Réagir : De l'incident de sécurité à la crise

Eric DUPUIS[1,2*]

Résumé
Ce document donne les grands principes de la gestion des incidents, et la conduite de gestion de crise.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document finale unique.
Ce document ne constitue pas à lui seul le référentiel du cours. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique.

Mots clefs
Incidents, forensic, crise

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *RSSI Orange Cyberdefense*
***email** : eric.dupuis@cnam.fr – eric.dupuis@orange.com

1. Réagir

1.1 de l'alerte à l'incident

1.1.1 de l'alerte à l'incident

Comme nous avons vu dans le chapitre sur la détection des attaques certains événements peuvent conduire à des alertes. Ces alertes doivent être analysé par les ingénieurs spécialistes analystes SOC pour caractériser si un événement passé à un niveau d'alerte doit être traité comme un incident de sécurité. L'alerte positionne les équipes dans un état de vigilance toutefois l'enregistrement d'un événement en incident engage les processus de réponse à incident.

1.1.2 L'incident

La problématique de la réaction à un incident dit "cyber" c'est à dire un incident qui peut mettre en doute la confiance que l'on peut avoir dans son propre système système d'information, est de l'usage du SI lui même pour opérer la

réaction. Dans un premier dans nous allons donc partir de principe que le système d'information dispose de mécanisme permettant d'avoir confiance dans les systèmes qui opèrent pendant la réponse à incident. Nous allons aborder la réaction à incident suivant les 3 volets :

- Remédier et reconfigurer pour limiter l'impact ;
- Enquêter sur l'incident ;
- Neutraliser les sources de menaces ;

Néanmoins avant de s'engager dans la descriptions des activités liées à la réponse à incident cybersécurité, je souhaitais évoquer les bonnes pratiques ITIL qui donnent des pistes sur l'organisation de la gestion d'incident. Il ne faut en effet pas considérer la réponse à attaque comme une activité que technique bien que l'urgence nécessite le plus souvent de passer outre les processus classiques de traçabilité.

1.2 L'integration dans la gestion des incidents 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 ») du management du système d'information.

La Gestion des incidents vue du côté d'ITIL inclut tout événement qui perturbe, ou pourrait perturber, un service. Ceci inclut les événements communiqués directement par les utilisateurs, via le Centre de services, une interface web ou autrement. Ce processus appartient au sens ITIL à l'étape Service Operation(SO) du cycle de vie d'un SI.

Même si les incidents et les demandes de service sont rapportés au Centre de services, cela ne veut pas dire qu'ils sont de même type. Les demandes de service ne représentent pas une perturbation de service comme le sont les incidents. Voir le processus Exécution des requêtes pour plus d'information sur le processus qui gère le cycle de vie

Les objectifs du processus de Gestion des incidents sont :

- Veiller à ce que des méthodes et des procédures normalisées soient utilisées pour répondre, analyser, documenter, gérer et suivre efficacement les incidents.
- Augmenter la visibilité et la communication des incidents à l'entreprise et aux groupes de soutien du SI.
- Améliorer la perception des utilisateurs par rapport aux TI via une approche professionnelle dans la communication et la résolution rapide des incidents lorsqu'ils se produisent.

- Harmoniser les activités et les priorités de gestion des incidents avec ceux de l'entreprise.
- Maintenir la satisfaction de l'utilisateur avec la qualité des services du SI.

Généralement, cette gestion d'incident s'inscrit dans une chaine d'outillage avec des processus permettant de définir l'état ou le statut de l'incident.

- **Nouveau** : un incident est soumis, mais n'a pas été assigné à un groupe ou une ressource pour résolution.
- **Assigné** : un incident est assigné à un groupe ou une ressource pour résolution.
- **En traitement** : l'incident est en cours d'investigation pour résolution.
- **Résolu** : une résolution a été mise en place.
- **Fermé** : la résolution a été confirmée par l'utilisateur comme quoi le service normal est rétabli.

On ne peut toutefois pas oublier, que la gestion de la sécurité dans une entreprise mature, doit s'intégrer aux processus IT de l'entreprise et de remarquer que certaines activités de sécurité peuvent aussi s'intégrer dans un respect du référentiel ITIL.

- Le centre de services (service desk) cf le niveau 1 d'un « Security Operation Center » ;
- La gestion des incidents (incident management) ;
- La gestion des problèmes (problem management) ;
- La gestion des changements (change management) voir les mécanismes de couverture de vulnérabilités (patch management par exemple) ;
- La gestion des mises en production (release management) ;
- La gestion des configurations (configuration management).

