LES DOSSIERS TECHNIQUES

Gestion des incidents de sécurité du système d'information (SSI)

Mai 2011

Groupe de travail « Gestion des incidents »

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS
11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.asso.fr – www.clusif.asso.fr

Table des matières

Table des figures

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Les responsables successifs du groupe de travail :

Robert	**BERGERON**	*CAPGEMINI*
Witold	**POLOCZANSKI**	*CAPGEMINI*

Les contributeurs :

Michel	**BERTIN**	
David	**BIZEUL**	*SOCIETE GENERALE*
Annie	**BUTEL**	*BNP PARIBAS*
Philippe	**LARUE**	*CBP*
Sébastien	**MAUPTIT**	*SYSTALIANS*
Lionel	**MOURER**	*ESR CONSULTING*
Gérard	**PETITIT**	*GRAS SAVOYE*
Dominique	**POURCELLIE**	*CNAMTS*
Manuel	**PRIEUR**	*HP ENTERPRISE SERVICES*

Nous remercions aussi les nombreux adhérents du CLUSIF ayant participé à la relecture.

1 - Introduction

La notion d'incident est très large et couvre des domaines variés : incident technique, incident fonctionnel, incident social, incident de sécurité, incident de communication, incident de paiement, incident financier, etc. D'une manière générale, un incident peut être défini comme un événement causant des dommages ou susceptible de le faire à des personnes ou à des organisations.

Concernant les Systèmes d'Information, il existe différentes définitions de la notion d'incident :

- pour le COBIT :
  Incident informatique : tout évènement qui ne fait pas partie du fonctionnement normal d'un service et qui cause, ou peut causer, une interruption ou une réduction de la qualité de ce service (IT Incident, définition conforme à l'IT Infrastructure Library, ITIL),
  Problème : en informatique, cause à la base d'un ou de plusieurs incidents.

- pour ITIL :
  Incident : tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service.
  Problème : la cause inconnue d'un incident significatif ou la collection de plusieurs incidents présentant les mêmes symptômes. La gestion des problèmes consiste en une analyse visant à anticiper les incidents à venir.

- pour l'ISO 27000 (sécurité de l'information) :
  Incident : un ou plusieurs évènements intéressant la sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information [ISO/CEI TR 18044:2004[1]].

Quelle que soit l'approche, la gestion des incidents a pour objectif la détection et le traitement des incidents (à priori et à posteriori). Le processus de gestion des incidents inclut en général la détection de l'incident, les analyses et diagnostics, la résolution de l'incident et/ou le rétablissement du service affecté. Un aspect important de la gestion des incidents est le suivi (reporting) de ce processus et la capitalisation (bilan).

La qualité de service et la performance des organisations exigent la mise en place d'une gestion efficace des incidents et des problèmes. La gestion des incidents est également un dispositif amont essentiel du Plan de Reprise d'Activité car elle définit les procédures d'escalade qui permettent d'être plus réactif pour le déclenchement des plans de secours.

[11] La norme ISO/CEI TR 27035 en préparation va remplacer cette norme prochainement.

2 - Périmètre du document

2.1. Objectifs du document

Ce document n'a pas pour ambition de couvrir tous les types d'incident. Son objet est de constituer un guide de mise en place d'un système de gestion des incidents de Sécurité du Système d'Information et d'apporter une aide à la classification et à l'analyse de ces incidents. Il fournit également en annexe des fiches de recommandations pour les incidents de sécurité les plus courants.

Le document concerne donc principalement dans une organisation, les personnes en charge de :

- la Sécurité du Système d'Information (RSSI, administrateurs de la sécurité, correspondants sécurité, etc.),
- la gestion des risques (suivi et évaluation des risques avérés),
- le contrôle interne, l'audit, l'inspection, le contrôle périodique,
- la qualité (taux de disponibilité, fréquence des événements, etc.),
- la production.

Les raisons qui conduisent à la mise en place d'un système de gestion des incidents peuvent être diverses, par exemple :

- la décision de mise en place d'un processus d'amélioration continue,
- la nécessité de se conformer aux exigences réglementaires du secteur d'activité,
- la mise en œuvre d'un plan sécurité avec un objectif de réduction du nombre et de l'impact des incidents,
- la décision d'améliorer la gestion d'incidents existante (meilleure réactivité, meilleure efficacité du traitement des incidents, etc.),
- la mise en place de « procédures d'escalade » dans le cadre d'un projet d'élaboration d'un Plan de Continuité d'Activité (PCA), d'un Plan de Gestion de Crise, etc.,
- la volonté de mettre en place un SMSI, voire d'obtenir une certification (ISO 27001 par exemple).

2.2. Définition d'un incident SSI dans le cadre de ce document

La suite du document concerne les incidents de Sécurité du Système d'Information (SSI). Mais qu'est-ce qu'un incident SSI exactement?

Reprenant les définitions citées dans l'introduction, nous désignerons par incident SSI un événement, potentiel (au sens « signes précurseurs ») ou avéré, indésirable et/ou inattendu, impactant ou présentant une probabilité forte d'impacter la sécurité de l'information dans ses critères de Disponibilité, d'Intégrité, de Confidentialité et/ou de Preuve.

Un incident SSI correspond à une action malveillante délibérée, au non-respect d'une règle de la Politique de Sécurité du Système d'Information (PSSI) ou, d'une manière générale, à toute atteinte aux informations, toute augmentation des menaces sur la sécurité des informations ou toute augmentation de la probabilité de compromission des opérations liées à l'activité.

Concernant la disponibilité, on fera la différence entre les sinistres majeurs (incendie, inondation, etc.) nécessitant l'activation d'une cellule de crise et les autres incidents (panne d'un serveur). Une atteinte à la disponibilité pourra être considérée comme étant un incident de sécurité (déni de service suite à intrusion) ou non (panne de serveur suite à défaillance d'un composant), après analyse des causes.

3 - Organisation de la gestion des incidents SSI

3.1. Introduction

La mise en œuvre d'un processus de gestion des incidents de sécurité nécessite la définition :

- du périmètre,
- des objectifs (politique de gestion des incidents),
- des mesures (processus, bonnes pratiques, etc.),
- des moyens associés (organisation des ressources matérielles / humaines / budgétaires).

3.2. Politique de gestion des incidents de sécurité

Une politique de gestion des incidents de sécurité passe par la définition de deux objectifs majeurs :

- garantir que le mode de notification des événements et des failles liés à la sécurité de l'information permet la mise en œuvre d'une action complémentaire ou corrective dans les meilleurs délais,
- garantir la mise en place d'une approche cohérente et efficace pour le traitement des incidents liés à la sécurité de l'information.

3.3. Les Mesures à mettre en place

Les mesures suivantes sont essentielles à l'atteinte de ces deux objectifs.

1. *Les événements liés à la sécurité de l'information doivent être signalés, dans les meilleurs délais, par les circuits appropriés*

Bonnes pratiques :

- des procédures formelles de signalement, de remontée d'informations et de réponses en cas de détection d'un incident lié à la sécurité de l'information doivent définir les mesures à prendre à la réception d'un appel signalant un tel événement,
- le Service Desk, l'équipe de réponse aux incidents et le RSSI peuvent être les points d'entrée pour le signalement des événements liés à la sécurité de l'information,
- tous les utilisateurs doivent être informés des points d'entrée, des procédures de signalement et de leur obligation de signaler tout événement lié à la sécurité de l'information dans les meilleurs délais (charte, sensibilisation).

2. *Il doit être demandé à tous les salariés, contractants et utilisateurs tiers des systèmes et services d'information de noter et de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services*

Bonnes pratiques :

- tous les salariés, contractants et utilisateurs tiers sont tenus de signaler ce type de problème au Service Desk, dans les meilleurs délais, afin d'éviter tout incident lié à la sécurité de l'information,
- le mécanisme de signalement doit être le plus simple, le plus accessible et le plus disponible possible. Il est recommandé à ces personnes de ne jamais tenter d'apporter la preuve de failles de sécurité soupçonnées.

3. *Des responsabilités et des procédures doivent être établies, permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information*

Bonnes pratiques :

- outre le signalement des événements et failles liés à la sécurité de l'information, il est recommandé de mettre en place une surveillance des systèmes, des alertes et des vulnérabilités afin de détecter les incidents liés à la sécurité de l'information,
- des priorités de traitement des incidents de sécurité doivent être définies,
- une description des incidents de sécurité et les modes opératoires de résolution spécifiques permettent de gérer les différents types d'incidents liés à la sécurité de l'information,
- de manière optimale, la clôture d'un incident de sécurité est confirmée par le déclarant. Le RSSI donne une appréciation qualitative sur la résolution de l'incident (délais, solution proposée, amélioration potentielle, etc.).

4. *Des mécanismes (organisation, procédures, outils, etc.) doivent être mis en place, permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume et les coûts associés*

Bonnes pratiques :

- les informations recueillies lors de la résolution d'incidents liés à la sécurité de l'information pour identifier les incidents récurrents ou ayant un fort impact sont réévaluées à la fin de l'incident,
- l'évaluation d'incidents liés à la sécurité de l'information peut faire apparaître la nécessité d'améliorer les mesures existantes ou d'en créer de nouvelles, afin de limiter la fréquence des futurs incidents ainsi que les dommages et les coûts associés, ou afin d'intégrer ces mesures dans le processus de réexamen de la politique de sécurité. En ce sens, une analyse « à froid » des incidents ayant donné lieu à une cellule de crise est réalisée lors des comités exécutifs (afin d'identifier les éventuelles actions préventives à engager),
- une revue des incidents réalisée régulièrement permet notamment de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume, les coûts associés et leurs impacts sur les processus métier.

5. *Un programme d'assurances adapté doit être mis en œuvre pour protéger les personnes, les investissements, les informations et l'ensemble des actifs de l'entreprise ou de l'organisme. La définition du périmètre à assurer fait en règle générale l'objet d'une analyse de risques menée avec l'assureur. Il faut évaluer le plus précisément possible, la nature des risques encourus, les conséquences financières qu'ils peuvent engendrer, puis arbitrer entre l'auto-assurance (provision, franchise) et le transfert de risques à l'assureur.*
   Ces contrats d'assurances doivent couvrir également les risques informatiques (pannes, destruction, vol de matériel, fraude, etc.) et tout particulièrement le poste « surcoût d'exploitation en cas de sinistre ». Des assurances de type « pertes d'exploitation » permettent de surmonter les difficultés financières engendrées par un sinistre.

Bonne pratiques :

- actualiser régulièrement le périmètre à assurer et réviser les contrats en conséquence,
- démontrer l'efficacité de l'organisation en place pour la gestion des incidents. C'est une aide pour négocier des tarifs d'assurance préférentiels.

6. *Lorsqu'une action en justice civile ou pénale peut être engagée contre une personne physique ou un organisme, à la suite d'un incident lié à la sécurité de l'information, les éléments de preuve doivent être recueillis, conservés et présentés conformément aux dispositions légales relatives à la présentation de preuves régissant la ou les juridiction(s) compétente(s)*

Bonnes pratiques :

- si elles existent, réaliser les déclarations CNIL (ou équivalent) pour les logiciels d'analyse des événements de sécurité,
- avoir une procédure interne qui définit les exigences de sécurité en matière de collecte des traces techniques de sécurité, de leur conservation, de leur protection et de leur accès,
- seules les autorités judiciaires sont autorisées à collecter les preuves légales.

3.4. Organisation

3.4.1 Préambule

Une fois l'incident qualifié en tant qu'incident de sécurité il doit être confié à une équipe spécialement constituée pour l'analyse, l'évaluation d'impact, les actions correctives et la remise en fonction du service affecté. Cette équipe porte très souvent le nom de CSIRT (**Computer Security Incident Response Team) ou ISIRT (Information Security Incident Response Team).**

En fonction de la taille de l'entreprise ou de l'organisme cette équipe peut avoir une organisation très différente :

- modèle centralisé (CCSIRT) – une équipe unique et centralisée prenant en charge tous les incidents de l'organisation/entreprise. Ce modèle est efficace pour les organisations de taille limitée ou les grandes organisations avec les moyens informatiques très centralisés,
- modèle distribué (DCSIRT) – plusieurs équipes dispersées géographiquement en fonction de la localisation de centres d'hébergement de ressources informatiques. Il est important, pour une meilleure efficacité et communication, que ces équipes soient malgré tout administrées par une autorité centrale pour garantir l'application des procédures homogènes et un échange efficace d'informations entre les équipes,
- entité de coordination – dans le cas du modèle distribué fortement dispersé ou d'une communauté d'organisations indépendantes l'équipe de coordination remplit les rôles suivants :
    - coordinateur des actions des différents DCSIRT quand l'incident a un impact sur plusieurs entités,
    - centre d'expertise et d'assistance,
    - émetteur de recommandations et des bonnes pratiques,
    - gestionnaire de base de connaissances partagée par tous les membres d'organisation ou communauté.

      Un exemple de centre de coordination pour la communauté d'utilisateurs d'Internet est le CERT/CC (Central Emergency Response Team / Coordination Center situé à l'université de Carnegie Mellon aux États-Unis) ou le CERTA (Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques) du gouvernement français (liste non exhaustive).

