A N D S I

Association Nationale des Directeurs des Systèmes d'Information

www.andsi.fr

Security Operation Center (SOC)

Compte rendu de la présentation du 12 novembre 2013 – Sénat

Par

Stéphane SCIACCO, Direction de la sécurité, Orange Business Service (OBS)

Compte rendu rédigé par Isabelle MAURANGES & ANDSI

En bref…

En 2005, France Télécom mettait en place un SOC pour détecter les attaques sur ses « services ». Ce SOC détecte, qualifie les incidents de sécurité et délivre les plans de réaction.

Dans son exposé, Stéphane SCIACCO insiste sur le choix des périmètres à mettre en supervision de sécurité, la mise en place des processus, la gouvernance, l'outillage et le facteur humain.

Reprenant avec beaucoup d'exemples et de détail les différentes phases de mise en place de cette supervision (initialisation, implémentation et réalisation technique, analyse des besoins, étude de faisabilité et tuning), Stéphane SCIACCO illustre au travers de cas concret, la complexité et la puissance de cette supervision sécurité. Il présente certains éléments tels que la détection de logs, la désactivation volontaire des services, le déni de service, les apports connexes sur l'évaluation des barrières de défense et l'évaluation des politiques internes de sécurité.

Enfin, avant de conclure, Stéphane SCIACCO aborde la problématique de la résilience et de l'évolution de maturité des équipes au fur et à mesure de leur montée en puissance. Quelques mots également sur le coût de ces solutions, la tentation forte d'externalisation accompagnée de l'apparition des «faux positifs», sans oublier l'indispensable, «expert sécurité».

Introduction par Pierre DELORT, Président de l'ANDSI

L'action de guerre revêt essentiellement le caractère de la contingence. C'est ainsi que Charles de GAULLE débuta un de ses écrits majeurs, le Fil de l'Epée. Quatre-vingt années après, les DSI des Opérateurs d'Importance Vitale (OIV) se préparent à la défense des intérêts fondamentaux de la nation.
Quel sera le caractère de leurs actions de cyber-défense ? Quatre personnes vous nous éclairer…
…parmi eux Monsieur Stéphane SCIACCO de la Direction de la Sécurité d'Orange Business Services présente la mise en place d'un Security Operation Center (SOC).
[L'ensemble des supports et comptes-rendus de la conférence sont à consulter sur www.andsi.fr]

Exposé

Quand France Télécom met en place un SOC en 2005, le souci n'est pas de savoir si « nous allions être attaqué mais plutôt de détecter le plus rapidement possible toute intrusion ou attaque » afin d'éviter que les systèmes ne tombent. Les besoins de la Direction portent sur le renforcement des réseaux d'entreprise, la sécurité des plates-formes de service, la protection du SI. Les enjeux sont de protéger l'image de marque et surtout les biens sensibles.

Security Operation Center (SOC)

Un SOC pour Orange est un service fournissant des services de détection, recevant des alertes de sécurité à qualifier en incidents de sécurité. Ensuite, il délivre des plans de réactions qui seront implémentés ou non par l'expert « système/réseau ». Tout ceci nécessite beaucoup d'expertises et présente un coût. Stéphane SCIACCO décrit schématique les phases d'une attaques : le renseignement (prise d'empreinte, scan des systèmes à attaquer) puis de dépôt d'un code malicieux, et enfin, de fuite d'information (récupération de password, coordonnées bancaires, données sensibles…).

Le scope de supervision de sécurité
Les périmètres de supervision identifiés sont : les **«infrastructures»,** les backbones et leurs zones d'administration.
Les services **«applicatifs»,** comprennent les zones d'hébergement et les services data.
Les équipes ont travaillé durant 18 mois avant de mettre en place le premier service en **supervision de sécurité**.
Les quatre grandes étapes de construction d'un SOC sont:

1. La **mise en place des processus** - rédaction de l'expression de besoins, spécification du champ concerné par la supervision de sécurité, qualification des processus et choix critiques, processus de la chaine de traitement des alertes ;
2. La **gouvernance** – prioriser les services à superviser suite à une analyse de risque par exemple ;
3. L'**outillage** - le choix des capteurs (IDS, Intrusion Detection System, concentrateur de log, quel seuil à mettre sur ces indicateurs ?,…) ;
4. Et, surtout, **l'humain** - incluant la mise en place et la capitalisation sur une réelle équipe 24 heures sur 24 (idéalement ingénieur sécurité) très bien formée (test d'intrusion, capteurs, corrélation, attaques..).

