INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

INHESJ

TRAVAUX DES AUDITEURS

COMMENT ORGANISER UNE CELLULE DE CRISE EN CAS D'ATTAQUE CYBER ?

Cycle « Sécurité des usages numériques »
Travaux de la 5e promotion (2014-2015)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

en partenariat avec le
cigref Réseau de Grandes Entreprises

JUILLET 2015
ISSN 2265-447X

Les **AUTEURS**

Les auteurs de ce travail intitulé : « **Comment organiser une cellule de crise en cas d'attaque cyber ?** » sont :

- **M. BEDARD Yann**
- **BEGON Jérôme**
- **MARTIN Bertrand**
- **EL BOUHATI Nour Eddine**
- **SEIMANDI Norbert**

Sous la direction de **Nicolas Arpagian**, *directeur scientifique du cycle « Sécurité des usages numériques ».*

REMERCIEMENTS

Nous tenons à remercier, M. Jean-François PEPIN, délégué général du CIGREF et M. Nicolas ARPAGIAN, directeur scientifique du cycle « Sécurité des usages numériques », mais également les différents intervenants pour leur disponibilité et la qualité de leur intervention.

L'Institut national des hautes études de la sécurité et de la justice publie chaque année des rapports et études sur les champs de la sécurité et à la justice.

Dans le cadre du cycle de spécialisation « *Sécurité des usages numériques* », les auditeurs stagiaires réalisent un travail collectif tutoré par le département sécurité économique de l'INHESJ. Ces travaux sont effectués en toute liberté grâce à l'indépendance dont les auteurs bénéficient au sein de l'institut.

L'étude ci-dessous publiée est un document à vocation scientifique. Il ne saurait être interprété comme une position officielle ou officieuse de l'Institut ou des services de l'État. Les opinions et recommandations qui y sont exprimées sont celles de leurs auteurs. Le document est publié sous la responsabilité éditoriale du directeur de l'institut.

Les études ou recherches de l'INHESJ sont accessibles sur le site de l'INHESJ.

Directeur de la publication M. Cyrille SCHOTT, directeur de l'INHESJ

Sommaire

EXECUTIVE SUMMARY

La question n'est plus pour les entreprises de savoir si elles vont être victimes d'une attaque cyber mais plutôt de savoir quand et comment elles le seront. La croissance exponentielle des sources et modes d'attaque doit conduire les entreprises à s'organiser pour les affronter. Même celles qui sont déjà aguerries à la gestion de crise (« traditionnelle ») doivent intégrer cette dimension cyber et revoir en conséquence leurs organisation, processus et moyens de gestion de crise. En effet, faire face à une telle attaque impose aux entreprises de mettre en œuvre un certain nombre de moyens spécifiques complémentaires (SOC et CERT, partenaires externes, outils de détection et protection...) qui seront déterminants pour assurer une gestion efficace de la crise.

L'anticipation et la préparation sont donc tout à fait essentielles et doivent adresser les trois enjeux de Prévention, Détection et Réponse. Il faut donc, dans un premier temps, évaluer et réduire ses vulnérabilités pour diminuer le risque et l'exposition aux attaques cyber. Il faut ensuite améliorer sa capacité à détecter et qualifier les événements ou attaques pouvant conduire à une crise. Et enfin, lorsque la crise n'a pu être évitée, il faut également être capable d'avoir un dispositif et des moyens immédiatement activables et opérationnels. Ainsi, par exemple, une veille active et continue des menaces cyber permettra à une entreprise de pouvoir détecter les attaques plus tôt et donc de déclencher les ripostes plus rapidement. Mais cela permettra également de constituer un socle de connaissances et un réseau d'expertises (au travers de ressources internes ou externes) qui pourront être mobilisés dans le traitement de la crise.

Les entreprises doivent également adapter leurs stratégies de communication interne et externe. En temps de crise, communiquer est vital pour coordonner l'ensemble des acteurs mobilisés. Mais les canaux numériques utilisés pour cette communication n'ont-ils pas été compromis par l'attaquant ? De plus, toute information relative à l'attaque peut devenir virale (parfois même à l'initiative de l'agresseur qui en assure la publicité sur Internet) et causer des dommages de réputation et d'image plus importants que les dommages matériels de l'attaque elle-même.

Connaître les menaces, anticiper les modes de réponse et savoir gérer une crise sont des éléments clefs que les entreprises doivent maîtriser pour gérer efficacement une crise cyber. Ce mémoire s'attachera à décrire chacun de ces thèmes. Mais il proposera également un ensemble de conseils et guides pratiques qui, nous l'espérons, aideront les entreprises à finaliser leur organisation et formaliser leurs plans d'actions en réponse à une crise cyber. Ces plans devront être documentés, partagés et testés avec l'ensemble des ressources internes et externes qui pourront être sollicitées pendant la crise. Et ils devront également être mis à jour régulièrement pour prendre en compte l'évolution des menaces et des risques.

INTRODUCTION

Le monde actuel est en train de vivre une révolution numérique. Les nouvelles technologies (et en particulier celles liées à l'informatique et aux télécommunications) sont en train de bouleverser le monde des entreprises. Le *Cloud Computing*, l'Internet 2.0 et les media sociaux, le *Big Data*, les terminaux mobiles et d'autres innovations telles que l'Internet des objets, la robotique (...) offrent de nouvelles opportunités pour les entreprises. Certaines les utilisent pour créer de nouveaux produits et services, d'autres pour développer leurs relations avec leur clients et consommateurs, beaucoup pour changer leurs modes de fonctionnement internes et améliorer leur efficacité opérationnelle. En conséquence, le patrimoine digital se développe dans toutes les entreprises et devient à la fois un élément clef pour leur fonctionnement et un capital vital à protéger pour maintenir leur position concurrentielle vis-à-vis de l'ensemble de leurs compétiteurs.

Cette révolution numérique a donc également des répercutions sur la sécurité des entreprises. Leur niveau d'exposition aux risques en général et aux risques cyber en particulier est depuis quelques années en perpétuelle augmentation et est devenu un sujet d'attention et de préoccupation pour les dirigeants des entreprises. La mondialisation et la numérisation du monde des affaires et des échanges commerciaux ont fait apparaître de nouvelles sources et de nouveaux types de menaces. Les Systèmes d'Information (SI) des entreprises hébergent une multitude d'informations qui attirent la convoitise, que ce soit de la part de compétiteurs, de cyber-délinquants, voire même de personnes internes à la société. Ces mêmes systèmes d'information sont de plus en plus interconnectés et ouverts (par exemple sur Internet), et offrent donc une exposition de plus en plus large aux intrusions et aux attaques qui peuvent être initiées depuis n'importe quelle partie du monde. Il faut noter également que le nombre de cyber criminels est en très forte augmentation et que leurs pratiques se professionnalisent et deviennent de plus en plus sophistiquées. Les hackers d'autrefois (en recherche de notoriété liée à leurs « performances ») ont désormais laissé la place à des experts du cyber crime dont la principale motivation est de gagner de l'argent.

En conséquence, les entreprises doivent repenser leurs modèles de gestion des risques et de crise, pour intégrer la dimension numérique croissante dans les crises. L'objectif de ce mémoire est précisément de donner des éléments spécifiques de préparation et de gestion de crise dans un contexte d'attaque cyber. Nous reprendrons donc rapidement les principes généraux de gestion de crise et détaillerons ensuite les points d'attention nouveaux et particuliers induits par la dimension cyber de notre sujet d'études.

Ce mémoire se veut très opérationnel, sans pour autant être réservé à des professionnels de la sécurité informatique. Nous l'avons conçu de manière à pouvoir être compris et transposé par n'importe quel cadre en charge de la gestion d'une crise cyber en entreprise. Il propose en particulier un *vade-mecum* qui, après avoir été adapté au contexte de l'entreprise, pourra être diffusé à tous les échelons pour faire connaître à tous les acteurs concernés les bonnes pratiques à mettre en œuvre dès que survient une crise cyber.

Quelques définitions : crise, attaque cyber et crise cyber

Il convient d'abord de rappeler la définition d'une « crise » : « *Événement soudain causant des pertes et des dommages importants, entraînant une interruption d'une ou plusieurs activités critiques ou un arrêt de l'organisme, ayant des impacts à long terme et nécessitant le recours à la Cellule de crise et, le cas échéant, à un site alternatif. Une crise peut avoir des conséquences sur la survie même de l'entreprise.* » [1]

(1) Source AFNOR

Par conséquent, la crise est une résultante de la matérialisation de risque(s) ayant des impacts non maîtrisables pouvant mettre en péril la réputation, les opérations, voire la pérennité même, de l'entreprise ou de la structure qui la subit. En règle générale, la crise est imprévisible, et lorsqu'elle se matérialise, elle est généralement source de désorganisation et l'entreprise qui en est victime doit être en mesure de fournir immédiatement des réponses adaptées et justement calibrées en fonction de la typologie de celle-ci.

Nous pouvons ensuite définir simplement le concept d'« attaque cyber » comme étant « *une attaque mettant en œuvre des moyens numériques et effectuée au travers de réseaux informatiques* ».

Par extension, nous pouvons proposer la définition suivante d'une « crise cyber » : « *une crise cyber est une crise liée à une attaque cyber qui vise spécifiquement le patrimoine numérique, les infrastructures techniques ou le Système d'Informations d'une entreprise.* »

Comme nous le verrons dans le chapitre suivant, les attaques cyber peuvent être conduites de l'extérieur ou au sein même de l'entreprise. Et elles peuvent être de différentes natures en fonction de l'objectif et de la cible de l'attaquant.

Éléments de contexte et catégorisation d'attaques cyber

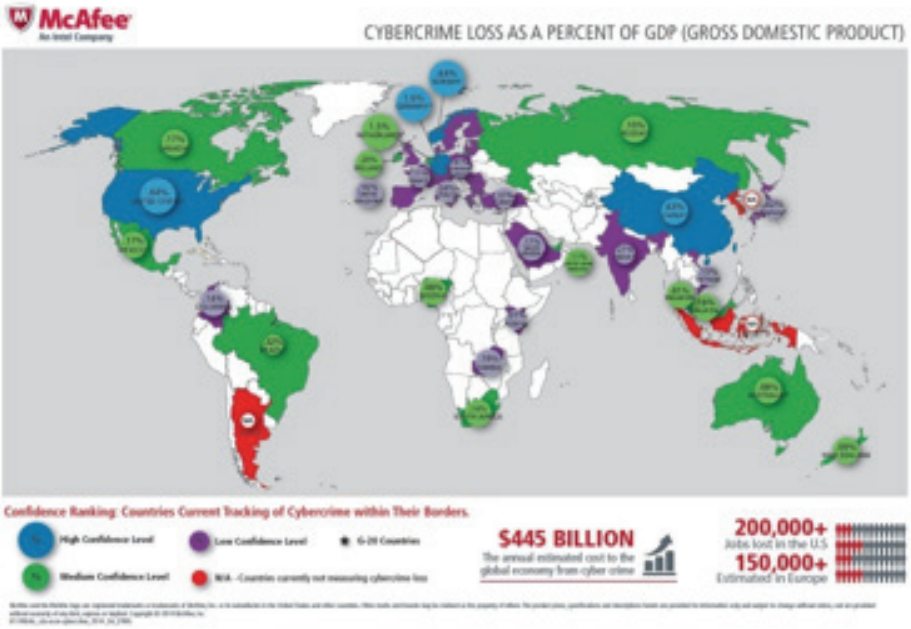
Cyber criminalité en forte croissance

D'après une étude de Cap Gemini [2], entre 2013 et 2014, le nombre des cyberattaques a augmenté de 120% dans le monde et le coût estimé de la cybercriminalité pour les entreprises s'élève en moyenne à 7,6 millions de dollars par an, soit une augmentation de 10%. En outre, les *hackers* ont considérablement accru leurs connaissances des systèmes ciblés. De ce fait, les conséquences de leurs attaques sont de plus en plus importantes.

(2) http://www.globalsecuritymag.fr/Le-groupe-Capgemini-lance-une,20150212,50774.html

Cette tendance est confirmée par *MacAfee* [3], qui estime le coût global de la cybercriminalité dans le monde à un total astronomique de plus de 400 milliards de $.

