**Université Cheikh Anta Diop**

****

École Supérieure Polytechnique Département Génie Informatique

**Management Sécurité**

**Mini-projet 1 : PRI, PRA & PCA**

**Votre tâche consiste à rédiger trois plans : PRI, PRA et PCA de manière indépendante. Vous pouvez utiliser les ressources fournies dans ce laboratoire ou tout ce que vous trouverez en ligne. Cependant, votre plan doit se situer dans le domaine des soins de santé. L'hôpital Principal pourrait être un scénario dans votre plan**

*Date : 18/03/2024*

**s**

| **Prénom** | **Nom** | **Classe** |
| --- | --- | --- |
| *Ibrahima Diagne* | *Seck* | *M2 GLSI* |

# Partie I : Planification de la réponse aux incidents

**Plan de Réponse aux Incidents - Hôpital de Fann**

L’Hôpital de Fann, situé à Dakar, Sénégal, est un établissement hospitalier pionnier dans le domaine de la psychiatrie en Afrique subsaharienne. Voici un plan de réponse aux incidents spécifique à cet hôpital :

## Découverte de l’incident:

* + Toute personne découvrant un incident (qu’elle soit membre du département informatique ou non) doit immédiatement alerter le bureau de la sécurité des locaux.
  + Sources possibles de découverte d’incidents :

#### Helpdesk

#### Personnel de surveillance de la détection d’intrusion

#### Administrateur système

#### Administrateur de pare-feu

#### Partenaire commercial

#### Manager

#### Service de sécurité ou personne responsable de la sécurité

#### Source externe

* + Chaque source doit disposer d’une procédure de contact et d’une liste de contacts.

## Membre du département informatique ou du département affecté:

* + Si la personne découvrant l’incident est membre du département informatique ou du département concerné, elle doit passer à l’étape 5.

## Personne extérieure au département informatique:

* + Si la personne découvrant l’incident n’est pas membre du département informatique ou du département concerné, elle doit appeler le département de sécurité des locaux joignable 24/7 au numéro xxx-xxx.

## Enregistrement des détails :

* + Le bureau de sécurité des locaux consultera la liste de contacts d’urgence informatique ou la liste de contacts du département concerné.
  + Ils appelleront les numéros désignés dans l’ordre de la liste.
  + Le bureau de sécurité des locaux enregistrera les informations suivantes :

#### Le nom de l’appelant.

#### L’heure de l’appel.

#### Les informations de contact concernant l’appelant.

#### La nature de l’incident.

#### Quel équipement ou quelles personnes étaient impliquées ?

#### Lieu de l’équipement ou des personnes impliquées.

#### Comment l’incident a été détecté.

#### Quand l’événement a été remarqué pour la première fois, supportant l’idée que l’incident s’est produit.

## Contact du personnel informatique ou du département concerné :

* + Le membre du personnel informatique ou du département affecté qui reçoit l’appel (ou découvre l’incident) consultera sa liste de contacts.
  + Ils contacteront à la fois le personnel de direction à joindre et les membres de l’équipe de réponse aux incidents.
  + Le membre du personnel appellera ceux désignés sur la liste.
  + Ils contactent également le gestionnaire de réponse aux incidents en utilisant à la fois des e-mails et des messages téléphoniques.
  + Ils veilleront à ce que d’autres personnes appropriées et les gestionnaires désignés soient également contactés.
  + Le membre du personnel enregistrera les informations reçues dans le même format que le bureau de sécurité des locaux lors de l’étape précédente.
  + Ils pourraient éventuellement ajouter les éléments suivants :

#### L’équipement affecté est-il critique pour l’entreprise ?

#### Quelle est la gravité de l’impact potentiel ?

#### Nom du système ciblé, ainsi que système d’exploitation, adresse IP et emplacement.

#### Adresse IP et toute information sur l’origine de l’attaque.

## Réunion de l’équipe de réponse aux incidents :

* + Les membres de l’équipe de réponse contactés se réuniront ou discuteront de la situation par téléphone.
  + Ils déterminent une stratégie de réponse en répondant aux questions suivantes :

#### L’incident est-il réel ou perçu ?

#### L’incident est-il encore en cours ?

#### Quelles données ou biens sont menacés et quelle est leur importance ?

#### Quel est l’impact sur l’entreprise si l’attaque réussit ? Minimal, grave ou critique ?

#### Quel(s) système(s) sont ciblés, où sont-ils physiquement situés et sur le réseau ?

#### L’incident est-il à l’intérieur du réseau de confiance ?

#### La réponse est-elle urgente ?

#### L’incident peut-il être rapidement contenu ?

#### La réponse alertera-t-elle l’attaquant et cela nous importe-t-il ?

#### Quel type d’incident est-ce ? Exemple : virus, ver, intrusion, abus, dommage.

## Création d’un ticket d’incident :

* + Un ticket d’incident sera créé pour documenter l’ensemble du processus.
  + L’incident sera classé dans la catégorie la plus applicable parmi les suivantes :

