GS Days « Journée Francophone de la sécurité : Convaincre sans contraindre » - 3 avril 2012

Table des matières

Le 3 Avril 2012, s'est tenu aux salons de la Rose-croix, le GS Day « **Journée Francophone de la sécurité » qui avait pour thème convaincre sans contraindre » organisé par Marc Jacob.**

Avec plus de 10 conférences et ateliers.

Conférence I : « Entrée en matière par un cas pratique »

La journée a commencé par une pièce de théâtre de 45 mn basée sur un cas réel, illustrant ainsi les différents faits, enjeux, comportements, rencontrés par les protagonistes, qu'ils soient victimes ou agresseurs avec :

- Eric Doyen, RSSI de Generali et président du Club 27001
- Diane Mullenex, avocate, Ichay & Mullenex
- Philippe Humeau, consultant en sécurité, dirigeant NBS System

Une bonne préparation

L'apparence de la vérité est l'élément clé d'un détournement de fond réussi. Pour qu'une opération de détournement soit réussie, les agresseurs doivent acquérir une connaissance très fine des procédures et des intervenants dans les procédures comptables, financières et informatiques de leurs victimes. Cela suppose avoir identifié le maillon faible, acquis une bonne connaissance des procédures, du top management de l'entreprise, de points d'entrées informatiques, téléphoniques afin que le mensonge ait l'apparence de la vérité.

Identifier le maillon faible de la structure

Première étape de l'opération, le maillon faible est avant tout la victime principale. Isolée physiquement, géographiquement ou hiérarchiquement, les trois cas pouvant se cumuler, l'individu pris pour cible détient un pouvoir que les agresseurs veulent, en général un pouvoir de signature auprès d'instances financières. L'entreprise quant à elle se sent protégée par ses procédures, ses contrôles et les contrôles réalisés par ses partenaires.

Les agresseurs vont donc soumettre leur victime à un stress important, voire à un harcèlement psychologique afin d'obtenir de leur victime son adhésion. La victime finira par céder, pour ne plus être soumis, endormira son sens critique et réalisera les opérations demandées.

Compter sur l'inertie de la structure

Toute les structures présentent des forces de résistances et d'inertie. L'une des forces les plus importantes est la forte tendance des entreprises à être dans la non prise de décision qui se manifeste par l'ouverture des parapluies à la moindre difficulté. Pour reprendre un des propos tenus « *On ne va pas faire sauter le conseil d'administration pour la perte dans la nature d'un ou deux millions d'euros* »...

Une fois le lièvre soulevé et passée la « mauvaise » surprise, le principe de réalité reprend le dessus. Une fois la volonté de mettre en place des « enquêtes et audits » afin d'établir les points faibles de la structure et de l'organisation, éventuellement pointer les responsabilités. Bien vite cependant l'entreprise souhaite opérer un calcul coûts / bénéfices entre les risques qu'une nouvelle opération utilisant les mêmes modes opératoires et les investissements et réformes à mettre en œuvre pour sécuriser l'entreprise.

Conclusion de la présentation

Avant de fantasmer sur l'ingénierie sociale, des opérations simples telle que l'identification des points faibles matériels, la faiblesse des mots de passe et des procédures peuvent être menées.

Ne plus voir la sécurité comme un centre de coûts mais un levier potentiel de bénéfices. De même avoir un œil sur ses sites internet, notamment les plus anciens qui offrent souvent de failles techniques criantes notamment quand ils sont confiés à des opérateurs extérieurs. Et bien plus encore quand ils stockent des données sensibles.

Conférence II : « Sept manières infaillibles de faire condamner son RSSI **»**

Intervenants : Thiébaut Devergranne, conseil de la Société Générale qui présente les leçons retenues dans le cadre de l'affaire Kerviel.

La présentation évoque les risques juridiques majeurs, l'axe choisi est volontairement didactique. La présentation s'adresse donc volontairement aux Rssi, afin qu'ils puissent protéger leur responsabilité personnelle.

Méthode 1 : Faire de l'Intelligence économique sauvage. C'est le cas Edf/GreenPeace.

Le RSSI fut poursuivi, 1 an de prison ferme fut requis. 1,5 millions d'Euros d'amende et 700.000 euros de dommages et intérêts, soit l'intégralité de son patrimoine.

