Cyber résilience : PCA et PRA

Qu’est-ce que la résilience cyber ?

La résilience cyber peut être définie comme la capacité d'une organisation à répondre rapidement et efficacement aux menaces cyber, et à se rétablir promptement après un incident majeur affectant son SI. Pour ce faire, deux éléments clés sont nécessaires : L'existence d’un **plan de continuité des activités (PCA)** et d’un **plan de reprise d'activité (PRA)** qui soient efficaces.

Quels sont les éléments clés d’un PCA ?

La mise en place d'un PCA implique plusieurs étapes essentielles pour garantir la préparation d'une organisation à faire face à des incidents. Voici les étapes clés pour son élaboration :

Évaluation des risques

- Déterminer les actifs informatiques et les données essentielles à la continuité des opérations.
- Évaluer les menaces potentielles (piratage, ransomwares, perte de données, etc.) et les vulnérabilités existantes dans le SI.

Développement d'un plan d'action

- Créer un plan clair détaillant la manière de réagir en cas d'incident, y compris les étapes à suivre, les responsabilités des membres de l'équipe et les procédures de communication.

Collaboration et communication

- Définir des protocoles pour coordonner les actions entre les équipes lorsqu'un incident survient. Par exemple, qui est responsable de quelles actions, comment se déroule la remontée d'information, etc**.**

Tests et mise à jour du PCA

- Réaliser des tests réguliers pour évaluer l'efficacité du PCA et identifier les lacunes.
- Revoir et mettre à jour régulièrement le PCA en fonction des nouvelles menaces, des évolutions technologiques et des changements dans l'organisation.

Quels sont les éléments clés d’un PRA ?

L’élaboration d’un PRA est cruciale pour assurer la reprise rapide des activités, en cas d'incidents ou de situations imprévues. Ci-après sont énumérées quelques étapes essentielles pour sa mise en place :

Identification des processus critiques

- Identifier et prioriser les processus métier critiques qui doivent être restaurés en priorité pour éviter l’interruption des activités.

Stratégies de sauvegarde et de restauration

- Elaborer des stratégies de sauvegarde conformes à la règle 3-2-1 : trois copies des données (originale et deux sauvegardes) sur deux supports distincts, dont une copie hors site.
- Concevoir des procédures de reprise pour restaurer rapidement les opérations critiques après un événement.

Elaboration de solutions de secours

- Identifier des alternatives ou des solutions de secours pour chaque ressource critique. Cela peut inclure des sauvegardes régulières, l'utilisation de fournisseurs de secours ou la mise en place de systèmes redondants.

Tests et mise à jour du PRA

- Testez régulièrement le plan de reprise pour vérifier son efficacité et sa capacité à restaurer les opérations rapidement.
- Évaluez les résultats des tests et apportez les ajustements nécessaires pour améliorer le PRA.

Ressources mises à disposition

- Un guide pratique de la continuité d’activités issus de la PGSSI-S [PDF]
- Un modèle de PCA fourni par l’**ENISA** [PDF]
- Un modèle pour l’identification des actifs fourni par l’**ENISA** [PDF]
- Un ensemble de directives, pour garantir la résilience, issues du **NIST** [PDF]