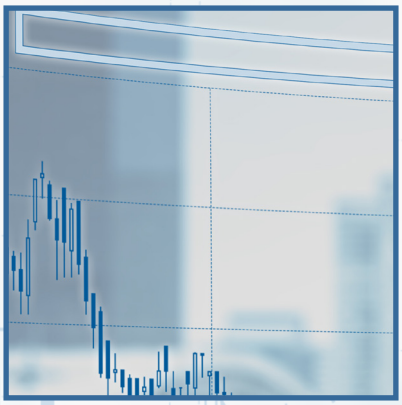
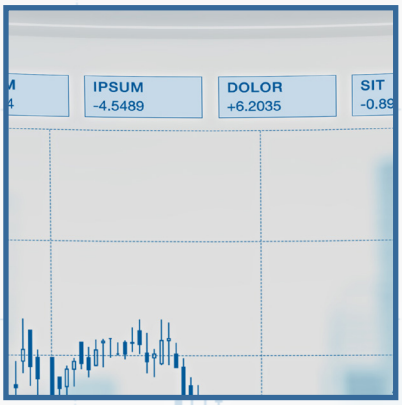
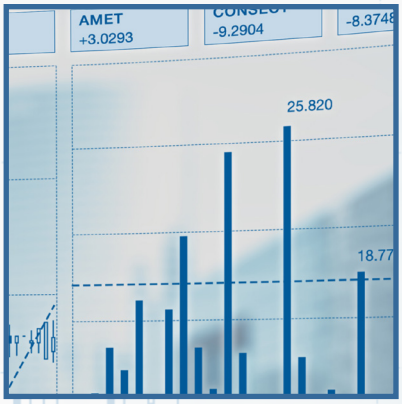
CYBER-CRISE

BONNES PRATIQUES DANS LA GESTION DE CRISES DE CYBERSÉCURITÉ







CCN-CERT BP/20

RAPPORT DE BONNES PRATIQUES

OCTOBRE **2020**

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

Édité par:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.02.05 17:01:08 +01'00'

Centre Cryptologique National, 2020

Date de Publication : janvier de 2021

TABLE DES MATIÈRES

1. Le CCN-CERT, CERT Gouvernemental National

Le CCN-CERT est la Capacité d'Intervention face à des incidents de Sécurité de l'Information du Centre Cryptologique National, le CCN, assigné au Centre National de Renseignements, le CNI. Ce service a été créé en 2006 en tant que **CERT Gouvernemental National espagnol**, et ses fonctions sont reprises dans la Loi 11/2002 régissant le CNI, le RD 421/2004 qui régit CCN, et le RD (Décret Royal) 3/2010, 8 janvier, régissant le Schéma National de Sécurité (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission consiste donc à contribuer à l'amélioration de la cyber-sécurité espagnole, en tant que centre d'alerte et de réponse nationale qui coopère et aide à répondre de manière rapide et efficace aux cyber-attaques et à affronter activement les cyber-menaces, en incluant la coordination au niveau public gouvernemental des différentes Capacités de Réponse aux Incidents ou des Centres d'Opérations de cyber-sécurité existants.

Et ce, afin de parvenir à un cyber-espace plus sécurisé et plus fiable, en préservant l'information classifiée (selon l'art. 4. F de la Loi 11/2002) et les données sensibles, en défendant le Patrimoine Technologique espagnol, en formant le personnel expert, en appliquant des politiques et des procédures de sécurité, en employant et en développant les technologies optimales à cet effet.

Conformément à cette réglementation et à la Loi 40/2015 du Régime Juridique du Secteur Public, la compétence du CCN-CERT inclut la gestion de cyber-incidents affectant tout organisme ou entreprise publics. Dans le cas d'opérateurs critiques du secteur public, la gestion de cyber-incidents sera effectuée par le CCN-CERT en coordination avec le CNPIC.

2. Introduction

Par crise l'on entend toute circonstance, délibérée ou fortuite, provoquée en interne ou non, et causant un déséquilibre dans une organisation avec son service, ses clients, ses actionnaires, ses travailleurs et ses représentants syndicaux, les autorités ou d'autres entreprises ou organismes, affectant ou nuisant à l'image et à la réputation publique, donnant lieu à une perte financière conséquente ou à un manquement légal, pouvant mettre en danger sa viabilité économique et/ou son avenir professionnel.

Une autre définition plus brève pourrait être : situation peu probable qui, si elle se produit, a un **impact important** et dont les effets **perdurent dans le temps**.

Face à une crise, trois éléments sont à prendre en compte : le degré de menace envers l'organisation, l'élément de surprise (imprévisible et inattendu) et la durée limitée pour la prise de décisions. Dans tous les cas, les menaces ou les circonstances doivent être gérées avant, pendant et après leur survenue, en s'assurant qu'il n'est pas nécessaire qu'un problème réel existe pour se trouver en situation de crise. Il suffit qu'une rumeur ou un événement passe à l'opinion publique pour que le processus s'accélère, voire, au vu de la place actuelle des réseaux sociaux, cela se propage sans contrôle, créant la panique auprès des groupes d'intérêt concernés. Ceci compliquera encore plus la gestion de crise.

La gestion de toute sorte de crise est une discipline qui a connu un développement important au cours de la dernière décennie dans des domaines très différents, particulièrement ceux concernant la Sécurité de l'Information (SGSI) et la Communication. S'agissant de situations particulièrement graves, qui peuvent arriver à compromettre le fonctionnement de l'organisation, voire son avenir, cette gestion s'est transformée en capacité de plus en plus indispensable pour un nombre croissant d'organisations. Parmi les nombreux facteurs qui ont facilité leur développement, il convient de souligner, entre autres, une exigence supérieure en matière de prestation de services, d'accroissement de la responsabilité sociale, et d'impact potentiel des réseaux sociaux sur sa réputation et son image.

Dans ce contexte, il commence déjà à exister un corpus de connaissances de base très heuristiques, qui oriente vers les **ressources les plus appropriées** en vue de permettre aux organisations de développer cette capacité et les **pratiques de gestion plus recommandables** afin d'affronter avec succès toute sorte de crise.

Les effets d'une crise sur une organisation portent sur:

Toute crise implique une **prise de décisions sous tension** dans des **délais et avec des informations limités** et sur **divers fronts à la fois**, avec l'intervention de nombreux agents et personnes.

Indépendamment de l'origine de la crise, l'on voit clairement la **composante de gestion** qu'implique sa résolution. Pour cela, l'organisation affectée a besoin d'avoir été dotée des **capacités et des structures de gestion** appropriées lui permettant de l'aborder avec des garanties de succès.

Dans toute crise. deux sphères d'action différentes sont donc identifiées :

- **Opérationnelle et réponse technique à l'incident nte**: elle concerne la raison qui en est l'origine et dont les effets immédiats doivent être contenus et résolus par une équipe de réponse spécialisée. Une équipe ou la capacité de réponse à des cyber-incidents qui, détectant rapidement des attaques et des menaces, diminue la perte ou la destruction de biens technologiques ou d'information, réduit l'exploitation malveillante des points faibles des infrastructures, et parvient à rétablir les services dès que possible[1]. Il s'agit d'une activité complexe qui doit prévoir l'adoption de méthodes de collecte et d'analyse de données et d'événements, de méthodologies de suivi et de procédures de typification de danger et de priorisation.
- **Organisation et stratégie** car son impact affecte différents domaines de l'organisation (service, opérations, image et réputation, relation avec le régulateur, groupes d'intérêt, présence sur les réseaux sociaux, etc). Cela exige une réponse coordonnée à haut niveau, décidant des canaux de communication avec d'autres unités ou organismes, propres et/ou étrangers,

Les capacités et les structures de gestion nécessaires pour faire face à une crise ne s'improvisent pas au moment de son apparition, il est indispensable de les développer à l'avance afin de disposer de la préparation nécessaire le moment venu.

Les capacités et les structures de gestion nécessaires pour faire face à une crise ne s'improvisent pas au moment de son apparition, il est indispensable de les développer **à l'avance** afin de disposer de la préparation nécessaire le moment venu.

1 Guía CCN-STIC 817_Gestión de Ciberincidentes: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Comme cadre de référence, les Tableaux 1 et 2 présentent le profil générique d'une crise et ses principaux stades, autour desquels s'articulera la proposition de bonnes pratiques développée dans le présent document:

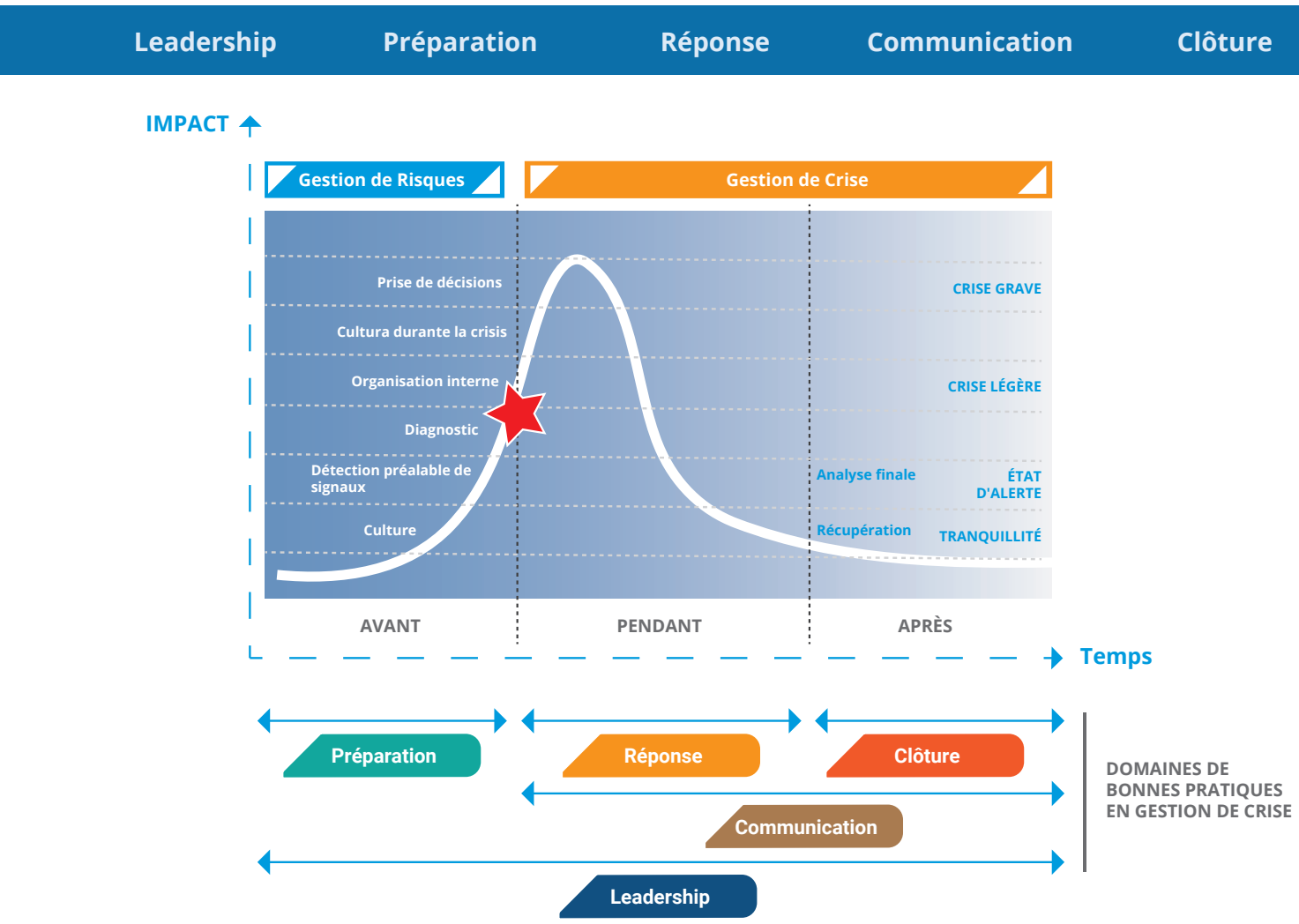


Tableau 1. Profil d'une crise[2]

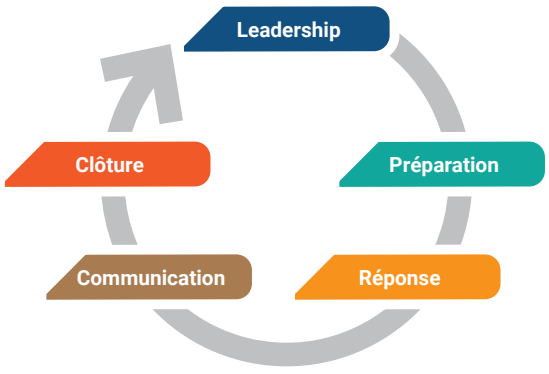


Tableau 2. Domaines fondamentaux pour aborder une crise

2 Bonnes pratiques dans la gestion de crise Institut Soie (Figuras 1 y 2)

En ce sens, il faut insister sur l'importance du travail préalable afin de préparer l'organisation quand la crise se présente : l'analyse de risques, la mise au point des plans d'action associés et la définition des structures de gestion appropriées en exerçant une prospective constante en vue d'estimer le type de cyber-attaque le plus probable pour devancer le problème en concevant la manière de la gérer face au moindre indice de matérialisation.