Indépendamment du modèle d'organisation les membres de chaque équipe doivent disposer des moyens fiables et sécurisés de communication interne, mais également externe pour collaborer avec les équipes concernées dans le cadre de leur activité.

Un autre aspect de l'organisation de moyens de gestion d'incidents de sécurité est la décision du mode de gestion des ressources humaines et des services.

Dans le cas le plus simple l'équipe est constituée d'employés de l'entreprise ou de l'organisme et prend en charge l'ensemble des services. Dans certains cas, elle fait appel au support offert par les sociétés externes. Ce modèle peut être difficile à faire fonctionner à cause du large éventail de compétences exigées dans plusieurs domaines d'une part et de

l'obligation d'opérer le plus souvent 24h/24 et 7j/7, d'autre part. Seules les grandes entreprises / organisations peuvent s'offrir ces capacités.

À l'opposé du modèle précédent il est possible d'externaliser entièrement la gestion des incidents de sécurité à des prestataires de services spécialisés (MSSP Managed Security Services Provider). Dans ce cas les tâches de prise d'appel, de monitoring et détection, d'analyse, d'évaluation d'impact et de reporting sont entièrement prises en charge par le prestataire et les actions correctives et de restitution des services sont faites en collaboration avec les équipes de production (internes ou externes).

Souvent le modèle mixte de répartition des tâches entre le personnel interne et prestataires peut être le mieux adapté.

Dans de nombreux cas, il est très important de définir précisément, de publier et de communiquer les missions et les services à fournir par chacune des entités concernées.

Enfin, les équipes opérationnelles, dans de nombreux cas, seront obligées de communiquer avec les décideurs, l'administration et le support technique. Elles doivent donc disposer à tout moment d'une liste à jour des contacts nominatifs représentant différentes entités comme :

- la Direction Générale,
- le RSSI,
- les télécoms et réseaux,
- le support IT,
- les services juridiques,
- la communication (relations presse et média),
- les RH,
- les acteurs du PCA,
- la sécurité physique,
- les services généraux.

3.4.2 Équipe de réponse aux incidents SSI

Pour que les incidents de sécurité puissent être correctement traités, il est nécessaire qu'une structure existe et qu'elle soit dédiée à la gestion d'incidents. Les sigles CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team) décrivent les activités de telles équipes.

Cette structure est amenée à être sollicitée par sa hiérarchie ou par des contacts techniques pour qualifier des événements et intervenir sur un incident de sécurité. Pour cela, cette équipe doit être clairement identifiée comme un point de passage obligé dans tout circuit de notification d'incident.

Cette équipe doit également disposer de la légitimité nécessaire pour pouvoir agir rapidement. Pour cela, le management doit être persuadé de l'intérêt des actions de l'équipe, il doit donc être impliqué dans la définition des objectifs de l'équipe et être bénéficiaire de services offerts par l'équipe.

3.4.2.1 Fonctionnement

Une équipe de réponse aux incidents de sécurité doit répondre à différents objectifs imposés par son environnement. Parmi ses objectifs on peut lister :

- la rationalisation de la veille dans l'entreprise ou l'organisme,
- la nécessité de traiter rapidement tout type d'incident de sécurité par du personnel qualifié habilité et avec des modes opératoires éprouvés,
- la nécessité d'avoir une vue du risque d'exposition du SI de l'entreprise ou de l'organisme.

Ces objectifs répondent à des stratégies d'entreprise ou d'organisme (conformité réglementaire, protection de l'image, efficacité opérationnelle, etc.).

L'environnement d'une équipe de réponse aux incidents de sécurité est constitué de cercles d'acteurs / partenaires avec lesquels elle travaille (cf. Figure 1) :

- cercle de premier niveau : les commanditaires du service (responsables hiérarchiques ou fonctionnels),
- cercle de second niveau : les acteurs internes pour lesquels elle intervient (responsables sécurité, responsables informatiques),
- cercle de troisième niveau : les acteurs internes avec lesquels elle travaille au quotidien (équipes de production, support informatique, équipes projet),
- cercle de quatrième niveau : les acteurs internes avec lesquels elle a besoin de travailler ponctuellement (juristes, ressources humaines, chargé de communication, cellule de crise),
- cercle de cinquième niveau : les acteurs externes avec lesquels elle travaille (fournisseurs de services, prestataires de service),
- cercle de sixième niveau : les acteurs externes avec lesquels elle échange (CERTs, forces de police, chercheurs indépendants, etc.).

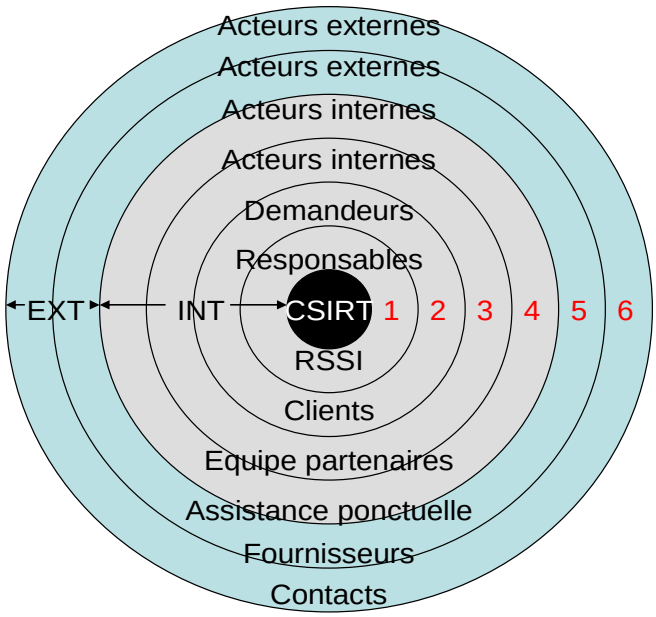

Figure 1 - Acteurs / partenaires de l'équipe de réponse aux incidents de sécurité

Cet environnement complexe requiert d'être maintenu à jour pour assurer une pleine capacité de réaction à l'équipe de réponse aux incidents. Une veille permanente et attentive aux nouvelles tendances et méthodes d'attaques est également nécessaire.

Pour être contactée rapidement, l'équipe de réponse aux incidents doit bénéficier d'une bonne visibilité en interne comme en externe. L'atteinte de cet objectif nécessite du temps et la mise en œuvre de différentes actions telles que : rencontres, présentations orales, participations à des conférences.

Il est utile de fournir à l'équipe une adresse de messagerie générique et un numéro de téléphone.

Les compétences requises au sein de l'équipe de réponse aux incidents sont multiples et dépendent des services qui sont fournis par l'équipe. Dans la plupart des cas, il sera nécessaire de disposer :

- de compétences techniques pour pouvoir analyser précisément le contexte opérationnel dans lequel l'incident s'est produit et identifier rapidement des contre-mesures pouvant être mises en œuvre sans mettre en péril le Système d'Information,
- d'une connaissance du contexte et des enjeux métier,
- de compétence rédactionnelle pour pouvoir formaliser correctement toutes les actions entreprises dans les cas de réponse à incident,
- d'une aisance relationnelle pour pouvoir échanger facilement avec les acteurs concernés en adaptant le discours en fonction du profil des interlocuteurs.

3.4.2.2 Services et périmètre

L'équipe peut offrir de multiples services liés à la gestion d'incidents de sécurité. Ces services peuvent être regroupés en trois grands domaines d'activité (cf. Figure 2) :

- services réactifs,
- services proactifs,
- services qualitatifs.

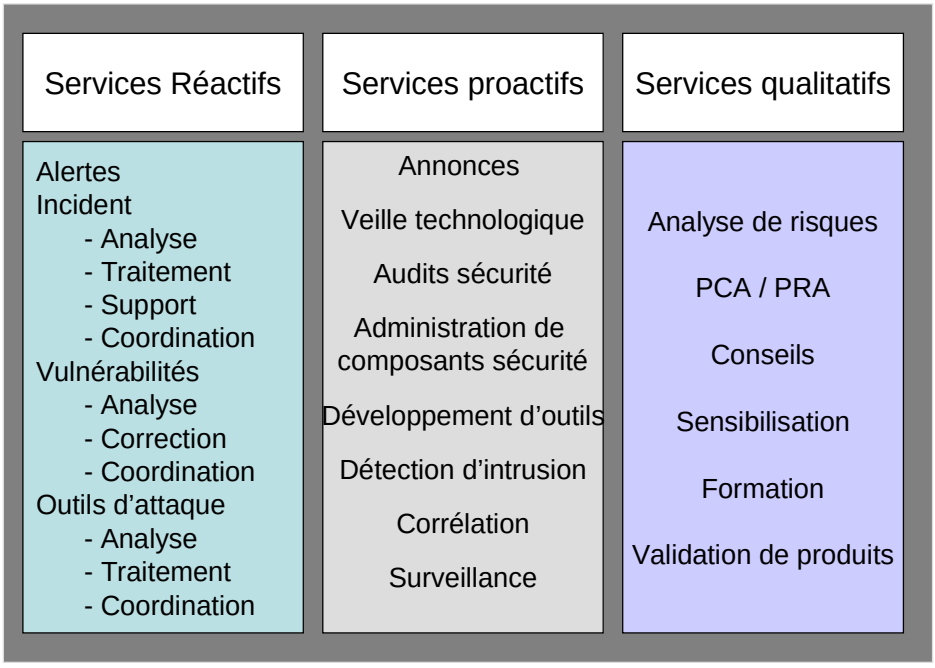

Figure 2 – Grands domaines d'activité des services liés à la gestion d'incidents de sécurité

Services réactifs

Le domaine réactif regroupe tous les services qui peuvent être mis en œuvre lors du traitement d'un incident de sécurité. Les services suivants sont rattachés à ce domaine :

- service d'alerte : ce service a pour objectif de notifier les parties prenantes d'un danger à très court terme. Des contremesures sont listées permettant de remédier au problème,
- service de traitement des incidents : ce service assure la prise en charge partielle ou totale de l'incident par l'équipe de réponse aux incidents de sécurité. L'équipe pourra apporter une simple assistance téléphonique, fournir des modes opératoires ou assister physiquement les équipes opérationnelles lors de cet incident. L'équipe intervenant sur l'incident aura à sa charge la détection, l'isolation et la remédiation de la menace associée à l'incident. Un service sous intervention est préférable mais demande des compétences multiples, des procédures rodées et de l'outillage,
- service de gestion des vulnérabilités : ce service consiste à centraliser les vulnérabilités sur le périmètre de l'entreprise ou de l'organisme, à les analyser et à coordonner leur correction,
- PCA/PRA : un incident analysé et jugé important pourra engendrer la nécessité de déclencher un plan de continuité d'activité (PCA) voire un plan de reprise d'activités (PRA.) Dans ce cas, il est capital que l'équipe en charge du traitement de l'incident soit

intégrée aux procédures d'alerte et de qualification du PCA. L'équipe de réponse aux incidents pourra contribuer à la gestion de crise selon la nature de l'incident.

Services proactifs

Le domaine proactif regroupe des services qui ont pour objectif de prévenir l'apparition d'un incident ou tout du moins d'anticiper son traitement. Les services suivants sont rattachés au domaine proactif :

- annonces : diffusion d'informations permettant d'anticiper une menace (informations concernant les vulnérabilités ou l'état de la propagation d'une menace constatée en externe),
- veille technologique : mise à disposition d'une synthèse sur les informations de sécurité essentielles sur une période donnée,
- audits de sécurité et tests d'intrusion : ces services permettent d'avoir une meilleure visibilité du niveau du risque et de repérer les points de faiblesse de certains pans du SI,
- administration de composants sécurité : ce service permet d'assurer l'administration des briques de l'infrastructure sécurité de façon à garantir la maîtrise du traitement en cas d'incident,
- développement d'outils : ce service vise à développer quelques outils sécurité,
- détection d'intrusions : ce service permet d'avoir une visibilité sur les attaques à destination du SI,
- corrélation d'événements de sécurité : ce service permet d'associer les événements de sécurité pour identifier s'ils donnent lieu à un incident de sécurité,
- surveillance : ce service très générique peut être décliné en activités distinctes suivant le métier de l'entreprise /organisme ou ses centres d'intérêt. Dans tous les cas, des services de surveillance permettront d'identifier des comportements anormaux probablement caractéristiques d'un incident de sécurité.

