

BROSSARD Théo (20190049)

RUELLE Raphaël (20214849)

Etudiant en M2 CNS SR à L’Université d’Évry Val D’Essonnes

23 Bd François Mitterrand, 91000 Évry-Courcouronnes

Projet SSI (Sécurité des systèmes informatiques)

Professeur Encadrant : M.PLOIX

[SSI : le contexte du projet 3](#_Toc155271750)

[Situation de l’entreprise (pré-contexte) : 3](#_Toc155271751)

[Organigramme : 3](#_Toc155271752)

[Définition du contexte étudié : 4](#_Toc155271753)

[Comment ? Axes d’analyses 4](#_Toc155271754)

[Le niveau de l’entreprise avec ISO/CEI 27002 7](#_Toc155271755)

[Organisation de la sécurité de l'information 7](#_Toc155271756)

[Relations avec les fournisseurs 7](#_Toc155271757)

[Conformité 8](#_Toc155271758)

[Sécurité liée aux ressources humaines 8](#_Toc155271759)

[Gestion des informations et des actifs 9](#_Toc155271760)

[Mesures techniques : contrôle d’accès 9](#_Toc155271761)

[Mesures techniques : Ops 9](#_Toc155271762)

[Sécurité physique et environnementale 9](#_Toc155271763)

[Gestion des incidents liés à la sécurité de l’information 10](#_Toc155271764)

[Mesures techniques : surveillance du SI 10](#_Toc155271765)

[Mesures techniques : architecture des systèmes 10](#_Toc155271766)

[Mesures techniques : architecture réseau 11](#_Toc155271767)

[Mesures techniques : Dev (Sec) 11](#_Toc155271768)

[Politique de sécurité de l'information 11](#_Toc155271769)

[Etude des risques à l’aide de MEHARI 12](#_Toc155271770)

[But de l’étude 12](#_Toc155271771)

[Détermination des DIC 12](#_Toc155271772)

[Tableau T1 : 12](#_Toc155271773)

[Données applicatives (bases de données) 12](#_Toc155271774)

[Données applicatives isolées, en transit Messages : 12](#_Toc155271775)

[Fichiers bureautiques partagés 13](#_Toc155271776)

[Courrier électronique 13](#_Toc155271777)

[Archives informatiques 13](#_Toc155271778)

[Tableau T2 : 14](#_Toc155271779)

[Services du réseau étendu 14](#_Toc155271780)

[Services du réseau local 14](#_Toc155271781)

[Services bureautiques communs 14](#_Toc155271782)

[Equipements mis à la disposition des utilisateurs 14](#_Toc155271783)

[Services de publication sur site web 15](#_Toc155271784)

[Services généraux environnement de travail 15](#_Toc155271785)

[Services télécom 15](#_Toc155271786)

[Tableau T3 : 15](#_Toc155271787)

[Protection des renseignements personnels 15](#_Toc155271788)

[Communication financière 15](#_Toc155271789)

[Protection des systèmes informatisés 16](#_Toc155271790)

[Risque présent après le DIC 16](#_Toc155271791)

[Traitement du risque 16](#_Toc155271792)

[Risque actif après les scénarios 21](#_Toc155271793)

[Etablissement d’un plan d’action 21](#_Toc155271794)

[Choix du plan d’action 21](#_Toc155271795)

[Service à améliorer 22](#_Toc155271796)

[Sauvegarde des données applicatives 22](#_Toc155271797)

[Sauvegardes de secours (recours) externalisées 23](#_Toc155271798)

[Niveau de risque après le plan d’action 23](#_Toc155271799)

SSI : le contexte du projet

Situation de l’entreprise (pré-contexte) :

Il s'agit d'un site français de vente de manga et de Light Novel et d'objets d'asiatiques, appelé "Le repère des Otakus". L'activité se déroule principalement dans des pays francophones tel que la France, la belgique, la suisse et à Québec uniquement.

L'entreprise stocks des objets dans 2 entrepôts en France et au 1 à Québec près de prestataire de livraison comme Chronopost ou des services de postes locales.

Du fait de la multiplicité des locaux, les informaticiens s'occupant du site et du logiciel de logistique interne aux entrepôts sont en télétravail. Il y a une petite équipe informatique de 3 personnes dans chacun des entrepôts pour les petits problèmes du quotidien. Cependant les grosses taches, comme les pannes généralisées, une intrusion dans le système, etc.… sont gérées par une entreprise spécialisée. Le site web, les bases de données de clients, les commandes ou encore le logiciel de logistique sont stockés sur des datacenters de prestataires externes comme AWS ou OVH.

Les produits sensibles (les plus chères) sont stockés dans un espace réservé dans chacun des entrepôts dans lequel, il faut un accès par badge et donc être habilité à y entrer. Les différents sites sont surveillés par vidéo de caméra surveillance et les vidéos sont stockées sur les serveurs du prestataire ayant installé le système de sécurité.

L'entreprise obtient les livres via des distributeurs en France (hachette...) et les divers objets asiatiques, via imports des pays asiatiques dont ils sont issus comme la Chine, le Japon….

Organigramme :



Définition du contexte étudié :

*Quelles sont les principales missions / processus / activités / informations, leurs finalités ?*

* **Missions principales :** Vente en ligne, Logistique.
* **Processus principaux :** Vente en ligne (Financier+, Image++, Réglementaire+), Logistique (Financier++, Image 0, Réglementaire +).
* **Activité principale :** Vente en ligne
	+ **Gestion des accès**
	+ **Gestion du site :**
		- **Installation :** Site installer un serveur dédier sous linux. Le site est créé de toute pièces et est rendu disponible grâce à un programme comme apache ou nginx. Le site utilise cependant des add-on pour les transactions bancaires.
		- **Maintenance :** Mise à jour de l’OS, et des outils lier au site quand c’est nécessaire.
	+ **Gestion du contenue :**
		- **Contenu initial :** Page d’accueil présentant les produits phares
		- **Maintenance :** mise à jour régulière des produits à vendre…
	+ **Gestion des données : hébergement, sauvegarde…)**

*Quels sont impact en terme financier / image / humain / réglementaire / environnemental d’un disfonctionnement de chacune de ces missions ?*

