RAPPORT DE PROJET

PROJET FIL ROUGE – WOOD – LOT 3

ATES Bünyamin, El BADAOUI Ilyes, TOUVEREY Paul, TATER Antoine, GODBILLOT Theo

I.Table des matières

II.Introduction

Ce livrable numéro trois a plusieurs cibles. Il suit les livrables techniques qui vous fournit toutes les solutions techniques que nous déploierons dans votre entreprise. Dans cette partie, nous vous présenterons les parties budgétaires, sécurisation du système d'information et vous démontrerons la viabilité du projet.

Par conséquent, le but de ce document est de déterminer les coûts associés au projet, ainsi que d'étudier la sécurité du système et de ses composants. Nous prouverons également que notre solution peut répondre à toutes les exigences exposées dans le livrable précédent.

1. IPTAB

a) Présentation

Nous représentons l'entreprise « IP TAB » qui œuvre dans le domaine de l'informatique & réseaux depuis 2001. Notre entreprise a commencé son activité en effectuant de la réparation d'ordinateurs. Après un chiffre d'affaires en hausse, « IP TAB » a réussi à obtenir de nombreux partenaires de plus en plus prestigieux. Nous travaillons avec de nombreux partenaires tels que VMWare, Dell, Microsoft et Google Workspace, ce qui nous permet d'obtenir des prix très compétitifs sur les différents produits et d'avoir des relations privilégiées pour le support.

Nos secteurs d'activités

- Maintenance informatique (systèmes et réseaux)
- Audit informatique, conseil
- Installation et configuration de serveurs
- Vente de matériel informatique

2. État des lieux

Avant le remplacement du parc informatique en 2019, aucun projet informatique n'a été mené dans l'entreprise.

Le Groupe Wood possède un « petit service informatique » interne (un technicien en intérim), un alternant et un responsable (plus l'aide des prestataires), aucun schéma directeur n'est en place. Ce manque de conduite claire sur l'informatisation du groupe depuis 10 ans a freiné la croissance de l'entreprise. Aujourd'hui, cela représente un blocage majeur qui a amené la direction a décidé d'investir dans une série de projets informatiques sur les trois années à venir. De plus, la direction a été sensibilisée aux risques informatiques et à la cybersécurité.

Le portefeuille de projets informatiques a été confié au directeur administratif et financier. Ce dernier a décidé de faire appel à un prestataire externe afin de sous-traiter l'intégralité de la mise en œuvre du projet ainsi que le passage en parti opérationnel (maintenance, support, qualité de service…).

La société de service devra être également une force de conseil sur l'évolution stratégique de l'entreprise et notamment sur la partie DSI. Le DAF a fixé une ligne de conduite pour les projets qui seront menés en parallèle :

- Évolution de l'architecture système et Réseaux
- Adoption d'un nouvel outil informatique type ERP
- Mise en place de processus de qualité de service informatique
- Sécurisation des informations

Chacun de ces projets a été approuvé par la direction du groupe. Les budgets ont été approuvés ; le DAF a confirmé qu'il était capable de les financer sur les trois années à venir.

3. Problématique

Nous avons pu remarquer que le groupe WOOD ne se préoccuper pas spécialement de la sécurité au sein de leurs infrastructures informatique. Du fait de la refonte que nous avons proposée sur les 2 premiers lots, concernant l'infrastructure systèmes et réseaux. Plusieurs points sont donc à revoir et pour ce lot 3 en termes de sécurité, nous avons la capacité de vous proposer des recommandations sur plusieurs points de sécurité qui pourrait être mis en place.

4. Objectifs

- Adopter un nouveau système d'information pour être plus réactif que la concurrence. Ce SI doit être spécifique aux métiers de l'entreprise.
- Pouvoir gérer une volumétrie de commandes au moins 30% plus élevé que celui qu'elle traite actuellement (la direction pense tripler le nombre de commandes grâce à son nouveau produit)
- Augmenter sa notoriété grâce à l'augmentation de la qualité de ses produits. La notoriété sera testée auprès des cibles particulières et collectivités par une étude par questionnaire chaque année. Cela sera complété par une étude d'image de marque gérée par le service qualité.
- Gagner des parts de marché à l'export. Aucun chiffre n'est actuellement annoncé par la DG mais le SI doit pouvoir s'adapter à une augmentation des ventes à l'export.

5. Périmètre

La politique de sécurité du système d'information s'applique à l'ensemble du groupe WOOD mais également tous ses prestataires ainsi que les intervenants sur le système d'information (stagiaires, salarié, sous-traitant, directeur des systèmes d'information…). Le plan s'appliquera donc à tous les sites du groupe WOOD.

- Le site de Lille : C'est le siège social. Il couvre les bureaux de la direction, un site de production et un entrepôt de stockage des matières premières et des produits finis.
- Le site de production (Dax) : Le site de Dax a été ouvert en 1993, il couvre un site de production, un entrepôt ainsi que des bureaux.
- Le site de production (Annecy) : Le site de Dax a été ouvert en 2012, il couvre un site de production, un entrepôt ainsi que des bureaux. Il a été ouvert pour les maisons modulaires en bois.
- Les magasins : Brest et Mâcon.

6. Enjeux

Le Groupe Wood table fortement sur le lancement de son nouveau produit, les maisons modulaires, pour dynamiser son chiffre d'affaires et pour gagner des parts de marché sur ses concurrents européens.

Malheureusement, la structure actuelle du Système d'Information (SI) du Groupe n'accompagne pas la croissance de l'entreprise.

La direction du Groupe a donc décidé en 2021 de moderniser son système d'information par le lancement de plusieurs projets informatiques qui seront réalisés sur l'année à venir, ainsi qu'en 2022.

Elle doit maintenant faire évoluer son infrastructure système et réseau pour accompagner l'évolution de l'information de ses processus métier.

7. Contraintes

- **Technique :** les solutions techniques (surtout les plus coûteuses) ne pourront être retenues que si elles fournissent un gain substantiel à l'entreprise.
- **Financière** : Une enveloppe 200 000 € pour la sécurisation de l'ensemble de l'infrastructure
- **Organisationnelle** : Le projet devra être mené en utilisant une métrologie ou un référentiel. De plus, il devra être piloté par les risques projet (et produit).
- **Temporelle** : 11 mois ont été accordés afin de mener à bien le projet.
- **Sociale** : La mise en place doit être transparente pour les employés. La solution doit être mise en place en parallèle des activités de l'entreprise

III.Conception de la sécurité

8. PSSI

Le groupe WOOD n'est pas à l'abri d'une panne, d'un sinistre, d'une erreur humaine ou d'une attaque informatique. Avec une politique de sécurité du système d'information, ou PSSI, nous pourrons limiter les dégâts, afin de prévenir l'incident et par la suite exécuter les démarches à suivre pour une reprise de l'activité rapide du client.

La PSSI est un ensemble de documents qui présentent les règles de sécurité à appliquer et à respecter, ainsi que l'organisation qui permet sa mise en œuvre dans une entreprise.

Basée sur l'analyse des risques, la PSSI est un véritable plan d'action, qui va assurer un niveau de sécurité dans le changement du système informatique du groupe WOOD.

C'est aussi un outil de communication sur l'entreprise et sur les méthodes de sécurité informatique.

Il reflète une vision stratégique et s'inscrit dans une démarche globale d'amélioration continue pour le groupe WOOD.

Il suit la structure de la norme ISO 27002, qui est une norme internationale de sécurité des systèmes d'information de l'ISO, elle permet de protéger de la manière la plus efficace le patrimoine que représentent les systèmes d'information

Le PSSI s'articule autour de dix principes directeurs qui sont :

- Gestion des actifs et des risques,
- Respect des règles de sécurité par le personnel,
- Organisation de la sécurité des systèmes informatiques,
- Classification des informations,
- Contrôle d'accès et habilitations,
- Gestion de l'exploitation et des communications,
- Continuité d'activité,
- Sécurité Physique,
- Gestion des incidents,
- Développement de système et maintenance.

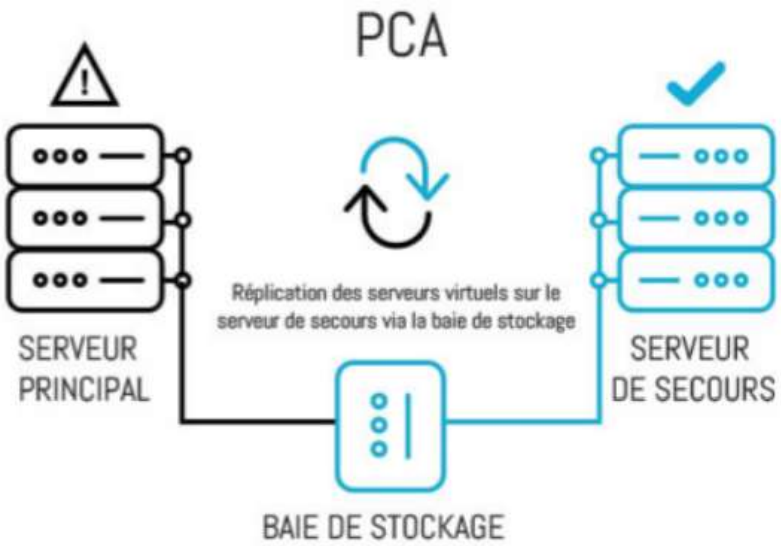
9. PCA & PRA

a) PCA

On sait bien que la résilience des systèmes d'information et de plus en plus critique pour les entreprises, en effet l'interruption du système d'information a d'énorme répercutions sur la production des entreprises et donc des enjeux financiers s'ensuivent.