L'O.C.L.C.T.I.C. recommande que les contrats d'intelligence économique fassent l'objet d'une attention particulière et que la rédaction soit confiée à un juriste et revu par un expert. Car la rédaction trop imprécise peut être source de litiges. Le terme générique de veille pouvant être considéré comme une couverture et engager la responsabilité de l'entreprise.

Sur la base de l'article 323-1, le raisonnement du tribunal sera de dire que l'entreprise à payé pour avoir un accès frauduleux. Le recel sera quant à lui constitué par la conservation des fichiers sur un support matériel et que l'entreprise a tiré partie des informations.

http://www.donneespersonnelles.fr/les-derives-de-l-intelligence-economique

Méthode 2 : « Laisser un sentiment d'impunité, qu'il est parfaitement acceptable de commettre un délit ».

Jurisprudence du TGI de Versailles du 4 Mars 2002. « La jurisprudence et l'obligation de sécurité des données personnelles ».

« Dans cette espèce, le tribunal condamnait en effet le directeur des ressources humaines d'une grande entreprise pour avoir constitué un fichier de gestion du personnel dont une partie avait été transmise à la presse. Le raisonnement de la Cour était le suivant : il « *appartenait à X qui dirigeait la constitution du fichier d'assurer la totale confidentialité des opérations.* **La fuite des 38 documents communiqués à la presse montre qu'il n'a pas pris toute les précautions utiles** *; Il sera donc déclaré coupable de ces faits* ». Parce que le résultat n'a pas été obtenu (la confidentialité des documents), c'est donc que les moyens de sécurité n'étaient pas suffisants.

Pour résumer : la jurisprudence n'hésite pas à exiger du responsable du traitement une obligation de résultat. Contrairement à une opinion répandue, celle-ci est parfaitement normale et est la conséquence d'une interprétation traditionnelle de la loi en matière pénale. Plus une personne a de moyens, de compétences et plus les juges sont sévères. Pour aller plus loin sur ce thème voici le lien vers le blog de l'intervenant :

http://www.donneespersonnelles.fr/jurisprudence-et-obligation-de-securite-des-donnees-personnelles

Méthode 3 : Assurez-vous que le RSSI développe une mauvaise compétence des règles de droits, évitez les formations. Poussez-le à riposter contre les attaques.

L'article 122-5 rappelle que la riposte « doit être strictement nécessaire ». Peut-on faire autrement que riposter ? A-t-on un firewall ? couper la connexion, ou avertir la police. Peut-on neutraliser l'agression ? Si la réponse est positive, alors la riposte n'est pas nécessaire. En revanche, vous avez l'obligation de prévenir les instances compétentes.

Méthode 4 : Confirmez-lui qu'il n'y a aucune sanction en cas de défaut de conformité CNIL.

Vrai et Faux. Le contrôle ciblé ne se fait que sur la moitié du territoire et se concentre principalement sur les grandes zones économiques. Les sanctions sont faibles. Le risque vient plus des conséquences et non de la non-conformité en elle même.

Méthode 5 : Inutile de conserver les données de connexions.

Article 6 de la LCEN, Article 25.02.2011. Attendre que la jurisprudence se dessine pour mettre en place une politique et des actions.

Méthode 6 : Cacher les déclarations à la CNIL (sans commentaire)

Méthode 7 : Donnez-lui l'idée de faire un procès.

C'est la Jurisprudence Zataz / FLP. : La société Forever Living Products France (FlP) a pour activité la fabrication et la distribution de produits à base d'aloé vera et se place au premier rang mondial de producteur, manufacturier et distributeur d'aloé vera.

Le 2 octobre 2008, Damien B., fondateur et rédacteur en chef du site internet "zataz.com" a contacté, par téléphone, la société FLP pour l'informer d'intrusions sur un de ses serveurs, en signalant une faille de sécurité informatique, qui aurait permis ces intrusions.

A partir du 7 octobre 2008, la société FLP a constaté la publication par Damien B. sur son site internet, d'un article intitulé « Données bancaires en accès libre chez Forever Living Products France » avec, comme accroche, « *Exclusif : Le premier producteur mondial d'aloé vera avait un disque dur connecté sur internet bourré de données bancaires et informations sensibles* ».

