CR conférence cyberstratégie des entreprises	
Auteur : Christophe Poirier	**Visa :**
Référence : **CR-I2D-2013-XXX**	**Date :**
Accessibilité : *libre*	
Objet : Conférence cyberstratégie des entreprises : stratégie compréhensive et outils ***Date : 2 décembre 2013*** ***Lieu : MEDEF IdF*** ***Durée :*** 1/2 journée	
Participants : Christophe Poirier	

1. BUT DE LA REUNION

Le lundi 2 décembre 14h00-19h00, au siège du Medef Ile-de-France, 10 rue du Débarcadère Paris 17eme (près de la porte Maillot), la chaire Castex de cyberstratégie, l'atelier sécurité de Forum ATENA, le Medef et l'ARCSI organisent le deuxième volet des évènements qui répondent à la question "Pourquoi les entreprises ont-elles besoin d'une cyberstratégie ?".

Cette conférence qui fait suite à une première journée « Les cybermenaces, quels risques pour les entreprises ? », se proposait d'aborder la question de l'élaboration et la mise en œuvre d'une cyberstratégie pour les entreprises. Comment définir l'information stratégique ? Comment et où affecter les ressources ? Quels sont les outils de pilotage financier ? Quelles sont les difficultés à surmonter ? Quelles sont les solutions à l'étranger ?

Les présentations sont disponibles en ligne sur le site de Forum Atena :

http://www.forumatena.org/node/458

2. SOLANGE GHERNAOUTI : DEFINIR L'INFORMATION STRATEGIQUE : UNE ANALYSE COUT/BENEFICE

Solange Ghernaouti, professeur à l'université de Lausanne a cherché à donner une définition de l'information stratégique. L'essentiel des éléments figure dans les planches de sa présentation. Néanmoins, elle a insisté sur le caractère multiforme de l'information stratégique en faisant l'analogie avec les failles de sécurité. En effet, une vulnérabilité dite « zéro day » a beaucoup de valeur sur le marché car beaucoup de systèmes sont vulnérables. La valeur de la vulnérabilité diminue ensuite avec le nombre de systèmes qui bénéficient d'un correctif. De la même manière, l'information définie comme stratégique à un instant donné peut très bien ne plus l'être plusieurs mois ou semaines après. De plus, il s'agit bien d'Information qui par définition se trouve partout : PC, clef USB et même dans la mémoire des collaborateurs (voire partenaires) de l'entreprise. La définition d'un tel type d'information est donc complexe, multiforme et variable dans le temps et il convient donc de ne pas oublier de « support » d'information stratégique dans son analyse.

Enfin, le professeur concluait sa présentation par un proverbe : « les tuiles qui protègent de la pluie ont été faites par beau temps ». Cela rappelle l'importance de l'anticipation et de la définition préalable de l'information stratégique.

3. CHRISTIAN AGHROUM : LES DIFFICULTES D'UN DIALOGUE ENTRE DECIDEURS ET TECHNICIENS

Le commissaire divisionnaire Christian Aghroum, ancien chef de OCLCTIC et désormais responsable sécurité d'un grand groupe Suisse a présenté son point de vue sur la place du RSSI dans l'entreprise.

Selon lui, le RSSI ne doit pas faire partie de la DSI, mais être situé en dehors de la chaîne hiérarchique informatique pour ne pas être à la fois juge et partie. De plus, il convient plutôt de traiter la sécurité des systèmes d'information avec la sécurité du patrimoine afin de pouvoir tirer partie des signaux faibles et faire de la corrélation. Par exemple associer des informations sur le vol d'un PC et une tentative d'intrusion sur le SI afin de mieux qualifier la menace.

4. ALLAN FRIEDMAN : LES PME/PMI, QUELLES SOLUTIONS ?

La présentation d'Allan Friedman, directeur de recherche aux USA à la brookings Institution a présenté une sensibilisation à la cybersécurité pour les PME. Bien qu'à priori plutôt destinée aux PME, cette présentation a apporté des éléments sur la relation entre grands groupes et PME. En particulier aux USA, beaucoup de grandes entreprises seraient dépendantes des PME. Pour remédier à cela, le présentateur ne voit que deux alternatives : soit racheter la PME stratégique, soit travailler avec elle pour l'inciter à se sécuriser.