Dans ces processus le cycle de vie de l'incident suis un cycle connu et reconnu :

- **Identification** : détecter ou rendre compte d'un incident ;
- **Enregistrement** : les incidents sont enregistrés dans le système de gestion des incidents ;
- **Classement** : les incidents sont classés par priorité ;
- **Priorisation** : l'incident est classé par ordre de priorité, sur la base de son impact et de son urgence, pour une meilleure utilisation des ressources et du temps disponible par l'équipe de support ;

- **Escalade** : l'équipe de support doit-elle obtenir de l'aide de la part d'un autre service ? Si oui, on engage une procédure de demande de service sinon, la résolution de l'incident s'effectue au niveau du support initial.
- **Diagnostic** : révélation du symptôme complet de l'incident ;
- **Résolution et rétablissement** : une fois que la solution est trouvée et que la correction est apportée alors l'incident est résolu ; La solution peut alors être ajoutée à la base des erreurs connues dans l'optique de résoudre plus rapidement un incident similaire dans le futur.
- **Clôture de l'incident** : l'enregistrement de l'incident dans le système de gestion du management est clôturé en appliquant le statut « terminé » à celui-ci.

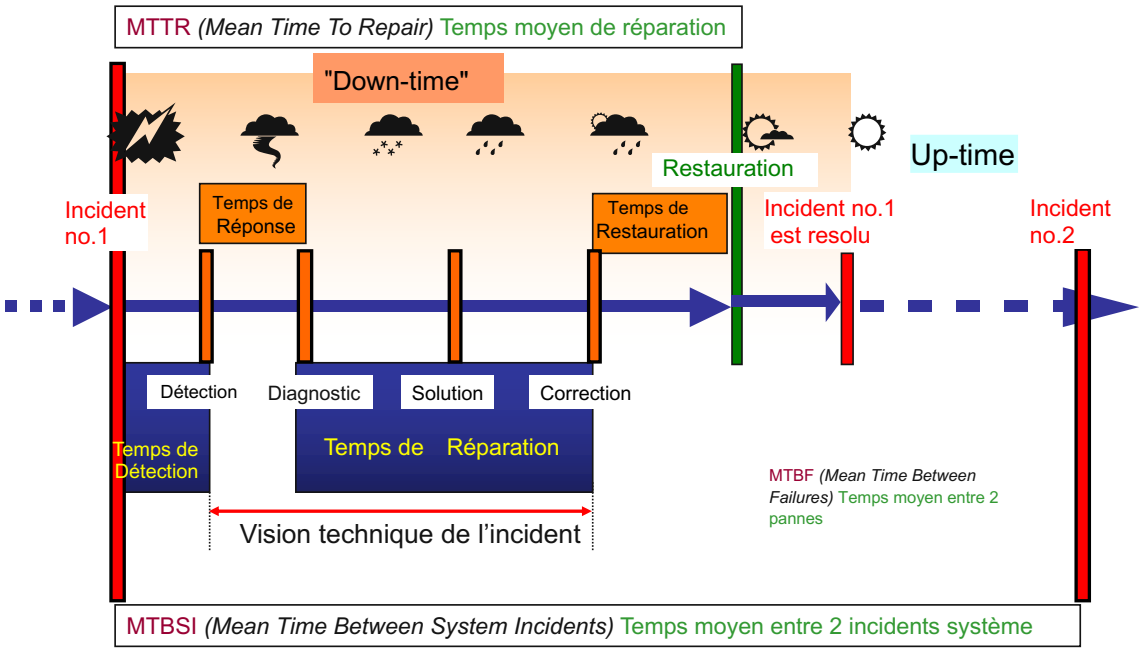

FIGURE 1. Incidents

1.3 Threats Hunting

Mettre place une interaction entre l'attaque et la défense, pour provoquer une continuité de l'attaque avec des objectifs qui peuvent aller du maintien de l'attaque pour découvrir les scénarios

Exemple se mettre en proxy et modifier les fichiers ex-filtrées pour les corrompre et faire en sort que l'attaquant reste plus longtemps. Réagir, gestion de crise, à quel moment géré t'on la crise.

FIGURE 2. Incidents

1.4 HoneyPots

1.5 Haqckback

ceci est un texte

2. de l'alerte à l'incident

`

3. de l'incident à la crise

3.1 PCA/PRA et PCI/PRI

3.2 se préparer et s'entrainer

4. Remédiation

Une question qui se pose lors d'une reprise d'activité est la confiance que nous avons dans le système. La difficultés après une attaque informatique ou une compromission, ou tout simplement une suspicion c'est la simple question de savoir si nous savons enlever toute la source de l'attaque. Reste-t-il des résidus.