(3) http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf



Et au-delà des chiffres publiés dans tous ces rapports, il est saisissant de voir l'augmentation du nombre d'incidents et d'attaques cyber qui font désormais régulièrement la une des journaux. Comme démontré par les quelques exemples cités ci-après, ces attaques sont de multiples natures et concernent des organisations très diverses : organismes publics, grandes entreprises et même des entreprises intervenant dans le secteur de la sécurité numérique !

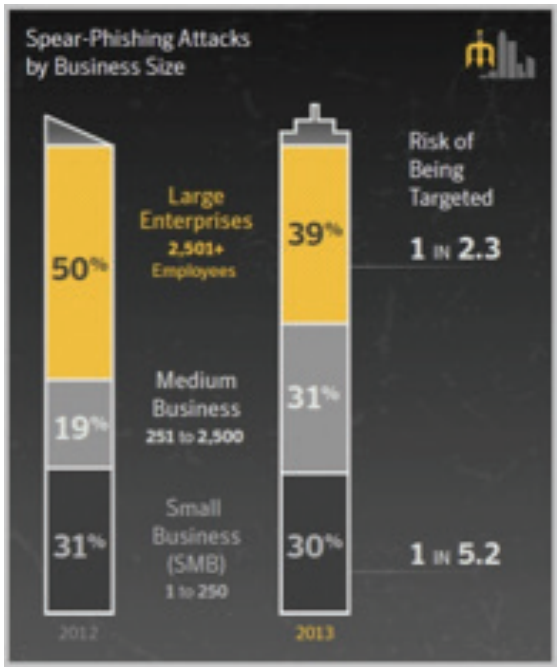
Source[4] *: Solucom*

(4) Avril 2012 - SOLUCOM - Attaques ciblées : Quelles évolutions dans la gestion de crise ?

(5) http://www.symantec.com/fr/fr/security_response/publications/threatreport.jsp

Il est également important de noter que, au-delà de toutes ces affaires médiatisées, toutes les entreprises sont maintenant touchées, y compris les petites structures. *Symantec*, dans son rapport 2014 *Annual Threat Report*[5], indique pour 2013 que 30% des attaques de type *spear-phishing* ont ciblé des petites entreprises (de moins de 250 salariés) et que près de 20% de ces petites entreprises ont subi des attaques de ce type.

Un dernier élément de contexte intéressant concerne l'affaire « Snowden ». Nous citons moins ce cas pour sa dimension de cyber espionnage que pour l'illustration des risques encourus par une organisation du fait de ses partenaires externes. En effet, Snowden, qui travaillait dans une société sous-traitante de la NSA a eu accès à un très grand nombre d'informations hautement stratégiques et a réussi à les exfiltrer pour les rendre publiques.



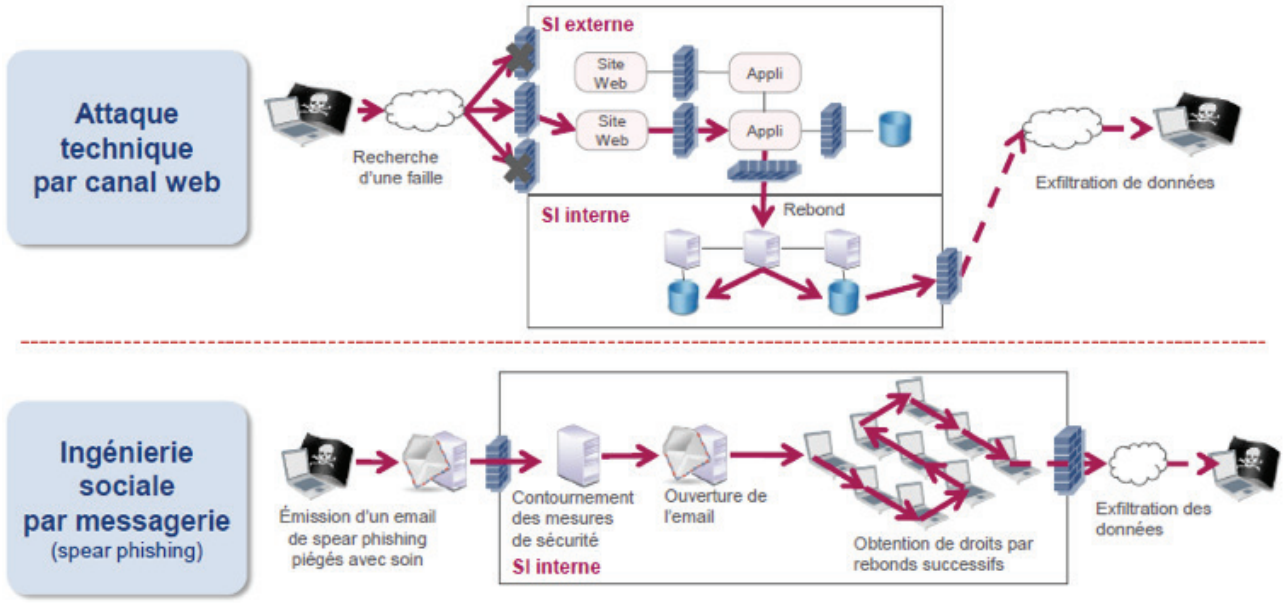
Catégorisation des attaques cyber

En regard de l'évolution de la cybercriminalité, il faut savoir catégoriser les attaques pour mieux les analyser et se préparer à y répondre. Verizon, dans sa dernière étude annuelle[6], propose une démarche intéressante pour faire cela. Verizon a précisé, après avoir analysé les données de plus de 100 000 incidents de sécurité sur 10 ans, que 96 % des attaques peuvent être réparties en 9 types de menaces (les attaques de *malwares*, la perte ou le vol d'appareils, les attaques *DDoS*, les arnaques à la carte bancaire, les attaques d'applications web, le cyber-espionnage, les intrusions, le vol interne et les erreurs humaines).

(6) Verizon – 2015 *Data Breach Investigation Report.*

Ainsi, en analysant chacune de ces menaces et en étudiant les pratiques et méthodes utilisées par les cybercriminels, les entreprises vont pouvoir développer leurs capacités de prévention, de détection et de protection.

Illustrons notre propos au travers des deux mécanismes d'exfiltration de données schématisés ci-après :

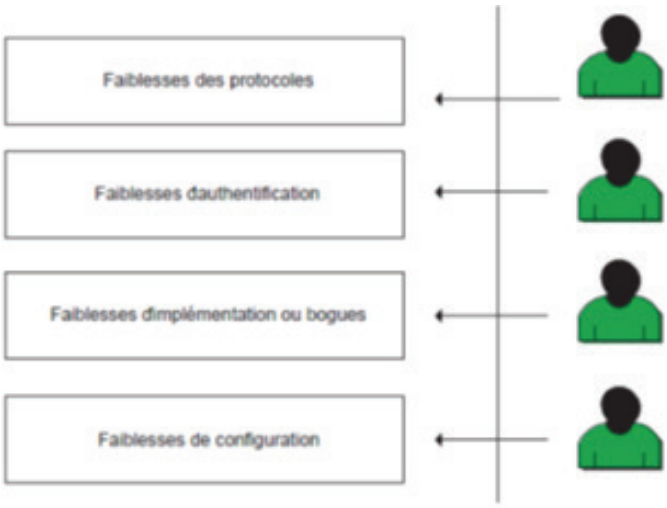


Source : SOLUCOM[7]

(7) Avril 2012 – SOLUCOM – Attaques ciblées : Quelles évolutions dans la gestion de crise ?

Dans le premier cas, connaître les failles des systèmes web et comprendre comment les cybercriminels les exploitent pour compromettre un site sont essentiels pour mettre en place les protections adéquates.

Les techniques d'attaques des systèmes réseau sont nombreuses et variées. La publication de programmes permettant d'exploiter les vulnérabilités des systèmes ne renforce évidemment pas la sécurité de ces systèmes et met gratuitement à la disposition des pirates des outils redoutables. Un des moyens de limiter l'impact de telles attaques est de découper le réseau d'entreprise en périmètres de sécurité logiques regroupant des entités ou fonctions afin de mettre en place des niveaux de sécurité à la fois imbriqués et séparés.



De même, dans le second cas, il est très important de comprendre les techniques de *phishing* utilisées par les cybercriminels. Cela permettra à la fois d'améliorer les dispositifs de protection (comme par exemple le pavé numérique virtuel qui est utilisé pour saisir les mots de passe de connexion aux comptes en ligne à l'aide de la souris et permet donc de contrer les *keyloggers* qui enregistrent les frappes de clavier). Mais cela permettra également de mettre en place des programmes de sensibilisation et de formation des salariés qui les préparent à acquérir les bons réflexes et ne pas faire « le clic de trop » qui installera un *malware* en contournant les mesures de sécurité du SI.

Et on retrouve les mêmes enjeux pour les mécanismes de rebonds ou d'exfiltration de données. Savoir comment les cyber criminels opèrent guidera les entreprises dans leurs démarches de détection et de protection.

En complément de l'analyse précédente des types de menaces et modes opératoires des cybercriminels, il est également important pour les entreprises de faire une évaluation des impacts encourus au travers des attaques cyber.

Les conséquences d'une attaque cyber peuvent être très différentes mais nous pouvons néanmoins citer les exemples suivants :

- Pertes économiques dans le cas d'exfiltration de données stratégiques (propriété intellectuelle).
- Pertes financières dans le cas de vol de coordonnées bancaires.
- Crises d'exploitation dans le cas d'attaques visant le SI ou les systèmes industriels.
- Atteintes à l'image et à la réputation en cas de divulgation d'informations confidentielles ; ...

Comme nous le verrons dans le chapitre « *Comment se préparer à gérer une crise cyber ?* », c'est au travers d'une **analyse de risques** qui met en regard les menaces cyber, leur probabilité d'occurrence et l'évaluation de leur impact que les entreprises pourront définir leur **stratégie de continuité d'activité** et arrêter leurs plans de cyber sécurité (à la fois en termes de prévention et de réponses aux attaques).

Gestion de crise cyber

D'après le RSSI[8] de l'Institut national des hautes études de la sécurité et de la justice, la « gestion de crise » est l'ensemble des moyens humains, juridiques, techniques et matériels permettant à une organisation de se préparer aux risques et de faire face aux impacts pouvant affecter le bon fonctionnement de cette dernière. Puis d'ajouter, que de tirer les enseignements de l'événement est une bonne chose mais il faut que ce retour d'expérience serve de base solide à des procédures visant à l'anticipation des risques, la réponse aux impacts et ce, dans une vision prospective.

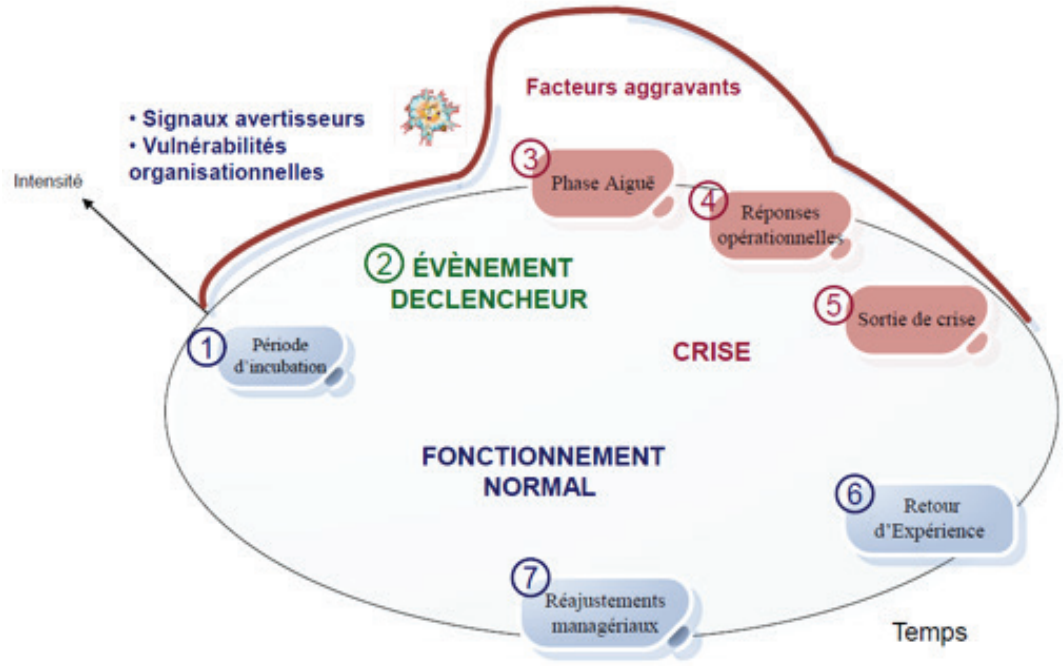
(8) M. Bertrand MARTIN, RSSI de l'INHESJ de 2001 à 2014.