#### **Catégorie un** : Une menace pour la sécurité publique ou la vie.

#### **Catégorie deux** : Une menace pour les données sensibles.

#### **Catégorie trois** : Une menace pour les systèmes informatiques.

#### **Catégorie quatre** : Une perturbation des services.

## Choix de la procédure appropriée :

* + Les membres de l’équipe établiront et suivront l’une des procédures suivantes en fonction de l’évaluation de l’incident :

### a) Procédure de réponse aux vers.

### b) Procédure de réponse aux virus.

### c) Procédure de panne du système.

### d) Procédure de réponse aux intrusions actives : Ils évalueront si des données critiques sont en danger.

### e) Procédure de réponse aux intrusions inactives.

### f) Procédure de réponse à l’abus du système.

### g) Procédure de réponse au vol de propriété.

### h) Procédure de réponse aux attaques par déni de service sur le site Web.

### i) Procédure de réponse aux attaques par déni de service sur la base de données ou les fichiers.

### j) Procédure de réponse aux logiciels espions.

* + L’équipe peut également créer des procédures supplémentaires non prévues dans ce document. Si aucune procédure applicable n’existe, l’équipe doit documenter ce qui a été fait et établir ultérieurement une procédure pour l’incident.

## Techniques d’investigation :

* + Les membres de l’équipe utilisent des techniques d’investigation, notamment :

#### L’examen des journaux système.

#### La recherche de lacunes dans les journaux.

#### L’examen des journaux de détection d’intrusion.

#### L’interrogation des témoins et de la victime de l’incident pour déterminer comment l’incident s’est produit.

* + Seul le personnel autorisé devrait mener des entretiens ou examiner des preuves, et le personnel autorisé peut varier selon la situation et l’organisation.

## Recommandations pour prévenir les récidives :

* + Les membres de l’équipe recommandent des changements pour empêcher que l’incident ne se reproduise ou n’infecte d’autres systèmes. Ces recommandations peuvent inclure :

#### Mises à jour de sécurité régulières.

#### Renforcement des politiques de sécurité.

#### Formation du personnel sur les meilleures pratiques en matière de sécurité informatique.

#### Amélioration de la surveillance des systèmes.

#### Révision des procédures d’accès et d’authentification.

## Mise en œuvre des changements :

* + Après l’approbation de la direction, les changements recommandés seront mis en œuvre. Cela peut inclure des ajustements dans les configurations, des correctifs logiciels, des modifications de processus, etc.

## Restauration des systèmes affectés :

* + Les membres de l’équipe restaurent le(s) système(s) affecté(s) à l’état non infecté. Ils peuvent effectuer l’une ou plusieurs des actions suivantes :

### a) Réinstallation à partir de zéro et restauration des données : Si nécessaire, ils réinstallent le(s) système(s) affecté(s) à partir de zéro et restaurent les données à partir de sauvegardes. Ils veilleront à préserver les preuves avant de le faire.

### b) Changement des mots de passe des utilisateurs : Si les mots de passe ont pu être interceptés, ils feront changer les mots de passe des utilisateurs concernés.

### c) Sécurisation du système : Ils s’assureront que le système est sécurisé en désactivant ou désinstallant les services inutilisés.

### d) Application des correctifs : Ils veilleront à ce que le système soit entièrement patché.

### e) Vérification de la protection antivirus et de la détection d’intrusion : Ils s’assureront que la protection antivirus en temps réel et la détection d’intrusion fonctionnent correctement.

### f) Configuration des journaux d’événements : Ils veilleront à ce que le système enregistre les événements corrects et au bon niveau.

## Documentation :

* + Les éléments suivants doivent être documentés :

### a) Comment l’incident a été découvert.

### b) La catégorie de l’incident.

### c) Comment l’incident s’est produit (par e-mail, pare-feu, etc.).

### d) D’où venait l’attaque (adresses IP et autres informations sur l’attaquant).

### e) Quel était le plan de réponse ?

### f) Qu’a-t-on fait en réponse ?

### g) L’efficacité de la réponse.

## Conservation des preuves :

* + Faites des copies des journaux, des e-mails et autres communications.
  + Gardez une liste des témoins.
  + Conservez les preuves aussi longtemps que nécessaire pour mener à bien des poursuites et au-delà en cas d’appel.

## Notification des agences externes appropriées :

* + Informez la police et d’autres organismes appropriés si la poursuite de l’intrus est possible.
  + Indiquez ici les organismes et les numéros de contact.

## Évaluation des dommages et des coûts :

* + Évaluez les dommages causés à l’organisation.
  + Estimez à la fois le coût des dommages et le coût des efforts de confinement.