Le plan de continuité d'activité aura pour objectif de continuer l'activité sans perte de service, ou avec une légère dégradation acceptable afin de rendre résilient le système d'information du groupe WOOD. Le PCA permettra aussi aux utilisateurs du groupe WOOD de travailler avec leurs outils informatiques afin d'avoir aucun problème en production.

Pour ce faire, nous préconiserons différents moyens à mettre en œuvre et assurer la continuité de vos activités.

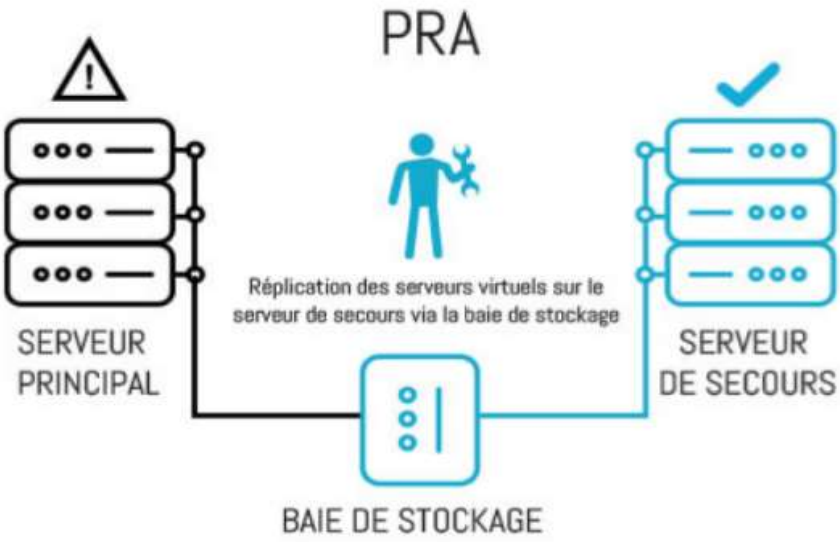


b) PRA

Le PRA (Plan de Reprise d'Activité) est considéré comme un complément du PCA ou comme un palliatif en cas d'absence du PCA. Il se compose de processus à mettre en œuvre après la survenue d'un incident pour permettre à l'entreprise de reprendre son activité normale progressivement.

Il permettra en cas de problème majeurs ou situation critique du système d'information du groupe WOOD, de pouvoir reconstruire ou de basculer sur un système de relève.

Pour ce faire, le PRA doit être précis, en effet il doit être mis à jour régulièrement durant la continuité du projet au risque d'être inefficace le jour où nous aurons besoin de l'activer au sein du groupe WOOD.



c) PRA / PCA – Quelles sont les différences ?

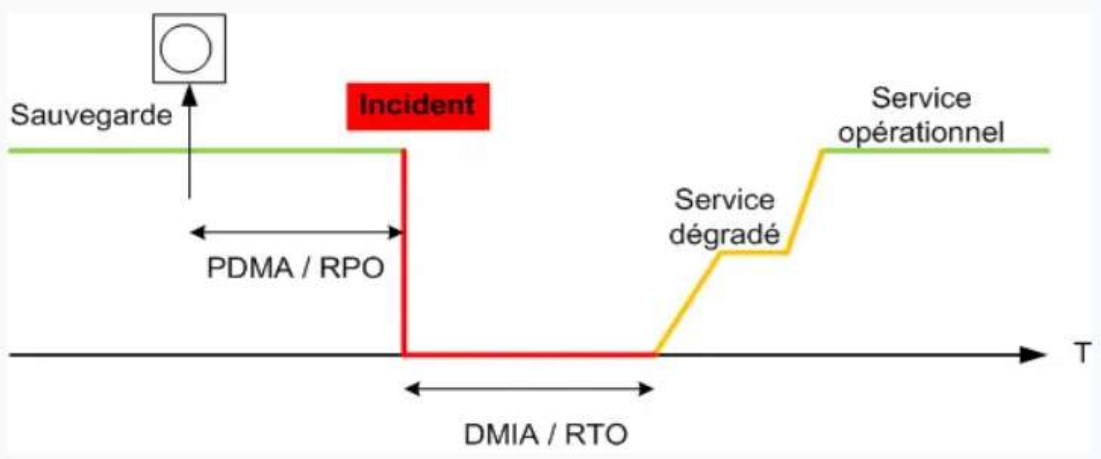
Les différences entre PRA et PCA se situe principalement sur le temps acceptable, pour une entreprise, d'arrêt de production ou d'activité, mais aussi au niveau financier car le PCA opte pour des solutions plus chères car plus pousser et plus réactive qu'un PRA.

Plus précisément, deux notions marquent cette différence :

-le RTO (Recovery Time Objective) représente la durée maximale d'interruption admissible de vos services à la suite d'une panne ou d'un sinistre.

-et le RPO (Recovery Point Objective) qui désigne la durée maximum d'enregistrement des données qu'il est acceptable de perdre lors d'une panne.

En synthèse, un plan de reprise d'activité informatique aura toujours un RTO supérieur à zéro et un RPO supérieur ou égal à zéro, et un plan de continuité d'activité informatique aura toujours un RTO égal à zéro et un RPO égal à zéro.



En cas de panne, le groupe WOOD bénéficiera d'un meilleur temps de rétablissement de service. Cela permettra de limiter l'impact financier, pendant laquelle l'entreprise ne produira pas, pour cela nous allons mettre en place un PCI (Plan de continuité informatique)

d) PCI

Le plan de continuité informatique (PCI) est une sous partie du plan de continuité d'activité (PCA), qui permettra la reprise du système d'information (SI) lorsque celui-ci est impacté par un sinistre ou défaillance majeure. Son but est de contribuer à redémarrer l'activité du le plus rapidement possible et de minimiser la perte de données.

La démarche de mise en œuvre du PCI permettra d'identifier le degré des activités critiques en les analysant afin d'éviter les impacts qui résulteraient d'un arrêt d'activité.

Il permettra d'estimer les besoins en matière de ressources humaines et physique (poste de travail), en permettant au groupe Wood une reprise du SI en fonctionnant en mode dégradé et ne pas avoir une coupure en production.

Cette approche perme*t d'identifier les mesures nécessaires pour réduire les risques, et dans certains cas, les annuler.*

Nous mettrons donc en place des sauvegardes de toutes les données ainsi que des serveurs de redondances qui permettront d'avoir pour chaque site un recours en cas de panne ou de donnée effacé, par exemple les données des machines virtuelles situé au siège à LILLE seront redondées sur un autre serveur tandis que les données des machines auront un backup sur un NAS locale.

Les délais de rétablissement établis dans le tableau ci-dessous sont basés sur des systèmes redondants mais également sur l'engagement vis-à-vis de plusieurs prestataires.

Service	Impact sur la production	Durée d'interruption accepté (/mois)	Temps de rétablissement estimé
Serveur de sauvegarde	Majeur	2 heures	Inférieur à 1 heure
Réseau LAN	Majeur	15 minutes	Inférieur à 3 minutes
Réseau WAN	Majeur	15 minutes	Inférieur à 3 minutes
Serveurs de fichiers	Majeur	15 minutes	Inférieur à 3 minutes
Active Directory	Majeur	30 minutes	Inférieur à 3 minutes
Accès WI-FI	Mineur	5 heures	Inférieur à 3 heures
Supervision	Modéré	3 heures	Inférieur à 1 heure
Service d'assistance aux utilisateurs	Mineur	3 heures (astreinte disponible)	Inférieur à 1 heure
DNS	Majeur	30 minutes	Inférieur à 3 minutes
DHCP	Majeur	30 minutes	Inférieur à 3 minutes

10. Justification des normes ISO 9001 et PCI DSS

a) Définition

La norme ISO 9001 'Systèmes de management de la qualité — Exigences' est un référentiel basé sur le principe de l'amélioration continue qui permet d'instaurer un système de management axé sur la qualité et la satisfaction de vos clients pour le produit/service vendu.

Cette démarche est certifiable et permet de faire valoir votre engagement en termes de système de management de la qualité.

b) Pourquoi mettre en place une norme ISO 9001 ?

La mise en place de cette norme a pour objectif de cadrer votre système de management par la qualité. En effet, la norme ISO 9001 traite de l'organisation à mettre en place sur la base de 3 chapitres de généralités et 7 chapitres d'exigences opérationnelles.

Sur le plan stratégique, elle permet de garantir un nombre de non-conformité en baisse et donc, limite tous les coûts liés à la non-qualité.

Sur le plan commercial, ce gage de qualité est souvent demandé par vos clients et vous ouvre les portes de nouveaux marchés

c) Comment mettre en place la certification ISO 9001 ?

Mettre en place la certification ISO 9001 est un projet important à bien préparer. Ainsi, nous proposons un plan de déploiement avec des étapes simples permettant de déployer un SMQ. Il s'agit de déployer les lignes directrices d'un référentiel international. Celui-ci est exigent et demande de la préparation. Ainsi environ 10 étapes sont nécessaires pour **mettre en place la certification ISO 9001**.

1. Connaître son contexte
2. Définir les objectifs et rédiger sa politique Qualité
3. Identifier ses enjeux internes et externes
4. Identifier et suivre ses parties intéressées
5. Décrire son périmètre de certification (processus)
6. Impliquer le personnel et affecter les moyens
7. Assurer la maitrise de ses produits et/ou prestations
8. Maitriser les achats et les prestataires externes
9. Mesurer la satisfaction des clients
10. Surveiller et évaluer les performances
11. Améliorer / progresser

Par exemple la maitrise de vos produits et/ou services se décline grâce à la maitrise opérationnelle. Cela passe par le suivi, l'analyse et les correctifs de vos processus opérationnels / de réalisation. Cette étape est le prolongement l'étape 5 qu'est l'approche processus. La maitrise opérationnelle est très importante et s'appuie sur un chapitre majeur de l'ISO 9001 : la maitrise des activités opérationnelles.