En nous centrant sur l'objet de ce Rapport, nous pouvons donc définir une cyber-crise comme un événement, dans l'environnement de la cyber-sécurité, ayant un impact important sur l'activité de l'organisation et exigeant de prendre des décisions rapides malgré une information limitée. La probabilité de cet événement dépendra du degré de préparation préalable de l'organisation : elle sera très faible si l'on a pris un grand nombre de mesures préventives en les augmentant progressivement avec la diminution du travail de prévention antérieur.

Ce guide de bonnes pratiques dans la gestion de cyber-incidents se base sur des analyses détaillées d'épisodes récents réels dont dérivent des recommandations pour aborder la crise en général, en distinguant dans chaque cas la bonne praxis de gouvernement en matière de crises dérivées d'incidences de cyber-sécurité.

L'on prévoit à cet effet un décalogue de treize (13) bonnes pratiques[3], résumées dans le tableau 3, qui prévoit des composants fondamentaux du modèle de succès pour aborder une crise et organisé dans les cinq domaines signalés précédemment -**leadership**, **préparation**, **réponse**, **communication et clôture**- portant sur le profil générique d'une crise.

Le paragraphe 4 développe ces bonnes pratiques de gestion de crise concernant des cyber-incidents.

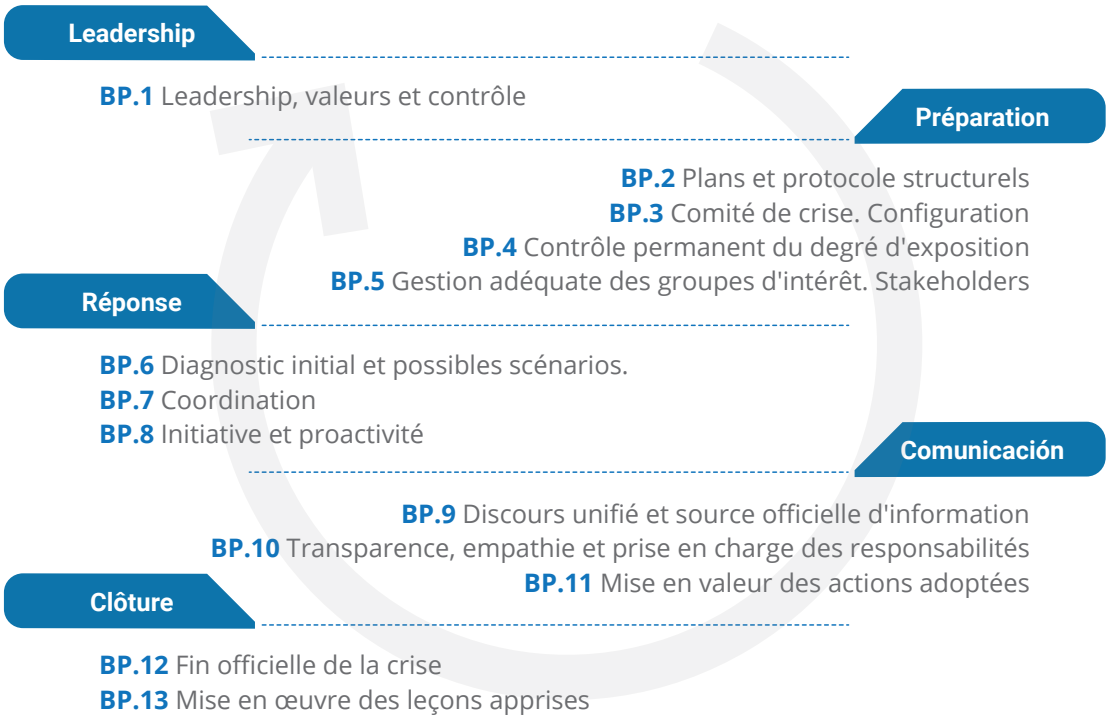


Tableau 3. Résumé des bonnes pratiques

3 Ce décalogue de bonnes pratiques vient d'une adaptation de la publication de l'Institut Cerdà « Monographie 4. Bonnes pratiques dans la gestion de crise " de décembre 2018

3. Cas d'étude

Afin d'illustrer concrètement les bonnes pratiques détaillées aux points suivants, les Annexes 1, 2 et 3 présentent des exemples didactiques en matière de cyber-crise, résumant les recommandations du CCN-CERT face à ce type de situations. Bien que ces bonnes pratiques soient communes pour tous les cas de gestion de cyber-crise, toutes les crises provoquées par des cyber-incidents n'exigent pas le même type d'actions.

Cas d'étude permettent de montrer de manière pratique les principales actions à effectuer face aux situations concrètes détaillées.

1

Cyber-espionnage :

cette annexe explique les points dont la prise en compte est nécessaire pour la gestion de cyber-crise face à un cas de cyber-espionnage.

2

Ransomware :

cette annexe explique les points dont la prise en compte est nécessaire dans la gestion de cyber-crise provoquée par une attaque ciblée via un malware du type ransomware.

3

Extorsion et soustraction de fonds:

cette annexe explique les points dont la prise en compte est nécessaire dans une gestion de cyber-crise face à de éventuelles attaques destinées à l'extorsion et à la soustraction de fonds de la victime.

4

Résumé des principales conclusions

4. Bonnes pratiques dans la gestion de crise concernant des cyber-incidents

BP.1 Leadership, valeurs et contrôle

Il est important de diriger, prendre et conserver l'initiative pendant la crise et, en cas de perte de l'initiative, chercher les opportunités permettant de la récupérer. Il est presque toujours mieux de prendre des mesures raisonnables que de ne rien faire ; **cependant grâce à une préparation et un Plan préalablement** tracé, il sera plus facile d'adopter les mesures pertinentes dans une brève période de temps (généralement habituel dans ces situations) s'il y a un travail préalable que s'il n'y en a pas. L'on évitera ainsi de tomber dans la nervosité ou dans l'improvisation, omniprésents à ce moment.

Dans le cas des cyber-incidents, la fonction de Responsable de Sécurité de l'Information est fondamentale. Ce sera le premier à catégoriser l'événement et la pertinence de convoquer ou non le Comité de Crise.

D'autre part, si avant une crise, les organisations se sont fait une **réputation** reposant sur des valeurs explicites qu'elles ont respectées pendant toute leur activité, elles dépasseront en confiance, en crédibilité et en capacité d'empathie celles qui ne l'ont pas fait. Peu importe la taille de l'organisation, si son histoire se base sur des principes moraux et professionnels, il lui sera beaucoup plus simple de gagner la confiance de tous ses groupes d'intérêt et, donc, de surmonter la situation.

La prise de décisions doit partir des dirigeants qui sont les seuls ayant la capacité d'assurer les ressources matérielles et humaines nécessaires, ainsi que des différents niveaux de prise de décisions. Dans le cas des cyber-incidents, la fonction de **Responsable de Sécurité de l'Information** est fondamentale. Ce sera le premier à catégoriser l'événement et la pertinence de convoquer ou non le **Comité de Crise**, en assumant que sa notification rapide profite non seulement à l'organisation elle-même, mais aussi qu'elle aboutit à un accroissement de la sécurité générale, du secteur et du pays, et sa concrétisation est donc un engagement moral face à la société.

BP.2 Plans et protocoles structurels

Les crises se préparent en temps normaux. Tout ce qui n'est pas prévu à ce moment est pratiquement impossible à improviser pendant l'urgence. Il est vrai que la prévention parfaite est pratiquement impossible : le risque zéro n'existe pas ; mais l'une des clés pour une gestion effective de la crise est la capacité **d'anticipation et d'identification des domaines les plus vulnérables** (**gestion de risques**) qui peuvent arriver à se transformer en situations critiques. L'identification de ces risques potentiels dans l'activité sera clef pour savoir répondre le cas échéant et en réduire l'impact le plus possible.

Les crises se préparent en temps normaux.

De ce point de vue, les cyber-menaces exigent un **exercice constant de prospectives** afin d'avoir conscience des faiblesses de l'organisation et, ainsi, pouvoir s'y préparer et les anticiper.

De nombreuses analyses de crise permettent de constater que le principal problème est que **le risque qui l'a causée n'avait pas été prévu** et qu'il n'existait donc pas de planification rigoureuse pour le gérer, laissant l'organisation dans un état de vulnérabilité permanente.

Dans ce sens, de nombreuses organisations (reprises, par exemple, dans les standard internationaux comme ISO 27001 et 22301 pour l'implantation d'un SGSI[4]) établissent des **Plans de Gestion de Crise**, en suivant diverses méthodologies comme celle de BCM[5], qui indique les missions nécessaires permettant de pouvoir gérer une crise et d'identifier les principales actions à exécuter afin de répondre à une situation grave ou à une catastrophe. Ces plans comprennent généralement un **Manuel de Crise** servant le cas échéant d'environnement de référence, disposant d'un scénario des actions à réaliser en matière de continuité, de contingence, de communication, de ressources humaines, etc., et attribuant clairement les responsabilités.

Ces Plans doivent être convenablement diffusés au sein de l'organisation et de ses responsables en utilisant des exercices ou des sessions de formation spécifiques.

4 Système de Gestion de la Sécurité de l'Information qui reprend un ensemble de politiques, de procédures et de directives pour une protection correcte des actifs de l'information de toute organisation.
5 De l'Anglais *Business Continuity Management* (BCM), un programme intégral qui incorpore la continuité de l'activité, la récupération en cas de catastrophes et la gestion de crise.

Un **Comité de Crise** doit être l'organe décisoire maximal pour la gestion unifiée d'une situation de crise et il devra préalablement être défini. Sa mission principale sera d'accélérer le processus de prise de décisions pour résoudre des incidences, en définissant les priorités, en établissant la stratégie et la tactique à suivre. Il devra décider des principaux scénarios à prévoir, comment agir et comment contrer, en dirigeant toutes les équipes de récupération et de communication.

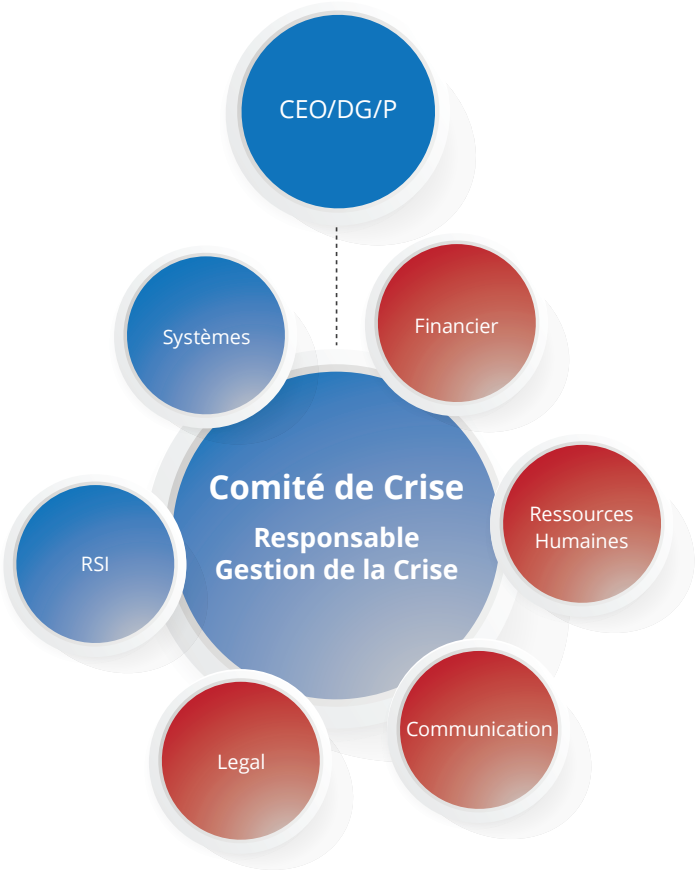


Tableau 4.Comité de Crise

Il doit être composé d'un petit groupe de personnes de différents profils exécutifs et très décisifs, ayant une capacité de réaction face à des situations de stress et d'initiative en matière de direction des équipes et de prise de décisions. Il sera dirigé par le Responsable du Comité de Crise, figure dotée d'une capacité de décision maximale (CEO de l'entreprise ou le plus haut responsable de l'organisme, pour le secteur public). Ce groupe devrait représenter chacun des secteurs de base d'une organisation : Responsables de Sécurité de l'Information (RSI), Infrastructure, Processus, Ressources Humaines, Légal et Communication. En effet, la gestion d'une crise, bien que son origine soit un cyber-incident, n'est pas le fait exclusif de l'équipe de sécurité, mais elle implique toute l'organisation.