Services qualitatifs

Le domaine qualitatif regroupe des services qui participent à l'élévation du niveau de sécurité par des actions de fond. Ces services ne sont pas propres à la gestion d'incident, mais une équipe de réaction aux incidents peut souvent y apporter une forte valeur ajoutée. Les services suivants sont rattachés à ce domaine :

- analyse de risques : une équipe de réponse aux incidents peut apporter une aide précieuse pour identifier rapidement les menaces et leurs impacts sur un actif de l'entreprise ou de l'organisme. Dans ce cas, une interaction doit être créée entre les équipes projets ou d'architecture en charge des analyses de risque et l'équipe de réaction aux incidents,
- PCA/PRA : une équipe de réponse aux incidents acquière rapidement de l'expérience sur les typologies d'incidents rencontrés dans l'entreprise ou l'organisme et sur le mode de traitement le plus adapté pour leur éradication. L'équipe de réponse aux incidents pourra contribuer à la gestion de crise selon la nature de l'incident,
- qualification des incidents de sécurité : l'équipe de réponse aux incidents de sécurité contribue à l'élaboration de guides de qualification des incidents, notamment pour l'équipe d'assistance de premier niveau,
- conseils : la bonne maîtrise des attaques et des contremesures confère à l'équipe de réponse aux incidents des connaissances qui pourront être mises à contributions pour

des missions de conseil. Tout du moins, il est important que l'équipe soit reconnue par les équipes projet pour solliciter son conseil sur des points précis,

- sensibilisation : les incidents rencontrés par l'équipe de réponse aux incidents lui procurent une bonne visibilité des choses à faire et à éviter. Cette connaissance peut être mise à contribution pour des actions ponctuelles ou récurrentes de sensibilisation auprès de publics variés (salariés, managers, développeurs, etc.),
- formation : l'équipe de réponse aux incidents peut, dans certains cas offrir un service de formation permettant de développer des compétences particulières en interne dans l'entreprise/organisme,
- validation de produits : dans certains cas, il peut être pertinent de disposer dans l'entreprise/organisme d'une équipe à même de tester certains produits tiers pour les estampiller comme respectueux des engagements de qualité attendus.

La liste des services n'est pas exhaustive et la mise en œuvre devra tenir compte du contexte de l'entreprise/organisme. Tous les services ne sont pas nécessairement offerts par l'équipe de réponse aux incidents. Si des services ne lui incombent pas, il est par contre du ressort de l'organisation d'identifier tous les acteurs qui offrent ces services et d'établir un contact durable entre eux et l'équipe de réponse aux incidents de sécurité.

Dans une perspective de réponses aux incidents, le domaine réactif est un élément fondateur et il est nécessaire qu'au moins un des services rattachés à ce domaine soit mis en œuvre dans l'équipe.

3.5. Processus de traitement des incidents

Le processus de gestion des incidents de sécurité est représenté par le schéma ci-dessous.
La particularité du traitement des incidents de sécurité tient à l'intervention de l'équipe de réponse aux incidents de sécurité. Les autres volets du processus appartiennent soit au processus général de gestion des incidents (prise en compte de l'incident, catégorisation, qualification, traitement), soit au processus de gestion de crise.

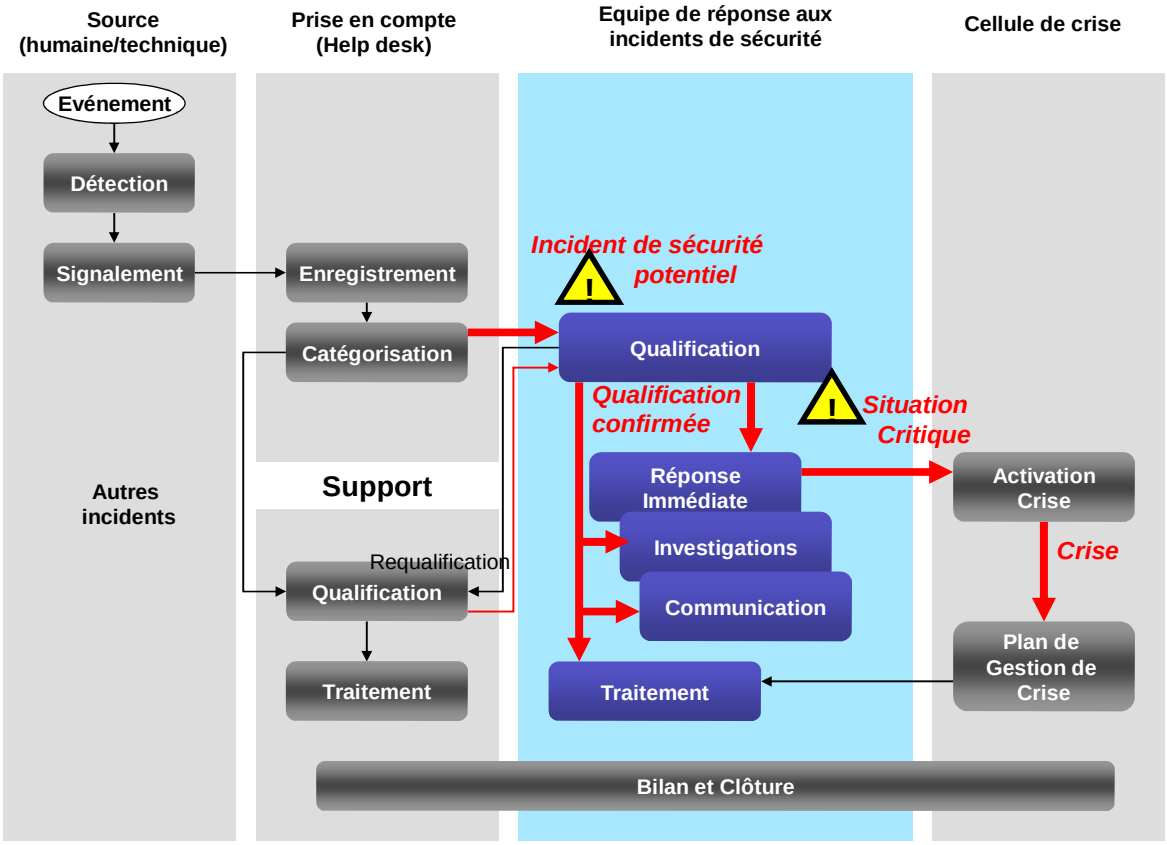

Figure 3 – Schématique du processus de gestion des incidents

Le signalement d'un événement susceptible d'être qualifié d'incident de sécurité est réalisé soit par une personne (utilisateur, administrateur, etc.) ou par des moyens techniques (outils de surveillance, sites Internet spécialisés, etc.).

La prise en compte est réalisée en général par un Help Desk. D'autres circuits peuvent exister. Dans tous les cas, il est nécessaire que l'événement soit enregistré de manière à pouvoir en faire un suivi.

C'est à ce stade de la prise en compte que l'événement est catégorisé. Il peut être catégorisé « incident de sécurité » ou être confié à des experts pour qualification.

Les incidents catégorisés « incident de sécurité » sont immédiatement soumis à l'équipe de réponse aux incidents de sécurité. Les autres types d'incident sont transmis aux équipes compétentes pour leur traitement (support).

L’équipe de gestion des incidents de sécurité, après analyse, confirme ou infirme la catégorisation « incident de sécurité » (qualification). Les incidents non confirmés « incident de sécurité » sont retransmis aux équipes support.

Les incidents qualifiés « de sécurité » font alors l’objet d’un traitement spécifique dont les particularités sont développées dans le chapitre suivant. Outre les investigations complémentaires, le traitement des incidents de sécurité peut nécessiter des actions spécifiques telles que la préservation des preuves ou des actions adaptées de communication.

Lorsque l’équipe de gestion des incidents de sécurité n’est plus à même de gérer la situation, ou lorsque les conséquences potentielles sont à un niveau trop important, la cellule de crise est alertée et juge de l’opportunité de passer en mode « gestion de crise ».

4 - Gestion des incidents de SSI

Ce chapitre détaille les étapes du processus de gestion des incidents présenté d'une manière générale dans le chapitre 3.5.

4.1. Détection et signalement

La détection peut avoir pour origine :

- toute personne qui a connaissance d'un fait ou d'une menace pour l'organisme (par exemple comportement anormal d'un équipement, d'une application ou d'une personne),
- un administrateur lorsqu'il est informé par un dispositif de supervision ou lorsqu'il constate une anomalie lors de contrôles,
- un acteur de la sécurité lorsqu'il est informé par un outil de surveillance (détection d'intrusion ou d'action frauduleuse) ou lorsqu'il constate une anomalie lors de contrôles.

L'anomalie doit pouvoir être signalée à une personne compétente dans les plus brefs délais. Le contact habituel pour l'utilisateur est le help desk. Cependant, il doit également être possible de contacter directement un responsable de la sécurité en toute discrétion si la situation l'exige. Les utilisateurs doivent être sensibilisés et informés sur les différents niveaux d'alerte.

Dans tous les cas, on doit s'assurer que les moyens d'alerte sont suffisamment rapides, y compris en dehors des heures ouvrées, pour permettre une réponse adaptée (empêcher que l'incident se poursuive, préserver les preuves, etc.).

Des mesures immédiates peuvent être associées à la détection, soit sous forme de consignes pour la personne qui détecte, soit par l'activation automatique de mécanismes de protection.

4.2. Prise en compte

4.2.1 Enregistrement de l'incident

Comme indiqué précédemment, un incident supposé de sécurité peut être signalé à différentes personnes, en général le help desk, selon des procédures devant être connues de tous. Dans tous les cas, la personne qui réceptionne l'appel ou l'alerte doit en accuser réception. L'événement doit immédiatement être enregistré dans une base de données des incidents.

A ce stade de la procédure, l'événement n'est pas encore qualifié d'incident de sécurité mais il est catégorisé. L'enregistrement de l'événement doit comporter à minima la date et l'heure de l'alerte, son origine (personne ou dispositif technique), les coordonnées du déclarant, une description aussi précise que possible de l'événement et sa catégorisation. Comme pour tout incident, un numéro de dossier est généré et communiqué si nécessaire au déclarant. La personne qui enregistre l'événement doit également mentionner l'action immédiate

déclenchée (par exemple transmission à une équipe support ou directement à l'équipe de traitement des incidents de sécurité pour qualification).

L'enregistrement de l'événement est essentiel à plusieurs titres. Il permet de garder une trace de chaque événement et d'en effectuer un suivi dans toutes les phases ultérieures, d'analyse ou de traitement, jusqu'à la fermeture du dossier.

La base des événements constitue également un outil d'analyse a posteriori dans le cadre d'analyses de risques, pour évaluer l'efficacité des dispositifs en place ou pour identifier des incidents récurrents pouvant être qualifiés de « problème ».

4.2.2 Catégorisation par une équipe support

Une fois l'incident identifié comme « incident de sécurité potentiel», l'équipe support peut être habilitée pour prendre des mesures ou transmettre l'incident à l'équipe de gestion des incidents de sécurité.

L'équipe de réponse aux incidents de sécurité établit des consignes d'alerte sécurité (fiches par type d'incident) pour les équipes support.

Pour les incidents identifiés, ces consignes indiquent le mode opératoire du traitement de ces incidents pour les équipes de support. Dans les autres cas, c'est l'équipe de réponse aux incidents de sécurité qui doit être immédiatement sollicitée.

Par exemple : l'équipe de réponse aux incidents de sécurité peut également être sollicitée à chaque fois qu'une équipe support ou qu'un membre du personnel pense être face à un événement susceptible d'avoir un impact fort sur l'organisation.

Les consignes peuvent éventuellement spécifier que tout incident susceptible d'être d'origine malveillante ou concernant certains équipements ou logiciels ou encore signalé par certains dispositifs techniques, doit être transmis à l'équipe de réponse aux incidents de sécurité.

4.2.3 Qualification par l'équipe de réponse aux incidents de sécurité

Une première analyse, conduite par l'équipe de réponse aux incidents de sécurité, confirme ou infirme la catégorisation « incident de sécurité ».
Les incidents non confirmés « incident de sécurité » sont transmis aux équipes support pour traitement.

L'équipe de réponse aux incidents de sécurité procède si nécessaire à des investigations complémentaires pour qualifier l'événement. Les critères d'évaluation d'impact prenant en compte différents axes d'analyse (impacts financiers, impacts sur l'image, impacts sur les clients ou partenaires, risques de poursuite judiciaire, etc.) doivent être préétablis et mis à la disposition de l'équipe. Typiquement ces critères sont issus de l'analyse de risque.

Il est nécessaire de tenir un journal de bord horodaté et précis des événements et actions dès sollicitation de l'équipe.

4.3. Réponse à l'incident SSI

4.3.1 Mesures de réponses immédiates

Suite à la qualification, des mesures d'urgence peuvent être prises pour limiter les impacts et préserver les traces. En effet, même sans connaître précisément la nature de l'incident, son origine ou son impact réel qui seront l'objet de la phase d'analyse, le simple fait d'identifier le type de danger peut déclencher des actions palliatives, comme par exemple :

- un confinement (ex : débranchement du réseau d'un poste infecté pour le mettre dans un VLAN de quarantaine),
- une isolation (ex : couper tous les flux de messagerie Internet),
- une communication ciblée de recommandations.

Certaines de ces mesures peuvent être prévues à l'avance dans des procédures du support et de l'équipe sécurité.
Si ces mesures s'avèrent insuffisantes ou/et si la situation n'est pas maitrisée ou/et si le niveau d'impact de l'incident le justifie, au regard des critères d'évaluation, la cellule de crise doit être activée.

4.3.2 Investigations

L'analyse de l'incident a pour objectif de préciser les éléments suivants :

- la nature de l'incident,
- le fait générateur,
- le périmètre concerné,
- l'impact.

Ces éléments permettront de définir les actions à entreprendre. Dans certains cas les conclusions de l'investigation peuvent conduire à l'activation de la cellule de crise.

4.3.2.1 Préservation des traces

Certaines précautions doivent être prises. En particulier, en cas de piratage (par exemple), si le but de l'analyse est de remonter à la source de la manipulation frauduleuse et de prendre des mesures légales à l'encontre des auteurs des faits, il est nécessaire de préserver les informations d'origines (logs, etc.) afin de conserver le contexte de preuve.