5. Aspect juridique de la réaction

`

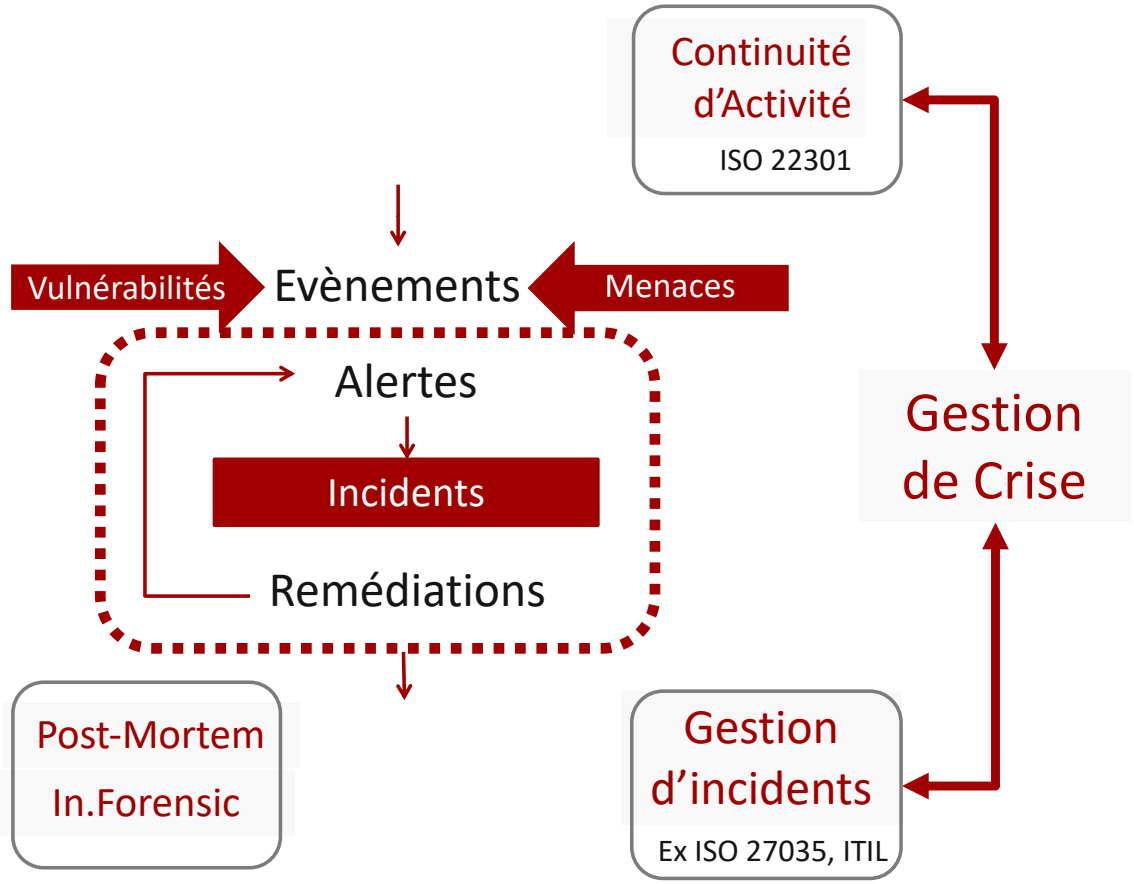

FIGURE 3. Incidents

5.1 hackback

6. Forensic

7. CERT et CSIRT

7.1 un peu d'histoire

un peu d'histoire, dans les années 80, au coeur du réseau IP les plus célèbre ARPANET, un étudiant de CORNELL UNIVERSITY implanta, sur le réseau, un ver qui se propageait, se répliquait et exploitait les failles de sécurité UNIX de l'époque. Afin d'exterminer ce ver internet, une équipe d'analyse, en compagnie d'experts MIT, a été créée pour identifier et corriger les failles d'une part, et d'autre part développer des solutions d'éradication. A la suite de cet incident, le DARPA (Defense Advanced Research Projects Agency), maitrise d'ouvrage d'ARPANET, décida la mise en place d'une structure dédiée, le CERT coordination Center,

pour résoudre tous types d'incidents sécurité. Le terme CERT est le plus utilisé et le plus connu mais il s'agit d'une marque américaine qui appartient à l'université Carnegie Mellon. Les CSIRT peuvent demander l'autorisation d'utiliser le nom de « CERT ». Aujourd'hui, environ 80 CSIRT sont affiliés et autorisés à utiliser cette marque CERT.