* Impacts Financier :
	+ La vente en ligne est l’activité principale de l’entreprise, si le site de vente n’est plus disponible, les utilisateurs ne peuvent plus commander et donc il y a une perte d’argent dans l’immédiat. Cela peut en plus envoyer les client la concurrence et donc perdre de l’argent sur le plus long terme
	+ Si l’approvisionnement, l’envoie des marchandises ne se fait pas correctement, on peut se retrouver dans l’incapacité de livrer les produits, les utilisateurs peuvent demander à terme des remboursements. Si cette activité ne fonctionne pas correctement, l’entreprise ne peut exercer l’activité pour laquelle elle existe.
* Impact sur l’image :
	+ Dans un site peux ergonomique, avec des transactions qui ne fonctionne pas correctement peux léser le consommateur et l’amener à faire des critiques négative qui peuvent avoir un impact non souhaité sur les ventes.
	+ Si les produits sont reçus endommager ou encore sont de mauvaise qualité, le client peux ou encore critiquer la marque la marque et nous faire perdre en visibilité.
* Impact humain :
	+ Vente en ligne : Pas d’impact/On ne sait pas
	+ Logistique : Pas d’impact/On ne sait pas
* Réglementaire :
	+ Cas de la Vente en ligne : RGPD, hébergement de données, données nominatives de contrôle d’accès aux sites
	+ Cas de la logistique : Aucun
* Environnementaux :
	+ Cas de la Vente en ligne : Surconsommation des serveurs si utiliser de façon détourner de son utilisation nominale
	+ Cas de la logistique : En cas d’erreur d’envoi, il y a un nouveau transport à faire, qui peut être polluant.

Comment ? Axes d’analyses

*Quels sont les services numériques, applications, réseaux informatiques, structures organisationnelles, ressources humaines, locaux, etc. qui permettent de mener à bien ces processus ou de traiter ces informations ?*

Actifs de type « information » :

**Cas de vente en ligne :**

* **Données applicatives (bases de données) :** Base de données de type SQL pour le stock disponible, les commandes effectué, base de données des utilisateurs.
* **Données applicatives isolées, en transit Messages :** Pas de données isolées, seulement des confirmations de commandes par mail à destination des utilisateurs.
* **Fichiers bureautiques partagés :** Les bases de données
* **Fichiers bureautiques personnels :** Non
* **Documents personnels :** Non
* **Listings ou états imprimés :** Non
* **Courrier électronique :** Oui, certaines communications en interne se font par mail. Les informations sur l’évolution d’une commande sont envoyées par mail à l’utilisateur
* **Courrier postal :** Non
* **Fax Archives documentaires :** Non
* **Archives informatiques :** Oui, toutes commandes et les stocks sont sauvegarder pourconsultation ultérieure.

**Cas pour la logistique :**

* **Données applicatives (bases de données) :** Base de données de type SQL pour le stock disponible, les commandes effectuées.
* **Données applicatives isolées, en transit Messages :** Non
* **Fichiers bureautiques partagés :** Les bases de données
* **Fichiers bureautiques personnels :** Non
* **Documents personnels :** Non
* **Listings ou états imprimés :** Non
* **Courrier électronique :** Oui, certaines communications en interne se font par mail.
* **Courrier postal :** Non
* **Fax Archives documentaires :** Non
* **Archives informatiques :** Oui, toutes commandes et les stocks sont sauvegarder pourconsultation ultérieure.

Actifs de type « services » :

**Cas de vente en ligne :**

* **Services du réseau étendu :** oui, Internet
* **Services du réseau local :** oui, un intranet est disponible
* **Services applicatifs :** Non
* **Services bureautiques communs :** hébergement des procédures (SP, Teams, OneDrive, …)
* **Equipements mis à la disposition des utilisateurs :** Ordinateurs, Imprimante, Connexion internet (Box).
* **Services systèmes Communs (Systèmes, périfs , etc.) :** Ordinateurs, Imprimante, Intranet, Internet.
* **Services de publication sur site web :** oui
* **Services généraux environnement de travail :** Office 365, Environnement de programmation au choix, GitHub
* **Services télécom :** Téléphone portable pour les télétravailleurs et ceux des services informatiques.

**Cas pour la logistique :**

* **Services du réseau étendu :** oui, Internet
* **Services du réseau local :** oui, un intranet est disponible
* **Services applicatifs :** Non
* **Services bureautiques communs :** hébergement des procédures (SP, Teams, OneDrive, …)
* **Equipements mis à la disposition des utilisateurs :** Ordinateurs, Scan.
* **Services systèmes Communs (Systèmes, périfs , etc.) :** Imprimantes
* **Services de publication sur site web :** Non
* **Services généraux environnement de travail :** Office 365, Gestionnaire de logistique comme Infolog
* **Services télécom :** Téléphone portable pour les chefs.

Actifs de type « Lois et règlements » :

|  |  |  |
| --- | --- | --- |
|   | Processus | Informations |
| **Actif** | **Vente en ligne**  | **Logistique**  | **Vente en ligne** | **Logistique** |
| Protection des renseignements personnels | Oui | Oui | RGPD |
| Communication financière | Oui | Non | Site marchant vers la Banque |   |
| Vérification de la comptabilité informatisée | Non | Non |   |   |
| Protection de la propriété intellectuelle | Non | Non |   |   |
| Protection des systèmes informatisés | Oui | Oui | Dans les 2 cas, il peut y avoir des données client |
| Sécurité des personnes et protection de l'environnement | Non | Oui |   | Equipement pour les salariés et règles interne |

Le niveau de l’entreprise avec ISO/CEI 27002

Organisation de la sécurité de l'information

* Comment s’organise la cyber sécurité au sein de l’entreprise et l’ensemble du management est-il bien sensibilisé ?

Notre entreprise dispose d’un service sur la sécurité informatique qui est une section indépendante du pôle informatique. Elle est constituée d’un chef qui a à sa disposition une petite équipe sur chaque site avec l’aide d’un prestataire en cas de grosse attaque ou de problème non résolue. Il est organisé régulièrement des campagnes de sensibilisation sur le danger cyber avec des tests réguliers sur des attaques de type phishings où de bon résultat pour un service pourrait permettre d’avoir des récompenses avec des primes.