En effet, l'analyse peut, dans certains cas modifier (le travail d'analyse génère lui-même des traces qui se confondent ensuite avec les traces laissées par l'agresseur), voire effacer, les traces du passage d'un 'attaquant'. De fait, il est nécessaire de sauvegarder (par exemple via une copie intégrale, de type bit à bit) les informations avant d'entreprendre toute action susceptible de nuire à l'intégrité des données sur le support d'origine.

Si une copie complète des disques n'est pas réalisable ou l'est difficilement, il faut au moins conserver une copie des logs (journaux de connexions au système). Toutefois, cette sauvegarde n'est pas toujours simple à mettre en œuvre et peut nécessiter des outils et/ou des compétences particulières.

Enfin, les données ainsi sauvegardées doivent être protégées physiquement et un cadre opératoire doit être mis en œuvre qui précisera notamment par qui ces sauvegardes ont été effectuées, à quel moment, comment elles ont été protégées et qui y a eu accès. En fonction des enjeux, il peut être recommandé de faire appel à un huissier de justice.

Le travail d'investigation pourra alors commencer, si possible sur les copies de sauvegarde, les disques durs d'origine étant rangés en lieu sûr (une procédure pouvant durer des mois, voire des années). Ces derniers ainsi que la sauvegarde des logs, pourront servir de preuves en cas de poursuites judiciaires.

4.3.2.2 Environnements potentiellement concernés

Durant l'investigation il est important de déterminer le périmètre concerné :

- OS,
- réseau et téléphonie,
- serveurs,
- applications,
- locaux,
- groupe de personnes,
- données,
- services,
- clients, fournisseurs, partenaires, …

4.3.2.3 Aide à l'analyse

Dans chaque environnement technique il existe des outils qui peuvent aider à déterminer l'étendue de l'attaque menée.

Des procédures peuvent également être mises en œuvre, intégrant des check-lists qui permettent de réaliser l'analyse dans les meilleures conditions. Par exemple, on peut positionner les actions suivantes :

- vérifier les performances des systèmes,
- rechercher des processus ou des applications non autorisées en cours d'exécution,
- si des logs existent, y rechercher d'éventuelles connexions inhabituelles, tentatives d'ouverture de session infructueuses, tentatives d'ouverture de session avec des comptes par défaut, etc.,
- déterminer si du matériel non autorisé a été connecté au réseau,
- examiner les groupes clés (administrateurs, etc.) afin de vérifier qu'ils ne contiennent pas de membres non autorisés,
- etc.

4.3.2.4 Identification du fait générateur et analyse de l'impact

L'objet principal de l'analyse de l'incident proprement dit permet de répondre à plusieurs questions qui se posent, comme par exemple :

- quelle est la vulnérabilité ou la faiblesse qui a rendu possible l'incident ? C'est la question la plus importante ! En effet, si aucune réponse claire n'est trouvée à cette question, le système restera vulnérable une fois remis en service ; il pourrait être attaqué à nouveau,

- quel est l'inventaire des dégâts ou quel est l'impact de l'incident (déni de service, baisse de la qualité du service, perte de donnée, divulgation d'information confidentielle, etc.).

4.3.3 Traitement

4.3.3.1 Mesures pour éviter l'aggravation des conséquences

En complément des mesures de réponses immédiates déjà prises dès la qualification de l'incident, des mesures peuvent être prises pour éviter l'aggravation des conséquences.

Disposant à ce stade des informations obtenues lors des investigations, ces mesures seront plus ciblées que les réponses conservatoires d'urgence :

- activation de la Cellule de Crise : s'elle n'a pas été activée lors de la phase de réponse immédiate, la gestion de crise du PCA peut être déclenchée à ce stade, si la situation s'est dégradée entre temps et l'impose,
- restrictions temporaires d'accès aux réseaux ou/et aux applications : ces restrictions peuvent être, suivant les cas, des blocages ou des simples filtrages. (exemple : interdiction d'accès à certains sites Web),
- communications ciblées : pour adapter la communication, il faut évaluer très rapidement la durée de la perturbation (exemple : évaluer la durée de restauration par rapport au volume de données à restaurer en cas de pertes de données). On identifie trois types de communication :
    - communication vers les utilisateurs. Le communiqué contient en règle générale à minima :
        - les faits qui doivent être édulcorés dans certains cas,
        - les activités impactées du fait des restrictions temporaires en place,
        - des consignes de comportements (exemple : ne pas ouvrir les pièces jointes),
        - l'heure prévisionnelle de retour à la normale,
    - communication technique entre homologues (d'autres sites ou filiales) :
        - les faits précis,
        - les recommandations d'actions,
        - une proposition d'actions coordonnées,
    - communication vers les externes (clients, assureurs, fournisseurs, etc.). On peut utiliser si besoin la communication de crise prévue dans le cadre du PCA.

4.3.3.2 Déclarations aux assurances

Procéder aux déclarations de sinistres en faisant attention à :

- la tenue des délais : généralement 48 heures pour le vol, 5 jours ouvrés au maximum dans la plupart des autres cas,
- ne rien « toucher » avant la venue de l'expert en assurances sauf nécessité.

En cas d'urgence, on peut remplacer le matériel et mettre le matériel endommagé de côté (cette mesure ne peut être prise qu'en cas d'urgence, afin d'éviter l'arrêt de l'exploitation).

Si le sinistre est important, des photos peuvent ne pas suffire, il faut procéder à un constat par huissier et faire mettre toutes les preuves sous scellés.

4.3.3.3 Résolution de l'incident

Sans être exhaustifs, les quelques points ci-dessous nécessitent une attention particulière.

Appels aux supports externes

L'entreprise ou l'organisme peut avoir besoin d'urgence de compétences externes qui interviendront à distance ou sur site et qu'il faut réserver en priorité en raison des délais d'intervention.

Éradication

L'éradication du problème dépend du type d'incident rencontré.

On peut noter deux grandes tendances entre lesquelles il faudra choisir :

- le mode « réparation », souvent manuel mais qui peut être automatisé par un script,
- le mode « restauration ou réinstallation » en repartant d'une sauvegarde ou d'une image système.

Les critères de choix entre ces deux méthodes sont :

- le temps total (estimation) pour éradiquer l'incident,
- le niveau de certitude d'avoir bien identifié tous les impacts précis liés à l'incident,
- le niveau de perte de données acceptable.

Dans les cas complexes, il peut être important d'écrire le plan d'action correctif pour bien ordonnancer les étapes.

Détermination du point zéro de l'incident

Les éléments permettant de déterminer le point zéro sont (entre autres):

- le recueil des preuves et journaux,
- le témoignage des utilisateurs,
- tous les outils de supervision et reporting.

Cette compréhension de l'origine de l'incident permet de vérifier la pertinence des mesures correctives et de réduire le risque de reproduction.

Délai de Réapprovisionnement de matériel

Même si l'entreprise/organisme utilise le matériel de secours, il n'est pas recommandé de « rouler trop longtemps sans roue de secours ». C'est pourquoi le réapprovisionnement du matériel est également une priorité.

Retour à la normale

Le retour à la normale doit être associé à une communication spécifique.

4.3.3.4 Méthodes et outils

Du début à la fin de l'incident, les outils indispensables sont :

- outil d'enregistrement des évènements ainsi que les moyens d'accès associés (téléphone, messagerie, etc.),
- outil de supervision.

D'autres outils peuvent être utiles ou nécessaires :

- outils de diagnostic,
- outils de confinement :
  - VLAN de confinement,
  - blocage au niveau de l'annuaire d'entreprise/organisme ou des comptes locaux des équipements,
  - blocage ou filtrage sur tout équipement de sécurité (pare-feu, relais filtrant http ou SMTP, etc.),
  - etc.,
- outils de réparation :
  - antivirus / kit de décontamination antiviral (exemple : clé USB bootable ou le CD (pour des matériels plus anciens) contenant des anti-malwares et outils systèmes basées de préférence sur un OS différent de celui qui est installé et pouvant prendre en charge de façon fiable le système de fichier à examiner (exemple : LINUX pour examiner NTFS).
  - outils de déploiement de patchs systèmes et/ou d'applications,
  - outils de restauration d'images systèmes, de données ou d'environnement virtuel,
  - etc.

Enfin, l'accès aux moyens de communication téléphoniques et informatiques et à Internet est indispensable pour communiquer ou s'informer.

En cas d'incident empêchant l'accès à ces outils, les équipes d'intervention doivent bénéficier de dispositifs alternatifs.

4.3.3.5 Exemples de traitements

Quelques exemples de traitement (synthétisé sous forme de Fiche) sont décrits dans les fiches suivantes du chapitre 5 - Exemples de typologie des incidents :

- vol de PC portable,
- installation d'un logiciel non autorisé,
- présence d'un logiciel non autorisé,
- dysfonctionnement pouvant provenir d'un logiciel malveillant,
- intrusions logiques,
- usage inapproprié,
- incidents concernant les habilitations,
- déni de service Messagerie par saturation du relais public de messagerie,
- cas des incidents liés.

4.4. Revues post-incident

4.4.1 Investigation post-incident

Une fois l'incident maîtrisé, il est possible qu'il soit nécessaire de lancer des investigations complémentaires pour bien comprendre comment cet incident a pu avoir lieu. Si tel est le cas, il ne faut pas hésiter à consacrer le temps nécessaire à cette étape qui viendra enrichir le dossier de synthèse.

Si des éléments de preuve sont encore présents et que l'incident a vocation à être présenté devant un tribunal, la collecte des indices devra être particulièrement précise et se conformer aux bonnes pratiques techniques en adéquation avec les obligations légales.

4.4.2 Rapport de synthèse

Chaque incident de sécurité doit être accompagné d'un dossier de suivi et si possible d'un rapport de synthèse. Ce rapport doit être rédigé par l'équipe en charge de la résolution de l'incident. Il peut servir de cadre directeur lors d'une revue post-incident.

Le rapport de synthèse doit pouvoir répondre aux questions suivantes :

- éléments techniques :
  - quel est l'objet de l'incident ?,
  - quand a eu lieu l'incident ?,
  - où a-t-il eu lieu ?,
  - comment l'incident s'est-il produit ?,
  - comment l'incident a-t-il été maîtrisé ?,
- bilan processus :
  - qu'est-ce qui n'a pas fonctionné ?,
  - qu'est-ce qui a bien fonctionné ?,
  - qu'est-ce qui nécessite d'évoluer en matière de SMSI ?,
  - la communication aux parties concernées a-t-elle été bien faite ?,
- bilan financier :
  - quel est le coût de l'incident en matière de perturbation du SI (impact métier) ?,
  - quel est le coût induit de l'incident en matière d'incapacité de travailler pour le personnel ?,
  - quel est le coût de l'incident en matière de temps de résolution passé par les différentes équipes ?,
  - quel est le coût de la contre-mesure mise en place ?,
  - quelles pertes ont pu être économisées grâce à l'équipe de réponse à incident ?

Le rapport de synthèse doit être rédigé au plus près de la date de résolution de l'incident afin d'éviter que le temps n'efface dans la mémoire des acteurs des éléments ou des détails importants pour la compréhension et l'analyse de l'incident.
Le rapport doit prioritairement présenter des conclusions claires compréhensibles par les responsables.

Ce rapport doit être conservé dans un espace dédié servant de base de connaissance aux incidents de sécurité. Cette base d'information pourra par la suite être mise à profit pour une meilleure anticipation des incidents, pour définir les contremesures les plus appropriées ou encore pour vérifier si les décisions actées ont été suivies d'effets.

4.4.3 Analyse post-incident

L'analyse post-incident s'inscrit dans une démarche d'amélioration continue et de qualité PDCA permettant de prendre connaissance des éléments qui doivent évoluer dans le Système d'Information.

Cette analyse post-incident doit impliquer les responsables pour que les engagements soient pris rapidement en matière d'évolution du Système d'Information. Celle-ci peut prendre la forme d'un comité de pilotage ou tout autre type de réunion impliquant les décideurs adéquats.

Un compte-rendu de l'analyse post-incident doit être rédigé pour acter des évolutions du Système d'Information.

4.5. Actions post-incident

4.5.1 Bilan de l'incident

Les informations et les mesures déterminées lors du traitement de l'incident doivent être conservées et permettre d'enrichir la base de connaissances.

Dans le traitement d'un incident majeur, il est important d'analyser avec recul, ce qui a bien fonctionné et ce qui a moins bien fonctionné.
Cela doit se traduire par la rédaction d'un bilan adressé aux directions concernées. La mise en place des mesures du bilan, de préférence sous forme de plan d'actions précis, devra être suivie par le responsable sécurité.

4.5.2 Le Recours

Dans le cas d'une attaque, la responsabilité de l'auteur de celle-ci est d'abord d'ordre pénal. La loi française réprime certains actes commis ou tentés, notamment :

- l'accès illégal à un système,
- la modification ou la suppression illicite de données,
- l'entrave au fonctionnement d'un système,
- l'association de malfaiteurs informatiques (en tant qu'élément aggravant).

