'en informer immédiatement votre supérieur hiérarchique.

➔ Se méfier du contenu

• Des pages d'authentification

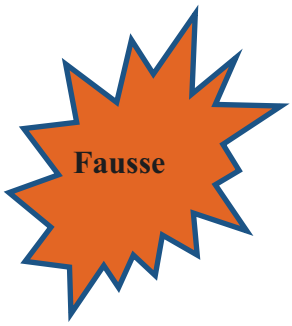
Les pages sécurisées comportent toujours un cadenas dans la barre des adresses URL ou en bas à droite de la page cela dépend du navigateur (Internet Explorer, Google Chrome, Safari, etc.).

Le site est sécurisé avec le cadenas et le certificat pour l'origine du site.

• Des pages Internet

- Les pages qui suivent sont des exemples de falsification des sites internet :
  - au niveau du rendu visuel, du design
  - de la barre d'adresses internet ou URL

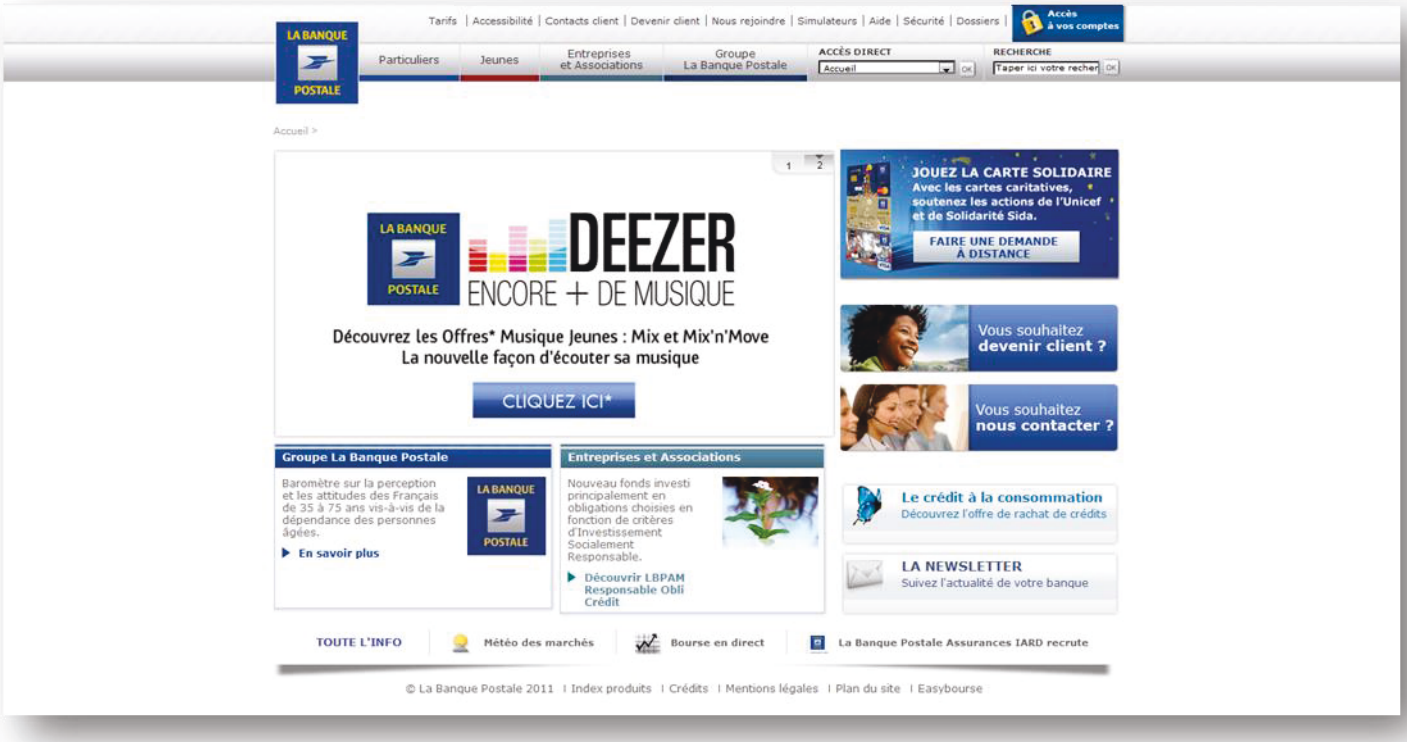
<u>La vraie page est :</u>



www.fr-banquepostale.tk

La vraie page est :

LA BANQUE POSTALE [FR] https://www.labanquepostale.fr/index.html



• Des courriers électroniques

- Vérifier le ou les expéditeurs
- Vérifier le contenu du message

Attention à l'orthographe qui peut révéler les faux courriels.

Ne pas ouvrir de pièce jointe envoyée par courriel d'un expéditeur inconnu.

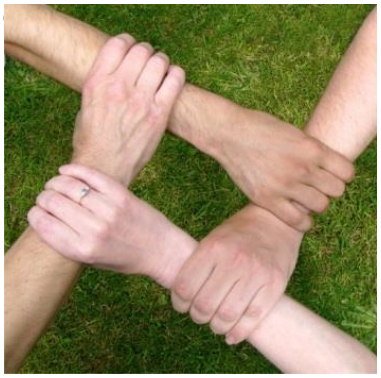
En cas de doute, merci de contacter l'émetteur ou le service informatique.