De plus, l'étapes Améliorer / progresser correspond à l'amélioration continue. Il s'agit de tous les outils liés à l'identification des dysfonctionnements, des non-conformités, les analyses de causes.

11. PCI DSS: Payment Card Industry Data Security Standard

a) Qu'est-ce que la norme PCI DSS ?

La **norme de sécurité de l'industrie des cartes de paiement** est un standard de sécurité des données qui s'applique aux différents acteurs de la chaîne monétique. Elle est établie par cinq principaux réseaux cartes (**Visa, MasterCard**, **American Express**, **Discover Card** et **JCB**) et est gérée par le **Conseil des normes de sécurité PCI.** Cette norme a été créée afin d'augmenter le contrôle des informations du titulaire de la carte dans le but de réduire l'utilisation frauduleuse des instruments de paiement.

b) Conditions

Le PCI DSS spécifie **12 conditions de conformité**, regroupées dans 6 groupes appelés **« objectifs de contrôle** ».

Ces 12 conditions ont été divisées en sous-conditions plus précises mais celles-ci n'ont pas changé depuis la création du standard.

Les 6 objectifs de contrôle :

-Création et gestion d'un réseau et d'un système sécurisé
-Protection des données du titulaire
-Maintenir un programme de gestion des vulnérabilités
-Mise en œuvre de mesures de contrôle d'accès strictes
-Surveillance et test réguliers des réseaux
-Maintenir une politique de sécurité des informations

c) Les 12 conditions divisées en sous-conditions

1. Installer et gérer une configuration de pare-feu pour protéger les données du titulaire de carte
2. Ne pas utiliser les mots de passe et autres paramètres de sécurité par défaut définis par le fournisseur
3. Protéger les données stockées du titulaire
4. Chiffrer la transmission des données du titulaire sur les réseaux publics ouverts
5. Protéger tous les systèmes contre les logiciels malveillants et mettre à jour régulièrement les logiciels anti-virus ou programmes
6. Développer et gérer des systèmes et des applications sécurisés
7. Restreindre l'accès aux données du titulaire aux seuls individus qui doivent les connaître
8. Identifier et authentifier l'accès aux composants du système
9. Restreindre l'accès physique aux données du titulaire
10. Suivre et surveiller tous les accès aux ressources réseau et aux données du titulaire
11. Tester régulièrement les processus et les systèmes de sécurité
12. Maintenir une politique qui adresse des informations de sécurité pour l'ensemble du personnel

12. Respect du RGPD

Le Règlement Général sur la Protection des Données, ou RGPD, est un document publié par le Parlement européen le 27 avril 2016. Ses principaux objectifs sont d'accroître à la fois la protection des personnes concernées par un traitement de leurs données à caractère personnel et la responsabilisation des acteurs de ce traitement. Pour résumer : Un encadrement des données des personnes, et un encadrement des personnes y avant accès.

Si le règlement n'est pas appliqué, la Commission Nationale de l'Informatique et des Libertés (CNIL), à le pouvoir de dissuader et de sanctionner.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Afin d'être conforme à ce règlement, il est nécessaire de prendre plusieurs dispositions. Tous les sujets et exemples évoqués ici sont retrouvables sur le site internet de la CNIL.

a) Constituez un registre de vos traitements de données

Le registre permet de recenser toutes les activités de l'entreprise qui traitent des données personnelles. Pour chaque activité, il est important de répertorier :

- **L'objectif poursuivi** (exemple : la fidélisation client)
- **Les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire)
- **Qui a accès aux données** (exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs)
- **La durée de conservation de ces données** (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

Ce registre sera placé sous la responsabilité du dirigeant de Wood.

Il est important de communiquer régulièrement avec chaque service de l'entreprise afin d'avoir un registre exhaustif et à jour.

b) Faites le tri dans vos données

Avoir beaucoup de données veut dire plus de travail pour les traiter et les stocker. Il est donc important de trier les données, et de retirer celles qui seraient superflues.

Pour chaque fiche de registre créée, il faudra vérifier que :

- Les données que vous traitez sont nécessaires à vos activités (par exemple, il n'est pas utile de savoir si vos salariés ont des enfants, si vous n'offrez aucun service ou rémunération attachée à cette caractéristique)
- Vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter. Nous reviendrons sur ce point plus tard.
- Seules les personnes habilitées ont accès aux données dont elles ont besoin
- Vous ne conservez pas vos données au-delà de ce qui est nécessaire.

Il est important de minimisez la collecte de données, en éliminant toutes les informations inutiles. Il faudra potentiellement redéfinir qui aura accès et à quelles données dans l'entreprise.

Il faut penser à mettre ça quand cela est possible, des règles automatiques d'effacement ou d'archivage au bout d'une certaine durée dans les applications.

c) Respectez les droits des personnes

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).

À chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Vérifiez que l'information comporte les éléments suivants :

- Pourquoi vous collectez les données (« la finalité » : par exemple pour gérer l'achat en ligne du consommateur)
- Ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime »)
- Qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.)
- Combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle »)
- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
- Si vous transférez des données hors de l'UE (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Pour éviter des mentions trop longues au niveau d'un formulaire en ligne, vous pouvez par exemple, donner un premier niveau d'information en fin de formulaire et renvoyer à une politique de confidentialité / page vie privée sur votre site internet.

Une fois ces mentions renseignées sur tous les supports, vous avez répondu à votre obligation de transparence.

Il est important de faciliter les personnes à faire valoir leurs droits. Pour ce faire, il y a plusieurs solutions possibles. En utilisant le site web de WOOD, il est possible de mettre en place un formulaire de contact spécifiquement dédié à cela. Concernant les achats en ligne, si l'utilisateur dispose d'un compte client, il est possible de lui mettre à disposition une option permettant à l'utilisateur d'exercer leurs droits à partir de leur compte directement.

Il est intéressant de mettre en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum) afin de répondre le plus efficacement aux demandes des personnes.

Conseil de la CNIL :

Bonne pratique : soyez réactifs !

Bien traiter les demandes des consommateurs quant à leurs données personnelles, c'est :

- .Renforcer la confiance qui sécurise la relation-client ;
- .Vous mettre à l'abri de critiques sur les réseaux sociaux, ou de plaintes auprès de la CNIL.

d) Sécurisez vos données

Étant donné que le risque zéro n'existe pas en informatique, il est nécessaire de prendre les mesures nécessaires pour sécuriser les données. Grace à ces mesures mises en place, les risques de pertes de données ou de piratage seront réduits.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas de d'incident.

Des réflexes doivent être mis en place : mettre à jour de vos antivirus et logiciels, bien choisir ses mots de passe, chiffrer vos données dans certaines situations et faire des sauvegardes.

Les failles de sécurité entraînent également des conséquences pour ceux qui vous ont confié des données personnelles : Ayez à l'esprit les conséquences pour les personnes et pour votre entreprise.

Conseil de la CNIL :

BONNE PRATIQUE

Pour évaluer le niveau de sécurité des données personnelles dans votre entreprise, voici quelques questions à se poser :

- .Les comptes utilisateurs internes et externes sont-ils protégés par des mots de passe d'une complexité suffisante ?
- .Les accès aux locaux sont-ils sécurisés ?
- .Des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?
- .Avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?

IV.Charte utilisateur

Un projet de charte utilisateur a été mis en place afin d'accompagner les collaborateurs. En effet, la charte utilisateur est la première barrière entre l'utilisateur et les dangers d'internet.

Elle a pour but d'expliquer au mieux à l'utilisateur tous les outils qui sont mis en place pour le protéger lui et le réseau de l'entreprise. Elle a aussi pour but de lui expliquer les bons principes d'usage du matériel qui lui est mis à disposition, et lui explique également les dangers qu'une mauvaise utilisation de ces derniers, peut provoquer. Cette charte servira à avertir des potentielles sanctions encourues lors du non-respect de cette dernière.

Voici quelques règles d'exemple de notre charte utilisateur que nous souhaitons mettre en place :

- . Verrouiller son ordinateur dès que l'on quitte son poste
- . Ne jamais télécharger des pièces jointes de mail sans être sans connaitre l'envoyeur
- . Toujours regarder l'url si nous allons sur un site incertain
- . Ne pas divulguer son identifiant/mot de passe à qui que ce soit
- . Ne pas installer de logiciel sans l'autorisation du service informatique
- . Or autorisation donnée de la direction, le matériel informatique pro ne doit pas sortir de l'enceinte de l'établissement
- . Rien de chez soi ne rentre en contact avec le matériel de l'entreprise (par exemple les clefs USB)
- . Les téléphones pros sont donnés à des fins professionnelles, il ne doit pas être utiliser pour autre chose.
- . Marquer tous documents comportant des données sensibles.
- . Utiliser les outils de chiffrage mis à disposition pour tout document sensible transmis (exemple, 7zip)

V.Sécurisation

1. Sécurisation physique de l'infrastructure

Comme nous l'avons évoqué dans le lot 2, nous avons mis en place de la redondance sur la plupart des liaisons switch et routeur. Cela permettra en cas de panne d'assurer le bon fonctionnement du réseau informatique sans pour autant que de grosses perturbations se ressentes.

Nous avons ensuite procédé à la mise en place du sticky mac, plus communément appelé Security Port. Le principe du Security Port et d'attribuer, à chaque port de switch, une adresse mac unique, de sort à ce que personne ne puisse avoir accès au réseau en se branchant à n'importe quel port.

Cette mesure a encore une fois été prise pour apporter plus de sécurité et de sureté au réseau.

Le seul inconvénient à cette prise de décision va être le temps supplémentaire qui va être mit à reconfigurer les adresses uniques de ports à chaque changement de place d'un poste utilisateur.

