UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T E.409

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(05/2004)

SÉRIE E: EXPLOITATION GÉNÉRALE DU RÉSEAU, SERVICE TÉLÉPHONIQUE, EXPLOITATION DES SERVICES ET FACTEURS HUMAINS

Gestion de réseau – Gestion du réseau international

Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication

Recommandation UIT-T E.409

RECOMMANDATIONS UIT-T DE LA SÉRIE E

EXPLOITATION GÉNÉRALE DU RÉSEAU, SERVICE TÉLÉPHONIQUE, EXPLOITATION DES SERVICES ET FACTEURS HUMAINS

EXPLOITATION DES RELATIONS INTERNATIONALES	
Définitions	E.100–E.103
Dispositions de caractère général concernant les Administrations	E.104–E.119
Dispositions de caractère général concernant les usagers	E.120–E.139
Exploitation des relations téléphoniques internationales	E.140–E.159
Plan de numérotage du service téléphonique international	E.160–E.169
Plan d'acheminement international	E.170–E.179
Tonalités utilisées dans les systèmes nationaux de signalisation	E.180–E.189
Plan de numérotage du service téléphonique international	E.190–E.199
Service mobile maritime et service mobile terrestre public	E.200–E.229
DISPOSITIONS OPÉRATIONNELLES RELATIVES À LA TAXATION ET À LA COMPTABILITÉ DANS LE SERVICE TÉLÉPHONIQUE INTERNATIONAL	
Taxation dans les relations téléphoniques internationales	E.230–E.249
Mesure et enregistrement des durées de conversation aux fins de la comptabilité	E.260–E.269
UTILISATION DU RÉSEAU TÉLÉPHONIQUE INTERNATIONAL POUR LES APPLICATIONS NON TÉLÉPHONIQUES	
Généralités	E.300–E.319
Phototélégraphie	E.320–E.329
DISPOSITIONS DU RNIS CONCERNANT LES USAGERS	E.330–E.349
PLAN D'ACHEMINEMENT INTERNATIONAL	E.350–E.399
GESTION DE RÉSEAU	
Statistiques relatives au service international	E.400–E.404
Gestion du réseau international	**E.405–E.419**
Contrôle de la qualité du service téléphonique international	E.420–E.489
INGÉNIERIE DU TRAFIC	
Mesure et enregistrement du trafic	E.490–E.505
Prévision du trafic	E.506–E.509
Détermination du nombre de circuits en exploitation manuelle	E.510–E.519
Détermination du nombre de circuits en exploitation automatique et semi-automatique	E.520–E.539
Niveau de service	E.540–E.599
Définitions	E.600–E.649
Ingénierie du trafic des réseaux à protocole Internet	E.650–E.699
Ingénierie du trafic RNIS	E.700–E.749
Ingénierie du trafic des réseaux mobiles	E.750–E.799
QUALITÉ DE SERVICE: CONCEPTS, MODÈLES, OBJECTIFS, PLANIFICATION DE LA SÛRETÉ DE FONCTIONNEMENT	
Termes et définitions relatifs à la qualité des services de télécommunication	E.800–E.809
Modèles pour les services de télécommunication	E.810–E.844
Objectifs et concepts de qualité des services de télécommunication	E.845–E.859
Utilisation des objectifs de qualité de service pour la planification des réseaux de télécommunication	E.860–E.879
Collecte et évaluation de données d'exploitation sur la qualité des équipements, des réseaux et des services	E.880–E.899

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T E.409

Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication

Résumé

La présente Recommandation a pour objet d'analyser, de structurer et de proposer une méthode permettant d'organiser la prise en charge des incidents au sein d'une organisation de télécommunication participant à la fourniture de télécommunications internationales, en fonction du déroulement et de la nature des incidents. Le déroulement des incidents et leur prise en charge interviennent lorsqu'il s'agit de classer un événement comme un simple événement, comme un incident, comme une atteinte à la sécurité ou comme une situation de crise. Le déroulement des incidents joue aussi un rôle dans les premières décisions importantes qui doivent être prises.

L'emploi fortement accru de l'ordinateur dans le domaine des télécommunications internationales entraîne dans son sillage la criminalité informatique. Au cours des dernières années, cette criminalité a littéralement explosé, ainsi que l'ont démontré plusieurs enquêtes menées aux niveaux international et national. Dans la plupart des pays, on ne connaît pas le nombre exact d'intrusions informatiques, ni d'incidents, en particulier ceux qui sont liés aux télécommunications internationales.

La majorité des organisations ou des sociétés de télécommunication ne sont pas spécialement organisées pour gérer les atteintes à la sécurité des réseaux d'information et de communication (ICN, *information and communication network*), bien qu'elles puissent disposer d'équipes de crise polyvalentes gérant les différents types de crises. Lorsqu'un incident relatif à la sécurité d'un réseau ICN se produit, il est traité ponctuellement, c'est-à-dire la personne qui le détecte prend la responsabilité de le traiter au mieux. Dans certaines organisations, on a tendance à oublier et à dissimuler les atteintes à la sécurité des réseaux ICN, parce qu'elles sont susceptibles d'affecter la production, la disponibilité et les recettes.

Souvent, lorsqu'une atteinte à la sécurité d'un réseau ICN est détectée, la personne qui la détecte ne sait pas qui elle devrait aviser. Dans le secteur informatique, il se peut alors que l'administrateur du système ou du réseau se borne, pour se débarrasser du problème, à trouver une solution de rechange ou un bricolage hâtif. Il ne dispose ni des pouvoirs, ni du temps, ni de l'expérience nécessaires pour apporter des corrections au système afin que l'incident touchant à la sécurité du réseau ICN ne se reproduise plus. Pour ces raisons majeures, il vaut mieux disposer d'une unité ou d'un groupe formé qui puisse prendre en charge promptement et correctement les atteintes à la sécurité. De nombreuses questions peuvent en outre concerner des domaines aussi divers que celui des relations avec les médias, le domaine juridique, le domaine relatif à l'application des lois, celui de la part de marché ou le domaine financier.

L'emploi de classifications différentes, lors de la notification ou de la prise en charge d'un incident, peut conduire à des malentendus qui peuvent par la suite empêcher qu'une atteinte à la sécurité d'un réseau ICN reçoive l'attention convenable ou la prise en charge rapide qui seraient nécessaires pour y mettre fin, pour la contenir et pour l'empêcher de se reproduire. Cela peut avoir de sérieuses conséquences sur l'organisation touchée (la victime).

Pour maîtriser la prise en charge des incidents et leur notification, il convient de comprendre comment ils sont détectés, pris en charge et résolus. L'établissement d'une structure générale de traitement des incidents (à savoir, les incidents physiques, administratifs ou organisationnels, et logiques) permet d'obtenir une image générale de la nature et du déroulement d'un incident. Une terminologie uniformisée assure une compréhension commune des mots et des termes.

