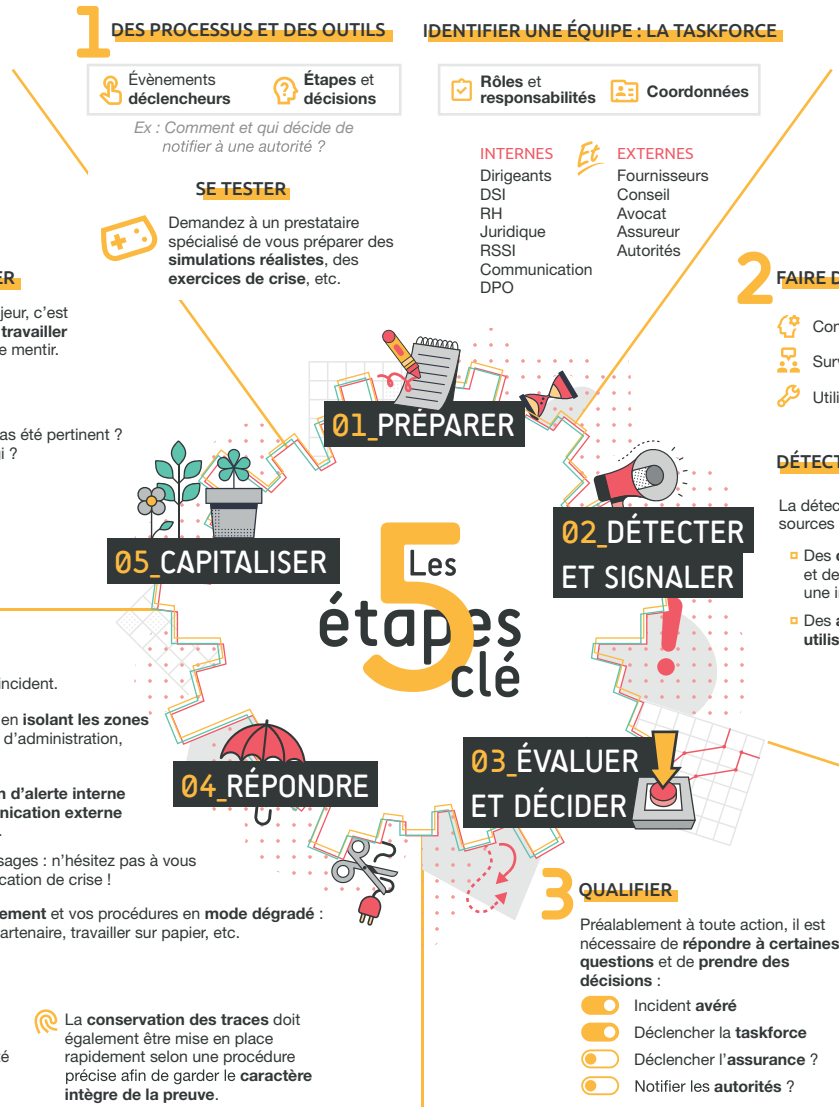
INCIDENTS
DE SÉCURITÉ INFORMATIQUE
GÉRER L'IMPRÉVU, ÇA NE S'IMPROVISE PAS !

Une méthodologie pour gérer vos incidents de sécurité informatique.
Si vous ne disposez pas de l'expertise nécessaire, **privilégiez le recours à des prestataires spécialisés en cybersécurité**.



1 DES PROCESSUS ET DES OUTILS

- Évènements **déclencheurs**
- **Étapes** et **décisions**

Ex : Comment et qui décide de notifier à une autorité ?

IDENTIFIER UNE ÉQUIPE : LA TASKFORCE

- **Rôles** et **responsabilités**
- **Coordonnées**

INTERNES
Dirigeants
DSI
RH
Juridique
RSSI
Communication
DPO

Et

EXTERNES
Fournisseurs
Conseil
Avocat
Assureur
Autorités

SE TESTER

Demandez à un prestataire spécialisé de vous préparer des **simulations réalistes**, des **exercices de crise**, etc.

2 FAIRE DE LA VEILLE

- Connaitre les **faiblesses** de son SI
- Surveiller des **cercles spécialisés**
- Utiliser des **outils de veille**

DÉTECTER

La détection peut se faire grâce à plusieurs sources :

- Des **outils automatiques** de détection et de remontée d'alertes, couplés à une intervention/surveillance humaine
- Des **alertes remontées par des utilisateurs**/prestataires vigilants

3 QUALIFIER

Préalablement à toute action, il est nécessaire de **répondre à certaines questions** et de **prendre des décisions** :

- Incident **avéré**
- Déclencher la **taskforce**
- Déclencher l'**assurance** ?
- Notifier les **autorités** ?

ÉVALUER

- Connait-on la **cause**/motivation ?
- Quelles **méthodes** sont utilisées ?
- Quels **impacts** immédiats et futurs ?

4 RÉSOUDRE L'INCIDENT

La réponse est à adapter au type d'incident.

- Protéger ce qui est encore sain en **isolant les zones compromises** : serveurs, outils d'administration, postes de travail, etc.
- Procéder à une **communication d'alerte interne** dans certains cas. Une **communication externe** peut également être nécessaire.

  Adaptez les moyens et les messages : n'hésitez pas à vous entourer d'experts en communication de crise !
- Activez vos **plans de contournement** et vos procédures en **mode dégradé** : travailler dans les locaux d'un partenaire, travailler sur papier, etc.

CORRECTION TECHNIQUE

- Généralement avec l'**aide d'experts**. Il est important de garder en mémoire la temporalité et la **priorité** des actions recommandées.
- La **conservation des traces** doit également être mise en place rapidement selon une procédure précise afin de garder le **caractère intègre de la preuve**.

5 ANALYSER POUR S'AMÉLIORER

Capitaliser sur un incident cyber majeur, c'est analyser ce qui a bien fonctionné et **travailler sur les axes d'amélioration** sans se mentir.

- Comment mieux surveiller ?
- Comment mieux alerter ?
- Comment mieux mobiliser ?
- Au sein de la taskforce qui n'a pas été pertinent ?
- Comment les « autres » ont réagi ?

Créer un **plan d'action** et en effectuer le **suivi** !

NOTIFER

Créer une fiche d'incident et, le cas échéant, déclarer l'incident à :

VOTRE ASSURANCE
LES AUTORITÉS ET AGENCES
ANSSI, CNIL, ARS...
LA POLICE/GENDARMERIE

BOITE À OUTILS

RÉPERTOIRE DES PRESTATAIRES
e-magazine.solutions-logiciels.com/GUIDE%20CYBER%202019

BONNES PRATIQUES
ssi.gouv.fr/en-cas-dincident/
enisa.europa.eu/publications/good-practice-guide-for-incident-management
cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresser
cybermalveillance.gouv.fr/tous-nos-contenus/

Édité par Syntec Numérique en Décembre 2019 - 148 boulevard Haussmann 75008 Paris - SIRET 38471900100024

syntec numérique

Décembre 2019

Avec le soutien de
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

syntec-numerique.fr
148, BD HAUSSMANN - 75008 PARIS - 01 44 30 49 70 - CONTACT@SYNTEC-NUMERIQUE.FR

Comité de rédaction Cybersécurité :
Julien Beaussart (Devoteam)
Matthieu Grall (Sodifrance)
Vincent Nguyen (Wavestone)

Conception graphique : Eric Schmitlin

ANATOMIE D'UN INCIDENT

Cet incident fictif s'inspire de cas réels issus d'échanges entre profesionnels du numérique.

syntec numérique

TÉLÉPHONE — il y a 3 mn

Astreinte DSI HNO
Appels manqués (3)

Samedi 7:02

On a un problème, je pense que la messagerie est tombée.

C'est un problème technique ou un incident sécu ? Je t'appelle, tu peux commencer à investiguer ?

Samedi 9:09

C'est l'horreur là je pense que c'est un ransomware qui a explosé l'annuaire et pas mal de serveurs. J'ai une demande de rançon sur l'écran. Ça doit pas être répertorié car l'antivirus n'a rien vu...

J'arrive dans 10 min, je suis dans un taxi. Tu peux envoyer des échantillons contaminés à l'éditeur de l'antivirus ?

Samedi 10:32

Incident en cours (Ransomware). Messagerie indisponible, activation de la cellule de crise. Veuillez vous rendre dès que possible dans les locaux.
Le RSSI

WHATISUP — maintenant

RSSI @ Taskforce Cyber
J'ai créé un groupe Whatisup avec tout le monde pour échanger vu qu'on n'a plus de mails...