2. Sécurisation logique de l'infrastructure

a) Comptes utilisateurs :

GPO

Dans le même axe de sécurité, l'ajout de GPO utilisateur est apparu comme une bonne idée. En effet, les gpo permettent de créer les règles supplémentaires pour les utilisateurs afin d'ajouter de la sécurité. Dans ce sens, nous avons donc créés une gpo permettant de verrouiller automatiquement une session au bout d'un certain temps d'inactivité.

Ce choix a été fait après avoir remarqué de beaucoup d'utilisateurs partent de leurs postes en le laissant allumé et déverrouillé, ce qui constitue une faille de sécurité important car n'important qui pourrait prendre possession de ces ordinateurs en question et pourrais en faire ce qu'ils veulent.

La GPO a donc été réalisée dans la catégorie stratégie de groupe et dans la sous-partie options de sécurité. Après réflexion de la part du service, nous avons décidés de mettre le verrouillage de la session pour inactivité au bout de 15 minutes, après une validation du CODIR (comité de direction) de l'entreprise.

Droits utilisateurs

Nous avons procédé à la création d'un compte administrateur local universel sur tous les postes, que nous appellerons « Admin », au cas où le service est besoin d'intervenir sur le poste sans que l'utilisateur ne soit là pour rentrer ses identifiants de connexion. Dans un second temps, nous opérerons ensuite avec la suppression des droits d'administrateurs des utilisateurs.

Pour ce faire, nous sommes passé par la création d'un script permettant de créer le fameux compte administrateur local universelle à tous les postes dans un premier temps, et d'ensuite supprimer les droits administrateurs aux utilisateurs.

En effet, si l'ensemble des utilisateurs étaient administrateurs de leurs postes, cela représenterait une faille de sécurité très importante, dans un premier temps car l'utilisateur peut accéder à l'ensemble des paramètres systèmes de son poste alors qu'il n'en a pas l'utilité.

Dans un second temps cela est aussi une faille importante car l'utilisateur peut installer n'importante quel programme sans autorisation d'un administrateur, ce qui peut être très dangereux si l'utilisateur installe un programme comportant un logiciel malveillant par exemple.

Horaires d'accès

En plus de l'ajout de toutes ces règles que le verrouillage automatique des postes et la suppression des droits administrateurs, une plage d'horaire fixe a été mise en place afin de limiter les abus de dépassement d'horaire.

En effet, passé une certaine limite l'heure, la session e verrouillera automatiquement et l'utilisateur verra sa connexion impossible jusqu'à la prochaine plage d'horaire fixé. Cet ajout a été possible grâce au gestionnaire de parc Active Directory, qui intègre cette option.

b) Postes de travail

Mot de passe

La meilleure solution est d'instaurer une politique de mot de passe fixe et pour tout le monde.

La première chose qui a été mené est la réflexion de la complexité des mots de passe qui nous allons imposer. Plusieurs possibilités s'offrent à nous, il est possible le jouer avec le nombre de caractère minimum (en général cette dernière est placée à 8 caractères minimum), il est aussi possible de demander des caractères minuscules ou majuscules, des chiffres ou bien encore des caractères spéciaux.

La question suivante à nous poser a été sur quelle durée les mots de passes se réinitialisent et combien est le nombre de mot de passe enregistrer dans l'historiques.

Par exemple, nous pouvons mettre un renouvellement des mots de passe tous les mois avec un historique de mots de passe de 12, ce qui signifierais que l'utilisateur peut réutiliser son premier mot de passe rentrer le 13 mois après l'application de la politique.

Le souci de ce temps de renouvellement est que cela devient vite contraignant pour les utilisateurs et un énervement pourrais se ressentir et ce n'est pas le but.

Le risque majeur de ce dispositif est que l'utilisateur le prenne comme une contrainte et ne veille pas jouer le jeu à cause d'un manque d'adhésion. Qu'il se plaigne constamment parce que ça l'embête ou autre, alors que ce dispositif est simplement là pour lui créer plus de sécurité.

Ce qui peut malheureusement aussi arriver si l'utilisateur ne joue pas le jeu, c'est qu'il va simplement marquer son compte d'accès sur un post-it et le coller sur le rebord de son écran, chose qui a pu être constaté dans les précédant mois dans l'entreprise.

C'est donc avec toutes ces exigences la que nous avons fait le choix de partir sur une politique de mot de passe comportant 8 caractères minimum, devant posséder au moins 3 des 4 spécificités suivantes, chiffre, lettre majuscules ou minuscules, ainsi que symboles. Ces mots de passe auront une durée de vie de 6 mois avec un historique d'ancien mot de passe de 5.

Nous avons fait ce choix avec la certitude que cette durée est la plus optimale pour que la stratégie reste sécuritaire sans pour autant que cela devienne une contrainte pour l'utilisateur.

c) Verrouillage après échecs

Pour plus de sécurité des postes, un verrouillage du compte va être mis en place après trop d'échec de mot de passe.

En effet, après 5 mauvaises tentatives de mots de passe pour accéder au compte, le compte en question se verrouillera automatiquement pour une durée de 30 minutes.

Passé ce délai de 30 minutes, l'utilisateur peut retenter son mot de passe, encore une fois avec 5 essais possible.

Cette méthode permet d'éviter les personnes malveillantes voulant prendre le contrôle du poste d'un collaborateur. Cette méthode est surtout efficace contre la méthode dite "Brute-force" qui consiste à enchainer toutes les tentatives de mot de passe possible.

Ce paramètre a pu être mit en place encore une choix grâce à l'outil Active Directory.

d) WSUS: Windows Server Update Services :

Ne pas réaliser les mises à jour de sécurité les plus récentes peut devenir une faille de sécurité pour votre réseau. WSUS est un service permettant de distribuer les mises à jour pour Windows et d'autres applications Microsoft sur les différents ordinateurs au sein de votre parc informatique. Ce serveur télécharge et stocke ponctuellement l'ensemble des mises à jour disponibles auprès des serveurs Windows Update de Microsoft et rend possible le contrôle de la diffusion de celles-ci dans le parc. Le serveur WSUS est déjà en place au sein de l'infrastructure du groupe WOOD il faudra le remettre à jour et s'assurer que les machines reçoivent bien les mises à jour.

e) WDS

Qu'est-ce que WDS ?

Windows Deployment Services, est un rôle inclus dans le système Windows 2012 R2. Ce rôle consiste à déployer automatiquement des images système via le réseau. Une image standard ou modifiée est clonée sur les machines se connectant au réseau de l'entreprise. Ceci permet ainsi un déploiement rapide et automatique au sein du parc informatique.

Fonctionnalités associées au serveur WDS :

PXE serveur :

Le PXE serveur permet aux clients de démarrer depuis le réseau via la méthode « boot PXE ». Il dispose également de son propre serveur DHCP.

Image serveur : L'image serveur fournit les images d'installation stockées sur le serveur WDS. TFTP serveur : Le serveur TFTP permet aux clients de télécharger les fichiers contenus dans WDS.

Principe de fonctionnement :

Client : Le client boot sur le réseau, demandant alors au serveur DHCP une adresse IP pour pouvoir initialiser le clonage de l'image sur son système. Une fois son adresse IP attribuée, le client télécharge l'image disponible sur le serveur WDS et l'installation se lance.

Serveur DHCP :

Le serveur certifie du droit de la demande d'adressage IP. Si le client est éligible à avoir accès, le serveur DHCP donne au client l'accès au serveur TFTP.

Serveur WDS :

Le serveur WDS héberge les images, les fichiers de boot, et le serveur TFTP. V. Avantages et inconvénients : Avantages : o Installation rapide et simple o Déploiement en masse o Facilité de prise en main o Personnalisation des images déployées Inconvénients : o Le trafic réseau est ralenti le temps de transfert de l'image o L'intégration de drivers nécessite des connaissances plus spécifiques.

Avantages et inconvénients :

Avantages :

- Installation rapide et simple
- Déploiement en masse
- Facilité de prise en main
- Personnalisation des images déployées

Inconvénients :

- Le trafic réseau est ralenti le temps de transfert de l'image
- L'intégration de drivers nécessite des connaissances plus spécifiques.

f) Antivirus

Pour assurer la sécurité de l'ensemble de votre infrastructure, nous souhaitons mettre en place ESET comme nous avions déjà pu en parler au lot 1. Le déploiement d'un antivirus au sein du groupe va permettre de protéger vos ordinateurs contre les malwares et également contre les attaques des personnes malveillante. Il va analyser les données, les logiciels et les pages web qui transitent par le réseau vers vos appareils. C'est un outil essentiel pour la sécurité de votre réseau.

Caractéristique principale d'eset :

- Protection des systèmes d'exploitation : Windows, macOS, Android
- Protection contre les malwares, ransomwares & hameçonnages
- Surveillance des objets connectés et protection du réseau
- Gestionnaire de mots de passe
- Chiffrement des données sensibles
- Protection contre les menaces inconnues

g) VLAN

Pour un meilleur cloisonnement des matériels réseaux, nous allons mettre en place des vlan afin que chaque matériel aille dans son propre sous réseau. Cela permet d'augmenter la sécurité et l'étanchéité du réseau étant donné que seuls les machines dans le même Vlan peuvent discuter entre elles. Par exemple, même si une personne malveillante arrive à obtenir une adresse réseau dans le Vlan des postes de travail, il lui sera impossible de récupérer des informations venant des serveurs qui ne sont pas dans le même Vlan.