En réponse a une question de la salle, le présentateur a également indiqué que la réaction des entreprises à des incidents de sécurité pouvait être bien vue par le grand public et améliorer leur notoriété, à condition toutefois d'être efficace ! Il a cité deux exemples : un site de vente en ligne de chaussures américain qui a immédiatement communiqué vis-à-vis de ses clients et a mis en avant son orientation client, et le site voyages-sncf.com qui a réussi à capitaliser sur le traitement rapide d'une panne à la mi 2008 (reprise du fonctionnement normal en moins de 24h).

5. GERARD GAUDIN : VERS UNE GOUVERNANCE SECURITE PLUS MOBILISATRICE POUR L'ENTREPRISE

Gérard Gaudin, consultant indépendant a présenté les activités du club R2GS qui réalise un benchmark anonyme des évènements et coûts de sécurité sur la base des indicateurs standardisés ETSI ISG ISI.

L'objectif est de permettre aux entreprises de partager leurs indicateurs de sécurité, via deux axes : d'une part standardiser les remontées pour pouvoir les comparer et d'autre part les agréger au niveau du club utilisateur afin de les anonymiser.

6. MARTIAL IMBERTI : CAPITAL HUMAIN DANS LA STRATEGIE CYBER DES ENTREPRISES

Martial Imberti de EADS-Cassidian a présenté les travaux conjoints de la chaire Castex avec l'ANSSI autour de la gestion des profils et des formations en SSI. Un référentiel de postes SSI, défini conjointement avec l'ANSSI sera publié fin janvier 2014. L'idée est de faire une synthèse entre les 6 profils définis dans l'outil ROME de Pôle Emploi et les 50 profils différents identifiés par l'Etat Major des Armées. Le référentiel devrait comporter 17 profils.

Le groupe de travail a également brossé un état des lieux de l'emploi en SSI. Ainsi, certains profils (ingénieur développement cybersécurité, ingénieur PRA/PCA, ingénieur menaces et veille, architecte sécurité, analyste sécurité, expert forensics) correspondent à des compétences clef alors que les personnes disponibles sur le marché de l'emploi sont rares (le conférencier annonce un ratio 1 :4). A l'inverse, se pose également le problème de salariés ayant un profil très pointu, généralement hacker étique par exemple, mais non diplômés par

l'éducation nationale et qu'il convient de positionner dans les grilles salariales et d'aider à développer leurs compétences pour combler les besoins en recrutement.

Une quinzaine d'universités ont pris la formation en cybersécurité en compte, en particulier l'ENST Brest qui propose un cursus post ingénieur, ainsi que l'institut Mines Télécom qui a signé un partenariat avec Cassidian autour de deux filières : pentesteur et architecte cybersécurité. Deux cursus sont ouverts : une spécialisation dans le cadre du cursus ingénieur classique de l'ENST, ainsi qu'un cursus modulaire en formation continue du type CNAM, afin de compléter ponctuellement les compétences de salariés ingénieurs déjà en poste.

Par ailleurs, Cassidian indique être fréquemment sollicité par des clients pour des formations sur les thématiques suivantes : réponse aux incidents de sécurité, analyse inforensique sous Android, gestion de crise cyber. Cassidian juge indispensable la présence d'une plateforme transportable pour permettre de faire des TP pendant les formations. Cette plateforme doit également être reconfigurable et accessible aux stagiaires. Des LMS (Learning Management Systems) seraient bienvenus pour faire de la formation en cybersécurité et constitueront probablement une des prochaines étapes du groupe de travail formation avec l'ANSSI. Par ailleurs, sur la question de la sensibilisation des utilisateurs, Cassidian considère qu'une formation efficace doit cibler certaines populations au sein de l'entreprise et ne pas être globale.

7. PHILIPPE BLOT : LA LABELLISATION DES PRODUITS DE SECURITE ET LA CONFIANCE NUMERIQUE

Pour l'ANSSI, les moyens de détection d'attaque informatiques sont des éléments de souveraineté de l'Etat. Cela a d'ailleurs été rappelé dans le livre blanc 2013. L'appel à projets « investissements d'avenirs » cible d'ailleurs le développement de ce type de produits pour les systèmes de contrôle commande.

L'ANSSI a par ailleurs étendu son portefeuille de produits labellisés, qui s'ouvre désormais sur des produits à destination des entreprises et plus uniquement à destination des utilisateurs étatiques. Un référentiel de prestataires de détection est en cours de réalisation et est prévu pour début 2015.