L'article comportait en annexe une "vidéo", indiquée comme ayant été mise en ligne le 6 octobre 2008 sur le site YouTube par le site Zatazdotcom, et portait le titre « Données sensibles sur protection sur internet ».

L'article qui aurait pu passé inaperçu ou cantonné à un public ciblé a fait l'objet d'une attention particulière de la presse généraliste et grand public. Après avoir corrigé la faille, les frais engagés par FLP auprès du tribunal en expertises, avocats et frais divers (50.000 €) ont dépassé les bénéfices escomptés. FLP abandonne la procédure, mais le mal est fait, l'image de l'entreprise est atteinte.

Conclusion : La défaillance dans l'information juridique et dans l'action sont deux facteurs de risques pour le RSSI. Le manque de sensibilité juridique assorti d'un travail en vase clos, l'absence d'audit extérieurs, de mauvais choix de conseils juridiques et des contrats juridiques rédigés par les DSI, sont autant de facteurs de risques qui peuvent mettre en jeu la responsabilité du RSSI.

Conférence III : « Un tableau de bord sécurité comme outil de communication »

Intervenants : Olivier Allaire et Sébastien Michaud, Lineon

Olivier Allaire et Sébastien Michaud se sont attachés à apporter des éléments de réponse à la question « *Comment communiquer avec les partenaires privés et publics qui ne sont pas RSSI* ».

La première étape de la démarche est de définir les besoins :

- Comment communiquer avec les différents partenaires ?
- Repérer l'information synthétique importante
- Organiser le suivi des indicateurs plus périodiques
- Une visualisation des indicateurs plus ponctuels
- Les méta-indicateurs et les indicateurs nécessaires à ces différents besoins.

Répondant à des exigences techniques comme :

- La stabilité des supports graphiques
- Compréhension par les différents supports métiers.

Plusieurs méthodes permettent d'arriver à choisir ses indicateurs

- Soit de manière intuitive
- Soit de manière mathématique
- Soit par une approche réseau.

La solution proposée est la dernière, par les réseaux dit « bayésien » afin de réaliser des graphes causals, des calculs de condition.

Pour conclure, l'intérêt majeur de cette approche est la capacité d'apprentissage du modèle.

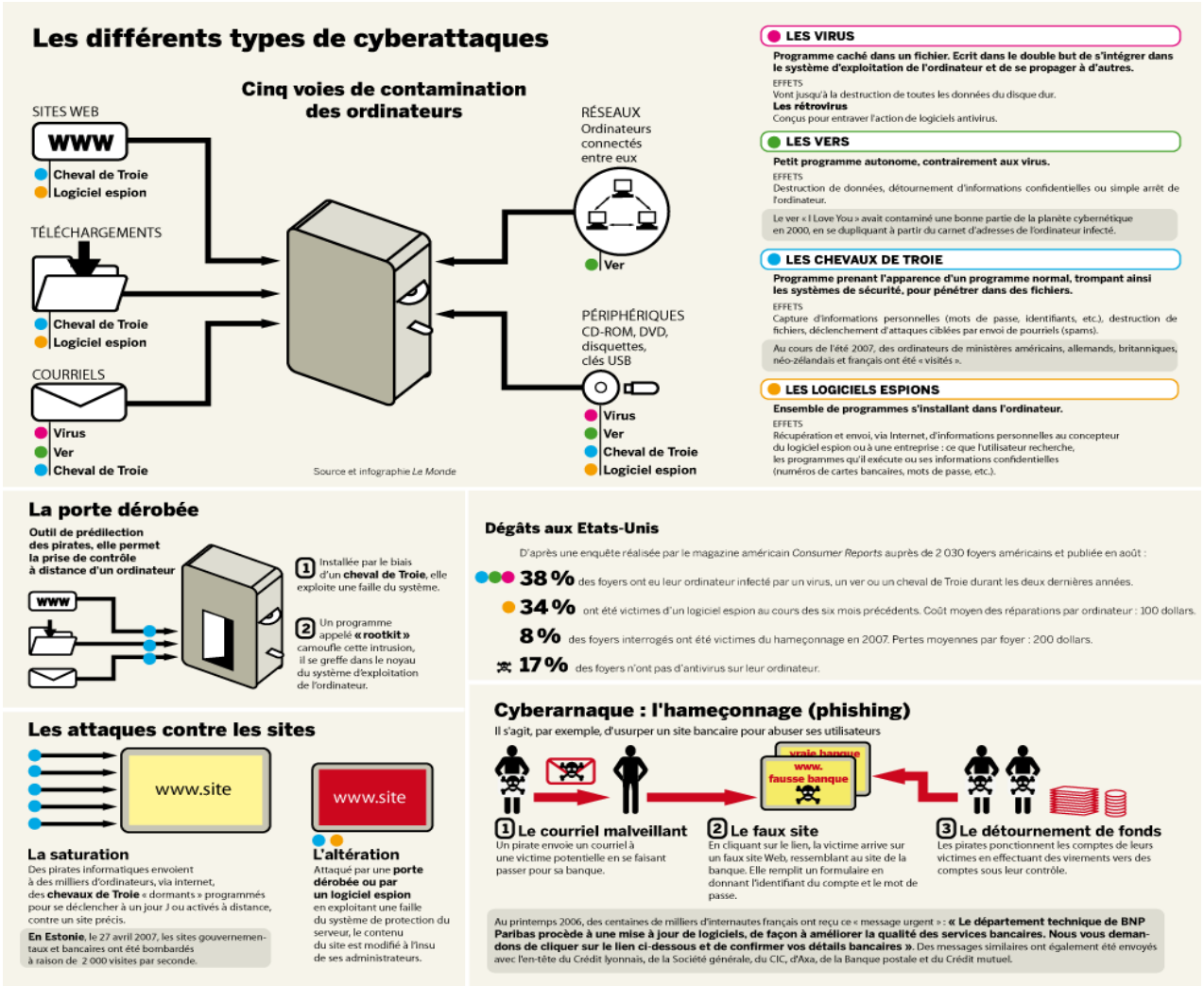
Conférence IV : « La Fédération des Professionnels des Tests Intrusifs, 12 ans après »

