MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE NATIONALE SUPÉRIEURE DE MANAGEMENT ENSM.

Pôle Universitaire de KOLÉA

MEMOIRE DE FIN D'ETUDES

Master en management stratégique et système d'information

Thème :

AUDIT DE SÉCURITÉ DU SYSTEME INFORMATIQUE

CAS : SIEM OOREDOO ALGERIE.

Elaboré par : MESSEKDJI Mimi. **Encadré par : Dr TOUMI Djamila.**

Année universitaire 2021/2022

Résumé

A l'heure du numérique, l'importance des systèmes d'information dans les entreprises n'est plus à démontrer. Celles-ci utilisent de manière intensive et investissent lourdement dans les technologies et systèmes. Mais ces systèmes sont vulnérables et sont exposés à différents risques. A cet effet les organisations sont appelées à faire face à ces risques, par l'élaboration de politiques et procédures adéquates afin d'assurer la sécurisation de ses systèmes.

Mots clés

Audit, Politique de l'information, RSSI (Responsable de la sécurité des systèmes d'information), Sécurité, Actifs informationnels.

ABSTRACT

In the digital âge, the importance of information Systems in compagnies Is Wella established. They make intensive use of and invest heavily in technologies and systems. But these systems are vulnerable and exposed to different risks. To this end, organisations are called upon to face these risks, by developing appropriate policies and procedures to ensure the security of its systems.

Keywords

Audit, Information Policy, RSSI (Head of Information Systems Security), Security, Information Assets.

ملخص

في العصر الرقمي، أصبحت أهمية نظم المعلومات في الشركات راسخة. وهي تستخدم التكنولوجيات والنظم بكثافة وتستثمر فيها بكثافة. لكن هذه الأنظمة معرضة للخطر ومعرضة لمخاطر مختلفة. ولهذه الغاية، تُدعى المنظمات إلى مواجهة هذه المخاطر، من خلال وضع سياسات وإجراءات مناسبة لضمان أمن أنظمتها.

الكلمات الرئيسية

مراجعة الحسابات . سياسة المعلومات . رئيس امن نظم المعلومات. الامن. نظم المعلومات

REMERCIEMENTS

Je remercie le grand dieu tout puissant pour m'avoir accordé la force et le courage pour accomplir ce travail. Je voudrais exprimer ma profonde reconnaissance à mon père, ma mère et ma sœur qui m'ont aidé et encouragé tout au long de mon parcours.

Mes reconnaissances à Mme TOUMI Djamila pour son encadrement, sa disponibilité, ses conseils et son soutien tout au long de l'élaboration de mon mémoire.

Mes vifs remerciements à tous mon encadrante de stage Mme. Baha YADEL pour son chaleureux accueil, et pour son écoute et sa disponibilité tout au long de la réalisation de ce travail.

Je tiens à exprimer toute ma reconnaissance à M.Boucheloukh Mohamed Faouzi mon prof de l'ENSM pour son aide et sa disponibilité.

Et enfin je tiens à remercier tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations, sigles et acronymes

Abréviation	Désignation
SI	**Système informatique**
RSSI	**Responsable de la sécurité du système d'information**
SMSI	**Système de management de sécurité de l'information**
SIEM	**Security information and event management**
SSI	**Sécurité du système informatique**

INTRODUCTION GENERALE

L'information est un actif précieux des entreprises. A ce titre, il faut la protéger contre la perte, l'altération et la divulgation. Les systèmes qui la supportent doivent, quant à eux, être protégés contre l'indisponibilité et l'intrusion. Les entreprises doivent impérativement adopter des mesures de contrôle, c'est-à-dire élaborer des méthodes, politiques et procédures qui garantissent la protection de ses éléments d'actif, la précision et la fiabilité de ses enregistrements et la conformité de ses normes de gestion. Pour mesurer l'efficacité du contrôle, les entreprises doivent effectuer des vérifications complètes et systématiques. Un audit des systèmes d'information permet de repérer tous les contrôles qui régissent les systèmes d'information et d'évaluer leur efficacité.

L'audit des systèmes d'information couvre des domaines divers. Il peut porter, par exemple, sur :

- Le pilotage des systèmes d'information ;
- La sécurité informatique ;
- La production informatique ;
- Des applications informatiques en service ;
- Le support utilisateurs et de la gestion du parc informatique ;
- La fonction études ;
- Des projets ;

Notre étude est axée autour de l'audit de la sécurité informatique en utilisant la norme ISO 27001. Notre choix pour cette thématique est motivé par le fait que la sécurité informatique est un sujet d'actualité majeur.

Pour mieux comprendre cette étude notre problématique s'articule autour de la question suivante :

«Dans le cadre de la sécurité du système informatique, comment évaluer l'efficacité des moyens de contrôle mises en place par l'organisation pour faire face aux risques et menaces informatiques ? »

Nous avons effectué notre stage auprès de l'entreprise OOREDOO ALGERIE, la pertinence de ce terrain est justifiée par le fait de cette entreprise de services est tenue impérativement de sécuriser son système informatique ;

Dans le cadre de notre mémoire, nous nous sommes intéressés à l'évaluation des procédures mises en œuvre par cette entreprise dans ce but. Notre intérêt est étroitement lié à la thématique de notre mémoire.

Dans un premier temps, nous avons adopté la méthode descriptive basée sur la consultation d'ouvrages et d'articles ainsi que des thèses divers dont l'objet est de faire un cadre théorique., et nous avons opté pour une enquête basée sur les entretiens avec les agents concernés combinée à l'exploitation des documents internes de même que l'observation de la réalité ; afin d'analyser et d'interpréter les informations recueillies

Notre travail est structuré de la façon suivante :

Dans le premier chapitre qui s'articule sur la revue littérature et le cadre conceptuel de ce projet pour mieux définir les notions et théories de notre recherche afin de comprendre l'importance ces deux notions dans l'organisation.

Et le deuxième chapitre sera consacré à la présentation dans la section une au choix méthodologique, les outils de collecte et d'analyse d'information et la section suivante portera sur le contexte organisationnel, nous présenterons dans cette section l'organisme d'accueil, la fonction sécurité informatique au niveau de l'organisation et sa mission aussi, et une présentation du responsable de cette fonction sera abordée.

Enfin dans le dernier chapitre, dont l'intitulé est résultat et discussions, nous allons présenter les résultats des entretiens.

CHAPITRE 01: Revue de la littérature et cadre conceptuel

1. REVUE DE LITTERATURE

Dans le cadre de notre mémoire de fin d'études, nous avons pris connaissance de certaines publications universitaires et de contributions recueillies dans des revues spécialisées traitant de la sécurité informatique, en rapport avec notre mémoire de fin d'études dont la thématique est : l'Audit de sécurité informatique.

1.1. Article réalisé par Kenneth Laudon :

Kenneth Laudon est professeur de système d'information à la Stern School of business de l'université de New York.

L'intitulé ce cet article est : **La sécurisation d'un SI une exigence absolue.**

Selon l'auteur, La sécurisation d'un SI est une exigence permanente. Elle requiert des actions organisationnelles, techniques et juridiques auprès de nombreuses parties prenantes (dirigeants, salariés, clients, fournisseurs, etc..). Elle concerne d'abord les données en tant qu'actif clé de l'entreprise, mais aussi les logiciels et les matériels, qu'ils soient accessibles localement ou à distance. Les préjudices que subissent les entreprises suite à des défaillances de la sécurité de leur SI peuvent provenir d'actes internes, mais la part externe est croissante, via Internet. La cybercriminalité est avant tout à finalité financière. Elle utilise toutes les failles du SI et les technologies toujours en évolution (spamming, phishing, virus, cookies, etc.). Un SI étant une construction de composants et de sous-systèmes hétérogènes (matériels centraux et terminaux, réseaux, logiciels, etc…) et de provenances multiples (constructeurs, éditeurs, etc…), tout changement qui affecte l'un de ses composants est un risque d'affaiblissement du niveau de sécurisation antérieurement atteint.

Des méthodes et outils préventifs de contrôle et d'audit de la sécurité du SI existent, et leur mobilisation peut être coordonnée sous la responsabilité du responsable de la sécurité du système informatique de l'entreprise (RSSI). La

nécessaire continuité opérationnelle de l'entreprise, même en cas de sinistre informatique, requiert de disposer d'un plan global de reprise d'activité régulièrement actualisé et testé.

1.2. Article réalisé par le docteur Amir DJENNA, intitulé : La création en Algérie d'une Ecole Supérieure en Cyber sécurité, une nécessité absolue.

Le Docteur Amir Djenaa est expert-spécialiste en cyber sécurité. Université de Constantine.

Dans cet article, l'auteur milite pour la création en Algérie d'une Ecole Supérieure en Cyber sécurité.

L'auteur débute sa contribution en soulignant un développement très accéléré et une évolution spectaculaire du numérique. Il met en exergue le fait que la technologie d'Internet s'est développée de façon exponentielle depuis sa création. Cependant, cette avancée technologique se heurte à de nombreux problèmes de sécurité qui constituent une menace accablante.

L'auteur constate que devant l'ampleur des menaces, il y a les cyber attaques de très haut niveau : Stone, NotPetya, Sam-Sam, Memcached, Mirai et Wanna Cry (la liste n'est évidemment pas exhaustive).

L'auteur cite des cas concrets avec de lourdes conséquences. Parmi la série des cybers attaques célèbres, inédites qui a marqué l'histoire jusqu'à présent, il cite chronologiquement les cas ci-dessous :

- En 2010, Stuxnet, un malware très sophistiqué contre les centrifuges nucléaires des systèmes industriels en Iran ;

- En 2012, Shamoon, un maliciel enregistré contre les compagnies d'hydrocarbures en Arabie Saoudite ;

- En 2014, BlackEnergy, cyberattaque de déni de service contre les centrales électriques en Allemagne ;

- En 2015, BlackEnergy, cyberattaque de déni de service contre les centrales électriques et les réseaux intelligents en Ukraine ;

- En 2016, Mirai, cyberattaques contre les objets connectés au niveau mondial ;

- En 2017, WannaCry, cyberattaques contre les CPS/Cyber santé à l'échelle mondiale ;

- En 2020, SolarWinds, cyberattaque à grande échelle débutée en mars 2020, réalisée via une mise à jour compromise de la plateforme de gestion et de supervision. Parmi les victimes : des institutions gouvernementales, Microsoft, FireEye, Palo Alto Networks, Malwarebytes et Mimecast.

- Février 2021, Ransongiciel contre les CPS santé : l'Hôpital de Oloran-Sainte-Marie en France était victime de cette cyberattaque, par laquelle le système d'information était paralysé, aucune application n'était en service et aucune connectivité réseau interne ou externe n'était disponible.