Source

La Recommandation UIT-T E.409 a été approuvée le 28 mai 2004 par la Commission d'études 2 (2001-2004) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T E.409

Organisation en cas d'incident et prise en charge des incidents relatifs à la sécurité: lignes directrices destinées aux organisations de télécommunication

1 Introduction

1.1 Domaine d'application

La présente Recommandation a pour objet d'analyser, de structurer et de proposer une méthode permettant d'organiser la prise en charge des incidents au sein d'une organisation de télécommunication participant à la fourniture de télécommunications internationales, en fonction du déroulement et de la nature des incidents. Le déroulement des incidents et leur prise en charge interviennent lorsqu'il s'agit de classer un événement comme un simple événement, comme un incident, comme une atteinte à la sécurité ou comme une situation de crise. Le déroulement des incidents joue aussi un rôle dans les premières décisions importantes qui doivent être prises.

La présente Recommandation donne un aperçu général et des orientations en ce qui concerne la préparation de l'organisation en cas d'incident et de la prise en charge des atteintes à la sécurité.

La présente Recommandation est générique par nature et n'énonce ni n'aborde des prescriptions destinées à des réseaux particuliers.

La présente Recommandation vise à faciliter l'amélioration à l'échelle internationale de la sécurité des réseaux de télécommunication. Cette amélioration pourrait être facilitée si les prescriptions énoncées dans la présente Recommandation pouvaient également être appliquées aux réseaux d'information et de communication (ICN, *information and communication network*) nationaux.

Pour maîtriser la prise en charge des incidents et leur notification, il convient de comprendre comment ils sont détectés, pris en charge et résolus. L'établissement d'une structure générale de traitement des incidents (à savoir, les incidents physiques, administratifs ou organisationnels, et logiques) permet d'obtenir une image générale de la nature et du déroulement d'un incident. Une terminologie uniformisée assure une compréhension commune des mots et des termes.

L'emploi de classifications différentes, lors de la notification ou de la prise en charge d'un incident, peut conduire à des malentendus qui peuvent par la suite empêcher qu'une atteinte à la sécurité d'un réseau ICN reçoive l'attention convenable ou la prise en charge rapide qui seraient nécessaires pour y mettre fin, pour la contenir et pour l'empêcher de se reproduire. Cela peut avoir de sérieuses conséquences sur l'entreprise touchée (la victime).

La présente Recommandation décrit le déroulement et la prise en charge d'un incident.

La définition d'un incident varie suivant les professions, les organisations et les personnes.

Au sens général, un incident peut être un événement quelconque, allant d'une sauvegarde erronée, une interruption des services, un virus jusqu'à une intrusion informatique.

1.2 Définitions

L'ISO 17799 mentionne les incidents, les atteintes à la sécurité et les atteintes à la sécurité informatique.

Seule "l'atteinte à la sécurité" est définie comme étant "une infraction à la sécurité, une menace à l'égard de celle-ci, une faiblesse et un dysfonctionnement qui pourraient avoir une incidence sur la sécurité des biens institutionnels". Nulle part, il n'est donné d'explication des termes "incident" et "atteinte à la sécurité informatique". Dans la présente Recommandation, on suppose qu'un incident est moins grave qu'une atteinte à la sécurité et qu'une atteinte à la sécurité informatique est un type particulier d'atteinte à la sécurité.

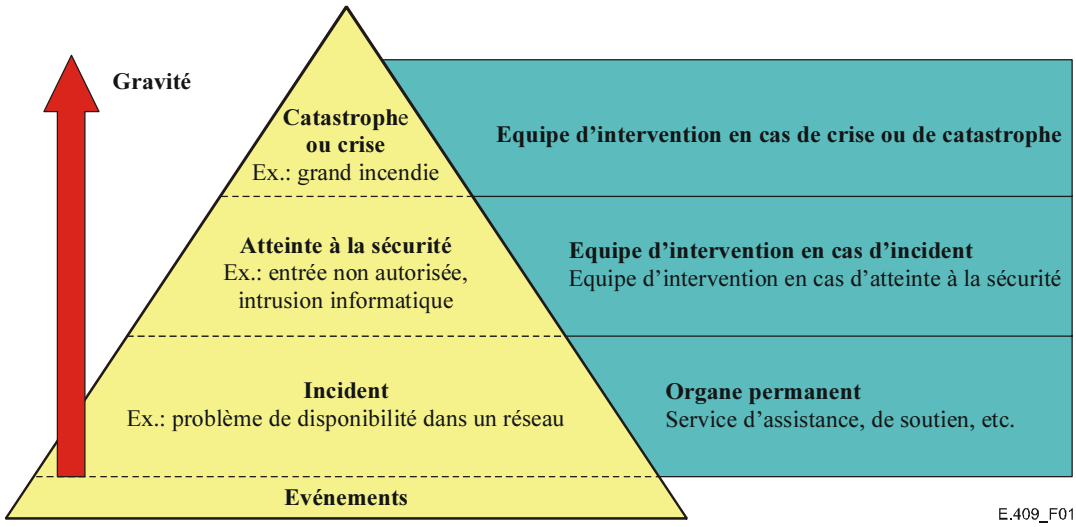

Figure 1/E.409 – Pyramide des événements

La Figure 1 illustre la pyramide des événements. A la base est situé l'événement, suivi de l'incident, de l'atteinte à la sécurité, et au sommet sont situées la crise et la catastrophe. Au plus, un événement est proche du sommet, au plus il est grave. Afin qu'il soit fait usage d'un vocabulaire commun et pertinent en ce qui concerne la prise en charge des incidents dans les réseaux ICN, la présente Recommandation définit les termes suivants:

1.2.1 **événement**: fait observable, qu'il n'est pas possible de prédire ou de contrôler (complètement).

1.2.2 **incident**: événement pouvant conduire à un fait ou à un épisode peu grave.

1.2.3 **atteinte à la sécurité**: tout événement préjudiciable pouvant menacer certains aspects de la sécurité.

1.2.4 **atteinte à la sécurité des réseaux d'information et de communication (ICN)**: tout événement concret ou soupçonné d'être préjudiciable, en rapport avec la sécurité des réseaux ICN. On peut indiquer à titre d'exemple:

- l'intrusion par le réseau dans les systèmes informatiques des réseaux ICN;
- la présence de virus informatiques;
- le sondage par le réseau de la vulnérabilité d'une gamme de systèmes informatiques;
- la perte d'appels au niveau des autocommutateurs privés;
- tout autre événement non désiré résultant d'actions non autorisées ou extérieures.

1.2.5 **crise**: état résultant d'un événement ou de la connaissance d'un événement à venir qui pourrait avoir de graves conséquences néfastes. Au cours d'une crise, on peut, dans le meilleur des cas, avoir la possibilité de prendre des mesures pour éviter que cette crise ne devienne une catastrophe. Lorsqu'une **catastrophe** se produit, on dispose généralement d'un plan d'urgence pour les entreprises (BCP, *business continuency plan*) et d'une équipe de gestion de la crise pour prendre en charge la situation.