* La séparation des tâches est-elle prise en compte ?
	+ Comment s’organisent les activités « sensibles » au sein de l’entreprise ?
	+ Comment s’organise la gestion du contenu des sites ?

Au sein de l’entreprise, il existe des services qui assurent chacun un rôle particulier comme la rédaction des règles au niveau informatique qui est fait par le service de la sécurité informatique ou la faisabilité d’un projet au sein de l’entreprise au niveau de l’informatique par le service des gestions des risques informatique.

La gestion du contenu des sites est gérée par une autre équipe dans le pôle e-commerce, service webmaster en coopération avec le service web designer.

* Des PME/ETI clientes ont-elles des métiers particuliers/sensibles ?

On ne dispose pas de PME/ETI clientes à notre entreprise mais seulement de prestataires.

* Comment l’entreprise est-elle au courant des menaces liées à l’hébergement des sites, à la version WordPress utilisée, … ?

Les personnes travaillant dans le service sécurité informatique se tiennent souvent au courant en allant consulter les dernières failles de sécurité rencontrées mise en ligne et une réunion hebdomadaire est mise en place pour comparer les dernières failles trouvées par chaque membre du personnel.

* Comment et à qui sont remontés les incidents et les évènements de sécurité ?

En cas d’incidents ou d’évènement de sécurité au sein de l’entreprise, ses problèmes sont remontés au sein du service de sécurité de l’information par des systèmes de logs et/ou la mise en place de systèmes de détection de problème. Si le problème ne peut pas être résolu par l’équipe, il est alors renvoyé vers notre prestataire qui nous aide en cas de gros problème de sécurité informatique interne à l’entreprise.

Relations avec les fournisseurs

Au sein de l’entreprise, il existe un service qui assure la communication avec les prestataires en négociant les contrats avec eux, en mettant en place des indicateurs de performances et des sanctions en cas de non-respect de ses indicateurs. Il est indiqué dans ce contrat que le prestataire gère la sécurité informatique entre Internet et les machines virtuelles que l’on utilise mais il est cependant de notre responsabilité, la prise en charge de la sécurité à l’intérieur de ces machines. Un sous-traitant supplémentaire palie aux problèmes liés à de grosses attaques sur notre système.

Conformité

Au sein de l’entreprise, il existe un service vérifiant le respect des normes en vigueur dans notre secteur comme le RGPD. Il est à l’étude au sein de l’entreprise de faire de plus en plus de certification du respect de ses normes pour apporter une image plus positive aux clients. Chacune de ses normes fait l’état d’une étude mise en place.

Dans le cas du RGPD, un audit est effectué régulièrement pour éviter la fuite de données de nos clients mais aussi échapper aux amendes qui sont importantes dans ce secteur d’activité.

Sécurité liée aux ressources humaines

* Les fonctions/métiers sensibles sont-ils identifiés ?

Les fonctions à responsabilité et les métiers du pôle informatique sont identifiés comme sensible.

* Des contraintes réglementaires sont-elles présentes sur ces fonctions/métiers et intégrées aux processus RH ?

Pour les candidats de ces fonctions/métiers sensibles, il est exigé dans le processus de recrutement d’avoir fait un entretien physique avec le responsable du service concerné.

* Les chartes liées à l’utilisation des moyens numériques et à l’administration sont-elles en place ?

Une charte écrite par le service de sécurité informatique est à signer dans la première semaine d’embauche ou lors de sa modification. En cas de non-signature, les droits d'accéder à une machine sont retirés jusqu’à signature.

* Des sensibilisations récurrentes sont-elles réalisées ?

Le service RH propose régulièrement des initiations pour les employés notamment des stages sur les enjeux de la cybersécurité.

* Des activités internes ou interventions externes nécessitent-elles des NDA ?

On n’est pas soumis à une NDA

* Le TAD est-il autorisé pour toutes les activités et comment sont sécurisées les activités réalisées en situation de TAD ?

Le télétravail est autorisé pour seulement certains postes comme l’équipe de développement s’il n’a pas besoin de faire des tests. La sécurité du télétravail est assurée par un mécanisme de double-authentification et l’usage d’un point de connexion non-public. En cas de déplacement dans une région à risque, l’entreprise peut fournir une machine dédiée pour ce problème.

Gestion des informations et des actifs

* L’ensemble des actifs est-il connu et correctement décrit (CMDB, urbanisme des processus, traitements et des données, …) ?

L’arrivé d’actif fait l’usage d’un enregistrement dans la base de données des actifs avec ses informations comme le type d’actifs, le numéro de série, les configurations si besoin, etc… Une modification d’une de ses caractéristiques doit être reportée dans la base de données.

Un scan du réseau est effectué régulièrement afin de vérifier si les actifs sont toujours présents et qu’il n’y a pas d’intrusion. Ce scan permet aussi de savoir si les actifs sont bien à jour.

* L’utilisation des actifs est-elle maîtrisée (principes du moindre privilège et du besoin/droit d’en connaître) et tracée ?

L’utilisation de ses actifs fait l’usage d’authentification pour pouvoir s’en servir et les droits accordés à l’utilisateur. De base, tous les utilisateurs ont comme droit le principe du moindre privilège. L’usage d’un actif en dehors de ses droits doit faire une demande d’utilisation qui peut être approuvée par le chef de service ou le chef de la sécurité informatique dans certains cas. Les actifs sensibles sont logués pour garder en mémoire les utilisateurs et leurs usages.

Mesures techniques : contrôle d’accès

L’entreprise applique le principe du moindre privilège pour ses employés et accorde des droits selon le groupe d’utilisateur de l’employé. Il est possible dans des cas légitimes de faire des demandes pour accéder à certaines applications qui peuvent être validées par le chef de service ou le chef de la sécurité informatique pour un temps donné. Pour accéder à des applications sensibles, il est demandé de pratiquer la double authentification avec un token attribué à l’employé toujours dans une optique de les loguer et d’identifier les actions d’une personne sur un service.