Dans ce contexte, l'auteur estime que l'amélioration de la posture de cyber sécurité est une question extrêmement urgente. Il existe donc un besoin crucial en ressources humaines pour pouvoir produire des compétences capables de concevoir et de mettre en place des contre-mesures résilientes et efficaces pour la détection, l'atténuation et la prévention.

Le cyber sécurité est un sujet capital pour la sécurité du patrimoine, du territoire et de la Nation.

C'est dans cette optique que la création d'une Ecole Supérieure en tant que pôle d'excellence en cyber sécurité relève d'une nécessité absolue.

1.3. Article réalisé par Cyril André :

L'intitulé de cet article est **: Audit des systèmes d'information, cet article a pour but de souligner les bénéfices obtenus par l'audit des systèmes d'information.**

Dans cet article, l'auteur a montré l'importance de disposer d'un système d'information bien sécurisé, afin de garantir son efficacité dans le but d'assurer la sécurisation des actifs informationnels de l'entreprise, et pour permettre également une prévention des risques.

L'auteur a démontré qu'un audit des systèmes d'information nous permet d'avoir une visibilité sur le degré de sécurisation du système informatique que dispose l'entreprise, et de nous permettre notamment d'avoir une connaissance sur la capacité de l'entreprise à faire face aux différents risques.

2. CADRE CONCEPTUEL

Cette deuxième section s'articule autour des points suivants :

Cette section sera consacrée au cadre conceptuel dans laquelle nous présenterons dans un premier temps, et d'une façon succincte, les systèmes d'information, et l'infrastructure technologique du SI et ses plateformes. Ensuite nous introduirons la sécurité informatique. Après avoir donné une définition de la sécurité informatique, nous présenterons essentiellement les principaux défauts de la sécurité informatique, les failles de la sécurité informatique, les systèmes de protection. Nous parlerons également des exigences juridiques et règlementaires. Enfin, le rôle de l'audit dans le processus général de contrôle en utilisant la norme ISO 27001 sera abordé.

2.1 Section 01 : Les systèmes d'informations informatisés formels, et l'infrastructure technologiques du SI

2.1.1 Présentation des Systèmes d'information informatisés formels :

Techniquement, un système d'information (noté SI) se définit comme un ensemble de composantes inter reliées qui recueillent (ou récupèrent) de l'information, la traitent, la stockent et la diffusent afin d'aider à la prise de décision, à la coordination et au contrôle au sein d'une organisation.

Les SI contiennent des informations sur des personnes, des lieux et des objets importants dans l'organisation ou dans son environnement. Le terme « information » recouvre les données présentées sous une forme utile et utilisables par les personnes. Les « données », au contraire, sont des valeurs à l'état brut représentant des évènements qui ont eu lieu dans ou en dehors des organisations. Elles n'ont pas encore été organisées de façon à ce que les utilisateurs puissent les comprendre et s'en servir.

Dans un SI, trois activités participent à la production de l'information nécessaire à l'organisation : l'entrée, le traitement et la sortie. L'entrée est le

processus au cours duquel les données brutes sont données au système en provenance de l'organisation ou de son environnement. Le traitement est le processus qui transforme ces données brutes pour leur donner un sens. La sortie est le processus de diffusion de l'information traitée aux utilisateurs qui en ont besoin. Un SI se fonde également sur la rétroaction, c'est-à-dire le processus de transmission des informations de sorties aux utilisateurs appropriés pour les aider à évaluer l'étape antérieure et à y intervenir de nouveau si besoin (pour mise à jour, par exemple).

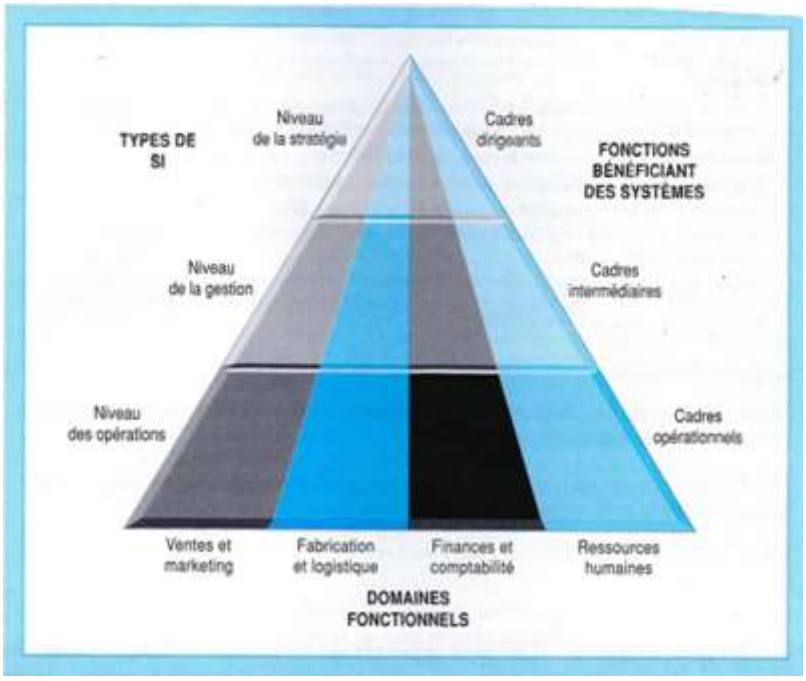
Les systèmes formels sont fondés sur des définitions établies, des procédures de collecte, de stockage, de traitement, de diffusion et d'utilisation de données. Ils sont structurés, c'est-à-dire qu'ils fonctionnent conformément à des règles prédéterminées relativement stables et difficiles à modifier.

Les systèmes informatisés utilisent et dépendent des technologies informatiques (matérielles et logicielles).

Bien que les SI informatisés se fondent sur la technologie informatique pour traiter des données brutes et les transformer en informations signifiantes, il faut distinguer, d'une part, les éléments qui constituent les infrastructures de nature technique (matériels et logiciels de base) et, d'autre part, le SI qui englobe les données et les usages faits de toutes ces potentialités technologiques. Les logiciels et les ordinateurs qui les supportent sont le fondement technique, les outils le substrat des SI modernes. Les ordinateurs et les réseaux sont le support matériel nécessaire au fonctionnement des logiciels. Ces derniers sont des ensembles d'instructions d'exploitation qui définissent, exécutent et contrôlent le traitement informatisé. Il convient d'en connaître les principes de fonctionnement et les potentialités pour concevoir des solutions, à la fois ambitieuses et réalistes, aux problèmes organisationnels. Pour comprendre les SI, il faut saisir les problèmes qu'ils doivent résoudre, leurs éléments

architecturaux et conceptuels, ainsi que les processus organisationnels qui mènent aux solutions.

Figure 1: La pyramide des types de systèmes présents dans une organisation



Source : Management des systèmes d'information p48 Par l'auteur Eric Fimbel, année 2013.

Cette dernière est analysée selon divers niveaux (opérations, management, stratégie), puis selon quatre catégories fonctionnelles (vente et marketing, fabrication, finances et comptabilité, ressources humaines). Les systèmes sont construits pour supporter efficacement ces différents intérêts organisationnels.

2.1.2. Infrastructure technologique du SI et ses plateformes :

L'infrastructure technologique comprend des investissements en matériel, en logiciels et en services associés (conseil, éducation et formation) communs à l'ensemble de l'entreprise ou qui touchent toutes ses unités.

L'infrastructure technologique d'une entreprise est l'une des composantes maîtresse de sa performance opérationnelle.

Figure 2 : Infrastructure réseau de l'entreprise

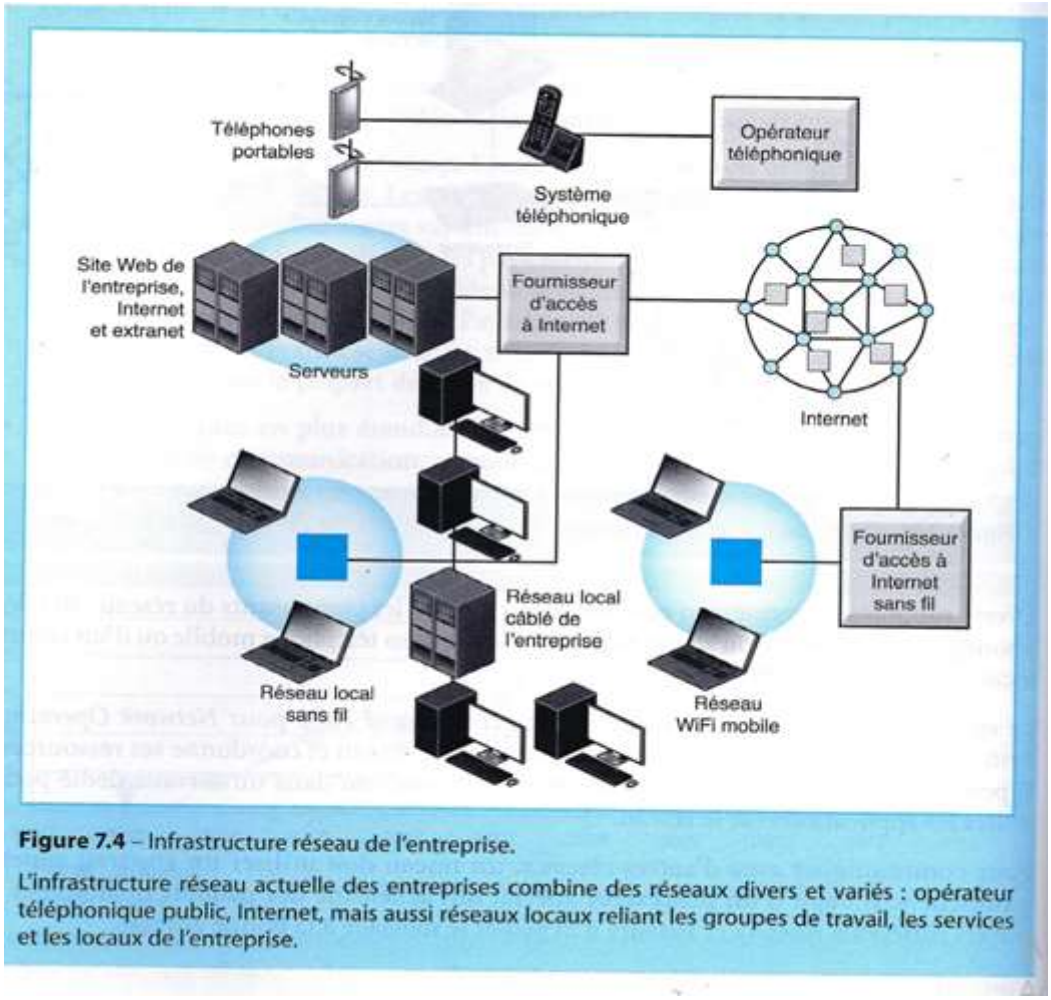


Figure 7.4 – Infrastructure réseau de l'entreprise.

