Cyberattaque et résilience grâce à Nuabee

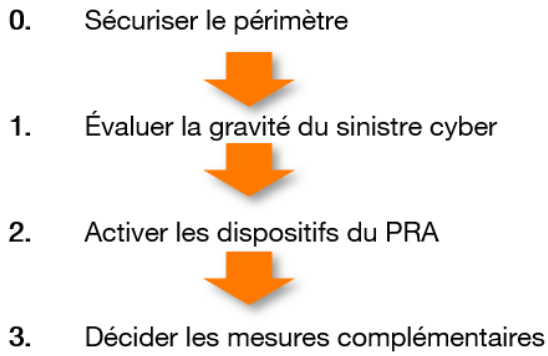
Cyber-Résilience by Nuabee · https://preview.nuabee.fr/documents/cyberattaque-resilience-pra-nuabee/

La spécificité des cyberattaques

En comparaison à d'autres scénarios de crise, les crises cyber ont des caractéristiques propres qu'il est important d'appréhender :

- Une double temporalité, avec des impacts immédiats et une remédiation longue pouvant s'étendre sur plusieurs semaines, voire plusieurs mois ;
- Une incertitude concernant le périmètre de la compromission ;
- Une absence d'unicité de lieu de réalisation, qui sous-entend une potentielle propagation à d'autres organisations/entreprises en raison de l'interconnexion des SI ;
- Une menace pouvant s'adapter aux mesures d'endiguement et de remédiation ;
- Une complexité pour comprendre les objectifs de l'attaquant et attribuer l'origine de l'attaque.

(extraits de documents de l'ANSSI)



En comparaison à d'autres scénarios de crise pouvant nécessiter l'activation d'un PRA, les crises cyber ont des caractéristiques propres :

- Des impacts immédiats (arrêt de certaines activités, impossibilité de délivrer des services, ...).
- Des incertitudes concernant le périmètre de la compromission.
- De la complexité pour décider ce qu'il est possible de redémarrer ou non en mode PRA, et dans quel ordre, cela étant lié :

- Au vecteur de l’attaque : est-ce un vers, un ransomware commandé de l’extérieur, …
- À une potentielle propagation à d’autres organisations en raison de l’interconnexion des SI.

> Dans les premières heures, il peut être difficile de distinguer un incident IT d’un incident cyber.
> Les équipes techniques doivent tenter de détecter les signaux faibles pour couper si nécessaire les systèmes.

Etape 0 : sécuriser le périmètre

Liste des actions à mener	Détail des actions	Responsables de mise en œuvre	Outils et documents disponibles
Isoler les périmètres touchés et sécuriser les périmètres pas encore impactés	Il s’agit d’activer des mécanismes d’isolation des environnements / VM / réseaux.	RSSI+ Responsable Informatique	Procédures techniques + fiches réflexes
Décider de couper les réseaux WAN & LAN	Il s’agit de décider de couper les réseaux : • Accès Internet • VPN IPsec / SSL • Wifi / Bluetooth Endpoint …	Equipe Informatique Client + Prestataires télécoms	Procédures techniques Clients
Mobiliser les prestataires habituels techniques externes	Il s’agit de mobiliser les acteurs externes qui pourront être nécessaires pour diagnostiquer les incidents, signaux, ….	Responsable Informatique + Equipe Informatique	Liste externalisée des coordonnées des prestataires
Mettre en astreinte les équipes Nuabee	Même avant de savoir s’il faut basculer en mode secours, il faut mettre en astreinte les équipes Nuabee**.** Il peut être décidé d’activer le redémarrage de certains serveurs en priorité.	Personne habilitée à activer le PRA Nuabee	Procédure d’activation du PRA dans la console PRA

Mobiliser des experts cyber externes pour avoir un avis / support sur l'importance de la crise cyber	• Si abonnement à un CSIRT ou Réponse à incident de type **Incident Response** d'OCD • Sans abonnement : « best effort »	RSSI+ Responsable Informatique + Responsable financier	Liste externalisée d'experts

Etape 1 : évaluer la gravité du sinistre cyber

- Quels sont les métiers (services) concernés ?
  - Quels sont les métiers (services) capables ou non de travailler ?
  - Quels sont les applications informatiques concernées ?
  - Quels applications informatiques peuvent continuer à être utilisés ?
- Les données des employés et/ou des clients sont-elles affectées ?