La France dispose d'une législation précise sur le sujet (Articles 323-1 à 323-7 du Code pénal relatifs au piratage informatique) et les pirates sont passibles de sanctions parfois conséquentes. C'est pourquoi, il ne faut pas hésiter à l'utiliser si vous êtes victime d'une tentative de piratage, que l'attaquant réussisse ou non à la mener à bien.

Il faudra alors réunir les éléments suivants :

- les faits énoncés clairement, de manière chronologique, en incluant tout détail utile,

- une liste, la plus complète possible, de tous les préjudices subis (dommages, préjudice financier, perte de temps pour vérification de l'intégrité du site ou des données, perte de crédibilité auprès des internautes ou des clients de l'entreprise, etc.),
- les éléments de preuve constitués lors de l'analyse de l'incident (pour que ces éléments aient une valeur juridique leur collecte et leur conservation doivent obéir à des règles très strictes).

Dans un second temps, il faut identifier auprès de qui porter plainte, en gardant en tête que c'est généralement le lieu des faits qui est l'élément déterminant.

Des contacts utiles peuvent être trouvés sur le site Internet du CLUSIF : www.clusif.fr/fr/production/cybervictime/.

4.5.3 Révision des contrats

Il peut être nécessaire de réviser les contrats d'assurance ou d'engagement avec des fournisseurs.

4.5.4 Communication interne spécifique (sensibilisation, etc.)

Les incidents rencontrés par l'équipe de réponse aux incidents lui procurent une bonne visibilité des choses à faire et à éviter. Cette connaissance peut être mise à contribution pour des actions ponctuelles ou récurrentes de sensibilisation auprès de publics variés (salariés, managers, développeurs, etc.).

4.6. Amélioration de la gestion des incidents SSI

Les enseignements tirés des traitements des incidents de sécurité doivent contribuer à l'amélioration générale des processus et des moyens de gestion de ces incidents.

L'ensemble des éléments doit être revu périodiquement suite aux incidents ayant un impact fort sur le SI, et donner lieu à des évolutions :

- politique de gestion des incidents
- organisation (principaux acteurs)
- processus :
  - prévention,
  - détection :
    - help desk, numéro dédié (circuit spécifique) :
      - pré-qualification,
      - création fiche incident,
      - escalade,
    - outils de monitoring
  - analyse :
    - problématique de préservation des preuves,
    - classification,
    - l'appréciation des risques,
  - actions :
    - correction (ex : rétablissement d'un service),

        - mise en sécurité du périmètre concerné,
        - déclaration (autorités),
        - rapports d'intervention (base d'incidents),
    - suivi :
        - contrôle du processus de gestion de l'incident,
        - tableaux de bord sur les différents types d'incidents (fréquence, impacts),
        - analyse post-incident,
        - alimentation de la gestion des problèmes,
    - recours :
        - juridique (recherche de preuve),
        - assurance,
    - communication :
        - information des utilisateurs,
        - communication externe,
- processus annexes (PCA, gestion des problèmes, etc.),
- audit.

5 - Exemples de typologie des incidents

5.1. Présentation du format des fiches par type d'incident

Ce chapitre présente quelques fiches de description de différents types d'incidents de sécurité. Le formalisme de chaque fiche est décrit ci-dessous, sur la base des thèmes suivants :

- description du type d'incident de sécurité,
- mesures préventives possibles,
- détection,
- qualification,
- analyse,
- traitement,
- actions post-incident.

5.1.1 Description du type d'incident de sécurité

Dans ce thème, on retrouve les points suivants :

- définition de l'incident,
- illustrations (exemples, différentes formes, etc.),
- classification :
    - impacts potentiels selon les deux axes interne et externe (type d'impact, niveau),
    - situations aggravant la potentialité de l'événement générateur,
    - domaine concerné (locaux, personnel, réseau étendu, réseau local, applications, développements/maintenance, systèmes, domaines métier, sécurité générale, SSI, organisation, fournisseurs, etc.),
    - type de propagation (immédiat, progressif, dégressif).

5.1.2 Mesures préventives possibles

Dans ce thème, on retrouve les points suivants :

- mesures organisationnelles,
- mesures techniques.

5.1.3 Moyens de détection

Dans ce thème, on retrouve les points suivants :

- manifestation de l'incident,
- mesures organisationnelles de détection spécifiques,
- outils de détection disponibles,
- type d'alerte (Qui alerte ? Qui alerter ?).

5.1.4 Qualification

Dans ce thème, on retrouve les points suivants :

- recueil des informations et recoupements pour catégoriser le type d'incident et en déduire son niveau de sévérité,
- premières mesures d'urgences (réponse immédiate).

5.1.5 Analyse

Dans ce thème, on retrouve les points suivants :

- précautions nécessaires (préservation de preuve),
- mesures immédiates (information, déclaration, anticipation du traitement, etc.),
- environnements potentiellement concernés,
- outils d'aide à l'analyse (logiciels, tests, check-lists, centres de support, internet, etc.),
- type d'escalade (notamment vers le RSSI ou le RPCA).

5.1.6 Traitement

Dans ce thème, on retrouve les points suivants :

- mesures pour éviter l'aggravation des conséquences (confinement, information, évacuation, etc.),
- déclarations réglementaires,
- résolution de l'incident (éradication, reprise, déblocage, activation du PCA, filtrage, etc.),
- selon type d'incident : méthode, outils, etc.

5.1.7 Actions post-incident

Dans ce thème, on retrouve les points suivants :

- recours juridique,
- assurance,
- communication spécifique (sensibilisation, etc.),
- audit,
- recommandations,
- réexamen de l'appréciation des risques.

5.2. Fiches par type d'incident

5.2.1 Vol de PC portable

5.2.1.1 Description du type d'incident de sécurité

Déclaration de vol de portable par un utilisateur.
Exemples : Vol de portable dans les locaux de l'entreprise/organisme, vol de portable dans les transports en commun, vol de portable par l'utilisateur, etc.
Classification :

- impact variable selon la nature des informations contenues et leur niveau de protection (contrôle d'accès, chiffrement),
- potentialité forte si le portable n'est ni surveillé ni protégé physiquement,
- origines possibles : défaut de contrôle d'accès aux locaux, absence de mesure de sécurité (équipement de sécurité, règlement, sensibilisation, etc.), non respect des consignes,
- type de propagation : immédiat pour le matériel, progressif possible pour le contenu.

5.2.1.2 Mesures préventives possibles

Mesures organisationnelles :

- politique de protection des informations,
- charte utilisateur,
- responsabilisation du personnel (sensibilisation, sanctions, etc.),
- inventaire du matériel,
- accompagnement des visiteurs,
- contrôles périodiques du respect des règles de sécurité,

Mesures techniques :

- marquage de sécurité des équipements (marquage société, dispositif RFID, etc.),
- attache de sécurité,
- contrôles d'accès aux locaux (fermeture des accès, caméras de surveillance, etc.),
- protection des issues,
- contrôles d'accès aux données sensibles,
- chiffrement des données.

5.2.1.3 Moyens de détection

Manifestation de l'incident : déclaration de vol.
Mesures organisationnelles de détection spécifiques : découverte lors d'un contrôle d'inventaire.
Outils de détection disponibles : vidéosurveillance, portique de détection (RFID).
Type d'alerte (qui alerte : l'utilisateur concerné ; qui alerter : selon organisation).

5.2.1.4 Qualification

Le niveau de gravité d'incident dépend de la fonction du détenteur, de l'usage du portable, du lieu du vol, etc.

Mesures de réponse immédiates. Ex : blocage immédiat de tous les accès au SI de l'entreprise/organisme à partir de ce PC, changement/ réinitialisation des mots de passe, des codes d'accès et d'autres authentifiants (certificats…) qui ont pu être mémorisés sur la machine, etc.

5.2.1.5 Analyse

Précautions nécessaires (préservation de preuve) : préserver les enregistrements de vidéosurveillance, les logs de contrôle d'accès.
Mesures immédiates (information, déclaration, anticipation du traitement, etc.) : dépôt de plainte de l'utilisateur.
Environnements potentiellement concernés : activités métier, SSI.
Analyse de l'historique des connexions et des journaux pour retrouver la dernière connexion, voire les dernières actions.
Outils d'aide à l'analyse (logiciels, tests, check-lists, centres de support, internet, etc.) : néant.
Type d'escalade (notamment vers le RSSI ou le RPCA) : selon organisation, impact potentiel ou situation de l'utilisateur.

5.2.1.6 Traitement

Mesures pour éviter l'aggravation des conséquences (confinement, information, évacuation, etc.) : hors mesures préventives et blocage des accès il n'y a pas d'actions efficaces.
Déclarations réglementaires.
Déclencher le réapprovisionnement du matériel et s'assurer que toutes les mesures préventives de sécurité ont été prises.

5.2.1.7 Actions post-incident

Recours juridique.
Assurance.
Communication spécifique (sensibilisation, etc.).
Reporting.
Audit.
Recommandations.

5.2.2 Installation d'un logiciel non autorisé

5.2.2.1 Définition de l'incident

Toute tentative d'installation de logiciel non autorisé, volontaire ou non, doit être considérée comme un incident de sécurité.

L'installation d'un logiciel non autorisé peut être faite :

- lors d'une attaque réseau (virus),
- lors d'une intrusion,
- lors de l'installation d'un progiciel non certifié,
- lors d'opérations de maintenance,
- par un utilisateur,
- lors de l'utilisation d'un support amovible (clé USB)
- lors d'une synchronisation d'un smartphone comportant des applications non certifiés avec le poste fixe de l'utilisateur de l'entreprise/organisme.

5.2.2.2 Mesures préventives possibles

Mesures organisationnelles :

- mise en œuvre d'une politique antivirale : identification des besoins, des moyens adaptés au niveau de gravité des menaces, des responsabilités pour une détection d'un code malveillant qui doit être faite au plus près de son arrivée dans le SI,
- contrôle des mises en production,
- certification des progiciels,
- contrôle des opérations de maintenance,
- responsabilisation des utilisateurs et des équipes informatiques.

Mesures techniques

- limiter les privilèges d'administration,
- anti-malware,
- durcissement du poste de travail (interdiction de transferts de données de/vers les clés USB, interdiction de lecture / gravure CD/DVD, listes blanches des programmes autorisés à être exécutés).

5.2.2.3 Moyens de détection

Gestion du parc.
Contrôle du code.
Scellement des programmes en production (Signature des programmes déployés et détection d'exécution du code non signé).
Détection d'intrusion.
Anti-malware.

5.2.2.4 Analyse

Déterminer le type de logiciel installé et escalader vers différentes équipes en fonction de la dangerosité du code.
Vérifier les droits correspondant au profil d'utilisateur.

5.2.2.5 Traitement

Informer l'utilisateur.
Revenir à l'état initial (reconfiguration du poste).
Appliquer la réponse adaptée à la nature du logiciel.

5.2.2.6 Actions post-incident

Revoir les besoins d'utilisateur et éventuellement adapter les profils d'utilisation.
Revérifier les failles de sécurité.
Sensibilisation adaptée à la situation de personnel.

5.2.3 Dysfonctionnement pouvant provenir d'un logiciel malveillant

5.2.3.1 Définition de l'incident

Constat d'un comportement anormal ou inhabituel d'un système ou d'une application susceptible d'être causé par un malware. L'anomalie peut revêtir des formes très diverses :

- perte ou modification de données,
- blocages d'application,
- dégradation des temps de réponse,
- accès disques inhabituels,
- surcharge réseau inhabituelle,
- messages inhabituels,
- modification de l'affichage,
- etc.

Illustrations (exemples, différentes formes, etc.) : perte ou vol de données, de fichiers, perte du contrôle de la souris, déni de service, dégradation des performances, etc.

Classification – On distingue ainsi différents types de logiciels malveillants ou malwares :

- les virus informatiques écrits dans le but de se propager à d'autres ordinateurs via un programme hôte,
- les bombes logiques se déclenchent suite à un événement particulier (date système, activation distante, etc.),
- les vers sont capables de se propager à travers un réseau en exploitant les différentes ressources de l'ordinateur qui les héberge pour se reproduire. Ils n'ont pas besoin d'un programme hôte, contrairement aux virus,
- les backdoors ou portes dérobées permettent le contrôle à distance d'un PC par un pirate. Un ordinateur infecté et contrôlé à distance par un pirate est appelé BOT ou zombie. Un réseau de PC infectés est un botnet.
- les rootkits permettent à un pirate de maintenir dans le temps un accès frauduleux à un système. Un rootkit s'utilise après une intrusion et l'installation d'une porte dérobée. Il a pour but la furtivité en cachant par exemple certains processus, certains fichiers et clefs de registre. Il opère au niveau du noyau, d'où son nom de « kit racine »,
- les chevaux de Troie (troyens) sont conçus pour effectuer diverses tâches à l'insu de l'utilisateur. Cela peut aller de l'installation d'autres malwares, à la désactivation de certains logiciels de protections (antivirus, pare-feu, etc.), en passant par l'envoi de messages de SPAM ou bien d'autres fonctionnalités,
- les spywares ou logiciels espion, mouchards ou espiogiciels sont conçus pour dérober/collecter des informations/données, sans que l'utilisateur en ait connaissance,
- les keyloggers ou enregistreurs de frappe sont des logiciels ou matériels espion qui enregistrent les touches frappées sur le clavier et les transmettent via les réseaux, afin de dérober des mots de passe ou autres informations susceptibles d'être recueillies par un pirate pour les revendre (adresse e-mail, CB, etc.), obtenir un accès sur un serveur, etc.,
- les adwares sont des logiciels publicitaires qui ouvrent des fenêtres de publicités.

