2012-12-19T19:29:00+01:00

CERT XMCO

Résumé du CNIS Event du 13 décembre 2012

Le CERT-XMCO était présent lors du dernier CNIS Event de l'année qui s'est déroulé le jeudi 13 décembre 2012 à l'hôtel Intercontinental à Paris autour du thème suivant : Comment administrer la sécurité du SI aujourd'hui ?
Afin d'animer la réflexion autour de cette problématique, plusieurs intervenants nous ont fait part durant cette matinée de leurs retours d'expérience sur le sujet :

- Les risques d'une mauvaise administration de la SSI, par Hervé Schauer (Clusif)
- Gérer l'inconnu : comment se protéger de ce que l'on ne connait pas, par Arnaud Kopp (Palo Alto Networks)
- L'externalisation, une solution pour l'administration de la sécurité ?, par Matthieu Garin (Solucom)
- Les attaques ciblées, fiction ou réalité ?, par Cyrille Badeau (Sourcefire)
- La minute Juridique, par Maîtres Olivier Itéanu et Garance Mathias
- Marché, Tendance et Évolutions de la gestion des identités, par Alexandre Garret (Atheos)
- Table Ronde, avec Eric Barbry (cabinet Alain Bensoussan), Olivier Caleff (Cert Devoteam), Gérard Gaudin (Club R2GS) et Meydéric Leborgne (RIM), animée par Bertrand Garé (Analyste IT)

Risques d'une mauvaise administration de la SSI

La matinée a débuté par la présentation d'Hervé Schauer, présent en tant qu'ambassadeur du CLUSIF.
La première partie de sa présentation a par ailleurs consisté en un rappel sur le fonctionnement et les activités récentes du CLUSIF. Il a notamment rappelé que le Club a pour vocation, grâce à des groupes de travail, de produire des documents facilitant la mise en place d'actions relatives à la sécurité. Il a ainsi annoncé la création de plusieurs de ces groupes pour avancer sur les sujets suivants :

- la norme ISO 27035,
- la sécurité des systèmes d'information dans le milieu médical,
- la sécurité des systèmes industriels (ICS).

Dans un deuxième temps, Mr Schauer est revenu sur le rôle de l'humain dans l'administration de la sécurité. Rappelant que même s'il s'agit souvent du maillon faible, seul l'humain fait la sécurité. Il a également mis en garde contre les pièges de l'automatisation et des solutions «clé en main». En effet, il faudra toujours du personnel compétent pour administrer et faire évoluer les mécanismes de sécurisation mis en place par les professionnels de la sécurité.
La présentation s'est terminée par quelques conseils de bonne hygiène en matière de sécurité :

- mettre en place des procédures de sécurité et les mettre à l'épreuve ;
- exploiter correctement la journalisation ;
- proscrire l'utilisation de mots de passe constructeurs par défaut ;
- toujours prendre en compte le facteur hu-

Résumé du CNIS Event du 13 décembre 2012

main.

Gérer l'inconnu : comment se protéger de ce que l'on ne connait pas

Lors de cette présentation, Arnaud Kopp a présenté, au travers des fonctionnalités de sécurité implémentées par les firewalls Palo Alto, comment réagir face aux inconnues en matière de SSI.
Il a commencé par redéfinir ce qui peut être considéré comme inconnu dans un SI:

- les applications : en effet, nombre d'entre elles ne disposent pas de signatures dans les référentiels des IDS/IPS, notamment les applications métiers conçues en interne,
- les utilisateurs : avec la virtualisation des postes utilisateur et les problématiques BYOD, comment s'assurer de l'authenticité des utilisateurs connectés au SI ?
- les sites web : de la difficulté de différencier les flux web légitimes des flux malveillants
- les attaques : avec le marché des vulnérabilités 0day, comment se prémunir d'attaques encore inconnues ?
- les malwares : comment identifier un malware spécifiquement conçu pour pénétrer mon SI ?