C'est ce Comité qui décidera si l'on se trouve face à une crise ou non, son niveau ou son degré (en fonction des niveaux préalablement prévus), l'établissement des mesures et le partage des responsabilités, ainsi que les différents niveaux de comités, avec leurs différents responsables dans chaque cas ; il décidera de l'aspect opérationnel qui doit limiter et résoudre l'incident, jusqu'à la coordination et la communication qui veillera à la réputation de l'organisation, il établira la politique d'information, avec les messages les plus appropriés et les canaux pertinents.

CEO/DG/P	Légal	RSI	Communication	Financier	Ressources Humaines	Systèmes
Il lance la gestion de crise et préside le Comité de crise Il délègue les responsabilités Il est constamment informé Il agit comme porte-parole si les circonstances l'exigent	Il décide de la responsabilité légale directe provoquée par l'incident Il effectue le suivi des actions à réaliser en fonction des Lois applicables Il oriente sur toutes les questions légales	C'est le premier à prendre connaissance de l'incident et il doit décider s'il est nécessaire d'en informer ou non le Comité de Crise Il notifie immédiatement le CERT de référence Il décide des premières actions opérationnelles pour l'atténuation	Il intègre le Comité de Crise et adopte le Manuel de Communication de Crise préalablement élaboré Il décide des messages clefs, du format et du canal les plus appropriés, en fonction des groupes d'intérêt Il active le suivi et la répercussion de la crise dans les différents moyens de communication et les réseaux sociaux. Il maintient le contact avec les médias	Il analyse les fonds nécessaires pour la résolution de la crise Il recueille l'information, évalue les faits, et propose des options Il maintient la communication avec les compagnies d'assurances	Porte-parole face aux employés et, le cas échéant, aux représentants des travailleurs. Il communique, le cas échéant, avec les affectés et leur fournit l'information ou l'assistance de base Il évalue l'état d'esprit des employés et recommande des actions permettant d'éviter leur démotivation ou une évolution non prévue	Il garantira la continuité du service en utilisant, le cas échéant, un centre alternatif opérant les services critiques Il révisera l'environnement commun à toutes les applications (communications, firewall, DNS, etc.), ainsi que celles spécifiques à chaque application. Il engagera rapidement des serveurs virtuels en cas de besoin Politique de copies de sécurité

Tableau 5. Le comité de crise et ses responsabilités

Du point de vue opérationnel, il convient d'espérer qu'en fonction du niveau du cyber-incident établi sur la base des critères de danger et d'impact, le Comité de gestion approprié ait été préalablement créé.

À titre d'orientation et bien que cela dépende de la taille et des capacités de l'organisation, voici un schéma de gestion.

Dangers Faible et Moyen	**Équipes de niveau opérationnel (*bronze*)**
Dangers Élevé et très Élevé	**Comité de Crise (*silver*)**
Danger Critique	**Comité de Crise stratégique (*gold*)**

Tableau 6. Comité de Crise selon le Niveaul

En réalité, les incidents de danger faible et moyen ne devraient pas requérir la convocation d'un comité de crise, parce que nous ne nous trouvons pas face à une situation pouvant être définie comme telle. Sous la responsabilité directe du RSI, les équipes techniques disposent des connaissances suffisantes pour résoudre le problème d'un point de vue opérationnel.

Cette configuration de comités n'est pas exclusive, la constitution de l'un des niveaux supérieurs implique, en général, le maintien de l'activité des niveaux antérieurs. C'est-à-dire, lors d'une cyber-attaque de catégorie critique, c'est le sommet de l'organisation (Administrateur/ice Délégué/e, Direction Générale et membres préalablement désignés) qui prendra les décisions finales dans le Comité *gold* selon les contributions, et le comité *silver*, composé -par exemple- par des représentants des directions fonctionnelles et avec probablement plus d'une équipe bronze travaillant sur des aspects opérationnels, très spécialisés et concrets. En revanche, d'autres cyber-incidents requerront seulement l'intervention d'un comité *bronze* peut-être avec une implication ponctuelle du comité *silver*.

Si l'organisation est grande, la dimension et la complexité normalement associées à ses opérations justifient en soi l'existence des différents niveaux de comités mentionnés, alors que de petites ou moyennes entreprises disposeront d'un seul Comité de Crise.

En ce sens, la décision concernant le niveau de l'organisation et de la structure qui doit assumer la gestion est également un élément à prendre en compte pour décider du niveau de l'incident/crise (voir tableau).

Établi / origine	Attribut	Niveau 1 FAIBLE	Niveau 2 MOYEN	Niveau 3 ÉLEVÉ	Niveau 4 TRÈS ÉLEVÉ	Niveau 5 CRITIQUE
Autres attributs de Gestion de Crise	Déclaration de crise	Non	Non	Oui, niveau Élevé	Oui, niveau Très Élevé	Oui, niveau Critique
	Cadre de gestion / gouvernement de la crise	Ne requiert pas de comité de crise RSI / Équipe de réponse incident	Requiert Comité de Crise / BRONZE TEAM	Requiert Comité de Crise / SILVER TEAM	Requiert Comité de Crise / SILVER TEAM	Requiert Comité de Crise / GOLD TEAM

Tableau 7. Critères de gestion

BP.4 Contrôle permanent du degré d'exposition

Un élément clef dans la gestion de crise est de tester constamment les plans, les procédures et les configurations conçues.

Un élément clef dans la gestion de crise est de tester constamment les plans, les procédures et les configurations conçues. Cela doit se faire à travers des initiatives pour l'évaluation du degré d'exposition des organismes, en identifiant les vulnérabilités associées à leurs services et leurs applications.

L'objectif essentiel consiste à promouvoir la confiance des citoyens dans l'utilisation des moyens électroniques, tout en promouvant leur utilisation sécurisée si le degré d'exposition à la cyber-menace est mesurable, contrôlé et adapté à l'écosystème en question : secteur public, infrastructures critiques, centres de recherche, universités, secteur santé, etc....

En définitive, le sens commun exige d'être capables de mesurer la sécurité. Si nous mesurons, nous pouvons gérer, et si nous gérons, nous avançons à la recherche d'un équilibre entre les capacités et les fonctionnalités que nous offre la technologie et leur usage sûr.

Il faut également tenir compte du fait que faire face à une crise, c'est essentiellement un exercice de gestion composé d'équipes humaines de différente sorte (intervention physique, allocation de ressources, communication interne et externe, gestion de stakeholders, coordination, etc.) et que, pour qu'une équipe fonctionne correctement à un moment d'exigence maximale, elle doit être bien formée. Il est donc recommandable d'effectuer périodiquement des **simulacres** de différents types (opérationnels ou de bureau) qui soumettent les participants aux situations de gestion que leur imposera très probablement la crise afin que, dans un environnement d'incidence simulée, l'équipe s'exerce et apporte toute sorte d'améliorations pour les rendre disponibles dans une situation réelle.

BP.5 Gestion appropriée des groupes d'intérêt. Stakeholders

Les groupes d'intérêt ou ***stakeholders*** : ce sont des personnes ou des groupes de l'environnement de l'organisation qui peuvent se voir affectés par toute activité effectuée par celle-ci. Pendant une cyber-crise, il est très probable qu'il y ait une interaction avec l'un d'eux, partie active de la situation, et qui est même une partie au moins aussi affectée que l'organisation elle-même.

Il est donc conseillé de développer ce que l'on appelle « **Carte des *stakeholders*** » où les différents niveaux hiérarchiques de l'organisation doivent identifier qui peut se voir affecté par la crise.

La vision traditionnelle des groupes d'intérêt comprend les clients, les fournisseurs et les pouvoirs publics, outre les propres actionnaires (*shareholders*). De nos jours -et, une fois encore, suite à l'ubiquité des possibilités de communication et du poids de l'opinion publique-, des groupes additionnels doivent être prévus en fonction de trois grands secteurs et, évidemment, en fonction de l'activité de l'organisation:

Groupes

- **Internes** ..... *miembros del Consejo de Administración/accionistas, empleados actuales y anteriores por categorías y departamentos; familiares y representantes sindicales.*
- **Externes** ..... *autorités et gouvernements, organismes régulateurs et de surveillance, le CERT ou le CSIRT[6] de référence, l'Agence de Protection de Données espagnole, les clients, les fournisseurs, les patients, le public en général, les investisseurs, les compagnies d'assurances, les associations, la concurrence, les influenceurs, etc.*
- **Moyens de communication** ..... *en incluant les moyens traditionnels et online (réseaux sociaux, blogs, etc).*

En fonction de l'incident, il faudra réviser tous les groupes d'intérêt, leurs attentes et la stratégie à suivre avec chacun d'eux.

Dans le cas concret des cyber-incidents l'on voit **l'importance fondamentale** des Groupes d'Intervention à des Incidents de Sécurité : le **CERT**, qui apporte des services d'assistance et de gestion face à ce type d'événements. Dans certains cas, et en fonction du danger ou de son impact sur l'organisation, la notification au CERT de référence est obligatoire. Par exemple, en Espagne, tous ces incidents catalogués, dans le Secteur Public, de danger Élevé, Très Élevé ou Critique[7], doivent être notifiés au CCN-CERT, du Centre Cryptologique National. Cette classification est

6 CERT (Computer Emergency Response Team) et CISRT (Computer Security Incident Response Team) sont des termes employés pour se référer au même type d'Équipes ou de Capacités. Le terme CERT est enregistré par CERT Coordination Center (CERT/CC) et il est donc nécessaire d'avoir son autorisation pour l'utiliser.
7 Sur une échelle de cinq valeurs : Bas, Moyen, Elevé, Très Elevé et Critique.

effectuée en fonction de différents critères comme le type de menace, son origine, les systèmes et les utilisateurs affectés ou l'impact que peut avoir l'incident sur l'organisation[8].

Au-delà de cette notification, il est **indispensable d'avoir conscience de sa disponibilité** et de sa **fonction responsable de la sécurité de l'information**, aussi bien au niveau de l'entreprise individuelle qu'à celui du tissu organisationnel et institutionnel du pays.

Il faut tenir compte du fait que la mission des CERT est de se constituer comme **ressource permanente de cyber-sécurité**, et les connaissances et les moyens d'action dont ils disposent sont constamment **mis à jour**.

Dans ce contexte, un autre groupe d'intérêt fondamental est l'**Autorité compétente** qui gère la cyber-sécurité au niveau national. Tel que commenté dans la BP7 sur la Coordination, dans certaines situations l'organisation a l'obligation de notifier l'incident. Pour cette raison, une bonne pratique de cette communication consiste à avoir prévu l'organisme pertinent, l'information à apporter, etc.

Une autre question concerne l'affecte pour l'organisation d'un cyber-incident qui génère une crise chez un fournisseur important. La dépendance de la chaîne d'approvisionnement doit être étudiée et, dans certains cas, il convient d'exiger des certifications ou des garanties des fournisseurs concernant leur protection face à des cyber-attaques. Le tableau 3 résume les stratégies génériques de gestion de fournisseurs en matière de cyber-sécurité.

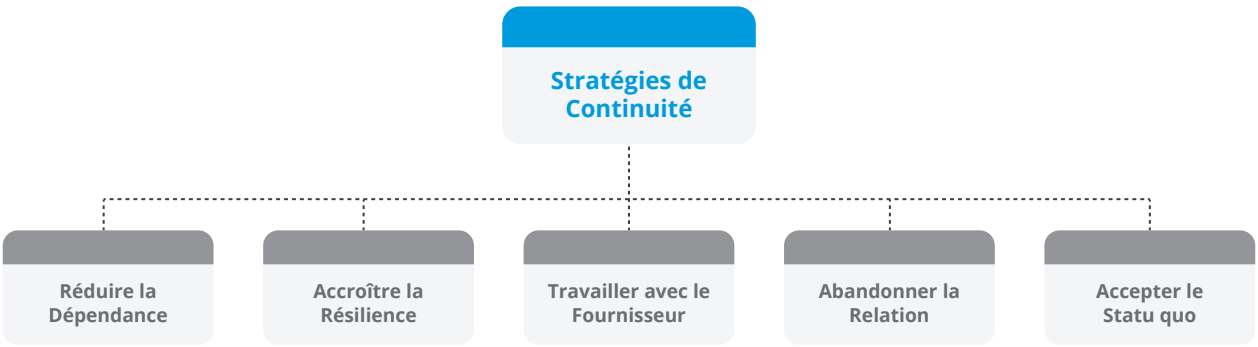


Tableau 8. Stratégies de continuité dans la chaîne d'approvisionnement

8 Voir : Classification/Taxonomie des cyber-incidents. Guide CCN-STIC 817 Gestion de Cyber-incidents (ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-cyberincidentes/file.html)

BP.6 Diagnostic initial et scénarios possibles

La première étape dans la gestion puis la résolution d'une cyber-crise consiste à réaliser un **diagnostic**[9] dde ce qui se passe. Dans l'analyse de crises réelles, l'on observe très souvent que, ne disposant pas d'un diagnostic initial, l'organisation présente un comportement erratique pendant l'urgence, elle perd l'initiative, elle prend du retard par rapport aux événements et elle subit une perte de réputation claire.