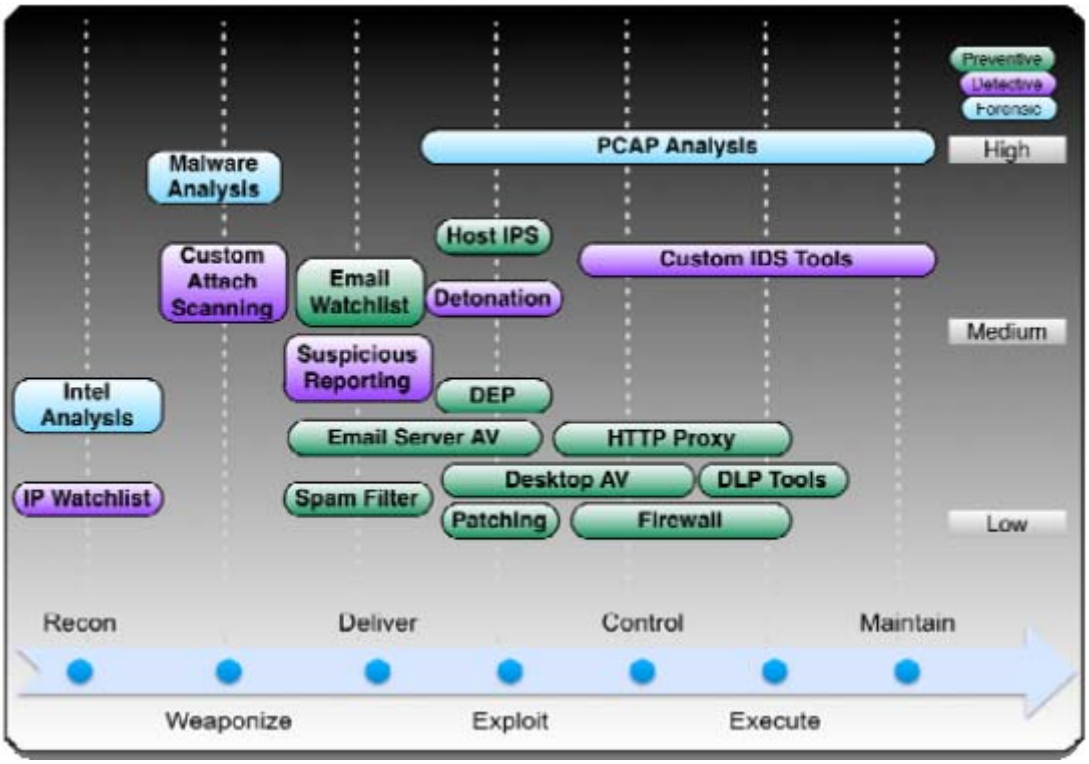
Patrick Pailloux a été nommé responsable du groupe de travail cybersécurité du programme France Numérique 2020. Un des objectifs de ce groupe de travail est de promouvoir à l'export les produits français de cybersécurité (l'ANSSI reconnait que les performances à l'export dans ce secteur sont insuffisantes actuellement). Outre ce groupe de travail, l'ANSSI va également accentuer ses efforts sur la normalisation en cybersécurité. La France travaille d'ailleurs avec l'Allemagne sur un référentiel commun de sécurisation des systèmes SCADA.

8. DAVID SENTY : LES STRATEGIES À L'ÉTRANGER (US, GB, ALL)

David Sentry, directeur des operations cyber au sein de MITRE Corporation, un think tank américain, a présenté sa vision de la gestion des menaces en cyberdéfense. Pour lui, la mise en place de patch n'est pas une bonne solution et il illustre cela en prenant une photo de gardien de but de hockey sur glace qui tournerait le dos au jeu.

