PRA-PRASN

(Valentin RYCKAERT, Louis BRUNET-LECOMTE, Lucas POURRERON)

Contexte

Une architecture est mise en place :

- BATIMENT A :
  - client windows 11
  - AD windows server
- BATIMENT B :
  - serveur web Fedora Server hébergeant une stack docker WordPress / MariaDB
  - RODC de l'AD
  - client windows 11

Roles dans l'entreprise :

- 1 développeur (Valentin)
- 2 administrateurs systèmes (Lucas, Louis)

Scénario 1 : Panne réseau totale

PRA (Plan de Reprise d'Activité)

Titre	Action	Responsable	Durée estimée
Détection de la panne	Un administrateur système détecte la panne réseau totale.	Lucas ou Louis	5 minutes
Identification de la cause	Vérification des connexions réseau physiques et des configurations VLAN.	Lucas ou Louis	10 minutes
Reconnexion des cartes réseau	Reconnecter toutes les cartes réseau des machines du bâtiment affecté.	Lucas ou Louis	20 minutes
Restauration des configurations VLAN	Remettre les configurations VLAN initiales pour chaque carte réseau.	Lucas ou Louis	15 minutes
Vérification du réseau	Tester la connectivité réseau sur toutes les machines.	Lucas ou Louis	10 minutes
Redémarrage des services	Redémarrer les services réseau (DHCP, DNS, etc.).	Lucas ou Louis	10 minutes

PRASN (Plan de Retour à une Situation Normale)

Titre	Action	Responsable	Durée estimée
Validation de la reprise	Vérifier que toutes les machines sont opérationnelles et connectées au réseau.	Lucas ou Louis	15 minutes
Documentation des actions	Documenter toutes les actions effectuées et les résultats obtenus.	Lucas ou Louis	10 minutes
Rapport final	Rédiger un rapport détaillé pour la direction.	Lucas ou Louis	20 minutes

Scénario 2 : Intrusion AD (Active Directory)

PRA (Plan de Reprise d'Activité)

Titre	Action	Responsable	Durée estimée
Détection de l'intrusion	Un administrateur système détecte une intrusion dans l'AD.	Lucas ou Louis	5 minutes
Isolation de l'AD	Déconnecter l'AD du réseau pour éviter toute propagation.	Lucas ou Louis	10 minutes
Restauration des mots de passe	Restaurer les mots de passe des comptes utilisateurs	Lucas ou Louis	20 minutes
Vérification des comptes	Vérifier que tous les comptes sont accessibles et fonctionnels.	Lucas ou Louis	15 minutes
Reconnexion de l'AD	Reconnecter l'AD au réseau.	Lucas ou Louis	10 minutes

PRASN (Plan de Retour à une Situation Normale)

Titre	Action	Responsable	Durée estimée
Validation de la reprise	Vérifier que l'AD fonctionne normalement et que tous les comptes sont sécurisés.	Lucas ou Louis	15 minutes
Documentation des actions	Documenter toutes les actions effectuées et les résultats obtenus.	Lucas ou Louis	10 minutes
Rapport final	Rédiger un rapport détaillé pour la direction.	Lucas ou Louis	20 minutes

Scénario 3 : Coupure d'alimentation

PRA (Plan de Reprise d'Activité)

Titre	Action	Responsable	Durée estimée
Détection de la coupure	Un administrateur système détecte une coupure d'alimentation totale.	Lucas ou Louis	5 minutes
Redémarrage des machines	Redémarrer toutes les machines du bâtiment affecté (Bâtiment A ou B).	Lucas ou Louis	20 minutes
Vérification des services	Vérifier que tous les services critiques (AD, serveur web, etc.) sont opérationnels.	Lucas ou Louis	15 minutes
Restauration des données	Restaurer les données à partir des sauvegardes si nécessaire.	Lucas ou Louis	30 minutes
Tests de fonctionnalité	Effectuer des tests pour s'assurer que toutes les applications fonctionnent correctement.	Valentin	20 minutes

PRASN (Plan de Retour à une Situation Normale)

Titre	Action	Responsable	Durée estimée
Validation de la reprise	Vérifier que toutes les machines et services sont opérationnels.	Lucas ou Louis	15 minutes
Documentation des actions	Documenter toutes les actions effectuées et les résultats obtenus.	Lucas ou Louis	10 minutes
Rapport final	Rédiger un rapport détaillé pour la direction.	Lucas ou Louis	20 minutes