Intervenants Matthieu Hentzien (HSC) et Olivier Revenu (EdelWeb), FPTI.

Matthieu Hentzien (HSC) et Olivier Revenu (EdelWeb), Président et Vice Président de la FPTI ont présenté l'association, son histoire, sa mission et les principaux membres.

Née au début des années 90, l'association a eu un renouveau en 2009, suite à une prise de conscience des principaux acteurs. Après l'engouement général pour les tests d'intrusions et les dérives qui ont suivies. Les différents errements comme le dumping des prix et les tensions sur le marché ont donné à l'AFPTI l'impulsion nécessaire pour proposer une « moralisation » et une charte de bonnes pratiques.

Parmi ces différentes missions, l'association souhaite lutter contre les « prestations bas de gamme », d'être un lieu d'échanges entre professionnels et autorités (Arjel, Anssi), et aussi être producteur de communication (livres blancs, articles).



Conférence V : « Attaques ciblées : quelles évolutions dans la gestion de crises »

Gérome Billoil et Frédéric Chollet de Solucom

Présenté par Gérome Billoil et Frédéric Chollet de Solucom, cabinet de conseil en réseaux et télécoms crée en 1990. L'ambition de Solucom pour 2015 est de devenir le 1er cabinet de conseil indépendant en France avec plus de 1000 consultants.

La présentation s'attache à l'un des trois risques courus par les entreprises.

Les attaques ciblées. Elles se différencient des autres attaques informatiques par la sensibilité des informations visées. Ses auteurs sont mandatés par un commanditaire pour viser une entité particulière avec un objectif clair. Ils disposent du temps pour comprendre et analyser l'organisation, préparent des scénarii d'attaques et utilisent tous les moyens internes et externes à leur disposition, simples comme complexes afin d'atteindre leur but.

Le terme d'APT ou « *Advanced Persistent Threat* » est utilisé par la communauté sécurité pour décrire ces menaces avancées et persistantes.

Les attaques les plus courantes reposent sur des mails piégés émis à destination de personnes-clés ou encore par des attaques sur des plateformes externes (sites web) permettant ensuite des rebonds multiples sur le réseau interne pour atteindre les données de l'organisation visée.

Comment doit réagir le RSSI face a ces questions et ces menaces ?

Les questions de sécurité sont de plus en plus prégnantes au sein des entreprises. Très médiatiques, ces attaques, quand elles deviennent publiques, font le buzz. Mais de nombreuses attaques moins spectaculaires demeurent ignorées du grand public et des institutions. Or, l'année 2011 a été très riche dans le domaine, mais aussi en nouveautés, nouveaux rebonds, nouveaux canaux notamment.

