Index

[*Périmètre (Contexte):* 3](#_Toc5765137)

[*Inventaire :* 3](#_Toc5765138)

[Applications métiers : 3](#_Toc5765139)

[Salle serveur et réseau Magasin (chaque magasin) : 3](#_Toc5765140)

[Plateforme Administrative Nancy : 4](#_Toc5765141)

[Plateforme Commercial Metz : 4](#_Toc5765142)

[*Infrastructure informatique* 4](#_Toc5765143)

[Serveurs : 4](#_Toc5765144)

[Réseau : 5](#_Toc5765145)

[Firewall : 5](#_Toc5765146)

[DMZ (Zone démilitarisée) : 5](#_Toc5765147)

[Reverse proxy : 5](#_Toc5765148)

[Sonde réseau : 5](#_Toc5765149)

[Proxys : 5](#_Toc5765150)

[Méthode pour sauvegarde : 6](#_Toc5765151)

[Cartographie des risques : 6](#_Toc5765152)

[Panne de courant : 6](#_Toc5765153)

[Panne d’un serveur : 7](#_Toc5765154)

[Panne du réseau : 7](#_Toc5765155)

[Base de données non disponible : 7](#_Toc5765156)

[Incendie : 8](#_Toc5765157)

[Mesures préventives : 8](#_Toc5765158)

[Panne de courant : 8](#_Toc5765159)

[Panne d’un serveur : 8](#_Toc5765160)

[Panne du réseau : 9](#_Toc5765161)

[Base de données non disponible : 9](#_Toc5765162)

[Incendie : 9](#_Toc5765163)

[Préconisations : 9](#_Toc5765164)

[Surveiller : 10](#_Toc5765165)

[Serveurs : 10](#_Toc5765166)

[Base de données : 10](#_Toc5765167)

[Sensibilisation des utilisateurs : 10](#_Toc5765168)

[Conclusion : 10](#_Toc5765169)

# *Périmètre (Contexte):*

L’entreprise Motuc est une chaine de magasins spécialisés dans la distribution de produits culturels, tels que des CD’s, Blu-rays, livres, matériels home-cinéma, consoles, jeux-vidéos, etc.

L’entreprise n’ayant pas définit de PRA, ce document a pour but de fournir une ligne directrice pour le projet PRA. Ce document est donc la création d’un nouveau PRA et remplacera tout document officiel ou non servant de PRA.

L’entreprise Motuc est dans une situation de crise suite à une cyber-attaque et toute l’infrastructure a été impactée. Afin d’améliorer la sécurité pour se prémunir d’une nouvelle attaque, la mise en place d’un PRA et d’un PCA est nécessaire.

Grâce à l’analyse PRA/PCA l’entreprise peut identifier les menaces et les risques. Ainsi, le PRA/PCA permettra :

* D’établir des plans, procédures et mesures qui améliorent la réponse de l’entreprise quand il y aura un problème.
* D’améliorer la sécurité dans chaque bâtiment (Nancy, Metz et Magasins).
* De réduire les pertes économiques, de temps et des données.
* De Minimiser les interruptions (serveur, données, etc.).

# *Inventaire :*

### Applications métiers :

* Des schémas d’architectures du SI (cryptés)
* Des schémas/workflow (cryptés)
* Des processus métiers (cryptés)
* Archives :

1. Plans géographiques et internes des structures (Sauf magasins)
2. Plans des salles serveurs et réseaux (non à jour)
3. Listing des mesures de sécurité existantes
4. Listing des incidents survenus depuis un mois.

### Salle serveur et réseau Magasin (chaque magasin) :

Serveur :

* Serveur AD, DHCP, DNS
* Serveur de messagerie, proxy et d’inventaire
* Serveur de fichiers, d’application et d’impression
* Serveur de base de données pour le secteur caisse
* Serveur de base de données pour l’atelier de réparation

Matérielle réseau

* Tiroirs optiques
* Bandeaux réseaux
* Routeur
* Cour de réseau
* Switch
* Bandeaux électriques
* Prise électrique

### Plateforme Administrative Nancy :

Serveurs :

* Serveurs AD, DNS, DHCP
* Serveur Antivirus et anti spam
* Serveur Web
* Serveur de messagerie
* Serveur de sauvegarde
* Serveur de base de données
* Serveur d'applications
* Serveur de sauvegarde avec lecteur de bandes

Matérielle réseau :