1.3 Démarche logique

Il est recommandé que les organisations de télécommunication créant, en une première étape, des équipes d'intervention en cas d'incident (relatif à la sécurité informatique), fassent savoir, pour éviter des malentendus, qu'ils emploient une classification. La collaboration est beaucoup plus facile si l'on emploie le même "langage".

Il est aussi recommandé que les organisations utilisent les termes "incident" et "atteinte à la sécurité des réseaux ICN", et définissent leurs subdivisions en fonction de la gravité de ceux-ci. Par nature, une atteinte à la sécurité d'un réseau ICN est un événement non désiré ou non autorisé. Cela veut dire que les atteintes à la sécurité des réseaux ICN englobent les intrusions informatiques, les attaques par déni de service ou les virus, en fonction de la motivation, de l'expérience et des ressources documentées disponibles dans l'entreprise. Dans les organisations qui disposent de vraies équipes destinées à combattre les virus, ceux-ci peuvent ne pas être considérés comme des atteintes à la sécurité des réseaux ICN, mais seulement comme des incidents.

Un exemple ou modèle d'une telle subdivision est le suivant:

- Incidents
  - violation de l'éthique en vigueur sur Internet (pollupostage, contenu abusif, etc.);
  - violation des politiques en matière de sécurité;
  - virus isolés.
- Atteintes à la sécurité des réseaux ICN
  - explorations et sondages;
  - intrusions informatiques;
  - sabotage et endommagement informatiques (attaques bloquant l'accessibilité telles que le bombardement, attaques par déni de services);
  - logiciels malveillants (virus, cheval de Troie, vers, etc.);
  - vol d'informations et espionnage;
  - usurpation d'identité.

En employant la même granularité et la même précision dans la terminologie, il est possible d'acquérir de l'expérience en ce qui concerne les sujets suivants:

- indication relative à la gravité et à l'étendue;
- indication quant à la nécessité d'être rapide;
- effets en ce qui concerne les contre-mesures;
- coûts éventuels impliqués.

2 Description du système

2.1 Nature et déroulement

En établissant une structure générale de traitement des incidents (à savoir, les incidents physiques, administratifs ou organisationnels, et logiques), nous obtenons une image générale de la nature et déroulement d'un incident.

2.1.1 Principes de protection

Les mécanismes de protection qu'une organisation implémente devraient tenir compte des prescriptions imposées par sa politique en matière de sécurité des réseaux ICN ou par d'autres lignes directrices, y compris les aspects juridiques. L'organisation de la prise en charge des incidents et ses tâches doivent aussi respecter ces prescriptions.

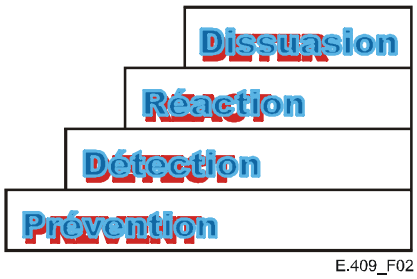

Figure 2/E.409 – Principes de protection

La Figure 2 illustre la nécessité de commencer "à zéro". Afin d'assurer une protection cohérente, l'organisation devrait être telle que toutes les étapes impliquées dans les mécanismes de protection en matière de sécurité soient mises en implémentées.

Les mécanismes *préventifs* sont appliqués en premier lieu. Lorsque des mécanismes appropriés sont mis en place, à savoir lorsque la protection physique et logique est assurée, il est alors possible de procéder à l'identification et d'activer les mécanismes de détection.

Les mécanismes de *détection* pourraient, dans leurs formes les plus simples, consister en la vérification des fichiers de consignation, l'émission d'alertes logiques ou physiques, à savoir des alertes antivol, des alertes d'incendie ou d'autres fonctions de surveillance. Un tel mécanisme est par exemple le système de détection de l'intrusion (IDS, *intrusion detection system*).

Après avoir détecté un incident, il convient de prendre des mesures. Ces mesures comprennent habituellement les tâches suivantes:

- arrêter un incident en cours;
- définir l'étendue de l'incident ou l'échelle à laquelle il se produit;
- limiter les dégâts;
- prendre des mesures afin d'enquêter sur le cours des événements;
- empêcher que l'événement ne se reproduise.

Les mesures pour arrêter et limiter l'incident (ou le contenir) et empêcher qu'il ne se reproduise sont prises par l'organe permanent, à savoir le service d'assistance ou de soutien. Si l'incident dégénère en crise, un groupe de crise spécialement constitué entre en action. En ce qui concerne l'enquête et l'analyse de l'incident, il est recommandé que ce soit l'équipe d'intervention en cas d'incident qui s'en charge.

Une fois que ces trois mécanismes de protection ont été mis en place et fonctionnent, il convient d'être dissuasif, ce qui veut dire que l'agresseur est informé du fonctionnement des mécanismes de protection et que la détection et la réaction aux incidents seront rapides. Cet effet dissuasif peut être renforcé en réagissant à tous les incidents et en signalant tous les incidents illicites aux autorités chargées de l'application des lois.

2.1.2 Structure de la prise en charge des incidents

Afin de comprendre le rôle de la prise en charge des incidents et de l'organisation du traitement de ceux-ci dans l'organisation, il est recommandé d'employer une structure de prise en charge des incidents. Cette structure permet de donner un aperçu général du déroulement de l'incident, en décrivant ses occurrences, les mesures susceptibles de le maîtriser, la récupération et le suivi.

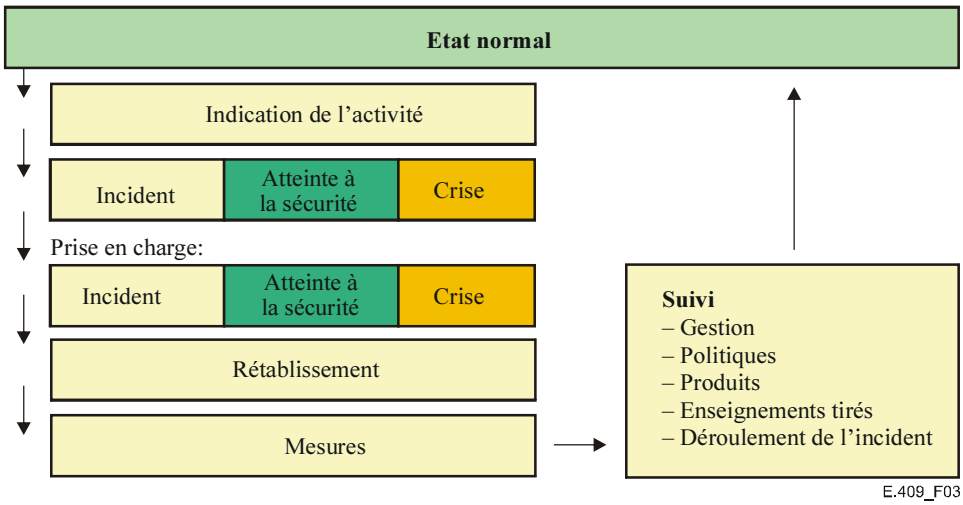

Figure 3/E.409 – Structure de la prise en charge d'un incident

La structure indique (voir Figure 3) que tous les événements, tous les incidents, toutes les atteintes à la sécurité et toutes les crises surviennent dans un état normal, c'est-à-dire dans une organisation fonctionnant normalement.

