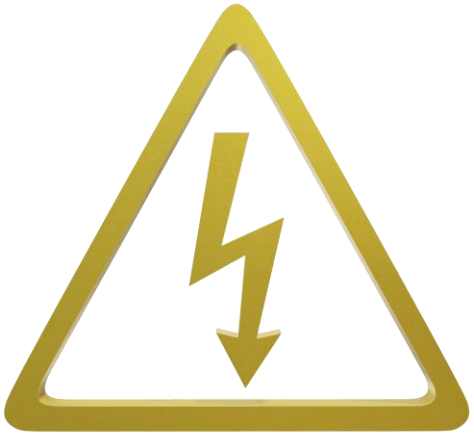
BUSINESS CONTINUITY PLAN
THE SUN COMPANY



ABDEL KHAMALLAH / BASTIEN DOS REIS / AUGUSTIN DELANNOY / MAXIME LAROUQUERRE / JULIEN DHORNE

Contexte du document :

Ce document a pour but d'accompagner les équipes du SI dans la mise en place du Plan de Reprise d'Activité.

Un incident cyber majeur vient de se produire et oblige le déclenchement du plan de reprise d'activité (PRA).

La gestion de cette crise cyber va donc impliquer de mettre en place des mesures initiales de préservation et de mobiliser des structures de gestion de crise de l'organisation SUN Company.

L'activation de ce dispositif de crise peut être activé soit par le haut, c'est-à-dire la partie stratégique de l'organisation, soit par le bas, c'est-à-dire les équipes du SI habilitées à prendre la décision de mettre en place des actions immédiates (extinction des serveurs, coupure de courant, etc.).

1. Références du document

1.1 Qualité

Nom	Fonction
Nom du document	Business Continuity Plan
Classification	Confidentiel
Type du document	Procédure Administrateur
Etat du document	En cours de validation
Auteur(s)	Team RPONET
Propriétaire	Groupe 3 AIS
Objet	Création

1.2 Diffusion

Société	Service	Fonction, titre ou nom
SUN Company	IT Infrastructure	System Administrators

1.3 Historique des versions

Version	Objet	Date	Nom
1.0	Création	13/06/2023	Abdel Khamallah
2.0	Mise à jour	26/06/2023	Abdel Khamallah
3.0	Correction et mise en page	07/09/2023	Julien Dhorne
3.1	Correction et mise en page	13/09/2023	Julien Dhorne

1.4 Visas

Approuvé	Date	Nom

2. Contacts

2.1 Participants à cette réponse

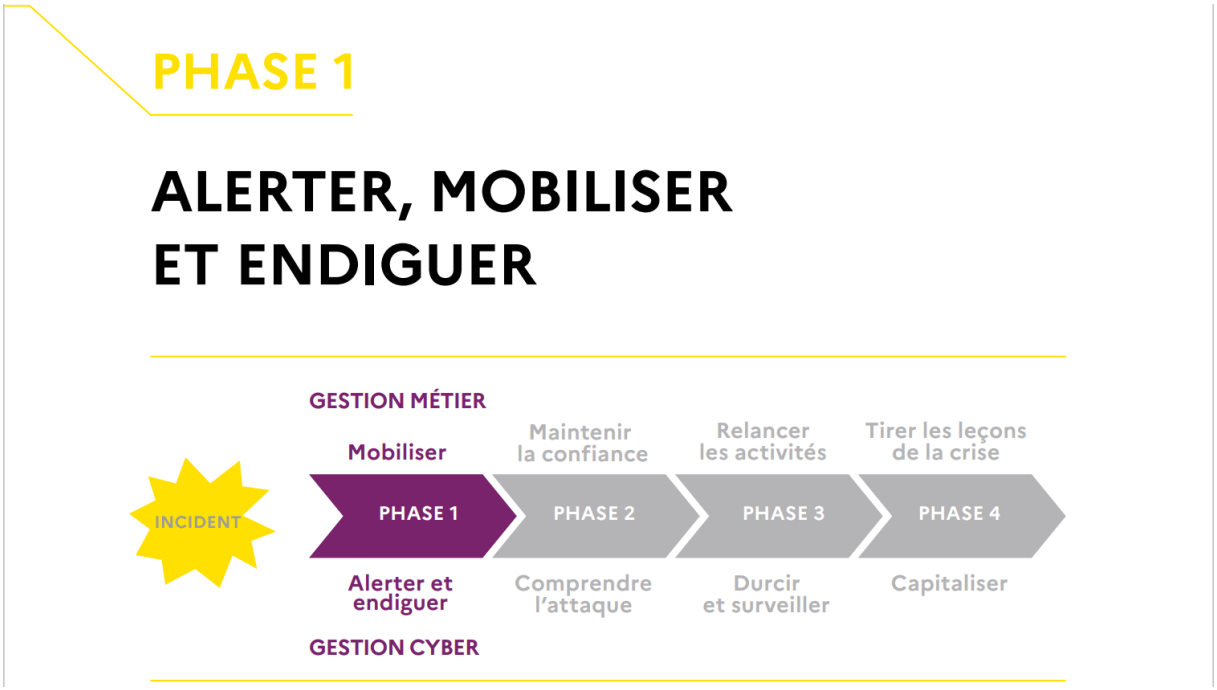
Nom	Fonction	Téléphone	E-mail
Augustin Delannoy	Administrateur		
Bastien Dos Reis	Administrateur		
Abdel Khamallah	Administrateur		
Maxime Larouquerre	Administrateur		
Julien Dhorne	Administrateur		