Scénario 4 : Panne sauvegarde

PRA (Plan de Reprise d'Activité)

Titre	Action	Responsable	Durée estimée
Détection de la panne	Un administrateur système détecte que les sauvegardes sont inopérantes.	Lucas ou Louis	5 minutes
Identification de la cause	Vérifier les configurations réseau, les ports, et les règles de pare-feu affectant le processus de sauvegarde.	Lucas ou Louis	15 minutes

Titre	Action	Responsable	Durée estimée
Restauration des configurations	Remettre les configurations réseau (IP, ports, DNS) à leurs valeurs initiales.	Lucas ou Louis	20 minutes
Redémarrage du processus de sauvegarde	Relancer le processus de sauvegarde et vérifier son bon fonctionnement.	Lucas ou Louis	15 minutes
Vérification des sauvegardes	Effectuer une sauvegarde complète pour s'assurer que le processus fonctionne correctement.	Lucas ou Louis	30 minutes

PRASN (Plan de Retour à une Situation Normale)

Titre	Action	Responsable	Durée estimée
Validation de la reprise	Vérifier que les sauvegardes sont complètes et opérationnelles.	Lucas ou Louis	15 minutes
Documentation des actions	Documenter toutes les actions effectuées et les résultats obtenus.	Lucas ou Louis	10 minutes
Rapport final	Rédiger un rapport détaillé pour la direction.	Lucas ou Louis	20 minutes

Scénario 5 : Crash du service Web

PRA (Plan de Reprise d'Activité)

Titre	Action	Responsable	Durée estimée
Détection du crash	Un administrateur système détecte que le service web est en panne.	Lucas ou Louis	5 minutes
Identification de la cause	Vérifier les fichiers de configuration modifiés (httpd, .cnf, certificats, etc.).	Lucas ou Louis	10 minutes
Restauration des fichiers de configuration	Restaurer les fichiers de configuration à partir des sauvegardes.	Lucas ou Louis	15 minutes
Redémarrage du service web	Redémarrer le service web (Apache, Nginx, Docker).	Lucas ou Louis	10 minutes
Vérification du service	Tester le service web pour s'assurer qu'il fonctionne correctement.	Valentin	15 minutes
Restauration des fichiers de log	Restaurer les fichiers de log à partir des sauvegardes.	Lucas ou Louis	10 minutes

PRASN (Plan de Retour à une Situation Normale)

Titre	Action	Responsable	Durée estimée
Validation de la reprise	Vérifier que le service web fonctionne normalement.	Lucas ou Louis	15 minutes
Documentation des actions	Documenter toutes les actions effectuées et les résultats obtenus.	Lucas ou Louis	10 minutes
Rapport final	Rédiger un rapport détaillé pour la direction.	Lucas ou Louis	20 minutes

Scénario 6 : Base de données compromise

PRA (Plan de Reprise d'Activité)

Titre	Action	Responsable	Durée estimée
Détection de la compromission	Un administrateur système détecte que la base de données est compromise.	Lucas ou Louis	5 minutes
Isolation de la base de données	Déconnecter la base de données du réseau pour éviter toute propagation.	Lucas ou Louis	10 minutes
Restauration de la base de données	Restaurer la base de données à partir de la dernière sauvegarde valide.	Lucas ou Louis	20 minutes
Vérification de l'intégrité des données	Vérifier que toutes les données sont intactes et cohérentes.	Lucas ou Louis	15 minutes
Reconnexion de la base de données	Reconnecter la base de données au réseau.	Lucas ou Louis	10 minutes
Surveillance post-compromission	Surveiller la base de données pour détecter toute activité suspecte.	Lucas ou Louis	30 minutes

PRASN (Plan de Retour à une Situation Normale)

Titre	Action	Responsable	Durée estimée
Validation de la reprise	Vérifier que la base de données fonctionne normalement et que toutes les données sont sécurisées.	Lucas ou Louis	15 minutes
Documentation des actions	Documenter toutes les actions effectuées et les résultats obtenus.	Lucas ou Louis	10 minutes