* Bandeaux électriques
* Routeur
* Firewall
* Bandeaux réseaux
* Tiroir optiques
* Cour de réseau
* Switches SAN
* Lecteurs de bandes
* Système de détection d'incendie
* Prise électrique
* Switch KVM

### Plateforme Commercial Metz :

Serveur :

* Serveur AD, DHCP, DNS
* Serveur de fichiers, d'application et d'impression
* Serveur de base de données
* Serveur de messagerie, proxy et d'inventaire
* Serveurs téléphonie

Matérielle réseau :

* Tiroirs optiques
* Bandeaux réseaux
* Routeur
* Cœur de réseau
* Switch
* Bandeaux électriques
* Prise électrique

# *Infrastructure informatique*

## Serveurs :

Les serveurs bénéficient de mesures de durcissement de leur système d’exploitation concernant notamment :

* La sécurisation de l’accès au BIOS
* Le contrôle d’accès logique au système
* La désactivation des ports et services non utilisés (Telnet, ftp…)
* Les mises à jour des correctifs de sécurité
* La gestion des comptes et privilèges d’administration
* La mise en œuvre des traces d’audit.

A l’exception des informaticiens, les utilisateurs ne sont pas administrateur de leur poste. Comptes système dédiés aux prestataires : Les comptes destinés à l’installation ou à la maintenance d’un produit sont désactivés dès l’opération d’installation ou de maintenance terminée. Les mots de passe qui ont été attribués sont changés dès la fin des opérations.

*Dans le cadre d’une externalisation de certains éléments informatiques (serveurs d’application, de données…), le client exige de conserver un serveur servant de RCD (Serveur de réplication) sur chaque site pour minimiser d’éventuelles coupures WAN même si le fournisseur d’accès à Internet est soumis à une garantie de rétablissement de deux heures. (Des fonctions complémentaires pourront être implémentées sur ce serveur.)*

## Réseau :

### Firewall :

Au nombre de deux :

* Ils assurent le trafic entre les différentes zones de confiance et filtrent les flux qui y transitent.
* Le but de leur mise en place est de mettre à disposition des personnes, une connectivité qui soit contrôlée et maîtrisée entre les divers niveaux de confiance, notamment grâce à la mise en œuvre d’un modèle de connexion basé sur le principe du moindre privilège.

### DMZ (Zone démilitarisée) :

Au nombre de deux :

* Les DMZ mises en place permettent de disposer de sous réseaux séparés du réseau local et isolés d’internet par les pare-feu.
* La première DMZ contient le Reverse proxy permettant de contrôler l’accès des utilisateurs voulant au serveur web qui est situé dans la DMZ 2.

### Reverse proxy :

* La mise en place de ce reverse proxy permet donc aux utilisateurs externes d’accéder au serveur web.
* Le reverse proxy contient des fonctions de sécurité qui permettent de protéger le serveur web contre des attaques provenant de l’extérieur.

### Sonde réseau :

* Le but de mise en œuvre de la sonde réseau est d’avoir une visibilité complète sur le trafic et de pouvoir être alerté en cas de problèmes majeurs.

### Proxys :

Au nombre de deux

* Ils permettent de contrôler l’accès et l’utilisation de l’internet.
* Les accès et les flux sont indirects et transitent donc par les serveurs mandataires.

# Cartographie des risques :

Pour mieux comprendre les risques, vous trouverez ci-dessous quelques descriptions es risques les plus importants, suivi par un graphique permettant de mieux visualiser l’information de chaque risque.

## Panne de courant :

Suspension de la distribution du courant électrique dans une région attribuée. Ceci peut provenir d’un défaut dans une centrale électrique, de l’équipement de distributions endommagées, un court-circuit ou une surcharge du système. Une panne de courant peut entraîner l'arrêt des serveurs, entraînant des pertes économiques importantes en fonction du temps nécessaire à la résolution du problème. De plus, si la panne survient lors de la copie de sauvegarde de certaines données importantes, cela pourrait impliquer la perte de celle-ci.

|  |  |
| --- | --- |
| Probabilité de survenance du risque  (Fréquence) | Gravité de l’impact du risque  (Gravité) |
| 1 : Très fiable (1 x an) | 1 : Négligeable |
| 2 : Fiable (1 x moins) | 2 : Mineur |
| 3 : Moyenne (1 x semaine) | 3 : Majeur |
| 4 : Importante (1 x jour) | 4 : Critique |
| 5 : Très important (1 x heure) | 5 : Catastrophique |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 3  Gravité |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 1 |  |  |  |  |  |
|  | 1  Fréquence | 2 | 3 | 4 | 5 |

|  |  |
| --- | --- |
| Probabilité de survenance du risque  (Fréquence) | Gravité de l’impact du risque  (Gravité) |
| 1 : Très fiable (1 x an) | 1 : Négligeable |
| 2 : Fiable (1 x moins) | 2 : Mineur |
| 3 : Moyenne (1 x semaine) | 3 : Majeur |
| 4 : Importante (1 x jour) | 4 : Critique |
| 5 : Très important (1 x heure) | 5 : Catastrophique |