L'infrastructure réseau actuelle des entreprises combine des réseaux divers et variés : opérateur téléphonique public, Internet, mais aussi réseaux locaux reliant les groupes de travail, les services et les locaux de l'entreprise.

Source : Management des systèmes d'information p264 Par l'auteur Eric Fimbel, année 2013.

2.1.2.1. Définition :

L'infrastructure technologique est un concept que l'on peut appréhender en tant qu'ensemble de potentiels de services offerts à l'entreprise, budgétisés par les managers et incluant les ressources humaines et techniques qui permettent le fonctionnement optimisé et sécurisé. Ces services comprennent les éléments suivants :

- les plateformes technologiques, qui incluent les ordinateurs centraux, locaux, portables et des ordinateurs de bureau, des assistants numériques personnels et

des applications internes et/ou accessibles localement ou à distance via un intranet, un extranet ou Internet ;

- les services de télécommunication, qui permettent de transmettre des données, de la voix et des images, sur de courtes comme sur de très longues distances intercontinentales ;

- les services de gestion de données, qui permettent de stocker, de gérer et d'analyser les données de l'entreprise ;

- les logiciels d'application, qui offrent des possibilités de traiter en temps réel et/ou différé les opérations et les processus structurant les différents métiers et activités opérationnels :

- les services de gestion de l'infrastructure technologique, qui servent à planifier et à développer l'infrastructure, à coordonner les services de l'infrastructure technologique pour toutes les unités, à gérer les comptes reliés aux dépenses en infrastructure technologique et à diriger des projets ;

- les normes associées à cette gestion des services de l'infrastructure technologique, qui offrent à l'entreprise et à ses unités des politiques précisant les technologies de l'information à utiliser et mode d'utilisation ;

- les services de formation et d'aides aux usages, qui préparent les employés à l'utilisation des systèmes et les managers à la planification et à la gestion des investissements en infrastructure technologique ;

- la recherche et le développement en services de l'infrastructure technologique, qui offrent des informations sur les projets à venir et sur les investissements susceptibles d'aider l'entreprise à en tirer des bénéfices durables et éventuellement différenciateurs.

2.1.2.2. Niveaux de l'infrastructure technologique :

L'infrastructure technologique affecte trois principaux niveaux : le domaine dit « public », l'entreprise et, enfin, chacune des unités opérationnelles.

Les choix de chaque entreprise en matière d'infrastructure dépendent des infrastructures publiques tant nationales qu'internationales : Internet, réseau téléphonique public, systèmes de câblodistribution, réseaux mobiles, etc.

L'infrastructure d'entreprise comprend des services comme le courrier électronique, le site Web d'entreprise, les intranets et les divers logiciels d'application. Selon le degré d'autonomie accordée au sein de l'entreprise, chaque unité opérationnelle (usine, entrepôt) disposera d'une infrastructure plus ou moins spécifique.

2.1.2.3. Composants de l'infrastructure technologique :

Sept composants principaux constituent actuellement l'infrastructure. Pour une entreprise, ces composants sont des investissements qui doivent être coordonnés les uns aux autres pour aboutir à une structure cohérente et fiable dans la durée.

Ces composants sont :

- Plateformes matérielles ;

- Systèmes d'exploitation ;

- ERP ;

- Organisation et stockage des données ;

- Equipements de réseaux et de télécommunication ;

- Plateforme Internet

- Services de conseil et d'intégration des systèmes.

2.2 Section 02 : La sécurité informatique

La sécurité informatique s'intéresse à la protection contre les risques liés à l'informatique ; elle doit prendre en compte :

- les éléments à protéger : matériels, données, utilisateurs ;

- leur vulnérabilité ;

- leur sensibilité : quantité de travail impliqué, confidentialité…

- les menaces qui pèsent sur eux ;

- les moyens d'y faire face (préventifs et curatifs) : complexité de mise en œuvre ;

- coût…

Voici le texte introductif de la norme **ISO 27001** visant à la sécurité de l'information :

« L'information est un actif qui, comme les autres actifs importants, a une valeur pour l'organisation et doit, en conséquence, être protégée. La sécurisation des SI vise à protéger l'information d'un large éventail de menaces, de façon à garantir le fonctionnement de l'entreprise, diminuer les pertes et maximiser le retour sur investissement et opportunités de marché. »

Source : Management des systèmes d'information, p310.

2.2.1. Définition et contexte d'études :

La sécurité informatique est un ensemble de moyens pour réduire la vulnérabilité d'un système aux menaces accidentelles ou intentionnelles. Le but de la sécurité informatique est de s'assurer que les ressources matérielles et/ou logicielles d'un parc informatique ne sont utilisées que dans le cadre prévu par du personnel habilité.

Il est nécessaire d'identifier les exigences de base en matière de sécurité informatique, qui décrivent les attentes de sécurité des utilisateurs de systèmes informatiques :

Confidentialité : Seul le personnel autorisé peut accéder aux données. Toutes les interceptions ne doivent pas réussir.

L'intégrité : Il doit toujours y avoir l'assurance que les données en circulation sont exactement ce que nous pensons avoir été et n'ont pas été altérées (volontairement ou involontairement) au cours du processus de communication. L'intégrité des données doit vérifier l'exhaustivité, l'exactitude et la validité des données.

La disponibilité : Il est nécessaire d'assurer le fonctionnement normal du système avec un accès facile aux services et aux ressources. La disponibilité d'un appareil est mesurée divisant le temps pendant lequel l'appareil a fonctionné par le temps ou il aurait dû fonctionner.

La non-répudiation : Aucune partie communicante ne peut refuser une transaction. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait au moyen d'un certificat numérique utilisant une clé privée.

L'authentification : Elle limite l'accès au personnel autorisé. Il est nécessaire de s'assurer de l'identité de l'utilisateur avant d'échanger les données.

Figure 3 : Figure de l'authentification

Source : www.nist.gov. Date de la consultation : Le 27 Avril 2022, à 08h00.

Les organisations utilisent souvent des noms d'utilisateurs et des mots de passe pour effectuer l'authentification. Il existe également des certificats numériques qui offrent des techniques d'authentification plus sûre et d'autres avantages en termes de sécurité.
D'une manière générale, la technique d'authentification dépend du niveau de sécurité recherchée. Mais les organisations doivent surtout envisager des techniques d'authentification plus sophistiquées.

Figure 4 : Objectifs de la SSI.

Source : https://protectam.fr Date de la consultation : 21 Avril 2022, à 9h00.

2.2.2. Etudes des risques liés à la sécurité informatique :

L'utilisation de l'outil informatique expose l'entreprise à plusieurs types de risques :

- Défaillance d'un traitement informatique en cours : il suffit de le redémarrer ;
- Les événements bloquent et doivent être corrigés avant que le travail puisse continuer. Cependant, il convient de noter que ces mêmes événements peuvent avoir des conséquences plus fâcheuses ;
- Les données sont irrémédiablement perdues ou altérées, les rendant inutilisables par la suite ;
- Indisponibilité permanente des données ou des traitements, pouvant entrainer l'arrêt de la production ou des services ;

- Divulguer des informations confidentielles ou trompeuses pouvant profiter à une entreprise concurrente ou porter atteinte à l'image de marque de l'entreprise ;

2.2.3. Typologie des risques informatiques :

En sécurité informatique, il existe principalement grands types de risques, à savoir : les risques humains et les risques matériels.

2.2.3.1. Risques humains :

Ce sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent non seulement sur les utilisateurs, mais aussi sur les experts informatiques eux-mêmes. Nous pouvons citer :

Maladroit : Faire des erreurs ou effectuer des traitements indésirables, ou effacer par inadvertance des données ou des programmes ;

Imprudence et ignorance : Introduire des programmes malveillants sans le savoir (par exemple lors de la réception d'un courrier). Les utilisateurs de nombreux outils informatiques ignorent les risques qu'ils font passer sur les systèmes qu'ils utilisent. Mener des opérations imprudentes (à l'aide de logiciel et de matériel) ;

Malveillance : Ces dernières années, les divers problèmes de virus et de vers ne peuvent être ignorés. Certain utilisateurs peuvent volontairement compromettre les systèmes d'information en introduisant délibérément des virus ou en introduisant volontairement de mauvaises informations dans des bases de données. On parle même de « cybercriminalité » ;

L'espionnage : En particulier l'activité industrielle, utilisent la même méthode et bien d'autres pour obtenir des informations sur l'activité concurrentielle, les processus de fabrication, les projets en cours, les produits futurs, les politiques de prix, etc.

2.2.3.2. Risques matériels :

Ils sont liés aux pannes et défaillances inévitables que connaissent tous les systèmes matériels et logiciels. Ces événements sont plus ou moins fréquents selon les précautions prises dans le processus de fabrication et l'application des procédures de test effectuées avant la mise en service des ordinateurs et des programmes. Certaines de ces défaillances ont des causes indirectes, voire très indirectes, les rendant difficilement prévisibles. Nous pouvons citer :

- Événements liés au matériel : La plupart des composants électroniques modernes produits en série peuvent présenter des défauts de fabrication. Ils s'effondreront un jour. Certaines de ces pannes sont difficiles à détecter car elles sont intermittentes ou rares. Parfois, ce sont des erreurs de conception.

- Événements liés au logiciel : Ce sont les plus courants. Les systèmes d'exploitation et les programmes deviennent de plus en plus complexes car ils font de plus en plus de choses. Ils nécessitent les efforts concertés de dizaines, de centaines voire de milliers de développeurs. Ces derniers peuvent commettre des erreurs individuellement ou collectivement, et les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent les éliminer complètement.

- Événements liés à l'environnement : Les machines électroniques et les réseaux de communication sont sensibles aux changements de température ou d'humidité et aux champs électromagnétiques. Par conséquent, les ordinateurs peuvent tomber en panne de manière permanente ou intermittente en raison de conditions météorologiques anormales ou de l'influence d'installations électriques, en particulier d'installations industrielles.

2.2.4. Gestion des risques informatiques :

La gestion des risques informatiques est un ensemble d'opérations consistant à gérer et à diriger les différentes incidences liées à la manipulation de l'outil informatique. La gestion des risques consiste en trois actions majeures :

- Etudier les risques potentiels (identifier/mettre au jour ces risques) ;

- Mettre en place des règles de sécurité appropriées pour réduire ces risques ;

- La formation de l'utilisateur.

2.2.4.1. Etudier les risques potentiels :

Cette étape comprend une inspection complète de la méthodologie de l'étude des risques informatique en vigueur. Cela se matérialise aux moyens :

- Définition de l'environnement : Définition des acteurs et leurs intérêts ; Importance de la sécurité dans la stratégie de l'entreprise ; Type de données impliquées ; Visibilité extérieure de la sécurité (importance pour la clientèle, le public).

- Etude des menaces : Identifier la nature de la menace: accidentelles (désastre, bugs…) ou intentionnelles (attaques, vols…) ; S'enquérir des sources de la menace: personnel non autorisé, intrus, logiciel ; Localiser la menace : procédures manuelles, informatique (software, réseau, stockage, hardware), infrastructure (concrète et abstraite).