Voici une description des différents VLAN :

Réseau	Plage IP	Passerelle	VLAN	Nombre d'adresses disponibles	Détails
10.59.10.0/24	10.59.10.0 - 10.59.10.254	10.59.10.254	10	254	Postes de travail
10.59.20.0/24	10.59.20.0 - 10.59.20.254	10.59.20.254	20	254	Serveurs
10.59.30.0/24	10.59.30.0 - 10.59.30.254	10.59.30.254	30	254	VoIP
10.59.40.0/24	10.59.40.0 - 10.59.40.254	10.59.40.254	40	254	Wifi
10.59.50.0/24	10.59.60.0 - 10.59.60.254	10.59.50.254	50	254	Imprimante

Comme vous pouvez le constaté, le réseau de chaque site est divisé en 5 Vlan distincts.
Le premier, qui est le Vlan 10, est utilisé pour l'ensemble des postes de travail des collaborateurs. Le deuxième, qui est lui le Vlan 20, est utilisé pour les équipements serveurs. Le troisième, le 30, est quant à lui pris pour les VoIP, ce qui correspond à toute la partie téléphonie. Le Vlan 40 correspond lui aux adresses utilisées pour le Wifi. Enfin, le Vlan 50 est utilisé pour les imprimantes des collaborateurs, allant de la petite imprimante de bureau, aux gros photocopieurs.

VI.Sécurisation des salles serveurs

La salle serveur représente véritablement le cœur de l'entreprise du groupe WOOD. Toutes les précautions doivent être prises afin d'éviter tous dommages (numériques mais aussi physiques) qui pourraient mettre en péril l'activité de l'entreprise. C'est pour cela que nous vous recommandons les mesures de sécurité suivantes :

- Key Blue Smart pour l'accès à la salle serveur réservé au SI
- Caméra de surveillance devant l'entrée de la salle serveur
- Mettre en place deux Climatisations
- Mettre une sonde de température pour être alerter en cas d'une hausse de température
- Equiper la salle d'extincteurs à poudre pour les feux d'origine électrique
- Peindre les salles serveurs avec de la peinture ignifuges.
- Mettre des onduleurs en redondances
- Mettre un système d'alerte et de détection d'incendie
- Porte coupe-feu
- Condamnation des fenêtres

VII.Sécurisation réseau de l'infrastructure

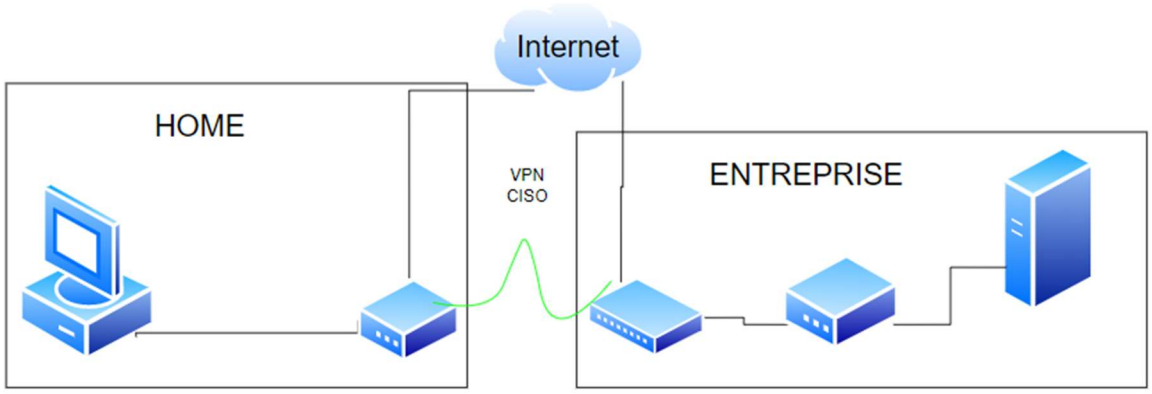
1. VPN

Le VPN ou Virtual Private Network est comme son nom l'indique un réseau virtuel privé. Il permet de créer un « tunnel » chiffré de bout en bout entre 2 points. Par exemple, l'ordinateur d'un collaborateur lorsqu'il est chez lui, jusqu'un serveur.

Pour développer, cela permet d'avoir accès aux ressources d'un réseau accessible uniquement en faisant partie de ce même réseau. Par exemple, avec un accès VPN, je peux, de chez moi accéder aux serveurs de données ou imprimante de l'entreprise. Entre autres, il permet aussi de naviguer sur le web de manière anonyme et sécurisé. Le VPN est utile car il réalise une connexion chiffrée, entre notre ordinateur et un serveur VPN, ce qui rend difficile pour quelqu'un d'extérieur (un pirate par exemple), de savoir ce qui est communiqué entre les deux terminaux. De plus, notre adresse IP ne sera pas indiquée, à sa place, ce sera celle du serveur VPN.

Le fonctionnement du VPN :

Un VPN repose sur un protocole, appelé protocole de tunnelisation (tunneling), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.



a) Pare-feu

Afin de rajouter une couche supplémentaire de sécurité, nos routeurs Meraki sont équipés d'un pare-feu.

Ce pare feu permet plusieurs fonctionnalités :

- Gérer le(s) VPN mentionné(s) ci-dessus
- Gérer les règles et les ouvertures de port
- Gérer le SD-WAN
- Gérer les catégories bloquées (voir exemple ci-joint)
- Gérer les adresses IP émanant de certains pays (Les bloquer, ou non)

Grâce à toutes ces fonctionnalités, nous nous assurons qu'il n'y est pas (ou peu à minima) de données pouvant fuiter vers l'extérieur.

Nous nous assurons aussi que le réseau n'est pas accessible, ou de manière limitée, depuis l'extérieur.

2. Sécurisation des données

a) Données utilisateurs

Les données utilisateurs sont très souvent une source d'attaque. En effet, une majorité de virus s'attaquent à celles-ci (Phishing, ransomware, etc.)

Pour pallier ces attaques, il est important de les sécuriser.

Pour cela, plusieurs choix s'offrent à nous :

- Mettre en place des sauvegardes régulières

  Des sauvegardes régulières permettent de récupérer des données perdues, volées ou corrompues. Il est important que ces sauvegardes soient régulières, afin de perdre le moins de temps de travail possible.

- Mettre en place BitLocker

BitLocker est une fonctionnalité intégrée de base à Windows. Il s'attaque aux menaces que constituent le vol ou l'exposition de données provenant des ordinateurs perdus, volés ou mis hors service de façon inappropriée.

- Sensibiliser les utilisateurs

Un utilisateur sensibilisé est un risque en moins. En effet, la formation des utilisateurs à ces diverses attaques leurs permettrons de les reconnaitre plus facilement. Faux mail, pièce jointe infectée, lien de téléchargement suspicieux, etc. Tous ces risques connus réduiront la perte de donnée.

b) Données serveurs

Les données des serveurs, comme les données des utilisateurs, ont besoin d'être sauvegardées. Au-delà de tous les risques liés aux attaques pirates, il y a tous les risques liés au matériel, ainsi que ceux liés aux incidents pouvant survenir.

Tous les points mentionnés ci-dessus s'appliquent donc ici. Nous pouvons tout de même ajouter quelques autres points :

- Mettre en place un archivage régulier

Des données archivées peuvent être stockées sur plusieurs support (bande magnétique, disque dur, etc.) Ces données archivées (Donc non modifiable, uniquement consultable !), de par leur nature, éviterons aux utilisateurs de modifier ces données, ou même de les supprimer.

- Gérer les habilitations

Il est important de limiter l'accès des utilisateurs aux données sensibles. Des utilisateurs ayant un accès restreint limite la fuite de données, qu'elle soit intentionnelle ou non.

3. Supervision

a) Utilité et importance supervision en entreprise

Avant de nous pencher sur l'utilité de la supervision, nous allons tout d'abord présenter son principe.

La supervision informatique est une technique de surveillance, d'analyses et d'alertes permettant de pallier les problèmes liés à tous les niveaux de fonctionnement informatique d'une entreprise. En d'autres termes, elle permet un suivi de l'activité des équipements informatiques au sein de l'entreprise. Nous allons voir son utilité au sein du groupe WOOD. Comme nous l'avons énoncé précédemment, elle permettra de surveiller toutes les équipement réseaux, en ce qui nous concerne les machines virtuelles installées ainsi que les hardwares et softwares des divers serveurs des sites WOOD. Ainsi la supervision permettra de réagir plus rapidement, voire d'anticiper un éventuel disfonctionnement et par conséquent permettre d'éviter un arrêt de production entre les divers sites, ce qui représenterait un gros coût pour l'entreprise WOOD.

L'intérêt d'une bonne supervision informatique est une gestion optimale du parc informatique à tous les niveaux. Les enjeux en matière de supervision sont colossaux, car ils conditionnent la performance de l'entreprise et remet en question sa productivité.

b) Situation initiale

Chez groupe WOOD, il n'y avait pas de logiciel de supervision existant, c'est pour cela que nous avons eu l'idée d'y implémenté un logiciel de supervision afin d'améliorer la gestion et le suivi du nouveau parc informatique, afin d'être prédictif sur les alertes pouvant remettre en cause la productivité chez le client.

c) Problématique

Ce que nous souhaitons mettre en place, c'est une application qui serait capable de donner l'état en temps réel des serveurs, des machines virtuelles, et de certains services, que ce soit au siège ou sur les sites extérieurs, et d'avoir une supervision centralisée entre les divers sites avec divers moyens de supervisons comme des graphiques. Cet applicatif devra également prévenir les administrateurs lors d'un disfonctionnement et être gratuite.

d) Elaboration du cahier des charges

Nous allons tout d'abord établir un cahier des charges et ainsi pouvoir répondre pleinement à celle-ci.

• La première fonction que doit impérativement remplir la solution est que cette dernière doit être capable de superviser les équipements réseaux du groupe WOOD aussi bien au siège que sur nos sites externes.

• La seconde fonction principale est que la solution proposée doit pouvoir surveiller les serveurs du groupe WOOD, à savoir leurs composants et leur fonctionnement.

