Comment nos solutions s’inscrivent dans un Plan de Continuité d’Activité ?

Cyber-Résilience by Nuabee · https://preview.nuabee.fr/documents/solutions-nuabee-plan-continuite-activite/

Définitions pour se comprendre : qu’est un Plan de Continuité d’Activité

Dans le vocabulaire de la Continuité d’Activité, un PCA (Plan de Continuité d’Activité) représente l’ensemble des éléments formant un plan qui doit permettre à une entreprise de fonctionner même en situation de désastre et ce à minima en mode dégradé.

Ce Plan de Continuité d’Activité contient plusieurs dimensions :

- une **dimension logistique** : les locaux ont brûlé, comment va t’on reloger les collaborateurs et quels sont ceux que l’on peut envoyer en télétravail ?
- une **dimension métier** : quels sont les processus métiers qui doivent continuer à fonctionner (et ceux qui sont moins ou pas critique et que l’on va mettre en sommeil) ?
- une **dimension informatique et réseaux** : quelles sont les applications qui supportent les activités métiers les plus importantes. On parle souvent de PRA (Plan de Reprise d’Activité) ?
- enfin une **dimension de gestion de crise** qui doit traiter, suivant le scénario de sinistre avéré, l’articulation de la vision métiers, de la communication interne et externe, des relations avec les clients et les autorités.

Comment Nuabee s’inscrit dans un Plan de Continuité d’Activité

En tant que solution de Plan de Reprise d’Activité, Nuabee se focalise avant tout sur la dimension reprise de l’informatique et des réseaux mais participe également à la gestion de crise dans sa dimension IT.

Donc, en plus d’une dimension très technique de redémarrage des serveurs dans le bon ordre et en respectant les délais de redémarrage (normalement issus des besoins des métiers), Nuabee

accompagne les clients dans leur gestion de crise IT.

Ceci prend encore plus d'importance dans un contexte de crise lié à une cyberattaque où, dans les premières heures, il peut être difficile de distinguer un incident IT d'un incident cyber.

Le contexte particulier de la cyberattaque

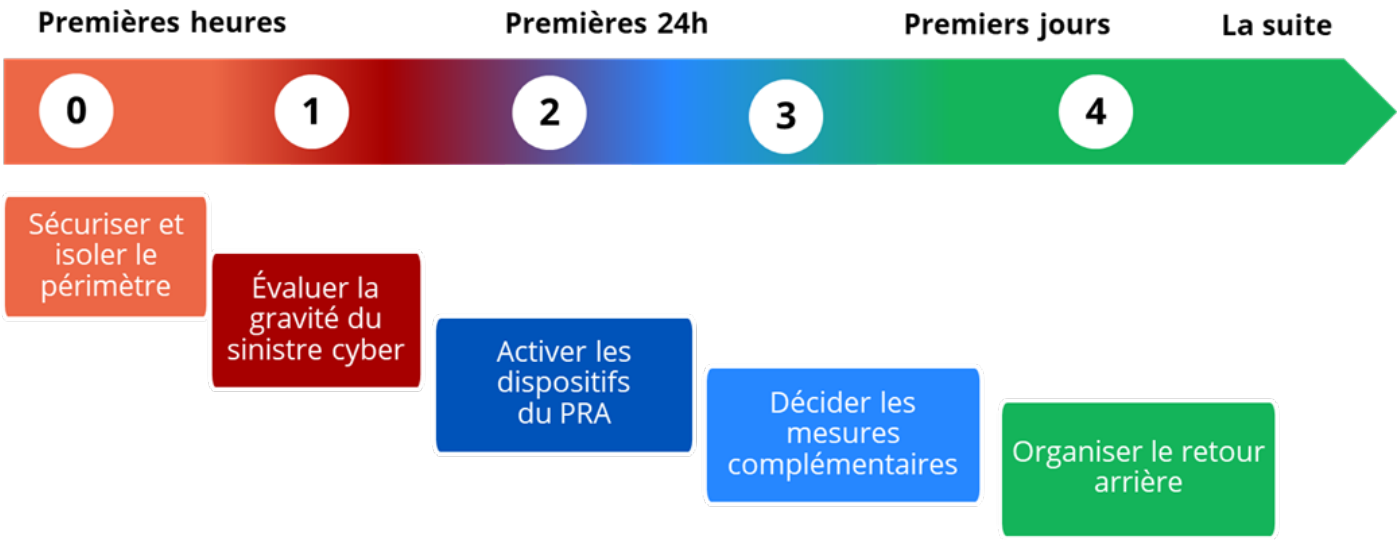
En comparaison à d'autres scénarios de crise, les crises cyber ont des caractéristiques propres qu'il est important d'appréhender :

- 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 double temporalité, avec des impacts immédiats et une remédiation longue pouvant s'étendre sur plusieurs semaines, voire plusieurs mois.

Cette crise implique un certaine complexité pour comprendre les objectifs de l'attaquant et attribuer l'origine de l'attaque.

L'implication de Nuabee dans la chronologie d'une crise cyber

Les principales étapes d'un crise cyber sont les suivantes :



Nuabee peut vous accompagner dans ces 4 étape et peut proposer des actions complémentaires avant la réouverture des applications aux utilisateurs comme :

- Exécution de scan anti-virus sur les disques et les VM
- Exécution d’outils d’investigation numérique (forensique) sur les disques et les VM
- Mise à disposition d’un environnement isolé pour le prestataire de sécurité du client afin de pouvoir exécuter des outils d’investigation numériques.