Le **processus de mise en place d'une supervision** de sécurité dans un service suppose une phase d'**initialisation** (rédaction de l'expression du besoin) à la demande du client. Orange dispose maintenant d'un document générique remis à la MOA et qui traite de manière macro de la supervision de sécurité (quelles sont les fonctions du service concerné ? Quelles sont les briques qui vont assurer ce service ?). Ensuite c'est la phase d**'implémentation** où le SOC fournit sa réponse technique sur les capteurs à acquérir, les règles à utiliser, les corrélations à activer …

Lors de la **réalisation technique**, on implémente le capteur, on récupère les logs et on réalise une phase de tuning. La **phase de tuning** dure un certain temps avant de passer en **phase opérationnelle**. C'est le SOC qui réalise et plus on avance en phase de supervision, plus on tend vers le régime de croisière. Le SOC fournit des alertes et du reporting. Tout ce qui est traitement est à la charge de **l'expert** de la plate-forme. L'expert de la plate-forme connaît exactement son système et sait exactement si un plan que lui a fourni le SOC va dégrader son service ou pas. Nous avons vraiment séparé la partie «détection /qualification» de la partie «traitement de l'incident» lui même. Ceci pose d'ailleurs des problèmes en termes de communication.

Les délais sont approximatifs. La partie **analyse des besoins** dure de cinq à dix jours. Cinq jours, par exemple, pour un portail web à mettre en supervision de sécurité. Dix jours pour un backbone qui est quelque chose de plus compliqué. **Etude de faisabilité et tuning** prennent quinze jours pour un serveur web. Pour le backbone nous avons mis près d'une soixantaine de jours. La phase de test et tuning dure de un à trois mois. C'est toujours le même travail : nous regardons si les règles sur les IDS correspondent au scope supervisé et ne génèrent pas trop de faux positif ou de pollution. Après c'est le rythme de croisière.

Au niveau de la **détection**, petit rappel sur les capteurs de sécurité : IDS analyseurs de log et modélisation de trafic.

La **concentration de logs** permet de récupérer les logs de firewalls, de routeurs, de proxy… On met tout dans un concentrateur de logs, on élabore une pseudo règle de corrélation et si un attaquant commence à nous titiller, une alerte part vers le service de supervision de sécurité pour qu'il qualifie et puisse dire «attention, là, il y a quelqu'un qui est entrain de faire une tentative d'intrusion sur un site web ».

Dans le SOC, nous avons des personnes qui travaillent sur des attaques à déni de service. C'est relativement simple à détecter, je dis «relativement simple» car la remédiation l'est beaucoup plus. La remédiation permet de faire soit un «blackholing» (poubellisation de l'ensemble du trafic d'attaque) ce qui est drastique, soit tenter de dépolluer le trafic de son (cleanning) le flux d'attaque.

Principe de fonctionnement de l'IDS : sur une infrastructure de type web l'attaquant va tenter d'exploiter les vulnérabilités du serveur WEB. Nous positionnons notre IDS en dérivation pour capter tous les flux. Ensuite l'IDS analyse le flux pour identifier des attaques à partir par exemple d'une base de signature. Petit point de vigilance : un

IDS se bypasse ! Il existe des techniques pour éviter que l'IDS détecte les flux d'attaques. Demandez à votre fournisseur d'IDS s'il a mis en place des tests spécifiques pour ce genre d'attaque.

S'agissant de la **chaine de qualification**, quand un « gentil attaquant nous titille », l'IDS tente d'identifier, via ses règles de détection, une attaque. On pourrais s'arrêter là et juste faire confiance à ces règles mais cela génère énormément de faux positifs et la qualification risque d'être très compliqué voir inefficace. Nous allons donc rajouter la qualification de l'hôte. On va enrichir notre IDS via la détermination de la version du système attaqué, un Windows 2008, un linux version X, un Apache version Y … On injecte aussi les vulnérabilités associées à ce système : Ex : si je suis sur un Apache version Y je vais injecter la liste des vulnérabilités qui peuvent être exploitées pour cette version. Il y a une « corrélation » entre la détection via les signatures, la qualification de l'hôte et les vulnérabilités. Je tente ainsi d'améliorer la qualification. Pour cela il faut un outillage qui embarque directement cet enrichissement ou un système ouvert sur laquelle on injecte les données de qualification de l'hôte et des vulnérabilités.