- Etude des vulnérabilités : Etudes des faiblesses engendrées par l'exécution d'une menace.

- Etude des risques : Probabilité d'occurrence de ces menaces conduisant à une vulnérabilité.

- Estimation du risque et du plan stratégique : Risque (Coût des pertes à court, moyen et long terme engendrées, Coût de la mise en place de la contre-mesure tant au niveau logique que logistique, Comparer la perte potentielle au coût de la contre-mesure) ; Plan stratégique (Planning de l'implémentation avec prise en compte des besoins futurs en termes de sécurité ou non, Planning du suivi de l'implémentation).

- Mise en place du plan de sécurité : Les mécanismes de sécurité mis en place peuvent gêner les utilisateurs et les consignes et règles y définies peuvent devenir de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. Raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité dont la mise en œuvre s'effectue en quatre phases:

. Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;

. Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;

Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;

Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace.

2.2.4.2. Imposer des règles de sécurité adéquats :

Cela inclut la définition des procédures internes de l'entreprise basées sur :

- Règles administratives : Respect des normes de sécurité (normes ISO) ; respect des lois.

- Règles physiques : Gardiens, caméras, sirènes, serrures et accès aux locaux sécurisés par biométrie.

- Règles techniques : Détermination des niveaux de classification des données ; définition des niveaux d'accès à ces données ; traitement et stockage des informations par cryptographie

2.2.4.3. Formation des utilisateurs :

Il est de plus en plus admis que la sécurité est essentielle. Le coût de la perte de données due aux cybers attaques et autres logiciels malveillants a considérablement diminué d'année en année. Compromettre l'utilisateur et son environnement est beaucoup plus facile que l'algorithme de cryptage utilisé, tel que :

- l'utilisateur ne connaît pas le risque de conserver la liste des mots de passe utilisés à côté de l'ordinateur ;

- Il est souvent plus simple de s'introduire dans l'ordinateur de l'utilisateur afin de retrouver le texte en clair (hacking, vol, . . .) ;

- Il est possible de l'espionner, le pousser à la délation, pratiquer le shouldersurfing ou tout autre technique dite de "social engineering", ...

Il ne s'agit donc pas ici d'expliquer aux salariés comment fonctionnent les algorithmes qu'ils vont utiliser, mais comment et dans quelles conditions ils vont les utiliser, en définissant des règles à ne pas enfreindre. Il existe également plusieurs façons de gérer le risque, allant de la plus « sûre » à la moins consciente :

- Transférer le risque à la compagnie d'assurances ;

- Réduisez les risques en mettant en œuvre les contre-mesures suivantes :
Dissuasives : empêcher une attaque ;

Préventive : faire échouer l'attaque ;

Corrective : réduire les dégâts causés par l'attaque :

- Ignorer les risques ;
- Accepter le risque si les contre-mesures sont trop coûteuses

Bien sûr, il y a toujours un risque, aussi petit soit-il. Par conséquent, il est nécessaire de peser le pour et le contre lors de la mise en œuvre d'éventuelles contre-mesures

2.2.5. Etablissement et éléments d'une politique de sécurité :

Une stratégie de sécurité doit être préparée après la recherche des risques et avant la mise en place des mécanismes de protection. C'est elle qui fixe les principaux paramètres, notamment les niveaux de tolérance et les coûts acceptables. Un élément de politique de sécurité est un ensemble de lignes directrices qu'une organisation suit en matière de sécurité. Elle est élaborée au niveau de système de pilotage « Direction » avec le principal responsable de la sécurité de l'information de l'entreprise, car elle concerne l'ensemble des employés de l'entreprise. Elle est matérialisée dans un document codifié qui reprend l'ensemble des enjeux et qui contient la vision, les objectifs et l'orientation de l'entreprise, elle vise à maximiser la sécurité de l'information ainsi à garantir la disponibilité, l'intégrité et la confidentialité des données,

Le volet réglementaire et légal du pays est important dans la politique de sécurité de l'information

Des mises à jour de la politique de sécurité, doivent être faites régulièrement, selon le besoin et le développement de la technologie

La sécurité informatique d'une entreprise repose sur une bonne compréhension des règles par les collaborateurs, grâce à des actions de formation et de sensibilisation des utilisateurs, mais elle doit aussi aller au-delà, en couvrant les champs suivants :

- Mise en place des correctifs ;

- Classifications des documents ;

- Définition de la police de sécurité ;

- Les KPI et les matrices des responsabilités ;

- Une stratégie de sauvegarde correctement planifiée ;

- Description de la sécurité (de l'infrastructure physique, des données informatiques, des applications, du réseau) ;

- Plan en cas de sinistre (Un plan de reprise après incident) le PCA qui est le plan de continuité d'activité ;

- Sensibilisation du personnel aux nouvelles procédures

- Sanctions en cas de manquements.

2.2.6. Principaux défauts de sécurité informatique :

Les failles de sécurité peuvent être considérées comme des modifications accidentelles ou involontaires du fonctionnement normal de l'équipement informatique. Les vulnérabilités de sécurité des systèmes d'information les plus fréquemment observées sont :

- Installer les logiciels et le matériel par défaut.

- Aucune mise à jour effectuée.

- Mot de passe inexistant ou par défaut.

- Conserver les services inutiles.

- Traces inexploitées.

- Pas de séparation des processus opérationnels des processus de gestion du système.

- Des procédures de sécurité obsolètes.

- Eléments et outils de test conservés en configuration de production.

- Authentification faible.

2.2.7. Principales attaques informatique :

Dans le monde informatique, les attaques sont nombreuses, certaines sont connues des utilisateurs, d'autres sont cachées par les experts. Toutes ces attaques visent à modifier le comportement du SI. En plus de ces attaques, nous rencontrons également diverses actions ou actions de logiciels malveillants conçus pour atteindre le noyau. Le but de ces attaques est de perturber le système. Une fois que l'intrus pénètre dans le système, il agit en exploitant la vulnérabilité afin d'utiliser le système et, dans la plupart des cas, continue d'y accéder à l'insu de l'utilisateur légitime. Mais selon les buts et les objectifs, les attaques existent. Certaines des attaques les plus connues incluent :

Les logiciels malveillants :

Un logiciel malveillant, également appelé logiciel indésirable ou programme malveillant ou pourriciel ("malware"), est un programme conçu pour endommager un système informatique sans le consentement de l'utilisateur dont l'ordinateur est infecté.

Les virus informatiques :

Un virus informatique est un automate auto réplicatif à la base n’est pas malveillant, mais aujourd'hui classifié comme logiciel malveillant, conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre par tout moyen d'échange de données numériques comme les réseaux informatiques et le CD-ROM, les clefs USB, les disques durs, etc.

Les vers informatiques :

Un ver informatique est un logiciel malveillant qui se réplique sur plusieurs ordinateurs à l'aide d'un réseau informatique, tel qu'Internet. Une fois exécuté, il a la capacité de se répliquer. Contrairement aux virus, les vers n'ont pas besoin d'être liés à d'autres programmes exécutables pour se propager. Il convient également de noter que les données corrompues ou détruites par des vers informatiques ne sont généralement pas récupérables. Même ainsi, le ver a parfois d'autres usages. Certaines entreprises les utilisent pour tester la sécurité de leurs réseaux intranet.

Le Cheval de Troie :

Un cheval de Troie (Trojan horse en anglais) est un type de logiciel malveillant, qui ne doit pas être confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Le rôle du cheval de Troie est de faire entrer ce parasite sur l'ordinateur et de l'installer à l'insu de l'utilisateur. C'est par analogie, que ce type de programme a été baptisé « cheval de Troie », en référence à la ruse qu'Ulysse utilisa pour contourner les défenses adverses. Le cheval de Troie prend l'apparence d'un logiciel existant, légitime et parfois même réputé, mais qui aura été modifié pour y dissimuler un parasite.

Les rootkits :

Un rootkit (Aussi appelé « outil de dissimulation d'activité », « maliciel furtif », « trousse administrateur pirate », parfois simplement « kit », est un ensemble de techniques mises en œuvre par un ou plusieurs logiciels, dont le but est d'obtenir et de pérenniser un accès (généralement non autorisé) à un ordinateur de la manière la plus furtive possible, à la différence d'autres logiciels malveillants.

Les portes dérobées :

Dans un logiciel, une porte dérobée (de l'anglais backdoor, littéralement porte de derrière) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel. L'introduction d'une porte dérobée dans un logiciel à l'insu de son utilisateur transforme le logiciel en cheval de Troie.

Espionnage informatique :

L'espionnage informatique est une surveillance secrète et désobligeante accomplis par un attaquant au moyen de l'outil informatique afin de s'acquérir des informations dont il n'est pas censé obtenir. L'espionnage informatique peut s'effectuer de plusieurs manières, les plus usuelles sont :

- L'homme du milieu (Environnement informatique) ;

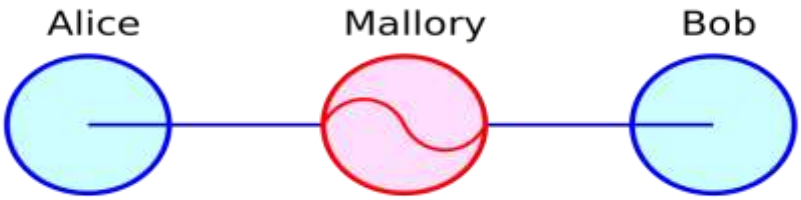
- Les espiogiciels ;

- Les cookies.

L'homme du milieu :

Lorsqu'un pirate, prenant le contrôle d'un équipement du réseau, se place au milieu d'une communication il peut écouter ou modifier celle-ci. On parle alors de « l'homme du milieu » (man in the middle). C'est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de communication entre elles a été compromis.

Figure 5: Schéma de l'attaque informatique « l'homme du milieu » : Mallory intercepte les communications entre Alice et Bob.



Source : https://fr.wikipedia.org

Les espiogiciels :

Un logiciel espion (aussi appelé mouchard ou espiogiciel ; en anglais spyware) est un logiciel malveillant qui s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données. Le terme de logiciel espion, est une traduction du mot anglais spyware, qui est une contraction de spy (espion) et software (logiciel).

Les cookies :

Le cookie est l'équivalent d'un fichier texte de petite taille, stocké sur le terminal de l'internaute. Existant depuis les années 1990, ils permettent aux développeurs de sites web de conserver des données utilisateur afin de faciliter la navigation et de permettre certaines fonctionnalités. Les cookies ont toujours

été plus ou moins controversés car elles contiennent des informations personnelles résiduelles pouvant potentiellement être exploitées par des tiers. Ces informations censées être privées ne le sont pas vraiment, puisqu'elles sont accessibles à un certain point.