Bien qu'aux premiers moments de la crise, l'information soit souvent confuse et incomplète, il est très important de comprendre ce qui se passe et ses dysfonctionnements éventuels à court et moyen terme (scénarios possibles). Cet exercice permet de **prioriser des actions et de prendre les premières décisions** ; et au fur et à mesure que l'on dispose d'informations, l'on affinera le processus.

En phase de diagnostic, il est en outre absolument nécessaire de classer la crise en cours en fonction de la gravité de l'impact perçu et possible afin de pouvoir anticiper des décisions de gestion postérieures. Pour cela, il est indispensable de **définir préalablement un schéma de classification et de changement d'échelle d'incidents**. Ce schéma doit inclure des niveaux de gravité et d'impact, ainsi que les critères d'évaluation et de classification à utiliser.

L'Annexe 4 présente un exemple de **critères d'évaluation et de classification** qui peut servir d'inspiration à cet effet, en prenant comme point de départ les critères établis pour la classification du Niveau de danger et du Niveau d'impact potentiel du Guide de Sécurité des TIC CCN-STIC 817 et du Guide National de Notification et de Gestion de Cyber-incidents[10], auxquels est ajoutée la suggestion d'autres concepts possibles à étudier afin d'aider à discerner la nature de la crise et la pertinence d'activer le comité de crise respectif.

Ce premier diagnostic doit inclure la **notification initiale au CERT** de référence pour recevoir une aide adaptée au problème, des indications d'action spécifiques, des outils de diagnostic et des opérations complémentaires et de mise à jour. Tout cela permet une réaction rapide qui viendra souvent totalement à bout de l'attaque ou en limitera fortement les impacts sur l'organisation et sur le tissu entrepreneurial affecté.

Selon la nature de l'organisation affectée et le type d'incident, il peut exister une obligation d'effectuer cette notification[11]. dans ce cas les autorités compétentes pourront demander toute l'information qu'elles considèreront nécessaire sur l'incident pour le résoudre et minimiser son impact sur la sécurité nationale[12].

9 Si possible, cela est idéal, mais le plus important est de le faire car il représente un exercice prospectif qui permet d'anticiper des champs d'action que la simple analyse du problème à traiter ne facilite pas.
10 Guide National de Notification et de Gestion de Cyber-incidents et le Guide CCN-STIC 817 déjà cité
11 Par la Directive NIS, l'ordre juridique espagnol est transposé par le décret-Loi royal 12/2018, du 7 septembre, pour les Opérateurs de Services Essentiels, ou la RGPD en cas de vol de données.
12 Dans certains cas, au vu de la gravité ou de la situation médiatique du cyber-incident, la Commission Permanente de Cyber-sécurité a été activée, en tant qu'organe suprême au niveau national où sont traités certains cyber-incidents .

BP.7 Coordination

La coordination est la clé de la bonne résolution d'une cyber-crise. Même des organisations qui ont été correctement préparées pour aborder une situation grave de ce type ont tendance à improviser. Et l'improvisation et le manque de coordination sont les ingrédients d'une recette pour l'échec.

Le fait de disposer d'un Comité de Crise tel que précédemment indiqué, avec expérience et capacité de gestion, est donc l'une des premières étapes essentielles à suivre pendant une crise, parce que ce sont les personnes qui assumeront et assigneront des responsabilités, des compétences et des ressources pour résoudre le problème.

Cette coordination est indispensable dans la prise de décisions et leur exécution, ainsi que dans les missions de communication, et la figure de porte-parole de ce Comité est donc très importante.

Dans l'action la plus opérationnelle, apparaît comme fondamentale la figure du Responsable de Sécurité de l'Information (RSI) étant donné que c'est sur elle que pivotera cette coordination en tant que point de contact des équipes opérationnelles d'action (*bronze*[13]), le **Comité de Crise** (*silver* o *gold*) et le **CERT de référence**.

Dans ce contexte, il est par ailleurs important de mentionner que les cyber-crises impliquent souvent la perte d'informations confidentielles dont la gestion est soumise au Règlement Général de Protection de Données (RGPD). Il s'agit donc d'une bonne pratique qui, dans la résolution de la crise, outre le RSI, inclut également directement la figure du **Responsable du Traitement** de Données qui fait partie du Comité de Crise pour garantir que l'information confidentielle reçoit le traitement approprié tout en assurant une bonne coordination avec le reste des membres.

Cette coordination est fortement conditionnée par des particularités telles que:

Aspects

- *Les valeurs de l'organisation et sa culture, c'est-à-dire, que ces valeurs soient partagées.*
- *Le travail préalable effectué pour identifier des risques et décider des plans d'action, comprenant forcément les besoin de coordination.*
- *Le degré d'expérience du comité et sa bonne dynamique d'équipe.*
- *L'existence d'une relation mûre avec les stakeholders, afin de faciliter les missions de coordination avec les différents agents de la crise.*

On observe donc que **la gestion de crise est une discipline holistique** qui va au-delà de l'existence d'outils et de ressources spécifiques (manuel de crise, comités...) et qui pivote autour d'une **conscience du cyber-risque** et d'une **culture générale de couverture** de celui-ci et d'autres risques identifiés.

13 Voir Annexe 6 pour les définitions sur les types de comités.

BP.8 Initiative et proactivité

L'analyse de la grande variété de cyber-crises permet d'observer que la cyber-attaque trouve souvent dans l'organisation un manque d'attention à changer de priorité au quotidien face à la crise. Son diagnostic n'est pas bon et elle perd un temps initial qui, d'une part, donne un avantage aux agresseurs en n'assurant pas **l'intervention rapide du CERT** et, d'autre part, prend du retard par rapport aux événements.

Il en résulte l'adoption d'une **politique essentiellement** réactive, plus occupée à répondre aux critiques ou aux pressions reçues de l'environnement de travail qu'à définir et communiquer la stratégie adoptée pour résoudre la situation.

C'est la raison pour laquelle il est si important, face à un premier avertissement de crise, que l'organisation **réagisse avec rapidité et avec force** en effectuant une **notification initiale sans prendre de retard** et en prenant l'initiative. Il s'agit donc que l'organisation soit pro-active et non pas réactive, qu'elle prenne ses décisions rapidement et qu'elle se positionne en vue de diriger la gestion de la crise.

Un aspect qui démontre l'initiative et la proactivité face aux cyber-risques est le fait que face à une cyber-attaque, l'organisation -en cas de manque de ressources propres- ait prévu à l'avance l'intervention rapide d'une entreprise de services spécialisée. L'action de cette entreprise, en coordination avec le CERT de référence qui connaîtra les systèmes et les protections de l'organisation, permettra ainsi une action très rapide, ce qui est indispensable dans ce type de situations.

Tel que commenté dans la BP-7 sur la coordination, l'inclusion dans les actions de la connaissance spécialisée du CERT facilite la prise de conscience et la proactivité. Tout cela est clairement illustré dans les cas décrits en annexe.

BP.8

BP.9 Discours unifié et source officielle d'information

Après avoir considéré qu'un incident est passé à la catégorie de crise, il est fondamental d'élaborer les informations les plus pertinentes en tenant compte du facteur temps, du degré de priorité et du groupe d'intérêt (stakeholder). En fonction de ces deux paramètres, et suivant les conseils du secteur de la Communication, l'on définira le type d'information à offrir, les messages clefs, le format et le canal ou les moyens (réunions informelles, vidéo-conférences, courriers électroniques, listes de distribution, appels, interventions présentielles, discours, ensemble d'actionnaires, *Dark Site*[14], messagerie de type WhatsApp ou Telegram, etc.)

Il ne faut pas oublier que le mieux, dans une crise, c'est que la principale source de renseignements vienne de l'**organisation elle-même**. Pour cela, il est indispensable que l'entreprise soit pro-active et qu'elle prenne l'initiative, mais sans se précipiter. En outre, il est très important que le Comité de Crise fixe des messages clairs que personne dans l'organisation ne devrait enfreindre. Quel que soit le format et le canal choisis, l'information sera donc la même, sans contradictions.

Lo mejor que puede pasar en una crisis, es que la principal fuente de información sea la propia organización.

Groupe d'intérêt	Priorité	Temps	Messages clef	Format	Canal/-moyen
Internes, externes et/ou moyens de communication	Élevée, Moyenne, Basse	1 h., 2 h. 3 h	X, Y, Z	Communiqué de presse, notification, courrier électronique, avis, vidéo, rapport, lettres personnalisées…	Portable, sites web du Dark Web, liste de distribution, messagerie, Réseaux sociaux, conférence de presse…

Tableau 9. Modèle d'exemple de planification de la communication de crise[15]

14 Site web créé face à l'irruption d'une crise éventuelle, susceptible de nuire à l'image et à la réputation d'une organisation, mais qui n'est pas visible publiquement jusqu'à ce que se présente une difficulté dans laquelle l'on décide de mettre online. Ses objectifs sont :
- Être prêt à réagir immédiatement en cas de crise.
- Protéger et maintenir le fonctionnement normal du site web de l'organisation.
Disposer d'un site auquel peuvent s'adresser tous les publics partie prenante d'une crise (comme journalistes, autorités, membres de la famille).

15 Carles Montaña, « Atelier de Communication de Crise ». Escuela de Periodismo UAM-El País

Ces messages doivent comporter les caractéristiques suivantes:

- *Ne jamais refuser la réalité. Ne jamais mentir, être transparent*
- *Toujours donner la version de l'organisation, en se présentant comme la source d'information la plus crédible et la plus précise*
- *Transmettre la confiance. Agir avec sérénité, fermeté et professionnalisme*
- *Démontrer d soin, du respect et un engagement total envers toutes les personnes ou entités concernées*
- *Présenter des excuses et, si besoin, assumer les responsabilités (ne pas accuser autrui)*
- *Mettre en valeur toutes les actions*
- *Assurer que l'activité/l'entreprise est viable*

Proactividad y discurso unificado

Proactivité et discours unifié sont donc des éléments très importants de la politique de communication qui doivent tenir compte de l'information externe (moyens de communication, web, réseaux sociaux, etc.), et cette unicité de message doit également être pratiquée en interne, vers le personnel lui-même, les fournisseurs et/ou les clients. Il faut bien se souvenir qu'en cas de crise, tout employé de l'entreprise peut agir -volontairement ou involontairement- comme source d'information sur ce qui se passe.

Pour ce qui est des cyber-incidents, il faut tenir particulièrement compte du besoin d'**équilibre entre une communication externe transparente** -qui peut signaler aux agresseurs que l'attaque a été découverte et que l'on agit, aspect qui n'est peut-être pas nécessaire en un premier temps-, et le fait de **partager rapidement avec le CERT de référence** ce qui, à son tour, sera coordonné avec d'autres organisations et instances gouvernementales nationales et internationales.

Il est donc important de concevoir un **discours unique** tout en modulant le rythme et la cadence de communication.

BP.10 Transparence, empathie et prise en charge des responsabilités

Tel que mentionné, le mensonge, la narration mensongère des faits, le mutisme ou la passivité sont les pires options en matière de communication en cas de cyber-incident. Pour protéger la réputation de l'organisation, il faut éviter l'incertitude. Cette attitude est également importante pour une notification rapide au CERT de référence, étant donné qu'il en résulte un bénéfice global.

En général, une société expérimentée accepte que, dans une organisation, les choses ne fonctionnent pas toujours comme on le voudrait, et que des impondérables peuvent se présenter. Ce que l'on ne comprend pas, et que l'on n'accepte pas, c'est que ses responsables ne réagissent pas à temps ou qu'ils ne le fassent pas bien.

Il n'est pas facile de maintenir la transparence pendant une crise, mais les dommages peuvent être compensés ou minimisés par l'adoption d'un **politique transparente et responsable** qui, même si à court terme elle peut favoriser les critiques, à long terme elle améliore la crédibilité et la réputation de l'organisation.

Cette approche ne signifie pas qu'il faille prendre absolument tout en compte. En règle générale, il est nécessaire de gagner du temps jusqu'à parvenir à mieux connaître la portée de la situation. L'on évitera donc de mentionner les causes de l'incident, son responsable, les données que l'enquête peut révéler ou les éventuelles conséquences pour l'organisation ou pour un autre groupe d'intérêt.

L'on évitera donc de mentionner les causes de l'incident, son responsable, les données que l'enquête peut révéler ou les éventuelles conséquences pour l'organisation ou pour un autre groupe d'intérêt.

BP.10

BP.11 Mise en valeur des actions adoptées

En période de crise, malgré un travail intense et de nombreuses actions simultanées réalisées, l'on ne dispose souvent pas de résultats présentables à l'opinion publique et aux groupes d'intérêt.

Dans un contexte comme celui précédemment décrit de proactivité et de transparence, c'est le bon moment pour mettre en valeur toutes les mesures prises jusqu'à présent par l'organisation, préventives (coordination avec le CERT et d'autres institutions, développement de plans préalablement conçus, investissement dans des ressources), ou correctives (équipes d'intervention, comités de crise, sous-traitances, exécution de contrats, révision de protocoles, etc).