Mesures techniques : Ops

Dans le cadre d’un projet, l’entreprise fait toujours une étude avec le service de la gestion des risques informatique sur la capacité nécessaire et futur d’un projet et la surveillance régulière sur cette limite avec un indicateur de seuil. De plus, on vérifie régulièrement dans un rapport documenté, les différentes configurations dans le projet et les modifications futures de ses configurations.

Avant chaque changement, un comité est organisé pour indiquer les changements qui vont être faits. De plus, l’entreprise effectue des sauvegardes pour palier la corruption de données ou la perte de données. Chaque procédure doit faire l’usage d’un document rédigé par de futurs collaborateurs mais aussi d’aider à la compréhension en cas de soucis.

L’entreprise mise un niveau de maturité de 3 dans l’espoir futur de le passer à 4.

Sécurité physique et environnementale

* Quelle sécurisation pour les locaux de l’entreprise ?

Les sites font l’usage de caméra de surveillance avec un contrôle des accès à badge pour rentrer dans les salles sensibles (entrepôt des produits sensibles, le pôle informatique et ressource humaine). Il y a présence d’un gardien pour la surveillance de jour comme de nuit.

* Quelle sécurisation pour le datacenter ?

Le datacenter n’est pas physiquement sur le site.

* Les matériels informatiques de l’entreprise sont-ils gérés (sécurité, maintenance, …) ?

Pour éviter le vol de matériels informatiques, chaque appareil est accroché par un système de lien. De plus, la maintenance est assurée par l’équipe de la sécurité informatique.

* Des stockages externes (USB) sont-ils utilisés / nécessaires ?

L’usage de stockages externes n’est pas nécessaire au sein de l’entreprise.

Gestion des incidents liés à la sécurité de l’information

Pour faire face aux incidents liés à la sécurité de l’information, un plan de réaction a été préparé. Il est prévu que si le problème peut être géré par nos équipes, on prend en charge ce problème sinon, on le délègue à notre prestataire. Après un incident, on effectue une réunion pour déterminer la cause de l’apparition du problème ayant pour but, de le corriger et renforcer notre sécurité. De plus, on effectue une enquête avec l’aide des autorités en cas de délit grave en recueillant les preuves des attaques afin d’éviter à d’autres entreprises d’en être victimes. En cas d’attaque critique sur notre système d’information, on a décidé de couper la connexion de notre entreprise vers l’extérieur, stoppant de facto, l’activité de l’entreprise.

Mesures techniques : surveillance du SI

* Une collecte des informations est-elle en place ?

Au sein de l’entreprise, il existe un système de logs qui enregistre pour chaque utilisateur et application les actions réalisées qu’elle soit légitime ou non.

* Un SIEM / SOC est-il en place ?

Le personnel du service de la sécurité informatique dispose d’outils de surveillance et d’alerte en cas de comportement suspect sur le réseau informatique.

Mesures techniques : architecture des systèmes

L’entreprise utilise des PKIs permettant l’utilisation de certaines applications et/ou d’accéder à la base de données des clients. Cela permet de restreindre l’accès à ces données seulement a ceux qui ont le droit d’en savoir. De plus, pour éviter l’impact d’une fuite de données nous avons mis en place un chiffrement des données échanger entre les machines en plus d’un système de sauvegardes en cas d’effacement. Nous utilisons les algorithmes qui sont reconnus comme solide dans le milieu informatique tout en restant au courant de la fiabilité de nos algorithmes. Cependant ces algorithmes ne sont pas post-quantiques pour l’instant.

L’attribution et l’utilisation de privilèges sont enregistrer tout comme les actions effectuées sur les systèmes. L’élévation de privilèges fait aussi partie des éléments surveillés.

Tout élément externe passe par un anti-virus qui indique une note selon la confiance de l’expéditeur.

Le temps des machines provient d’un serveur de temps NTP.

Mesures techniques : architecture réseau

Au sein de l’entreprise, l’architecture réseau est séparé entre le réseau d’administration et le réseau de production. Comme architecture réseau, nous avons opté pour la périmétrisation où entre chaque périmètre un filtrage est effectué pour laisser passer seulement les flux légitimes. Un filtrage est effectué pour que les clients aient accès à seulement ce que le client doit avoir accès.

Mesures techniques : Dev (Sec)

* Les bonnes pratiques d’architecture et de codage (WordPress) sécurisé sont-elles connues / appliquées ?

Nous fournissons aux développeurs les bonnes pratiques pour le développement de leur programme. Cependant, on ne sait pas si ses pratiques sont bien respectées.

* Des revues de la sécurité sont-elles réalisées à chacune des phases du cycle de vie des systèmes ?

Un audit sur le code est réalisé lors de grosse mise à jour.

* Les environnements développement/intégration/préproduction/production sont-ils cloisonnés ?

Ses environnements sont isolés du reste du réseau.

* Qui a accès au code source ?

Seul le personnel de développement et le chef des différents services informatiques ont accès au code source. Le reste du personnel doit faire des demandes pour y accéder.

* Quelles données sont utilisées pour le développement l’intégration les tests ?

Il s’agit de données crées et non de vraie information

* La gestion des vulnérabilités est-elle en place ?

Il a été décidé que la mise en place des tests n’est pas reliée au reste du réseau de l’entreprise et à Internet.

* Un/des environnement/s sont-ils en place pour les tests de sécu ?

Plusieurs machines sont mises à disposition pour des tests déconnecté du reste du réseau de l’entreprise.

* Le développement externalisé est-il sécurisé ?

Le développement externalisé est sécurisé par l’usage de PKI pour accéder à l’environnement de développement de l’entreprise. Cependant, les tests restent à effectuer dans les installations de l’entreprise.

Politique de sécurité de l'information

Nous procédons à une vérification annuelle des politiques de sécurité de l’information pour déterminé si toutes les mesures sont rigoureuses respectées ou s’il faut ajouter nouvelles règles.

Etude des risques à l’aide de MEHARI

But de l’étude

Il ne s’agit pas d’une étude complète. On portera un point de vue plus précis pour diminuer les risques sur les « données applicatives » dans le cas de la disponibilité.