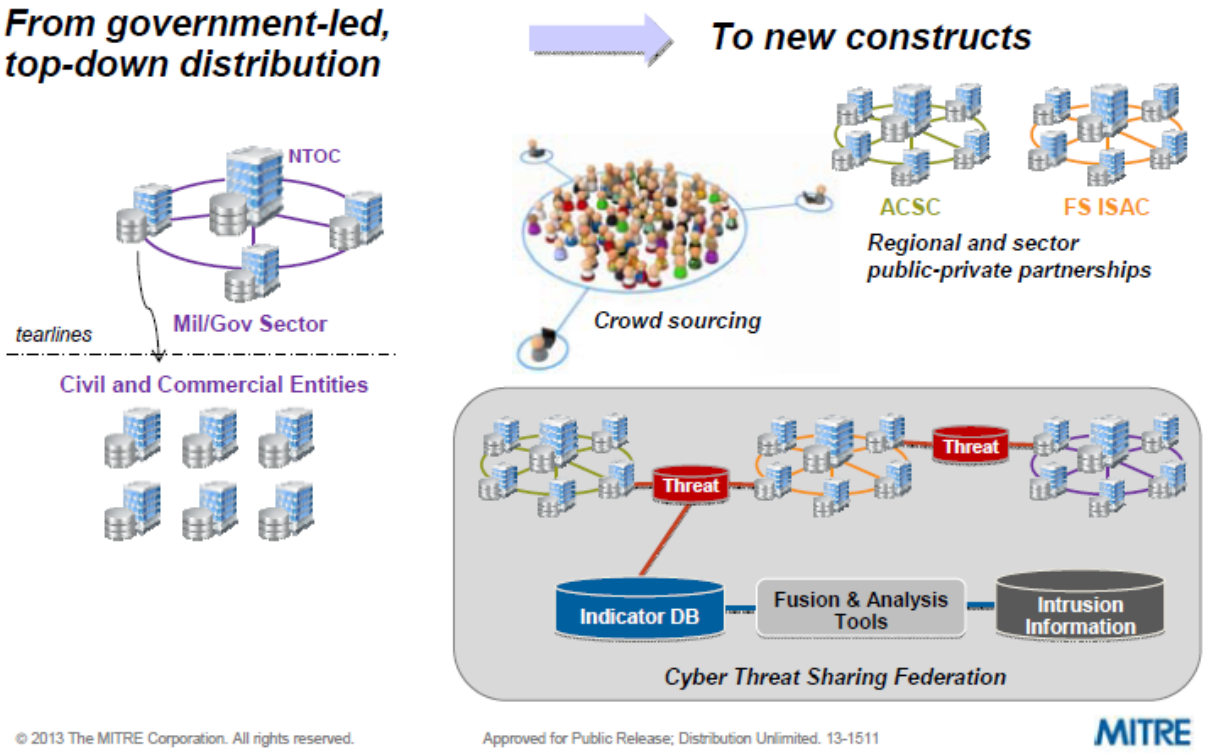
En effet, en utilisant les valeurs moyennes de la gestion de patch (voir planche 4), à savoir dans le meilleur des cas 72 heures pour patcher un système exposé à en moyenne 8 failles de type 0-day par an, le système reste exposé à au moins une faille 0-day plus de 65% de l'année. Par conséquent, la réduction de la surface d'attaque est difficile, voire impossible et il est impossible de dire qu'un système ne présente pas de vulnérabilité.

The MITRE Corporation propose au contraire une nouvelle approche, basée sur la réduction des risques, la détection et la réponse aux incidents. Pour cela, il est indispensable de partager les informations sur la menace. Les défenseurs sont demandeurs d'informations, mais en fait ils sont également producteurs au travers du retour d'expérience des cyber attaques. Il convient de comprendre les éléments de la menace via une défense en profondeur tel qu'illustré sur la figure suivante et d'avoir un modèle de partage efficace des menaces.



Il est surtout intéressant de partager les indicateurs et outils utilisés (tant pour se défendre que ceux utilisés par les attaquants), plus que les impacts. Par ailleurs, l'attribution de l'attaque est souvent un enjeu survalorisé, alors qu'en général, il importe surtout de répondre et d'arrêter l'attaque plus que d'en connaître l'attaquant. Cette information est surtout intéressante pour la connaissance des TTP (Target, Technique & Procedures).

Pour arriver à partager efficacement les informations, il convient de mettre en place de nouveaux modèles de partage. Actuellement, le mode privilégié est piloté par le gouvernement et est descendant. En cible, il semble préférable de viser des communautés basées sur le crowdsourcing, organisées en fédérations sectorielles de partage et d'analyse de l'information, tel que présenté sur le schéma suivant :



Cette présentation faisait opportunément écho aux outils normalisés de partage d'évènements de sécurité portés par le club RGS.