Donc la gestion d'une crise ne s'improvise pas. Elle doit être anticipée par l'entreprise avec la mise en place en amont d'une évaluation des risques qui servira de base à la mise en place d'un plan de gestion de crise.

Dans un monde idéal, avec un budget et des ressources illimités, chaque entreprise disposerait, hormis ce plan de gestion de crise régulièrement mis à jour, de moyens logistiques adéquats, d'une équipe de gestion de crise avec des titulaires et/ou des suppléants régulièrement entraînés. La finalité est la mise en place de réponses appropriées à chaque situation afin de leur permettre d'être réactifs. La réalité est cependant tout autre. Malheureusement et dans la grande majorité des organisations, la gestion de crise est réduite à sa plus simple expression. Cette notion ne prend sens que lorsque ces mêmes organisations sont directement impactées.

Dans le présent chapitre, nous nous attacherons à traiter la gestion de crise au sens large du terme. Puis, nous aborderons spécifiquement la question des crises cyber.

Les fondamentaux de la gestion de crise



Source : INHESJ[9]

(9) Janvier 2010 – INHESJ – Gérard PARDINI – Gestion de Crise.

Dans la schématisation ci-dessus, la crise représente la situation hors des standards du fonctionnement normal d'une entreprise, qui prend naissance du fait d'un événement déclencheur et dont la sévérité peut être amplifiée par la présence de facteurs aggravants. La crise est donc la succession des activités depuis son déclenchement en phase 2 jusqu'à sa clôture qui correspond aux phases 5 de sortie de crise et 6 de retour d'expérience.

Dans le cas d'une attaque par le biais d'un virus informatique, la gestion de la crise provoquée par l'attaque pourrait donc correspondre à la séquence d'activités suivante :

Pour gérer efficacement l'ensemble de ces activités, l'entreprise va devoir mettre en place une organisation, des moyens et des processus spécifiques que nous allons décrire succinctement.

Source : SOLUCOM [10]

(10) Mai 2014 – INSA Toulouse & SOLUCOM – Qualité et gouvernance des SI : La gestion de crise.

Organisation, moyens, processus

Les bonnes pratiques en termes d'organisation recommandent de scinder les rôles entre une cellule de direction de crise et une ou plusieurs cellules opérationnelles de crise, qui assumeront respectivement des responsabilités de pilotage et d'exécution.

La collaboration et la coordination entre les deux types de cellule doivent être établies avec soin. Un pilotage surdimensionné conduit au piège de la **pyramide inversée** qui étouffe la capacité d'exécution du dispositif (les opérationnels passent plus de temps à rendre compte qu'à traiter). Et, *a contrario*, un pilotage sous-dimensionné peut être tout aussi inefficace en laissant les ressources et énergies se disperser dans de mauvaises directions.

La composition de ces cellules dépend évidemment du contexte de chaque entreprise et de la nature de chaque crise mais on retrouvera, de manière très classique, les participants suivants :

Cellule de direction de crise :

- Pilote de crise *(en liaison avec la Direction générale)* ;
- Directions Métiers *(en fonction de la nature de la crise)* ;
- Direction Communication ;
- Direction des Ressources humaines ;
- Direction des Systèmes d'information ;
- Direction Juridique ;
- Direction Gestion des risques ;...

Cellule(s) opérationnelle(s) de crise :

- des ressources opérationnelles Métier ;
- des ressources informatiques et sécurité ;
- des ressources Communication ;
- des partenaires externes en cas de besoin *(expertise légale, expertise sécurité...)*.

Ces cellules doivent ensuite disposer de **moyens** pour assurer leur mission. Parmi ces moyens, on notera tout d'abord les salles de crise. Ces salles devront permettre aux cellules de se réunir en un même lieu et devront également être équipées de moyens de communication (système de téléphonie, site web pour échanger des documents,...) et de moyens de traitement opérationnels (ordinateurs connectés aux réseaux de l'entreprise et à Internet...). Mais il faudra également fournir aux cellules les informations, documents de référence et outils qui leur permettront de piloter et coordonner leur activité (annuaire de crise, journal de crise, tableaux de bord de pilotage,...).

Et enfin, ces cellules doivent pouvoir opérer en se référant à des guides opératoires et processus de fonctionnement qui auront été définis au préalable. Cela concerne aussi bien les **processus** de déclenchement (procédures d'alerte et d'escalade, procédure de qualification du niveau de crise) que les processus de traitement (fiches réponses décrivant les modes opératoires de traitement et correction, guide de communication rappelant les messages clefs et règles à respecter dans toute communication externe,...).

Les phases clefs de la crise : du déclenchement à la clôture

Dans toute gestion de crise, les organisations vont être confrontées aux enjeux suivants. Comment :

- Détecter et gérer l'entrée en crise ?
- Évaluer la gravité de la crise ?
- Répondre à la crise ?
- Détecter la fin de la crise ?
- Capitaliser ?

Détecter et gérer l'entrée en crise est une tâche délicate. Cela impose aux organisations d'avoir établi les processus et/ou les réflexes qui permettent d'identifier, dans leurs lots d'incidents quotidiens, ceux qui sont générateurs de risques importants et qui sont des déclencheurs potentiels de crises. Cela suppose de mettre en place une discipline de qualification des événements et incidents qui permette de faire rapidement ce tri et de donner l'alerte quand il le faut.

L'évaluation de la gravité de la crise est également une étape importante. En effet, c'est cette évaluation (avec par exemple des classifications du type niveau Rouge ou niveau Orange) qui permettra non seulement de décider s'il faut déclencher une crise mais également de dimensionner le dispositif de réponse.

Répondre à la crise nécessite d'identifier et mobiliser toutes les ressources pour enrayer le développement de la crise et exécuter les actions qui en corrigeront les impacts. Cela réclame une grande capacité de pilotage et de coordination ainsi qu'une bonne communication interne et externe.

Détecter la fin de la crise permettra de mettre fin au dispositif exceptionnel de gestion de crise. Cela ne doit pas être fait trop tôt (attention à l'effet boomerang d'un problème supposé résolu qui resurgit) mais il faut également veiller à ne pas prolonger le dispositif inutilement.

Capitaliser, après la sortie de crise, consiste à faire une analyse *post-mortem* ou un **Retour d'Expérience** sur l'ensemble du déroulement et des événements de la crise. Cette activité est essentielle pour permettre à chaque organisation d'identifier des axes d'amélioration et ajuster leur plans et processus de gestion de crise en conséquence.

Ce retour d'expérience doit se faire :

- À chaud, pour recueillir ce qui est bien présent dans la mémoire de chacun des acteurs.
- À tiède (quelques semaines plus tard), pour valider les enseignements et propositions de plan d'actions post-crise à engager.
- À froid (par exemple à la date d'anniversaire), pour évaluer plus sereinement l'impact réel de la crise initiale et vérifier que les leçons et plan d'action post-crise du Retour d'Expérience ont bien été appliquées.

Les spécificités d'une gestion de crise cyber

La gestion de crise cyber doit être pluridisciplinaire : elle est notamment au croisement de la gestion du risque et de la sécurité informatique (donc technique). Les experts techniques seront au service du décisionnaire dans cette gestion. Plus les choses auront été préparées en amont, notamment la cartographie des risques, l'analyse des vulnérabilités et des vecteurs et modes d'attaques, plus la gestion de la crise pourra être efficiente.

Et cette gestion doit naturellement prendre en compte les spécificités d'une attaque cyber qui sont de plusieurs natures :

- Les attaques cyber sont généralement **invisibles** ou difficiles et longues à identifier contrairement à d'autres types classiques de crises tels qu'un séisme, un incendie, une crue,... Les entreprises doivent donc développer leur capacité de détection des signes précurseurs et des « signaux » faibles d'attaques avant que celles-ci ne deviennent majeures.

- La deuxième spécificité tient au fait que l'étendue des attaques est bien souvent très difficile à évaluer et qu'elle peut évoluer très vite. En effet, les attaques ont pu être détectées longtemps après leur occurrence et ont donc pu « contaminer » de multiples parties du Système d'Information de l'entreprise. De plus, ces attaques peuvent également continuer à se propager très rapidement. Cela doit conduire les cellules de crise à définir des plans d'actions pour confiner les attaques et enrayer leur propagation. Elles devront ensuite mener des opérations de correction et de reconstruction, tout en continuant à garder sous surveillance les parties du SI qu'elles vont progressivement « assainir ».

- La troisième spécificité est directement liée à la dimension technique des attaques. La cellule de crise doit pouvoir mobiliser une multiplicité d'expertises et de compétences technologiques pour pouvoir contenir et remédier à une attaque cyber. Il lui faudra donc pouvoir solliciter très rapidement un grand nombre de spécialistes en interne ou en externe tels que : des experts en analyse technique post-incident, des équipes CERT, des agences nationales de lutte contre la cybercriminalité tels que l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), l'Agence nationale de la sécurité des systèmes d'information (ANSSI), voire même la Direction centrale du renseignement intérieur (DCRI).

Une autre particularité des crises cyber est que l'attaque, en altérant le SI de l'entreprise, peut directement diminuer sa capacité de réponse. Il convient donc de disposer d'un dispositif de gestion de crise qui permette de pallier à cette possibilité et par conséquent :

- de prévoir des moyens de gestion de crise hors SI ;
- de se doter de postes de travail durcis hors des domaines d'administration ;
- d'exploiter des services d'échange et de communication externes (par exemple des services *cloud*).

Attention ! Les attaquants ont pu également compromettre les messageries personnelles des personnalités ciblées.

Les enjeux de la communication dans la gestion de crise

Depuis l'avènement du Web 2.0 et des media sociaux, les entreprises se trouvent bien souvent dans une situation de communication externe « **asymétrique** » : c'est-à-dire qu'elles continuent majoritairement à utiliser des canaux de communication traditionnels alors que l'opinion publique devient de plus en plus sensible et influencée par la viralité des informations diffusées sur Internet. Les entreprises comprennent désormais qu'Internet doit devenir pour elles un canal de communication « officiel » et elles doivent adapter leur stratégie de communication en conséquence.

De nouveaux enjeux de communication externe

C'est particulièrement vrai en temps de crise quand la communication externe doit veiller à **préserver la réputation de l'entreprise** et que cette réputation peut se retrouver menacée sur Internet. Des organisations, des groupes d'internautes ou même de simples individus peuvent ternir directement l'image d'une entreprise et déclencher ou aggraver une crise en diffusant de fausses informations ou des informations confidentielles sur Internet. Il faut être capable de détecter ces menaces/attaques mais également de proposer une riposte « symétrique », c'est-à-dire dont l'impact positif sur Internet permettra d'éteindre l'impact négatif initial sur le public.

Mais cela ne s'improvise pas et chaque entreprise devra, dans un premier temps, établir sa présence, développer ses propres réseaux et asseoir sa crédibilité sur ces nouveaux média. Pour cela, il lui faudra :

- organiser une **veille continue sur les communications sur Internet** ayant un rapport avec son activité et pouvant constituer des signaux faibles ou éléments déclencheurs de crise ;

- comprendre et apprendre les **bonnes pratiques de communication** sur les réseaux sociaux ;
- identifier les **communautés, cercles et *leaders* d'opinion** ayant une influence sur son activité ;
- créer les liens et établir la communication et les échanges avec ces acteurs.

L'enjeu consiste ensuite à tirer les fruits de ce travail de veille en élaborant des messages ou stratégies de communication qui soient personnalisés pour chaque audience visée et qui puissent être diffusés directement par l'entreprise ou relayés par les communautés et groupes avec lesquels elle a établi un lien.

Tout va très vite sur Internet. Aussi pour pouvoir réagir rapidement en cas de crise, l'entreprise devra définir en amont la liste des personnes habilitées à communiquer en son nom.

Sans oublier la communication interne

Communiquer en interne en période de crise est primordial pour coordonner l'ensemble des acteurs mobilisés dans la gestion de la crise (ex : équipes de supports locales, spécialistes de la cellule de crise, équipes techniques, équipes juridiques,...). Il convient donc de donner à chacun les informations dont il a besoin pour assumer ses activités et responsabilités mais également maintenir son engagement et investissement dans la gestion de l'événement.