Détermination des DIC

Tableau T1 :

Données applicatives (bases de données)



D : Dans notre cas, on fait de la vente en ligne, l’accès aux base de données pour le bon fonctionnement de l’application web est primordiale pour le bon fonctionnement de l’activité de l’entreprise, en effet, sans le site de vente, l’activité de l’entreprise est retardée voir complétement arrêtées, on a donc choisi de mettre le niveau maximum, car une non-disponibilité de la base de données peux être bloquante pour l’activité car on ne pourrait afficher les produits disponibles, autorisé les connections sur les comptes client (ou admin), pendant un temps, temps pour laquelle l’activité est à l’arrêt.

I : Les données en BDD doivent être fidèle à la réalité ou très proche, en effet, le stock afficher doit-être correct, les commandes doivent être enregistrer pour le bon client, le client qui se connecte doit avoir accès au bon compte. En effet, si une commande est affectée au mauvais client ou qu’elle n’est simplement pas enregistrée, le client ne recevra jamais sa commande, on n’aura pas de trace de la commande côté logistique ce qui rends le moyen de détecter le problème presque impossible. Le client pourrait cependant prouver l’achat par un mail ou une trace du payement. L’information peut-être donc seulement récupérée partiellement. De ce fait, on a choisi de mettre cette métrique à 3 pour sa difficulté de détection et de correction.

C : On a choisi de mettre cette métrique à 3, en effet, la base de données contient notamment, les données client comme le nom, le prénom, l’adresse, les données bancaires qui sont des données sensibles et destinées uniquement à ceux qui ont « besoin d’en savoir ».

Données applicatives isolées, en transit Messages :



D : Il n’est pas utile que ce service soit en permanence disponible, en effet, on ne l’utilise que pour la confirmation des commandes. La non-disponibilité n’a donc aucun impact sur l’activité de l’entreprise, Niveau 1.

I : Il s’agit toujours d’indiquer à l’utilisateur l’avancée de sa commande, si les informations envoyées sont erronées, le confort de l’utilisateur peut en être impacté, mais cela ne présente aucun impact sur l’activité de l’entreprise. Niveau 1

C : Il s’agit ici de données destinées uniquement à ceux qui ont « besoin d’en savoir », en effet, on pourrait y voir une adresse, le nom, le prénom du destinataire. De ce fait, l’accès à ces informations doit être restreint. Niveau 3.

Fichiers bureautiques partagés



Comme on utilise les mêmes bases de données que pour les données application on y appose donc même niveau de métrique pour ce cas précédent. La disponibilité au niveau 4, l’intégrité au niveau 3 et la confidentialité au niveau 3.

Courrier électronique



D : Les informations sur les comptes des utilisateurs, comme un accès non autorisé, ou encore une confirmation de commande sont envoyé par mail, une forte disponibilité est donc recommandée, mais elle n’arrête pas l’activité de l’entreprise, cela n’a d’ailleurs aucun impact en cas de non-disponibilité. Cependant, la plupart des communications en interne de l’entreprise se font par mail notamment pour le signalement et la résolution de problème, une haute disponibilité est donc recommandée, car pourrait lourdement impacter l’activité de l’entreprise.

I : Bien qu’il s’agisse d’informations utiles à l’utilisateur, le fait qu’une information soit erroné dans le mail ne devrait pas avoir de grosses conséquences, si ce n’est de l’inconfort. En effet, ces informations comme une confirmation de commande ou de tentative de connexion sont juste créer pour le confort pour l’utilisateur. Ces erreurs peut-être facilement vérifiées par l’utilisateur en se connectant sur son profil et donc retrouver les bonnes informations au besoin. Du fait de la non-criticité de données erronées, et de la facilité de la consulter ailleurs, on a défini ce niveau à 2.

C : Il peut parfois s’agir de données sensibles comme une adresse qui sont envoyées par mail, il n’y a donc que ceux qui ont besoin d’en savoir qui doive avoir accès à ces informations, niveau 3.

Archives informatiques



D : Le principe des archives, c’est qu’il s’agit d’informations stockées pour une consultation ponctuelle et non-régulière, la non-disponibilité n’a donc pas d’impact sur l’activité de l’entreprise, donc on définit cette métrique à 1.

I : Il s’agit d’archive qui contient des informations importantes comme l’historique des ventes, des stocks ou encore d’informations personnelles sur les clients, cela en fait des informations très sensible qui ne doivent être altérer. De plus du fait de la non-vérification régulières des archives, des données altérées sont difficilement détectable et sera probablement impossible à récupérer, cette métrique est donc de 4.

C : Il s’agit, pour les mêmes critères que l’intégrité de données qui peuvent être très sensible, ces informations sont donc limitées à un accès très restreint. Le client ne peut lui aussi consulter ces données, elles sont donc limitées à un nombre très restreint de membres du personnel du fait de la confidentialité des informations et seules les personnes autorisées peuvent y accéder, de plus, on sait qui l’a consulté ou modifié et quand. Cette métrique est donc définie à 4.

Tableau T2 :

Services du réseau étendu



D : Le réseau étendu permet l’accès aux différents services stockés sur les serveurs des prestataires comme AWS ou OVH. Une non-disponibilité rendrait l’application inaccessible ce qui est inadmissible puisque cela présente le gain pain de l’entreprise, une non-disponibilité, dans le pire des scénarios implique un arrêt total de l’activité. Niveau 4.

I : Les informations circulant dans le réseau doivent être fiable, une information erronée sera difficile à détecter et/ou difficile à corriger voire non-récupérable, une erreur peut donc être critique. Niveau 4.

Services du réseau local



D : L’indisponibilité a un impact majeur mais non bloquant, en effet, on parle d’ici d’un intranet d’entreprise, s’il est inaccessible, cela n’empêche pas les clients faire leur commande, cela peut en revanche empêcher les membres du personnel d’effectuer une maintenance sur les différents services de l’entreprise, cependant dans le pire des cas, si on doit faire une maintenance sur quelque chose de critique cela peut aller jusqu’à un arrêt du service et donc de l’activité de l’entreprise. Niveau 4.

I : Les informations circulant dans le réseau doivent être fiable, une information erronée sera difficile à détecter et/ou difficile à corriger voire non-récupérable, une erreur peut donc être critique. Niveau 4.

