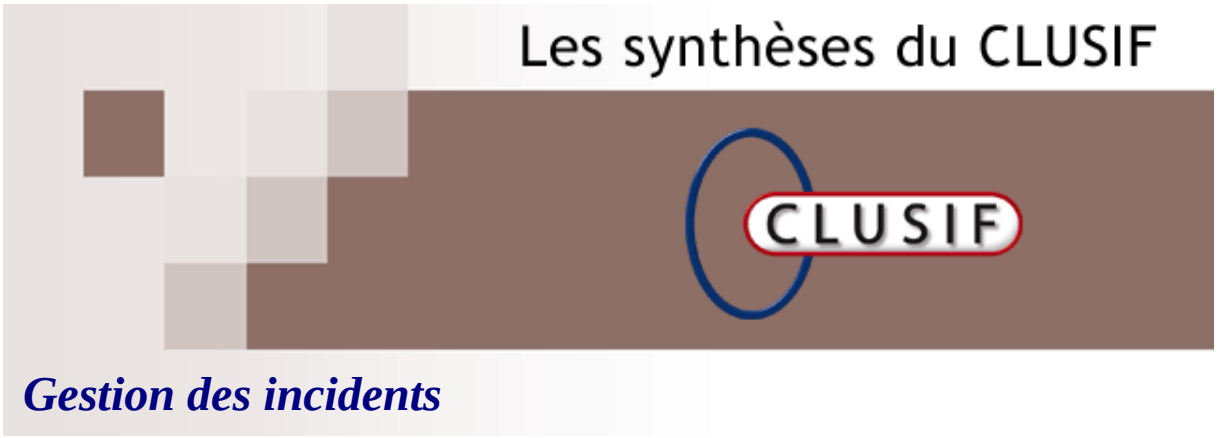

Gestion des incidents

Synthèse de la conférence thématique du CLUSIF du 16 juin 2011 à Paris

David Maillard, Alcatel Lucent.

David Maillard rappelle que les activités de sécurité, au sein d'Alcatel Lucent, ont démarré au début des années quatre vingt-dix au travers d'un partenariat avec le CNES qui s'ouvrait à Internet. Cela a continué avec France Telecom et Météo France sur des activités de type tests d'intrusion et enfin avec la création du premier CERT indépendant français : le CERT IST à destination de l'Industrie, des Services et du Tertiaire. Au cours des dernières années l'activité sécurité a connu une forte progression.

Au niveau mondial, La Business Unit « Sécurité » représente quatre vingt (80) personnes. Elle travaille au développement de l'offre, au portfolio, au support de l'avant vente et au lancement local des prestations. Elle s'appuie sur des compétences locales pour la partie commerciale et le support après vente.

Le métier de la supervision de sécurité selon le TMC (Transportation Management Center) consiste en :

- la collecte et l'analyse des journaux de façon à détecter les intrusions sur les équipements de sécurité mais aussi sur les équipements terminaux,
- l'archivage à des vues de rejeu d'incidents ou pour opposer une preuve sachant qu'aujourd'hui la plupart des SIEM font du scellement de traces.,
- La détection des attaques,
- La garantie de la traçabilité et de l'imputabilité des actions.

Le centre de supervision dispose d'une équipe de premier niveau capable de répondre à une activité mondiale en fonctionnant 24h/24 et 7j/7 et d'instruire, au moins en préliminaire, un certain nombre d'incidents de sécurité. Une équipe de second niveau fait de la veille technologique et effectue un travail d'investigation autour de l'incident de sécurité. Enfin, un troisième niveau ou niveau de support, plus transverse, est capable de contextualiser l'incident dans un environnement client ou dans un environnement matériel.

« L'architecture type » de collecte et de traitement dans l'environnement Alcatel Lucent comprend pour chaque environnement client un site actif et un site passif, dans lequel on trouve :

- la notion de collecte dans les environnements Syslog, Windows ou SQL, en bref tout ce qui va générer des traces (y compris celles de type applicatif),
- des outillages de concentration qui permettent de collecter des traces, de les centraliser et de les ré-aiguiller, vers des collecteurs, sous forme de flux sécurisés et horodatés. Ces

derniers se trouvent dans un environnement infogéré et dédié à chaque client. Ces traces sont ensuite injectées dans l'infrastructure mutualisée - TMC - en vue d'une corrélation permettant de récupérer et détecter les incidents.

L'architecture logique intègre :

- l'environnement client et les autres serveurs qui envoient leurs journaux vers des collecteurs d'évènements,
- les secteurs applicatifs et les applications métier,
- tout ce qui est équipement réseau que ce soit des équipements de maillage ou des équipements de sécurité.