2.2.8. Les systèmes de protection informatique :

Un système de protection informatique est un ensemble des techniques permettant de se prémunir contre les attaques et piraterie informatique, en interdisant la copie de contenus d'un support (logiciel) ou en rendant inutilisable toute intrusion dans le système. Les systèmes de protection informatique les plus connus sont :

- Les anti-virus ;

- Les systèmes de détection (et prévention) d'intrusion (IDS) ;

- Les firewalls ;

- Les mots de passe ;

Les anti-virus :

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique ne sont qu'une catégorie). Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur (le plus souvent ceux du système d'exploitation). Il est intéressant de noter qu'une fois un fichier infecté, il ne l'est jamais deux fois.

Lorsque le virus est détecté par l'antivirus, plusieurs possibilités sont offertes pour l'éradiquer :

- Supprimer le fichier infecté ;

- Supprimer le code malicieux du fichier infecté ;

- Placer le ou les fichiers infectés en "quarantaine" pour un traitement futur.

Les systèmes de détection d'intrusion :

Un système de détection d'intrusion (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Les firewalls (pare-feu) :

Un pare-feu (parfois appelé coupe-feu, garde-barrière, barrière de sécurité, ou encore firewall. Dans un environnement Unix BSD (Berkeley Software Distribution), un pare-feu est aussi appelé packet filtre. Littéralement appelé: mur de feu, est un logiciel utilisé pour appliquer les politiques de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Le pare-feu a pour objectif principal de surveiller et contrôler les applications et les flux de données (paquets), en empêchant les connexions non-autorisées sur un réseau informatique ou autres.

Les mots de passe :

Un mot de passe est un mot ou une suite de caractères utilisé comme moyen d'authentification pour prouver son identité lorsque l'on souhaite accéder à des lieux protégés, à des ressources (notamment informatiques) ou accéder à des services restreints et protégés. Les mots de passe doivent être gardés secrets pour empêcher des tiers non autorisés d'accéder aux ressources ou aux services. C'est une façon de vérifier qu'une personne correspond bien à ce qu'elle prétend être. Cela prouve que nous sommes propriétaires et que nous communiquons avec le service chargé d'autoriser l'accès.

2.2.9. Exigences juridiques et règlementaires :

Gestion des documents informatiques :

Des mesures et règlementations locales ou nationales cohabitent avec des dispositions internationales. La gestion des documents informatiques (GDI) comprend les politiques, les procédures et les outils visant à gérer les conservations, la destruction et le stockage des documents électroniques.

Preuves et sciences légales :

La sécurité, le contrôle et la gestion des documents électroniques sont devenus essentiels pour se protéger en cas de poursuites. Les preuves utilisées dans les cas de fraudes en valeurs mobilières, de détournements de fonds, de vols de secrets commerciaux, de délits informatiques et dans plusieurs affaires civiles se présentent souvent sous forme numérique. Outre les documents imprimés ou dactylographiés, les affaires judiciaires modernes ont de plus en plus recours aux preuves présentées sous forme de données stockées sur des clés USB, des lecteurs de disques durs, des cédéroms, ainsi que des courriels.

Une politique efficace de conservation des documents électroniques fait en sorte que les documents électroniques, les courriels et les autres documents soient bien classés et accessibles, et qu'ils ne soient pas conservés trop longtemps ou détruits trop précocement. Elle reflète également une volonté de préserver des preuves potentielles utilisables devant un tribunal. Cela concerne la satisfaction des exigences judiciaires potentielles suivantes :

- Récupérer des données dans ordinateur tout en préservant leur intégrité en tant que preuves ;

- Stocker et manipuler correctement des données électroniques qui ont été récupérées ;

- Trouver l'information pertinente dans un gros volume de données ;

- Fournir de l'information à un tribunal.

Une preuve électronique peut se dissimuler dans un média de stockage sous la forme de fichiers informatiques invisibles pour l'utilisateur moyen. Par exemple, il peut s'agir d'un fichier qui a été supprimé dans un disque dur. Les données effacées par un utilisateur sont récupérables à l'aide de diverses techniques. Des experts agréés par les tribunaux tentent de récupérer ces données cachées.

Continuité des affaires :

La couverture fonctionnelle de l'informatisation s'étend à la quasi-totalité des activités de l'entreprise. Il est donc vital que des mesures spécifiques soient prises pour assurer le maintien en fonctionnement du SI, support des activités opérationnelles. La non-disponibilité est la période pendant laquelle un système n'est pas opérationnel.

La planification de la reprise sur sinistre consiste à élaborer des plans pour restaurer des services informatiques et de communications interrompus, quelle que soit la cause de cette interruption de service. Les plans de reprise sur sinistre comprennent un volet technique, mais également des volets organisationnels et humains (formation, simulation, dispositifs palliatifs, etc…).

2.3 Section 03 : Le rôle de l'audit dans le processus général de contrôle et la norme ISO 27001

Les organisations doivent effectuer des vérifications complètes et systématiques. Un audit des systèmes d'information permet de repérer tous les contrôles qui régissent les SI et d'évaluer leur efficacité. Pour ce faire, les auditeurs doivent connaître :

- Les activités d'exploitation ;
- Les installations physiques ;

- Le réseau de télécommunication ;
- Les systèmes de contrôle ;
- Les objectifs de la sécurité des données ;
- La structure organisationnelle ;
- L'organigramme de l'entreprise ;
- Les procédures, politiques, manuelles (documentation)
- Les applications individuelles.

Ils demandent habituellement à des utilisateurs clés qui exploitent un SI précis de leur décrire leurs activités et les procédures qu'ils emploient. Ils examinent les applications, les contrôles d'intégrité globaux et les règles de contrôle. Ils analysent aussi un échantillon des transactions qui se déroulent dans le système et effectuent des tests, à l'aide, au besoin, d'un logiciel de vérification automatisée.

Ils dressent ensuite la liste hiérarchisée de toutes les faiblesses révélées par l'audit des contrôles et estiment la probabilité de leur occurrence. Ils évaluent, enfin, les conséquences financières et organisationnelles de chaque risque.

La protection des ressources informatiques exige une politique globale de sécurité fiable et un ensemble de contrôles.

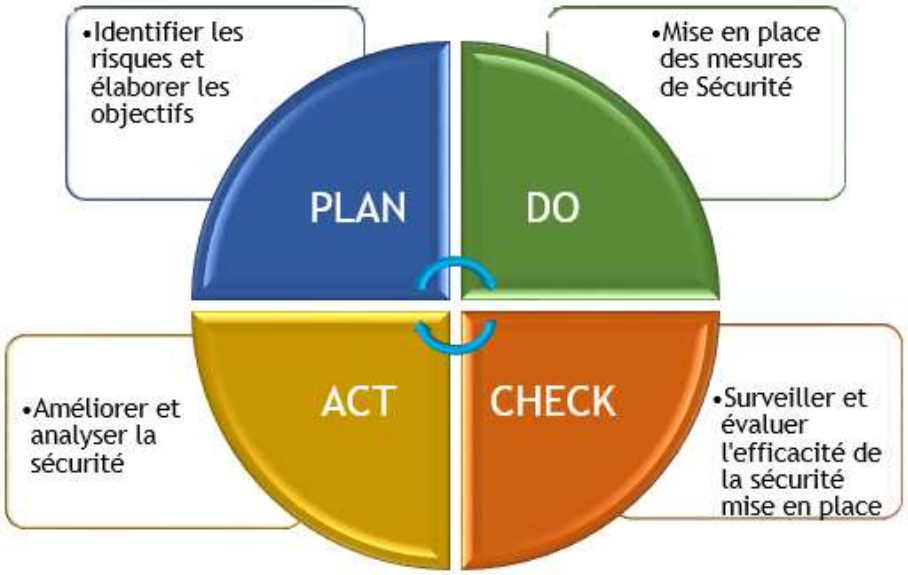
La norme 27001, un regroupement de normes internationales de sécurité er de contrôle, offre des repères utiles en ce sens. Elle spécifie les pratiques les plus appropriées en matière de sécurité et de contrôle des SI, incluant les politiques de sécurité, la planification de la continuité des affaires, la sécurité du matériel informatique, le contrôle d'accès, la conformité aux normes et la création d'une fonction dédiée à la sécurité au sein d'une organisation. Elle vise à assurer la disponibilité des informations et des services, sécuriser l'intégrité des données critiques. Garantir la confidentialité des données sensibles ou des données clients.

Figure 6: Figure de la norme ISO 2700

Source : https://www.iso.org

La norme ISO 27001 est orientée processus et propose en toute logique une démarche d'amélioration continue de type PDCA.

Figure 7: Le schéma de la démarche d'amélioration continue PDCA



Source : réalisé par nous même.

Le PDCA propose 4 temps : Plan ; Do, Check ; Act

- **Plan :**

Elaboration de la politique de sécurité des SI, précision du périmètre d'intervention, définition des objectifs, analyse et maitrîse des risques, identification et évaluation, cartographie.

- **Do :**

Plan et déploiement des mesures de sécurité, élaboration et application des procédures spécifiques, sensibilisation et formation, séléction des indicateurs et réalisation des tableaux de bord de la sécurité.

- **Check :**

Audit et contrôles internes, revue.

- **Act :**

Action corrective, identification des voies d'amélioration, bouclage.

CHAPITRE 02 : CADRE METHODOLOGIQUE DE LA RECHERCHE ET CONTEXTE ORGANISATIONNEL

Après avoir abordé les différents points théoriques du chapitre précédent, dans ce chapitre, nous aborderons la méthodologie suivie et présenterons le contexte organisationnel sur lequel se base notre travail.

Ce chapitre est reparti en deux sections, la première sera consacrée à la présentation de différents outils de collecte et d'analyse de donné utilisé. Dans la deuxième section nous allons exposer l'organisme d'accueil.

Section 01 : Cadre méthodologique

Suite à la présentation des fondements théoriques dans lesquels s'articule la présente recherche, il serait pertinent de traiter la méthodologie qui la caractérise.

Dans ce sens, nous allons exposer dans ce deuxième chapitre la méthodologie retenue afin de répondre à l'objectif de recherche. Ainsi, nous allons présenter les différentes étapes de la démarche de recherche, à savoir : le choix du type d'étude.

1.1. Choix du thème :

Le rôle joué par les systèmes informatiques dans les entreprises est si essentiel que leur sécurité et leur contrôle sont devenus une nécessité vitale, la sécurisation comprend les politiques, les procédures et les moyens techniques.

De ce fait, l'audit de la sécurité informatique est aussi une nécessité vitale.

Ce qui a motivé notre choix pour cette thématique.

1.2. Choix de l'entreprise :

Nous avons effectué notre stage auprès de l'entreprise OOREDOO ALGERIE, la pertinence de ce terrain est justifiée par le fait de cette entreprise de services est tenue impérativement de sécuriser son système informatique ;

Dans le cadre de notre mémoire, nous nous sommes intéressés à l'évaluation des procédures mises en œuvre par cette entreprise dans ce but. Notre intérêt est étroitement lié à la thématique de notre mémoire.