D'un autre côté le renforcement de la législation, comme le secret des affaires offre aujourd'hui des moyens accrus de défense aux entreprises.

Le RSSI doit savoir catégoriser les attaques pour y répondre.

Les APT n'ont pas vocation à devenir publiques. Au contraire, la volonté de leurs auteurs est de les laisser confidentielles. De plus, l'auteur de l'attaque, par son initiative, prend un coup d'avance sur ses concurrents. En général, une entreprise sensibilisée met 4 à 6 jours pour détecter une attaque. Mais bien souvent ce sont des tiers qui la lui révèle (96%).

La sollicitation de divers canaux, Web, ingénierie sociale, parfois excessive, peut éveiller des soupçons auprès des tiers.

Un chiffre : **77 % des attaques se font avec des outils publics.**

Les impacts sur la gestion de crises :

Un constat : les réponses traditionnelles ne sont pas adaptées. Elle sont trop linéaires, séparées les unes des autres à l'image des directions (DSI et Gestion de crises). Pour Solucom, il est nécessaire de rapprocher les métiers et les parties prenantes autour d'une Direction Générale mobilisée.

Identifier les enjeux à un instant T. Les attaques ciblées peuvent être la combinaison de plusieurs attaques, elles sont alors précédées de signaux faibles.

La présence d'un correspondant informatique et liberté permettra de faire remonter l'information et de comprendre les enchaînements, de réagir et de prendre des contre-mesures, ainsi que d'informer les autorités compétentes pour accompagner l'entreprise si la nature de l'attaque venait à changer. En étant par exemple utilisée comme rebond.

L'attaque ciblée est une crise au long cours qui nécessite de prendre du recul. Pour en comprendre la finalité et définir un mode de réponse, il est nécessaire de mobiliser dans la durée les équipes et d'offrir une réponse adaptée.

Il faut anticiper le syndrome de la pyramide inversée, c'est-à-dire un sureffectif dans la gestion de crise et un sous-effectif au niveau des opérationnels.

Un des risque majeur dans le domaine est la perte de confiance dans le SI. Danger pour l'entreprise et danger pour le SI. Pour garder cette confiance, l'entreprise doit disposer de moyens de gestion de crises hors système d'information. Poursuivre par un plan de reconstruction. Faire comprendre à la direction la nécessité de faire évoluer le système d'information.

- Mais surtout abandonner le mode linéaire pour adopter un mode itératif.
- Surveiller les composants de la chaîne.
- Conserver la maîtrise de sa communication.
- Ne pas oublier de remplir une notification de fuite : nouvelle obligation qui impose aux entreprises de signaler toute fuite d'informations auprès de la CNIL et de la RGS.

L´article 38 de l'ordonnance du 24 août 2011 qui institue une obligation de notification en cas de violation de données personnelles,

(http://legifrance.gouv.fr/affichTexteArticle.do?idArticle=JORFARTI000024502894&categorieLien=id) et pour les institutions publiques, il y a le RGS (http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/).

L'ordonnance n° 2011-1012 du 24 août 2011 est très simple et peut être résumée en quelques mots :

- Obligation de notification sans délais à la CNIL de la violation
- Obligation de notification à chaque usager impacté lorsque la fuite peut porter atteinte aux caractères personnel ou à la vie privée sauf si les données sont chiffrées
- Obligation de garder à jour un inventaire de ces violations et des contre mesures mises en place

Une stratégie de réponse à moyen terme :

Évaluer son attractivité et connaître ses actifs réels.

Mettre en place des mesures avancées (ce qui suppose d'avoir conscience du secteur où l'entreprise évolue et quel est son positionnement sur le marché).

On peut alors, par exemple :

- inclure les scénarii de cybercriminalité,
- anticiper les effets des futures obligations de notifications,
- sanctuariser les périmètres sensibles et revenir aux fondamentaux de la sécurité,
- envisager des solutions plus audacieuses (comme inclure des fausses données),
- des actions plus efficaces dans les secteurs les plus ciblés.

Conclusion :

Solucom conseille :

- augmenter le niveau de protection,
- diminuer le niveau d'exposition
- ajuster le niveau de protection aux risques.