Un pré traitement est entrepris sur chaque évènement dans le SIEM pour faire une taxonomie et un parsing. Il s'agit de les reformater au standard du SIEM afin d'établir des statistiques. Ils sont ensuite injectés :

- dans une base de données à des fins d'archivage,
- puis dans une base de corrélation dont les règles permettent de faire de la gestion d'incidents sur seuil ou de faire remonter une alerte.

Enfin une exécution de scripts transpose ce ticket d'incident SIEM en ticket d'incident dans un outil ITIL qui permet d'interagir avec le client de manière normalisée. Ces informations contenues dans des bases ITIL sont, à leur tour, réinjectées pour archivage et consolidation dans les bases de données.

Un dernier environnement « tiers » re-travaille les données de la base et les propose en mode asynchrone, autorisant ainsi les différentes entités de l'entreprise à recueillir celles qui lui sont pertinentes, soit sous forme de reporting soit sous forme de flux, de traces, ou d'incidents.

Le TMS regroupe la supervision de sécurité chez Alcatel Lucent. Cela représente un peu moins de 2 500 équipements supervisés pour 14 clients et 5 milliards d'enregistrements de traces par jour. L'outil d'agrégation et de corrélation génère en moyenne une cinquantaine d'alertes par jour réparties sur les 14 clients. Un prétraitement réalisé par l'équipe de premier niveau permet d'évacuer un certain nombre de faux positifs. En moyenne, 5 alertes par jour sont transmises au second niveau. Enfin, le rejeu des évènements permet de mener des investigations sur les situations à risque du client.

Les indicateurs de sécurité sont classifiés en trois familles de type « métrologique », « pertinence » et « tendanciel ».

Les indicateurs de type « Métrologie Sécurité » sont basés sur de la volumétrie : par exemple une croissance des règles journalisées est constatée et permet d'identifier une augmentation du volume d'activités qui peut-être significative d'une tentative d'attaque.

Les indicateurs de type « Pertinence » utilisent des outils automatisés pour prendre en compte l'intégralité de l'environnement qui se trouve autour de l'équipement supervisé (notions de matrice de flux, de comportements…). A titre d'exemple il détecte deux firewalls logiquement dissociés qui remontent deux tentatives de connections simultanées avec le même UID venant d'un environnement géographique différent.

Les indicateurs de type « veille tendancielle » permettent de faire du « early warning » sur un certain nombre de vulnérabilités ou de comportements réseaux. Un exemple : un ver qui se propage par le port 80 avec une augmentation significative de paquets ou des signatures de comportement type click jacking sur Facebook.

Le CERT fait de la veille technologique autour des vulnérabilités mais il fait aussi de la gestion d'incident. Veiller que le CERT soit référencé dans un organisme mondial permet une coordination avec d'autres CERT.

Quelques exemples d'incident de sécurité :

1) Glissement des usages d'un opérateur : des clients souhaitent valider des comportements de TMA ou de tiers mainteneurs ou de tiers administrateurs. Ce sont des entreprises qui externalisent cette activité. Il s'agit de transposer les engagements contractuels pris dans le cadre du PAQ sous forme d'éléments techniques permettant d'identifier les glissements ou la redondance de noms de connections en veillant à ce qu'il n'y ait qu'un seul User ID qui se connecte depuis la même adresse IP. Ou qu'un même User ID ne se connecte pas depuis deux adresses IP simultanément à une application.

2) Trafic « libidineux et/ou ludique » : on lit les statistiques d'un proxy et on voit les usages.

3) Dans le milieu bancaire, le rejeu des paquets multicasts. Certaines banques jouent sur le décalage qui existe dans la synchronisation des cours financiers. Le décalage entre deux cours est minuscule (quelques centimes d'euro), le laps de temps est très rapide (de l'ordre d'une seconde) et dans ce délai, certains jouent sur l'effet de levier en achetant massivement et en revendant sur un autre marché. Ces mécanismes sont gérés par des paquets de multicast : pour faciliter les choses, la collecte est faite en multicast et se distribue dans tous les centres de traitement en multicast. Cela veut dire que quand un équipement ne reçoit pas un paquet il fait une demande de rejeu. Cette demande impacte énormément la latence du réseau et fait donc perdre potentiellement de l'argent au client. Pour détecter l'incident, des sondes descendent très bas dans les couches réseaux, qui vont jusqu'au niveau Ethernet. Elles peuvent monter aussi très hauts puisque les flux financiers sont traités au niveau de la couche applicative.