Il faut néanmoins veiller à trouver la bonne limite dans le partage d'informations. Communiquer plus que nécessaire ou plus largement que nécessaire peut s'avérer contre-productif car cela peut créer des risques supplémentaires de fuite d'information vers l'extérieur avec toutes les conséquences décrites précédemment sur un public recevant un message qui n'a pas été conçu pour lui. Il est donc préférable de communiquer de façon **ciblée** plutôt que globale afin de rendre l'information **parcellaire** et ainsi limiter les impacts négatifs en cas de propagation au-delà du cercle des personnes habilitées.

Et bien sûr, il faut là encore être capable d'agir vite. Cela impose à nouveau de définir soigneusement au préalable la liste des personnes habilitées à communiquer en interne et de rappeler aux autres acteurs (internes mais aussi aux partenaires externes) leur devoir de réserve et leur obligation de confidentialité. Il est d'ailleurs conseillé de faire signer à tous un engagement de non divulgation (*Non Disclosure Agreement* – NDA). Cela donnera les leviers juridiques de réponse aux fuites éventuelles d'information hors de la cellule de crise. On pourra également organiser une veille informationnelle dans l'entreprise afin de détecter et gérer les rumeurs, fuites, et être capable soit de les démentir, soit de les stopper.

Comment se préparer à gérer une crise cyber?

Comme évoqué précédemment, une entreprise doit anticiper et se préparer aux situations de crise en développant une **stratégie de continuité d'activité**. Pour assurer sa continuité, l'entreprise doit savoir à quelles menaces d'interruption de ses activités elle est exposée. Il lui faut donc connaître le champ des risques encourus pour pouvoir étudier les options permettant d'en réduire les effets au travers de mesures de prévention, de protection, de détection et de réponse face aux attaques cyber.

Il faut donc commencer par une **analyse de risques**.

Analyse de risques cyber

L'analyse de risques est de manière classique la démarche qui permet à une société d'évaluer la probabilité et l'impact des menaces sur ses activités et actifs critiques. Dans notre contexte cyber, cette analyse ciblera plus particulièrement les menaces informatiques visant les actifs numériques d'une société.

Patrimoine et actifs numériques « à protéger »

Le mot « actif » est pris au sens le plus large : il désigne ici tout ce qui concourt à la bonne marche de l'entreprise. Ces actifs couvrent de manière classique :

- les **ressources intangibles** – fichiers, bases de données (informatiques ou non), informations confidentielles ou secrètes, procédures, mais aussi l'image de la société sur son marché, sa bonne réputation, etc. ;
- les **biens tangibles** – locaux, machines, logistique, serveurs et postes de travail, téléphonie, réseau, etc. ;
- les **ressources humaines** – personnel, compétences particulières, savoir-faire humains, titulaires de droits d'accès spéciaux aux logiciels, etc.

Dans le contexte actuel de transformation numérique des entreprises, une attention particulière doit être apportée aux données qui sont une cible prioritaire pour les cybercriminels. Il faut conduire un exercice détaillé de cartographie de l'ensemble des données de l'entreprise qui permette de définir :

- leur **typologie** : données personnelles, bancaires, stratégiques…
- leur **sensibilité** : confidentialité, intégrité, disponibilité
- leur **attractivité** : quelles sont les informations qui peuvent avoir un intérêt et une valeur pour un cybercriminel et à quelles fins ?
- leur **localisation** : sur quels supports (CMDB), dans quelles applications, et comment sont-elles sauvegardées ?
- leur **circulation** et « cycle de vie » : qui en est propriétaire et qui les administre ?, qui a accès à ces données et quels sont les processus métiers concernés ?,…

L'analyse de ces informations permettra à chaque entreprise de définir des mécanismes de protection des données. Il s'agira par exemple des procédures d'attribution et de contrôle d'accès. Ou encore de règles de gestion qui imposent que certaines données (avec un fort niveau de sensibilité) soient systématiquement chiffrées sur les postes et dans les transferts *via* réseau ou messagerie.

Identification et analyse d'impact des menaces cyber

Sont considérées comme des menaces cyber toutes les situations qui peuvent survenir ayant pour conséquence une détérioration des moyens informatiques utilisés pour mener à bien l'activité de l'entreprise. Toute menace comporte trois caractéristiques principales qui doivent être analysées avec soin :

1. **Elle a des conséquences considérées comme nuisibles à l'activité**. Ces conséquences peuvent être de gravité variable. Un incendie, par exemple, peut endommager l'ensemble d'un site informatique ou, au contraire, être circonscrit aux poubelles de la cantine. On voit bien ici que le même événement menaçant « incendie » peut avoir différentes conséquences.
2. **Elle possède une probabilité d'occurrence**. Cette probabilité est considérée comme suffisamment forte pour que l'on ait à s'en soucier. Quantifier les probabilités d'occurrence est un art difficile dans bien des cas, mais il est au moins possible de déterminer ce qui est plus probable par rapport à ce qui l'est moins, en raisonnant uniquement par valeur relative.
3. **Elle a une origine, soit humaine, soit technique, soit naturelle**. Cette caractéristique est importante, car elle influencera les moyens mis en œuvre en prévention.

L'évaluation des impacts et conséquences possibles des menaces est tout à fait essentielle. Il s'agit de répondre à la question suivante : si tel événement se produit sur les actifs considérés, combien perd la société ? L'estimation est établie pour une occurrence de sinistre, la perte se chiffrant en euros. Il faut faire preuve de bon sens et accepter d'entrer dans des raisonnements « à la louche », qui seront affinés plus tard.

Plan de continuité d'activité

Au cours des phases présentées ci-avant, l'entreprise a déterminé ses activités et actifs critiques. Elle a fait le point sur les risques qu'elle encourt : tout au moins ceux pouvant lui causer les dommages les plus forts. Les délais de reprise et les temps d'immobilisation maximum acceptables de ses activités critiques ont été étudiés et sont désormais connus. La probabilité d'occurrence des risques ainsi que le chiffrage des pertes qu'ils pourraient générer ont également été évalués.

Elle est alors en capacité de constituer son Plan de Continuité d'Activité en choisissant pour chaque risque parmi les quatre options suivantes :

1. **Accepter le risque** : cela consiste à ne rien faire face au risque.
2. **Éviter ou supprimer le risque, en éliminant les conditions de sa réalisation** : on effectue alors un changement important qui fait que le risque ne s'applique plus.
3. **Réduire le risque, en jouant sur ses deux paramètres de probabilité d'occurrence et de coût/impact.**
4. **Transférer le risque à une autre entité par la sous-traitance ou l'assurance.**

Dans la suite de ce chapitre, nous allons voir comment les entreprises peuvent se préparer aux choix de suppression et de réduction des risques en développant leurs capacités de prévention, de protection, de détection mais également de réaction et réponse aux menaces cyber. Nous ne mentionnerons pas les deux autres options d'acceptation et de transfert même si cette dernière peut également être tout à fait pertinente pour couvrir certains risques cyber, comme en témoigne la très forte croissance actuelle du marché de la cyber-assurance.

Moyens de prévention et de protection

Mise en place d'un SOC

Il est vital pour chaque entreprise de se doter d'une capacité de traitement des incidents de sécurité informatique. Cette activité est clairement identifiée et organisée dans la plupart des grandes sociétés ou dans celles ayant un bon niveau de maturité sur les problématiques de sécurité de l'information. Mais ce n'est pas toujours le cas dans les plus petites structures où le traitement des événements et incidents de sécurité est englobé dans le cadre général du traitement des incidents informatiques.

Pour améliorer leur efficacité, les entreprises devraient donc mettre en place un SOC « *Security Operations Center* ». La mission d'un SOC peut varier d'une organisation à l'autre mais elle doit couvrir *a minima* les responsabilités de surveillance, détection et traitement des incidents de sécurité ainsi que l'administration de tous les moyens de sécurité mis en œuvre par la société pour protéger ses équipements (réseaux, serveurs, ordinateurs, *smartphones*,...).

Le SOC joue donc un rôle critique dans la prévention et la protection contre les menaces cyber. En établissant un processus de gestion des incidents de sécurité informatique, il donne un cadre clair pour que les salariés puissent signaler avec promptitude tout incident et éviter, grâce à un traitement rapide que la menace et ses impacts ne se propagent dans le SI. De même, en maintenant à jour le niveau de sécurité de tous les équipements du SI (*patching* des serveurs, mise à jour régulière des anti-virus...), le SOC réduit l'exposition de l'entreprise aux attaques. Ce point est particulièrement important quand on sait qu'une étude [11] a indiqué que 71 % des attaques ont exploité des vulnérabilités dont la correction était disponible depuis plus d'un an.

(11) Verizon – 2015 *Data Breach Investigation Report.*

Le SOC peut également mettre en œuvre des moyens complémentaires de prévention contre la perte de données. Ce sont, par exemple, les applications de type DLP (*Data Loss Prevention*) qui peuvent contrôler et bloquer l'accès à des données sensibles (qu'elles soient stockées dans le SI interne ou dans le *Cloud*) mais également empêcher qu'elles puissent être transférées vers l'extérieur de l'entreprise par messagerie ou *via* un réseau.

Le facteur humain : sensibilisation et éducation des salariés

Personne ne peut ignorer l'existence de risques de sécurité informatique. C'est devenu un élément de notre quotidien et nous avons été tous confrontés ou exposés au sujet dans nos vies personnelles (il suffit, pour preuve, de se référer au nombre de communications liées à la cybercriminalité et relayées dans la presse grand public). Mais il est frappant de voir combien peu de salariés se sentent **directement** concernés par cette problématique dans leur environnement professionnel. Cela tient soit à un « optimisme naïf » (« *cela n'arrive qu'aux autres* ») soit, pire, à la croyance que la société et son département informatique ont couvert tous les risques et traité le problème. Dans tous les cas, cela génère des impératifs d'éducation et d'information pour les entreprises vis-à-vis de leurs employés.

Guillaume POUPARD de l'ANSSI et François ASSELIN de la CGPME[12] parlent de l'enjeu fondamental de « *sensibiliser les collaborateurs de l'entreprise aux règles d'hygiène informatique* » et proposent une démarche intéressante et pragmatique pour cela. Ils listent un ensemble de douze recommandations et bonnes pratiques à respecter (sur des thématiques allant des politiques de mots de passe, de sécurisation des accès *wi-fi* jusqu'aux principes de séparation des usages informatiques personnels et professionnels) et les illustrent par des exemples concrets et vécus de désagréments que cela permet d'éviter.

(12) CGPME-ANSSI – Guide des bonnes pratiques de l'informatique.

Dans le même esprit et avec le même objectif d'engager les salariés à acquérir et adopter les bons comportements en matière de sécurité informatique, nous recommandons des approches innovantes d'éducation et de formation telles que le *serious game* « *Keep an Eye Out* » conçu au travers d'un partenariat entre l'INHESJ, le CIGREF et l'ANSSI. La sensibilisation au travers d'un *serious game* présente le bénéfice de susciter une implication et une appropriation fortes en évitant de traiter le sujet de manière trop théorique.

Des outils de contrôle d'accès et de protection des données

Comme évoqué en début de chapitre, les données sont un actif clef pour les entreprises et elles sont par ailleurs la cible prioritaire d'un grand nombre d'attaques cyber. Il faut donc apporter une attention toute particulière aux moyens de protéger ces données.

La première priorité consiste à mettre en œuvre une gestion robuste des **habilitations et des contrôles d'accès** aux données. En s'appuyant sur la cartographie détaillée présentée dans le paragraphe « *Patrimoine et actifs numériques "à protéger"* », l'entreprise devra sécuriser les conditions d'accès

aux données (quels que soient leur localisation et support) avec une attention plus particulière sur les données les plus sensibles ou les plus attractives. Les droits d'accès doivent également être revus de manière régulière pour vérifier qu'ils ont bien été adaptés au gré des changements de fonctions ou responsabilités des personnes dans l'organisation. Notons enfin que cette gestion des droits d'accès doit également permettre une **traçabilité des accès** (à des fins d'investigation technique mais également d'analyse d'imputabilité des transactions).