Lorsqu'on observe une activité susceptible de provoquer un incident ou porter atteinte à la sécurité, le problème est pris en charge par l'organe permanent comme décrit ci-dessous. Le temps qui s'écoule entre l'indication et le moment où se produit l'incident ou l'atteinte à la sécurité peut être très court. Le type d'indication d'un incident peut être l'existence d'un virus au niveau d'une seule station de travail, un dysfonctionnement dans le réseau, etc. En ce qui concerne les atteintes à la sécurité, on trouve des indicateurs dans les fichiers de consignation, dans les filtres pare-feu, etc. Des indications pourraient aussi être le déclenchement des alertes, des informations fournies par les caméras de surveillance, etc.

Lorsqu'un *incident ou un incident touchant à la sécurité se produit*, il est évalué en fonction de son étendue et de ses conséquences. Un incident peut dégénérer en atteinte à la sécurité ou en crise. L'organe permanent prend en charge les incidents, tandis que l'équipe d'intervention en cas d'incident informatique (CSIRT, *computer incident response team*) prend en charge les atteintes à la sécurité. Un groupe de gestion de crise spécialement constitué prend en charge les crises.

Une équipe CSIRT peut former l'ensemble de l'équipe de sécurité pour une organisation de télécommunication ou être totalement distincte de celle-ci. Ou alors, bien qu'une organisation de télécommunication ne dispose pas d'une équipe CSIRT distincte, ce rôle peut en fait être implicitement assumé par l'équipe de sécurité de l'organisation.

Les *mesures* sont prises suivant une procédure de routine bien établie ou suivant une procédure type. Dans le cas de graves atteintes à la sécurité ou de crise, les mesures dépendent de l'étendue et des conséquences de l'incident. Elles sont appliquées par l'équipe de sécurité ou l'équipe d'intervention en cas d'incident.

Au cours du *rétablissement*, des mesures sont prises afin que les choses redeviennent normales. En fonction de l'événement qui s'est produit, cela signifie le redémarrage des systèmes informatiques ou de réseau, la réinstallation des programmes ou la récupération des sauvegardes. Ces mesures pourraient consister en la remise à l'état initial des alertes, la reconstruction des biens endommagés, etc.

Tandis que ces travaux sont effectués, il convient aussi d'évaluer s'il faut donner des suites juridiques à un événement. Cela pourrait nécessiter une enquête plus approfondie et l'obtention des preuves, etc.

Il est important d'assurer le *suivi* des tâches accomplies pendant la prise en charge des incidents et des atteintes à la sécurité, ainsi que des crises. L'objectif de ce suivi est d'améliorer les opérations et les procédures normales afin d'empêcher les nouvelles occurrences et de minimiser les conséquences et les coûts éventuels.

Le rapport de suivi peut induire un changement dans la procédure de traitement des incidents, dans les produits et dans les politiques. Il est donné à la direction un résumé des incidents et des atteintes à la sécurité survenus, leurs étendues, leurs conséquences et leurs coûts. Ce résumé devrait aussi porter sur l'efficacité de l'organisation de la prise en charge des incidents. Il conviendrait d'élaborer un fichier contenant les leçons ou les enseignements tirés afin de pouvoir comparer les différents incidents et de trouver des méthodes et des pratiques plus efficaces de détection et de prise en charge des incidents et des atteintes à la sécurité.

2.2 Déroulement des incidents

Le déroulement d'un incident ou d'une atteinte à la sécurité est décrit ci-après. Cette démarche est fondée sur les enseignements tirés et devrait pouvoir s'appliquer à toutes les organisations de télécommunication et tous les types d'incidents, puisque le déroulement est simple et général. Le déroulement des incidents peut être comparé à ce qui se passe lorsque des mesures sont prises dans le cas d'un accident, d'un incendie, etc. Le point de départ, ou le paramètre, est le fait qu'un événement se produise, qui a des conséquences sur l'organisation.

2.2.1 Phases de la prise en charge des crises

Dans la gestion des crises, on considère qu'une crise passe par les trois phases suivantes:

- **phase préalable**: phase où existent des indications que quelque chose pourrait ne pas fonctionner comme il convient. Dans cette phase, il faudrait être attentif et décréter l'état de préparation;
- **phase d'urgence**: phase où se produit la crise. Une situation d'urgence est toujours inattendue et se produit au mauvais moment, souvent en dehors des heures de travail ou au cours des week-ends. Comme chaque crise est différente, il est important que la prise en charge ne se fasse pas suivant une procédure de routine type quelconque, qui établisse toutes les mesures à prendre à l'encontre d'une menace précise. Il est important de savoir que la gestion des crises est une question de domination de la situation, et il est nécessaire de pouvoir improviser;
- **phase ultérieure**: phase où sont subies les conséquences, qui est essentielle si l'organisation s'apprête à résoudre la crise et à la surmonter. Cette phase consiste en plusieurs autres sous-phases telles que celle des premiers secours psychologiques, celle de la prise de mesures pour reprendre les activités, celle des enseignements tirés, etc.

2.2.2 Phases de la prise en charge des incidents

La prise en charge des incidents est fondée sur la phase d'urgence de la gestion des crises. Cette phase a été complétée par deux phases supplémentaires, la *phase de prise en charge* et la *phase de suivi* (voir Figure 4). Ces phases sont décrites ci-après.

Dans ce cas, on n'emploie pas les mêmes phases qu'au cours de la gestion des crises, parce que la phase préalable en ce qui la concerne comporte les phases de prise en charge des incidents comme un tout. Dans des circonstances normales, une prise en charge des incidents n'atteint pas le stade de la gestion de la crise. Si un incident doit être traité dans le cadre de la gestion des crises, cela signifie que cet incident a dégénéré en crise.