Le rôle d'un MSSP :

- centraliser et archiver les traces,
- analyser les journaux, les corréler et détecter les incidents,
- vérifier que le niveau de sécurité est adapté et ceci en temps réel,
- gérer les incidents de sécurité.

Remarque : le centre opérationnel de sécurité opère dans un environnement client et agit en son nom. Le superviseur de sécurité se limite à faire de la collecte et de la détection d'incidents.

Si dans le principe, la gestion de crise c'est la perte de l'univers de référence, David Maillard conclue qu'en réalité, il y a bien un univers de référence après la perte de l'univers de référence.

Olivier Callef, Devoteam BU Sécurité et CERT Devoteam

Olivier Callef insiste au début de sa présentation sur la nécessaire collaboration, dans la gestion des incidents de sécurité, entre toutes les parties prenantes (entreprise, CERT, autres entités de sécurité…).

Devoteam a commencé son activité de veille en 1996 en intervenant dans une grande banque française sur les problèmes de sécurité liés à internet.

En 2003, dans le cadre de leur intervention, suite à un incident grave chez un grand opérateur français Devoteam a trouvé l'information nécessaire en Australie où ce type d'incident s'était déjà produit. Afin d'entrer en relation avec les structures australiennes, l'un des premiers CERT français, le CERT IST, a été contacté. Ce dernier faisait partie du réseau « Inter CERT » et a permis d'échanger très rapidement avec les Australiens.

Comprenant la nécessité de travailler tous ensemble Devoteam a continué la démarche en rejoignant non pas le FIRST mais le TF–CSIRT qui est une organisation qui regroupe les entités de type CERT en Europe. D'autres communautés de sécurité

existent, parfois très actives, parfois très ciblées, et il ne faut pas les négliger.

Le CERT/CC Américain publie l'ensemble des services offerts par un CERT : services réactifs, services proactifs et services de qualité. Le détail des activités, visible sur leur site, montre que le CERT n'est pas seulement là pour faire du traitement d'incidents et peut aller jusqu'à la sensibilisation.

Dans le cas de Devoteam, SSII qui travaille dans le domaine de la sécurité, certaines choses sont faites directement en tant qu'entité CERT. En cas d'incident spécifique impliquant une activité de type « forensic », le CERT Devoteam fait appel ou recherche la coopération avec les éditeurs d'outils de « forensic ». L'équipe de Devoteam affectée à cette tâche n'est pas forcément étoffée mais elle s'appuie sur des relais divers.

La véritable dénomination pour cette activité est : « CSIRT » (*Computer Security Incident Response Team)*. CERT est une marque déposée et toute entité qui veut s'appeler CERT doit en faire la demande auprès du CERT américain. Les détails et standards qui déterminent les activités d'un CERT sont consignés dans le RFC 2350 sur les sites des CERT.

Olivier Callef insiste sur l'importance des mots « confiance », « équipe » et rappelle que la confiance se construit.

Concernant la communication externe, vis-à-vis des clients (qui peuvent être le grand public), le CERT est le point d'entrée. En interne, il peut être vu au contraire comme un fédérateur ou comme un offreur de services centraux vis-à-vis d'entités qui sont disséminées dans différents pays.

Les approches sont différentes et le traitement des incidents s'en ressent. Dans un cas, on a une vision de partage avec l'extérieur et dans l'autre cas, des problèmes internes qu'il faut régler avec éventuellement des remontées un peu plus longues.

Les quatre grands principes pour traiter un incident de sécurité sont :

- être préparé avant l'évènement,
- analyser et identifier : est-ce vraiment un incident ?
- contenir, résoudre, restaurer : limiter les dégâts,
- investiguer et surtout assurer le suivi des incidents.

Toutes ces étapes nécessitent organisation, répartition des tâches et communication.

Pour constituer un CSIRT il faut considérer tous les éléments nécessaires pour traiter ces incidents : aspect organisationnel, juridique, humain et technique.

Quatre critères permettent de savoir à quel CSIRT il faut s'adresser :

- Son rôle sera-t-il fonctionnel, opérationnel ou mixte ?
- Son positionnement sera-t-il central, CERT local ou entre les deux ?
- Son périmètre sera-t-il très large ou focalisé sur un point particulier ?
- Quelle est sa vocation ? Par exemple, le CERTA qui couvre toutes les administrations et qui a aussi la vocation de représenter la France auprès de certaines instances a une approche différente des CERT orientés constructeurs (grands éditeurs de logiciel..).

