


Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

Suivi des modifications :

Version	Référence	Auteur	Date	Commentaires
A	DM_20221146_MCr	Crosnier Mathieu	20 nov. 2022	Création

Objet :


Création d'un serveur web et installation des logiciels présentés dans l'annexe C.

Diffusion :

BTS SIO - M.Watine

Table des matière

Objet :	1
Diffusion :	1
Table des matière	1
Plan PRA	2
Définition	2
Tableau Risques et menaces	2
Inondation	3
Incendie	4
Panne de courant/coupure d'électricité	5
Rançongiciel / Ransomware	6
Plan PCA	7
Définition	7
Tableau Risques et menaces	7
Mise à jour	8
Vol de données	9
Destruction et/ou panne de matériel	10
Vol de matériel	11

Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

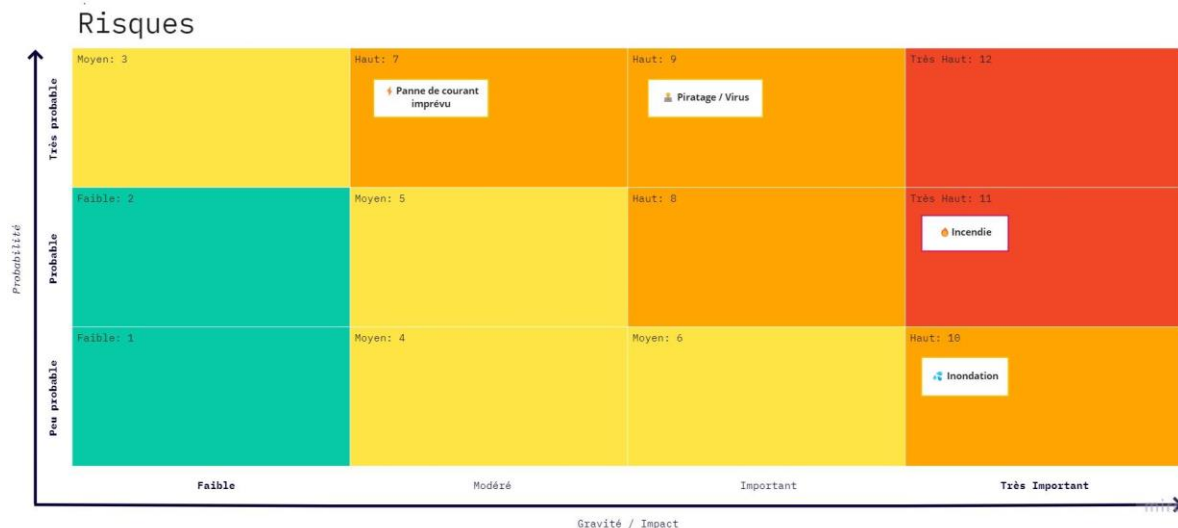
Plan PRA


Définition

Le plan PRA offre une aide en cas d'interruption totale, d'imprévu, d'une impossibilité de faire fonctionner du matériel ou de tout problème ne permettant pas la reprise des activités de l'entreprise. Le plan PRA doit permettre une reprise sans l'appareil défectueux et/ou d'un redémarrage rapide des systèmes informatiques de l'entreprise. Cependant, il est préférable d'éviter tout problème qui amènerait à une interruption totale des activités de l'entreprise à l'utilisation du plan PRA.

Tableau Risques et menaces

Le tableau ci-dessous définit la dangerosité d'un risque en fonction de son importance et de sa probabilité à arriver.



Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022


Inondation

Pour éviter de perdre le matériel informatique en cas d'inondation, il est préférable de ne pas installer les salles informatiques et les datacenters au rez-de-chaussée. Il est aussi souhaitable de ne pas les disposer sous des salles humides (ex: toilettes). En cas de risque d'inondation des étages au-dessus, il est possible d'isoler le plafond des salles informatiques.

Il est aussi recommandé d'utiliser un onduleur sur les serveurs et/ou matériel informatique importants au cas où l'inondation détruirait le réseau électrique du bâtiment. De plus, l'utilisation de sauvegarde des données à distance ou sur un disque dur externe est conseillée et préférable.

Liste des solutions à apporter afin d'éviter le pire en cas d'inondation :

1. Salle informatique en hauteur : à l'étage ou sur des pieds (ces derniers prévenant juste temporairement d'une inondation).
2. Plafond isolant en cas d'inondation par le haut : éviter les salles humides au-dessus des salles informatiques et des datacenters.
3. Utilisation d'onduleur en cas de coupure d'électricité liée à l'inondation.
4. Utilisation de sauvegarde à distance et/ou sur disque dur externe.


Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

Incendie

Mettre en place des alarmes incendies, des portes couvre-feux ainsi que des systèmes d'arrosage (hors salle serveur et machines). Avoir des installations électriques en norme et en bon état afin d'éviter tout risque d'incendie. Interdire de fumer ou autre activité pouvant provoquer un incendie.

Liste des solutions à apporter afin d'éviter le pire en cas d'incendie :

1. Installation de détecteurs de fumée afin de prévenir activement en cas d'incendie.
2. Système anti-incendie : système anti-incendie à réduction d'oxygène dans les salles informatiques.
3. Éviter le surplus de matériel informatique dans une seule et même zone.

Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

Panne de courant/coupure d'électricité


Afin d'éviter tout problème lié aux pannes de courant, il est possible d'utiliser des onduleurs pour prendre le relais du secteur en cas de coupures de courant, laissant ainsi aux personnels le temps de réagir et de sauvegarder leur travail en cours avant que les appareils ne s'éteignent. Un générateur de secours pour les serveurs les plus importants et préférables en cas d'une coupure de longue durée.

Liste des solutions à apporter afin d'éviter le pire en cas de coupure de courant :

1. Installation d'onduleurs dans les salles informatiques.
2. Changement de fournisseur d'électricité en cas de coupure répétée.
3. Installation d'un générateur de secours afin de contrer les coupures longues durées.

Ce qu'il faut faire en cas de coupure :

1. **Localiser la panne (locale ou générale) :**
Pour vérifier que la panne est locale, il faut vérifier le disjoncteur (au cas où celui-ci aurait sauté), sinon, vérifier l'éclairage des autres locaux/autres entreprises.
2. **En cas de panne locale :**
Appeler un électricien qui pourrait prendre en charge le problème dans les plus brefs délais.
3. **En cas de panne générale :**
Appeler le fournisseur d'électricité afin de trouver une solution à la panne de courant.

Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

Rançongiciel / Ransomware


Afin d'éviter tout problème dû à des ransomwares, il est important de sécuriser le plus possible son réseau et son code. Chaque faille de sécurité est une porte d'entrée aux pirates et aux ransomware.

Liste des solutions à apporter pour se protéger des ransomwares :

1. Faire de la prévention auprès des salariés (faux mails malveillants et mot de passe sécurisé).
2. Sécuriser le réseau informatique de l'entreprise.
3. Effectuer les conseils de la CNIL.
4. Effectuer les mises à jour régulièrement.
5. Se tenir au courant des failles de sécurité connues.

En cas de piratage et de ransomware :

1. Couper les routeurs.
2. Ne pas payer la rançon.
3. Porter plainte.
4. Créer un dossier conservant toutes les preuves (exemple : logs).
5. Notifier la CNIL en cas de violation des données à caractère personnel.
6. Identifier les failles de sécurité.
7. Réinitialiser les systèmes/appareils touchés par l'attaque.
8. Faire des analyses des systèmes pour détecter de potentiel backdoor.

Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

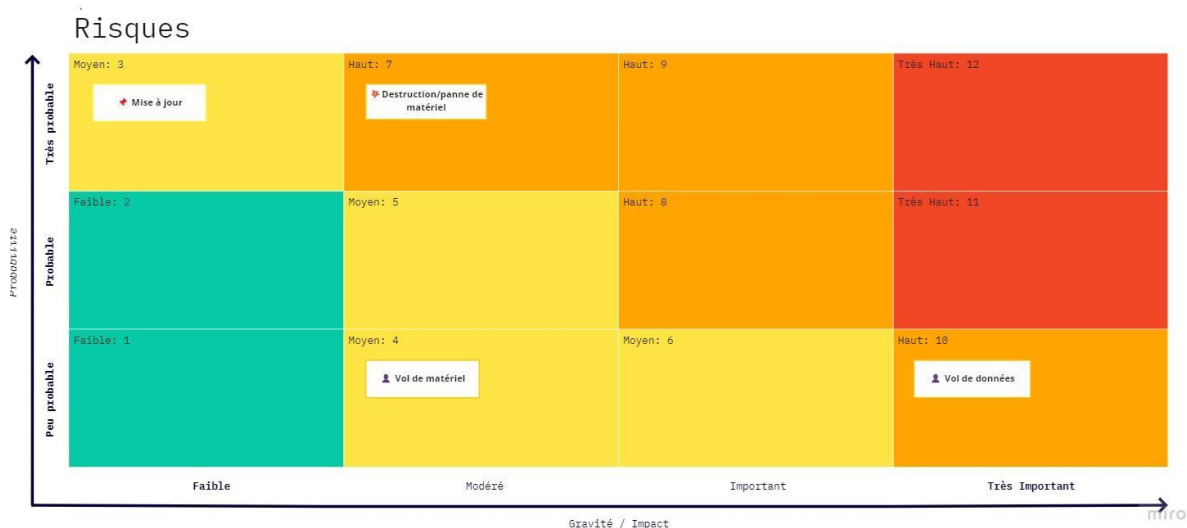
Plan PCA


Définition

Le plan PCA permet d'assurer la continuité des opérations en proposant des réponses/solutions à une panne donnée. Il aide les intervenants à identifier et à réparer les différents problèmes dans des moindres délais. Le plan PCA permet ainsi d'écourter ou d'empêcher tout arrêt d'activité de l'entreprise. En plus de tout cela, il est possible d'appliquer au plan PCA des directives à l'entretien du matériel et au remplacement des matériels obsolètes/âgés.

Tableau Risques et menaces

Le tableau ci-dessous définit la dangerosité d'un risque en fonction de son importance et de sa probabilité à arriver.



Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

Mise à jour


Afin de ne pas perdre du temps inutilement avec des mises à jour, il est conseillé de les faire en fin de journée, quand plus personne ne travaille sur les ordinateurs. Les mises à jours sont importantes pour le bon fonctionnement des logiciels mais aussi et surtout pour la protection des infrastructures et des clients.

Prévoir les mises à jour :

1. Utilisation des GPO pour programmer les mises à jour ;

En cas de mise à jour obligatoire :

1. Attendre que la mise à jour soit fini et ne pas éteindre les ordinateurs ;
2. Prévoir les prochaines mise à jour obligatoire en se renseignant (celle-ci étant souvent obligatoire car réparant un problème connu, et souvent grave) ;

Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

Vol de données


Veiller au respect de la Cnil au niveau de la programmation. Pensez à vérifier la protection des requêtes. Mettre en place des vérifications pour empêcher les injections SQL.
Sensibiliser le personnel à la cybersécurité.

Listes des solutions permettant d'éviter tout problème :

1. Envoyer des faux mails pour simuler un hameçonnage (phishing) pour sensibiliser le personnel de l'entreprise ;
2. Effectuer des réunions de sensibilisation du personnel ;
3. Éteindre les ordinateurs à la fin de la journée (ou quand les employés ne travail pas dessus) ;
4. Verrouiller les ordinateurs ;
5. Vérifier le code en appliquant des règles (DRY, clean code, etc...) afin d'éviter les erreurs et failles de sécurité.

En cas de vol :

1. Porter plainte ;
2. Recenser les données volées ;
3. Prévenir les principaux concernés (par exemple, prévenir les utilisateurs si leur mot de passe et leur vie privé est en danger) ;
4. En cas de rançon des données, ne pas céder à celle-ci ;

Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

Destruction et/ou panne de matériel


Système/disque de stockage qui lâche. Recenser toutes les pièces avec leur date d'utilisation et prévoir à partir d'une date des pièces de rechange. Toujours avoir des fonds et du matériel réservé pour ce genre de problème.

Anticiper/éviter le problème :

1. Prendre soin du matériel
2. Interdire la restauration dans les salles informatiques
3. Ne pas aller sur des sites malveillants
4. Avoir un stock de rechange

Solution en cas de panne matériel :

1. Changer le matériel dans les plus brefs délais.

Support et Mise à Disposition des services informatiques		
	Mon Epicerie	Version: A
	[SIO]_20221146_MCr_monEpicerie_Mission_6	20 nov. 2022

Vol de matériel

Le vol de matériel est peu probable, celui-ci reste néanmoins possible. Que ce soit de la part d'un employé ou d'un individu extérieur, l'entreprise se doit de sécuriser son matériel durant le temps de travail, mais aussi en dehors. Pour cela, nous pouvons utiliser la notion de moindre privilèges, ou chaque utilisateurs/salariés se voient attribués des accès selon ses capacités et son habilitation.

Afin d'éviter tout vols au sein de l'entreprise :

1. Mettre en place des câbles antivols sur le matériel important (principalement dans les salles sujet aux passages de beaucoup d'employés) ;
2. Protéger les serveurs et le stockage informatiques dans des locaux protégé par des cartes d'autorisation ou des badges ;

En cas de vol, il faut :

1. Trouver le responsable du vol et lui enlever les privilèges (si celui-ci en dispose) ;
2. Rechercher les diverses failles de sécurités utilisés pour s'introduire dans les salles/bâtiments ;