2.2 Destinataires

Nom	Fonction	Téléphone	E-mail
David	Formateur		
Arthur	Roi		

[Procédure à respecter strictement]

Rappel de la chronologie des différentes phases :



Etape 1 : Mobiliser

Dans le cas d'une TPE ou une PME : Ne pas éteindre ni modifier les ordinateurs et matériels.

Cf. Recommandations de l'ANSSI en page 28 de ce guide : www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-treize-questions/

Etape 2 : Qualifier l'importance de l'incident

Réaliser une première évaluation du périmètre avec les équipes du SI et des différents métiers de l'organisation.

Quels sont les dysfonctionnements métiers rencontrés ?

Notez et documentez toutes les informations par écrit ou à l'aide d'un poste hors ligne (mode avion activé), n'ayant eu aucun contact avec le SI dans le passé ni le jour de l'incident cyber.

Les ordinateurs personnels ayant déjà reçu un dispositif amovible du SI infecté est formellement proscrit.

Identifier le plus en amont possible la ou les sources de cet incident.

Il est nécessaire d'identifier les sources d'informations et les anomalies du SI avant d'alerter les services spécialisés.

Le but de cette démarche est de faire un état des lieux pour obtenir une vision globale la plus fiable possible.

Etape 3 : Observer pour évaluer la criticité de l'attaque

- Récolter les logs de manière sécurisée si cela est possible,

- Etudier les dysfonctionnements informatiques et leurs niveaux de perturbations,

- Détecter les arrêts de service, de machines et des serveurs,

- Détecter la disparition de fichiers ou l'impossibilité de les lire,

- Des systèmes distincts présentent-ils des anomalies, et si oui sont-elles liées ?

Etape 4 : s'orienter pour identifier les impacts potentiels et les actions à prendre

- L'incident est-il confirmé ?
    - S'il ne l'est pas, comment confirmer ou infirmer le signalement ?
    - La collecte d'informations doit-elle se poursuivre ?

- Estimer les impacts potentiels de la situation :
    - Le type d'attaque peut-il être déterminé ?
    - Les systèmes infectés comportent-ils des données sensibles ?

- Les systèmes suspectés d'être touchés sont-ils soumis à contraintes réglementaires ou contractuelles ?
- Les métiers ont-ils une visibilité sur l'incident ? Sont-ils impactés par l'incident ?
- Quels sont les actifs à mettre en sûreté en cas d'aggravation de l'incident ?
- Où sont les traces connues ou potentielles laissées par l'attaquant ?
- Identifier les obligations contractuelles qui s'appliquent à SUN Company ?

Etape 5 : Réagir

D'abord, on décide.

Il est impératif de synthétiser les réponses aux précédentes questions pour les décideurs métiers et la direction de la compagnie.

Il est aussi possible de prendre conseil auprès de spécialistes dont vous trouverez les coordonnées à la fin de document.

Si la criticité de l'incident est avérée et reconnue par la direction, il faut ensuite endiguer l'incident par des mesures adaptées à la situation, par exemple :

Effectuer des coupures de réseau,

Eteindre les machines,

Bloquer les accès distants,

Mettre en sûreté une copie des sauvegardes importantes

Troisièmement, on préserve les traces :

Mettre en sécurité les journaux de logs et d'événements (copie hors ligne ou sur ses systèmes isolés),

Prolonger les périodes de rotation des journaux systèmes et équipements,

Penser à tous les types de journaux (sécurité, systèmes, serveurs, postes clients, infrastructure).