De plus, pour répondre aux règles de gestion qu'elle aura définies pour les données les plus sensibles, chaque entreprise pourra mettre en place une palette complémentaire de moyens de protection tels que :

- le chiffrement des disques, fichiers et e-mails ;
- des services d'anonymisation sur les plateformes de développement ou dans les échanges avec les partenaires ;
- des principes de cloisonnement strict des environnements (accès restreints au strict minimum pour les partenaires, utilisation de serveurs de rebonds pour l'administration) ;
- voire des solutions de DRM (*Digital Rights Management*).

Moyens de détection

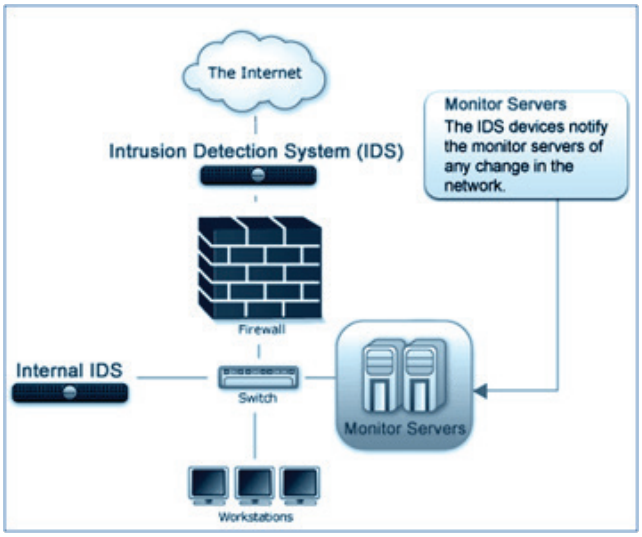
Les entreprises peuvent également mettre en place des moyens techniques et humains afin de renforcer la surveillance de leurs actifs numériques et de leur système d'information. Cela consiste à développer sa capacité de détection en mettant en place des **sondes techniques et humaines**.

Là encore, les SOC sont à la manœuvre. Ils peuvent tout d'abord utiliser des systèmes de détection d'intrusion (IDS *Intrusion Detection System*).

Il existe deux grandes familles d'outils de détection d'intrusion :

✓ ceux qui analysent les journaux des événements se produisant sur les équipements (en anglais, cette méthode est appelée « *host-based* ») ;

✓ ceux qui capturent et analysent le trafic en certain s points du réseau (en anglais, cette technique est appelée « *network-based* »).



Source image: interactivesys.net

Exemples d'outils de détection d'intrusion

Host-Based
- chkrootkit http://www.chkrootkit.org
- Tripwire http://tripwire.org
- md5sum http://www.md5summer.org/download.html

Network-based
- Snort http://www.snort.org
- TCPdump http://www.tcpdump.org

Les SOC peuvent également mettre en place des solutions SIEM (*Security Information Event Management*). Ce sont des applications qui fournissent une analyse en temps réel de l'ensemble des alertes de sécurité pouvant être émises par les équipements (réseau, base de données) ou les applications du SI.

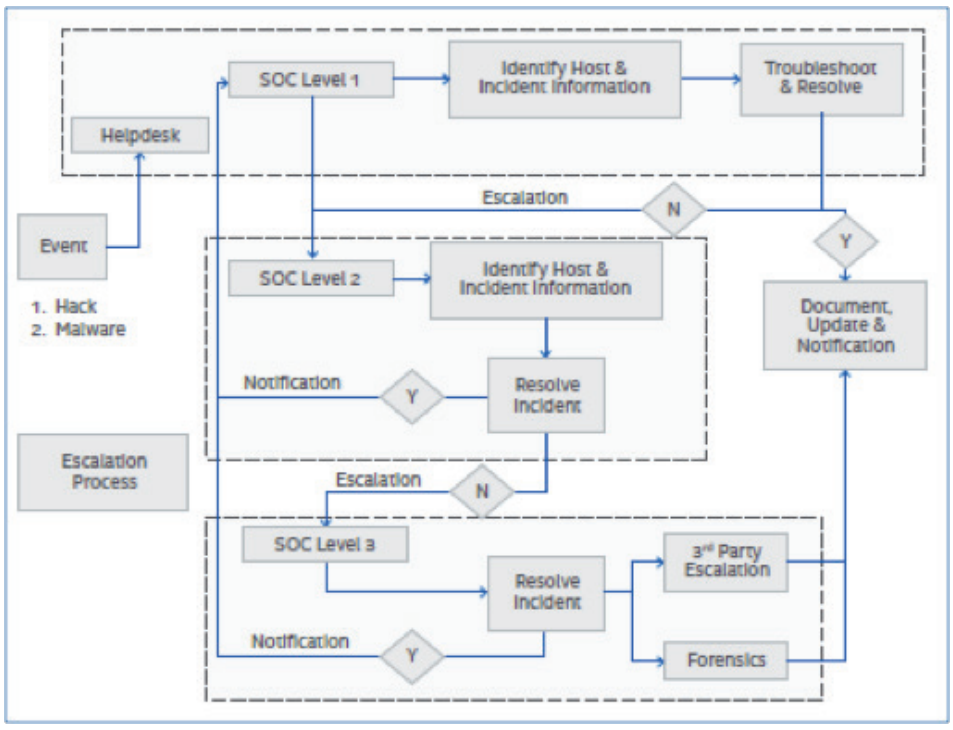
Moyens de réaction et de réponse

Un grand nombre d'entreprises ne survivraient pas à une interruption de leur système d'information pendant seulement trois jours. À l'heure où le principe de précaution prévaut, alors que les mesures de sécurité ont pour objectif de prévenir contre des menaces éventuelles, des approches nouvelles, organisationnelles et techniques se sont développées pour faire face aux conséquences des attaques et/ou des sinistres sur l'activité de l'entreprise.

Il faut donc non seulement **prévenir** mais aussi savoir **guérir**. Et cela peut également s'anticiper en termes d'organisation, de processus et de moyens.

Un SOC en place avec des procédures de réponse et une capacité à mobiliser rapidement des expertises complémentaires

Là encore, le SOC joue un rôle clef. Il doit non seulement développer sa capacité à contenir et répondre à des attaques en autonomie mais il doit également pouvoir faire appel à des expertises complémentaires nécessaires à la résolution de la crise en cas de besoin. Comme illustré dans le diagramme ci-dessous, le SOC s'est organisé pour pouvoir régler un certain nombre d'incidents de sécurité dans son groupe de niveau 1. Cela se fait essentiellement au travers de la formalisation de procédures préétablies (fiches Réponse) qui détaillent la liste des actions à exécuter pour répondre à certains types d'incidents. Quand le SOC niveau 1 ne trouve pas de réponse procédurée, il escalade à son niveau 2 (SOC niveau 2 ou CERT), qui lui-même peut avoir à escalader vers des partenaires externes à un niveau 3 en cas de besoin.



Source : MacAfee [13]

(13) 2013 - MacAfee - Creating and maintaining a SOC

http://www.mcafee.com/fr/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf

Le SOC documente ses activités et est en particulier responsable de formaliser la réponse aux incidents qu'il a traités dans des fiches Réponse qui permettront une résolution rapide si l'incident se reproduit.

Un Plan de Reprise d'Activité pour les parties critiques du SI

En informatique, un Plan de Reprise d'Activité (en anglais : *Disaster Recovery Plan* – DRP [14]) permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation.

(14) Wikipedia

Le plan de reprise d'activité doit donc permettre, en cas de sinistre sur une partie critique du SI, de basculer sur un système de relève capable de suppléer le système mis en défaut et donc assurer la continuité des services et opérations informatiques nécessaires à la survie de l'entreprise. Il existe plusieurs niveaux de capacité de reprise, et le choix doit dépendre des besoins exprimés par l'entreprise.

Le Plan de Reprise d'Activité (PRA) est donc une composante essentielle de tout Plan de Continuité d'Activité (PCA) et il doit être défini pour chaque partie critique du SI, en sus de toutes les autres mesures visant à se prémunir d'un sinistre.

Anticiper les situations de blocage opérationnel dans la gestion de crise

Une gestion de crise est un événement exceptionnel qui induit des modes de travail sortant du cadre normal de fonctionnement de l'entreprise. Et dans le même temps, les entreprises ont défini des procédures qui régissent justement leur fonctionnement normal en l'inscrivant dans le respect des lois et des réglementations externes. On peut donc se trouver dans une situation de blocage quand un traitement d'exception, réclamé de manière urgente par la cellule de crise, n'est pas prévu dans les procédures de la société.

Nous allons revoir dans ce chapitre des exemples de risques de blocage qui doivent être appréhendés en amont par les entreprises pour qu'elles puissent opérer efficacement en période de crise, tout en restant bien entendu dans la légalité. Et nous allons commencer notre exposé de manière très pratique avec la problématique du fonctionnement en 24/7 pour une cellule de crise.

Problématique du fonctionnement en 24/7

Imaginons, que dans sa gestion de crise, une entreprise décide de mobiliser un dispositif de crise composé de ressources internes et de prestataires externes, en mode 24/7.

Impact RH : elle devra d'abord s'assurer que les personnes internes pourront être mobilisées au-delà des conditions normales de leur contrat de travail mais tout en respectant les dispositions légales du code du travail. En France par exemple, cela pourrait conduire à prévoir pour les personnes concernées des contrats de travail dérogatoires aux contrats classiques qui précisent les conditions d'extension de la durée du travail (temps de travail étendu, modalités d'astreinte, l'extension exceptionnelle de la durée de travail, les taux de majoration des

heures travaillées de nuit ou le dimanche...) tout en respectant les contraintes légales (12 heures de repos quotidien, 36 heures de repos hebdomadaire, 6 jours de travail consécutifs maximum...). Bien entendu, ce type d'actions serait à adapter dans chaque pays, en fonction de son propre cadre légal et réglementaire.

Impact Achats : de même l'entreprise devra s'assurer qu'elle peut bien mobiliser les prestataires externes nécessaires dans son dispositif. Cela suppose que ces conditions d'intervention « en mode crise » soient clairement prévues et négociées dans les contrats de services externes.

Impact Services Généraux/Sécurité : imaginons maintenant que l'entreprise ait décidé d'installer son QG de crise sur un site qui ne fonctionne pas normalement en mode 24/7. Il faudra alors rapidement pouvoir en autoriser l'accès en mode 24/7 (cela peut nécessiter un processus spécial d'accréditation et d'attribution de badges d'accès) et mettre en œuvre des moyens logistiques pour les personnels mobilisés sur site (transfert sur site des personnes en taxi, mise en place d'un service de restauration...).

Autres points d'attention

Comme illustré précédemment pour le fonctionnement en mode 24/7, la meilleure démarche pour les entreprises consiste à intégrer en amont le cas des situations de crise dans ses règles et processus de fonctionnement tels que:

- PSSI ;
- Règlement intérieur ;
- Charte informatique ;
- Procédures écrites d'intervention sur poste, d'accès aux *logs*, d'information en cas d'usage présumé non conforme, etc. ;
- Procédure de gestion des droits d'accès ;
- Protection des données personnelles - informatique et liberté ;
- Politique et procédures Achats ;
- etc.

Donnons à nouveau un exemple pour illustrer ce point :

> Dans le cadre d'une crise, le manageur de la crise doit pouvoir engager immédiatement une prestation d'un montant important (> 500 K€) auprès d'une société externe (*Microsoft, Thales,...*).
>
> Mais il ne peut pas le faire car la politique Achats impose, pour un tel montant, de passer par un circuit de signataires qui ne sont pas tous d'astreinte et ne sont donc pas mobilisables rapidement.

Pour éviter ce blocage, l'entreprise pourrait par exemple intégrer dans sa politique Achats, la mise en place d'un *workflow* simplifié ou adapté aux situations de crise.

Il n'est évidemment pas possible de pouvoir prévoir à l'avance et en détail tous les cas possibles de traitements d'exception. Il convient donc également d'anticiper en décrivant de manière générale des **principes dérogatoires** aux règles dans les situations de crise.

Ces principes doivent néanmoins être manipulés avec précaution. En effet, s'ils permettent aux gestionnaires de crise de gagner en agilité et rapidité, ils ne doivent pas les exonérer de leur obligation d'opérer dans la légalité. Il faut donc que les traitements dérogatoires soient consignés par la cellule de crise et qu'ils fassent l'objet d'une revue, après la sortie de crise, par les responsables de la société. Et par la même occasion, il sera également utile de faire la revue de tous les points opérationnels qui, même s'ils n'ont pas fait l'objet d'un traitement dérogatoire, ont été difficiles à exécuter pendant la crise. Cela participera à l'amélioration continue du dispositif de gestion de crise.