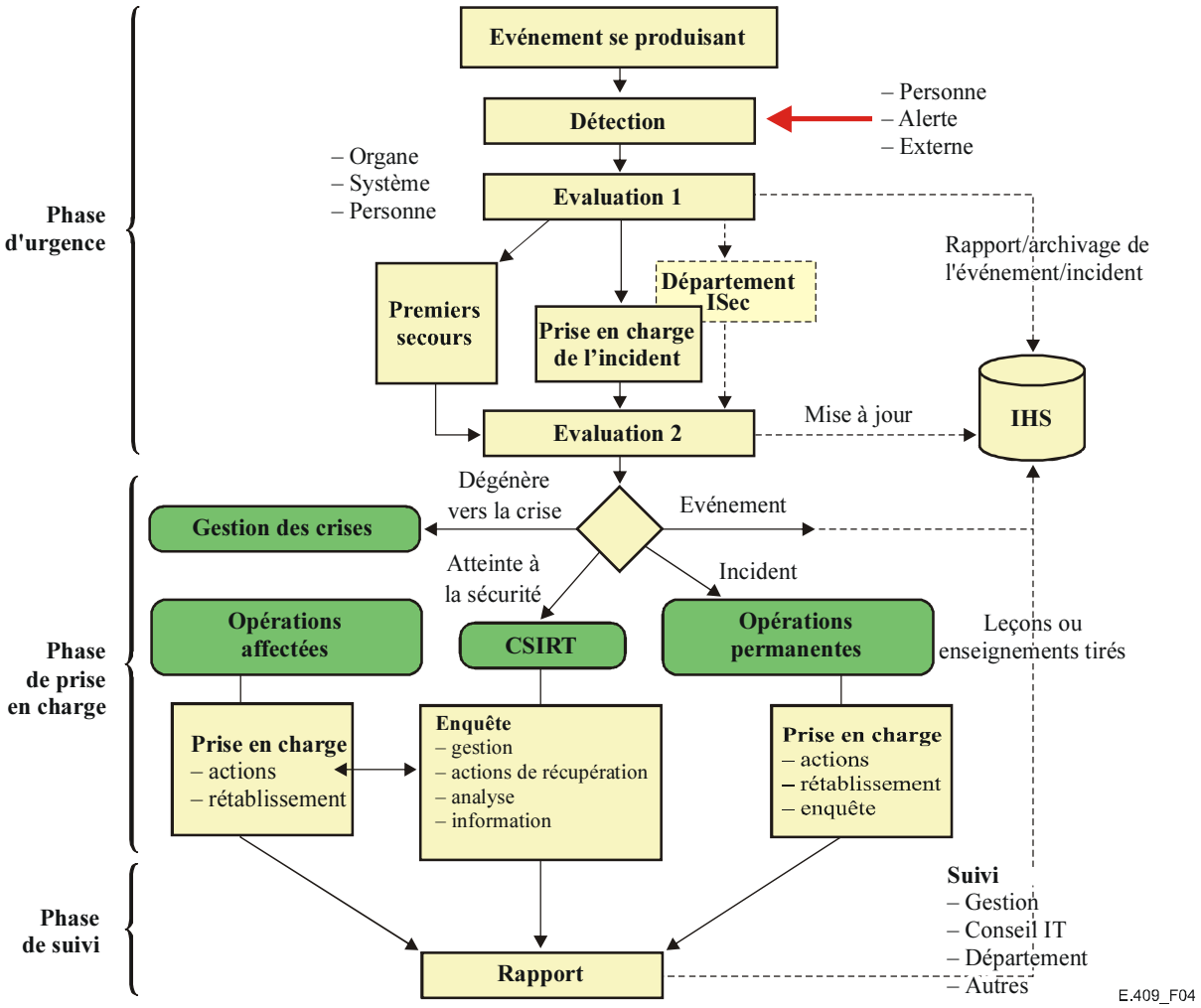

Figure 4/E.409 – Déroulement d'un incident

Le déroulement d'un incident est présenté ci-après dans ses différentes phases.

2.2.2.1 Phase d'urgence

Comme illustré sur la Figure 4, la phase d'urgence est la première phase. Cette phase peut être comparée avec la situation qui existe lors d'un accident de la circulation, où les premières mesures prises, souvent cruciales en termes de résultat final, ont en ce qui les concerne les conséquences les plus importantes. Les étapes de la phase d'urgence sont décrites dans l'ordre de leur application (voir Figure 5).

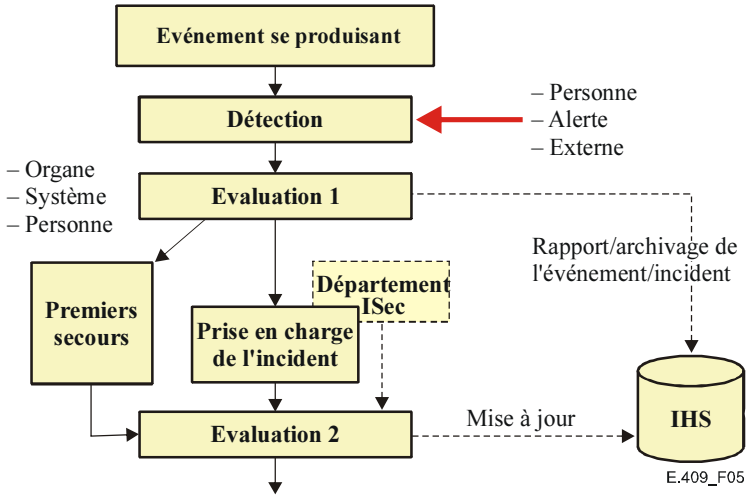

Figure 5/E.409 – Phase d'urgence

2.2.2.2 Détection

Une personne peut détecter un événement visuellement, c'est-à-dire en repérant les messages d'erreur, en lisant un fichier résultat ou au moyen d'un contrôle de vérification. La détection pourrait être visuelle lorsque l'opérateur observe quelqu'un qui fait une intrusion ou quelqu'un qui détecte un incendie. Un événement peut aussi être détecté par une personne qui a le sentiment que quelque chose ne se passe pas comme il faut, que quelque chose de douteux se passe.

Les alertes logiques sont celles qui appellent l'attention de l'utilisateur final, du personnel d'exploitation, des organes de sécurité, etc. Une telle alerte pourrait être une alerte déclenchée par le logiciel antivirus, le sous-système de vérification ou le système pare-feu et de détection de l'intrusion. Un événement pourrait aussi déclencher des alertes physiques telles que les alertes d'incendie, les alertes antivol, etc.

La détection est externe lorsque quelqu'un n'appartenant pas à l'organisation détecte l'événement. Dans le plus mauvais cas, cela pourrait figurer aux nouvelles ou être repéré par un reporter qui enquête sur les sources ou contacte l'organisation pour obtenir des commentaires au sujet d'un événement que l'organisation n'a pas encore détecté. Il se pourrait aussi que ce soient les autorités de la force publique qui avertissent le département de sécurité au cours d'une enquête sur une infraction ou un citoyen honnête qui découvre un trait peu plaisant sur le site Web de l'organisation de télécommunication.

Lorsqu'un événement est détecté, une évaluation initiale de la situation doit être faite afin de confirmer le classement et la gravité. Cela se fait en classant les événements selon leurs types. S'agit-il d'une atteinte à la sécurité, d'une crise ou simplement d'un événement? Après cela, on examine l'étendue et les conséquences. Ci-après est donnée une simple classification s'appliquant aux atteintes à la sécurité des réseaux ICN seulement, à employer pour déterminer la gravité d'un incident ou d'une atteinte à la sécurité.