Bien que la présentation ait pour but de mettre en valeur les fonctionnalités des produits Palo Alto, certains axes de prévention et de remédiation peuvent très bien être considérés dans le cadre de l'administration sécurité d'un SI, quelles que soient d'ailleurs les solutions techniques mises en oeuvre :

- cartographier le SI et identifier les flux légitimes aide à circonscrire les menaces potentielles,
- analyser les flux légitimes en détail; par exemple, les ports 80 et 53 sont réservés ;respectivement au trafic HTTP et DNS, il faut donc identifier et intercepter les tentatives d'y faire circuler des flux suspects ;
- les tentatives d'intrusion, fructueuses ou non, doivent être analysées.

Externalisation, une solution pour l'administration de la sécurité ?

Mathieu Garin a commencé son intervention par une courte présentation de l'activité de son entreprise (Solucom), qui réalise, entre autres, des prestations d'externalisation de l'administration de la sécurité.
Il a ensuite rappelé les trois piliers de l'administration de la sécurité :

- la gestion des équipements au travers de l'administration des firewalls, des antivirus et autres proxys ;
- la prévention par la réalisation de tests d'intrusion, d'audit techniques et la veille sur les technologies utilisées ;
- et enfin la surveillance et la réaction en cas d'incident, passant par une gestion correcte des événements sécurité, la mise en place de plan de gestion de crise et la réalisation d'audit inforensics.

Selon lui, les motivations de l'externalisation résident dans le fait que les menaces sur le SI s'internationalisent et deviennent de plus en plus complexes, mais également dans le fait que l'administration de la sécurité se révèle de plus en plus coûteuse et ces frais peuvent parfois être difficiles à justifier. C'est pourquoi l'externalisation de ces services peut se révéler être un bon moyen de maîtriser son niveau de sécurité.
Mr Garin a ensuite passé en revue les principaux

Résumé du CNIS Event du 13 décembre 2012

groupes d'acteurs dans ce domaine ainsi que les prestations qu'ils proposent, que l'on peut résumer en deux offres:

- l'externalisation de la gestion des équipements, une offre qui existe depuis de nombreuses années ;
- l'externalisation des services de surveillance, de prévention et de réaction, en mode SOC, qui se développe de plus en plus.

L'intervenant a fourni de nombreux conseils sur la façon de réussir l'externalisation de ces services, tout en rappelant la nécessité de ne surtout pas tout externaliser. L'externalisation ne devant s'appliquer en priorité qu'aux parties du SI peu ou pas contextuelles.
Il a conclu en citant les trois facteurs de succès de l'externalisation selon lui :

- établir une communication solide avec le prestataire d'externalisation ;
- commencer avec un petit périmètre tout en pensant dès le démarrage à l'évolutivité du service, en anticipant les évolutions futures ;
- prévoir les conditions contractuelles de réversibilité, c'est-à-dire la possibilité de changer de prestataire sans difficulté.

Attaques ciblées, fiction ou réalité ?

Cette présentation, animée par Cyrille Badeau, a démarré par la projection de cette vidéo. Réalisée par le cabinet Deloitte, elle met en scène une attaque informatique à grande échelle parvenant à mettre à mal une grande entreprise.
À la suite de cette projection, Mr Badeau est revenu sur les conditions qui peuvent permettre la réussite d'une telle attaque. Il a ainsi mis l'accent sur le fait que les attaquants chercheront toujours à obtenir l'»information superiority» avant de passer à l'attaque et qu'il est fort probable qu'ils soient très bien renseignés et ciblent les zones du SI qu'ils auront identifiées comme les plus vulnérables.
Après avoir mis en valeur les fonctionnalités offertes par les produits de sa société (SourceFire), Mr Badeau a néanmoins rappelé l'importance de connaître les limitations des produits utilisés pour l'administration de la sécurité.
L'intervenant a aussi rappelé, une fois de plus, l'importance d'identifier correctement et avec précision ses biens critiques ainsi que leur niveau d'exposition. Car c'est seulement une fois cette phase initiale de cartographie et d'identification réalisée qu'il est possible de mettre en place des mécanismes de protection efficaces. Il a également admis qu'il ne fallait jamais faire confiance à 100% à ces équipements. En cas d'intrusion ou de tentative d'intrusion, il faudra toujours être réactif et lancer les investigations nécessaires pour déterminer les méthodes d'attaques utilisées ainsi que les faiblesses exploitées par les attaquants, faisant allusion au concept des «boites noires» utilisées dans l'aviation.
Enifn, Mr Badeau a conclu en incitant à mettre en place un cycle de recherche continue des sources de risques, car celles-ci se déplacent après chaque remédiation et chaque mise en place de contre-mesures.