L'on transmet ainsi un multiple message:

Mensaje múltiple

L'organisation se préoccupe de son environnement immédiat et de ses groupes d'intérêt, elle s'est préparée à l'avance, elle dispose des protocoles d'action, d'un comité de crise, etc.

Bien que ne disposant pas encore de résultats concrets, elle fait tout ce qui est possible pour les obtenir en déployant des moyens et des ressources, tel que planifié.

Elle travaille en étroite collaboration avec d'autres organismes, institutions ou autorités pour la résolution rapide.

L'entreprise fait donc tout ce qui est possible pour résoudre la situation et, dans ces conditions, elle y parviendra sans doute.

En résumé, **toute crise offre une occasion** de démontrer la capacité de l'organisation à résoudre une situation complexe, en montrant que la gestion de l'événement disruptif est appropriée.

BP.11

BP.12 Cierre formal de la crisis

La crise ne prend pas fin avec la Crise. Le stress quotidien empêche souvent de clôturer ces événements de la meilleure façon. La principale pratique pour une bonne fin consiste à consacrer du temps et des ressources pour évaluer les dommages et, surtout, collecter les **leçons apprises** et les mettre en œuvre au sein de l'organisation, et en communiquer la fin, à niveau interne et externe.

La réalisation d'**analyses pertinentes**, les **conclusions**, la **définition d'un plan d'action** et le **suivi de sa mise en œuvre** sont donc des étapes indispensables dans la clôture de la cyber-crise et on ne les fait souvent qu'à moitié.

La communication ultérieure sur les activités réalisées et sur la fin officielle de l'épisode est une bonne manière de transmettre le message qui **a été appris de ce qui s'est passé**, et de faire savoir, aux *stakeholders* et à l'opinion publique en général, que l'organisation est mieux préparée pour l'avenir. C'est également un bon moment pour **exprimer sa gratitude** à toute personne ou institution ayant collaboré à la résolution de la situation.

Cette communication est seulement pertinente face à l'extérieur, mais il convient également, en parallèle, de la faire **en interne**. L'on envoie ainsi les messages de remerciement pour la mission accomplie et pour l'importance d'être préparés face à des situations de ce genre, ce qui renforce l'état d'alerte des membres de l'organisation.

La crise ne prend pas fin avec la Crise.

BP.12

BP.13 Mise en œuvre des leçons apprises

Cette bonne pratique est très similaire à la précédente et, de fait, elle en est une extension. De toute façon, l'on veut souligner le besoin de faire l'effort de résumer de ce qui s'est passé en le synthétisant dans les **actions concrètes à mettre en œuvre**. Tel qu'indiqué, le quotidien complique souvent une analyse détaillée, et l'adoption immédiate des mesures les plus urgentes et nécessaires peut faire penser que l'on a déjà tiré des conclusions de ce qui s'est passé et que l'on a agi en conséquence.

Cette attitude est une réaction très superficielle ; il est nécessaire de réaliser une analyse en profondeur et des **plans d'amélioration aux objectifs concrets et à l'évolution mesurable**, et de ne pas se satisfaire des relations de cause à effet les plus immédiates (par exemple, « il s'est agi d'une erreur humaine », mais pourquoi la personne s'est-elle trompée ?) tout en cherchant les **origines systémiques** du problème que l'on peut comparer aux législations existantes (alors, doit-on simplement aller au-delà des règlementations ? Faut-il chercher de nouvelles collaborations avec le régulateur ?), en abandonnant les bonnes pratiques (pourquoi a-t-on cessé de le faire ?), avec de mauvaises structures de communication (pourquoi ne nous sommes-nous pas compris ? Pourquoi ne nous sommes-nous pas correctement expliqués?), etc.

Le fait de ne pas se limiter aux **simples explications** est une caractéristique qui fait partie des valeurs d'une organisation résiliente et c'est également une condition nécessaire pour parvenir à la résilience.

En résumé, il faut traiter les crises comme une source d'apprentissage en organisation, en parvenant à des conclusions de ce qui s'est passé par l'analyse en profondeur et l'ajustement à ces apprentissages des plans d'action et des futurs investissementsaprendizajes de los planes de acción e inversión futuros.

BP.13

5. CONCLUSIONS ET RECOMMANDATIONS

Les différents cas décrits en annexe reflètent la gestion de crise du point de vue du CCN-CERT afin de visualiser très clairement comment aborder une cyber-crise et l'importance de disposer d'un support technologique approprié.

En synthèse de ce qui est exposé dans les cas, l'on aboutit aux **principales conclusions suivantes**:

- Pour gérer une crise hypothétique, il faut l'avoir prévue, disposer d'un Comité de Crise et de différents plans et manuels adaptés, voire d'effectuer des exercices ou des simulacres.

- L'on n'a pas suffisamment conscience de l'importance de la sécurité de l'information dans les organisations, soit par le fait de ne pas en avoir fait une des priorités, soit à cause d'une fausse sensation de sécurité provoquée par la disponibilité des ressources (systèmes et protections) qui résultent insuffisantes.

- Souvent, il n'existe pas une personne assumant clairement la fonction de Responsable de Sécurité de l'Information. Cette fonction, propre ou externe, est indispensable dans le monde actuel.

- Il est fondamental que les cadres supérieurs de l'organisation connaissent la menace en général, son impact éventuel sur le service, et le degré de préparation et, donc, les carences existantes.

- L'investissement en cyber-sécurité doit être une priorité pour les organisations. Malgré la difficulté de calculer son retour sur investissement exact (comme dans tout investissement en sécurité, quel qu'en soit le type), la fréquence de plus en plus élevée des cyber-attaques et leur impact élevé, qui affectent aussi bien le service prêté que la sauvegarde de l'information et la réputation de l'organisation elle-même, le besoin de cet investissement ne laisse aucun doute.

- Dans ce contexte, il convient de disposer de systèmes qui, tout en protégeant, facilitent la gestion face à une attaque (Firewalls, SIEM, EDR), ainsi que la disponibilité de ressources humaines (propres ou externes) pour la supervision permanente du réseau.

- La notification rapide d'une cyber-attaque au CERT de référence apparaît comme une étape fondamentale pour résoudre l'incident et minimiser son impact.

- La formation et la prise de conscience du personnel de l'organisation sont primordiales. De nombreuses attaques sont évitées si le personnel qui travaille avec des moyens informatiques est conscient des risques inhérents et des menaces qui affectent l'organisation.

- La communication est un facteur clef pour une bonne gestion de crise. Il faut avoir identifié préalablement tous les groupes d'intérêt ou stakeholders auxquels il faut savoir quoi dire et comment le faire à tout moment. Il faut pour cela un discours partagé unique de la part des différents membres de l'organisation, présentant une transparence totale tout en assumant des responsabilités si besoin et présentant les actions réalisées.

- Le facteur « sécurité de l'information » doit être pris en compte dans toute stratégie adoptée par l'organisation. L'adoption massive du télétravail pendant la crise du Covid-19 en est un exemple, car tout le monde n'a pas tenu compte de ce risque en travaillant depuis chez soi. Ceci a augmenté l'incidence de la menace.

Annexe 1.
Cas d'étude de Cyber-espionnage

LLa situation géopolitique des dernières années montre une tendance croissante des opérations de cyber-espionnage. Ces capacités comprennent les groupes appelés APT (menace persistante avancée, de l'Anglais *Advanced Persistent Threat*), incluant du personnel ultra spécialisé, disposant de connaissances techniques importantes et dotés de ressources financières et matérielles importantes, qui effectuent des intrusions dans les réseaux cible pour rester occultes le plus longtemps possible et pouvoir en extraire de l'information. Cette capacité s'adresse aussi bien au secteur public que privé, et elle provient généralement de pays qui souhaitent améliorer leur position au niveau politique, stratégique ou économique.

En définitive, le cyber-espionnage est une cyber-attaque spécifique et ciblée qui essaye d'être le plus discrète possible et rester secrète le plus longtemps possible, contrairement à la cyber-délinquance qui est plus voyante car elle cherche un bénéfice financier à court et moyen terme.

Que se passe-t-il généralement dans ce type de crise

Dans les cas le plus communs, les attaquants envoient des courriers électroniques adressés à des utilisateurs spécifiques pour les duper afin de leur faire ouvrir le fichier joint ou le lien malveillant contenu. Ils parviennent ainsi à infecter l'équipement de l'utilisateur, ce qui leur permet de contrôler la machine à distance et, une fois dans le réseau, ils essaient d'y progresser. Ils exécutent alors des commandes et/ou des outils additionnels avec lesquels ils cherchent à obtenir des accréditations d'utilisateurs avec des privilèges d'administrateur du domaine afin de prendre l'entier contrôle du réseau de l'organisation attaquée.

L'on peut également voir le cas où un groupe APT aurait obtenu des accréditations légitimes d'accès à distance aux systèmes de la victime, comme des VPN ou des sessions de bureau à distance.

Quand l'attaquant est parvenu à pénétrer dans le réseau cible, il effectue des missions de reconnaissance pour détecter l'information qui l'intéresse et chercher à y accéder pour la voler. Cette extraction d'information peut se faire en utilisant le code malveillant avec lequel il a infecté les récepteurs du courrier ou par des voies alternatives, comme le courrier électronique ou les services du cloud dans internet, pour en compliquer la détection.

Normalement, la façon d'agir de l'attaquant rend sa détection très difficile étant donné qu'il cherche à rester longtemps dans le réseau cible afin de pouvoir voler le plus d'informations possible.

Détection de ce type d'attaques

EL'intrusion est souvent communiquée par des tiers à l'organisation. Il est cependant possible que l'intrusion soit détectée par l'organisme et l'organisation victime, qui constate des incohérences ou des comportements étranges du réseau.

Objectif

L'objectif de ce type d'attaque est généralement le vol d'informations, de technologie ou de toute sorte de documentation. Il est important de souligner que l'activité des groupes APT ne se limite pas à attaquer leurs victimes, mais qu'elle compromet également d'autres systèmes pour les utiliser comme partie de son infrastructure d'attaque, soit comme serveurs de commande et de contrôle, soit par connexions et/ou par la gestion.

Que doit faire une organisation dans ce type de situations

Mesures de prévention pour éviter ce type d'attaques:

L'on a généralement observé que, pour pénétrer dans les systèmes, les groupes APT obtiennent les accréditations d'accès via des techniques de phishing ou, de plus en plus, par l'obtention d'accréditations disponibles sur internet et sur le dark web.

Ils y parviennent, en partie, à cause de la mauvaise praxis de réutilisation de mots de passe par les utilisateurs. L'obtention de ces accréditations ne requiert pas d'opérations sophistiquées. En fin de compte, l'erreur humaine prévaut. C'est la raison pour laquelle il s'avère indispensable de mettre en œuvre des politiques robustes incluant le changement périodique des mots de passe, de conscientiser et de sensibiliser les employés d'un organisme ou d'une organisation sur les menaces et procédés principaux qu'utilisent les cyber-attaquants pour parvenir à leurs fins.

La formation et la prise de conscience du personnel de l'organisation est tout aussi indispensable. De nombreuses attaques sont évitées si le personnel qui travaille avec des moyens informatiques est conscient des risques que cela suppose et des menaces qui affectent l'organisation.