Services bureautiques communs



D : L’indisponibilité a un impact limité et acceptable, en effet, si les services de bureautique sont inaccessibles en ligne, on peut toujours travailler de façon limitée avec ce qu’on a accès durant la panne. L’activité n’est donc pas à l’arrêt et l’activité n’est que faiblement impacté. Niveau 2.

I : Une information erronée sera difficile à détecter et/ou difficile à corriger, en effet, une information reçus erronée peut entraîner une incompréhension sur les ordres reçus, des fichiers envoyer peut-être corrompu durant l’envoi… Des erreurs qui peuvent être facilement détecté et corrigé dans certains cas, et beaucoup plus difficilement dans d’autres cas. Niveau 3.

Equipements mis à la disposition des utilisateurs



D : En cas de panne des actifs matériels, l’activité de vente peut toujours fonctionner. Cependant, il y a un impact majeur au sein de l’entreprise avec du personnel qui ne peut plus exercer leur activité au sein de la compagnie. Niveau 3

Services systèmes Communs (Systèmes, périfs, etc.)



D : Pour les mêmes raisons que pour le cas précédent, le niveau doit-être de 3.

I : Il faut que les données en commun soient intègre, car en cas de différences dans les données, il peut y avoir des conflits où plusieurs personnes travaillent sur des données censées être identique mais finalement différentes.

Services de publication sur site web



D : Le service de publication du web est un service critique de l’entreprise, il gère le site et ces composants. Sans ce service, l’application web serait difficilement mise en ligne ou maintenu. Etant un organe vital du fonctionnement de l’activité de vente et étant bloquante en cas de non-fonctionnement, on établit le niveau maximum de risque pour ce service.

I : Les informations transmises par le service de publication au site web doivent être correctes le niveau de risque est donc élevé, mais pas à son maximum, en effet, une information erronée, serai difficile à détecter et/ou à corriger. Niveau de risque à 3.

Services généraux environnement de travail



D : L’absence de ses environnements de travail des utilisateurs peut être embêtant pour pouvoir travailler. Cependant, ce problème ne pose pas de souci pour continuer l’activité.

Services télécom



D : L’outil de communication a été donné dans le but de faciliter la rapidité de communication en cas de problème. Un souci pour ce service n’a pas d’impact sur l’activité en cours, mais il peut retarder l’annonce du problème, car on doit passer par d’autres moyens de communications.

I : Une information mal transmise en cours d’utilisation de ses services peut être facilement corrigée en redemandant une correction de l’information à la personne transmettant le message.

Tableau T3 :

Protection des renseignements personnels



E : On est soumis aux différentes lois du RGPD puisque nous exerçons une activité sur le sol français et donc européen. En effet, nous stockons des données des utilisateurs et seulement les bonnes personnes doivent y avoir accès. Nous devons donc apporter une des exigences les plus élevées pour ce qui est des données, que ce soit pour les demandes de suppression (et s’assurer que cela a été fairt) et de la non-divulgation de ces informations. Niveau 4.

Communication financière



E : Oui, en effet, pour vérifier qu’une personne a la capacité de payer que la carte utilisée existe et/ou est valide, on doit interroger les services de la banque qui autoriseront ou non la transaction. Niveau 4

Protection des systèmes informatisés



E : On est une entreprise à moyenne échelle voir grande d’échelle puisqu’international, on traite aussi des données sensibles qui ne doivent pas fuiter comme des données client, de ce fait, on s’attend à des standards plus importants en ce qui concerne la protection des systèmes informatique, l’exigence est donc des plus importante, niveau 4.

Risque présent après le DIC



On peut voir qu’en mettant seulement les DIC pour les différents services, il y a déjà un aperçu du nombre de scénarios. Le but de la suite de cette étude est de diminuer les scénarios les plus graves en diminuant l’impact ou les conséquences.

Traitement du risque

|  |  |  |
| --- | --- | --- |
| **LIBELLÉ** | **Choix de gestion du risque** | **Justification** |
| Effacement accidentel de fichiers de données applicatives, suite à un incident d'exploitation | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. |
| Effacement par erreur de fichiers de données applicatives, par un utilisateur autorisé légitime, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Effacement par erreur de fichiers de données applicatives, par un utilisateur autorisé illégitime, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières et un contrôle régulier des rôles de chaque groupe d'utilisateur ou de l'utilisateur. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Effacement par erreur de fichiers de données applicatives, par un utilisateur non autorisé, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. Il y a utilisation de la double authentification pour accéder aux données applicatives (pour palier au vol de mot de passe), de plus toute modifications doivent-être validée par cette authentification et par un autre membre du personnel agréer. On autorise en plus uniquement des adresses MAC spécifique à se connecter au réseau interne de l'entreprise. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. |
| Effacement par erreur de fichiers de données applicatives, par un membre du personnel d'exploitation, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Effacement par erreur de fichiers de données applicatives, par un membre du personnel de maintenance, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Effacement malveillant de fichiers de données applicatives, par un utilisateur autorisé légitime, se connectant depuis le réseau interne | Acceptation | L'utilisateur étant de confiance à l'origine, nous ne pouvons lui restreindre plus les accès. Nous devons donc accepter se risque. De plus les sauvegardes permettent de récupérer les informations perdues. De plus comme toute modifications doivent-être validée par un autre membre du personnel agréer, Il faudrait au moins 2 personnes "malveillante" qui se serait concerté pour commettre le méfait, ce qui est encore moins probable. |
| Effacement malveillant de fichiers de données applicatives, par un utilisateur autorisé illégitime, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières et un contrôle régulier des rôles de chaque groupe d'utilisateur ou de l'utilisateur. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Effacement malveillant de fichiers de données applicatives, par un utilisateur non autorisé, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. Il y a utilisation de la double authentification pour accéder aux données applicatives (pour palier au vol de mot de passe), de plus toute modifications doivent-être validée par cette authentification et par un autre membre du personnel agréer. On autorise en plus uniquement des adresses MAC spécifique à se connecter au réseau interne de l'entreprise. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. |
| Effacement malveillant de fichiers de données applicatives, par un membre du personnel d'exploitation, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Effacement malveillant de fichiers de données applicatives, par un membre du personnel de maintenance, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Effacement malveillant de fichiers de données applicatives, par un tiers non autorisé, se connectant par un port de télémaintenance | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. Il y a utilisation de la double authentification pour accéder aux données applicatives (pour palier au vol de mot de passe), de plus toute modifications doivent-être validée par cette authentification et par un autre membre du personnel agréer. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. |
| Effacement malveillant total de fichiers et fichiers de sauvegarde de données applicatives, par un membre du personnel d'exploitation, se connectant par un port de télémaintenance | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Pollution accidentelle de fichiers de données applicatives due à une erreur de procédure, lors d'une opération de maintenance logicielle | Réduire | Sauvegardes pour revenir en arrière |