Impacts potentiels selon les deux axes interne et externe (type d'impact, niveau) :

- perte de productivité variant en fonction des moyens mis en œuvre pour la protection et prévention,

- atteinte à l'image d'entreprise/organisme,
- perte financière.

Potentialité de l'événement générateur est forte dans les situations suivantes
- anti-malware non installé ou désactivé,
- base de signatures d'anti-malware obsolète,
- nouveau « malwares » non encore géré par l'anti-malware,
- bug de l'anti-malware.

Domaine concerné (locaux, personnel, réseau étendu, réseau local, applications, développements/maintenance, systèmes, domaines métier, sécurité générale, SSI, organisation, fournisseurs, etc.) :
- tout dépend du contexte dans lequel se trouve la machine, si une segmentation du réseau est réalisée.

Type de propagation (immédiat, progressif, dégressif) : immédiate ou progressive (bombe logique).

5.2.3.2 Mesures préventives possibles

Mesures organisationnelles
- mise en œuvre d'une politique antivirale : identification des besoins, des moyens adaptés aux niveaux de gravité des menaces, des responsabilités pour une détection d'un code malveillant qui doit être faite au plus près de son arrivée dans le SI,
- mise en place d'une procédure d'alerte immédiate suite à la détection d'un code malveillant, pour assurer une réactivité maximale,
- mise ne place d'un contrôle du bon fonctionnement des moyens : Mise à jour automatique des signatures, etc.

Mesures techniques
- utiliser des moyens de protection différents et complémentaires ; plusieurs anti-malware, filtrage, contrôle d'intégrité, paramétrage des systèmes, des applications, etc.),
- application régulière des correctifs pour diminuer la vulnérabilité des postes,
- contrôles multi-niveaux (passerelles HTTP, SMTP, messagerie interne, serveurs de données, postes de travail),
- segmentation des réseaux - Firewall, contrôle d'intégrité, IPS,
- contrôle des ordinateurs portables et supports.

5.2.3.3 Moyens de détection

Par l'utilisateur.
Par analyse de l'activité (tableaux de bord).
Par des outils d'analyse de comportement (IDS, IPS, SIEM[2], etc.).

[2] Security Information and Event Management

5.2.3.4 Qualification

Dans le processus de qualification il faut prendre en compte : le périmètre potentiellement concerné, le comportement du malware, le recoupement rapide avec d'autres incidents ou alertes récentes du même type, etc.
Mesures d'urgence. Exemples : confiner les machines infectées, couper certains accès réseau, communication de recommandations ciblées.

5.2.3.5 Analyse

Précautions nécessaires pour la préservation de preuves : par exemple, sous Windows, copier le malware sur une clé USB préalablement vaccinée (avec fichier autorun sain et non supprimable), à moins que le logiciel s'y invite tout seul !
Vérification de l'efficacité des mesures d'urgences (sinon les compléter et les réévaluer).
Recherches pour identifier avec exactitude le malware, puis ses parades.
Recherches pour connaître l'étendue réelle de l'infection.
Déterminer le point zéro de l'infection.
Choisir le plan d'action correctif le plus approprié (exemple : choisir entre une simple désinfection par logiciel antivirus ou refaire le système à partir des sauvegardes).
Identifier les modifications effectuées par le malware.
Communication des recommandations vers les utilisateurs et escalade vers le RSSI ou le RPCA.

5.2.3.6 Traitement

Renforcement des mesures pour éviter l'aggravation des conséquences (confinement, information, filtrage, déploiement de patchs ou patterns, etc.).
Activation éventuelle du PCA.
Résolution de l'incident (éradication).
Vérification du bon retour à la normale (disparition des symptômes et alertes).
Retour à la situation normale : fin du confinement ou des filtres d'isolement, retour des systèmes sains dans le réseau.

5.2.3.7 Actions post-incident

Analyse de ce qui a bien marché et de ce qui n'a pas fonctionné, recommandations pour améliorer les procédures de gestion de crise virale et la politique de sécurité.
Communication spécifique (information et sensibilisation des utilisateurs et des acteurs).
Audit.
Assurance.
Recours juridique.

5.2.4 Intrusions logiques

5.2.4.1 Description du type d'incident de sécurité

Définition de l'incident

Intrusion logique : c'est le fait pour une personne le plus souvent malveillante de pénétrer, dans un espace logique défini où sa présence n'est pas souhaitée, aux fins 1] d'accéder à des informations auxquelles elle n'aurait pas accès en temps normal ou 2] de modifier, détruire en tout ou partie les informations auxquelles elle accède par cette intrusion.

La notion d'intrusion suppose qu'il existe une volonté de réserver l'accès à des personnes, des ressources physiques ou logiques, à certaines personnes désignées. L'intrusion est constatée dès le franchissement de la limite entre « l'extérieur » et « l'intérieur » même si cette limite n'est que symbolique.

Cadre juridique :

Les intrusions logiques sont soumises (entre autres) à la loi du 5 janvier 1988, relative a la fraude informatique, dite Loi Godfrain.

Illustrations (exemples, différentes formes, etc.) :

- personne / organisation malveillante (pirate informatique, « joueur », employé « déçu », etc.) réalisant une intrusion (depuis le réseau interne ou de l'extérieur) en vue de récupérer des informations confidentielles, de détruire ou d'altérer des informations, etc.,
- personne accédant involontairement dans un espace privé et s'y maintenant.

Classification :

- impacts potentiels selon les deux axes interne et externe :
  - fuite ou vol d'informations,
  - altération et/ou destruction d'informations,
  - atteinte à l'image (communication sur la présence d'une faille),
  - introduction de programme malveillant (exemples : spam, botnet, etc.),
- potentialité de l'événement générateur est forte dans les situations suivantes:
  - architecture mal conçue ou mal implémentée, mauvaise configuration, correctifs de sécurité non installés ou pas à jour, etc.,
  - zone privée mal identifiée, utilisateurs non informés/sensibilisés,
  - ouverture du Système d'Information,
- domaines concernés :
  - systèmes, applications, sécurité logique, habilitations, réseaux, téléphonie,
- type de propagation :
  - immédiat.

5.2.4.2 Mesures préventives possibles

Mesures organisationnelles :

- politique de sécurité du SI :
  - politique de contrôle et de gestion des droits d'accès SI,
  - politique d'audits et de tests,
  - politique de mise à jour des systèmes (patch),
  - SMSI,
- réponse aux intrusions / Cellule de crise,
- sensibilisation/formation,

- information sur le périmètre privé (délimitation, surveillance des accès, sanctions).

Mesures techniques :
- mise en place de système de détection d'intrusion (IDS / IPS),
- mise en place d'architecture sécurisée (cloisonnement, contrôle d'accès),
- mise en place de leurres (honeypot),
- mise en place de système de DLP – Data Leak Protection (détection des fuites d'information),
- tests de vulnérabilité et d'intrusion.

5.2.4.3 Moyens de détection

Manifestation de l'incident (une intrusion n'est pas toujours visible) :
- perte ou modification d'information (destruction),
- dégradation des performances, dysfonctionnements, blocages, etc.,
- visualisation d'informations confidentielles à « l'extérieur » (presse, sites Web, blogs, etc.),
- réduction d'avantage concurrentiel (espionnage par intrusion).

Mesures organisationnelles de détection spécifiques :
- Veille.

Outils de détection disponibles :
- Analyse des logs,
- IDS / IPS,
- DLP.

Type d'alerte (qui alerte ?, qui alerter ?) :
- qui alerte : Cellule de surveillance (NOC / SOC), les administrateurs et les utilisateurs, l'auteur de l'intrusion (chantage dans le cas d'une intrusion malveillante, alerte volontaire dans le cas d'un accès accidentel),
- qui alerter : selon le « niveau » de l'intrusion :
  - interne : RSSI, DSI, Direction Métier, DG, l'administrateur du système d'habilitations concerné
  - externe : police, gendarmerie.

5.2.4.4 Analyse

Précautions nécessaires (préservation de preuve) : logs.

Mesures immédiates :
- activation de la Cellule de crise selon le niveau d'impact,
- communication appropriée.

Environnements potentiellement concernés : systèmes, applications, réseaux, téléphonie.

Outils d'aide à l'analyse : NOC / SOC, IDS / IPS, DLP.

Type d'escalade
- interne : RSSI, DSI, Direction Métier, DG,

- externe : police, gendarmerie, huissier, éditeurs concernés.

5.2.4.5 Traitement

Mesures pour éviter l'aggravation des conséquences : blocage de réseaux et /ou de systèmes, communication appropriée interne / externe, désactivation des accès au SI injustifiés constatés.

Déclarations réglementaires : police, gendarmerie, assurance.

Résolution de l'incident :

- reprise, réinstallation, restauration des données perdues ou altérées,
- révision des dispositifs de cloisonnement et de filtrage, etc.

5.2.4.6 Actions post-incident

Recours juridique : dépôt de plainte.

Assurance : déclaration de perte (si contrat spécifique souscrit).

Communication spécifique (sensibilisation, etc.) : sensibilisation des utilisateurs, formation des personnes de la cellule de crise, de la cellule de gestion / suivi des incidents, etc.

Audit : ethical hacking.

Recommandation : vérification des autres domaines susceptibles d'être vulnérables à la même intrusion. Revoir la politique de contrôle des accès au SI.

5.2.5 Usage inapproprié des ressources informatiques

5.2.5.1 Description du type d'incident de sécurité

Définition de l'incident

Usage inapproprié: L'incident de ce type survient quand un utilisateur exécute des actions non-conformes à la politique de sécurité et/ou aux règles d'utilisation du Système d'Information.

Illustrations (exemples, différentes formes, etc.) :

- téléchargement d'outils de piratage de mots de passe,
- envoi de courriels agressant les collaborateurs,
- publication du site Internet personnel,
- publication ou diffusion des données illicites ou diffamatoires,
- téléchargement ou diffusion de contenus prohibés (sites pédophiles par exemple),
- publication ou acquisition des données / médias piratés (images, musique, vidéo, progiciels, etc.),
- envoi vers les correspondants ou sites externes des données internes sensibles,
- attaques de sites externes (Spam, DoS, altération d'un site web, achats en ligne avec les cartes de crédit volées, etc.).

Classification :

- impacts potentiels selon les deux axes interne et externe (type d'impact, niveau) :
  - dégradation d'image de l'entreprise/organisme,
  - diminution de la capacité des ressources du SI,
  - impact financier,
- potentialité de l'événement générateur :
  - politique et règles de sécurité non communiquées,
  - absence de charte et du code de déontologie,
  - droits d'accès mal maitrisés (trop permissifs) et vulnérabilités non maitrisées,
  - absence des moyens de monitoring, du contrôle du contenu et d'IDS,
- domaines concernés (locaux, personnel, réseau étendu, réseau local, applications, développements/maintenance, systèmes, domaines métier, sécurité générale, SSI, organisation, fournisseurs, etc.) :
  - applications, systèmes,
- type de propagation (immédiat, progressif, dégressif) :
  - non déterminé.

5.2.5.2 Mesures préventives possibles

Mesures organisationnelles :

- mise en œuvre de la politique de sécurité, de la charte,
- mise en place et communication des sanctions.

Mesures techniques :

- mise en place de détection par IDS/IPS,
- mise en place de systèmes anti-spam en entrée et en sortie,
- mise en place des moyens de protection réseau/protocole bloquant les outils non autorisés (peer2peer, etc.),

- mise en place des moyens de proxy et de filtrage d'URLs pour verrouiller l'accès aux sites non-conformes à la politique de sécurité,
- mise en place de contrôle de contenu des messages et de pièces jointes,
- restriction des droits,
- mise en place de surveillance des logs d'accès et systèmes.

5.2.5.3 Détection

Manifestation de l'incident :

- signalisation par un utilisateur interne,
- signalisation, plainte par un utilisateur ou organisation externe,
- détection par supervision sécurité (IDS/IPS, SIEM),
- utilisation anormale des ressources (CPU, mémoire, stockage, bande passante),
- présence de nouveaux, fichiers et répertoires non identifiés et/ou flux réseaux,
- exécution de nouveau processus non connu.

Mesures organisationnelles de détection spécifiques : mise en place de cellule d'analyse systématique des logs et des plaintes.

Outils de détection disponibles :

- supervision sécurité (IDS/IPS, SIEM),
- supervision des ressources (serveurs, réseau, etc.).

Type d'alerte (qui alerte ?, qui alerter ?)

- qui alerte :
  - cellule de surveillance (NOC / SOC),
  - cellule Supervision,
  - utilisateur,
  - personne / organisme externe,
- qui alerter - selon le type d'incident :
  - activité criminelle : ressources humaines, direction juridique, police, personne/organisation externe impactée (le cas échéant),
  - dégradation majeure : RSSI, DSI, direction générale, direction de la communication,
  - dégradation ou impact mineure : RSSI, DSI, ressources humaines.

5.2.5.4 Analyse

Précautions nécessaires (préservation de preuves) : archivage des logs et des alertes.

