Principes du retour-arrière suite à sinistre ou cyberattaque

Architecture solution de PRA · https://preview.nuabee.fr/documents/principes-du-retour-arriere-suite-a-sinistre-ou-cyberattaque/

Après un incident majeur ou une cyberattaque, la restauration du système d'information (SI) est une étape importante. La solution Nuabee propose plusieurs approches pour organiser le retour-arrière, adaptées à la nature de l'incident et aux contraintes techniques du client.

Récupération des disques : des options adaptées à chaque besoin

Depuis le cloud : rapidité et sécurité

- **Post-restauration des machines**
  - **Remédiation validée** : Après une cyberattaque, les machines sont restaurées dans un environnement isolé. Cette étape permet de valider la sécurité du système avant toute réintégration, afin d'éviter la réinfection ou la propagation de menaces.
  - **Activation du PRA** : Une fois la remédiation validée, le Plan de Reprise d'Activité (PRA) est déclenché pour redémarrer rapidement les services critiques et minimiser l'impact métier.
- **Mise à disposition des disques**
  - Nuabee dispose d'outillages pour générer des disques accessibles au format VMDK (VMware) ou VHDX (Hyper-V) via un lien S3 sécurisé.
  - Le client récupère ainsi ses disques en toute autonomie et rapidité, sans dépendre de ressources externes.

Depuis un NAS : flexibilité pour les gros volumes

- **Bande passante WAN limitée ou gros volumes de données**

- **Envoi d’un (ou plusieurs) NAS SSD préconfiguré** : Lorsque la connexion internet est insuffisante, Nuabee expédie un NAS SSD contenant les disques décrits ci-avant, prêt à l’emploi.
- **Transport sécurisé** : Le NAS est envoyé par transporteur spécialisé, puis récupéré par le client. Les données restent chiffrées tout au long du processus, garantissant la confidentialité et l’intégrité des informations.
- **Idéal pour le retour-arrière ou le chargement initial** : Cette méthode est particulièrement adaptée pour le retour-arrière après sinistre ou pour la migration de grandes quantités de données.

Reconstruction du système d’information : une reprise orchestrée

Séquencer et organiser la reprise

Nuabee est alignée avec les recommandations de l’ANSSI en pratiquant le principe de E3R : Endiguement, Éviction, Éradication, Reconstruction, **en participant activement aux étapes d’Éviction et de Reconstruction.**

- **Séquence de démarrage** : La console Atlas de Nuabee facilite la gestion de cette séquence, permettant une reprise progressive et maîtrisée des activités. Elle permet de consolider les informations nécessaires à la reprise dont l’ordonnancement de démarrage précis, tenant compte des dépendances entre serveurs et services critiques.
- **Planification rigoureuse** : Chaque étape est planifiée pour garantir la cohérence du SI et la sécurité des données, en évitant tout risque de corruption ou de perte d’information.

Restauration depuis l’agent Nuabee : simplicité et efficacité

Récupération locale du disque virtuel

- **Intégration directe dans l’hyperviseur** : Les disques sont restaurés localement, sans passer par les mécanismes Nuabee, pour une remise en service rapide des machines virtuelles (uniquement disponible sur VMware ESXi).
- **Restauration au niveau dossier/fichier** : Pour des besoins spécifiques, il est possible de restaurer uniquement certains dossiers ou fichiers à partir du disque virtuel, via l’agent

Nuabee.

Import du disque dans l’hyperviseur : documentation complète

- **Procédure détaillée** : Nuabee met à disposition une documentation complète pour guider l’importation des disques VMDK dans VMware ESXi, facilitant ainsi l’intégration fluide et sécurisée des machines virtuelles [1].

Mode PRA partiel : adaptabilité maximale

- **Retour-arrière partiel** : Selon la topologie réseau et les priorités métiers, le retour-arrière peut être réalisé de façon partielle. Cette approche permet de redémarrer progressivement les services critiques, tout en limitant l’impact sur le réseau et les utilisateurs.

Conclusion

- **Organisation du retour-arrière** : Après la restauration des machines dans le Cloud et la validation de la sécurité, le client organise le retour à la situation nominale, en collaboration avec ses équipes de sécurité.
- **Accompagnement Nuabee** : Les équipes Nuabee restent disponibles pour accompagner le client tout au long du processus, de la restauration à la remise en service complète du SI, garantissant ainsi une transition fluide et sécurisée.

Nuabee propose des solutions de retour-arrière flexibles, sécurisées et parfaitement alignées avec la séquence E3R de l’ANSSI.

Que la restauration s’effectue depuis le cloud, un NAS ou en local, le client bénéficie d’un accompagnement complet et d’outils performants pour garantir la résilience de son système d’information.

Avec Nuabee, la reprise d’activité après un sinistre ou une cyberattaque devient un processus maîtrisé, rapide et fiable.