MODES DÉGRADÉS

1 2 3

Fiche pratique pour la mise en oeuvre de votre plan d'actions cyber dans votre collectivité.

Description rapide de l'objectif visé :

J'ai formalisé les opérations nécessaires à la reconstruction de mon système d'information (SI).

Coût estimé :

0 €

Niveau de difficulté de l'action :

Compliqué

Ressources nécessaires :

Ordinateur, logiciel bureautique

Niveau d'accompagnement :

Elevé

Temps estimé :

8 heures

Public visé pour l'action :

Responsable informatique
Personne en charge de l'informatique

Organisation conseillée pour la mise en œuvre dans votre collectivité :

1. Qui fait quoi ? Définir les rôles et responsabilités.
Qui formalise les opérations ?
Qui communique et explique la fiche aux agents concernés ?
Qui rend compte des actions menées pour la reconstruction du système d'information ?

2. Pourquoi ?
Afin de pouvoir reconstruire dans les meilleures conditions un système d'information.

3. Comment ?
Identifier en amont tous les éléments nécessaires à la bonne restauration des services.
Formaliser, sauvegarder et imprimer les éléments et procédures portant sur le système d'information et son infrastructure.

4. Combien ?
Prioriser le site principal puis prendre les éléments par ordre de criticité.

5. Quand ?
Dès que possible car une panne ou un logiciel malveillant ne peuvent pas être anticipés.

Livrable de l'action terminée :

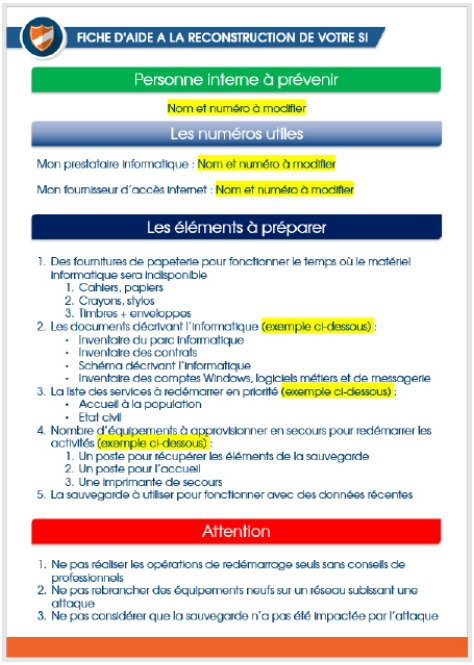
Fiches méthodes de la reconstruction du système d'information avec les procédures afférentes déjà produites.

Description étape par étape pour la mise en œuvre :

1. Noter les numéros des fournisseurs à contacter en cas de problème.
2. Identifier les personnes ayant les connaissances sur votre informatique en interne.
3. Recenser les documents déjà produits sur votre informatique.
4. Lister les éléments à redémarrer par priorité de besoin pour fonctionner et pour délivrer vos services.
5. Préparer une fiche méthode qui formalise les opérations nécessaires à la reprise de votre structure en cas d'incident.

Elle doit notamment reprendre les éléments précédents mais peut comprendre aussi :
- La gestion des approvisionnements en matériel de remplacement en précisant les délais ou la présence d'un stock tampon chez le fournisseur,
- La restauration d'une sauvegarde afin de reprendre avec des données récentes.

Attention : N'oublier pas de vous appuyer sur les documents existant pour approvisionner vos équipements si jamais ceux que vous avez ne peuvent pas être réutilisés sans risques.



FICHE D'AIDE A LA RECONSTRUCTION DE VOTRE SI

Personne interne à prévenir

Nom et numéro à modifier

Les numéros utiles

Mon prestataire informatique : Nom et numéro à modifier

Mon fournisseur d'accès internet : Nom et numéro à modifier

Les éléments à préparer

1. Des fournitures de papeterie pour fonctionner le temps où le matériel informatique sera indisponible
   1. Cahiers, papiers
   2. Crayons, stylos
   3. Timbres + enveloppes
2. Les documents décrivant l'informatique (exemple ci-dessous) :
   - Inventaire du parc informatique
   - Inventaire des contrats
   - Schéma décrivant l'informatique
   - Inventaire des comptes Windows, logiciels métiers et de messagerie
3. La liste des services à redémarrer en priorité (exemple ci-dessous) :
   - Accueil à la population
   - Etat civil
4. Nombre d'équipements à approvisionner en secours pour redémarrer les activités (exemple ci-dessous) :
   1. Un poste pour récupérer les éléments de la sauvegarde
   2. Un poste pour l'accueil
   3. Une imprimante de secours
5. La sauvegarde à utiliser pour fonctionner avec des données récentes

Attention

1. Ne pas réaliser les opérations de redémarrage seuls sans conseils de professionnels
2. Ne pas rebrancher des équipements neufs sur un réseau subissant une attaque
3. Ne pas considérer que la sauvegarde n'a pas été impactée par l'attaque

Pour aller plus loin :

ANSSI :
- Guide des bonnes pratiques de l'ANSSI
- Attaque par rançongiciels, tous concernés

Cybermalveillance :
- Fiche étapes clés et contacts
- Cyberattaque, fiche réflexe
- Diagnostic et assistance en ligne
- Contenus sur les rançongiciels