Mesures immédiates (information, déclaration, anticipation du traitement, etc.)

- analyse pour déterminer s'il s'agit ou non d'acte criminel,
- évaluation d'impact sur l'image de l'entreprise/organisation,
- communication à la direction générale, de la communication, juridique, ressources humaines et la police en fonction de la nature et de la gravité de l'incident,
- mesures techniques conservatoires pour limiter l'impact de l'incident.

Environnements potentiellement concernés : ressources du SI, ressources d'autres SI.

Outils d'aide à l'analyse (logiciels, tests, check-lists, centres de support, internet, etc.) : NOC / SOC, IDS / IPS, SIEM (supervision sécurité).

Type d'escalade (notamment vers le RSSI ou le RPCA) :

- interne : RSSI, DSI, RH, DG, Direction Juridique,
- externe : police, gendarmerie.

5.2.5.5 Traitement

Mesures pour éviter l'aggravation des conséquences (confinement, information, évacuation, etc.)

- sauvegarde des preuves et des traces (log)
- arrêt de processus non-conformes, blocage de flux réseau non-conformes,
- avertissement des utilisateurs concernés.

Déclarations réglementaires : assurance, police ou gendarmerie dans le cas d'acte criminel.

Résolution de l'incident (éradication, reprise, déblocage, activation du PCA, filtrage, etc.) :

- enquête pour déterminer les auteurs (assurer la discrétion),
- suppression des programmes et des données non-conformes,
- filtrage des flux, etc.,
- mesures techniques de restauration d'état initial,
- mise en œuvre de moyens supplémentaires de détection ou optimisation des règles.

5.2.5.6 Actions post-incident

Recours juridique : sanctions, dépôt de plainte (si acte criminel).

Assurance : déclaration d'incident si organisme externe impacté.

Communication spécifique (sensibilisation, etc.) :

- sensibilisation des utilisateurs,
- communication publique dans les médias (si dégradation majeure d'image).

Audit et Recommandations

5.2.6 Incidents concernant les habilitations

5.2.6.1 Description du type d'incident de sécurité

Définition de l'incident

- verrouillage de compte à privilèges (de type : comptes administration, comptes de service ou comptes d'exploitation),
- extension ou existence de privilège, non justifiée (exemple : création compte à privilège sans accord, compte non supprimé lors du départ d'une personne),
- utilisation non autorisée de comptes à privilège (comptes impersonnels, comptes génériques),
- cumul de droits attribués à une personne non conforme à la législation ou à la réglementation,
- usurpation d'identité numérique,
- l'un des cas précédents concernant un utilisateur VIP.

Illustrations (exemples, différentes formes, etc.) :

- connexion via un compte et un mot de passe découverts,
    - par écoute passive sur le réseau (interception des comptes et mots de passe sur le réseau),
    - suite à un vol de matériel informatique pouvant héberger des données de connexion (PDA, ordinateur portable),
- blocage de comptes à privilèges suite à des tentatives d'intrusion,
- connexion à des heures non autorisées ou non justifiées pour le profil,
- connexion du compte alors que la personne n'est pas présente,
- apparition de nouveaux comptes administrateurs.

Classification :

- impacts potentiels selon les deux axes interne et externe (type d'impact, niveau) : fuite d'informations, destruction d'informations, déni de service, changement de configuration, dysfonctionnements, blocages utilisateurs, perte de productivité,
- potentialité de l'événement générateur : mauvaise gestion des droits d'accès, mots de passe d'administration non changés,
- domaines concernés (locaux, personnel, réseau étendu, réseau local, applications, développements/maintenance, systèmes, domaines métier, sécurité générale, SSI, organisation, fournisseurs, etc.),
- type de propagation (immédiat, progressif, dégressif) : immédiat ou progressif.

5.2.6.2 Mesures préventives possibles

Mesures organisationnelles :

- politique de sécurité du SI / Politique de traces / Politique de gestion des droits d'accès,
- politique de ségrégation des tâches (Segregation of Duties = SoD en anglais),
- notion de Propriétaire de ressource,
- mise en place d'une Cellule de surveillance Sécurité (remontée d'événements non conforme aux politiques),
- gestion centralisée des habilitations et des règles,
- mise en place d'audits et de revues périodiques des habilitations système, applications et services,

- définition d'une politique de détection,
- information et sensibilisation.

Mesures techniques :
- dispositifs de contrôle d'accès,
- outils de gestion et de suivi des identités et des droits,
- outils de « provisioning ».

5.2.6.3 Détection

Manifestation de l'incident :
- via les outils de gestion des évènements de sécurité,
- via les outils de détection d'intrusions,
- via les revues périodiques des habilitations pilotées par les responsables des applications, des systèmes et des infrastructures,
- via des outils de surveillance des activités inhabituelles (dans la limite des législations et réglementations locales).

Mesures organisationnelles de détection spécifiques : audit interne et revues périodiques.

Outils de détection disponibles :
- outils de centralisation des logs, et remontées d'alertes (temps réel ou reporting),
- outils de détection d'intrusions, IDS/IPS,
- outils d'audit des habilitations.

Type d'alerte :
- qui alerte : Help-Desk, Cellule de surveillance Sécurité, Auditeur, Responsable de ressource,
- qui alerter : Cellule de surveillance Sécurité, RSSI.

5.2.6.4 Analyse

Précautions nécessaires (préservation de preuve) :
- Préservation des logs,
- Réalisation d'une copie des supports concernés pour faire l'analyse.

Mesures immédiates (information, déclaration, anticipation du traitement, etc.) : désactivation du compte, arrêt de l'équipement mis en cause.

Environnements potentiellement concernés : tous les éléments de l'infrastructure (réseau, système, application).

Outils d'aide à l'analyse (logiciels, tests, check-lists, centres de support, internet, etc.) :
- outils de gestion des évènements de Sécurité,
- outils de détection d'intrusions,
- outils d'analyse des logs des systèmes et applications.

Type d'escalade (notamment vers le RSSI ou le RPCA) :
- interne : RSSI, DSI, Responsable Métier,
- externe : éditeurs concernés, responsable d'un prestataire en cause, etc.

5.2.6.5 Traitement

Mesures pour éviter l'aggravation des conséquences (confinement, information, évacuation, etc.) :

- supprimer / désactiver le compte,
- supprimer / désactiver l'accès (tentatives extérieures),
- réactivation du compte en cas de verrouillage, avec réinitialisation du mot de passe,
- application de correctifs (système, applicatif, etc.),
- application de procédure disciplinaire.

Déclarations réglementaires et contractuelles : police, gendarmerie, assurance.

Résolution de l'incident (éradication, reprise, déblocage, activation du PCA, filtrage, etc.)

- reprise, réinstallation, restauration des données perdues,
- ajustement des droits si nécessaire.

5.2.6.6 Actions post-incident

Recours juridique : dépôt de plainte.

Assurance : suivi du dossier sinistre (si contrat spécifique souscrit).

Communication spécifique (sensibilisation, etc.) :

- sensibilisation des utilisateurs,
- chartes Utilisateurs et Administrateurs.

Audit.

Recommandations :

- gestion des habilitations en fonction des rôles, profils,
- limitation et surveillance des comptes génériques,
- comptes nominatifs,
- authentification forte,
- limitation du nombre de sessions concurrentes,
- traçabilité des actions sur comptes à privilèges,
- sécurisation des flux de connexion,
- réalisation de revues périodiques et correction des écarts,
- verrouillage de comptes après un nombre de tentatives définie,
- suppression des comptes après le départ,
- révision des droits après mobilité,
- révision des processus de gestion des habilitations après mobilité,
- changement des mots de passe par défaut,
- changement périodique des mots de passe.

5.2.7 Déni de service Messagerie par saturation du relais public de messagerie

5.2.7.1 Description du type d'incident de sécurité

Définition de l'incident :
Fortes perturbations du trafic de messagerie publique, voire privée, liées à une attaque externe sur les relais publics de messagerie (MX – Mail eXchanger).

Illustrations – Afflux massif de :

- connexions au relais de messagerie, sans dépôt de message valide,
- messages pour des destinataires internes n'existant pas,
- messages non sollicités pour des destinataires internes existants.

Classification :

- origines possibles : spammers, hackers, concurrence, mafia,
- impacts potentiels selon les deux axes interne et externe (type d'impact, niveau) :
    - messages provenant de l'extérieur :
        - parvenant aux destinataires internes avec un délai inhabituel,
        - pour lequel les expéditeurs externes reçoivent une alerte de leur propre messagerie indiquant un retard ou un échec de délivrance,
    - messages émis vers l'extérieur :
        - parvenant aux destinataires externes avec un délai inhabituel,
        - pour lequel les expéditeurs internes reçoivent une alerte de leur propre messagerie indiquant un retard ou un échec de délivrance,
    - messages internes à l'entreprise/organisme :
        - parvenant aux destinataires avec un délai inhabituel,
        - impossible à envoyer (connexion avec Messagerie interrompue),
- potentialité de l'événement générateur : forte,
- domaine concerné :
    - personnes utilisant la messagerie,
    - applications utilisant la messagerie,
    - systèmes hébergeant l'environnement messagerie,
    - applications hébergées sur ces mêmes systèmes,
    - réseaux hébergeant les systèmes de messagerie,
- type de propagation : progressif.

5.2.7.2 Mesures préventives possibles

Mesures organisationnelles :

- définir un plan progressif :
    - d'actions, pour contenir l'attaque et en limiter les effets,
    - de communication interne pour informer des ralentissements, et inviter les utilisateurs à utiliser des canaux de communication alternatifs.

Mesures techniques :

- s'équiper de systèmes adaptés pour assurer le service relais public de messagerie,
- superviser attentivement les relais.

Principales caractéristiques d'un environnement de relais de messagerie public adapté :

- ne pas mixer les services « Relais public de Messagerie » et « Messagerie » sur les mêmes systèmes,
- disposer de relais redondés, voir secourus :
  - 2 relais (1 principal, 1secondaire),
  - éventuellement, 1 troisième relais, invisible,
- isoler ces relais par un pare-feu,
- équiper tous les relais (et pas seulement le principal) d'un système de filtrage anti-spam évolué :
  - capable de détecter et bloquer la plupart de ces attaques massives,
  - communicant avec l'annuaire d'entreprise/organisme, pour ne relayer au système de Messagerie que les messages qu'il pourra délivrer,
- configurer finement les relais afin qu'ils supportent les surcharges de trafic (tailles des queues de traitement, délai de rétention des quarantaines, etc.),
- selon contexte – désactiver les avis de non-délivrance d'un message provenant de l'extérieur vers un destinataire interne inconnu :
  - car c'est un moyen de DOS : Si l'adresse émettrice est fausse, l'avis ne sera jamais délivré, saturera les files d'attente, voire surchargera le système d'une autre entreprise/organisme,
  - mais cela gênera les véritables utilisateurs externes qui ne seront pas prévenus s'ils saisissent mal une adresse de messagerie (dupon@domain.com au lieu de dupont@domaine.com),
- adapter le TTL (Time To Live) des déclarations DNS « MX » (Mail eXchanger) pour qu'elles soient propagées rapidement (quelques minutes),
- organiser le circuit de décision et d'action pour que rapidement :
  - les enregistrements DNS puissent être modifiés,
  - le trafic Internet vers un relais puisse être bloqué.

5.2.7.3 Détection

Manifestation de l'incident : délai inhabituel de délivrance des messages.

Mesures organisationnelles de détection spécifiques : sensibiliser le Help-desk au repérage des symptômes utilisateurs dans les appels traités > déclenchement d'alerte dans les meilleurs délais.

Outils de détection disponibles :

- test régulier du délai d'échange de messages entre 2 messageries publiques indépendantes (par exemple entre partenaires, ou avec le fournisseur Internet),
- superviser les relais publics de messagerie,
- superviser les systèmes de messagerie.

Type d'alerte (qui alerte ?, qui alerter ?) :

- sources : équipes Help desk ou Supervision,
- cibles : équipes (très variable selon organisations) gérant :
  - les applications fournissant le service relais public de messagerie (messagerie, réseau, sécurité),
  - les systèmes hébergeant ces applications (Windows, Unix, messagerie etc.),
  - les applications de messagerie (messagerie),

- les systèmes hébergeant la messagerie (Windows, Unix, etc.),
- le firewall (sécurité ou réseau),
- le WAN et le LAN (réseau).

5.2.7.4 Analyse

Précautions nécessaires (préservation de preuves) : archiver les journaux des relais de messagerie et du firewall.
Environnements potentiellement concernés : messagerie.
Outils d'aide à l'analyse : outils de supervision et de logs des relais et du Firewall.
Type d'escalade : RSSI.
Communication interne : si les délais s'allongent, alerte générale aux utilisateurs, avant que le système de messagerie devienne inopérant.

5.2.7.5 Traitement

Mesures pour éviter l'aggravation des conséquences (confinement, information, évacuation, etc.) :

- identifier le relais le plus saturé,
- aiguiller le trafic sortant sur le relais le moins chargé (voire un relais dédié à la sortie), afin qu'il ne soit pas impacté par l'attaque (action au niveau des systèmes de messagerie ou des déclarations MX du DNS privé),
- aiguiller le trafic entrant sur un relais moins chargé, pour absorber la suite du trafic (action au niveau des déclarations MX du DNS public),
- couper le trafic Internet vers le relais saturé, le temps qu'il vide ses files d'attente (action au niveau du firewall, éventuel redémarrage du système).