## Panne d’un serveur :

Parmi les causes d’une panne d'un serveur, les experts distinguent les menaces internes et externes. Les premiers sont tous les scénarios dans lesquels l'infrastructure informatique, l'alimentation ou une erreur humaine sont les déclencheurs, pour les deuxièmes inclut des attaques planifiées de l'extérieur et des événements imprévisibles, tels que des accidents ou des catastrophes naturelles. Lorsqu'un serveur cesse de fonctionner correctement, il peut en résulter des pertes économiques importantes, ainsi que des pertes de nouveaux consommateurs, dans le cas où le serveur Web est en panne.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 3  Gravité |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 1 |  |  |  |  |  |
|  | 1  Fréquence | 2 | 3 | 4 | 5 |

## Panne du réseau :

Problèmes de réseau sont une classe de problèmes d'optimisation sur les réseaux. Conjecturé insoluble, ces problèmes sont au centre de la construction pour sécuriser les réseaux et à la base des crypto-systèmes. Un problème sur le réseau implique une perte de communication entre les serveurs, entraînant une perte de données. De plus, il est impossible de se connecter à Internet, ce qui entraîne des pertes économiques considérables.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 3  Gravité |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 1 |  |  |  |  |  |
|  | 1  Fréquence | 2 | 3 | 4 | 5 |

|  |  |
| --- | --- |
| Probabilité de survenance du risque  (Fréquence) | Gravité de l’impact du risque  (Gravité) |
| 1 : Très fiable (1 x an) | 1 : Négligeable |
| 2 : Fiable (1 x moins) | 2 : Mineur |
| 3 : Moyenne (1 x semaine) | 3 : Majeur |
| 4 : Importante (1 x jour) | 4 : Critique |
| 5 : Très important (1 x heure) | 5 : Catastrophique |

## Base de données non disponible :

Les bases de données informatiques sont utilisées dans un grand nombre d’entreprises pour stocker, organiser et analyser les données. Une base de données est une collection d’informations organisées afin d’être facilement consultables, gérables et mises à jour donc, s’il est non disponible il n’y aura pas d’archivage ni de rapport ou bilans.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 3  Gravité |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 1 |  |  |  |  |  |
|  | 1  Fréquence | 2 | 3 | 4 | 5 |

|  |  |
| --- | --- |
| Probabilité de survenance du risque  (Fréquence) | Gravité de l’impact du risque  (Gravité) |
| 1 : Très fiable (1 x an) | 1 : Négligeable |
| 2 : Fiable (1 x moins) | 2 : Mineur |
| 3 : Moyenne (1 x semaine) | 3 : Majeur |
| 4 : Importante (1 x jour) | 4 : Critique |
| 5 : Très important (1 x heure) | 5 : Catastrophique |

## Incendie :

|  |  |
| --- | --- |
| Probabilité de survenance du risque  (Fréquence) | Gravité de l’impact du risque  (Gravité) |
| 1 : Très fiable (1 x an) | 1 : Négligeable |
| 2 : Fiable (1 x moins) | 2 : Mineur |
| 3 : Moyenne (1 x semaine) | 3 : Majeur |
| 4 : Importante (1 x jour) | 4 : Critique |
| 5 : Très important (1 x heure) | 5 : Catastrophique |

Un incendie est un feu violent et destructeur pour les activités humaines ou la nature. L'incendie est une réaction de combustion non maîtrisée dans le temps et l'espace. Un incendie peut avoir plusieurs causes: une surchauffe d'un appareil électrique, une défaillance de la prise de courant, entre autres. Il ne peut pas être prévue, mais quand il commence, dans on peut le détecter.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 3  Gravité |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 1 |  |  |  |  |  |
|  | 1  Fréquence | 2 | 3 | 4 | 5 |

# 

Table avec la Cartographie des risques (complet)

# Mesures préventives :

Afin d’obtenir un soutien au cas où l’une des situations présentées ci-dessus se produirait, voici quelques mesures qui pourraient être prises en compte pour éviter ou éliminer tout problème.

## Panne de courant :

* Installer des Onduleurs.
* Verrouillage des prises du bai réseau.
* Isolation des différents réseaux électrique par le SI, quand un réseau à une panne il n’affecte pas le reste de l’infrastructure.
* Vérification mensuel des groupes électrogène.

## Panne d’un serveur :

* Mise en place d’outils de monitoring qui permettent d’alerter sur une panne possible.
* Duplication des services du serveur sur un serveur de secours.
* Installer des Onduleurs (ça servira pour retenir la charge par un très court temps ou on pourra faire des copies de sécurité).

## Panne du réseau :

* Il faut éviter qu’une panne de réseau affecte tout le système, pour cela un réseau de secours peut-être envisagé. De plus une duplication des DMZ permettra un accès au site internet permanent.
* Vérifier le Hardware (câbles).

## Base de données non disponible :

* Un répliquât peut être utilisé en attendant le retour de la BDD principal, de plus on pourra archiver les données à deux endroits et pas un seul.
* Faire une copie de sécurité

## Incendie :

* Les bâtiments doivent être conçus pour respecter les normes de sécurité, de plus les produits dangereux (réserves groupes électrogènes) doivent être loin des zones de travail des employées et les pièces ayant un fort potentiel d'incendie doivent être loin des archives et serveurs.

# Préconisations :

* Choisir plusieurs fournisseurs Il est recommandé à une entreprise de faire appel à plusieurs fournisseurs d’infrastructures et réseaux pour minimiser les risques éventuels liés à l’externalisation d’un PCA/PRA. En cas de problème avec un fournisseur, un autre prestataire est alors en mesure d’assurer une continuité de service.
* Vérifier la qualité du réseau Un réseau de qualité est un critère primordial à prendre en compte dans le choix de son prestataire. En effet, la capacité du réseau de celui-ci, pour l’interconnexion des différents sites, la réplication des données et l’accès au SI de l’entreprise, doit permettre la réalisation d’un PCA/PRA dans des conditions optimales. Il est possible d’accéder au SI de l’entreprise de deux manières :
  + dans le cadre d’un hébergement “privé” d’applications métiers par exemple, l’identification des personnes se connectant au SI est alors connue, ce qui permet de gérer le réseau de bout en bout.
  + dans le cadre d’un hébergement “public” de sites internet par exemple, l’identification des internautes n’est pas connue à l’avance, ce qui crée une dépendance vis-à-vis des opérateurs réseaux. Dans ce dernier cas, le prestataire peut procéder à la bascule en : modifiant les enregistrements des zones DNS, ou de manière plus transparente et réactive grâce aux technologies CDN (Content Delivery Network).
* Adapter la réplication aux contraintes de l’architecture Dans le cadre d’une architecture physique, le professionnel s’orientera naturellement vers la réplication des données, tandis que pour une infrastructure virtuelle ou en mode cloud il privilégiera la réplication de l’environnement (OS et applications).
* Réaliser des tests réguliers. Un prestataire qualifié réalisera un test de mise en situation régulièrement (tous les mois par exemple), portant uniquement sur la disponibilité de la plateforme distante. Par ailleurs, au moins une fois par an, le professionnel prévoira une bascule en situation réelle. Ce dispositif de test permet ainsi de vérifier que le PCA/PRA fonctionne bien et d’effectuer quelques ajustements au besoin.

# Méthode pour sauvegarde :

Afin d’éviter toute perte d’information, il faut sauvegarder les données du serveur. On peut choisir différents moyens pour bien faire cette procédure.

Une réplication peut être faite pour copier tout l’information qu’il y a sur un serveur, de cette manière, on peut avoir 2 fois la même information en temps réel, parce que les 2 serveurs (l’original et la copie) ont un lien et si on change une donnée sur l’original, le deuxième fera un copie a l’instant.

On a une deuxième possibilité, faire un copie de sécurité et sauvegarder les données dans une unité de stockage externe. Ça permettra d’avoir les données toujours loin des appareils électriques et, s’il y a un problème avec l’électricité, il faudra justement télécharge les données de l’unité de stockage externe au serveur après le problème. De la même façon que dernier option, il y a certains problèmes avec cette méthode, si on utilise une unité de stockage externe, il y a une possibilité qu’elle cesse de fonctionner et aussi, qu’on la perde.