Cette évaluation peut être faite par la personne détectant l'événement, qui pourrait aussi choisir de le signaler à un organe responsable, à savoir le service d'assistance ou de soutien ou le département de sécurité informatique. Lorsqu'un événement est signalé à un organe responsable, cet événement passe sous sa responsabilité. Les organes responsables qui sont en mesure de recevoir des rapports de détection sont aussi nommés points de contact (POC, *point-of-contact*) et ils sont chargés de prendre en main la situation. Une alerte est normalement automatiquement transférée vers la personne, l'organe ou le système responsable. Tous les événements signalés doivent être consignés dans un système de prise en charge des incidents (IHS, *incident handling system*).

Un point de contact est une unité ou une personne à laquelle on peut signaler un événement. Parfois, il s'agit d'un service d'assistance, de contrôle de la production ou un département de sécurité ou de sécurité informatique (ISec, *information security*). Un événement ne peut toutefois pas être signalé à l'équipe CSIRT, parce que c'est un groupe virtuel qui est constitué au moment où l'atteinte à la sécurité se produit. Une telle atteinte à la sécurité peut être signalée au département de sécurité informatique (ISec) qui a la charge de l'équipe CSIRT ou de tout autre point POC où une évaluation correcte sera faite et le contact sera établi avec les unités responsables.

- Classe 4 Très grave — Atteintes à la sécurité ayant des conséquences importantes pour l'organisation, par exemple attaques coordonnées, intrusions informatiques, vol d'informations sensibles et confidentielles, etc.

  Une atteinte à la sécurité de cette catégorie est synonyme de contre-mesures d'envergure et de dégâts importants.

- Classe 3 Grave — Atteintes à la sécurité ayant des conséquences pour l'organisation, par exemple, sabotages informatiques, fraude informatique, intégrité, abus ou révélation d'informations relatives à l'entreprise ou aux clients.

- Classe 2 Peu grave — Atteintes à la sécurité telles que tentatives, abus des ressources informatiques, etc.

  Une atteinte à la sécurité de cette catégorie est synonyme de moins de conséquences ainsi que de contre-mesures peu importantes et de faibles dégâts.

- Classe 1 Sans conséquences — Incidents pris en charge par l'organe permanent mais pouvant dégénérer en atteinte à la sécurité, par exemple, explorations, virus isolés, abus, attaques dirigées contre les systèmes de courrier, etc. Dans cette catégorie, on trouve habituellement les incidents qui affectent la production normale.

  Une atteinte à la sécurité de cette catégorie est synonyme de contre-mesures mineures ou n'étant pas prises et de faibles dégâts ou pas du tout de dégâts.

Un événement est habituellement signalé au service d'assistance, en particulier lorsque c'est un utilisateur final qui le détecte. Les utilisateurs finals signalent normalement tous les événements et toutes les erreurs au service d'assistance. Dans les autres cas, l'administrateur du système ou l'opérateur peut détecter l'événement. Les centres de contrôle opérationnels, chargés des communications, de la sécurité des systèmes et de la sécurité physique, pourraient aussi détecter les événements après avoir reçu des alertes en provenance des capteurs logiques et physiques ou des sources externes.

Il doit être donné à tous les organes et à toutes les unités, susceptibles de recevoir une alerte ou une indication de l'existence d'un événement, des instructions leur indiquant comment réagir. Cela doit permettre d'éviter que des événements ou des alertes ne soient négligés ou incorrectement pris en charge.

2.2.2.2.1 Evaluation 1

Cette évaluation est faite par une personne ou un organe (point POC) ou un système (système IDS). Dans la plupart des cas, la personne recevant l'alerte ou des informations relatives à un événement se charge de faire l'évaluation.

Un événement doit être identifié comme appartenant à l'une des catégories suivantes:

- crise;
- atteinte à la sécurité;
- incident;
- événement;
- fausse alerte.

Si un événement ne peut être classé dans une des catégories ci-dessus, il doit être classé comme incident et pris en charge par l'organe permanent, à savoir le service d'assistance ou de soutien. Certains événements n'entraînent aucune mesure parce qu'ils sont considérés comme étant des "erreurs de la part des utilisateurs" ou de mauvaises interprétations.

En outre, l'événement doit aussi être évalué en tenant compte de l'effet qu'il a sur l'organisation ou les activités. Le "niveau de gravité" est évalué selon les quatre niveaux suivants:

- très graves conséquences pour l'organisation de télécommunication;
- graves conséquences pour l'organisation de télécommunication;
- certaines conséquences pour l'organisation de télécommunication;
- pas de conséquences pour l'organisation de télécommunication.

Ces évaluations devraient être consignées dans le système de prise en charge des incidents (IHS).

Dans le cas d'incidents, d'atteintes à la sécurité ou de crises, les premiers secours doivent être apportés immédiatement. Cela comprend le rapport initial sur les dégâts, l'estimation des conséquences et une évaluation sur la question de savoir s'il existe des solutions rapides qui peuvent être appliquées pour limiter les dégâts. Cette évaluation est souvent effectuée par la personne ou l'organe recevant l'alerte ou la notification de l'événement.

En ce qui concerne les incidents, la personne ou le point POC informe les départements touchés et commence à prendre des mesures. Au vu de l'étendue et des conséquences, cela peut aussi vouloir dire qu'il est immédiatement fait appel à des experts. S'il s'agit d'un virus informatique qui a touché un département seulement, l'organe de soutien peut y remédier au moyen d'opérations types.

Au même moment, on *indique* au service d'assistance en quoi consiste l'événement, quelles mesures ont été prises et quand le retour à la normale des systèmes informatiques et de réseau se fait. Ceci permet d'informer ceux qui assurent le service d'assistance, puisqu'il leur incombe de recevoir les appels en provenance des utilisateurs finals touchés par l'incident. Ils peuvent leur faire savoir que l'aide est amorcée. Une autre raison, plus importante encore, est que si quelqu'un d'autre signale la même chose ou un incident semblable, le service d'assistance sait qui il doit avertir de cette nouvelle occurrence.

Toutefois, si un virus informatique s'est répandu, et touche plusieurs départements, des efforts coordonnés doivent être fournis pour limiter concrètement les dégâts et éliminer le virus.

Toutes les *enquêtes extérieures* doivent être adressées au département informatique.

Avant qu'une décision ne soit prise en ce qui concerne les mesures ou interventions suivantes, l'incident doit être communiqué à la personne le prenant en charge ou au département de sécurité informatique (ISec). La personne prenant l'incident en charge est la personne qui est responsable du département touché ou propriétaire du système touché. C'est la personne qui doit assumer la responsabilité des pertes et des frais.

Si plusieurs départements sont touchés, le département qui encourt les pertes ou les coûts les plus importants est celui qui est considéré comme étant le département qui prend l'incident en charge. Si l'incident affecte l'infrastructure de l'organisation de télécommunication, le département

correspondant est responsable. Si le département prenant l'incident en charge ne peut être déterminé, le département de sécurité informatique (ISec) est considéré comme étant celui-là.