|  |  |  |
| --- | --- | --- |
| Pollution accidentelle de fichiers de données applicatives due à une erreur de procédure, lors d'une opération de maintenance à chaud | Réduire | On ne fait pas de maintenance à chaud |
| Pollution accidentelle de fichiers de données applicatives due à un incident d'exploitation | Réduire | Sauvegardes pour revenir en arrière |
| Pollution malveillante de fichiers de données applicatives, par un utilisateur autorisé illégitime, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières et un contrôle régulier des rôles de chaque groupe d'utilisateur ou de l'utilisateur. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Pollution malveillante de fichiers de données applicatives, par un utilisateur non autorisé, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. Il y a utilisation de la double authentification pour accéder aux données applicatives (pour palier au vol de mot de passe), de plus toute modifications doivent-être validée par cette authentification et par un autre membre du personnel agréer. On autorise en plus uniquement des adresses MAC spécifique à se connecter au réseau interne de l'entreprise. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. |
| Pollution malveillante de fichiers de données applicatives, par un membre du personnel d'exploitation, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Pollution malveillante de fichiers de données applicatives, par un membre du personnel de maintenance, se connectant depuis le réseau interne | Réduire | Pour pallier cet accident, on a décidé de réduire l'impact de ce risque en effectuant des sauvegardes régulières. On s'assure que l'utilisateur a uniquement accès à ce dont il a besoin. Toute modifications manuelles doivent-être validée par un autre membre du personnel agréer. |
| Perte, par destruction accidentelle, de media support de fichiers de données applicatives, dans les locaux de l'exploitation, suite à un incendie | Transfert | Comme nos bases de données et les applications sont chez un prestataire, c'est ce prestataire qui en a la responsabilité (d’après le contrat). |
| Perte, par destruction accidentelle, de media support de fichiers de données applicatives, dans les locaux de l'exploitation, suite à une inondation | Acceptation | On n’a pas de médiathèque, on accepte donc le risque |
| Perte, par destruction accidentelle, de media support de fichiers de données applicatives, en médiathèque, suite à un incendie | Acceptation | On n’a pas de médiathèque, on accepte donc le risque |
| Perte, par destruction accidentelle, de media support de fichiers de données applicatives, en médiathèque, suite à une inondation | Acceptation | On n’a pas de médiathèque, on accepte donc le risque |
| Perte, par disparition accidentelle, de media support de fichiers de données applicatives, en médiathèque | Acceptation | On n’a pas de médiathèque, on accepte donc le risque |
| Perte, par disparition accidentelle, de media support de fichiers de données applicatives, dans les locaux de l'exploitation | Transfert | Comme nos bases de données et les applications sont chez un prestataire, c'est ce prestataire qui en a la responsabilité (d’après le contrat). |
| Vol de media support de fichiers de données applicatives, dans les locaux de l'exploitation, par un membre du personnel non autorisé | Transfert | Assurances |
| Vol de media support de fichiers de données applicatives, dans les locaux de l'exploitation, par un membre du personnel d'exploitation | Transfert | Assurances |
| Vol de media support de fichiers de données applicatives, dans les locaux de l'exploitation, par un membre du personnel de service | Transfert | Assurances |
| Vol de media support de fichiers de données applicatives, en médiathèque, par un membre du personnel non autorisé | Acceptation | On n’a pas de médiathèque, on accepte donc le risque |
| Vol de media support de fichiers de données applicatives, en médiathèque, par un membre du personnel d'exploitation | Acceptation | On n’a pas de médiathèque, on accepte donc le risque |
| Vol de media support de fichiers de données applicatives, en médiathèque, par un membre du personnel de service | Acceptation | On n’a pas de médiathèque, on accepte donc le risque |
| Inexploitabilité accidentelle de media support de fichiers de données applicatives, dans les locaux de l'exploitation, due à une panne d'équipement | Transfert | Comme nos bases de données et les applications sont chez un prestataire, c'est ce prestataire qui en a la responsabilité (d’après le contrat). |
| Inexploitabilité accidentelle de media support de fichiers de données applicatives, dans les locaux de l'exploitation, due à un dégât des eaux | Transfert | Comme nos bases de données et les applications sont chez un prestataire, c'est ce prestataire qui en a la responsabilité (d’après le contrat). |
| Inexploitabilité accidentelle de media support de fichiers de données applicatives, dans les locaux de l'exploitation, due à une surcharge électrique | Transfert | Comme nos bases de données et les applications sont chez un prestataire, c'est ce prestataire qui en a la responsabilité (d’après le contrat). |
| Inexploitabilité accidentelle de media support de fichiers de données applicatives, dans les locaux de l'exploitation, due à un incident d'exploitation | Transfert | Comme nos bases de données et les applications sont chez un prestataire, c'est ce prestataire qui en a la responsabilité (d’après le contrat). |
| Inexploitabilité accidentelle de media support de fichiers de données applicatives, en médiathèque, due à une pollution | Acceptation | On n’a pas de médiathèque, on accepte donc le risque |
| Inexploitabilité accidentelle de media support de fichiers de données applicatives, en médiathèque, due à un dégât des eaux | Acceptation | On n’a pas de médiathèque, on accepte donc le risque |
| Disparition accidentelle de moyens nécessaires à l'accès aux fichiers de données applicatives | Réduire | Sauvegardes |
| Vol ou destruction malveillante de moyens nécessaires à l'accès aux fichiers de données applicatives | Transfert | Assurances + Sauvegardes |

Risque actif après les scénarios



À la suite de l’étude sur la gestion des différents scénarios dans le service étudié, on peut voir une diminution du nombre de scénarios à risque pour ce service. Cependant, il reste encore beaucoup de scénarios à grand risque. Donc dans une dernière partie, nous allons établir un ou des plans d’action pour couvrir ses scénarios.