• Des téléchargements

Ne pas télécharger un logiciel sans en avoir informé le service informatique.

Si vous téléchargez un document, faites attention à la source.

Attention aussi aux faux logiciels souvent proposés via des bannières publicitaires.



➔ Pratique

• Le travail à domicile

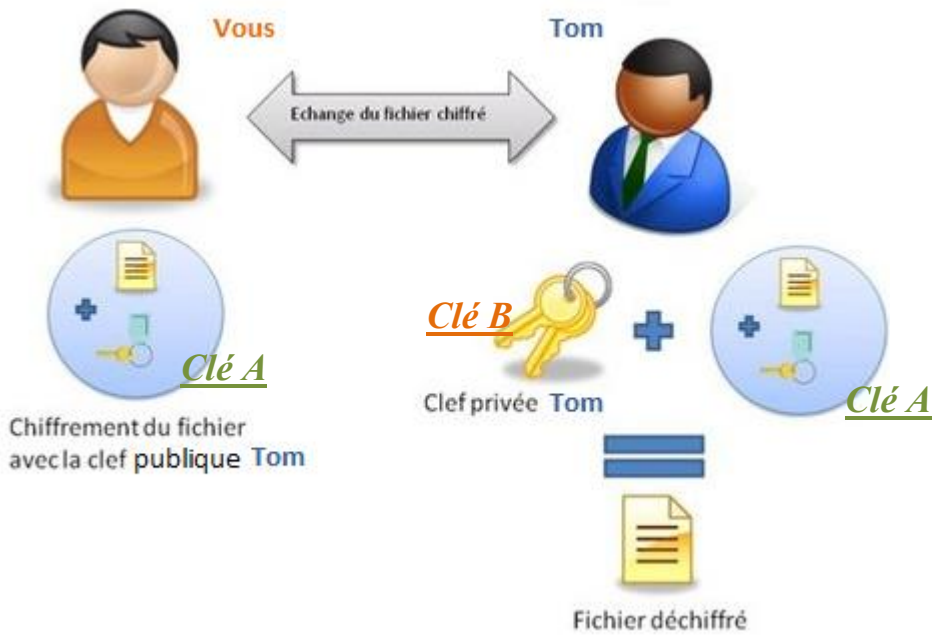
En termes de confidentialité, un courriel peut être comparé à une carte postale pouvant être lue par tous.

➔ Si vous utilisez votre adresse électronique, chiffrez vos messages

TOM vous a envoyé sa ***clé A*** [publique] **pour chiffrer le mail** que vous voulez lui envoyer.

Pour déchiffrer les mails que vous lui avez envoyés, il a besoin de sa ***clé B*** [privée] qui lui a été donnée à garder précieusement.

Ce système de double clé est appelée méthode de chiffrement asymétrique.



➔ Si vous employez des clés USB, chiffrez les documents

Merci de votre attention,

Pour toute question, le service informatique est là pour vous aider.

➔ Lexique

- **Abus :**

Divulgation, altération, pertes, accès illicite, indisponibilité des services de la CRAM.

- **Faille :**

Vulnérabilité permettant à des attaquants d'obtenir un accès non autorisé à un système.

- **Information :**

Elément de connaissance susceptible d'être conservé, traité ou transmis à l'aide d'un support et d'un mode de codification normalisé pour faciliter sa diffusion et sa communication par une ou plusieurs personne(s) au sein de la CRAM agissant sur son environnement.

Les photos, les courriers électroniques, les notes, les mots de passe sont des informations.

- **Risque :**

Possibilité qu'une menace interne (mauvaises manipulations, erreurs humaines) ou externe (programmes malveillants, hackers que l'on nomme pirates d'internet …) exploite une vulnérabilité créeant un impact financier et économique avec la divulgation et/ou la fuite d'information.

- **Risque résiduel :**

Risque qui subsiste après application des précautions et contre-mesures servant à réduire le risque.

- **Sécurité :**

La qualité d'être protégé contre des abus, des risques.

Liste des figures

Liste des tableaux

Etude de l'ensemble de la sécurisation d'un système d'information au sein d'une société.

Mémoire d'Ingénieur C.N.A.M, Le Havre 2013

RESUME

La sécurité informatique au sein d'un système d'information n'est jamais une priorité jusqu'au jour où un incident se produit et génère une perte financière plus ou moins importante pour l'entreprise.

Dans cette étude, sont détaillés les différents périmètres permettant une bonne sécurisation du système d'information puisqu'il est inutile de sécuriser de façon approfondie un périmètre si les autres ne le sont pas du tout ! Il sera alors plus judicieux de sécuriser l'ensemble des périmètres plutôt qu'un seul.

Les différentes parties traitées sont : la sécurité physique, la sécurité des réseaux, la sécurité logicielle puis la sécurité utilisateur.

Mots clés : sécurité informatique, sécurité physique, sécurité des réseaux, sécurité logicielle, sécurité utilisateur

---

SUMMARY

Information security within an information system is never a priority until an incident occurs and generates a financial loss more or less important for the company.

In this study, are detailed the various perimeters allowing a good security of the information system because it is useless to secure correctly one perimeter if the others are it not at all! He will then be more sensible to secure all the perimeters rather than only one.

The different parts are : physical security, network security, software security and users security.

Key words : IT security, physical security, security of networks, software security, users security