Celui qui est chargé de l'incident a l'autorité en la matière et la responsabilité de le prendre en charge.

2.2.2.2.2 Evaluation 2

Cette évaluation est faite par la personne ou par le département de sécurité informatique qui prend l'incident en charge (ISec). Le département de sécurité informatique et l'équipe CSIRT ont les compétences nécessaires en matière de sécurité et de sécurité des réseaux ICN. Ils peuvent être consultés pour une évaluation de l'étendue des dommages et des conséquences.

Cette évaluation consiste en une vérification de l'évaluation précédente en ce qui concerne la classification de l'incident (à savoir, s'il s'agit d'un événement, d'un incident, d'une atteinte à la sécurité ou d'une crise). La personne qui prend l'incident en charge décide si l'incident a été correctement évalué ou si des corrections doivent être faites. Elle décide aussi de la poursuite de la prise en charge de l'incident, et de la question de savoir si un groupe de gestion de crise, une équipe CSIRT ou l'organe permanent se chargerait de l'incident et de l'enquête.

La décision d'informer le service de soutien ou d'assistance est prise par la personne qui prend l'incident en charge. Dans certains cas, il vaut mieux qu'elle soit retardée jusqu'à ce que la personne qui prend l'incident en charge et l'équipe d'intervention soient en place.

Lorsqu'il y a un doute concernant la question de savoir si l'incident peut être pris en charge par l'organe permanent, il faut prendre contact avec la personne de l'équipe CSIRT qui en a la charge. En cas d'atteinte à la sécurité, il faut contacter l'équipe CSIRT. S'il y a lieu, on peut contacter le département de sécurité informatique. Au cours de ces travaux, l'étendue de l'atteinte à la sécurité doit être déterminée et une évaluation mutuelle quant à la gestion de la crise sera prévue ou non.

L'enregistrement de l'incident constaté, consigné dans le système de prise en charge des incidents (IHS) est mis à jour. Même les événements qui ne portent pas à conséquence devraient être consignés. L'enregistrement de tous les événements a pour objet de déterminer si un événement isolé ou plusieurs événements sont éventuellement liés à d'autres événements, à d'autres incidents ou à d'autres atteintes à la sécurité, même si à ce moment ce n'est pas évident. Si une atteinte à la sécurité a lieu, la relation entre ces événements et l'atteinte à la sécurité peut devenir évidente.

Après cette phase, l'atteinte à la sécurité entre dans une phase de prise en charge.

2.2.2.2.3 Phase de prise en charge

Au cours de la phase de prise en charge, l'événement est réellement pris en charge. Cet événement peut être un incident, une atteinte à la sécurité ou une crise. Lorsqu'il entre dans cette phase, il a le statut "d'officiel" et devrait être pris en charge comme suit.

Pendant la **crise** ou lorsque la situation **dégénère** vers la crise, l'équipe de gestion de la crise se déplace et reprend la prise en charge, conformément à des procédures de routine bien établies. Les mesures qui sont prises suivent aussi des procédures de routine bien établies et conduisent à la création d'un groupe de gestion de crise. La gestion de la crise et la prise en charge de celle-ci sortent du cadre de la présente Recommandation.

Un **incident** est pris en charge par l'organe permanent de l'organisation de télécommunication, à savoir un service de contrôle de la production, de soutien, de sécurité et de surveillance, etc. Un incident pourrait consister en la présence d'erreurs ou de perturbations, de visiteurs "libres", etc. L'organe permanent prend les incidents en charge en assurant les tâches suivantes:

- prise de mesures pour contrecarrer la cause et amortir les effets de l'incident et éviter qu'il se reproduise;
- récupération afin de reprendre les activités;

- enquête sur la cause de l'incident et ses conséquences et détail des mesures prises.

Il est suggéré que les incidents concernant la production soient pris en charge par l'unité de soutien de la production et son organe établi pour ce genre d'événements.

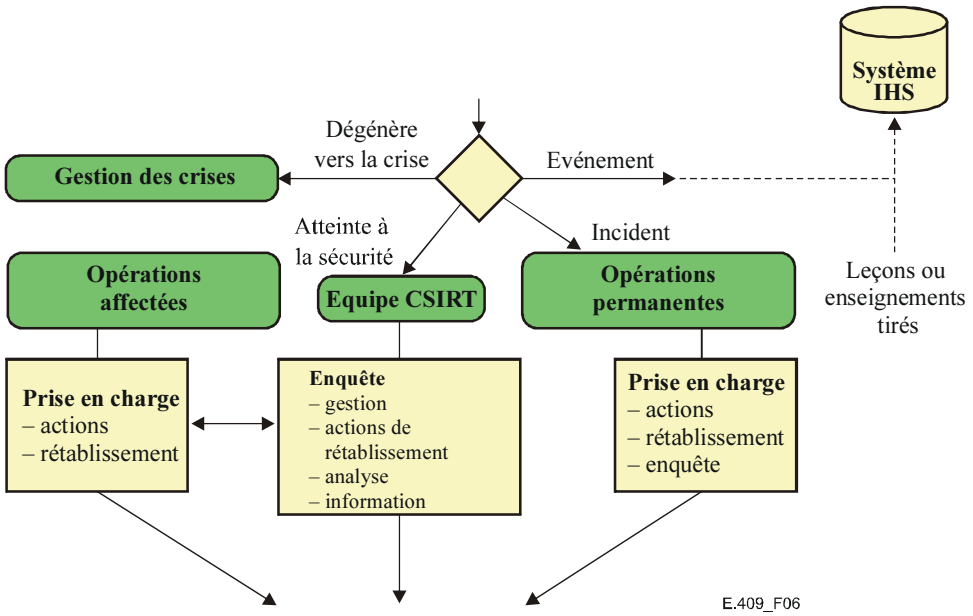

Figure 6/E.409 – Phase de prise en charge

Lorsqu'une **atteinte à la sécurité** entre dans sa phase de prise en charge, celle-ci s'effectue suivant des procédures de routine bien établies.

La personne qui prend l'incident en charge, en accord avec le département de sécurité informatique (ISec), crée et met sur pied une équipe d'intervention en cas d'incident, qui est virtuelle et temporaire, l'équipe CSIRT. Un chef d'équipe est aussi choisi. Il peut être toute personne issue des unités de soutien, de surveillance ou du département de sécurité informatique (ISec) touchés. L'équipe d'intervention en cas d'incident, l'équipe CSIRT, est constituée de personnes appropriées et des compétences requises.

L'équipe CSIRT enquête sur l'atteinte à la sécurité, ce qui veut dire qu'elle assume les tâches suivantes:

- gestion et exécution des travaux d'enquête;
- prise de mesures pour arrêter et limiter les conséquences de l'atteinte à la sécurité (endiguement). Cela se fait de concert avec le département touché. Normalement, l'équipe CSIRT joue le rôle de l'unité de soutien;
- rétablissement afin de reprendre les activités de télécommunication. Cela se fait de concert avec le département touché. Normalement, l'équipe CSIRT est l'équipe de soutien;
- analyse des circonstances et des causes de l'incident, de ses conséquences et exposé des mesures prises et des coûts;
- information des parties concernées, à savoir le service d'assistance ou de soutien, etc.