Recommandations en phase initiale de gestion de crise

Recommandations

- *Agir rapidement. La notification rapide d'une cyber-attaque au CERT de référence est une étape fondamentale pour la résolution de l'incident et la minimisation de ses impacts. Il convient d'indiquer que ce type d'incidents est généralement classé comme danger Très Élevé et Critique étant donné son impact grave sur l'organisation et, pour ce qui est du Secteur Public espagnol, tel que mentionné, il faut donc obligatoirement le communiquer au CCN-CERT.*
- *Tenir une réunion avec les responsables de la sécurité de l'information.*
- *Informer nécessairement la Direction de l'entreprise, et la tenir informée des progrès de l'enquête.*
- *Réunir le Comité de Crise créé préalablement à cet effet. C'est ce groupe qui doit gérer la situation et appliquer les plans prévus à cet effet.*

Activités réalisées dans la gestion de ce type de crise:

Les premières étapes dans la gestion de ce type de crise consistent à détecter depuis **quand l'attaquant vole les informations** afin d'évaluer la violation commise. L'on prendra ainsi, dans la majorité des cas, les actions suivantes:

Activités

- *L'équipe d'intervention **analysera les logs** disponibles, basiquement ceux des équipements de sécurité périmétrale via les proxy de navigation et les coupe-feu corporatifs. En cela, il est important de tenir compte du fait que de nombreuses organisations effacent fréquemment les logs, et il est possible que l'on ne puisse pas disposer de l'information complète. Il est donc recommandé **d'augmenter la capacité de rétention des logs**. Dans certains cas, les intrusions sont découvertes quand les attaquants sont dans le réseau depuis longtemps, et le fait de disposer de la plus grande quantité possible de logs aide donc à identifier l'origine de l'infection, et à reconstituer les actions des attaquants. **L'équipe de sécurité de l'organisation se charge de faire une révision permanente de ces logs pour détecter des anomalies**.*

    - ***Cette première étape exige, de la part de l'organisation, une communication interne fluide** avec le personnel TIC. Il peut arriver que, pour le déploiement d'outils spécifiques ou pour l'accès aux logs nécessaires des équipements spécifiques, l'équipe d'intervention d'incidents enquêtant sur l'incident ait besoin de l'aide du personnel TIC de l'organisation qui en est victime. À cet effet, et afin de ne pas prolonger les délais, l'organisation en question doit informer ces équipes de la situation et leur communiquer le besoin de remettre l'information demandée et nécessaire pour enquêter rapidement.*

    - *Il sera indispensable de **disposer des schémas et des diagrammes de réseau** qui permettront de découvrir de nouveaux indices en fonction des progrès de l'enquête. Il faut tenir compte du fait que l'analyse du réseau pour voir des mouvements étranges d'information entre ordinateurs prend beaucoup de temps. Il sera également nécessaire d'installer des outils spécifiques.*

*Bien que l'on recommande d'agir rapidement, le **principal défaut d'une organisation face à cette situation serait d'essayer de résoudre la situation trop rapidement**. L'attaquant doit se sentir sûr pour agir normalement. Ce n'est qu'ainsi que l'on pourra obtenir des preuves et savoir jusqu'à quel point il a accès au réseau, et quelles sont les portes dérobées ou les autres mécanismes employés pour se connecter au réseau.*

- *Dans différentes situations de ce type, le CCN-CERT a vérifié la criticité de cet aspect. Si l'attaquant a conscience d'avoir été découvert, il peut décider de cesser temporairement son activité ou d'utiliser d'autres moyens d'accès inconnus de l'équipe d'intervention de l'incident, ce qui complique énormément l'enquête. Le changement d'accréditation pour accéder au courriel, par exemple, n'est pas suffisant pour résoudre un incident de ce type.*

- *Cela débouche sur une situation complexe. D'une part, l'on a besoin de temps pour savoir jusqu'à quel point l'attaquant contrôle le réseau ; d'autre part, le représentant de l'organisme ou de l'organisation veut corriger au plus vite la violation en matière de sécurité.*

- *Sous ce point, il est primordial de **gérer le facteur temps** afin de pouvoir enquêter à fond et savoir jusqu'où est arrivé l'attaquant, sa connaissance du réseau et ses différents plans pour rester à l'intérieur. Il est nécessaire d'installer des outils de suivi et d'avoir le temps d'étudier la situation.*

Une fois connue l'envergure du risque, l'on effectue un plan détaillé d'atténuation, qui doit être approuvé par la Direction.

- *Sur ce point, il faut tenir compte du fait qu'une atténuation très précoce sans temps d'enquête suffisant empêche d'effectuer le nettoyage nécessaire face aux différents plans de l'attaquant.*

- *Le plan d'atténuation doit être le plus radical possible et il doit être exécuté en fin de semaine pour essayer de ne pas affecter le fonctionnement normal de l'organisation. Ainsi, et en général, les systèmes ne se voient pas affectés et les employés ne subissent aucune variation de leur activité. Aucun service n'est en panne et aucun système n'est bloqué.*

- *Cependant, après avoir décidé d'exécuter le plan d'atténuation, les employés devront ensuite changer leurs accréditations d'accès.*

- *La direction peut ne pas approuver le plan d'atténuation et décider de prendre des mesures insuffisantes susceptibles de provoquer une nouvelle attaque à l'avenir, voire que l'attaquant soit encore actif et puisse continuer à accéder au réseau attaqué.*

Apprentissages

Apprentissages

- *Les organisations doivent tenir constamment à jour les schémas et les diagrammes de réseau de l'organisme.*
- *Il ne suffit pas de disposer d'importantes mesures de sécurité dans une organisation. Il faut consacrer des ressources et du personnel pour effectuer un contrôle continu de l'activité suspecte.*
- *Il est important que l'organisation crée une équipe de supervision du réseau qui se transforme en équipe de sécurité de l'information, équipée et financée de façon permanente.*
- *Prise de conscience en matière de cyber-sécurité. Il est fondamental que l'organisation connaisse la menace en général, son impact éventuel sur le service, son degré de préparation, donc, ses carences.*
- *L'investissement en cyber-sécurité doit être une priorité pour les organisations. Malgré la difficulté d'en calculer le retour financier exact (comme dans tout investissement en sécurité, quel qu'en soit le type), au vu de la fréquence de plus en plus élevée des cyber-attaques et de leur impact important qui affecte aussi bien le service prêté que la sauvegarde de l'information et la réputation de l'organisation elle-même, sa réalisation ne doit faire aucun doute.*

Annexe 2.
Cas d'étude, le Ransomware

Le ransomware a été le type de code malveillant le plus destructif au cours de la dernière décennie. Ayant commencé par affecter les ordinateurs personnels, il est devenu l'une des grandes menaces pour les entreprises et pour les infrastructures critiques (hôpitaux, infrastructures énergétiques, etc).

Au cours des dernières années, les capacités de ce malware ont évolué, et, de déchiffrer uniquement des équipements d'utilisateur, elles sont passées à bloquer des réseaux complexes ayant des technologies hétérogènes, présentes dans les grandes entreprises et structures d'un pays.

La popularité de ce type de malware, ainsi que la croissance des variantes, se doit partiellement ce que l'on appelle *Ransomware* as a Service, service qui facilite aux délinquants la création du code malveillant à quelqu'un qui le demande en échange d'un pourcentage des profits obtenus par ce biais.

Au cours des dernières années, des secteurs comme la pharmacie, la finance, ou le commerce, ont été les victimes favorites des groupes de cyber-délinquants, et, en plus de voler et d'exfiltrer l'information, ils provoquent également la disruption des activités en infectant le réseau avec le ransomware. En outre, les attaquants emploient des techniques d'extorsion de fonds après avoir infecté le réseau en vue de monétariser l'attaque, en mettant un prix pour le sauvetage, la non publication de l'information soustraite et/ou le déchiffrement des fichiers affectés par ce code malveillant.

En ce sens, il est important de souligner que le fait de payer à un groupe de délinquants NE GARANTIT PAS à la victime que ses données ne seront pas publiées ou vendues sur le marché noir.

Que se passe-t-il généralement dans ce type de crise

TTraditionnellement, ces types de cyber-délits étaient très bruyants. L'on cherchait un gain à court terme. Toutefois, les grands groupes de cyber-délit agissent actuellement en suivant un *modus operandi* plus sophistiqué qui essaie d'abord de coloniser le réseau, en localisant les éléments vitaux de la victime, en exfiltrant la précieuse information pour une autre extorsion de fonds, puis en déployant le ransomware qui empêche l'accès à l'information.

Detección de este tipo de ataques

Dans la majorité des cas, la victime a conscience d'avoir subi une attaque de ransomware étant donnée l'impossibilité d'accéder à de multiples fichiers depuis plusieurs équipements, ou face à la désactivation de plusieurs de ses services essentiels.

Objectif

Le principal objectif du cyber-délit est de rentabiliser financièrement une infection en suivant plusieurs voies:

- Extorsion directe de fonds à la victime en la menaçant de publier l'information sensible soustraite.
- Perturbation de la disponibilité de l'information et de la prestation de services vitaux chez l'affecté, l'attaquant offrant la clé de déchiffrage de l'information pour pouvoir reconstituer le fonctionnement de l'organisme.

Que doit faire une organisation dans ce type de situations

Mesures de prévention pour éviter ce type d'attaques:

Pour prévoir ce type d'infections, il est généralement recommandé de suivre des politiques de sécurité au niveau du domaine empêchant, par exemple, l'exécution de macros dans des documents de bureautique (principale voie d'infection d'Emotet) et de Powershell dans tous les équipements qui n'en ont pas besoin (limitant ainsi partiellement l'exécution par l'attaquant d'une multitude d'outils)[16].

Il est également recommandé d'établir des politiques au niveau du réseau afin de contrôler de manière granulaire les connexions pouvant être établies entre les différents points et les équipements du réseau, donnant ainsi à l'équipe de sécurité plus de visibilité et de traçabilité de tous les événements générés, en détectant en temps opportun l'activité anormale qui pourrait indiquer un dysfonctionnement ou une intrusion potentielle dans le réseau.

La prise de conscience et la sensibilisation préalable du personnel d'un organisme ou d'une organisation sont également vitales pour éviter le succès de ce type d'attaques.

Recommandations en phase initiale de gestion de crise:

Recommandations

- *Agir rapidement. La notification rapide d'une cyber-attaque au CERT de référence est une étape fondamentale pour la résolution de l'incident et la minimisation de ses impacts. L'établissement urgent d'un canal de communication avec le CERT est vital pour commencer à gérer l'incident de sécurité.*
- *Il faut se réunir avec les Responsables de Sécurité de l'Information.*
- *Il est nécessaire d'informer la Direction de l'entreprise, et de la tenir informée des progrès de l'enquête.*
- *Réunir le comité de crise de l'organisation qui devra gérer la situation et appliquer les plans préalablement conçus. C'est le groupe qui décidera des actions à prendre et de la création éventuelle d'une équipe exclusivement dédiée à cette situation.*

16 Pour disposer d'une information plus détaillée sur la question, nous recommandons la lecture des Rapports suivants : CCN-CERT BP/04 Ransomware et CCN-CERT IA-11/18 Mesures de sécurité contre le ransomware (https ://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html?limit=25&limitstart=25)

Recommandations

- *Il faut effectuer une première évaluation de l'état du réseau informatique, des équipements, du personnel et des services que comporte le réseau informatique.*
- *Il est généralement très utile de refléter en un diagramme l'architecture des systèmes informatiques afin de connaître la situation au début de l'enquête. Il faudrait également faire l'inventaire de tous les équipements affectés afin de savoir exactement quelle est l'information et quels sont les services critiques compromis.*
- *Élaborer la Carte des stakeholders et définir clairement à qui il faut notifier l'incident. Dans un tel cas, et ce immédiatement pour éviter le danger d'infections collatérales, il faudra la communiquer aussi bien aux employés qu'à toutes les connectivités externes de l'organisation (clients, fournisseurs, utilisateurs, etc). En fonction du domaine de compétence de l'affecté, aussi bien s'il s'agit d'un organisme public que d'une entreprise privée qui offre des services TI à des tiers, par exemple, il faudra prévoir des scénarios dans lesquels, après la communication pertinente avec les affectés, l'on bloque à nouveau l'accès qui relie la victime au reste des organismes.*

Il est possible d'imaginer le cas de prestations de services d'une Mairie au citoyen, tel que l'accès à des données municipales (recensement, démarches télématiques, etc.), et que, après avoir été victime d'une infection de ransomware, elle doive réviser les ressources publiquement accessibles et qui peuvent contenir un code malveillant susceptible d'étendre l'infection.

Certains organismes publics délèguent également des missions comme la gestion des feuilles de paie à des entreprises tiers, avec lesquelles ils partagent des ressources en réseau, des accès au bureau à distance, des tunnels VPN, etc. Et il est tout aussi essentiel de bloquer les accès pour éviter la propagation du malware que d'alerter les tiers en vue de prévoir ou de minimiser toute contagion collatérale qu'ils pourraient avoir subi dans une phase initiale.

Dans le cas des MSP (« *Managed IT Services Provider* », par ses sigles en Anglais) ou entreprises fournissant une assistance en gestion TI, il est indispensable et critique de contacter tous leurs clients et les entreprises associées en vue d'éviter un effondrement total qui pourrait augmenter l'impact final de l'infection.

Actions réalisées dans la gestion de ce type de crise:

Actions

Contention de la menace

Il est nécessaire de contenir la propagation du code malveillant par le réseau informatique (chiffrage de dossiers partagés, mouvement latéral vers des équipements avec visibilité, etc.), afin d'éviter qu'un potentiel attaquant à distance, ayant accès aux systèmes, puisse poursuivre son activité (exfiltration d'information, déploiement de portes dérobées additionnelles, élimination ou destruction de preuves, etc). À cet effet, en fonction du volume des équipements affectés dans le réseau et de leur nature, l'on bloquera les connectivités physiquement (en déconnectant le câble du réseau) ou logiquement (en bloquant au niveau du Firewall).

Si le Firewall de l'organisation victime n'effectue pas une segmentation effective des différents sous-réseaux situés dans le parc informatique, un attaquant qui obtiendrait l'accès à un système de l'organisation pourrait avoir la visibilité sur tous les équipements. Pour le résoudre,

l'on redéfinit la segmentation du réseau avec les administrateurs de systèmes de l'organisation, en renforçant les politiques existantes du Firewall dont ils disposent, et en ajoutant un autre coupe-feu additionnel pour augmenter le niveau de sécurité.