• La troisième fonction principale de cette solution est la possibilité de superviser des services présents sur les serveurs

• et la quatrième fonction principale que devra remplir cette solution est la possibilité de prévenir les administrateurs par le biais de notifications email lors de chaque disfonctionnement.

e) Choix de l'outil de supervision

Pour le choix de l'outil de supervision, trois gros logiciels ressortaient du lot, avec Nagios, Centreon et Zabbix.

Nagios :

Donc Nagios (Anciennement appelé Netsaint) est un outil de supervision qui permet de surveiller les systèmes et réseaux au sein d'une entreprise. La première version de ce logiciel a vu le jour en 1996, il est programmé en C et il est publié sous licence GNU (ou GPL), c'est-à-dire qu'il est libre d'utilisation et de modification par tous les utilisateurs.

Avantages :

✓ Il est reconnu auprès des entreprises et possède un grand nombre de documentation sur le Web.

✓ La remontée des alertes est complètement paramétrable avec l'utilisation de plugins (alerte par courrier électronique).

✓ C'est une solution complète permettant la gestion de panne et d'alarme, gestion utilisateurs et la cartographie du réseau

Inconvénients :

✗ L'Interface non ergonomique et peu intuitive.

✗ Pour avoir toutes les fonctionnalités il est nécessaire d'installer des plugins.

✗ Il est difficile à installer et à configurer.

✗ Il n'y a pas de représentations graphiques, il faut pour cela passer par le mode ligne de commande pour effectuer les mises à jour et la configuration.

✗ Il dispose d'une interface compliquée et ne permet pas d'ajouter d'hôte via Web

✗ Payant à partir 100 équipements

Le développeur principal de Nagios montre sa volonté de ne plus diffuser Nagios sous licence libre, par conséquent dans un futur proche l'outil ne sera plus mis à jour et ne bénéficiera plus de nouvelles fonctionnalités.

Centreon :

Centreon est également une solution de monitoring système et réseaux. Au départ il n'était qu'une couche applicative web que l'on rajoutait à Nagios, elle permettait d'administrer plus facilement ce dernier en passant par une interface graphique.

Mais à partir de 2012 Centreon devient un logiciel de monitoring à part entière avec son propre noyau de fonctionnement. Il est présenté comme étant plus économique en ressource et plus sécurisés que Nagios. Il est développé en C++ et est également sous licence GNU (ou GPL). La dernière version de ce logiciel est la version 2.8.5 sorties le 29 mars 2017.

Avantages :

✓ La robustesse

✓ Interface complète

Inconvénients :

✗ Problèmes de compatibilités avec certains logiciels.

✗ Logiciel lourd

✗ Payant

Zabbix :

Zabbix est également un logiciel de supervision libre, il permet de surveiller l'état des matériels réseaux, des serveurs et des divers services réseaux. Sa principale force est la création de graphiques dynamiques. Sa première version voit le jour en 1998, il est écrit en C, PHP et Java et il est également sous licence GPL (ou GNU). La dernière version stable disponible à ce jour est la version 4.2.2 sorties le 27 Mai 2019. La communauté de Zabbix est plutôt active et l'applicatif est mis à jour régulièrement.

ZABBIX

Avantages :

✓ Assez simple à installer

✓ Open source

✓ Permet une gestion des alertes

✓ Communauté croissante donc mis à jour, maintenu et communauté à l'écoute

✓ Interface vaste avec plusieurs fonctions

✓ Possède une compatibilité avec divers gestionnaires de stockage de donnée MySQL, PostgreSQL, Oracle, SQLite

✓ Gratuit

Inconvénients :

✗ Nécessite un VPN pour la sécurité de nos données car l'agent Zabbix communique par défaut en clair les informations.

Tableau récapitulatif entre les 3 choix de supervision :

	Centreon	Zabbix	Nagios
Environnement	Unix	Unix	Unix
Base de données	C++	PHP, C, C++	PHP
Protocole	SNMP, SMTP, pop3, NNTP ICMP, HLDP	http, FTP, SMTP, SSH, ICMP, IMAP	SNMP, SMTP, pop3, NNTP ICMP, HLDP
Gestion authentification et rôles	Oui	Oui	Oui
Création de graphique	Oui	Oui	Non
Installation et configuration simple	Oui	Oui	Non
Agent sur les machines cibles	NRPE NSclient	Agent Windows/Unix	NRPE NSclient
Intégration simple d'un nouvel hôte	Oui	Oui	Non
Supervision centralisée entre plusieurs sous réseaux ou sites	Oui	Oui	Non
Payant ou Gratuit	Payant	Gratuit	Payant

Au vu du pic de popularité de Zabbix, ses mises à jour régulières et surtout sa volonté de rester gratuit, nous avons alors décidé de choisir ce dernier pour le projet puisqu'il remplit toutes les prérogatives et permet une supervision simple tout en étant gratuit.

f) Mise en place des solutions de recours

Lors de la mise en place du logiciel de supervision, il faudra aussi pensait à un recours en cas de problème, Il est donc nécessaire de mettre en place un système de sauvegarde, et de redondances pour la restauration des données à partir d'un serveur de secours.

En effet par rapport au plan de continuité d'activité concernant la supervision, la VM Zabbix sera situé sur le serveur principale à Lille et aura une redondance sur le serveur secondaire en cas de problème ou de panne du serveur ou de la VM en question.

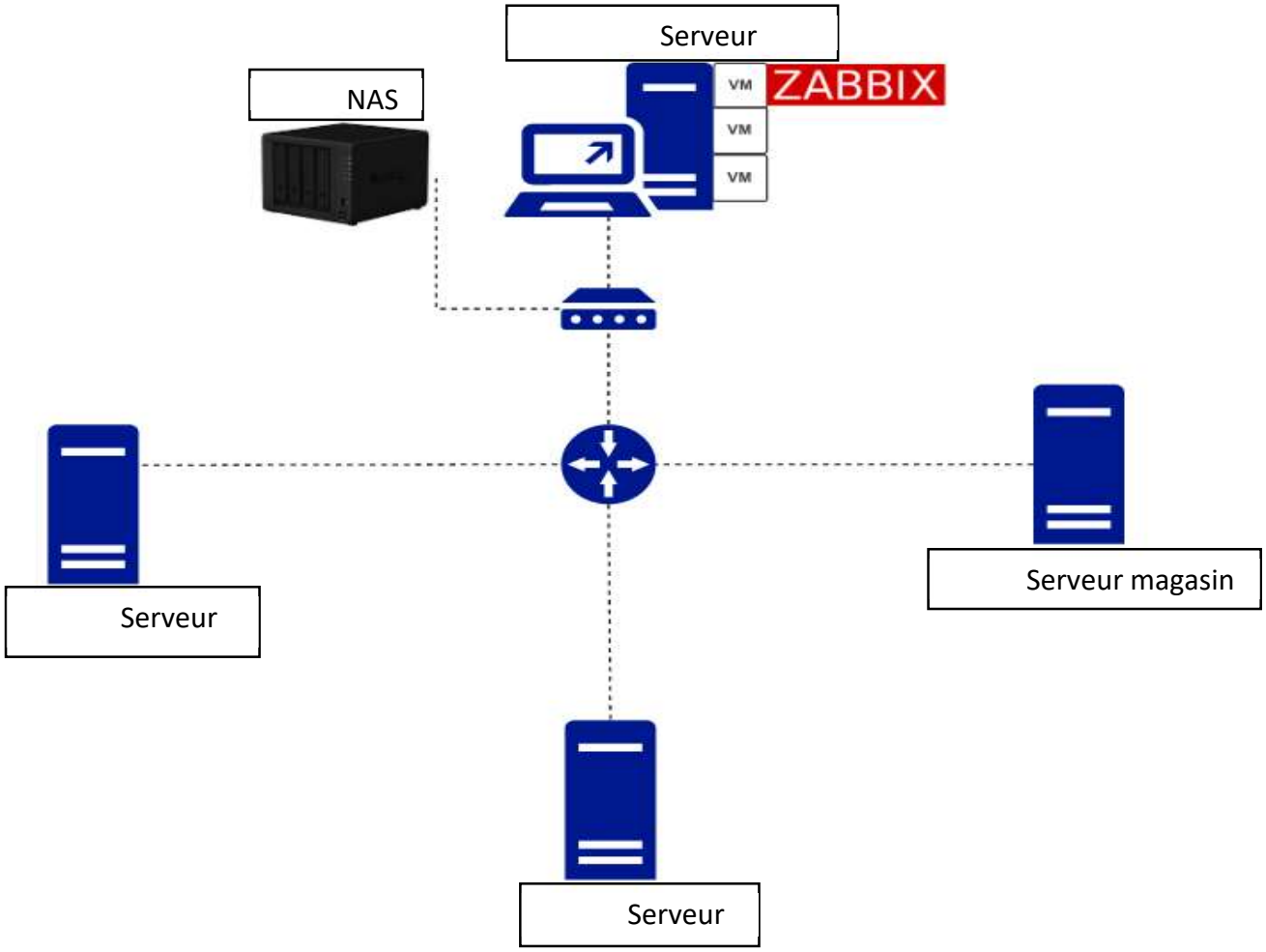
Nous allons aussi mettre en place un plan de reprise d'activité en faisant régulièrement des sauvegardes concernant la VM et des sauvegardes concernant la base de données qui va être stocké sur le NAS du site principale, en effet si la VM de supervision ne fonctionnement plus ou quelle devient défectueuse, nous aurons un plan de reprise d'activité en restaurant

l'image de la VM sauvegardée afin de toujours être proactif au niveau de la nouvelle infrastructure réseau, et de limiter une perte de production du groupe WOOD.