Il existe une troisième option, faire un copie de sécurité et sauvegarder les données dans le cloud. Comme le cloud est toujours actif on pourra télécharger les données sans soucis. Cette option est la meilleure parce que, grâce au cloud, il n’y a pas de pertes, et aussi, le cloud peut sauvegarder les données après une panne du courant. De plus, on peut faire un copie de sécurité automatiquement, chaque heure, chaque jour, chaque semaine, etc. avec l’aide d’un programme comme Comodo Backup, Aomei Backupper Standard, Areca Backup, Cobian Backup.

Après connaitre tous les possibilités qu’on a pour pouvoir sauvegarder les données et en rappelant que Motuc veut un deuxième serveur (réplica), le chemin à suivre sera de faire une réplication du serveur et, après, pour améliorer la sécurité et éviter des pertes des données à cause d’une panne courant, il est nécessaire de faire un copie de sécurité dans la cloud. Pour bien faire cette copie on doit utiliser certains logiciels, le plus facile à utiliser c’est Backup Manager Cloudbuilde. De plus, il peut travailler avec différents OS, différents serveurs simultanément.

# Surveiller :

## Serveurs :

Les serveurs sont un élément fondamental d’une entreprise qui doit avoir beaucoup d’informations sur le même réseau. C'est pourquoi nous devons avoir sous surveillance chacun de ces serveurs. Mais que devrions-nous regarder? Chaque fois qu'il y a une défaillance du réseau électrique, une sauvegarde doit être effectuée sur les informations comptabilisées jusqu'au moment voulu.

Une analyse doit être programmée toutes les 10 minutes pour pouvoir protéger la majorité des informations dont dispose l’entreprise sur ses serveurs. On peut faire cette analyse a l’aide de Centreon, de plus, on peut superviser plusieurs choses (le serveur web par exemple).

## Base de données :

Pour chaque entreprise, les informations qui y sont traitées sont très importantes. De plus, les informations sont la cible de nombreuses attaques informatiques. Pour cette raison, la base de données de la société devrait sans aucun doute être surveillée.

Comme le serveur, vous devrez effectuer une copie de sécurité toutes les 10 minutes pour éviter toute perte de données en cas de panne de courant. Pour effectuer cette action, il sera nécessaire d’utiliser un programme permettant de faire une copie de sécurité des informations, comme Comodo Backup, Aomei Backupper Standard, Areca Backup, Cobian Backup.

# Sensibilisation des utilisateurs :

Parfois, les utilisateurs des ordinateurs des entreprises ne réfléchissent pas aux conséquences pouvant découler de certaines actions pouvant paraître très simples. Un exemple de ceci est d'insérer directement une mémoire USB dans votre ordinateur. À l'intérieur d'une mémoire USB, il peut exister un programme d'origine inconnue qui vise à voler les données de l'entreprise. Un autre exemple pourrait être le fait qu’il arrive que les utilisateurs ouvrent un courrier électronique provenant d’un expéditeur inconnu. Ce courrier électronique peut contenir un fichier qui, au moment de l’ouvrir, attaque directement les données et les partage de manière secrète avec la personne qui les a envoyées. J'avais envoyé le courrier.

Lorsque vous travaillez dans une entreprise, vous devez tenir compte de nombreux éléments. Toute chose, aussi simple que cela puisse paraître, peut poser un problème trop important pour l'entreprise. Il est donc nécessaire que chaque utilisateur respecte les règles en vigueur dans chaque entreprise.

# Conclusion :

Chacune des actions menées a un but, lorsqu'un changement est effectué, que ce soit au sein d'une grande ou d'une petite entreprise, cela se fait en pensant à une amélioration de l'entreprise. Dans ce cas, plusieurs modifications doivent être apportées pour accroître la sécurité de Motuc. Ainsi, la possibilité de subir une nouvelle cyberattaque est supprimée ou minimisée.

Pour ce faire, il a été pensé de créer une sauvegarde qui sauvegardera les données directement dans le cloud. Cela se produira toutes les 10 minutes à l'aide d'un programme pouvant être sauvegardé et, en plus d'empêcher une nouvelle attaque, Il prévoit que les données ne seront pas perdues lors de tout autre événement important, tel qu'un incendie, une panne d'électricité, etc.

De la même manière, il faut garder à l'esprit que certaines règles doivent être établies pour assurer une sécurité encore plus grande, chaque utilisateur faisant partie de ce système à partir duquel il souhaite atteindre un meilleur niveau de sécurité, raison pour laquelle il doit, également, avoir votre propre changement.