En interne le CSIRT travaille avec des acteurs sécurité qui traitent la gestion de crise au sens large du terme (pas seulement informatique pure) et éventuellement des CSIRT locaux en contact avec la DSI.

Même si c'est le CSIRT qui déclenche un plan de crise parce qu'il a eu des informations sur un incident il doit contacter et travailler avec les différents acteurs de la sécurité. Ce qui compte, c'est l'impact sur le métier : voir ce qui est tolérable ou pas en terme de dégradation de services.

En externe, les partenaires du CSIRT sont technologiques (les éditeurs, par exemple, en relation directe avec la DSI), d'autres CSIRT (français ou non) et enfin parfois les autorités de police ou judicaires.

Intégrer un CERT se fait en général sous forme de parrainage.

Pour formaliser les échanges d'information, le *Traffic Light Protocol* (TLP) oblige celui qui transmet l'information à utiliser une couleur qui indique le degré de confidentialité de l'information. Le *Common Vulnerability Reporting Framerwork* (CVRF) donne des informations sur la vulnérabilité du reporting.

Un CERT, c'est un aspect technique (SIEM), des équipes (les SOC) et des procédures. S'ajoutent des remontées d'utilisateurs, voire d'autres entités de type CERT sur des cas de phishing par exemple. Ils doivent pouvoir s'adresser à un « guichet unique » qui fera le tri et traitera l'urgence.

En France, neuf CSIRT sont référencés. Les trois premiers ont été le CERT-IST, le CERTA et le CERT–RENATER. Au niveau européen, le TF CSIRT regroupe 150 sociétés référencées dont la moitié est « accréditée ». Au niveau international, le First regroupe 140 membres. Depuis une semaine, l'EU-CERPCT a pour objectif de créer un EU-CERT dont la vocation serait de traiter les incidents de sécurité pour les institutions européennes.

Une véritable coopération entre les différents CERT s'est instaurée au plus grand bénéfice de tous (remontées d'alertes, correction de vulnérabilités…).

Certains CSIRT sont transverses et portent sur des thématiques (DNS, Cloud…). Au sein de ces structures, des sociétés ayant des intérêts commerciaux opposés (Google, Microsoft, Amazon, etc.) travaillent conjointement à la résolution d'incidents de sécurité.

Pour conclure : le CSIRT est-il une belle façade ou a-t-il une réelle utilité ? Il peut avoir une belle façade mais il a surtout une réelle utilité.

David Bizeul , CERT Société Générale

David Bizeul propose de découvrir un CERT d'entreprise. Point d'entrée entre l'externe et l'interne, il faut structurer l'organisation qui gravite autour de lui. Il assure quatre activités phare :

- la gestion d'incidents,
- la lutte contre la cybercriminalité,
- la gestion des vulnérabilités (activité historique dont le but est d'entrevoir quelles sont les nouvelles vulnérabilités sur les activités informatiques de la Banque),
- enfin, une activité capitale : la veille technologique.

Les membres du CERT doivent posséder les « *clés relationnelles* » de l'entreprise mais en cas de blocage, ils peuvent être amenés à utiliser des procédés plus directifs.

Trois niveaux permettent d'appréhender les incidents de sécurité :

la détection qui provient :

- de composantes opérationnelles ou de composantes techniques (soit directement des machines soit d'inquiétudes des équipes opérationnelles),
- des salariés qui remontent des informations dont ils sont témoins,
- des utilisateurs (les clients internautes peuvent écrire directement),

la réaction qui exige :

- de répondre immédiatement et répondre tout le temps (l'incident de sécurité prime),

- d'apporter de la valeur ajoutée : développer des compétences pas forcément présentes dans la banque,
- de ne jamais lâcher et réussir à clore l'incident,
- de ne pas négliger les incidents minimes.

la communication

La nécessaire proximité avec le personnel de l'entreprise a été évoquée plus haut. Le CERT peut mettre à profit ce point de centralisation globale des incidents de sécurité pour en faire sortir des stratégies.

Cas concret : Un internaute très intéressé par les détections de vulnérabilité sur internet, détecte une vulnérabilité XSS sur une plate-forme associée à un partenaire de la Société Générale. Cet internaute publie l'information sur Twitter. Il est retrouvé *via* une veille de tous les mots clés de la marque sur Twitter. Le CERT informe l'internaute que cette vulnérabilité va être traitée. Il joue son rôle de traitement de l'incident en ne faisant pas lui-même les modifications du code sur le site web mais en faisant un test d'intrusion pour s'assurer que la correction a été bien faite. Le CERT informe alors le «hacker » que le problème a été résolu et l'invite à faire part de ses éventuelles nouvelles découvertes.