De même pour la base de données, nous aurons toujours la sauvegarde sur le NAS qui permettra de ne pas réintégrer tous les équipements et donc de ne pas perdre de temps.

g) Équipement à superviser :

Voici l'infrastructure des machines à superviser :



4. Sécurisation WI-FI

Il y a plusieurs raisons de sécuriser son WIFI aujourd'hui. Cela va vous permettre de limiter les risques d'intrusions malveillantes ou le détournement de la connexion internet. Voici quelques règles que nous conseillons d'appliquer pour votre WIFI.

Règle de sécurité WI-FI :

- Changer le nom et mot de passe par défaut
- Mettre un mot de passe fort contenant, caractère spéciaux, chiffre, lettre minuscule/majuscule et 8 caractères minimum
- Utiliser une clé de chiffrement WPA2 (AES)
- Cacher votre SSID
- Faire de la supervision pour voir les personnes connectées sur les bornes
- Maintenir à jour les bornes WIFI
- Mettre une restriction horaire sur les bornes WIFI

5. Sécurisation Administrateur

a) Quels sont les risques de cybersécurité liés aux comptes administrateurs ?

Les comptes administrateurs et autres comptes à privilèges élevés sont soumis à deux principaux dangers : les menaces externes et les menaces internes. Il est primordial de saisir la nature et l'ampleur de ces risques.

Les identifiants d'un administrateur sont très attrayants pour les cybercriminels, qui souhaitent les exploiter pour voler les données sensibles de l'entreprise ou compromettre sa cybersécurité. Plusieurs types d'attaques peuvent être mis en œuvre.

Les malwares de type Keylogging sont capables de capturer les pressions de touches sur le clavier de l'administrateur, afin d'acquérir son identifiant et son mot de passe.

Outre ces menaces d'origine extérieure, il faut tenir compte du risque qu'un administrateur abuse de ses privilèges. Un employé mal intentionné est par exemple en mesure de supprimer ou de transférer des données, d'altérer le fonctionnement d'un système, de créer des comptes "backdoor" avec des droits élevés, d'utiliser le compte d'un autre utilisateur, d'installer volontairement un malware sur le système, ou d'exploiter des vulnérabilités.

b) Comment protéger les comptes administrateurs ?

Il existe heureusement différentes solutions pour sécuriser et contrôler les accès administrateurs. Ces méthodes permettent d'assurer la sécurité contre les menaces internes et externes.

Tout d'abord, il est capital de ne pas utiliser les accès administrateur pour un usage quotidien. Les comptes à privilèges élevés ne doivent être utilisés qu'en cas de nécessité, pour éviter les tentatives d'hameçonnage ou de malwares.

Des solutions peuvent vous aider à réduire les risques liés aux comptes administrateurs grâce à la création automatique de comptes administrateur provisoires. Ces solutions permettent d'avoir juste assez de privilèges pour effectuer les tâches administratrices requises. Les comptes sont par la suite supprimés de sorte à éviter l'abus de comptes permanents ou les risques de piratage.

Les avantages de ce type de solution sont nombreux comme l'enregistrement de sessions, l'activation de comptes provisoires, l'extraction de journaux d'audit de l'activité, etc.

En parallèle, voici quelques tips pratiques à mettre en œuvre comme :

- Veiller à mettre en place un plan de sauvegarde et de restauration des données. Ainsi, même en cas de modification ou de suppression non autorisée, vous pourrez annuler les changements et récupérer les informations compromises.

- Implémenter des fonctionnalités de sécurité comme l'authentification multi-facteurs. Une approche bien connue aujourd'hui pour ajouter une couche de sécurité supplémentaire. Un acteur malveillant qui tentera d'accéder au réseau de l'entreprise à l'aide d'identifiants volés à un administrateur sera assez vite freiné.

- Protéger le hardware et les systèmes physiques avec autant de soin que les réseaux et systèmes virtuels. Les serveurs doivent être entreposés dans un endroit où seul le personnel autorisé peut accéder. Pour cause, il existe un risque que des criminels volent directement les machines pour en extraire les données.

Enfin, menez fréquemment des audits pour surveiller les systèmes et tracer toute modification. Une complémentarité non négligeable avec la sécurisation et de contrôle des accès administrateurs qui permet de monitorer les modifications, les configurations et les accès aux environnements informatiques.

L'audit fournit aussi des renseignements de sécurité pour identifier les failles, détecter des anomalies dans le comportement d'utilisateur et étudier des modèles de menace à temps pour éviter des dommages réels.

Des pratiques et solutions qui permettront une meilleure analyse de ce qui se passe dans votre entreprise, facilitera la détection en cas de problème, excellera votre sécurité informatique et assurera votre conformité réglementaire

6. Campagne de sensibilisation utilisateurs

Les utilisateurs peuvent être parfois la porte d'entrée des personnes malveillantes pour s'introduire dans le réseau.

C'et pour lutter contre cela que nous avons pris la décision de mettre en place des formations de sensibilisation aux utilisateurs concernant une multitude de sujet touchant l'informatique.

Les formations sensibiliseront les collaborateurs sur les cyber-attaques et que faire pour les éviter, en passant par une sensibilisation sur les ransomwares et les dégâts qu'ils peuvent causés, ou encore sur la simple utilisation des outils informatiques qui sont à la disposition de chacun.

7. Gestion des incidents

GLPI est un outil qui sera utilisé principalement pour l'usage des tickets, qui est un moyen très efficace de faire du ticketing. Il est actuellement un des meilleurs outils pour les entreprises souhaitant gérer au mieux leurs services support.

Cet outil possède une interface très claire et intuitive et est très documenté sur internet. L'ajout de plusieurs centaines de plugins est possible permettant de rajouter un notre de possibilité énorme, comme par exemple, le plugins Fusion inventory qui est l'un des plugins les plus utilisé permettant de dresser un inventaire rapide de l'ensemble d'un parc informatique. Ce plugin permet aussi notamment envoyer de paquet à plusieurs voir l'ensemble du parc inventorié.

Il permet aussi de créer une traçabilité ainsi que d'en ressortir des statistiques sur notamment quelles sont les points qui pose le plus de problème.

8. Sauvegarde

a) Qu'est-ce qu'une solution de sauvegarde

La sauvegarde est l'opération de copie préventive de données sur un support indépendant. Le but premier d'une sauvegarde est de prévenir une perte de données. Il est essentiel de toujours disposer d'une bonne solution de sauvegarde. Une corruption des fichiers et une panne du matériel peuvent survenir même si les fichiers sont récents et que l'ordinateur soit neuf ou fiable. Autrefois coûteuses et complexes, les sauvegardes sont à présent bon marché, simples à utiliser et, selon la solution adoptée, complètement automatisées.

b) Qu'est-ce que Veeam backup

C'est le logiciel principal et indispensable de la suite Veeam. Comme son nom l'indique, Backup & réplication va sauvegarder et répliquer les machines virtuelles sur un espace de stockage ou sur une autre infrastructure virtualisée (distante si possible).

Ce logiciel est à installer sur le serveur qui va gérer les sauvegardes, généralement une VM dédiée à Veeam. Le serveur Veeam sera physique ou virtuel mais nécessite un système d'exploitation Windows. Avec Veeam Backup on a à notre disposition une solution unique de sauvegarde pour protéger les serveurs virtuels des problèmes matériels et logiciels. Ces deux techniques de sauvegarde peuvent être utilisées avec ou sans VMware consolidâtes Backup (VCB), réduisant ainsi la charge sur la console de service et autorisant des récupérations des données plus rapides. Avec Veeam Backup, vous choisissez la meilleure option pour chaque machine virtuelle.

c) Importance d'une sauvegarde efficace

En informatique la sauvegarde a pour fonction de mettre en sécurité des informations et de pallier toute éventualité de panne matérielle, d'infection par un logiciel malveillant, et de suppression volontaire ou fortuite. L'utilité de la sauvegarde est de pouvoir restaurer le plus rapidement possible un système après une défaillance ou un incident. Pour enregistrer vos données, gagner du temps et économiser de l'argent, il est essentiel de mettre au point une stratégie de sauvegarde en mesure de protéger vos données, et de choisir le matériel et les logiciels adaptés à votre stratégie, elle est la seule solution pour protéger les données de votre entreprise ; la sauvegarde conditionne la reprise après sinistre ; les sauvegardes sont une condition imposée par de nombreuses réglementation

9. Archivages

En informatique, on appelle archivage le processus qui consiste à créer un fichier à partir de plusieurs autres pour en faciliter la portabilité et le stockage. Ce fichier est appelé archive et il est particulièrement utile car les fichiers qu'il contient et leurs métadonnées sont fusionnées, ce qui permet un stockage sur des systèmes de fichiers n'étant pas forcément compatible avec les formats de fichiers de base. Les utilitaires d'installation pour applications et logiciels sont d'ailleurs des archives qui vont décompresser les fichiers regroupant tout le code et le contenu dans un dossier choisi, on parle alors de paquet.