Détection de logs. On engendre énormément de logs sur nos équipements. En fonction de ces logs, nous allons essayer de détecter des commandes critiques qui sont passées sur les équipements.

Le **Déni de service** c'est rapidement la saturation de la bande passante du lien. Le principe de détection est par exemple la modélisation des comportements : pendant un certain temps on apprends le flux puis on positionne des seuils. Quand il y a une attaque le dépassement du seuil émet une alerte. Sur l'exemple, vous pouvez voir le débit de l'attaque, l'adresse IP de l'attaquant, l'adresse IP de destination et la durée de l'attaque. La détection est, somme toute, assez facile, la réaction est plus compliquée.

Les apports en dehors de la détection : vous avez bien compris que la détection est importante, néanmoins il y a aussi des apports supplémentaires à la mise en place d'un SOC, comme l'évaluation de nos barrières de défense ou le fait d'avoir une attaque avec impact. Par exemple s'il y a une attaque sans impact, nous l'aurons tout de même détectée mais nous ne ferons pas de reconfiguration des équipements réseaux, par contre si nous avons une attaque avec impact, il va forcément falloir reconfigurer les barrières de défense, voire, dans certains cas, re-sensibiliser les équipes.

Evaluation des politiques de sécurité. En cas d'attaque sans impact, on peut considérer que l'on a une politique (ici guides de configuration) efficace, si c'est avec impact c'est que notre politique ne l'est pas. Nous avons donc probablement mal rédigé nos guides de configuration de firewall, de proxy,….

Les apports indirects : On peut aussi tenter de mettre en place un ROI de nos investissement sécurité. Par exemple si la somme des attaques avec impact est supérieure à la somme des attaques sans impact, c'est que l'allocation des moyens de défense est insuffisante, mal positionnée, mal configurée ou mal employée. Il faut donc revisiter un peu notre design, « l'efficacité » des équipements… **La résilience** (disponibilité du service) est le fait de détecter plus rapidement la non-disponibilité du service.

Evolution de maturité dans le temps. Il est pertinent de commencer par la mise en place de détection liée aux attaques sur les schémas d'authentification. Ensuite passer par la mise en place d'IDS. Cela demande une expertise plus poussée et une connaissance du contexte mis en supervision. La détection des attaques par DDoS requière une expertise sécurité et réseau encore plus accrue. Enfin dernière évolution, la mise en place d'une détection sur les attaques « applicatives », très compliquée car il y faut analyser un grand volume de log variés.

Les coûts. Les coûts visibles de l'iceberg concernent l'activité de supervision. Ensuite vient l'activité d'ingénierie, par exemple, où placer le capteur, prend également beaucoup de temps. En sus des coûts de supervision, viennent les coûts des outils et, ce que l'on oublie souvent : le coût de **l'expert sécurité**. Enfin tout ce qui touche aux processus prend également beaucoup de temps.

Externalisation. Comme nous venons de le voir, la supervision de la sécurité a un coût non négligeable qui justifie d'étudier la mise en place d'une externalisation. Les conditions sont : avoir une chaine de remontée des alertes sécurisée.
Les difficultés proviennent souvent de ce que l'on appelle les «faux positifs». Comme le fournisseur de service de sécurité, le Managed Security Services Provider ne connaît pas ou peu votre environnement, il peut y avoir énormément de faux positif au départ, ce qui peut vous décrédibiliser ou vous mettre en porte-à-faux vis-a-vis du DSI qui considère qu'on l'alerte à tort. Tout ce qui relève de la chaine de communication (comment je transmets, à qui je transmets l'alerte puis le traitement des alertes) est aussi complexe.

Conclusion
Les conditions de réussite sont : la MOA du service doit être vraiment partie prenante. Elle met les moyens pour effectivement faire de la supervision. Il faut exactement savoir qui contacter en cas de d'attaque. La spécification des objets à superviser doit être très précise : c'est le cahier des charges que l'on met en place. Si la spécification est trop vague, la détection pourra engendre énormément de faux positifs.
Enfin, bien définir tout ce qui est rôles et responsabilités ? Qui détecte ? C'est le SOC, mais qui traite les alertes ? C'est à clairement identifier : niveau 1, niveau 2, ou niveau 3. De même pour ce qui est le traitements de corrélation.