Ces CSIRTs peuvent être internes à l'entreprise ou externes de type publique ou commercial.

Dans bien des entreprise, il y a des moments où il est indispensable de faire intervenir des équipes experts externes généralement nécessaires pour faire face à une crise évoluant rapidement. Ces équipes fournissent une assistance d'expertise en fonction de l'étendue et de la gravité de l'incident et de la charge nécessaire à sa remédiation.

Ces équipes de type CSIRT peuvent rapidement apporter les ressources et l'expertise adapté au contexte de l'incident.

Mais il y a beaucoup à faire par retirer tous les bénéfices de ce type de services. Et cela commence par une compréhension claire de la manière dont fonctionne le processus de réponse aux incidents, et ce que l'on attend d'une équipe externe dans une telle situation.

7.2 Les missions d'un CSIRT,

Les missions d'un CSIRT sont nombreuses, mais il est intéressants de prendre les 5 principales définies par le CERTA (CERT de l'Administration Française).

- Centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations : réception des demandes, analyse des symptômes et éventuelle corrélation des incidents ;
- Traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CSIRT, contribution à des études techniques spécifiques ;
- Etablissement et maintenance d'une base de données des vulnérabilités ;
- Prévention par diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou au pire leurs conséquences ;
- Coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CSIRT nationaux et internationaux.

7.3 Phase d'analyse

La première chose à laquelle souhaite accéder un CSIRT est un présentation de situation la plus clair et concise que possible.

Les organisations qui sont la cible d'une attaque par logiciel malveillant à plusieurs couches, ou d'une intrusion réseau, n'ont souvent pas une idée complète de l'origine ou de l'étendue du problème. Pourtant, il est vital de pouvoir fournir autant de détails que possible. « Normalement, lorsqu'un client entre en contact avec un spécialiste de la réponse à incident, la première chose que l'on veut savoir, est ce qui est en train de se passer », relève ainsi Bob Shaker, directeur des opérations stratégiques, préparation cyber et réponse, chez Symantec.

Un spécialiste de la réponse à incident va vouloir des informations sur ce qui conduit son client à penser qu'il a été compromis, quand et comment il l'a découvert, et encore s'il l'a fait grâce à une source interne ou externe, des autorités locales, par exemple, ou encore un émetteur de cartes bancaires.

Durant la phase d'établissement de l'étendue du problème, il est vital de disposer de personnes internes à l'organisation sachant quelles informations il est possible de fournir au prestataire, qu'il s'agisse de journaux d'activité ou de tout autre élément de preuve, explique Jim Aldridge, directeur de l'activité de conseil et Mandiant, l'unité de réponse aux incidents de FireEye.

Le prestataire va utiliser l'information qui lui est fournie pour évaluer l'étendue des dégâts et déterminer le type de ressources – y compris les experts à dépêcher sur place – nécessaires. « Lorsqu'une organisation contacte un prestataire de services de réponse à incident, il faut engager une discussion sur l'étendue du problème pour s'assurer que le prestataire comprend la situation sur laquelle il va intervenir », relève Aldridge.

La phase de contractualisation

Une fois que le prestataire a eu l'opportunité d'évaluer la situation, il pourra fournir une estimation de ce dont il aura besoin pour son intervention. Le contrat proposer doit généralement contenir des explications détaillées des services qui seront apportés, précisant au passage s'il aidera effectivement à remédier à l'incident, ou s'il ne fera que fournir les informations permettant à son client d'assurer seul la remédiation.

Dans cette phase, il est important de bien comprendre quelle documentation, accès et savoirs seront nécessaires au prestataire. Christopher Pierson, RSSI de Viewpost, une plateforme de paiement en ligne, estime qu'il est « crucial de s'assurer que les bonnes ressources seront fournies ». Les entreprises utilisant des applications et des services en mode Cloud sont parfois limitées dans le choix des tiers d'investigation qu'elles peuvent solliciter. Il est donc important d'examiner ces points avant de signer le contrat.

En outre, il est vital d'identifier les compétences que peut apporter le prestataire, ainsi que ses ressources technologiques, ses outils ou encore ses renseignements sur les menaces.

Signer pour un engagement de longue durée avec un prestataire, avant le premier incident, peut s'avérer profitable : ainsi, il n'est pas nécessaire de consacrer un temps critique en plein incident aux détails du processus de contractualisation, ou d'expliquer ses processus internes de réponse aux incident au milieu d'une crise. De fait, souligne Bob Shaker, « en pleine crise, la personne susceptible de signer un contrat est généralement sur le pont au centre de crise ». Réussir à l'en extraire peut s'avérer difficile. . .