L'archivage est souvent couplé à d'autres fonctionnalités :

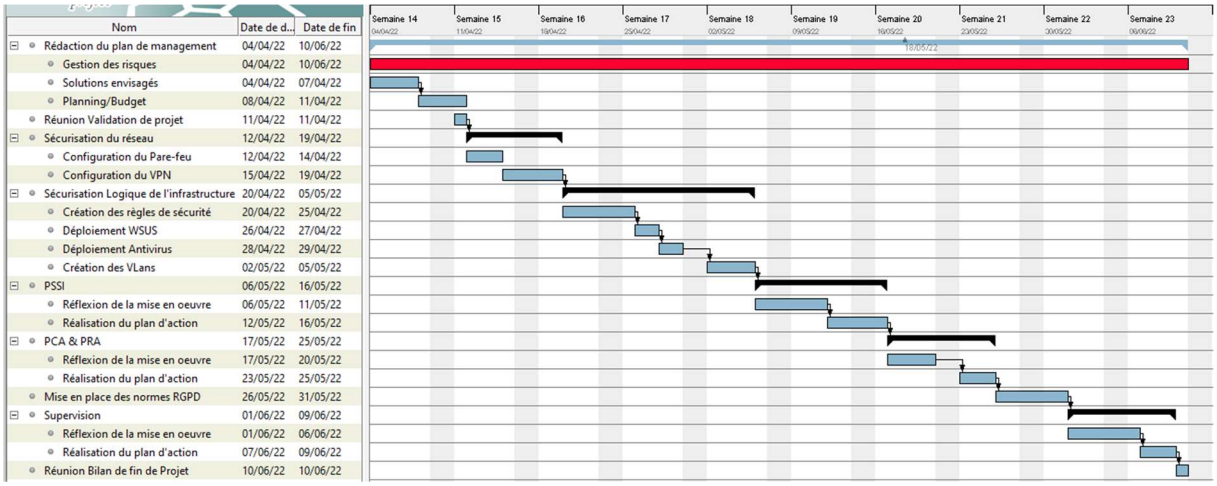
- La compression qui réduit le poids de l'archive en supprimant la redondance des données dans les fichiers qui la constituent ;
- Le contrôle de somme pour vérifier l'intégrité des fichiers ;
- La division d'un fichier volumineux en plusieurs archives ;
- Une forme de chiffrement asymétrique pour protéger les fichiers.

L'archivage dans l'entreprise WOOD servira à sauvegarder les documents et sera un moyen de faciliter son exploitation dans la conduite de la courante de l'activité. Ainsi, un accès facile et rapide aux documents et dossiers permettra de les traiter de façon optimale.

VIII.Gestion de projet

1. Planning prévisionnel

Ci-dessous, vous pouvez observer le planning prévisionnel de la partie 3 de notre projet, partie axée sur la sécurité. Dans ce planning vous pouvez y retrouver toutes les tâches qui seront effectuer au cours des prochains mois en suivant les plans d'actions définis. Ainsi, nous apercevons que la partie 3 de notre projet comme par la rédaction du plan de management, pour ensuite continuer sur la partie de sécurisation du réseau. Nous continuons avec la partie de sécurisation logique de l'infrastructure, ensuite, nous enchainons avec la partie PSSI, puis PCA & PRA. Nous finissons enfin avec la supervision.



Nom	Date de d...	Date de fin
Rédaction du plan de management	04/04/22	10/06/22
Gestion des risques	04/04/22	10/06/22
Solutions envisagés	04/04/22	07/04/22
Planning/Budget	08/04/22	11/04/22
Réunion Validation de projet	11/04/22	11/04/22
Sécurisation du réseau	12/04/22	19/04/22
Configuration du Pare-feu	12/04/22	14/04/22
Configuration du VPN	15/04/22	19/04/22
Sécurisation Logique de l'infrastructure	20/04/22	05/05/22
Création des règles de sécurité	20/04/22	25/04/22
Déploiement WSUS	26/04/22	27/04/22
Déploiement Antivirus	28/04/22	29/04/22
Création des VLans	02/05/22	05/05/22
PSSI	06/05/22	16/05/22
Réflexion de la mise en oeuvre	06/05/22	11/05/22
Réalisation du plan d'action	12/05/22	16/05/22
PCA & PRA	17/05/22	25/05/22
Réflexion de la mise en oeuvre	17/05/22	20/05/22
Réalisation du plan d'action	23/05/22	25/05/22
Mise en place des normes RGPD	26/05/22	31/05/22
Supervision	01/06/22	09/06/22
Réflexion de la mise en oeuvre	01/06/22	06/06/22
Réalisation du plan d'action	07/06/22	09/06/22
Réunion Bilan de fin de Projet	10/06/22	10/06/22

2. Analyse des risques

Afin de prévoir le futur du projet, nous avons identifié les risques qui pourraient nuire à au bon déroulement du projet. Un tableau des risques a donc été mis en place ainsi qu'une matrice des risques.

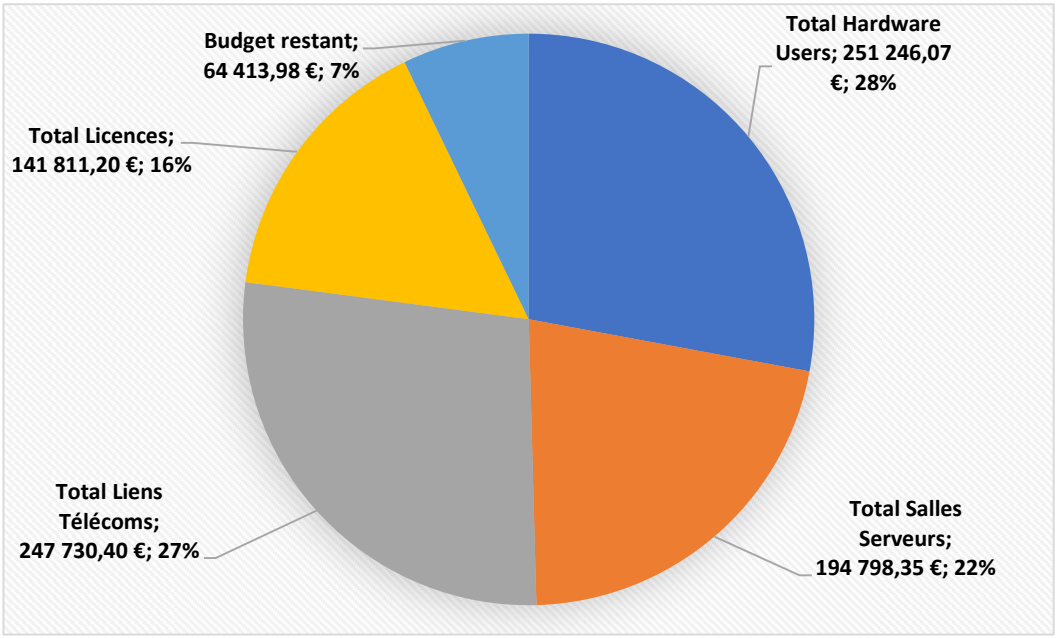
N°	Titre du Risque	Impact /4	Probabilité /4	Impacts	Score /16	Stratégie mise en place
1	Retard de livraison	3/4	3/4	-Retard sur le projet -Pas finir à temps	12/16	-Précommander en avance les équipements
2	Risque humain (maladie/décès)	2/4	2/4	-Perte de temps et de productivité au sein de l'équipe	6/16	-Réunion et suivi du projet
3	Dépassement du budget	4/4	3/4	-Manque de moyens pour finaliser le projet	15/16	-Contrôle et suivi du budget tout au long du projet
4	Vols	3/4	4/4	-Perte d'équipement et de temps	9/16	-Contrôle journalier avec accès restreint au stock
5	Mauvaise gestion projet	4/4	2/4	-Projet qui ne se finalise pas dans les délais voir pas du tout	16/16	-suivi des points d'avancements du projet hebdomadaire
6	Peur du changement	3/4	3/4	-Rester dans sa zone de confort et empêcher l'avancement du projet	6/16	-Suivi et transfert de compétence entre les employer afin d'accompagner les plus retissant
7	Compétences insuffisantes	3/4	2/4	-Désorganisation et conflits	8/16	-Formation mensuel
8	Destruction des équipements	4/4	2/4	-Pertes financières -Perte de temps	9/16	-Restriction des actions lors d'un départ d'un collaborateur ou d'un prestataire
9	Incendie sur les sites	3/4	1/4	- Perte du matériels	11/16	-Mise en place de détecteur de fumer et d'extincteur
10	Faillites fournisseur	3/4	1/4	-Matériels promis non disponible et donc mécontent	9/16	-Prévoir d'autre fournisseur en « backup » qui pourrait nous fournir le matériel demandé
11	Manque d'adhésion	3/4	2/4	-Manque de solidarité et de cohésion qui impactera directement l'avancement du projet	9/16	-Encourager les membres de l'équipe à s'échanger les idées
12	Mauvaise configuration des équipements réseaux	3/4	2/4	-Problèmes de liaisons des équipement réseaux	10/16	-Vérification de chaque configuration

3. Budget

L'un des facteurs les plus importants dans les projets informatiques est le budget. En effet, dans de nombreux projets, le risque est qu'il soit dépassé, c'est pourquoi il est nécessaire d'organiser un suivi des coûts.

Concernant ce lot, il n'y aura que très peu de coûts. En effet, malgré la multitude de logiciels prévus (Veeam, Eset, Zabbix, RDM) il n'y a que ESET qui est payant. Concernant le matériel physique, il n'y a que des onduleurs qui seront commandés.

Nous arrivons donc à :



IX.Conclusion / Bilan

Nous arrivons à termes de ce troisième et dernier lot ou nous vous avons présenté les solutions que nous estimons adaptées à vos besoins concernant la sécurité de votre nouvelle infrastructure réseaux.

De la supervision avec le Zabbix mise en place qui permettra de monitorer vos serveurs et d'être proactif sur la nouvelle infrastructure, jusqu'au chartes informatiques qui permettront d'avoir une sécurisation sur le plan matériel et humain du groupe WOOD.

Le projet de refonte du système d'information de Wood répond donc aux critères de disponibilité et de cout. Il ne dépasse pas le budget et offre une disponibilité avancée en cas de panne d'équipement. En effet, tous les équipements ont été remplacés et peuvent être garantis en cas de panne dans les prochaines années.

Pour la suite, notre entreprise IPTAB vous accompagnera dans la transition vers le nouveau parc informatique mis en place afin que vos équipes ne soit pas perdu et est une bonne intégration et utilisation de votre nouvelle infrastructure réseau.