1.3. La méthode de recherche :

Dans le but de répondre à notre problématique nous avons opté à une étude qualitative ; selon (taylor et begdan, 1984) « la recherche qualitative est une recherche qui produit et analyse des données descriptives, telles que les paroles écrites ou dites et le comportement observatoire des personnes ».

1.4. La méthode de collecte de données :

1.4.1. Recherche documentaire :

Nous avons récolté le maximum d'informations à travers les ouvrages, les articles et thèses et cela pour exposer nos concepts, nous avons aussi consulté les documents internes de l'entreprise ce qui nous a permis de décrire et présenter l'entreprise.

1.4.2. L'observation :

Les observations permettent d'appréhender une réalité vécue, elles permettent de recueillir des informations sur les comportements non-verbaux des sujets.

1.4.3. Entretiens :

Nous avons décidé de mener une étude qualitative sous forme d'entretiens, afin de collecter des informations qui nous aideront à tenter de répondre à notre problématique.

Dans notre étude, nous avons utilisé un entretien semi directif.

Entretiens semi directif :

L'entretien semi-directif, est une méthode d'étude qualitative. Son but est de récolter des informations qui apportent des explications ou des éléments de preuves à un travail de recherche.

« L'entretien semi directif est une technique de collecte de données qui contribue au développement de connaissances favorisant des approches qualitatives et interprétatives relevant en particulier des paradigmes constructiviste. » (Linclon, 1995)

La construction du guide d'entretien

L'élaboration d'un guide d'entretien est une étape importante pour d'effectuer nos entretiens, la création du guide d'entretien nous permet d'avoir une vision plus claire, ce qui nous permet alors de détecter les failles existantes et de mieux cerner les problèmes pour en sortir avec des solutions et des recommandations significatives.

Afin d'effectuer nos entretiens, nous avons élaboré un guide d'entretien (voir annexes A, B, C, D), nous avons interviewé l'ensemble des personnes en lien avec notre sujet.

Les personnes interrogées :

Pour mener à bien cette étude, et afin de donner une dimension empirique à notre travail, nous avons réalisé un entretien au sein d'OOREDOO ALGERIE, à travers un échantillon des personnes spécialisées dans le domaine.

La sélection des personnes interrogées est basée sur le poste qu'elles occupent au sein de l'entreprise et qui sont en relation avec notre sujet de recherche.

Tableau 1: Liste des interviewés.

Noms des personnes interrogées	**Poste**	**Durée de l'entretien**
Mme. YADEL Baha	**Chef de service information security, procès et audit management.**	**6h (3 fois)**
M. BELLILI Nassim	**Spécialiste Senior information security procès management.**	**1h**
M. KRELIFA Adel	**Spécialiste Senior risque management**	**1h**
Mme. OUBICHE Mehdia	**Chef de service Process management.**	**1h**

1.5. Traitements des données :

L'analyse de contenu :

Nous avons choisi l'analyse de contenu parce qu'il cherche à rendre compte de ce qu'ont dit les interviewés de la façon la plus objective possible.

Section 02 : Présentation d'Ooredoo Algérie – Contexte organisationnel

2.1. Dénomination sociale :

Premier opérateur multimédia de téléphonie mobile en Algérie, **Nedjma**, devenue **Ooredoo** le 21 novembre 2013, est la filiale algérienne du Groupe Ooredoo Qatar.

Présent en Algérie depuis le **23 décembre 2003**, date d'obtention de la licence de fourniture des services de téléphonie mobile en Algérie, la marque **Nedjma** a été commercialement lancée le **24 août 2004**, en offrant aux Algériens, qu'ils soient clients particuliers ou entreprises, une gamme d'offres et de services novateurs, en respect avec les standards internationaux.

Tout en prônant le changement dans la continuité, la nouvelle marque Ooredoo a été lancée le 21 novembre 2013, donnant naissance à une nouvelle ère, dans le respect des acquis de Nedjma et de ses valeurs, adoptés et enrichis par Ooredoo:

*** Caring** : Pour le soutien, la confiance, le respect d'autrui et la responsabilité que Ooredoo incarne
*** Connections** : Pour l'engagement de Ooredoo à travailler dans un esprit collaboratif et en intégrant parfaitement la communauté algérienne
*** Challenging** : Pour le progrès auquel aspire Ooredoo et la recherche continue de l'amélioration et de la différence

Ooredoo est certifié ISO 9001:2015 et iso 27001:2013 depuis 2013.

Figure 8: Document interne de l'entreprise ralatif à l'ISO 27001

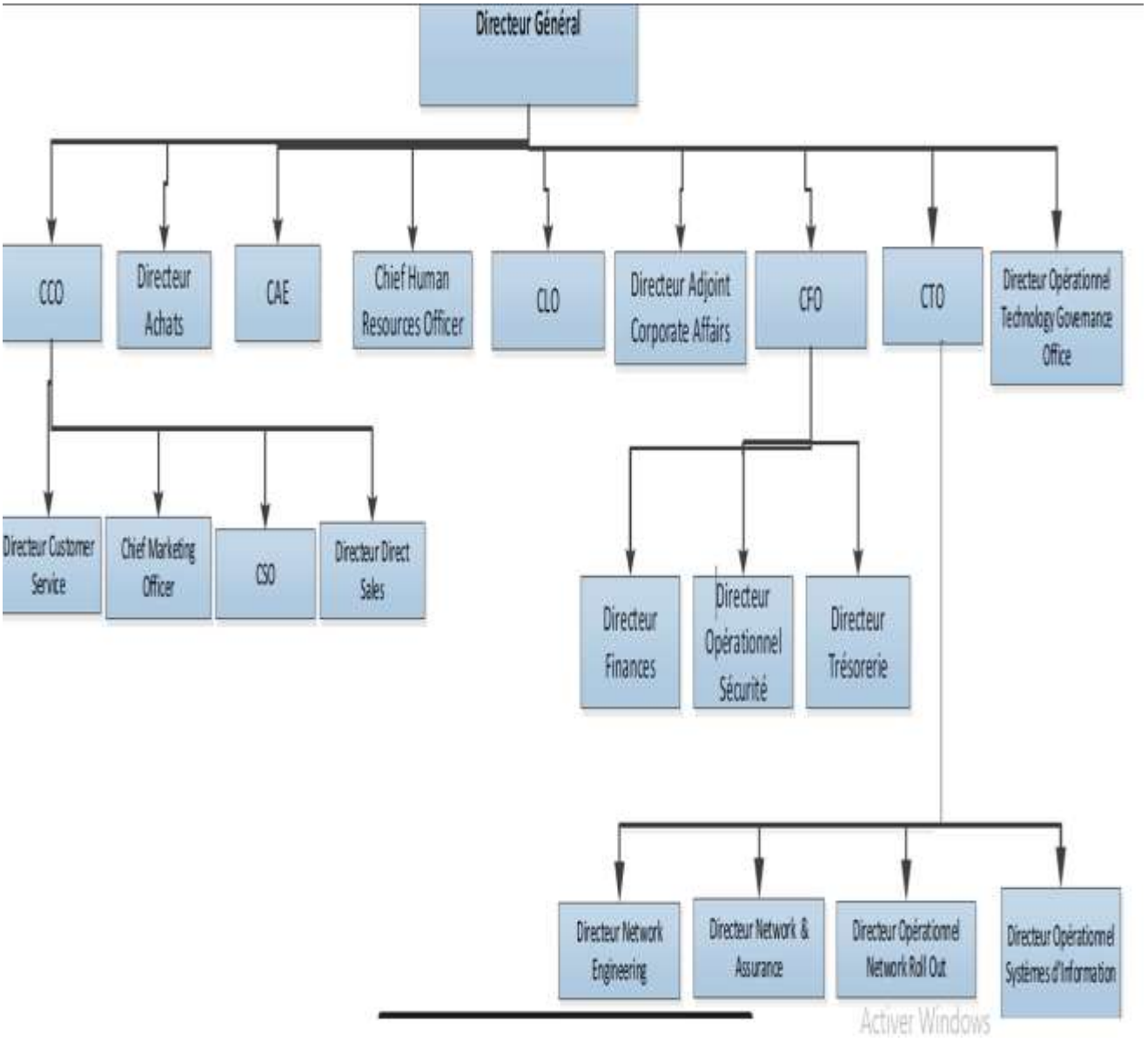
Tableau 2: Fiche technique d'Ooredoo Algérie

Nom de la société	**OOREDOO ALGERIE**
Capital sociale	**139,5 millions $ US**
Date de création	**25 août 2004 Création** **15 décembre 2013 Changement de nom (de Nedjma à Ooredoo)**
Forme juridique	**Société par action wataniya télécomme**

Actionnaire	**Koweït Projects Company (KIPCO)**
Activité	**Opérateur de télécommunications**
Produits	**Téléphonie mobile** **HSPA+** **3G++** **4G** **LTE** **Push to talk** **téléphones portables**
Logo	
Slogan	**« Ooredoo, Dima Mâakoum »**

Source : Réalisée par nous même à partir de document interne de l'entreprise.

Figure 9: Organigramme d'Ooredoo Algérie



Source : Document interne de l'entreprise.

2.2. Vision, objectifs et orientations d'Ooredoo Algérie :

Vision :

Ooredoo, leader du multimédia mobile, réinvente la façon de communiquer et contribue activement au renouveau algérien.

Dès son arrivé, le marché de la téléphonie mobile devient très concurrentiel.

Pour augmenter sa part de marché, Ooredoo s'impose comme l'opérateur leader de l'innovation et du multimédia mobile en Algérie. Elle offre aux clients une qualité spécifique dans le domaine de la téléphonie mobile.

Objectifs :

Considérant ses clients comme son ultime ressource, et convaincue que sa pérennité dépend de leur satisfaction et de leur fidélisation, Ooredoo s'inscrit dans une démarche de performance orientée client, basée sur l'amélioration continue.

Orientations :

Les énoncés suivants constituent les orientations que se donne Ooredoo en matière de qualité pour atteindre ses objectifs.

- Accroître la satisfaction de ses clients tout en cherchant à anticiper les attentes du marché,
- Optimiser l'utilisation des ressources techniques, technologiques et avant-gardistes dans le but de satisfaire les exigences implicites et explicites de ses clients.
- Développer en permanence les compétences distinctives.
- Tisser des relations privilégiées avec ses partenaires et prestataires externes.
- Assurer la conformité de l'ensemble de ses prestations aux exigences légales et réglementaires.
- Accroître la satisfaction de ses actionnaires en augmentant notre rentabilité.
- Promouvoir l'approche par le risque afin de prévenir et réduire tout effet indésirable.