## **Révision de la réponse et mise à jour des politiques** :

* + Planifiez et prenez des mesures préventives pour que l’intrusion ne se reproduise pas.
  + Voici les étapes à suivre :

**a) Évaluation des politiques existantes** :

#### Déterminez si une politique supplémentaire aurait pu empêcher l’intrusion.

**b) Analyse des procédures et des politiques** :

#### Déterminez si une procédure ou une politique n’a pas été suivie, ce qui a permis l’intrusion.

#### Envisagez ce qui pourrait être changé pour garantir que la procédure ou la politique soit suivie à l’avenir.

**c) Évaluation de la réponse à l’incident** :

#### Était-elle appropriée ?

#### Comment pourrait-elle être améliorée ?

**d) Communication en temps voulu** :

#### Vérifiez que chaque partie appropriée a été informée en temps voulu.

**e) Amélioration des procédures de réponse** :

#### Les procédures de réponse à l’incident étaient-elles détaillées et couvraient-elles l’ensemble de la situation ?

#### Comment peuvent-elles être améliorées ?

**f) Mise en place de mesures préventives** :

#### Des changements ont-ils été apportés pour éviter une nouvelle infection ?

#### Tous les systèmes ont-ils été patchés, les systèmes verrouillés, les mots de passe changés, l’antivirus mis à jour, les politiques de messagerie configurées, etc. ?

**g) Prévention des récidives** :

#### Des changements ont-ils été apportés pour éviter une nouvelle infection similaire ?

**h) Mise à jour des politiques de sécurité** :

#### Des politiques de sécurité doivent-elles être mises à jour ?

**i) Apprentissage des leçons** :

#### Quelles leçons ont été apprises de cette expérience ?

# Partie II : Planification de la reprise après sinistre

Un plan de reprise après sinistre (PRS) est essentiel pour garantir la continuité des opérations et protéger l’infrastructure informatique d’une organisation en cas de sinistre. Voici les étapes pour élaborer un plan de reprise après sinistre dans le domaine de la santé :

1. Définir le contexte et le périmètre :
   * Identifier les services informatiques essentiels pour les soins de santé.
   * Cartographier les processus opérationnels.
2. Identifier les objectifs et activités essentielles :
   * Déterminer les processus critiques pour la continuité des soins.
   * Formaliser les besoins du processus.
3. Mesurer les conséquences d’une interruption d’activité :
   * Évaluer l’impact sur les patients, le personnel et les opérations.
4. Définir les ressources nécessaires du PRS :
   * Identifier les équipements critiques (matériel, logiciels, données).
   * Prévoir des alternatives en cas de défaillance.
5. Tester et réviser :
   * Effectuer des exercices de simulation pour valider le plan.
   * Mettre à jour régulièrement le PRS en fonction des changements.

# Partie III : Plan de continuité des activités

Le processus de Planification de la Continuité des Activités (PCA) est essentiel pour garantir la résilience d’une organisation et sa capacité à maintenir ses fonctions vitales en cas de perturbations majeures. Voici les étapes clés pour élaborer un PCA dans le domaine de la santé :

## Initialisation du Projet :

* + Définir les objectifs de la continuité des activités et la portée de la couverture.
  + Mettre en place un Comité de Direction de la Continuité des Activités.
  + Établir des politiques de continuité des activités.

## Analyse des Activités :

* + Effectuer une analyse des risques et une analyse de l’impact sur les activités.
  + Envisager des stratégies alternatives de continuité des activités.
  + Réaliser une analyse coûts-avantages et sélectionner une stratégie.

## Conception et Développement (Conception du Plan) :

* + Constituer une équipe de reprise d’activité et attribuer des responsabilités aux membres.
  + Identifier la structure du plan et les principaux composants.
  + Développer des stratégies de sauvegarde et de récupération.
  + Élaborer des scénarios pour exécuter le plan.

## Mise en Œuvre (Création du Plan) :

* + Préparer les procédures d’intervention d’urgence.
  + Préparer les procédures d’activation du centre de commandement.
  + Préparer les procédures détaillées de récupération.
  + Préparer les contrats avec les fournisseurs et l’achat de ressources de récupération.

## Test :

* + Exécuter le plan sur la base du scénario sélectionné.
  + Produire un rapport de test et évaluer les résultats.
  + Fournir une formation et une sensibilisation à tout le personnel.

## Maintenance (Mise à jour du Plan) :

* + Examiner régulièrement le plan.
  + Mettre à jour le plan avec les changements ou améliorations.
  + Distribuer le plan aux membres de l’équipe de récupération.

Quelques considérations supplémentaires :

Voici quelques considérations supplémentaires pour élaborer un Plan de Continuité d'Activités (PCA) dans le domaine de la santé :

#### Exigences légales :

* + Outre l’analyse des activités, il est crucial de prendre en compte les exigences légales spécifiques au secteur de la santé. Ces réglementations peuvent influencer les décisions concernant la continuité des activités.

#### Tests réguliers :

* + Planifiez des exercices de simulation réguliers pour tester le PCA. Cela garantit que le personnel est préparé et permet d’identifier les éventuelles faiblesses.

#### Responsabilité du coordinateur :

* + Le coordinateur de la continuité des activités doit assurer la maintenance du plan et veiller à sa distribution aux propriétaires de documents.

#### Ressources et outils :

* + Des logiciels commerciaux et des outils sont disponibles pour faciliter le développement du PCA.
  + Des ressources en ligne telles que DRI International, Disaster Recovery Journal et The Business Continuity Institute offrent des conseils, des formations et des modèles de planification.

# 