La vitesse avec laquelle l'on agit pour freiner l'infection et éviter un impact plus grave est essentielle pour la résolution de l'incident. L'implication à tous les niveaux de l'entreprise affectée, de l'équipe technique à la Direction, permettra ainsi d'obtenir des résultats dès le premier moment.

Détection de la menace

Après la phase de contention, l'on détecte les équipements affectés par le code malveillant, parce que l'attaquant les aurait utilisés pour pivoter sur le réseau informatique ou pour chiffrer et/ou éliminer le contenu.

À l'heure actuelle, dans les cas où le CCN-CERT collabore à la résolution de l'incident, il installe le Système d'Alerte Précoce (SAT) dans la sortie à Internet de l'organisme pour identifier si, sur la base des modèles connus du CCN-CERT, il existe dans le réseau un trafic catégorisé comme malveillant, afin de pouvoir agir opportunément pour localiser puis neutraliser la menace.

En parallèle, tout en effectuant l'analyse légale des équipements affectés, les exemplaires de code malveillant trouvés sont envoyés à des spécialistes en ingénierie inverse, qui se chargeront d'examiner la fonctionnalité de chaque preuve de malware. Ce point est fondamental pour caractériser la menace, savoir quelles sont ses capacités, quels sont les points de persistance établis dans les systèmes, s'il s'agit d'un malware ou d'outils détectés dans d'autres incidents, etc.

Atténuation de la menace

Outre le fait de reconstruire le réseau en segmentant les différents environnements et de restaurer les équipements affectés (service de courrier, contrôleur de domaine, serveur de base de données, équipements client, etc.), l'on met à jour tout l'équipement du parc, en se centrant sur les services exposés face à Internet, qui sont les plus susceptibles d'être endommagés.

Dans ce type d'attaques, l'outil Mimikatz est fréquemment employé pendant une intrusion dans un réseau informatique pour obtenir les accréditations locales et de domaine lors de la fouille dans l'équipement infecté. Si les accréditations fouillées dans l'équipement infecté sont les mêmes dans le reste du domaine, l'on assume que tous les équipements ont été potentiellement compromis. La solution implique la réinitialisation des accréditations du domaine, après avoir recompilé le Contrôleur de Domaine avec le Répertoire Actif (AD). Il est également recommandé de réviser et d'éliminer les utilisateurs ayant des privilèges d'administration qui pourraient avoir été créés par l'attaquant.

Pour atténuer efficacement la menace et afin de prévoir de futurs cas d'infection similaires, l'on suggère donc de changer toutes les accréditations du domaine, aussi bien dans l'infrastructure exposée par l'entreprise ou l'organisme que dans le cloud (webmails, accès par VPN, etc.), et au niveau interne (Répertoire Actif, administrateurs locaux, etc). Dans cette phase, où l'on s'attache à la mission de révision et de nettoyage du parc d'équipements, et en vue de réaliser un contrôle adéquat des actifs qui n'ont pas encore été révisés, ceux qui sont infectés, et ceux qui ont déjà été nettoyés, il est important d'introduire le concept de ***réseau propre****.*

Actions

Ce réseau logique sera créé dans un directionnement interne différent de celui du réseau principal, dont il sera isolé par un firewall, par exemple, et sa fonction consistera à héberger progressivement chacun des équipements du réseau principal révisés et nettoyés. L'on crée ainsi une séparation appropriée qui permettra de reconstruire le réseau sans risquer de subir des réinfections.

Récupération de l'information et des services

Après un incident de sécurité ayant engendré un chiffrage et un effacement d'actifs, il est fondamental d'établir la portée de l'impact subi, en évaluant l'information récupérable et les services affectés.

Il est parfois possible de récupérer une partie importante de l'information qui a été chiffrée, en utilisant des copies de sécurité isolées qui n'ont pas été affectées et via le travail légal. Il faut également reconstruire les services essentiels de l'organisation qui pourraient être endommagés, et en profiter pour réaliser une installation propre et sécurisée permettant un suivi et une traçabilité plus clairs pour l'équipe de sécurité.

Apprentissages

Apprentissages

Ce type d'incidents prouve que l'inversion en sécurité est un besoin. Hélas, ce n'est souvent que quand des incidents de cette importance se produisent que la Direction commence à s'attacher aux demandes qui exigeraient plus de personnel consacré à la mission de sécurité, et qui pourrait effectuer la mission de suivi et d'entretien des systèmes et des réseaux. Il faut parier sur une équipe de sécurité bien préparée, disposant des moyens matériels appropriés, effectuant des audits pro-actifs du réseau et faisant prendre conscience à tous les utilisateurs des ressources techniques.

Il est indispensable de doter matériellement l'organisme de systèmes de sécurité comme Firewalls, SIEM, EDR, etc., afin de pouvoir effectuer plus rapidement la mission de veiller à la sécurité.

Cependant, il ne suffit pas seulement de disposer de personnes chargées de la sécurité informatique ou de moyens physiques pour pouvoir mettre en œuvre les mesures correctes, mais une pleine prise de conscience de la direction est également nécessaire pour que, face à des situations extraordinaires comme, par exemple, le télétravail, des procédures appropriées soient établies afin de s'assurer que le travail est réalisé avec des garanties de sécurité équivalentes à celles du travail depuis le poste de travail habituel.

L'expérience de ces dernières années démontre généralement le manque de culture en matière de sécurité au niveau de la direction des organismes et des entreprises.

Apprentissages

- *Il faut devancer l'inévitable, car dans le monde de la sécurité informatique, bien qu'il soit pratiquement impossible de prévoir une intrusion (par ignorance de toutes les vulnérabilités non publiques, ou parce que l'utilisateur est le maillon le plus faible de la chaîne) il faut disposer des moyens et des personnes permettant de détecter le plus rapidement possible qu'une attaque a lieu, afin de venir à bout, à un stade précoce, d'un incident critique potentiel.*
- *Le fait d'essayer de résoudre trop rapidement un incident dans une entreprise ou un organisme disposant d'un parc d'équipements informatiques important peut donner lieu à des décisions techniques précipitées. Il est important de ne pas oublier d'autres portes dérobées éventuellement déployées par l'attaquant, lui permettant de réinfecter rapidement le réseau informatique.*
- *Le point fondamental pour déterminer le succès dans la résolution de l'incident consiste à travailler in-situ dès le premier moment avec l'organisme affecté et disposer d'une équipe de personnes ayant une idée claire de la marche à suivre pour venir à bout de l'incident.*
- *La coordination entre tous les impliqués est vitale pour pouvoir expliquer de manière simple et pertinente les progrès de l'enquête.*
- *Ces incidents démontrent le besoin de réviser la conception du réseau, les politiques de sécurité et la méthode de télétravail.*
- *Toutes les entreprises et, concrètement, celles qui appartiennent à l'environnement des infrastructures critiques ou des services essentiels, doivent continuer à mûrir dans le cadre de la sécurité informatique afin d'éviter des incidents de sécurité qui peuvent, en dernier ressort, affecter gravement le service qu'elles prêtent aux citoyens.*

Annexe 3.
Cas d'étude Tentative de Soustraction de fonds

Le groupe attaquant connu comme « Carbanak/Cobalt Gang » et dont le nom vient du nom du code malveillant qu'il employait dans ses attaques : il est connu comme Carbanak jusqu'en 2014 et comme Cobalt Strike Beacon[17] à partir de 2015. Ce groupe est actif depuis au moins 2014[18] et l'on estime que jusqu'en 2019 il a volé au moins 1000 millions d'Euros aux organismes bancaires du monde entier. Son activité s'est centrée Initialement sur des banques russes et ukrainiennes, mais la rentabilité de ses attaques, l'a fait étendre rapidement ses activités illicites au reste du secteur bancaire international.

17 https://www.cobaltstrike.com
18 Kaspersky Labs – "Carbanak APT, the great bank robbery".

Que se passe-t-il généralement dans ce type de crise

Depuis quelques années, il existe des groupes cyber-délinquants, disposant de connaissances techniques importantes, qui effectuent des attaques ciblées. Après avoir pénétré dans le réseau et obtenu le contrôle de ses systèmes, les attaquants effectuent des transferts de fonds vers des comptes d'autres organismes dont ils ont le contrôle.

Ils utilisent pour cela des tactiques, des techniques et des procédures (TTP) plus propres d'intervenants parrainés par des États qui se consacrent au cyber-espionnage (connus comme groupes APT). Bien que la motivation de l'attaque ne soit pas d'obtenir des informations mais de réaliser un profit financier, les cyber-délinquants effectuent des actions similaires à celles des groupes APT lorsque leurs réseaux sont attaqués : des missions de reconnaissance méticuleuses pour identifier les actifs qui les intéressent et des missions d'apprentissage pour savoir comment opèrent les travailleurs de l'organisme. Ainsi, ils peuvent recommencer en restant inaperçus.

Que doit faire une organisation dans ce type de situations

Mesures de prévention pour éviter ce type d'attaques:

Mesures

- *Prise de conscience du personnel : de nombreuses attaques sont évitées si le personnel qui travaille avec des moyens informatiques est conscient des risques inhérents et des menaces qui affectent l'organisation.*
- *Création d'une équipe exclusive pour gérer la situation.*

Recommandations au stade initial de la gestion de crise:

Recommandations

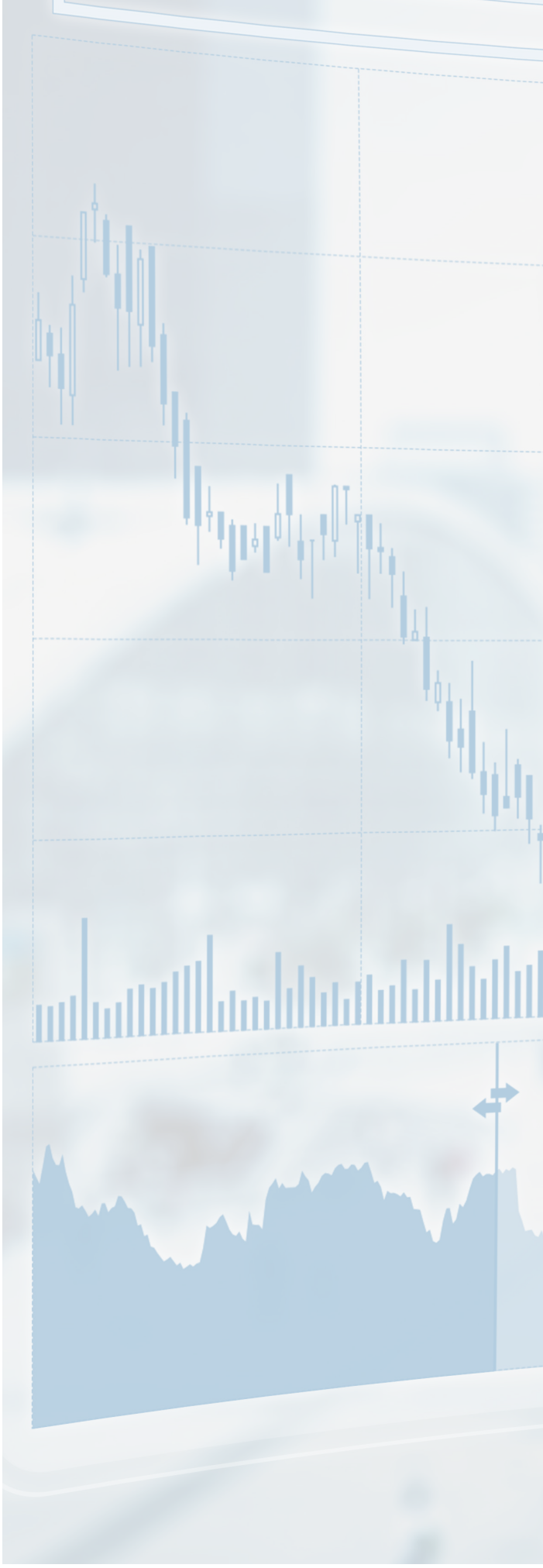
- *Agir rapidement. La notification rapide d'une cyber-attaque au CERT de référence est une étape fondamentale pour la résolution de l'incident et pour en minimiser les impacts. L'établissement urgent d'un canal de communication avec le CERT est vital pour commencer à gérer l'incident de sécurité.*
- *Il est fondamental de prioriser toutes les missions concernant l'enquête avec le support de la Direction, d'agir rapidement, et de créer une équipe exclusivement consacrée à gérer la situation, et qui est cruciale face à des attaques comme celle-ci. La collaboration totale et sincère de la victime et son engagement sont cruciaux, car c'est son personnel qui connaît le réseau informatique, les systèmes qui le forment, etc.*
- *La création d'une cellule de crise au niveau corporatif, incluant le personnel minimal et indispensable, est généralement positive. Ceci est important car l'on évite ainsi les vols d'information quand les rumeurs commencent à se propager. La cellule doit informer la Direction, en temps réel, des progrès de l'enquête et des mesures prises. Ce point est crucial, car l'assistance de la Direction est indispensable pour que faire passer l'information et pour que l'enquête arrive à bon port, plus encore dans le type d'enquêtes où un organisme externe demande une information très sensible sur le réseau informatique.*

Actions réalisées dans la gestion de ce type de crise:

L'on commence par identifier les machines qui effectuent ou qui ont effectué des connexions vers les serveurs de commande et de contrôle, afin de réaliser une analyse légale et de connaître les outils et les TTP qu'emploient les attaquants. Ces analyses permettent de découvrir que ce type d'attaque employait comme vecteur d'infection un courrier électronique malveillant ciblé (spear phishing)

Le courrier malveillant contient généralement un fichier Word joint qui, une fois ouvert, exploiterait plusieurs vulnérabilités de Microsoft Office et infecterait l'équipement de l'utilisateur avec le *malware*, donnant aux attaquants le contrôle sur cette machine.

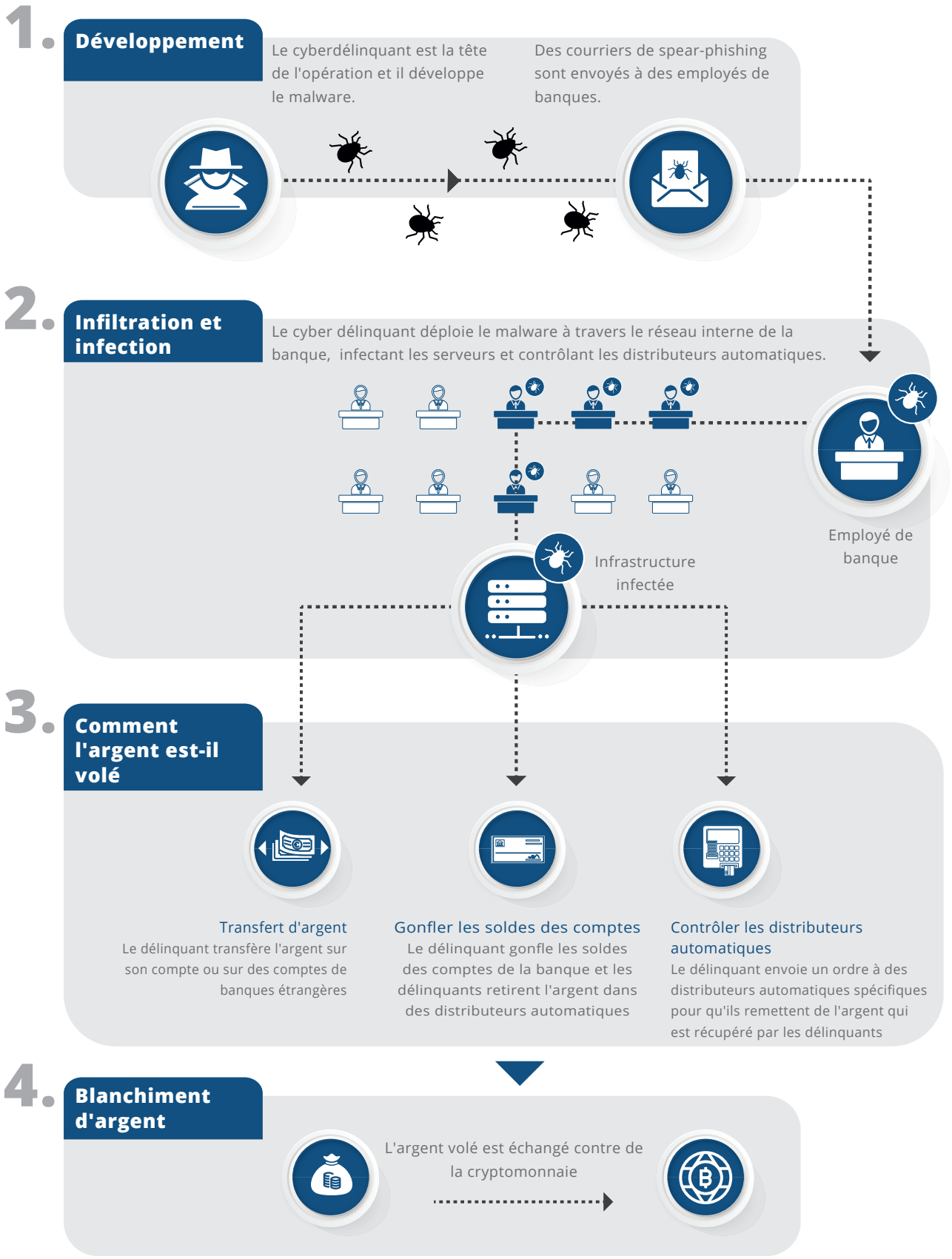
L'installation du malware donne aux attaquant le plein accès et le contrôle de la machine. Une fois obtenu l'accès au réseau, les attaquants y progressent rapidement et obtiennent très vite des accréditations d'utilisateurs avec des permis d'administrateur du réseau, ce qui leur permet de se déplacer avec une liberté totale et d'installer leurs outils sans problème.



L'attaque suivrait le schéma reflété dans le graphique d'Europol suivant:

Carbanak / Cobalt

Fonctionnement



Après avoir défini toute la portée de l'incident, l'on passe au stade de contention et d'atténuation, en prenant les mesures suivantes:

Mesures

- *Débranchement des serveurs principaux, en paralysant l'activité de l'organisation pendant des heures. Ce point est important car les mesures doivent être prises alors que l'attaquant n'a pas accès au réseau.*
- *Réinstallation et montage en plateforme de tous les équipements non critiques affectés. Dans certains serveurs, ceci n'est pas possible et un nettoyage manuel est effectué, en éliminant le code malveillant et en modifiant la configuration pour les protéger correctement.*

Apprentissages

Les leçons apprises au niveau technique sont:

Apprentissages

- *Besoin de disposer d'une équipe consacrée à la sécurité. Pour éviter ce type d'attaques, il est indispensable de maintenir un suivi et une surveillance constants. La sécurité doit être abordée de manière pro-active, et pas de manière réactive. Si l'organisation ne dispose pas de cette équipe, elle ne pourra pas détecter l'intrusion au tout premier stade.*
- *Augmenter la capacité de contention des logs. Dans certains cas, les intrusions sont découvertes quand les attaquants sont dans le réseau depuis longtemps. Le fait de disposer de la plus grande quantité possible de logs aide donc à identifier l'origine de l'infection et, dès lors, à reconstruire les actions des attaquants. L'équipe de sécurité mentionnée se charge de réviser constamment ces logs pour détecter des anomalies.*
- *Segmentation de réseaux : elle permet de limiter l'accès des attaquants si ceux-ci parviennent à infecter un utilisateur qui effectue une mission non essentielle.*
- *Application du principe de privilège minimal. Les utilisateurs devront disposer des accréditations strictement nécessaires pour effectuer leurs fonctions.*
- *Prise de conscience du personnel. De nombreuses attaques sont évitées si le personnel travaillant à l'aide de moyens informatiques est conscient des risques inhérents et des menaces qui pèsent sur l'organisation.*

Apprentissages

Les leçons apprises pour la gestion de la crise sont:

- *Informer la Direction dès que possible, clairement, en toute transparence. Son soutien est indispensable pour pouvoir prendre les décisions et exécuter les actions requises.*
- *Concrétiser la cellule/structure de gestion de crise. Il est indispensable de savoir « qui appeler » à tout moment.*
- *Maintenir le contrôle de l'information, établir des canaux sécurisés pour traiter l'incident en cours, afin que l'attaquant ne sache pas qu'il a été découvert jusqu'à parvenir à éviter son accès au réseau.*
- *Les organismes ont généralement une fausse sensation de sécurité. Ils disposent d'un grand nombre de produits portant sur la sécurité, mais n'ont pas le personnel adéquat pour les administrer ou pour les exploiter, et ils n'en tirent donc que peu de parti.*

Annexe 4.

Orientation sur les niveaux et les critères d'évaluation et de classification de cyber-crise

Établi/ origine	Typologie des impacts	Attribut	Niveau 1 BAJO
CNN-STIC817	Externe	Affecte la Sécurité Nationale	---
	Externe	Affecte la Sécurité des citoyens	---
	Interne	Affecte des infrastructures critiques/services essentiels	---
	Interne	Affecte des systèmes	Affecte les systèmes de l'organisation.
	Interne	Interrompt le service	Interrompt la prestation de service
	Interne	Ressources jour/personnes	Le cyber-incident a besoin de moins de 1 jour/personne pour être résolu
	Interne	Impact économique	De 0,0001% à 0,001% du PIB actuel
	Externe	Affecte géographique	Plus de 1 Région Autonome
	Externe	Impact réputationnel	Ponctuel, sans écho médiatique
AUTRES ATTRIBUTS DE GESTION DE CRISE	Interne/activité/ opérations	Affecte des processus critiques	N'affecte pas des processus critiques
	Social	Affecte des relations avec les groupes d'intérêt	Les attentes et la confiance des groupes d'intérêt ne sont pas affectées
	Social	Alarme sociale	Alarme sociale
	Économique	Nuit à des tiers/environnement	Sans dommages à des tiers/environnement
	Économique	Pertes financières (estimation)	Sans pertes ou pertes insignifiantes. Coûts acceptables en paramètres budgétaires.
	Légal	Implications légales	Sans implications
	De gestion	Déclaration de crise	Non

Niveau 2 MOYEN	Niveau 3 ÉLEVÉ*	Niveau 4 TRÈS ÉLEVÉ*	Niveau 5 CRITIQUE*
---	---	Affecte de manière appréciable les activités officielles ou les missions à l'étranger???	Affecte de manière appréciable la Sécurité Nationale
---	---	Affecte la sécurité des citoyens avec un danger potentiel pour des biens matériels	Affecte la sécurité des citoyens, avec un danger potentiel pour la vie des personnes
---	---	Affecte un service essentiel	Affecte une infrastructure Critique
Affecte plus de 20% des systèmes de l'organisation	Affecte plus de 50% des systèmes de l'organisation	Affecte des systèmes considérés RÉSERVÉ	Affecte des systèmes classés SECRET
		Affecte plus de 75% des systèmes de l'organisation	Affecte plus de 90% des systèmes de l'organisation
Interrompt la prestation de service à plus de 5% des utilisateurs	Interrompt la prestation de service pendant plus de 1 heure et plus de 10% des utilisateurs	Interrompt la prestation de service pendant plus de 8 heure et chez plus de 10% des utilisateurs	Interrompt la prestation de service pendant plus de 24 heures et à plus de 50% des utilisateurs
Le cyber-incident a besoin de 1 à 5 jours/personne pour être résolu	Le cyber-incident a besoin de 5 à 30 jours pour être résolu	Le cyber-incident a besoin de 30 à 60 jours pour être résolu	Le cyber-incident a besoin de plus de 100 jours pour être résolu
De 0,001% à 0,03% du PIB actuel	De 0,03% à 0,07% du PIB actuel	De 0,07% à 0,1% du PIB actuel	Supérieur à 0,1% du PIB actuel
Plus de 2 Régions Autonomes	Plus de 3 Régions Autonomes	Plus de 4 Régions Autonomes ou 1 TIS	Extension géographique supranationale
Dommages réputationnels appréciables, avec écho médiatique (large couverture des médias de communication)	Dommages réputationnels difficilement réparables, avec écho médiatique (vaste couverture des médias de communication) et en affectant la réputation de tiers	Dommages réputationnels pour l'image du pays (pour l'Espagne) et couverture continue des médias nationaux	Dommages réputationnels très importants et couverture continue des médias internationaux
Affecte des processus critiques et la récupération de l'activité interrompue dans son RTO (Objectif de Points de Reprise)	Récupération d'une activité interrompue légèrement plus que son RTO (%)	Récupération d'une activité interrompue plus que son RTO (%)	Récupération d'une activité interrompue ou inconnue ou beaucoup plus que son RTO (%)
Les attentes et la confiance des groupes d'intérêt ne sont pas affectées	Les attentes et la confiance des groupes d'intérêt seront peu affectées	Les attentes et la confiance des groupes d'intérêt seront considérablement affectées	Les attentes et la confiance des groupes d'intérêt et la relation avec ceux-ci se verront fortement affectées pendant longtemps
Sans alarme	Début d'alarme dans la population avec/sans cause justifiée	Alarme de la population avec/sans cause justifiée	Panique dans la population avec/sans cause justifiée
Légers dommages matériels (évaluation €?)	Dommages modérés (évaluation €?)	Dommages graves (évaluation €?)	Dommages très graves (évaluation €?)
Pertes à hauteur de/coût de remplacement	Pertes à hauteur de/coût de remplacement	Pertes à hauteur de/coût de remplacement	Pertes à hauteur de/coût de remplacement
Sans implications	Sans réclamations	Réclamations de tiers et/ou indices de délit	Réclamations massives de tiers et/ou matérialisation du délit
Non	**Oui, de niveau ÉLEVÉ**	**Oui, de niveau TRÈS ÉLEVÉ**	**Oui, de niveau CRITIQUE**

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es

CCN
centro criptológico nacional