Cahier des charges du projet AFNOR-SPEC : *« Continuité d'activité et résilience des organismes en cas d'indisponibilité prolongée du SI, suite à une cyberattaque»*

Projet : Le projet vise la rédaction d'un document de référence d'application volontaire, de type AFNOR-SPEC**,** sur la continuité d'activité et la résilience des organismes en cas d'indisponibilité prolongée du SI, **à la suite d'une cyberattaque.**

Contexte : Les typologies d'attaques cyber récentes, leur fréquence et leur multiplication dans tous les domaines sociétaux (ex : entreprises, hôpitaux, collectivités) ont montré que les organismes pouvaient se retrouver perturbés durablement, sans perspective claire de retour à une situation normale avant plusieurs semaines voire plusieurs mois. Nombreux sont les organismes qui peuvent se retrouver démunis à la suite d'une cyberattaque réputée inéluctable, considérant que l'impact organisationnel est d'autant plus élevé en l'absence de fonctions et de ressources dédiées pour en traiter les conséquences.

Dans ce contexte général d'incident grave ou de crise industrielle ou sociétale, la communauté des gestionnaires des risques et celle des responsables du plan de la continuité d'activité (RPCA) utilisent un cadre cohérent constitué de règles, d'usages et de bonnes pratiques qui varient selon les secteurs.

Le projet vise notamment à recommander les bonnes pratiques mis en œuvre principalement en France pour limiter l'impact des cyberattaques et assurer la continuité de l'activité de l'organisme dans le cas d'une indisponibilité prolongée du SI.

Objectifs

- Envisager la continuité d'activité de l'organisation hors SI nominal en parallèle de la reconstruction du SI
- Préparer le fonctionnement en modes perturbés/degradés pendant une période longue (plusieurs semaines)
- Fournir un état de l'art des bonnes pratiques dans la perspective d'un redémarrage d'un SI dégradé par une cyber-attaque

Le groupe AFNOR permet aux parties prenantes volontaires de se réunir au sein d'un groupe de travail dédié, pour valoriser leurs engagements, échanger sur leurs pratiques et ainsi établir de manière consensuelle un document de référence AFNOR-SPEC.

Contenu

En introduction, les bonnes pratiques de prévention et de protection face aux cyberattaques seront rappelées (hygiènes informatiques, dispositifs de sécurité, de détection, sensibilisation

des acteurs…). Le document sera ensuite organisé en deux parties correspondant aux deux fronts sur lesquels les organisations doivent se battre en cas de cyberattaques :

1. la reconstruction du SI par les équipes supports (reprise d'activité informatique).
2. la mise en œuvre de solution métiers hors SI nominal (continuité d'activité de l'organisme).

Nous proposons que les travaux soient dirigés en deux sous-groupes correspondant à ce découpage.

I. RECONSTRUCTION DU SI EN CAS DE CYBERATTAQUE

- Définition des rôles et responsabilités des différentes cellules techniques, décisionnelles, métiers
- Identification du périmètre de compromission et des impacts opérationnels associés
- Stratégie de compréhension et de réponse de l'incident de sécurité
    - Endiguement de l'attaque et activation d'un plan de défense (mesures de protection du SI)
    - Compréhension de la cyberattaque à travers une investigation numérique (vecteur d'intrusion, moyen de propagation, indicateurs de compromission, actions malveillantes réalisées sur le SI)
    - Mise en place d'une surveillance de circonstance du système d'information (complémentarité entre la détection et l'investigation numérique)
- Stratégie de reconstruction du SI
    - Définition des priorités de reconstruction pour les composants d'infrastructure et les applications métier
    - Construction d'un cœur de confiance (mise en place d'un réseau de sauvegarde isolé pour la restauration, poste autonome d'administration...)
    - Etude des scénarios de reconstruction par application (restauration des sauvegardes, migration vers un service externalisé / SaaS...)
    - Reconstruire mieux et différents pour limiter l'impact des attaques
    - Durcissement du système d'information, basé sur la base des vulnérabilités exploitées par l'attaquant ou usuellement exploités par un attaquant
- Mise en place d'un plan de communication auprès des parties prenantes (clients, managers & collaborateurs, partenaires & sous-traitants, actionnaires)

II. SOLUTIONS DE CONTINUITE D'ACTIVITE METIERS

- Evaluation du risque de cyberattaque (attaquants et attaques, source de risque, scenario d'attaques, temporalité…)
- Impacts des cyberattaques (risque résiduel, traitement et remédiation, bilan d'impact BIA, continuité d'activité…)
- Accompagner les besoins SI de chaque métier d'un organisme afin de leur permettre d'atteindre leurs nouveaux objectifs dans le cas d'un fonctionnement hors SI nominal
- Cartographier les besoins des métiers en cas d'indisponibilité prolongée du SI
- Définir une stratégie PCA (solutions métiers) en cas de cyberattaques (redéfinir la stratégie et les objectifs métiers au regard de la dégradation du SI pour tenter de les atteindre)
- Adapter les PCA existants en y intégrant le scenario d'indisponibilité prolongée du SI

- Retour d’expérience : Retex de cyberattaques vécues avec indisponibilité partielle/totale du SI plusieurs semaines
- Cas d’usage (ex : Ransomware, etc)

Destinataires du projet : Ce document s’adresse aux parties intéressées de tous les organismes, de toute taille, de tous les secteurs, à savoir :

- en premier lieu, les personnes en charge de la continuité d’activité, de la sécurité, de la sécurité du SI, de la sûreté, de la gestion des risques, de la gestion de crise, de la gestion des données internes ou externes ;
- en deuxième lieu, les personnes en charge de la gouvernance exécutive de l’organisme ;
- en troisième lieu, les fournisseurs critiques et les autorités d’audit et de contrôle.

Délai de réalisation : février 2022 – septembre 2022

Méthode de travail : Le document de référence sera élaboré sur la base de contributions successives des participants.

Agenda : Consultation organisée au mois de janvier 2022, ouverte à toute partie intéressée. Réunion de lancement prévue au mois de février.

Participation : Toute partie intéressée peut devenir une partie prenante au sein de la plateforme dès lors qu’elle confirme son intérêt auprès d'AFNOR.

Chef de projet AFNOR en charge du sujet : Mme Mélissa JEAN – melissa.jean@afnor.org