- Prendre en considération les évolutions des enjeux externes et internes dans l'établissement des processus et des politiques de l'entreprise.

2.3. Présentation du département sécurité de l'information de la société Ooredoo Algérie :

Afin d'assurer la protection de ses actifs informationnels, l'organisation, Ooredoo Algérie, s'investit massivement dans ce domaine. A cette fin, un département est dédié à la sécurisation. La mission de cette importante structure, concerne :

- L'élaboration de procédures régissant la sécurité informatique.
- La sensibilisation des utilisateurs.
- L'amélioration du processus de gestion des risques.
- La mise en place d'un processus de gestion des menaces et des vulnérabilités.
- Fournir un mécanisme solide de la gestion des accès.
- La conformité à toutes les exigences légales et réglementaires qui concerne la sécurisation.
- La mise en place d'un SMSI.

2.4. Présentation du responsable de la sécurité des systèmes d'Information (RSSI)

Le responsable de la sécurité des systèmes d'information (ou RSSI pour Responsable de la Sécurité des Systèmes d'Information) définit et développe la politique de sécurité de l'information de son entreprise. Il est garant de sa mise en œuvre et en assure le suivi.

Les responsables de la sécurité des systèmes d'information sont des spécialistes de la sécurité de l'information, des applications et des réseaux de télécommunications. Il identifie et met en œuvre les moyens et solutions nécessaires pour prévenir les menaces susceptibles d'affecter la sécurité des données et/ou les activités commerciales (par exemple, contre les risques de

virus malveillants et de piratage des données). Compte tenu de l'évolution du trafic lié à l'usage d'Internet, ces menaces sont de plus en plus fréquentes. La responsabilité du responsable des systèmes de sécurité informatique est d'assurer la sécurité, la fiabilité et l'intégrité des systèmes d'information de l'entreprise. Il doit définir une politique de sécurité et s'assurer qu'elle est appliquée de manière appropriée par tous les acteurs susceptibles d'accéder ou d'interférer avec les données informatiques confidentielles de l'entreprise.

2.5. Les objectifs du responsable de la sécurité des systèmes d'information :

Les objectifs premiers du RSSI sont d'identifier et de protéger le SI, et d'informer, conseiller, former et alerter les managers et les collaborateurs des risques liés à l'absence de sécurité des données ou des applications spécialisées. Concrètement, un responsable de la sécurité informatique analysera attentivement les différents systèmes d'information qui existent au sein d'une entreprise. Sur cette base, l'une de ses tâches est de soutenir et de sensibiliser les employés, les gestionnaires et les intervenants externes des différents services sur les différentes règles, les changements nécessaires et les actions à suivre pour assurer la sécurité des systèmes informatiques.

CHAPITRE 03 : ANALYSE ET DISCUSSION DES RESULTATS

Dans ce dernier chapitre qui est dédié à l'analyse, le traitement et la présentation des résultats de la recherche qualitative menée au sein de l'entreprise Ooredoo Algérie. Nous allons présenter leur système de sécurisation mis en place, ses fonctionnalités, ainsi que ses avantages qui sont la raison pour laquelle l'entreprise Ooredoo Algérie l'a choisi principalement pour sécuriser ses actifs informationnels.

Ensuite nous présenterons sous forme de projet de rapport d'audit nos résultats de la mission d'audit, ainsi qu'une évaluation continue du dispositif de contrôle interne et des recommandations d'améliorations afin de garantir la sécurité du SI au sein de l'entreprise.

Section 01 : Le système de sécurité informatique au niveau d'Ooredoo Algérie

Dans cette première section nous présenterons le SSI mis en place au niveau d'Ooredoo Algérie, ses fonctionnalités, ainsi que ses avantages.

1.1. Présentation du système de sécurité SIEM

Le SIEM fut adopté par Ooredoo Algérie pour la sécurisation des ses actifs informationnels. C'est un système de sécurisation et de protection qui englobe deux sous-systèmes :

1* Le SIM : Security information management.

2* Le SEM : Security event management

Les systèmes de security information and event management (SIEM) répondent aux trois défis qui limitent la réponse rapide aux incidents :

- La grande quantité de données de sécurité non agrégées rend difficile de voir ce qui se passe et de classer les menaces par ordre de priorité.

- Les équipes informatiques manquent de personnel et de formation en raison du manque de compétences en matière de cyber sécurité.
- La nécessité de démontrer la conformité prend du temps pour identifier les menaces et y répondre.

Les systèmes SIEM sont essentiels pour les organisations qui veulent atténuer les menaces.

1.2. Fonctionnalité du SIEM

La technologie SIEM recueille des informations liées à la sécurité à partir de serveurs, de dispositifs d'utilisateurs finaux, d'équipements de réseau et d'applications, ainsi que de dispositifs de sécurité. Les solutions de gestion des événements et des informations de sécurité (SIEM) classent les données par catégories et, lorsqu'un problème de sécurité potentiel est identifié, peuvent envoyer une alerte ou répondre d'une autre manière, selon des politiques prédéfinies. L'agrégation et l'analyse des données recueillies sur le réseau permettent aux équipes de sécurité d'avoir une vue d'ensemble, d'identifier les failles ou les incidents dès les premières étapes et de réagir avant que des dommages ne soient causés.

Les systèmes SIEM ingèrent et interprètent les journaux provenant d'un maximum de sources, notamment :

- Pare-feu/systèmes unifiés de gestion des menaces (UTM)
- Systèmes de détection des intrusions (IDS) et systèmes de prévention des intrusions (IPS)
- Filtres Web
- Sécurité des points terminaux
- Points d'accès sans fil
- Routeurs

- Interrupteurs
- Serveurs d'application

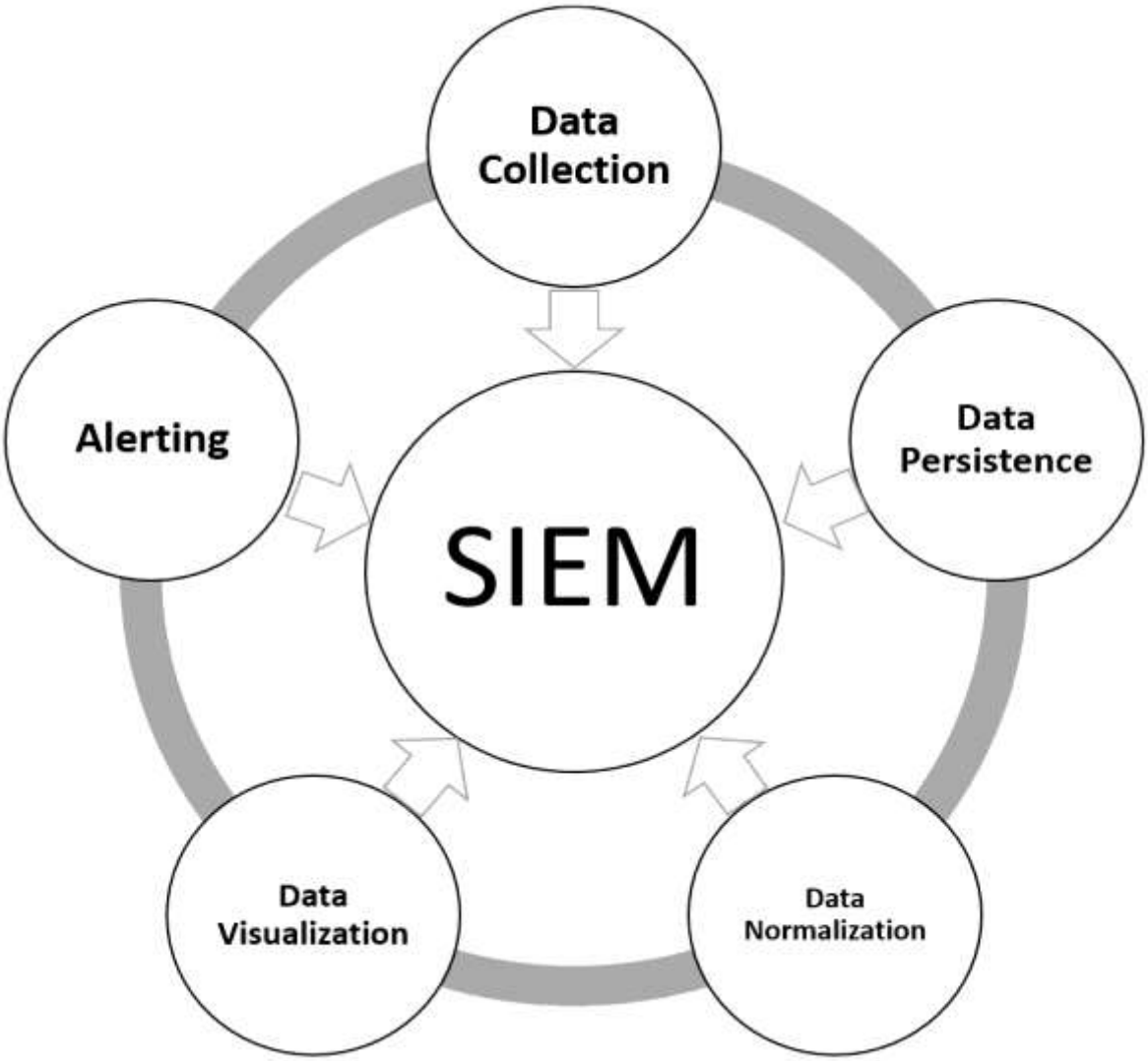
Les systèmes SIEM examinent à la fois les données d'événements et les données, les rapports et la surveillance. Sur la base de ces résultats, les équipes informatiques peuvent réagir de manière efficace et efficiente aux incidents de sécurité.

1.3. Avantages du SIEM

Le système SIEM offre des capacités de détection des menaces, des rapports en temps réel, des outils de conformité. Donc, ses avantages sont les suivants :

- L'Efficacités de la sécurité et une réponse plus rapide aux menaces.
- Démonstration de conformité efficace : Le système SIEM devrait également permettre aux équipes informatiques de suivre et de signaler facilement la conformité aux réglementations industrielles et gouvernementales et aux normes de sécurité.
- Réduction significative de la complexité : La consolidation des données d'événements de sécurité provenant de multiples applications et dispositifs permet une analyse rapide et complète.

Figure 10: Fonctionnalités du système SIEM



Source : Réalisé par nous même à partir d'un document interne de l'entreprise.

Section 02 : L'audit du système de sécurité SIEM

Dans cette section, nous présenterons la démarche de la mission d'audit pour évaluer l'efficacité du système, et afin d'arriver à faire un rapport d'audit de la sécurité du système.

Durant notre stage nous avons été sensibilisées à la démarche d'audit de sécurité informatique.