Titre	Action	Responsable	Durée estimée
Rapport final	Rédiger un rapport détaillé pour la direction.	Lucas ou Louis	20 minutes

Scénario 7 : Version logicielle non fonctionnelle

PRA (Plan de Reprise d'Activité)

Titre	Action	Responsable	Durée estimée
Détection de la panne logicielle	Un administrateur système ou le développeur détecte que l'application est inopérante.	Lucas, Louis, ou Valentin	5 minutes
Identification des modifications	Identifier les modifications apportées au code source.	Valentin	15 minutes
Restauration du code source	Restaurer le code source à partir de la dernière version stable.	Valentin	20 minutes
Recompilation et redéploiement	Recompiler et redéployer l'application.	Valentin	20 minutes
Tests de fonctionnalité	Effectuer des tests pour s'assurer que l'application fonctionne correctement.	Valentin	20 minutes

PRASN (Plan de Retour à une Situation Normale)

Titre	Action	Responsable	Durée estimée
Validation de la reprise	Vérifier que l'application fonctionne normalement.	Valentin	15 minutes
Documentation des actions	Documenter toutes les actions effectuées et les résultats obtenus.	Valentin	10 minutes
Rapport final	Rédiger un rapport détaillé pour la direction.	Valentin	20 minutes

Scénario 8 : Attaque ransomware

PRA (Plan de Reprise d'Activité)

Titre	Action	Responsable	Durée estimée
Détection de l'attaque	Un administrateur système détecte une attaque ransomware.	Lucas ou Louis	5 minutes
Isolation des systèmes affectés	Déconnecter les systèmes affectés du réseau pour éviter toute propagation.	Lucas ou Louis	10 minutes
Restauration des systèmes	Restaurer les systèmes à partir des sauvegardes non infectées.	Lucas ou Louis	30 minutes
Vérification des systèmes	Vérifier que tous les systèmes sont opérationnels et exempts de malware.	Lucas ou Louis	20 minutes
Reconnexion des systèmes	Reconnecter les systèmes au réseau.	Lucas ou Louis	10 minutes
Surveillance post-attaque	Surveiller les systèmes pour détecter toute activité suspecte.	Lucas ou Louis	30 minutes

PRASN (Plan de Retour à une Situation Normale)

Titre	Action	Responsable	Durée estimée
Validation de la reprise	Vérifier que tous les systèmes fonctionnent normalement.	Lucas ou Louis	15 minutes
Documentation des actions	Documenter toutes les actions effectuées et les résultats obtenus.	Lucas ou Louis	10 minutes
Rapport final	Rédiger un rapport détaillé pour la direction.	Lucas ou Louis	20 minutes

Scénario 9 : Inondation affectant les locaux

PRA (Plan de Reprise d'Activité)

Titre	Action	Responsable	Durée estimée
Détection de l'inondation	Un administrateur système détecte l'inondation affectant les locaux.	Lucas ou Louis	5 minutes
Arrêt progressif des machines	Éteindre progressivement toutes les machines du bâtiment affecté pour éviter les dommages matériels.	Lucas ou Louis	60 minutes
Évaluation des dommages	Évaluer les dommages matériels et identifier les machines affectées.	Lucas ou Louis	20 minutes

Titre	Action	Responsable	Durée estimée
Remplacement des composants endommagés	Remplacer les composants matériels endommagés par des neufs ou des pièces de rechange.	Lucas ou Louis	40 minutes
Redémarrage des machines	Redémarrer les machines et vérifier leur fonctionnement.	Lucas ou Louis	20 minutes
Tests de fonctionnalité	Effectuer des tests pour s'assurer que toutes les machines fonctionnent correctement.	Lucas ou Louis	20 minutes

PRASN (Plan de Retour à une Situation Normale)

Titre	Action	Responsable	Durée estimée
Validation de la reprise	Vérifier que toutes les machines et services sont opérationnels.	Lucas ou Louis	15 minutes
Documentation des actions	Documenter toutes les actions effectuées et les résultats obtenus.	Lucas ou Louis	10 minutes
Rapport final	Rédiger un rapport détaillé pour la direction.	Lucas ou Louis	20 minutes

Si vous avez besoin d'autres informations ou d'une présentation différente, faites-le moi savoir !