Déclarations réglementaires : Néant.

Résolution de l'incident (éradication, reprise, déblocage, activation du PCA, filtrage, etc.) : Pas de résolution – Il faut juste mettre en œuvre les mesures évitant l'aggravation, et les répéter jusqu'à ce que l'attaque s'essouffle.

Note : Les attaques ciblent souvent un seul des relais – L'arrêter totalement pendant plusieurs minutes peut mettre un terme à l'attaque.

5.2.7.6 Actions post-incident

Recours juridique : Déposer une plainte contre X (de principe, pour les statistiques – les attaques sont d'origines supra-nationales, donc aucun recours à espérer).

Assurance : Risque complexe à assurer (il est plus simple de se protéger).

Communication spécifique (sensibilisation, etc.) : équipes techniques concernées, pour disposer de la meilleure réactivité lors de la survenance de l'incident.

Audit : Analyse régulière des performances des relais.

Recommandations : Si l'impact d'une attaque a été jugé intolérable, ou si les impacts importants sont courants, il est nécessaire de réviser et renforcer l'architecture de relais public.

5.2.8 Cas des incidents liés

5.2.8.1 Description du type d'incident de sécurité

Définition de l'incident

Des incidents sont liés lorsque l'un d'entre eux n'a été possible qu'à la suite de la survenance d'un incident précédent. Le second incident n'est pas une conséquence directe du premier mais sa survenance a été rendue possible ou facilitée. Une chaine d'incidents liés les uns aux autres est également possible. La difficulté dans le cas d'incidents liés est de faire le rapprochement entre des incidents pouvant être de natures très différentes et d'apporter une réponse organisée aux différents phénomènes.

Illustrations (exemples, différentes formes, etc.)

- premier incident : défaut de mise à niveau des paramètres de sécurité d'un serveur suite à une opération de maintenance. Second incident : exploitation des vulnérabilités du serveur par un utilisateur indélicat,
- premier incident : infection d'un poste de travail par un malware permettant d'en prendre la main à distance. Second incident : attaque du réseau interne à partir de la station de travail par un individu ayant connaissance de cette vulnérabilité. Dans un tel scénario, les attaques successives sont susceptibles d'introduire de nouvelles vulnérabilités à la source de nouveaux types d'incidents, par exemple attaque d'une entreprise ou un organisme tierce à partir d'un serveur interne vulnérable.

Classification :

- les impacts dans de tels scénarios sont ceux des incidents considérés séparément, avec une possibilité d'amplification due à la simultanéité,
- la potentialité d'incidents liés dépend fortement de l'efficacité du processus de gestion des incidents de sécurité, c'est-à-dire d'une part à l'exhaustivité des cas gérés et de la rapidité de détection et de mise en œuvre des contre-mesures,
- domaines concernés (locaux, personnel, réseau étendu, réseau local, applications, développements/maintenance, systèmes, domaines métier, sécurité générale, SSI, organisation, fournisseurs, etc.). Les incidents liés peuvent concerner des domaines différents,
- type de propagation (immédiat, progressif, dégressif) : immédiat ou différé.

5.2.8.2 Mesures préventives possibles

Les mesures préventives sont celles associées aux différents types d'incident considérés séparément.

5.2.8.3 Détection

Manifestation de l'incident : ce sont les manifestations de chaque incident individuel.

Mesures organisationnelles de détection spécifiques : faire en sorte que les personnes chargées de la résolution de chaque incident aient une information sur les types d'incident en cours.

Outils de détection disponibles : centralisation des informations sur les incidents.

Type d'alerte (qui alerte ?, qui alerter ?) : alerter le RSSI et les responsables des domaines concernés.

5.2.8.4 Analyse

Précautions nécessaires (préservation de preuve) : propres à chaque type d'incident.

Mesures immédiates (information, déclaration, anticipation du traitement, etc.) : lors de l'analyse d'un incident, prendre en compte les scénarios d'extension possibles et identifier l'incident initial (exemple : vérifier le paramétrage des autres équipements du domaine).

Environnements potentiellement concernés : tous.

Outils d'aide à l'analyse (logiciels, tests, check-lists, centres de support, internet, etc.) Base des incidents, exploitation centralisée des journaux et analyses de corrélations.

Type d'escalade (notamment vers le RSSI ou le RPCA) : RSSI.

5.2.8.5 Traitement

Mesures pour éviter l'aggravation des conséquences (confinement, information, évacuation, etc.) : établir des priorités. En principe le premier incident générateur doit être traité en premier. Si tous les incidents ne peuvent être traités simultanément, établir des priorités en fonction des impacts potentiels et de l'importance des vulnérabilités résiduelles.

Déclarations réglementaires : propres à chaque type d'incident concerné.

Résolution de l'incident (éradication, reprise, déblocage, activation du PCA, filtrage, etc.) : propre à chaque type d'incident concerné.

Selon type d'incident : méthode, outils, etc. : propres à chaque type d'incident concerné.

5.2.8.6 Actions post-incident

Si nécessaire, révision des mesures de sécurité (mesures préventives, etc.) pour réduire la probabilité d'occurrence d'incidents liés et/ou de gestion des incidents (outils d'analyse, etc.).

Communication spécifique (sensibilisation, etc.) : établissement d'un rapport de suivi.

Recours juridique : propre à chaque type d'incident concerné.

Assurance : propre à chaque type d'incident concerné.

6 - Glossaire (source principale : Wikipedia)

Terme	Commentaire
CD	Un CD (abréviation de (en) **« Compact Disc »**), ou disque compact, est un disque optique utilisé pour stocker des données sous forme numérique.
CPU	Le **processeur, ou CPU** (de l'anglais Central Processing Unit, « Unité centrale de traitement »), est le composant de l'ordinateur qui exécute les programmes informatiques.
CERT	**Central Emergency Response Team** / Coordination Center situé à l'université de Carnegie Mellon aux Etats-Unis.
CERTA	**Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques** du gouvernement français.
COBIT	Le CobiT **(Control Objectives for Information and related Technology** – Objectifs de contrôle de l'Information et des Technologies Associées) est un outil fédérateur qui permet d'instaurer un langage commun pour parler de la Gouvernance des systèmes d'information tout en tentant d'intégrer d'autres référentiels tels que ISO 9000, ITIL.
CNIL	La **Commission nationale de l'informatique et des libertés** (CNIL) est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle exerce ses missions conformément à la loi n°78-17 du 6 janvier 1978 modifiée le 6 août 2004.
CSIRT	(Computer Security Incident Response Team) ou ISIRT (Information Security Incident Response Team).
DLP	Le terme **Data Loss Prevention (DLP)** fait référence à un ensemble de techniques de protection contre la fuite d'informations en informatique.
DNS	Le **Domain Name System** (ou DNS, système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.
DVD	Le DVD officiellement **Digital Versatile Disc** est un disque optique numérique exploité pour la sauvegarde et le stockage de données, notamment la vidéo pour sa déclinaison DVD Video.
Firewall	Un **pare-feu,** ou firewall (de l'anglais), est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés sur ce réseau informatique. Il mesure la prévention des applications et des paquets.
IDS	Un **système de détection d'intrusion** (ou IDS : Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée (un réseau ou un hôte). Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.
IPS	Un **système de prévention d'intrusion** (ou IPS, Intrusion Prevention System) est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. Les IPS peuvent donc parer les attaques connues et inconnues.
IT	Informatique et Télécoms (Information Ttechnology)
ITIL	ITIL **(Information Technology Infrastructure Library** pour « Bibliothèque pour l'infrastructure des technologies de l'information ») est un ensemble d'ouvrages recensant les bonnes pratiques (« best practices ») pour le management du système d'information, édictées par l'Office public britannique du Commerce (OGC).

Terme	Commentaire
LINUX	Linux est un logiciel libre créé en 1991 par Linus Torvalds et développé sur Internet par des milliers d'informaticiens bénévoles ou salariés. C'est le noyau de nombreux systèmes d'exploitation. Il est de type UNIX et compatible POSI.
MX	Un enregistrement **Mail eXchanger** (MX) est un type d'enregistrements du Domain Name System qui associe un nom de domaine à un serveur de messagerie électronique associé à son numéro de préférence.
NOC	Un **centre d'opération d'un réseau** (en anglais, Network Operations Center, abrégé NOC) est un service chargé du contrôle des transactions, de la surveillance des incidents, de la charge d'un réseau local ou interconnecté
NTFS	NTFS **(New Technology File System)** est un système de fichiers conçu pour Windows NT (et ses successeurs chez Microsoft) pour stocker des données sur disque dur.
MSSP	**Managed Security Services Provider** : fournisseurs de services d'infogérance en sécurité.
PC	Personal computer – ordinateur personnel.
PCA	Le **plan de continuité** ou **plan de continuité d'activité** (PCA) est à la fois le nom d'un concept, d'une procédure et du document qui la décrit. Ce plan doit permettre à un groupe (gouvernement, collectivité, institution, entreprise, hôpital..) de fonctionner même en cas de désastre ; quitte à ce que ce soit en mode dégradé, ou en situation de crise majeure.
PDA	Un **assistant numérique personnel** est un appareil numérique portable, souvent appelé par son sigle anglais **PDA** pour *Personal Digital Assistant.*
Peer2peer	Le **pair-à-pair** (traduction de l'anglicisme peer-to-peer, souvent abrégé « P2P »), est un modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur.
PRA	En informatique, un **plan de reprise d'activité** (en anglais Disaster Recovery Plan ou DRP) 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.
Proxy	Un **serveur mandataire ou proxy** (de l'anglais) est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur.
PSSI	La **politique de sécurité des systèmes d'information** (PSSI) est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration, État, unions d'États …) en matière de sécurité des systèmes d'information (SSI).
RFID	La **radio-identificatio**n plus souvent désignée par le sigle RFID (de l'anglais Radio Frequency IDentification) est une méthode pour mémoriser et récupérer des données à distance en utilisant des marqueurs appelés « radio-étiquettes » (« RFID tag » ou « RFID transponder » en anglais.
RPCA	Le responsable du plan de continuité d'activité
RSSI	Le responsable de la sécurité des systèmes d'information
SI	Un **système d'information** (SI) est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un environnement donné.
SIEM	**Security Information and Event Management** Le principe du Security Information Management (SIM) est de gérer les évènements du Système d'Information (SI). Appelés également SEM (Security Event Management) ou SEIM (Security Event Information Management) ou encore SIEM (Security Information and Event Management), ils permettent de gérer et corréler les logs. On parle de corrélation car ces solutions sont munies de moteurs de corrélation qui permettent de relier plusieurs évènements à une même cause.

Terme	Commentaire
SMSI	Un système de gestion de la sécurité de l'information (en anglais : Information security management system, ou ISMS) est, comme son nom le suggère, un système de gestion concernant la sécurité de l'information. L'expression Système de Management de la Sécurité de l'Information (SMSI) est également utilisée en français. Le plus connu des SMSI est ISO/CEI 27001, publié par l'ISO en complément de ISO/CEI 27002 (anciennement référencé ISO/CEI 17799.
SOC	Un centre d'opération de sécurité (en anglais, Security Operations Center, abrégé SOC) est un service chargé du contrôle de la sécurité des transactions et de la surveillance des incidents de sécurité.
SOD	**Separation of Duties** - La contrainte de séparation des pouvoirs est utilisée pour assurer le respect de la politique des habilitations.
SMTP	Le **Simple Mail Transfer Protocol** (littéralement « Protocole simple de transfert de courrier »), est un protocole de communication utilisé pour transférer le courrier électronique (courriel) vers les serveurs de messagerie électronique.
SSI	La **sécurité des systèmes d'information** (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information.
TTL	Le ***Time to Live*** (« temps de vie »), abrégé **TTL**, indique le temps pendant lequel une information doit être conservée, ou le temps pendant lequel une information doit être gardée en cache.
URL	Le sigle **URL (de l'anglais Uniform Resource Locator**, littéralement « localisateur uniforme de ressource »), auquel se substitue informellement le terme adresse web, désigne une chaîne de caractères utilisée pour adresser les ressources du World Wide Web : document HTML, image, son, forum Usenet, boîte aux lettres électronique, etc. Les URL constituent un sous-ensemble des identifiants uniformisés de ressource (URI). Le format (syntaxe) d'une URL est décrit dans le RFC 3986.
USB	**L'Universal Serial Bus** (USB) est une norme relative à un bus informatique en transmission série qui sert à connecter des périphériques informatiques à un ordinateur.
VIP	VIP signifie en anglais « personne très importante » (Very Important Person, de russe viesima imenitaïa persona) et désigne par exemple les chefs d'État, les politiciens, les personnes très riches, les célébrités.
VLAN	Un **réseau local virtuel**, communément appelé **VLAN** (pour *Virtual* LAN), est un réseau informatique logique indépendant. De nombreux VLAN peuvent coexister sur un même commutateur réseau (switch).
WAN	Un **réseau étendu** (terme recommandé au Québec), souvent désigné par l'anglais Wide Area Network (WAN), est un réseau informatique couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voire de la planète entière.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr