A N D S I

Association Nationale des Directeurs des Systèmes d'Information

www.andsi.fr

La cyber sécurité

En cas d'évènement indésirable, quelles sont les actions à mener ?

Compte rendu de la présentation du 12 novembre 2013 – Sénat

Par

Jocelyn DALLE, chef du groupe d'enquête piratage au sein de l'OCLCTIC

Compte rendu rédigé par Isabelle MAURANGES & ANDSI

En bref…

Le Capitaine Jocelyn DALLE présente l'organisation et les missions de l'Office Central de Lutte contre la Criminalité liée au Technologies de l'Information et de la Communication (OCLCTIC). Composé d'une plate forme de signalement, de quatre groupes d'enquête, et d'une section documentation et relations internationales, l'Office s'intéresse au coté technique mais surtout au coté humain quand la chaine des SI de l'entreprise est compromise.

Introduction malveillante de clé USB, lien de mail malveillant, lecture de CD Rom non vérifié, tel est le quotidien de l'Office. Suivant le préjudice subi, le niveau d'attaque, les conséquences et implications qui en découlent (déni de service, fuite d'information, compromission de base de données, remise en question de la sécurité d'une infrastructure) l'Office prend en compte les doléances et oriente vers le service compétent.

Comment réagir en cas de malversation ? Il suffit d'appeler l'Office et, éventuellement, transmettre la plainte au service juridique de l'entreprise. Pour travailler l'Office doit accéder aux logs. La plainte part souvent à l'international car l'Office est relai d'Interpol et les relations à l'international sont excellentes.

Le plus important c'est l'humain. A vous de sensibiliser, de faire signer une charte et de former en permanence chacun.

L'Association Nationale des Directeurs des Systèmes d'Information organise des débats et en diffuse des comptes-rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

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...
Pour notre dernière intervention, le capitaine Jocelyn DALLE de l'OCLCTIC, nous explique quelles actions mener suite à évènement indésirable grave.
[L'ensemble des supports et comptes-rendus de la conférence sont à consulter sur www.andsi.fr]

Exposé

Le Capitaine Jocelyn DALLE travaille à l'Office Central de Lutte contre la Criminalité liée au Technologies de l'Information et de la Communication (OCLCTIC). Cet office dépend directement de la police judiciaire et s'occupe exclusivement d'investigations de type judiciaires. Créé en 2000, il comprend une soixantaine de personnes.

L'OCLCTIC est composé :

1. d'une plate forme de signalement regroupant une vingtaine de personnes qui permet aux internautes de signaler les contenus ou les comportements présumés illicites au regard de la Loi ;
2. de quatre groupes d'enquêtes ;
    - piratage informatique (Hacking, piratage de bases de données et autres) ;
    - escroquerie sur Internet ;
    - fraude aux opérateurs de téléphonie (ouverture de lignes frauduleuses, piratage de PABX ou d'infrastructures…) ;
    - fraudes aux moyens de paiement, contrefaçon de Cartes bancaires ;
3. d'une section documentation et relations internationales.

Notre domaine de compétences (pour le groupe Piratage Informatique)
Dans la police nous nous intéressons au coté technique mais surtout au coté humain, car la chaine des SI est compromise par le maillon le plus faible qui est l'humain « l'erreur ou la faille est entre le clavier et la chaise ». A partir du moment où un employé, par négligence, par imprudence, par méconnaissance ou volontairement, introduit une clé USB avec un code malveillant ou clique sur le lien d'un mail malveillant qu'il a reçu, il est difficile d'assurer une sécurité à 100%.

Le but poursuivi par les attaquants qui vont mettre à disposition ce genre de code malveillant est, la plus part du temps, financier. Comment trouver de l'argent en attaquant les sociétés ? C'est le plus souvent en utilisant les données (adresse mail, tél, coordonnées bancaires…) que l'on peut revendre.
Dans la plupart des cas, ces attaques sont initiées depuis l'international et l'Office travaille en étroite collaboration avec Interpol. Actuellement, les principaux pôles de cybercriminalité sont les pays de l'Est (Russie, Ukraine) un peu la Roumanie et, en émergence, au Maghreb.

Comment l'attaquant procède t il ?
A l'étranger les personnes œuvrent anonymement. L'enquête est donc très fastidieuse et compliquée.

Quand contacter l'OCLCTIC ?
Tout dépend du préjudice subit, du niveau d'attaque, des conséquences de l'attaque et des implications qui en découlent. S'il s'agit d'un déni de service et d'une fuite d'information, une compromission de base de données, la remise en question de la sécurité d'une infrastructure, l'OCLCTIC prend connaissance des doléances et/ou vous oriente vers le service compétent (Si un OIV ou une société sensible est victime d'une intrusion l'Office ne sera pas forcement compétent et pourra vous envoyer à la Direction Centrale du Renseignement Intérieur (DCRI) qui a compétence sur tout ce qui est atteinte à la sureté de l'Etat et ce qui s'y rattache, ou bien directement à un service de la Police Judiciaire). Il faut venir lorsque vous avez un préjudice sérieux, de la donnée qui fuite, ou lorsqu'il y a potentiellement derrière une remontée possible.

Comment faire (ou ne pas faire) :
Appeler l'Office (si possible en présence d'une personne pouvant répondre aux questions techniques) afin de voir comment procéder et récupérer toutes les informations importantes pour nos enquêteurs et, éventuellement, transmettre la plainte au service juridique de l'entreprise. Surtout ne pas s'arrêter au seul service juridique qui risque de n'envoyer la plainte à l'Office que plusieurs semaines plus tard.
Saisir le service juridique et prévenir la police, notamment l'OCLCTIC, et rester maître du dossier car l'enquêteur aura besoin d'informations techniques et ce n'est pas le service juridique qui va lui transmettre ces informations. L'enquêteur a besoin de la personne qui dépose la plainte souvent en provenance de la DSI, du RSSI, des ingénieurs réseaux car il doit avoir accès aux logs. Dans tous les cas, si vous hésitez et ne savez que ou quand faire, contacter l'Office qui vous aiguillera.

Comment se déroule l'enquête ?
C'est une enquête de police constituée d'analyses et d'auditions pouvant aller jusqu'à la garde à vue. Après le dépôt de plainte, l'Office analyse tous les éléments avec la personne qui a déposé plainte. Au final, cela part souvent à l'international car nous sommes point de relai avec Interpol. Toutes les demandes en matière de cybercriminalité, faites par les polices ou gendarmeries de France, et, qui ont pour but de partir à l'international, passent par L'Office. Nous entretenons de très bonnes relations à l'international, nous développons des coopérations avec les pays, plus ou moins facilement d'ailleurs (USA et Russie c'est un peu compliqué…). Pour finir, j'insiste vraiment sur le coté humain, la faille est vraiment dans l'humain, sensibilisez toutes les personnes car c'est important. Leur faire signer une charte c'est très bien, mais la formation permanente c'est mieux.

A N D S I

Débat

Intervenant : Vous avez dit qu'il fallait d'abord vous avertir avant de parler au service juridique, sauf que lorsque le délit est à l'intérieur de l'entreprise, vous dépendez du pénal pour ce qui concerne la cyber criminalité mais aussi du droit du travail concernant l'employé et vous avez alors 2 procédures à faire. Forcément vous avez besoin des services juridiques.
OCLCTIC : Mon propos était bien de vous faire comprendre que l'on ne transmet pas seulement le dossier au service juridique. Il faut vraiment suivre le dossier en en informant l'Office.

Int. : Je voudrais rebondir sur votre intervention pour dire que j'ai été victime il y a quelques mois. Nous avons contacté la DCRI et informé le service juridique ET la police. Il est important que l'entreprise soit immergée dans le travail d'investigation. Notre cellule technique a immédiatement commencé le travail d'investigation ce qui a permis rapidement à la DCRI de remonter toute la chaine. Enfin, attention à l'image de marque : le dossier étant dans les mains de la Police, l'entreprise n'est plus maîtresse de sa communication…
OCLCTIC : pour ce qui est de la DCRI, nous travaillons en étroite collaboration avec elle. Effectivement, vous êtes les mieux placés pour expliquer ce qui s'est passé et nous aider dans la compréhension du dossier. Concernant l'image de marque de l'entreprise et la communication de crise, nous ne les gérons pas, mais nous essayons de faire en sorte que tout se passe dans les meilleures conditions possibles en gardant la confidentialité des informations. En revanche, à partir du moment où l'information est entrée en procédure, juge, avocats ou partie civile, tout le monde a accès aux informations et la communication peut déborder. Notre préoccupation n'est pas la communication, mais la découverte des coupables.

Int. : Les demandes des services de polices en matière d'information nécessitent beaucoup de temps pour l'ensemble des équipes informatiques, pourquoi ? Par ailleurs, combien de temps devons-nous garder nos données ?
OCLCTIC : je pense que vous évoquez les réquisitions judiciaires. C'est effectivement un problème. La réquisition judiciaire est un document, émis par un OPJ, dans lequel il ordonne de lui transmettre telle ou telle information, ou d'effectuer tel service. Je peux comprendre que vous ne saisissiez pas vraiment pourquoi vous recevez ces documents et que ce soit parfois compliqué. C'est pourquoi une coopération étroite dés le début de l'enquête est primordiale. S'agissant de la conservation des données, c'est la législation en la matière qui fait foi, à savoir : un an pour tout ce qui est identification des données. En revanche pour les logs de firewall il n'y a pas de législation, vous pouvez les garder autant de temps que vous voulez dés lors que ce ne sont pas des logs qui permettent d'identifier un utilisateur.

O.C.L.C.T.I.C. *101 Rue des 3 Fontanots - 92000 NANTERRE - Tel : 01 47 44 97 55 / 01.49.27.49.27*

Présentation de l'orateur

Le Capitaine Jocelyn DALLE est chef du groupe d'enquête piratage au sein de l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication).