Check-list Résilience

Cette check-list vise à améliorer la cyber-résilience de l'organisation. La cyber-résilience est définie comme la capacité d'une organisation « à anticiper, résister, récupérer et s'adapter à des conditions défavorables, à des stress, à des attaques ou à des compromissions sur des systèmes qui utilisent ou sont activés par des cyber-ressources.»[1]
Elle doit être imprimée et signée par un membre du conseil d'administration ou du comité exécutif. Cette liste de contrôle doit être conservée dans un endroit connu et accessible.

En cas de cyberattaque réussie contre votre organisation, n'oubliez pas

- Gardez votre calme et celui de l'organisation.
- Informez la personne de contact interne.
- Activez l'équipe de gestion de crise.
- Identifiez et limitez l'attaque/la compromission – conservez des enregistrements de journal !
- Définissez un plan de communication (et embargo) : Qui doit être informé, de quoi, quand et comment ?
- Identifiez les dommages et activez le plan de récupération des données, le cas échéant.
- Signalez l'incident aux autorités, enquêtez et tirer les leçons.

Pour les infrastructures critiques, une obligation de déclaration des cyberattaques pourrait s'appliquer (voir art. 74 let. b) et 74, let. d) du projet de loi sur la sécurité de l'information de 2022).

Check-list:

1. Personne de contact interne (et suppléant) à informer en cas de cyber-incident ou d'incertitudes concernant la compromission potentielle du système d'information :

	Nom	Numéro de téléphone
Personne de contact interne		
Suppléant		

1 See https://csrc.nist.gov/glossary/term/cyber_resiliency

2. En cas de cyberincident, qui est autorisé à couper l'internet ou à déconnecter l'organisation ?

☐ Personne de contact interne mentionnée en 1.

☐ Autre, veuillez préciser : nom :_____

téléphone:_____

3. Membres de l'équipe de gestion de crise :

Rôle	Nom	Numéro de téléphone
1. Responsable / leadership		
2. Responsable informatique		
3. Communication / porte-parole		
4. Spécialiste direction/gestion		
5. Spécialiste cyber		
6. Affaires juridiques		
7. Secrétariat (notes et compte rendu des principales décisions et mesures prises)		

4. En cas de cyberattaque réussie, la **sécurité physique et psychosociale des employés, des clients et des autres parties prenantes** est-elle potentiellement affectée ?

☐ Oui ☐ Non

Dans l'affirmative, veuillez préciser les risques et indiquer les mesures d'urgence visant à prévenir les risques physiques et psychosociaux :

Risques pour la sécurité	Mesures d'urgence

5. Listez les **trois principales activités génératrices de revenus ou vous permettant de remplir votre mission**, ainsi que des systèmes informatiques y relatifs (le cas échéant):

Principales activités	Système d'information principal	Systèmes d'information de soutien (dépendances)
1)		
2)		
3)		

6. Pour les **systèmes informatiques identifiés** au point 5, veuillez indiquer:

Système d'information	Sauvegarde hors ligne? (oui/non)	Objectif de temps de rétablissement?	Disponibilité hors ligne des informations d'identification (sauvegarde)?	Contact/ fournisseur

7. En cas d'attaque réussie, certaines de vos activités peuvent être interrompues. Cela peut avoir un impact sur **vos employés, clients et autres parties prenantes,** nécessitant ainsi une **communication proactive**. Veuillez énumérer les principaux contacts externes et parties prenantes et joindre une liste des employés et des coordonnées :

Parties prenantes	Contact	Canaux de communication (téléphone, communiqué de presse, réunion, etc)
Employés		
Clients/Citoyens		
Fournisseurs et partenaires		
- Fournisseur 1		
- Fournisseur 2		
Assurance, le cas échéant:		
Autorités (police, etc).		
- NCSC		
- Police cantonale		
Médias et public		

Date et lieu: Signature:

Principes directeurs de la communication de crise :

- Définissez le porte-parole. Communiquez en interne, puis en externe
- Définissez le message clé, soyez bref et simple
- Restez factuel, pas d'hypothèses ; si l'information est connue :
  - L'étendue des dommages et des impacts
  - Mesures d'urgence
  - Poursuite de l'enquête numérique
  - Implication des autorités
- Formulez des messages orientés vers l'action et les solutions.

Exemple de premier communiqué de presse

"Cyberattaque contre [nom de l'organisation]".
[Lieu et date] – Le [date de l'attaque], [Nom de l'organisation] a été ciblée par une cyberattaque. (Si possible : fournissez des détails sur la chronologie, l'identification de l'attaque, le type d'attaque.)

La principale préoccupation de [Nom de l'organisation] à la suite de cette attaque concerne les risques potentiels liés à cette brèche. En réponse, [Nom de l'organisation] a immédiatement renforcé ses mesures de sécurité, en engageant des actions tant internes qu'en recourant à un soutien externe spécialisé. (Par conséquence, les systèmes de [nom de l'organisation] ont dû être désactivés et déconnectés d'Internet en tant que mesure préventive). L'ampleur des impacts est en cours d'évaluation. En outre, [nom de l'organisation] a signalé le cas à la [police cantonale, GovCert] et travaille en étroite collaboration avec des experts en cybersécurité et les autorités.

(À ce stade, [nom de l'organisation] n'est pas en mesure de fournir d'indications sur la date de rétablissement complet des systèmes). (À notre connaissance, aucune donnée de [nom de l'organisation] n'a été chiffrée ni extraite. Si nos clients venaient à être affectés, nous les contacterions directement.) Nous mettons en œuvre toutes les mesures nécessaires de manière à rétablir une situation normale dans les plus brefs délais. Les clients et les fournisseurs peuvent communiquer avec leurs contacts au sein de [Nom de l'organisation] par téléphone.

Nous vous remercions pour votre patience et votre compréhension.

[Prochain communiqué de presse à 20h.]

Contact : porte-parole