Ensuite, on communique en interne :

Prévenir les équipes et les responsables habilités,

Identifier les points et moyens de contact (si ce n'est pas déjà fait). Tous les employés n'ont le même accès aux informations, surtout en cas d'incident majeur,

Penser à mettre des affiches si les postes clients ont été éteints (« NE PAS ALLUMER L'ORDINATEUR »),

Demander à chaque responsable de tenir un registre des actions menées par chaque collaborateur,

Tenir un reporting des événements dans chaque service,

Constituer une équipe de gestion de crise cyber avec les effectifs présents (si ce n'est pas déjà fait).

Enfin, on alerte : Prévenez directement la gendarmerie ou la police dès que possible dont les coordonnées sont mentionnées ci-dessous. Déposez plainte pour permettre de tracer le dommage et déclencher une enquête.

Ces éléments seront utiles aux enquêteurs.

En cas de rançongiciels, ne pas payer la rançon demandée. Les gendarmes ou les policiers possèdent des solutions de déchiffrement permettant de retrouver une activité normale.

Contacts

- Téléphone : 17

- Le commissariat ou la gendarmerie la plus proche

- CNIL : www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Pour plus d'informations, voici deux liens intéressants :

- Cybermalveillance : www.cybermalveillance.gouv.fr/diagnostic/accueil

- CERT-FR : www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dintrusion-sur-un-systeme-dinformation/

[Checklist à respecter strictement]

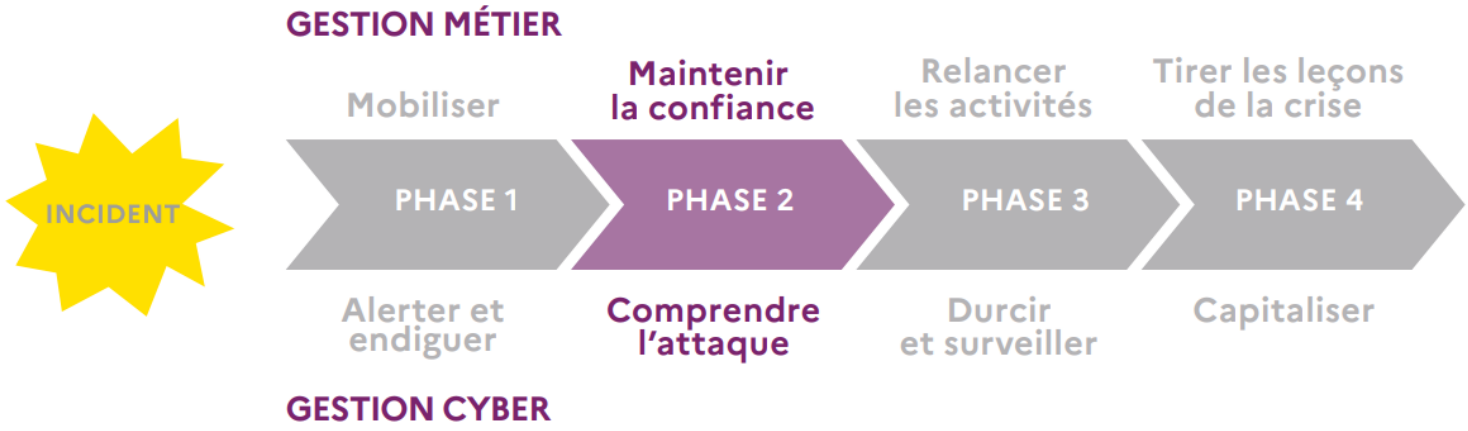
Actions	**Nom - Prénom**	**Date et heure précise** XX/XX/2023 17h19mn17s	**Statut** Réalisé Non fait En cours
1 Ne pas éteindre ni modifier les ordinateurs et matériels			
2 Réaliser une première évaluation du périmètre avec les équipes du SI et des différents métiers de l'organisation			
3 Notez et documentez toutes les informations par écrit ou à l'aide d'un poste hors ligne (mode avion activé)			
4 Identifier le plus en amont possible la ou les sources de cet incident			
5 Récolter les logs de manière sécurisée si cela est possible			
6 Etudier les dysfonctionnements informatiques et leurs niveaux de perturbations			
7 Détecter les arrêts de service, de machines et des serveurs			
8 Détecter la disparition de fichiers ou l'impossibilité de les lire			
9 Des systèmes distincts présentent-ils des anomalies, et si oui sont-elles liées ?			
10 L'incident est-il confirmé ?			