Hors projet
L'ingénierie des capteurs est réalisée par le SOC. En terme de détection et de qualification, si on n'a pas mis en place ou si on ne sait pas comment fonctionne le service, ce sera très compliqué de qualifier un incident de sécurité. Il faut aussi mettre en place une cellule de veille hors du SOC. Enfin il peut être utile de fournir au SOC une plateforme de simulation des attaques. Cette plateforme sera utilisée comme laboratoire de test par le SOC pour analyser les nouvelles attaques et regarder comment se comporte l'IDS voir les logs.

Stéphane SCIACCO considère que **la supervision de sécurité est une brique supplémentaire**. Vous avez toutes les briques, ne les jetez pas, gardez les. La supervision de sécurité avec les IDS et les logs vient compléter le dispositif et un jour il y aura surement d'autres barrières de défense mais, désolé, je ne sais pas encore lesquelles !

Débat

Intervenant : Faut il tout superviser ?
OBS : non il ne faut pas tout superviser. Il faut vraiment identifier par analyse de risque ou suite à incident de sécurité ce que vous devez mettre en supervision de sécurité. Cela coute cher, cela utilise du « Manpower » et requiert des investissements au niveau des IDS. Vous démarrez par des applications Top SOX, des Active Directories, un service WEB. Vous devez commencer doucement puis monter en compétence et surtout en supervision.

Intervenant : Vous avez beaucoup parlé des faux positifs mais il y a aussi des problèmes avec les faux négatifs car vous ne les connaissez pas.
OBS: Exact et là nous ne pouvons pour le moment pas faire grands choses. Malgré cela on peut se poser la question sur la problématique des fuites d'information. Il y a un gros travail pour regarder si l'on peut obtenir des signaux faibles de sorties, des mots de passe qui sorte, des données sensibles… Ces signaux ne seront pas massifs Il faut vraiment pister la fuite d'information, remettre des règles, analyser les logs sur la fuite d'information. Cette partie est très importante, c'est notre enjeu 2014/2015 et il est vraiment important.

Intervenant : Comment gérez-vous le facteur humain ?
OBS : Nous avons des programmes de sensibilisation très important mais malheureusement c'est un facteur que l'on ne maîtrise pas. Si quelqu'un, même très sensibilisé, veut volontairement ou involontairement mettre la clé USB qu'il a trouvée sur le parking sur son PC, on va avoir du mal a l'en empêcher … C'est pour ca qu'il faut détecter les fuites d'information et pas seulement les attaques en direct. On n'a pas pensé à tout en 2005 quand on a mis en place le service, les attaques externes on sait, on en aura, on sera malmenés, mais si quelqu'un réussi a s'introduire en interne il faudra savoir le détecter. Les signaux faibles vont être compliqués à mettre en place, c'est un enjeu pour les années à venir.

Intervenant : Tout ce qui est interconnexion réseau entre interne et externe passe, dans la société dont je suis DSI, par des matériels Orange, j'aimerai savoir comment je peux être rassuré sur la part qui est surveillée et celle qui l'est moins. Pourquoi cette surveillance pour nous est un service complémentaire, de bonne garantie de services vendus.
OBS : ce n'est pas un service vendu. Ce qu'on a mis en place, c'est un service de supervision des infrastructures et des services internes sur laquelle s'appuie notamment votre réseau. On tente de garantir qu'une attaque sur ce réseau soit détectée et ne perturbe pas votre service.

Présentation de l'orateur

Stéphane SCIACCO après un parcours d'auditeur et d'architecture sécurité a effectué 3 années au sein du CNSSI de France Télécom (Centre National de Sécurité des systèmes d'information) en charge notamment de la mise en place d'un centre de supervision de sécurité (SOC) en 2005. Il travaille actuellement à la Direction de la Sécurité d'Orange Business Services en tant qu'expert sécurité où il assure, entre autre, des missions d'implémentation de la norme ISO 27001, de coordination des actions de supervision de sécurité, de pilotage d'audits et de veille.