Etablissement d’un plan d’action

Choix du plan d’action



On a choisi le plan palliation de type E car il s’agit du plan d’action qui joue sur le plus de scénarios pour le service étudié.

Service à améliorer

Sauvegarde des données applicatives

|  |  |
| --- | --- |
| A-t-on procédé, avec les utilisateurs, à une étude préliminaire afin d’identifier les scénarios que les sauvegardes doivent permettre de surmonter ? | 1 |
| A-t-on fait une étude avec l'ensemble des utilisateurs afin de définir pour chaque fichier la durée maximale admissible entre deux sauvegardes ?*Cette étude qui se base sur la capacité de reconstitution des informations perdues permet de définir le cycle de sauvegarde minimum.* | 1 |
| A-t-on étudié les synchronismes nécessaires entre différentes sauvegardes, toutes plates-formes confondues, pour assurer le bon fonctionnement de la reprise des applications et la cohérence des données nécessaire à cette reprise ? | 0 |
| Les différentes procédures issues des études faites sont-elles consignées dans un plan de sauvegardes comprenant, pour chaque classe de fichiers, la fréquence, les modalités de constitution et les synchronismes nécessaires ? | 0 |
| Le plan de sauvegarde comprend-il un plan de contrôle indiquant les différents contrôles à effectuer et leur fréquence (volumétrie, durée, relecture, etc.) ? | 1 |
| Ce plan de contrôle indique-t-il la conduite à tenir en cas d'incident ou d'anomalie ? | 1 |
| Le plan de sauvegarde est-il mis à jour à chaque changement de contexte d'exploitation ?*On veillera, en particulier, à ce qu'il soit bien mis à jour à chaque création ou modification d'applications.* | 1 |
| Ce plan de sauvegarde est-il traduit en automatismes de production ? | 0 |
| Contrôle-t-on régulièrement qu'une reprise ou un redémarrage est effectivement possible à partir des sauvegardes réalisées (test complet vérifiant le fonctionnement d'ensemble et l'absence de problème de synchronisme ou de cohérence) ? | 0 |
| Les automatismes de production assurant les sauvegardes sont-ils strictement contrôlés vis-à-vis de toute modification illicite ou injustifiée ?*Un contrôle strict requiert une protection renforcée pour pouvoir modifier ces automatismes et un enregistrement et un audit de toute modification des automatismes de sauvegarde ou un contrôle par scellement électronique de toute modification.* | 0 |
| Les procédures de sauvegarde et de conservation des données offrent-elles des garanties de conformité aux régulations et aux engagements de l'organisation en ce qui concerne la confidentialité et l'intégrité ? | 0 |
| Procède-t-on régulièrement à des tests de relecture des sauvegardes des données applicatives ? | 0 |
| Dispose-t-on systématiquement de plusieurs générations de fichiers afin de pouvoir s'affranchir d'un manque ou d'un illisible, en organisant par exemple une rotation des supports de sauvegarde ? | 0 |
| L'ensemble des procédures et plans de sauvegarde de données fait-il l'objet d'un audit régulier ? | 0 |

Après l’interrogation sur les questions de « Sauvegarde des données applicatives », on organise un plan d’action pour pallier les manquements en se basant sur les réponses déjà présentes. Dans un premier temps, nous allons lancer une étude sur la synchronicité des sauvegardes que l’on effectue, le cas échéant, il faudra mettre en place un mécanisme de vérification de la synchronisation des sauvegardes.

On veut mettre en place ces sauvegardes avant tout pour pouvoir rétablir l’activité de l’entreprise en cas de grave incident.

Dans un second temps, on mettra en place un mécanisme d’automatisation des sauvegardes et non, une manipulation manuelle des équipes pour les effectuer.

Après avoir mis en place ses mécanismes, nous allons mettre en place des systèmes de contrôles de l’intégrité de ces sauvegardes ainsi qu’un contrôle de leur bon fonctionnement. On ajoutera en plus, des contraintes d’accès aux sauvegardes joint à un système de log qui enregistre les accès en lecture, en écriture, quand et par qui. De plus, dans les tests de relecture, on s’assure que les fichiers gardent leur niveau de confidentialité.

Après avoir mis en place ces principes, et assuré leur bon fonctionnement, on voudrait mettre en place des sauvegardes en mettant en place une « génération de fichiers » qui consiste à avoir plusieurs fois le même fichier, mais de versions différentes, on choisit un nombre maximum de versions et la prochaine sauvegarde le fichier écrase le fichier le plus ancien.

À la suite de toutes ses réformes, on a décidé de faire appel à un audit annuel pour vérifier notre système de sauvegarde. On prendra soin de ne pas choisir la même entreprise d’audit d’une année à l’autre.

Sauvegardes de secours (recours) externalisées

|  |  |
| --- | --- |
| L'ensemble des sauvegardes de logiciels et fichiers de configuration permettant de reconstituer l'environnement de production est-il également sauvegardé en dehors du site de production (sauvegardes de secours) ? | 0 |
| L'ensemble des sauvegardes de données est-il également stocké en dehors du site de production (sauvegardes de secours) ?  | 0 |
| Procède-t-on régulièrement à des tests de relecture des sauvegardes de secours ? | 0 |

Nous n’avons jamais pensé à effectuer des sauvegardes en dehors du site de production. Nous proposons le plan suivant pour le faire : comme effectué une sauvegarde de secours à intervalle régulier en le stockant directement dans nos locaux et pas seulement sur le cloud. Après avoir fait ses sauvegardes, on surveille bien qu’elles effectuent leur rôle ainsi que la possibilité de les utiliser pour faire des restaurations.

Niveau de risque après le plan d’action



En mettant en place le plan d’action, on peut voir que les scénarios à gravité forte ont diminué. La plupart des scénarios sont passés à un niveau de gravité 2 qui peut être acceptable.