Samedi

J'ai essayé d'appliquer le patch... Là on voit des exclusions apparaître dans les paramètres... En fait on n'a plus le contrôle de la console de l'antivirus ! C'est l'attaquant qui est toujours là et il contrôle tout, je suis très serieux. 18:04

Coupez tout ! L'application des correctifs, les entrées et sorties réseaux, on coupe tout ! 18:06

Nouveau message
adresseperso@fmail.com

À : monassureur@jassure.fr

Bonjour,
À la suite à notre appel, je vous confirme le déclenchement de l'assurance cyber.
Pouvez-vous me confirmer l'intervention d'experts dès cet après-midi ?

Console de supervision ×

https://super-vision.infra/console

Etat des services

- Annuaire
- Messagerie
- Téléphonie fixe
- Firewalls/Pare-feux
- Antivirus
- Intranet

Nouveau message
rssi@maboite.com

À : direction@maboite.com

Plan_action_v1.pptx

Vous trouverez, ci-joint, le plan d'action à la suite de l'incident informatique du mois dernier.
Quand peut-on se croiser pour parler du budget sécurité ?

SAMEDI 7H

Détection et signalement

Premiers signalements d'un incident technique impactant la messagerie.

Avoir des outils de détection et d'alerte ainsi que des **personnes disponibles pour traiter les alertes** est indispensable. Sans cette alerte du technicien d'astreinte, un weekend entier se serait écoulé sans aucune action !

SAMEDI 9H

Qualification et évaluation

Les premiers signes d'un ransomware se font savoir : une demande de rançon s'affiche sur certains écrans et l'annuaire de l'entreprise est compromis.

RANÇON : FAUT-IL PAYER ?

Non ! Pour commencer, il n'est pas assuré que vous récupériez vos données et que les hackers vous assistent dans cette tâche ! Enfin, cela contribuerait à alimenter cette forme de criminalité.
Pour finir, le caractère licite d'un paiment de rançon est plus que discutable en droit français.

SAMEDI 10H

Activation de la taskforce

Les fournisseurs de sécurité livrent leurs premières analyses qui confirment la qualification.
Le RSSI informe alors son dirigeant de l'incident et active officiellement la cellule de crise.

Savoir qui contacter chez ses prestataires et fournisseurs de sécurité. Prévoir une liste précise de personnes à contacter et des moyens de communication de crise alternatifs puisque les mails ne fonctionnent plus !

Tentatives de résolution

Les équipes travaillent à la mesure de l'étendue des dégâts et tentent de résoudre le problème. En soirée, les éditeurs mettent à disposition des correctifs de sécurité.

Laisser les équipes faire leur travail (informatique et RSSI, communication, métiers, juridique, etc.) et minimiser les égarements sur des sujets annexes.

SAMEDI 18H

Coupure et isolation du réseau

Découverte que l'attaquant est toujours présent au sein du réseau et a pris la main sur les outils de sécurité. La décision est prise d'isoler l'ensemble du réseau pour éviter des dégâts supplémentaires et stopper l'emprise du hacker sur le système d'information.

Définir des cas précis nécessitant la coupure du réseau, de façon à déporter cette prise de responsabilité sur une procédure validée et non une personne qui va forcément hésiter.

DIMANCHE 10H

Début de l'intervention de l'assurance

La cellule de crise contacte l'assurance, qui envoie des experts pour investiguer et trouver et appliquer des solutions. Les autorités (police/gendarmerie, CNIL et ANSSI) sont également contactées.

Les assurances servent aussi de pompiers et de soutien lorsque les ressources ou compétences internes ne sont pas suffisantes.

MERCREDI 17H

Premières reconstructions

La cellule de crise est activée en permanence et mène un vrai travail d'équipe ; l'annuaire est reconstitué à partir d'annuaires partiels et de sauvegardes déconnectées initialement du réseau, puis la messagerie.

Les sauvegardes sont souvent la première cible des attaques de cette nature, elles peuvent donc elles-mêmes être inutilisables.

VENDREDI 15H

Retour au nominal

Les équipements de sécurité, puis le reste, sont reconstitués. Pendant toute la semaine, l'enreprise a tenté de travailler avec des moyens informatiques limités ; et à l'issue, de nombreuses données restent perdues.

Les plans de continuité définis en amont des crises doivent prévoir les moyens de travailler avec des moyens informatiques réduits.

3 SEMAINES APRÈS

Retour d'expérience

Les investigations port-mortem des experts révèlent que l'attaquant est passé par un poste obsolète qui n'avait pas été recensé. La direction et les équipes débriefent et prévoient un plan d'action.

Disposer d'une vision claire de son parc informatique est la base de la sécurité. L'entreprise doit se nourrir de cette expérience pour capitaliser et s'améliorer.