Ces procédures peuvent être beaucoup plus détaillées que celles qui sont présentées ici et qui peuvent être employées en tant que lignes directrices.

La procédure de routine consiste en trois étapes différentes:

1) identification du type d'incident, de son étendue et de ses conséquences;
2) endiguement, à savoir arrêt des occurrences et limitation des conséquences de l'atteinte à la sécurité;
3) éradication de la cause et empêchement d'une nouvelle occurrence;
4) reprise des activités normales;
5) suivi.

Lorsque l'équipe CSIRT est constituée, "l'identification" est une procédure type de la mise au courant de ses membres. Ils sont aussi informés de l'atteinte à la sécurité, de l'état actuel de la situation, des mesures prises et des précautions à prendre, etc.

2.2.2.2.4 Phase de suivi

Dans la phase de suivi, la crise, l'atteinte à la sécurité ou l'incident a été résolu et les conséquences ont été réduites à un minimum. Il reste à évaluer l'événement et sa prise en charge, à en faire le rapport à la direction, au département de sécurité informatique, au service de contrôle de la production, etc.

Le rapport de suivi devrait décrire la détection de l'incident, les temps écoulés entre la détection et la réaction (les mesures prises), les mesures effectuées et l'efficacité et les résultats. Il devrait aussi indiquer les points faibles observés dans l'environnement initial (du réseau ICN), les insuffisances dans les procédures de prise en charge et les procédures. Tout ceci devrait être consigné dans un fichier leçons ou enseignements tirés, qui peut être employé pour éviter de refaire à nouveau les mêmes erreurs. Tant les coûts directs qu'indirects devraient être estimés.

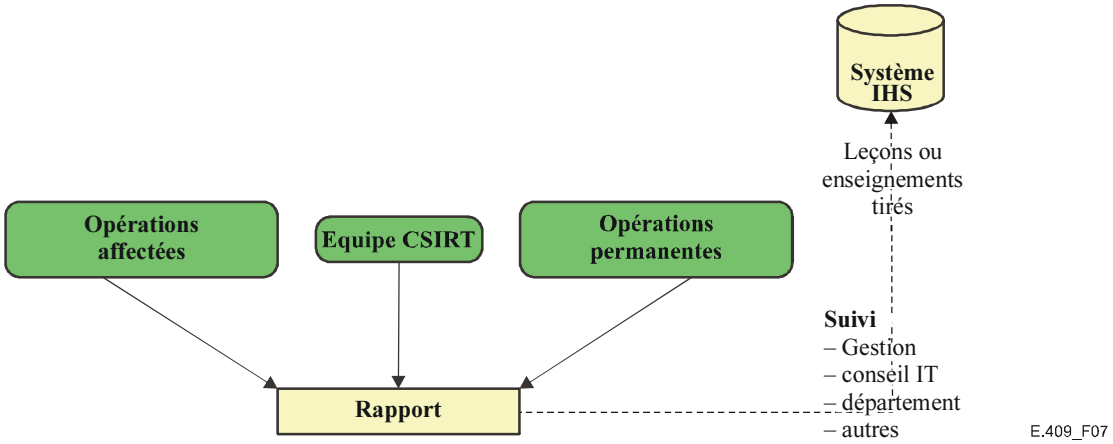

Figure 7/E.409 – Phase de suivi

Au cours de cette phase, l'achèvement de l'enregistrement de l'incident constaté se fait dans le système IHS. Il convient d'établir un fichier contenant les leçons et les enseignements tirés afin de rappeler ce qui s'est passé pendant les phases d'urgence, de prise en charge et de suivi.

3 Système de prise en charge des incidents

Il est essentiel de disposer d'un système de prise en charge des incidents qui garde la trace de chaque événement, incident, atteinte à la sécurité et crise détectés et rapportés. En examinant ces fichiers, il est possible de se rendre compte des types d'événements qui sont les plus courants, du motif de leur apparition, de la manière dont ils sont détectés, de leur étendue, de leurs conséquences et de leur coût. Un aspect important est l'enregistrement des événements qui ne sont pas des

incidents, des atteintes à la sécurité ou des crises. Bien que ces événements puissent ne pas constituer de menace, en tant qu'événement isolé, à plusieurs ils peuvent nous donner quelques indications sur les motifs de leur apparition. Ils pourraient contribuer à nous montrer les relations qui existent avec les atteintes à la sécurité dirigées contre l'organisation. Ce sont les incidents peu importants qui, pris isolément, peuvent ressembler à une demande incorrecte sur le réseau, mais qui, considérés dans leur ensemble, indiquent des explorations en profondeur du réseau des organisations de télécommunication, notamment du réseau et des systèmes informatiques.

BIBLIOGRAPHIE

– Extraits de la thèse de Master sur Incident Organization and Security Incident Handling, Jimmy Arvidsson, FIINA, 2001.

– CERT/CC (URL: http://www.cert.org) 2000-09-26.

– Federal Incident Response Capability (URL: http://www.fedcirc.llnl.gov) 2000-05-20.

– Internet Security Glossary; R. Shirey, GTE/BBN Technologies, May 2000.

– Informationssäkerhetshandbok, del 5 – Katastrofskydd för IT-verksamhet, v.2, Jan-Olof Andersson, JOA InfoSäk, 1999.

– Handbook for Computer Security Incident Response Teams (CSIRTs); Moira J. West-Brown, Dan Stikvoort, Klaus-Peter Kossakowski; Carnegie Mellons, Software Engineering Institute, 1998.

– Computer Security Incident Handling – Step by step, SANS Institute, NSWC, 1998.

– Intrusion Detection, Edward Amoroso, Intrusion.Net Books, 1998.

– Best Current Practice; Expectations for Computer Security Incident Response; N. Brownlee, The University of Auckland, E. Guttman, Sun Microsystems, June 1998.

– Computer Security Incident Handling Procedure, NSWC Dahlgren, October 1996.

– Computer Crime: A Crimefighter's Handbook, David Icove, Karl Seger and William – VonStorch, O'Reilly & Associates, 1995.

– An Analysis of Security Incidents On The Internet, 1989-1995, John Howard, CERT/CC (URL: http://www.cert.org/research/JHThesis/Start.html) 2000-05-20.

– Establishing a Computer Security Incident Response Capability (CSIRC), NIST, November 1991.

– "The Oxford Reference Dictionary"; Oxford University Press, 1986.

– A Common Language for Computer Security Incidents; John D. Howard and Thomas A. Longstaff; Sandia National Laboratories [Sandia Report: SAND98-8667].

– Intrusion Detection – Network Security Beyond The Firewall, Terry Escamilla.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	**Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains**
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2004