Tester son dispositif de gestion de crise

Comme nous l'avons vu précédemment, préparer son dispositif de crise est essentiel. Mais le tester en le mettant à l'épreuve de situations réelles l'est tout autant. En effet, il y a toujours des écarts et des surprises lorsque l'on passe de la théorie à la pratique et il vaut mieux, pour les entreprises, les découvrir dans un contexte simulé sans enjeux opérationnels réels plutôt que lors d'une vraie crise.

Les entreprises ont donc tout intérêt à **s'évaluer** et à **s'entraîner** régulièrement en organisant des **exercices de gestion de crise** qui doivent viser un double objectif :

- **Tester le niveau de maturité de l'organisation et sa capacité de détection et d'escalade des incidents** jusqu'au déclenchement de la crise. Cela permettra en particulier de mesurer l'efficacité des programmes et formations de sensibilisation aux risques cyber et de s'assurer que les procédures sont bien comprises et appliquées, que la détection des incidents critiques et le processus de déclenchement de crise sont efficaces.
- **Tester la capacité de réponse opérationnelle du dispositif de crise.** Il s'agit dans ce cas de mettre à l'épreuve les capacités de mobilisation et de réponse des cellules de pilotage et cellule opérationnelle. Cela consiste donc, dans un premier temps, à mesurer l'efficacité dans la mise en œuvre des moyens et de la logistique du dispositif de crise (QG, équipements...). Mais cela doit également permettre à la cellule de s'entraîner en exécutant, en situation proche des conditions d'une crise réelle, des activités de protection et/ou réponses à des menaces (*patching*, confinement d'une partie du SI, activation du DRP...)

La nature et la sophistication des exercices doivent être définies en fonction du niveau de maturité de chaque entreprise, pour participer à l'amélioration continue progressive de sa gestion de crise cyber.

Et comme pour une crise réelle, chaque exercice devra se conclure par une phase de clôture et d'analyse *post-mortem* qui permettra d'améliorer les dispositifs.

Comme illustré au travers des quelques exemples ci-après, les exercices devraient être, dans un premier temps, plutôt conçus en complément des programmes de formation et sensibilisation des salariés aux enjeux de cyber sécurité. Et ils pourront ensuite évoluer vers des scenarii « grandeur nature » de crise qui reproduisent les conditions de stress des situations réelles et mobilisent l'ensemble des ressources internes (Direction générale, Juridique, Communication, SI,...) et externes (experts techniques, juridiques, organismes publics tels que l'ANSSI,...).

Exercice 1 : ***Attaque virale via clé USB***

Le **scénario** de cet exercice consiste à disséminer des clés USB contenant un *malware* inoffensif (!) mais générant une action inhabituelle sur le poste de l'utilisateur l'ayant utilisé (génération d'un e-mail, création d'un document...).

Et **l'objectif** est de mesurer la bonne application de la PSSI concernant l'utilisation des clés USB (d'un point de vue global et « **anonymisé** » car il ne s'agit pas de pointer du doigt les déficiences individuelles mais de mesurer le niveau de maturité collectif), et de tester la bonne utilisation de la procédure d'escalade d'incident et la bonne prise en charge et résolution par le SOC...

Exercice 2 : ***Compromission d'un poste administrateur***

Dans cet exercice, le **scénario** est celui d'un cybercriminel qui a pris le contrôle d'un compte administrateur et qui génère des actions inhabituelles sur un applicatif métier critique.

L'objectif est à nouveau de mesurer la rapidité de détection et escalade des incidents de la part des utilisateurs.

Exercice 3 : ***Test d'intrusion* - Penetration testing *(Pentest)***

Le principe de cet exercice est de commander une prestation externe de test d'intrusion dans le SI de l'entreprise. L'exercice pourra cibler une partie spécifique (par exemple les sites web externes) ou la totalité du SI. Et il pourra être conduit de différentes manières : tout d'abord en mode collaboratif avec les équipes externes en charge du test d'intrusion pour aller jusqu'à un mode « *double blind testing* [15] » très proche des conditions d'une attaque réelle (dans ce cas, les équipes internes ne sont pas informées de la tenue de l'exercice).

(15) http://searchsoftwarequality.techtarget.com/definition/penetration-testing

L'objectif de ces exercices est bien entendu de mesurer en situation réelle la capacité de détection et de protection de l'entreprise aux intrusions dans son SI.

Exercice 4 : ***Attaque rendant indisponible un* Data Center**

Le principe de cet exercice est de simuler l'indisponibilité d'une part critique de son SI (par exemple un *Data Center*) suite à une attaque. Les scenarii d'attaque peuvent être très divers car les *Data Center* présentent de nombreuses vulnérabilités (thermiques, électriques, adductions aux réseaux de fibres optiques ...).

Quel que soit le scénario retenu, l'objectif de l'exercice est de mesurer la capacité de l'entreprise à réagir à l'indisponibilité du *Data Center* et à exécuter le plan de reprise d'activité (DRP) correspondant.

Autres exercices

Les types de menaces sont très variés. On peut donc imaginer un grand nombre d'exercices supplémentaires qui exposent les dispositifs de détection et protection à toutes sortes d'attaques, comme par exemple :

– Des attaques physiques

- *vol d'équipements* : l'attaquant pourrait essayer de cibler l'ordinateur portable du directeur général, des *smartphones*, des photocopieurs ou les enregistrements de sauvegarde de l'organisation. Quelle que soit la cible,

le but est le même : extraire des informations critiques, des noms d'utilisateur et des mots de passe.

- *Intrusion physique* : le but de cette technique est de tester les contrôles physiques de l'entreprise. Des systèmes tels que les portes, les barrières, les verrous, les gardes, la vidéosurveillance et les alarmes sont testés pour découvrir s'ils peuvent être contournés...

– Des attaques logiques menées depuis l'intérieur de l'entreprise

- cette technique d'intrusion simule le type d'activité malveillante qui pourrait être effectué par une personne autorisée disposant d'une connexion légitime au réseau de l'organisation. Par exemple, si les règles d'accès sont trop permissives, un administrateur IT peut verrouiller les autres personnes à l'extérieur du réseau.

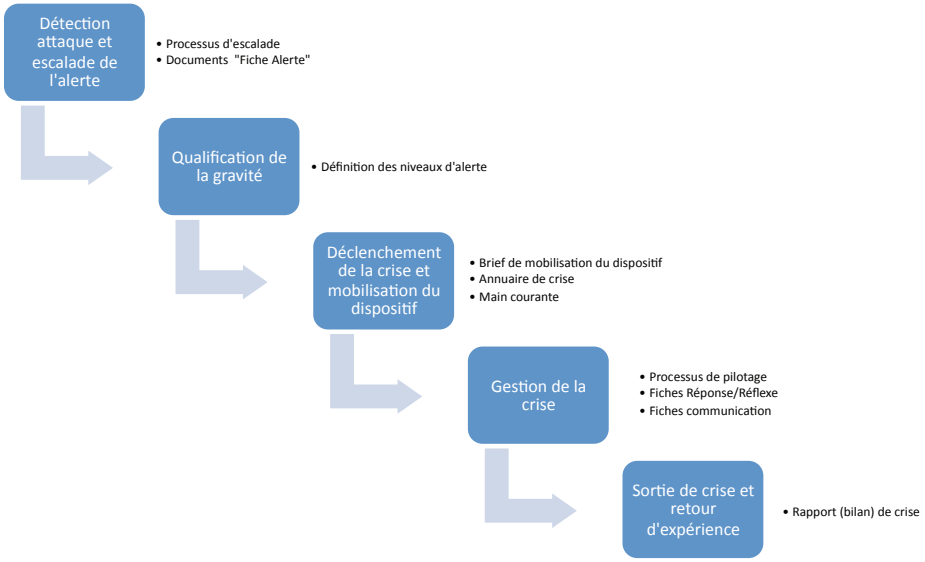
Vade-Mecum : modèles de documents opérationnels

Dans ce chapitre, nous allons présenter des modèles de document opérationnel qui permettent de guider les acteurs dans la bonne exécution de leurs activités dans le contexte d'une attaque cyber. Les documents que nous avons modélisés sont bien entendu génériques et devront être adaptés au contexte de chaque entreprise pour être réellement pertinents et utilisables en situation réelle. L'ensemble de ces documents constituera le Plan de Crise de l'entreprise et devra être partagé avec tous les acteurs appelés à intervenir lorsqu'une crise survient.

Nous avons organisé notre présentation de documents comme une succession d'éléments de réponse aux problématiques clefs rencontrées par les entreprises en période de crise.

Les problématiques clefs

Dans notre scénario d'attaque cyber, l'ensemble des phases clefs de la gestion de crise peut se représenter de la manière suivante :



Comme mentionné dans le diagramme, il est important d'établir pour chacune de ces étapes des processus et des documents qui décrivent et guident les acteurs dans la conduite des activités de chaque phase.

Ainsi dans la phase initiale de détection et escalade des alertes, un processus doit clairement définir à qui les alertes doivent être transmises, en fonction du type ou de la première évaluation de la criticité de l'attaque qui a été détectée. Ce processus est extrêmement difficile à modéliser de manière générique car il dépend fortement de l'organisation et de la répartition des rôles et responsabilités dans chaque entreprise. Mais il peut ensuite être détaillé sous la forme de fiches Alerte (*voir exemple d'une fiche alerte DDOS dans le chapitre suivant*) qui décrivent les noms et coordonnées des personnes à contacter pour chaque type d'attaque.

Ensuite, il convient de définir les principes d'évaluation de la gravité de chaque alerte. Cela peut être fait sous la forme d'une check-list de qualification du périmètre actuel de l'attaque, de son risque de propagation, de son impact actuel et futur et de son niveau de visibilité externe. Les modèles peuvent être plus ou moins sophistiqués mais aboutissent généralement à une échelle à 3 niveaux (vert → orange → rouge) dont le dernier peut conduire au déclenchement d'une crise. Un exemple d'une grille de définition de niveaux de gravité est présenté dans le chapitre « *Modèle de document : qualification d'alerte* ».

La phase suivante consiste à définir qui a autorité pour décider du déclenchement d'un dispositif de crise. Cela peut également être détaillé dans le processus de gestion des alertes adapté au contexte de chaque entreprise (décision prise par le Comité de direction, le responsable de la gestion des risques, le RSSI…). Et le Plan de Crise doit ensuite fournir des éléments qui guideront les organisations dans la mobilisation efficace de leur dispositif de crise (*voir les conseils pratiques pour mener une réunion de lancement du dispositif dans le chapitre* « Conseils pratiques pour la réunion de lancement d'une cellule de crise » *et des modèles d'annuaire et de main courante de crise dans les chapitres suivants*).

Pendant la gestion de crise proprement dire, les entreprises sont confrontées à des enjeux de pilotage et d'efficacité opérationnelle dans la réponse aux attaques (confinement, remédiation…). Là encore, le Plan de Crise doit fournir des processus et documents qui décrivent comment assurer ces activités. Les éléments clefs sont, pour cette phase, les fiches Réflexe ou Réponse qui donnent aux intervenants la description des tâches à mener en réponse à une situation donnée. Nous donnons deux exemples de telles fiches en fin de chapitre sur un aspect opérationnel et sur un aspect communication.

Modèle de document : fiche Alerte

Le document suivant est un exemple de fiche alerte permettant d'escalader la signalisation d'une attaque DDOS vers une cellule décisionnelle Groupe ou locale en fonction du périmètre de l'attaque.

Société XX - Fiche Alerte

Attaque DDOS

L'information arrive en général par le SOC, est communiquée au RSSI France / Groupe, en fonction du lieu/gravité d'impact et aux RSSI concernés.

S'assurer que les RSSI concernés sont avisés et que le SOC lance bien la mise en place d'une cellule de crise suivant la procédure concernée.

Attaque DDOS concernant un élément mutualisé important du groupe (passerelle Internet, backbone de messagerie, extranet)

Prévenir par téléphone

- le RSSI Groupe (XX.XX.XX.XX.XX)
- le responsable de l'équipe SOC (XX.XX.XX.XX.XX)
- l'astreinte technique du secteur concerné

Faire un email avec les informations connues aux destinataires suivants :

- le RSSI France et les RSSI concernés par l'élément mutualisé
- le DSI groupe
- le CTO groupe
- le responsable de l'équipe d'ingénierie groupe
- …

Attaque DDOS sur un élément cantonné de l'infrastructure en France

En fonction de la gravité et la nature de l'événement :

- le RSSI Groupe (XX.XX.XX.XX.XX)
- le responsable de l'équipe SOC (XX.XX.XX.XX.XX)
- l'astreinte technique du secteur concerné
- le RSSI de l'entité concernée

Faire dès que possible un email avec les informations connues aux destinataires suivants :

- le RSSI France et les RSSI concernés par l'élément (entité, site,…)
- le responsable de l'équipe SOC (XX.XX.XX.XX.XX)
- l'astreinte technique du secteur concerné
- les équipes locales (RSSI, équipe support proximité) concernées, pour obtenir des informations complémentaires sur les circonstances, les informations sur l'élément, etc.

Modèle de document : qualification d'alerte

Le niveau de gravité d'un incident de sécurité informatique peut être évalué, par exemple, grâce à l'échelle suivante, qui combine les 3 dimensions de qualification (type d'incident ou d'attaque), d'impact (estimation du risque et des dommages potentiels) et du périmètre (donnant la mesure de l'étendue de la menace).

En combinant ces trois dimensions, on peut obtenir la classification finale représentée dans le graphe ci-dessus avec les trois niveaux suivants :

- Niveau vert (Incident de niveau 1) : incidents évalués entre 1 et 4
- Niveau orange (Incident de niveau 2) : incidents évalués entre 6 et 9
- Niveau rouge (Incident de niveau 3) : incidents évalués entre 12 et 27

Qualification	Valeur
Vulnérabilité	1
Evénement	2
Incident prouvé	3

Impact	Valeur
Faible	1
Moyen	2
Elevé	3

Périmetre	Valeur
Local	1
National	2
Multinational	3

Qual. \ Per.	1	2	3
1	1	2	3
2	2	4	6
3	3	6	9

Impact \ Qual.*Per.	1	2	3	4	6	9
1	1	2	3	4	6	9
2	2	4	6	8	12	18
3	3	6	9	12	18	27

Cette classification permet ensuite de définir les seuils de déclenchement et le dimensionnement de la cellule de crise. Par exemple, on peut décider du déclenchement de la crise dès que les sous-paramètre Type et Impact sont évalués à 3 (incident confirmé avec impact élevé). Et le sous-paramètre Périmètre permettra de définir si la cellule de crise sera gérée, par exemple, à un niveau Groupe ou à un niveau national.

Conseils pratiques pour la réunion de lancement d'une cellule de crise

Effectuer une première réunion rapide, pilotée par l'équipe de direction, lors de la mise en place de la cellule de crise avec les différents acteurs :

- Exposer la situation de crise
- Définir le rôle de chacun en s'appuyant sur les fiches de poste et les fiches réflexe/réponse préalablement établies

Planifier les actions à l'aide du plan de crise

- Et établir les modalités de pilotage (planification des points de situation, définition des indicateurs de suivi…)

Etablir une main courante afin d'assurer le suivi de la situation

Informer et communiquer :

- Fixer les règles de diffusion de l'information
- Rappeler les règles de confidentialité (en interne et externe)

Modèle de document : équipement matériel de la cellule de crise

Voici un exemple non exhaustif

Informatique / bureautique	postes téléphoniques, télécopieurs ; téléphones portables dédiés ; système autonome fournissant de l'électricité ; L.A.N. autonome avec micro-ordinateurs et une imprimante ; annuaires de crise informatisés (internes et externe) ; main courante informatisée ; vidéo projecteur ; visio-conférence ; paper board et/ou tableau blanc ; marqueurs et/ou stylos spécifiques ; ensemble de ressources en papeterie (bloc, post-it,…) ;…
Documentations	annuaire de crise interne ; annuaire de crise externe ; plan du site avec emplacement de la cellule ; main courante papier ; registre pour annotation des points de situation et suivi du déroulement de gestion de crise.

Modèle de document : annuaire de crise

Ces fiches doivent être constamment mises à jour et un état des absences doit être fait avant le déclenchement de la gestion de crise. Les absents seront simplement barrés.

ANNUAIRE CELLULE DECISIONELLE

CELLULE Nom de la cellule	FONCTION ~~Personne absente~~	NOM Prénom NOM	TÉLÉPHONE Ligne PRO - **Poste**	PORTABLE Ligne PRO 24/24
ÉQUIPE DE DIRECTION	DIRECTEUR	Xxxxxxxxx XXXXXXX	+(33)0.00.00.**00.00**	+(33)0.00.00.00.00
	S/DIRECTEUR (1)	Xxxxxxxxx XXXXXXX		
	S/DIRECTEUR (2)			
	D.S.I.			
	DIR. R.H.			
	DIR. BUDGET			
	DIR. COM			
ÉQUIPE COORDINATION ET SYNTHÈSE	COORDONNATEUR LOCAL #1			
	COORDONNATEUR LOCAL #2			
	SECRÉTAIRE			
	RESPONSABLE MAIN COURANTE			

ANNUAIRE(S) CELLULE(S) OPERATIONNELLE(S)

CELLULE Nom de la cellule	FONCTION ~~Personne absente~~	NOM Prénom NOM	TÉLÉPHONE Ligne PRO - **Poste**	PORTABLE Ligne PRO 24/24
ÉQUIPE DE COORDINATION OPERATIONNELLE	REPRÉSENTANT DIRECTEUR	Xxxxxxxxx XXXXXXX	+(33)0.00.00.**00.00**	+(33)0.00.00.00.00
	COORDONNATEUR			
	SECRÉTAIRE			
	COMMUNICANT			
ÉQUIPE INFORMATIQUE	TECHNICIEN A.S.			
	TECHNICIEN			
	EXP. JURIDIQUE			
ÉQUIPE LOGISTIQUE …	GEST.INFRA			
	LOGISTICIEN			

ANNUAIRE PRESSE

MÉDIA - TYPE	FONCTION	NOM Prénom NOM	TÉLÉPHONE Ligne PRO - **Poste**	PORTABLE Ligne PRO 24/24
NOM DU MÉDIA AUDIOVISUEL	DIRECTEUR			
	CONTACT			
NOM DU MÉDIA PRESSE LOCALE	DIRECTEUR			
	CONTACT			
NOM DU MÉDIA NATIONAL	DIRECTEUR			
	CONTACT			

ANNUAIRE PRESTATAIRES

NOM ET TYPE PRESTATAIRE	FONCTION	NOM Prénom NOM	TÉLÉPHONE Ligne PRO - **Poste**	PORTABLE Ligne PRO 24/24
XXXXXXX / XXXXXXX	DIRECTEUR			
	CONTACT			
XXXXXXX / XXXXXXX	DIRECTEUR			
	CONTACT			
	CONTACT			

ANNUAIRE REPRÉSENTANTS NATIONAUX DE L'ÉTAT

SERVICE	SITUATION GÉOGRAPHIQUE	Prénom NOM DU CONTACT	TÉLÉPHONE Ligne PRO - **Poste**
SOUS-DIRECTION DE LUTTE CONTRE LA CYBERCRIMINALITÉ	PARIS	-	
DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE	PARIS	-	
BRIGADE D'ENQUÊTE SUR LES FRAUDES AUX TECHNOLOGIES DE L'INFORMATION	PARIS	-	
CENTRE DE LUTTE CONTRE LES CROMINALITÉS NUMÉRIQUES	PARIS	-	
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTEMES D'INFORMATION	PARIS	-	
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTEMES D'INFORMATION	ANTENNE REGIONALE	-	
CERT-FR	N.C.		

Modèle de document : main-courante de crise

La main courante peut être sous forme papier ou informatisée. Elle est la trace de tous les événements se déroulant entre le déclenchement et la fin de la crise.

En trace papier, le début du document doit préciser :

- la date et l'heure du démarrage de la cellule de gestion de crise ;
- la liste des présents et les fonctions tenues ;
- le nombre de page dans le registre, et à ce titre, toutes les pages seront numérotées.

Dans l'exemple proposé ci-dessous figurent :

Le n° d'enregistrement	N° d'inscription sur le cahier, référence principale lors d'une recherche
Type de message	En cas de recherches, 3 possibilités peuvent être envisagées
Heure	L'heure d'arrivée à la cellule (l'enregistrement est la première chose à faire avant l'exploitation
Objet	Retranscrire intégralement l'objet du message arrivé
Dest	Equipe(s) destinataire(s) du message
Réponse	Faite à un message et/ou numéro d'enregistrement d'un départ de nouveau message

Exemple :

N° enregistrement	……..	□ Point de situation	☑ Mess. entrant	□ Mess. sortant
Heure	8 : 00	Objet :	……	
Exp :	……	Dest :	Équipe(s)……	
Réponse :	Ex : message sortant enregistré sous ……			
N° enregistrement	…….	☑ Point de situation	☐ Mess. entrant	☐ Mess. sortant
Heure	8 : 00	**Objet :**	……	
Exp :	……	**Dest :**	Équipe(s)……	

Modèle de document : fiche Réflexe

Le document suivant est un exemple de fiche réflexe permettant de guider les actions des équipes en termes de réponse dans le cas d'une détection d'une intrusion sur un poste de travail de l'entreprise.

Société XX - Fiche Réflexe

Réponse à détection d'intrusion sur ordinateur

1- Déconnecter la machine du réseau

Déconnecter du réseau la machine compromise (ou les machines) permet de stopper l'attaque si elle est toujours en cours. S'il était toujours connecté à la machine, l'intrus n'a plus de contrôle sur celle-ci et ne pourra donc pas surveiller ce que vous faites et/ou modifier des fichiers. En revanche, **maintenez la machine sous tension et ne la redémarrez pas**, car il serait alors impossible de connaître les processus qui étaient actifs au moment de l'intrusion. Vous risqueriez de provoquer une modification sur le système de fichiers et de perdre de l'information utile pour l'analyse de l'attaque.

2- Prévenir le responsable sécurité

Prévenez immédiatement le responsable sécurité et votre hiérarchie qu'une intrusion a été détectée. Prévenez-les de préférence par téléphone ou de vive voix, car l'intrus est peut-être capable de lire les courriers électroniques échangés, depuis une autre machine du réseau.

Coordonnées du RSSI : XX.XX.XX.XX.XX

3- Faire une copie physique du disque

Attention, la copie physique d'un disque dur est une opération très délicate. N'hésitez pas à faire appel à votre CERT (Coordonnées CERT: XX.XX.XX.XX.XX) pour plus de détails sur la façon de procéder.

L'intervention d'un huissier « spécialisé » en cyber peut s'avérer nécessaire pour la constatation et la validité de la procédure entreprise. Une compromission des traces peut s'avérer désastreuse en cas de procédure pénale. Gardez une trace écrite de tout ce que vous faîtes avec un maximum de détails…

3-1 Pourquoi faire une copie du disque ?

D'une part, en l'absence de copie, l'altération des données provoquée par l'analyse rendrait inefficace toute procédure judiciaire, si vous souhaitiez mener cette démarche. D'autre part, même si aucune action judiciaire n'est envisagée, vous pourrez tout de même avoir besoin dans le futur d'une copie exacte du système tel qu'il était au moment de la découverte de l'intrusion.

3-2 Pourquoi faire une copie physique du disque ?

Une simple sauvegarde de fichiers ne fournit pas l'intégralité des informations contenues sur le disque, il est donc important de procéder à une copie de bas niveau du disque, y compris des secteurs non occupés.

Modèle de document : fiche Réflexe Communication

Le document suivant est un exemple de fiche réflexe permettant de guider les actions des équipes communication en termes de réponse à une information d'attaque informatique concernant l'entreprise XX relayée dans la presse..

Société XX - Fiche Réflexe Communication

Réponse à article presse sur attaque informatique concernant la société XX

Définition du niveau de gestion de la communication

- Pour les événements d'une particulière gravité ou pour toute information sensible divulguée par la presse, la stratégie de communication est coordonnée avec le DSI Groupe et RSSI Groupe, en relation directe avec le Comité Exécutif.

Etablir les messages de première heure

- Montrer que la société a pris la mesure de la situation
- Communiquer sur les premiers faits connus et certains
- Définir le rythme et les modalités de diffusion de l'information aux media…

Rassembler les supports essentiels à la communication

- Faits et chiffres sur la crise
- Modèles de communiqués de presse et dossiers de presse
- Questions/réponses détaillées par acteurs clefs…

Préparer des éléments de réponse aux 4 questions habituelles des journalistes

- Que fait votre entreprise pour faire face à la situation ?
- Y avait-il un moyen d'éviter cette situation ?
- Quand avez-vous appris la situation ? Qu'avez-vous fait depuis ?
- Est-ce votre faute ? Si non, comment savez-vous que ce n'est pas votre faute ?

Formaliser les éléments de langage

- La société XX ne commente pas les accidents auprès de la presse.
  - Comme toutes les grandes entreprises, la société XX fait l'objet d'attaques régulières. Cependant, nos dispositifs de sécurité montrent chaque jour leur efficacité quant à la détection et à la protection vis-à-vis de tentatives d'attaques.
  - La sécurité des systèmes d'information est une préoccupation permanente au sein de la société XX. Nous menons constamment des actions pour améliorer nos dispositifs de sécurité et répondre à l'évolution des menaces.

CONCLUSION

La lutte contre la cybercriminalité est-elle perdue ?[16] Le simple fait de se poser la question montre clairement l'étendue du problème pour les entreprises. Et l'analyse du contexte actuel et de l'évolution de la cybercriminalité peut venir renforcer nos doutes et notre pessimisme sur la question.

En effet, l'attaque a toujours un temps d'avance sur la défense. En innovant et créant continuellement de nouvelles armes, les cybercriminels peuvent contourner les mécanismes de défense que les entreprises ont bâtis sur la base des menaces « anciennes » qu'elles connaissaient. De plus, la confrontation est déséquilibrée car asymétrique. D'un côté, les cybercriminels dédient toutes leurs ressources et énergie aux attaques cyber. Alors que de l'autre, les entreprises sont concentrées sur leur métier et la conduite de leurs affaires et ne voient donc les enjeux de défense cyber que comme un « mal nécessaire » et une affaire de spécialistes.

Mais alors, à quoi bon investir dans la cyber sécurité et dans la gestion de crise cyber ?

Friedrich Nietzsche nous donne la réponse au travers de son adage : « ***tout ce qui ne nous tue pas nous rend plus fort*** ». En effet, la première mission d'un dispositif de gestion de crise est de faire en sorte que la société « survive » à une attaque et à ses conséquences. Et comme nous l'avons vu tout au long de ce mémoire, sa capacité à répondre et à contenir les impacts négatifs des attaques dépendra fortement de son niveau de préparation et d'anticipation. Mais sa mission consiste également à tirer les enseignements de chaque crise pour améliorer son dispositif. Nous ne souhaitons évidemment pas aux entreprises d'être attaquées pour progresser mais nous les invitons néanmoins à considérer chaque incident de sécurité auquel elles sont déjà confrontées aujourd'hui comme une opportunité d'apprendre, de s'améliorer mais également d'éduquer et de sensibiliser l'ensemble de leur organisation.

En étant plus fort dans leurs capacités de détection et de réponse et en impliquant plus directement l'ensemble de leurs salariés et partenaires dans la prévention et dans la protection, les entreprises vont rééquilibrer la confrontation avec les cybercriminels et la rendre plus symétrique. Mais elles vont aussi gagner un avantage concurrentiel majeur par rapport à toutes celles qui, en n'ayant pas fait ces investissements, vont devenir des cibles privilégiées car des proies plus faciles.

(16) Juillet 2014 – *Huffington Post* - La lutte contre la cybercriminalité est-elle perdue ?

http://www.huffingtonpost.fr/cyrille-badeau/lutte-cybercriminalite-perdue_b_5595494.html?utm_hp_ref=france

BIBLIOGRAPHIE

- Juin 2013 – *Business les Echos* – Cyber-attaques : se préparer pour réagir efficacement. http://business.lesechos.fr/directions-numeriques/cyber-attaques-se-preparer-pour-reagir-efficacement-7388.php?j1gottKMHGbi50x5.99
- October 2014 – EY – *Get ahead of cybercrime* – EY's Global Information Security Survey 2014.
- October 2013 – EY – *Under Cyber Attack* – EY's Global Information Security Survey 2013.
- June 2014 – MacAfee & CSIS – *Net Losses: Estimating the global cost of cybercrime*. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
- 2015 – Verizon – *2015 Data Breach Investigations Report.*
- April 2014 – Symantec – *2014 Internet Security Threat Report.*
- Mai 2014 – INSA Toulouse & SOLUCOM – *Qualité et gouvernance des SI : La gestion de crise.*
- Avril 2012 – SOLUCOM – *Attaques ciblées : Quelles évolutions dans la gestion de crise ?*
- 2013 – MacAfee – *Creating and maintaining a SOC* http://www.mcafee.com/fr/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf
- Janvier 2010 – INHESJ – Gérard PARDINI – *Gestion de Crise.*
- Juillet 2014 – *Huffington Post* - La lutte contre la cybercriminalité est-elle perdue ? http://www.huffingtonpost.fr/cyrille-badeau/lutte-cybercriminalite-perdue_b_5595494.html?utm_hp_ref=france
- 2005 – *Le magazine de la communication de crise et sensible* – Christophe ROUX-DUFORT – Gestion de crise – Premiers réflexes pour le pilotage – Guide pour les managers. http://www.communication-sensible.com
- 2012 – Éditions de l'entreprise DUNOD - Emmanuel BLOCH – *Communication de crise et media sociaux.*

FICHES DE CONTACTS GOUVERNEMENTAUX

CONTACTS GOUVERNEMENTAUX

NOTICE

Les éléments suivants vous aideront à avoir les bons réflexes et à contacter les bons correspondants.

La cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales susceptibles de se commettre sur les réseaux de télécommunication ou ciblant ces mêmes réseaux. Cette tentative de définition recouvre deux réalités :

- **Les infractions spécifiques aux technologies de l'information et de la communication parmi lesquelles :**

  - les atteintes aux Systèmes de Traitement Automatisé de Données (S.T.A.D.) sanctionnées par les articles L.323-1 et suivants du Code pénal;
  - les atteintes aux droits de la personne liés aux fichiers ou traitement informatiques (art. 226-16 à 226-24 du Code pénal / Loi 78-17 du 6 janvier 1978 dite « informatique et liberté » modifiée par la loi 2004-801 du 6 aout 2004).

- **Les infractions dont la commission est liée ou facilitée par l'utilisation des technologies de l'information et de la communication, parmi lesquelles :**

  - les atteintes aux mineurs (article 227-23 du Code pénal);
  - les infractions à la loi sur la presse (loi du 29/07/1881);
  - les atteintes aux personnes (menaces, usurpation d'identité…);
  - les escroqueries (phishing, fausse loterie, utilisation frauduleuse de moyens de paiement…).

Si vous êtes victime d'infractions mentionnées ci-dessus, vous pouvez directement déposer plainte auprès d'un service de Police nationale ou de Gendarmerie nationale ou bien adresser un courrier au Procureur de la République près le Tribunal de Grande Instance compétent.

Les fiches suivantes vous aideront à prendre contact, en fonction du périmètre, avec le service spécialisé dans le traitement judiciaire de la cybercriminalité.

FICHE	SERVICE CONCERNÉ
FICHE 1CY/GOUV	SOUS-DIRECTION DE LUTTE CONTRE LA CYBERCRIMINALITÉ DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE
FICHE 2CY/GOUV	BRIGADE D'ENQUETE SUR LES FRAUDES AUX TECHNOLOGIES DE L'INFORMATION CENTRE DE LUTTE CONTRE LES CRIMINALITÉS NUMÉRIQUES DU SERVICE CENTRAL DU RENSEIGNEMENT CRIMINEL DE LA GENDARMERIE NATIONALE
FICHE 3CY/GOUV	AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANNUAIRE CRISE **CONTACTS GOUVERNEMENTAUX** 1CY/GOUV

SOUS-DIRECTION DE LUTTE CONTRE LA CYBERCRIMINALITÉ (SDLC)

France – Particuliers & PME

Service interministériel qui dépend de la Direction Centrale de la Police Judiciaire (DCPJ). Cette Sous-direction reprend les missions traditionnelles de l'Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC) auxquelles doit être ajoutée celle de plateforme de signalement et d'orientation technique et judiciaire.

Infractions traitées : Piratages, fraudes aux moyens de paiement, téléphonie et escroqueries sur Internet.

SDLC/OCLCTIC

Téléphone : Tél. : +33(1) 47 44 97 55
Courriel : secretariat.anssi@ssi.gouv.fr

Site Internet :
http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite

Services de signalements en ligne de contenus illégaux sur l'Internet :
https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action

Plateforme téléphonique « Info-escroqueries » : 0811 02 02 17

DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE (DGSI)

France – État, secteurs protégés, OIV

La DGSI dépend du Ministère de l'Intérieur. Créée en mai 2014 à la suite de la DCRI (Direction Centrale du Renseignement Intérieur), cette direction générale en poursuit les missions de protection des intérêts fondamentaux de la Nation.

Infractions traitées : Actes de piratage ciblant les réseaux d'État, les établissements composés de Zones à Régime Restrictif et les Opérateurs d'Importance Vitale.

DGSI

Téléphone +33(1) 77 92 50 00 / Courriel : secretariat.anssi@ssi.gouv.fr

ANNUAIRE CRISE **CONTACTS GOUVERNEMENTAUX** 2CY/GOUV

BRIGADE D'ENQUETE SUR LES FRAUDES AUX TECHNOLOGIES DE L'INFORMATION (BEFTI)

Paris et petite couronne – Particuliers & PME

La BEFTI dépend de la Direction Régionale de la Police Judiciaire de Paris (DRPJ-PARIS). Composée de groupes d'enquêtes spécialisés et d'un centre d'assistance technique, cette brigade est compétente pour les investigations relatives aux actes de piratage sur Paris et ses trois départements limitrophes (92, 93 et 94).

BEFTI

Téléphone : +33 (0)1 55 75 26 19

Site Internet :
http://www.prefecturedepolice.interieur.gouv.fr/Nous-connaitre/Services-et-missions/Missions-de-police/La-direction-regionale-de-la-police-judiciaire/La-brigade-d-enquetes-sur-les-fraudes-aux-technologies-de-l-information

CENTRE DE LUTTE CONTRE LES CRIMINALITÉS NUMÉRIQUES DU SERVICE CENTRAL DU RENSEIGNEMENT CRIMINEL DE LA GENDARMERIE NATIONALE (C3N)

France – Particuliers & organismes

Ce centre dépend du Pôle judiciaire de la Gendarmerie nationale. Service à compétence judiciaire nationale, il regroupe l'ensemble des unités du PJGN qui traitent directement de questions (formation, veille et recherche, investigation, expertise) en rapport avec la criminalité et les analyses numériques (Département Informatique-Electronique de l'IRCGN). Il assure également l'animation et la coordination au niveau national de l'ensemble des enquêtes menées par le réseau gendarmerie des enquêteurs numériques.
Domaine de compétence : atteintes aux STAD, infractions visant les personnes et les biens.

SCRC/C3N

Téléphone : +33 (0)1 58 66 59 99

Site Internet :
http://www.gendarmerie.interieur.gouv.fr/fre/Notre-Institution/Nos-missions/Police-judiciaire/Cybercriminalite

ANNUAIRE CRISE **CONTACTS GOUVERNEMENTAUX** 3CY/GOUV

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

France – État, secteurs protégés, OIV

Service à compétence nationale, l'ANSSI est rattachée au Secrétaire général de la défense et de la sécurité nationale. Le SGDSN assiste le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.
Infractions traitées : Piratages, fraudes aux moyens de paiement, téléphonie et escroqueries sur Internet.

SGDSN/ ANSSI

Téléphone : +33 (0)1 71 75 84 05 ou +33 (0)1 71 75 84 06
Télécopie : +33 (0)1 71 75 84 00
Courriel : secretariat.anssi@ssi.gouv.fr

Site Internet :
http://www.ssi.gouv.fr

SGDSN/ANSSI/CERT-FR

Téléphone : +33 (0)1 71 75 84 50
Télécopie : +33 (0)1 71 75 84 20
Courriel : certa-svp@certa.ssi.gouv.fr

Lien CERT :
http://www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html

Lien plateforme signalements SPAM :
https://www.signal-spam.fr