Actions	**Nom - Prénom**	**Date et heure précise** XX/XX/2023 17h19mn17s	**Statut** Réalisé Non fait En cours
11 La collecte d'informations doit-elle se poursuivre ?			
12 Estimer les impacts potentiels de la situation			
13 Le type d'attaque peut-il être déterminé ?			
14 Les systèmes infectés comportent-ils des données sensibles ?			
15 Les systèmes suspectés d'être touchés sont-ils soumis à contraintes réglementaires ou contractuelles ?			
16 Les métiers ont-ils une visibilité sur l'incident ? Sont-ils impactés par l'incident			
17 Quels sont les actifs à mettre en sûreté en cas d'aggravation de l'incident ?			
18 Où sont les traces connues ou potentielles laissées par l'attaquant ?			
19 Identifier les obligations contractuelles qui s'appliquent à SUN Company ?			
20 Synthétiser les réponses aux précédentes questions pour les décideurs métiers et la direction de la compagnie			
21 Prendre conseil auprès de spécialistes			
22 Endiguer l'incident par des mesures adaptées à la situation (Effectuer des coupures de réseau, éteindre les machines, bloquer les accès distants, mettre en sûreté une copie des sauvegardes importantes, etc.)			

Actions	**Nom - Prénom**	**Date et heure précise** XX/XX/2023 17h19mn17s	**Statut** Réalisé Non fait En cours
23 Mettre en sécurité les journaux de logs et d'événements (copie hors ligne ou sur ses systèmes isolés)			
24 Prolonger les périodes de rotation des journaux systèmes et équipements			
25 Penser à tous les types de journaux (sécurité, systèmes, serveurs, postes clients, infrastructure)			
26 Prévenir les équipes et les responsables habilités			
27 Identifier les points et moyens de contact			
28 Penser à mettre des affiches si les postes clients ont été éteints (« NE PAS ALLUMER L'ORDINATEUR »)			
29 Demander à chaque responsable de tenir un registre des actions menées par chaque collaborateur			
30 Tenir un reporting des événements dans chaque service			
31 Constituer une équipe de gestion de crise cyber avec les effectifs présents			
32 Prévenez directement la gendarmerie ou la police dès que possible			

PHASE 2

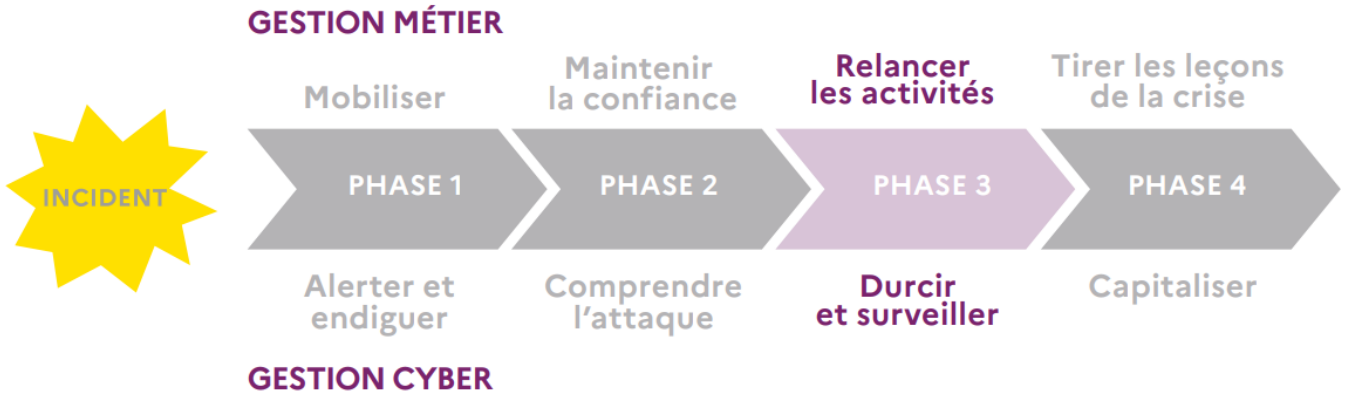
MAINTENIR LA CONFIANCE ET COMPRENDRE L'ATTAQUE



ABDEL KHAMALLAH / BASTIEN DOS REIS / AUGUSTIN DELANNOY / MAXIME LAROUQUERRE / JULIEN DHORNE

PHASE 3

RELANCER LES ACTIVITÉS MÉTIERS ET DURCIR LES SYSTÈMES D'INFORMATION



ABDEL KHAMALLAH / BASTIEN DOS REIS / AUGUSTIN DELANNOY / MAXIME LAROUQUERRE / JULIEN DHORNE