Minute Juridique

Lors de ce rendez-vous traditionnel des CNIS Events, l'un des principaux sujets abordés a été le cas de la «cyber légitime défense» et les deux intervenants présents, Maîtres Olivier Itéanu et Garance Mathias, ont eu l'occasion de nous fournir quelques précisions sur le sujet.
Tout d'abord, ils ont rappelé que la légitime défense est une exception à la loi et qu'à ce titre elle est très clairement définie par le Code pénal. Elle concerne avant tout la défense des personnes physiques et ne peut être tolérée que dans le cadre de la défense face

Résumé du CNIS Event du 13 décembre 2012

à un danger actuel ou imminent. De plus la réaction doit être proportionnée et nécessaire à la sauvegarde de la personne face à un dommage imminent. Voilà donc un cadre juridique que ne s'adapte guère à la «cyber contre-attaque», sujet de discussion très en vogue actuellement.
De plus, les deux avocats ont mis en garde contre les risques de se retrouver soi-même en infraction avec la loi. En effet, à se faire justice soi-même face à des attaques informatiques, on peut vite se retrouver en infraction pour des délits de recel d'information, de complicité voire même d'entrave au bon fonctionnement d'un système de traitement automatisé de données.
Les deux spécialistes ont d'ailleurs illustré leurs propos de cas concrets, dans lesquels les entreprises ou les particuliers ayant tenté ce type de contre-attaque se sont retrouvées à leur tour face au tribunal.
De nombreux autres sujets ont été abordés, tels que les problèmes de territorialité face aux attaques venant de l'étranger ou encore de la légitimité des «Honeypots», destinés à attirer les cybercriminels pour étudier leurs techniques d'attaque.

Marché, Tendance et Évolutions de la gestion des identités

Lors de cette présentation, assez courte, Alexandre Garret a fait le point sur l'état actuel du marché de la gestion des identités.
Après un résumé des évolutions passées dans ce domaine, il a rappelé les 4 grands axes de la gestion des identités : gouvernance, accès, identité, habilitation.
Mr Garret a également décrit plus en détail les différentes familles d'acteurs dans ce secteur, notamment les nouveaux arrivants (tels que Symantec, suite au rachat de VeriSign, SafeNet et Okta) avant de passer en revue les évolutions actuelles du marché de la gestion d'identités.
Parmi ces évolutions on retiendra surtout le passage de plus en plus prononcé à un mode de gouvernance des identités, plutôt qu'une administration purement IT. Toujours dans cette lancée, l'intervenant a conclu en notant que l'on passe d'ailleurs de plus en plus d'un modèle métier de l'identité à un système de gestion des exceptions dans ce domaine.

Table Ronde

Enfin, cette matinée s'est terminée par une table ronde, toujours sur le thème de l'administration de la sécurité. De nombreux sujets y ont été abordés et les intervenants ont répondu aux questions des personnes présentes.
Parmi les sujets abordés :

- Comment faire le lien entre décideurs et SSI ?
- BYOD et responsabilité
- Intégration du BYOD dans le SI
- Data Breach Protection, de l'importance de bien s'assurer
- Rédaction «intelligente» des contrats et des chartes SSI
- De l'importance de cartographier son environnement SI
- Quelle tolérance entre bonnes pratiques et réalité ?
- Quels référentiels utiliser dans le cadre des audits ?
- D'où viennent les faiblesses de mon SI ?