Liste des actions à mener	Détail des actions	Responsables de mise en œuvre	Outils et documents disponibles
Désigner le lieu de Rdv de la Cellule de Crise Cyber et la convoquer	Dans une cyber crise les bâtiments restent disponibles. Il faut définir un lieu et convoquer la première réunion de la CC.	RSSI+ Responsable Informatique	· Coordonnées acteurs CC · Logistique CC
Organiser la logistique de Cellule de Crise Cyber (local, outils de communication)	Il s'agit de définir en cas de cyberattaque : • Les moyens de communication à utiliser • Les outils de communication à utiliser Et de trouver un moyen pour les communiquer aux métiers et experts internes & externes.	RSSI+ Responsable Informatique	· Outils de communication de repli · Outils de prise de notes
Réceptionner les CR de situation	Via les moyens de communication décidés, recevoir les CR fournis par les métiers / intervenants externes	RSSI+ Responsable Informatique	Solution externe de messagerie de secours

Mobiliser des experts externes Cyber	Mobiliser des experts externes pour avoir un avis sur l'importance et le périmètre de la crise cyber.	RSSI+ Responsable Informatique	
Comprendre le type d'attaque et comment la circonscrire et la nettoyer.	Il s'agit de savoir si l'attaque est connue et si des actions peuvent être entreprises pour remédier à l'attaque	RSSI+ Experts externes	
Évaluer le niveau de gravité du sinistre	Il s'agit d'estimer les impacts potentiels de la crise et de produire un Compte Rendu qui indique une première approche du périmètre de la crise.	Tous les acteurs de la CC Cyber	

Etape 2 : Activer les dispositifs du PRA

Il s'agit dans cette étape de restaurer les applications et les données critiques pour reprendre le cœur des activités en définissant :

1. Le périmètre du PRA à activer, notamment
    1. Les choix des sites (si le PRA concerne plusieurs sites)
    2. La liste des VM
    3. La date de restauration (dernière sauvegarde ou date précise)
2. Les actions complémentaires à effectuer avant d'ouvrir les accès aux utilisateurs
    1. Exécution de tests de sécurité
    2. Lancement d'appliances de sécurité complémentaires dans l'espace de secours

Liste des actions à mener	Détail des actions	Responsables de mise en œuvre	Outils et documents disponibles et commentaires

Définir le périmètre du PRA à activer	Il s’agit de définir : • Les choix des sites (si le PRA concerne plusieurs sites) • La liste des VM (périmètre fonctionnel) • La date de restauration (dernière sauvegarde ou date précise)	Equipe Informatique Client	Console PRA qui contient la liste des serveurs
Décider d’actions complémentaires avant d’ouvrir l’espace de secours	Il s’agit d’identifier les actions optionnelles à mener avant d’ouvrir l’espace de secours aux utilisateurs : • Exécution de scan anti-virus • Réalisation de forensique • Isolation de certaines VM au redémarrage • …	Responsable Informatique + Experts Cyber Externes	o
Exécution de scan antivirus sur les serveurs redémarrés	Il s’agit de passer des scan d’antivirus sur les serveurs restaurés et redémarrés pour vérifier que les serveurs redémarrés ne contiennent pas de malware connus.	Equipe Informatique Client	• Par défaut utilisation d’un scan Windows Defender. • Autres solutions possibles.

Réalisation de forensique	Mise à disposition d'un espace Cloud dédié pour le cabinet de conseil Cyber : • Ouverture des droits d'accès • Copie des disques du périmètre projet • Accompagnement à l'utilisation de l'espace Cloud.	Experts Cyber Externes avec support équipes **Flexible Recovery**	
Isolation de certaines VM au redémarrage	Pour certaines VM, il peut être nécessaire de les isoler sur un VLAN spécifique sans aucune communication avec d'autres serveurs en attendant l'avis des experts en Cyber sécurité	Équipes **Flexible Recovery** + Client	
Décision d'ouverture des réseaux	Il faut décider : • Quels sont les réseaux qu'il est possible d'ouvrir. • Quels sont les sécurités et les surveillances mises en œuvre sur les réseaux ouverts.	Responsable Informatique	Transmission de la décision du Responsable Informatique aux Équipes **Flexible Recovery**

Etape 3 : décider les mesures complémentaires

Il faut garder à l'esprit que la remédiation pour donner suite à une crise cyber peut être potentiellement longue et peut durer plusieurs jours ou semaines, voire plusieurs mois.

Il faut établir la liste des actions urgentes complémentaires à mener, et identifier les responsables pour leurs mises en œuvre.

Il s'agit dans cette étape d'adapter le périmètre du PRA et de durcir les systèmes et de surveiller l'attaquant pour reprendre le cœur des activités.

En cas de cyber-attaque, il est possible (voire probable) que des modifications doivent être faites sur les l'infrastructures (architecture de sécurité, version des OS, durcissement des serveurs, modifications des architectures télécom…) avant d'envisager un retour à la situation nominale.

Etape 4 : organiser le retour arrière

Il s'agit d'organiser le retour à la situation nominale, après l'activation du PRA et son utilisation en réel par un Client.

L'objectif est de présenter le processus général et en fonction du contexte de la crise cyber, les mécanismes de mise en œuvre seront ajustés.

L'ensemble de ces phases sont expliquées dans un document spécifique : **Retour à la situation nominale après utilisation du PRA**