2.1. Présentation de la démarche d'audit

La conduite d'une mission d'audit se déroule en trois grandes phases :

- Phase de planification ;
- Phase de réalisation ou de vérification sur le terrain ;
- Phase de conclusion ou de restitution des résultats ;

2.1.1. Phase de planification :

C'est la phase qui consiste à préparer la mission, dans le but de faciliter le travail à faire sur terrain. Il s'agit de prendre les dispositions idoines, préalables à l'accomplissement d'une mission d'audit. Cette phase comprend :

A- Le lancement de la mission : La mission d'audit débute par l'élaboration de l'ordre de mission et de la lettre de lancement de la mission.

B- Les travaux de recherche et d'analyse documentaire : Cette étape consiste pour les auditeurs, d'une part de collecter toute la documentation disponible sur le thème d'audit et d'autre part, à analyser ces informations et à identifier les potentiels risques

C- La définition des objectifs d'audit de la mission : Cette étape se traduit dans un document appelé « rapport d'orientation ».

2.1.2. Phase de réalisation ou de vérification sur le terrain :

Cette phase est la conduite de la mission d'audit sur le terrain. En d'autres termes, c'est le déroulement de la mission.

C’est le lieu pour les auditeurs de mettre en œuvres les techniques d’audit qui vont leur permettre d’élaborer un diagnostic et de proposer des recommandations. Cette phase fait appel à la capacité d’investigation, de dialogue, de communication et de déduction des auditeurs pour détecter et évaluer les risques identifiés dans la structure.

La phase de vérification prend en compte les étapes principales suivantes :

- La communication avec la structure auditée ;
- L’intervention sur place ;
- Les débats des constats et des recommandations ;

Alors nous avons réalisés avec les collaborateurs relevant de la structure sécurité de l’information de la direction procès and audit management, pour savoir quels sont les risques liés au système SIEM au sein d’Ooredoo Algérie. (Annexes A, B, C, D).

2.1.3. Phase de conclusion ou de restitution des résultats :

Cette phase est le lieu pour les auditeurs de restituer les résultats de la mission d’audit. Et c’est dans cette phase que le projet de rapport doit être envoyé au responsable audité, contenant des propositions de recommandations d’amélioration. Afin de créer de la valeur ajouté à l’entreprise qui en bénéfice.

Pour cela notre étude portant sur l’audit de la sécurité du système informatique. Nous allons premièrement fixer les objectifs d’audit, afin d’évaluer le SIEM mis en place au sein de l’entreprise Ooredoo Algérie. Ensuite nous allons faire des constats après évaluation, et nous apporterons des recommandations qui pourront améliorer le système SIEM.

2.2. Objectifs d’audit du système SIEM au sein d’Ooredoo Algérie

A- S’assurer que l’organisation est capable de redémarrer les systèmes informatiques en cas d’arrêt ou destruction.

B- S’assurer que la sécurité du système informatique est adaptée au niveau de risque identifié et accepté par la direction.

C- S’assurer que les accès aux données et aux applications sont réservés aux personnes autorisées.

D- S’assurer que les applications informatiques sont fiables.

2.3. Constats du diagnostic

Suite à l’évaluation du système SIEM de Ooredoo Algérie, et suite à nos entretiens ;

A. **Ooredoo Algérie doit stocker ses sauvegardes dans un Backup extérieur de l’entité.**

Constat :

Nous avons décelé des problèmes dus aux sauvegardes qui ne sont pas stockées à l’extérieur de l’entité. En cas de sinistre, les informations seront définitivement perdues.

Elément d’évaluation :

Suite à l’entretien avec le senior risque management, nous avons pris connaissance que les données sont enregistrées dans le Datacenter situé à l’intérieur de l’entité, et non stockées dans le Backup à l’extérieur de l’entité. Si un incident survient au Datacenter l’information est perdue.

Recommandation :

Nous recommandons d’établir le stockage des sauvegardes à l’extérieur de l’entreprise dans un Backup, cela permet de prendre des mesures d’anticipation afin de sécuriser les actifs informationnels en cas de sinistre.

B. **L’équipe de sécurité doit être capable à tout moment, d’intervenir en cas d’événement de sécurité.**

Constat :

Nous avons également constaté que l'équipe de sécurité n'est pas capable d'intervenir en cas d'événement de sécurité, ce qui cause l'indisponibilité du système de sécurité.

Elément d'évaluation :

Vu les rotations de travail constatant qu'il n'y a pas d'équipe de sécurité travaillant la nuit, ni d'équipe d'intervention rapide si il y a une attaque informatique pour minimiser les dégâts et recouvrir les actifs informationnels.

Recommandation :

L'intervention en cas d'incident est très importante dans le maintien de l'activité, pour cela nous recommandons une sensibilisation et une formation de l'équipe d'intervention de sécurité.

C. **Ooredoo Algérie doit impliquer ses utilisateurs de système SIEM dans le développement informatique.**

Constat :

Il en est ressorti aussi que les utilisateurs du système ne sont pas impliqués dans le développement informatique, ce qui cause alors une méconnaissance des risques inhérents à la sécurité informatique, des difficultés à suivre et à gérer le changement et à impacter la culture de l'entreprise, une mauvaise utilisation des applications informatiques, et notamment une méconnaissance des nouvelles technologies de l'information.

Elément d'évaluation :

Nous avons pris connaissance des programmes de formation de l'entreprise, et nous avons constaté que les utilisateurs du système informatique SIEM, ne bénéficient pas d'une sensibilisation au développement informatique.

Recommandation :

Nous recommandons également l'implication des utilisateurs dans le développement des applications informatique, ce qui permet à l'entreprise d'évoluer en termes de technologie.

D. **Ooredoo Algérie doit élaborer des procédures de recensement d'anomalies.**

Constat :

Enfin, nous avons identifié une absence de procédures de recensement d'anomalies, ce qui entraîne que les anomalies peuvent être répétitives sans être corrigées.

Elément d'évaluation :

Vu le manque de système enregistrant les fichiers logs qui démontrent les moindres événements exécutés dans le système. Nous avons consulté les pièces comptables relatives à l'entretien et réparation du matériel informatique, et nous avons constaté que des pannes fréquentes surviennent (Carte-mère, remise en marche, réparations diverses) sans être recensées pour être corrigées.

Recommandation :

L'élaboration des procédures de recensement d'anomalies est fortement recommandée.

Conclusion du chapitre :

A l'issu des traveaux d'audit, nous avons relevé quelques anomalies susceptibles de compromettre le SIEM de Ooredoo Algérie, et donc l'intégrité, la confidentialité, et la disponibilité des informations.

A cet effet, il est vivement recommandé de mettre en place un plan d'actions efficace afin de prendre en charge les recommandations émises qui pourrait améliorer l'efficacité et du système informatique.

CONCLUSION GENERALE

En conclusion des points développés précédemment sur la sécurité informatique,

Nous retenons l'hypothèse selon laquelle la sécurité à 100% n'existe pas et que le risque zéro est un idéal que l'on ne peut atteindre. Comme dit le proverbe : la perfection n'est pas de ce monde !

En effet, ce que nous devons faire, c'est de protéger l'information qui est un actif précieux pour l'entreprise et le système informatique qui en est le support.

Ainsi, pour la sécurité informatique adéquate, il faut examiner deux éléments : ce qu'il faut protéger et comment le protéger ?

Assurer un niveau adéquat de sécurité n'est pas synonyme de surprotéger ce qui n'en vaut pas la peine, mais de protéger efficacement ce qui en vaut la peine, en plaçant la sécurité au niveau idoine dans l'administration de l'entreprise.

Cela étant, il ne faut jamais sous-estimer le facteur humain. Rien ne sert d'avoir des protections infaillibles si une personne interne de l'entreprise permet, à son insu, à un attaquant de déjouer toutes ces protections.

Aussi, faut-il rester attentif aux nouvelles technologies, aux mises à jour de logiciels de sécurité. Ne pas se fier totalement sur une sécurité jugée bonne à un moment donné.

La sécurité est omniprésente et nécessaire à tous les niveaux d'utilisation de l'information de sa création à sa destruction.

Enfin, la sécurité est un compromis entre efficacité et convivialité.

BIBLIOGRAPHIE

Ouvrage :

Application et action des dirigeants : Quelle piste pour améliorer la sécurité de l'information en PME. Auteur : Barlette Y. Année d'édition : 2011

Management des systèmes d'information. Auteurs : Kenneth et Jane Laidon. Année d'édition : 2013

Management de la sécurité de l'information-mise en œuvre, évaluation et pilotage de la sécurité de l'information dans les organisations.

Auteur : Cucchi A. Année d'édition : 2011

Article :

Kenneth LAUDON 2013 « La sécurisation d'un SI : une exigence absolue.»

Amir DJENNA 2022 « La création en Algérie d'une Ecole Supérieure en Cyber sécurité, une nécessité absolue »

Cyril André 2016 « Audit des systèmes d'information, le SI sous contrôle »

Site Web :

www.nist.gov

https://protectam.fr

https://fr.wikipedia.org

https://www.iso.org

ANNEXES

Annexe A : Guide d'entretien avec le spécialiste senior risque management.

Entité : Ooredoo Algérie	
Département / Service : Service d'audit interne.	
Fonction : Spécialiste senior risque management.	
Objectif de contrôle : S'assurer que l'organisation est capable de redémarrer les systèmes informatiques en cas d'arrêt ou destruction.	
Questions	**Réponses**
Les données sont-elles sauvegardées quotidiennement ?	
Les sauvegardes sont-elles stockées à l'extérieur de l'entité ?	
Les sauvegardes sont-elles testées régulièrement ?	

Annexe B : Guide d'entretien avec la spécialiste senior information security process management

Entité : Ooredoo Algérie
Département / Service : Service d'audit interne.
Fonction : Spécialiste senior information security process management

Objectif de contrôle : S'assurer que la sécurité du système informatique est adaptée au niveau de risque identifié et accepté par la direction.	
Questions	**Commentaires**
La politique de sécurité en place, est elle validée et supportée par la direction de l'entité ?	
Existe-t-il des outils de surveillance du système informatique ?	
L'équipe de sécurité est elle capable d'intervenir en cas d'événement ?	

Annexe C: Guide d'entretien avec le spécialiste sénior risque management.

Entité : Ooredoo Algérie	
Département / Service : Service d'audit interne.	
Fonction : Spécialiste senior risque management.	
Objectif de contrôle : S'assurer que les accès aux données et aux applications sont réservés aux personnes autorisées.	
Questions	**Commentaires**
La politique de gestion des mots de passe est elle efficace ?	

La gestion des droits d'accès est elle cohérente avec la séparation fonctionnelle des tâches ?	

Annexe D: Guide d'entretien avec Chef de service process management.

Entité : Ooredoo Algérie	
Département / Service : Gestion des processus	
Fonction : Chef de service	
Objectif de contrôle : S'assurer que les applications informatiques sont fiables	
Questions	**Commentaires**
Les utilisateurs sont ils impliqués dans les développements informatiques ?	
Existe-t-il des procédures de recensement d'anomalies ?	