Les enseignements :

- la structure CERT en interne doit gagner la confiance en faisant ses preuves,
- pour les acteurs de l'entreprise, l'existence d'un CERT interne est très rassurante,
- la structure est adaptée aux interactions internes/externes. La communication du CERT avec l'externe est comprise,
- les incidents sont gérés correctement parce qu'ils sont anticipés. Il faut pouvoir dérouler une méthodologie rapidement.

Les perspectives

- l'entreprise n'est plus une zone dont on maîtrise les frontières (télétravail, communication sur réseaux sociaux…). Il faut créer un réseau des contacts externes,
- la communication se libère : les clients font part de leur mécontentement sur le net. C'est pareil en sécurité,
- la réglementation pousse de plus en plus vers des notifications d'incidents,
- une veille connectée aux valeurs de l'entreprise donne beaucoup de crédit au CERT.

La Société Générale ayant monté le premier CERT d'entreprise en France, elle met à disposition de tous, des fiches de procédures opérationnelles : http://cert.societegenerale.com/fr/publications.html.

Alexandre Depret-Bixio, HP ArcSight France

Une approche CERT menée conjointement avec une approche SOC permet une action plus pro active sur la sécurité. Les systèmes d'information deviennent de plus en plus communicants et la maîtrise des personnes qui les administrent de plus en plus partielle.

Les outils internes, externalisés, infogérés ainsi que les projets de transplantation (le Cloud) génèrent une perte de contrôle progressive des équipes informatiques sur le système d'information.

Le DLP est souvent cité pour assurer la protection des données. Une approche SOC ou SIEM permet aussi d'atteindre cet objectif.

L'évolution des matériels rend nécessaire un renforcement de la sécurité physique mais la problématique réseau demeure (prévention, intrusion, firewall). L'entreprise est-elle capable de fournir à un instant « t » de bons indicateurs sur

l'état de son système d'information ? Le SIEM apporte cette réponse.

Les dernières attaques évoquées dans la presse étaient prévisibles et provoquent un déficit d'image. Chaque entité a tendance à utiliser son système en suivant ses propres règles alors que des processus standardisés ont été élaborés. Cela crée obligatoirement des « déviances ».

Une approche centralisée par la construction d'un SOC (centre opérationnel de sécurité) et la mise en place d'un outil de SIEM pour comprendre ce qu'on va collecter sur ses équipements de sécurité, est une bonne réponse.

Le SOC assure la détection des incidents et une partie de leur traitement. L'objectif n'est pas de traiter tous les incidents au même niveau, mais plutôt d'avoir un outil technologique qui est capable de s'adapter au contexte métier, à la politique et aux processus pour ensuite déceler le bon incident critique.

Le SOC aide aussi à contenir les attaques : différents experts, conjointement avec les activités des CERT, travaillent pour mieux comprendre comment évoluent ces attaques. La technologie permet aujourd'hui de voir en temps réel comment une menace évolue au sein du système d'information.

L'objectif est de ne traiter que les incidents critiques en gérant les priorités et en faisant suivre l'incident aux bonnes équipes et au bon moment. C'est aussi améliorer la politique de sécurité en fonction des nouvelles menaces. La technologie est un élément conséquent pour le choix d'un SOC.

Ce doit être une plate-forme ouverte :

- capable d'être enrichie par des données externes,
- capable de fonctionner avec une politique de risque en haute disponibilité,
- accessible par différents types de personnes qui doivent remonter les bons évènements.

Peu de projets de construction de SOC sont à l'étude sauf dans quelques grandes organisations qui ont les ressources nécessaires. Or, pour mettre en place une plate forme de SIEM on n'est pas obligé de penser SOC tout de suite.

L'outil SIEM permet :

- la collecte,
- la consolidation avec un outil qui centralise tous les évènements (on ne parle pas encore d'incident) et qui permet une analyse *post mortem* ou l'automatisation de rapport,
- la corrélation qui, en plus de faire parler tous les logs dans un même langage, les met en commun afin de détecter une éventuelle déviance.

Questions et Réponses avec l'assistance.

Cette conférence comportait également un débat avec la salle, non retranscrit dans ce document mais disponible en vidéo à l'adresse suivante : http://www.clusif.asso.fr/fr/production/videos/#video110616.

Retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF
http://www.clusif.asso.fr/fr/infos/event/#conf110616.