Enquêter sur l'incident

Le CSIRT aura besoin de toute l'information possible : logs systèmes et réseau, diagrammes de topologie réseau, images systèmes, rapports d'analyse du trafic réseau, etc.

Souvent, il est tentant de céder à la panique et d'arrêter les systèmes dans la précipitation. Mais pour Shaker, c'est une mauvaise idée : « la première chose importante est de ne pas éteindre les systèmes. Une fois qu'un système est éteint, une quantité considérable d'éléments de preuve peuvent être effacés, en particulier tout ce qui réside en mémoire vive ».

Les équipes d'investigation utilisent les informations fournies par les entreprises clients, ainsi que celles qu'elles collectent elles-mêmes sur leurs points de terminaison et d'autres sources, via des outils propriétaires, pour identifier des indicateurs de compromission, relève Kevin Strickland, consultant réponse à incident sénior chez Dell SecureWorks.

C'est après cela que le prestataire est généralement en mesure d'informer son client sur ce qui s'est passé, sur la manière dont l'intrusion est susceptible d'avoir commencé, ou comment le logiciel malveillant a été introduit sur le réseau, et sur quoi faire pour contenir l'incident : « nous allons fournir cette information et indiquer où des actions sont requises », explique Stickland. Et si les options recommandées sont difficiles à mettre en œuvre, il peut y avoir alors quelques aller-retour.

Contrôle et remédiation

L'équipe responsable de la remédiation travaille souvent en tandem avec l'équipe chargée de l'investigation, selon Aldridge. « Nous avons deux flux de travail. Le premier est lié à l'enquête et vise à identifier quels systèmes, comptes et données ont été compromis ; le second touche à la remédiation ». Et dès que la première équipe trouve des éléments relatifs à l'incident, elle les transmet à la seconde qui travaille avec le client à la mise en œuvre des mesures correctrices.

Mais discrétion peut s'avérer essentielle. Pour Strickland, il n'est pas question de laisser les attaquants savoir que l'on est sur leurs traces : « il est très important de comprendre ce qui se passe avant d'effectuer des changements drastiques ».

7.4 Création de son équipe CSIRT

Quelles sont les motivations pour créer un CSIRT dans son entreprise :

- Une augmentation exponentielle du nombre d'incidents sécurité
- Une augmentation du nombre et type d'organisations affectées par des incidents sécurité
- Un focus de la part des entreprises sur le besoin de politiques sécurité dans le cadre de leur management du risque
- Nouvelles lois et régulations impactant les entreprises en terme de protection des données
- Réaliser que les administrateurs systèmes et réseaux ne peuvent pas protéger l'entreprise à eux seuls

Un CSIRT est composé de plusieurs experts dans différents domaines de la sécurité (intrusions, forensics, malwares, crytpo, etc..) qui préviennent mais surtout réagissent en cas d'incident. Ces experts sont en constante mise à jour des nouveaux vecteurs d'attaques (nouveaux malwares, nouvelles vulnérabilités), tout ceci afin de traiter les incidents de la manière la plus aboutie qui soit. Une véritable équipe CSIRT dans une entreprise à un coût non négligeable, il convient d'en étudier les modalités de de fonctionnement et de couverture.

Création d'un CSIRT

La création d'un CSIRT dans son entreprise, n'est pas chose facile, c'est un vrai sujet de RSSI dans le sens ou des choix sont a faire tant sur les compétences, les moyens, les procédures de travail. C'est un vrai sujet de mémoire pour la fiche techno.

8. Gestion de crises

9. Contributions

9.1 Comment contribuer

Les notes et les présentations sont réalisées sous LaTeX.

Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBERDEF101). Les contributions peuvent se faire sous deux formes :

- Corriger, amender, améliorer les notes publiées. Chaque semestre et année des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF) [1] . Le fichier Tex/Contribute/Contribs.tex contient la liste des personnes ayant contribué à ces notes.
Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les détails de contributions.

9.2 Les contributeurs/auteurs du cours

Les auteurs des contributions sont :

9.2.1 Années 2019

- **François REGIS** (Orange) : CyberHunting

9.2.2 Années 2018

- **Julia HEINZ** (Tyvazoo.com) : ISO dans la gouvernance de la cybersécurité

1. https://github.com/edufaction/CYBERDEF

Table des matières

Table des figures