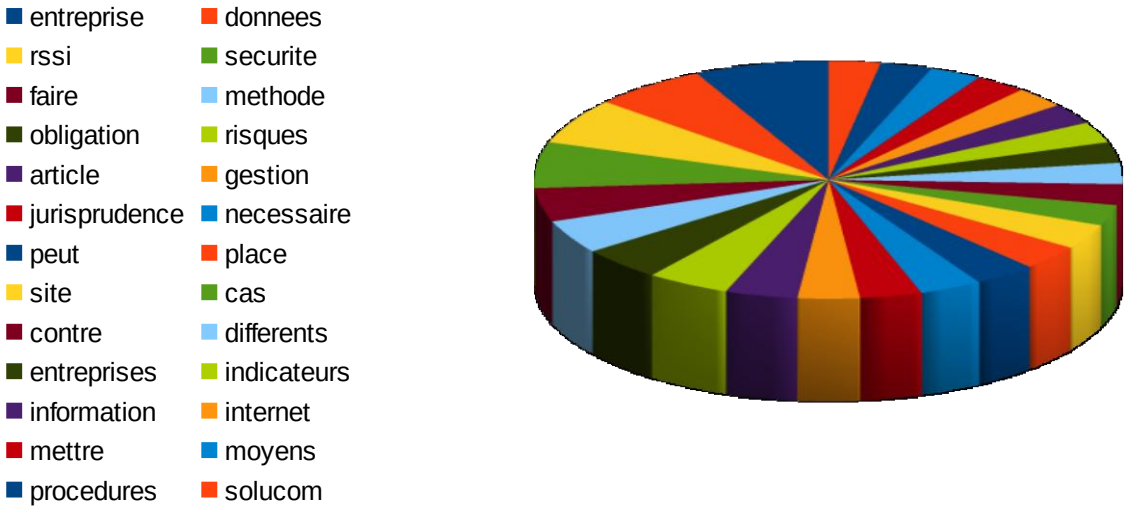
Le RSSI est un acteur majeur de la sécurité informatique,

Liens

htpp://www.linkedin.com/company/lineon
http://www.lineon.fr/
http://www.lineon.com
http://www.solucom.fr/
http://www.eads.com/
http://www.advens.fr/
http://www.devoteam.fr
https://www.sstic.org/user/lbutti/
http://www.orange.fr/
http://www.hsc.fr/
http://www.scrt.ch/
http://www.donneespersonnelles.fr/
http://www.edelweb.fr/
http://www.courtois-lebel.com/
http://www.nbs-system.com/
http://www.generali.fr/
http://www.conseils-avocats.com
http://www.ichay-mullenex.fr/

Quelques graphiques

Excel



A noter parution : Mars 2012 du numéro 19 des Cahiers de la sécurité

19 - Cahiers de la sécurité (Les) Sécurité publique sécurité privée...partenariat ou conflit ?

En consacrant ce numéro aux liens entre la sécurité publique et la sécurité privée, les Cahiers de la sécurité entendent renseigner une évolution majeure dans la société française qui dépasse d'ailleurs largement le sujet abordé. Le fonctionnement des institutions françaises réserve les principales compétences, celles qui sont appelées régaliennes, à l'Etat détenteur de l'exercice de la puissance publique. Outre les fonctions qui définissent le champ de la souveraineté, il est admis que la protection et le maintien de l'ordre public relèvent de l'État, seul garant de l'impartialité et de l'égalité qui doivent inspirer la protection des personnes et des biens contre les menaces encourues du fait d'autres individus.

Pourtant, la notion de sécurité rend plus complexe cette représentation, comme le montre Olivier Gohin dans son article sur la privatisation de la sécurité au regard de la Constitution. En effet la sécurité, telle qu'elle est définie et telle qu'elle inspire les politiques publiques spécifiques, va bien au-delà de la fonction traditionnelle de maintien de l'ordre public. Elle renvoie à un certain nombre de concepts, de stratégies d'action, face à un ensemble de menaces et de risques qui globalisent la notion de danger, tant dans les manifestations qu'il peut revêtir que dans l'espace qu'il occupe. C'est cette vision globale qu'adopte le « Livre blanc sur la Défense et la Sécurité Nationale » pour cerner les contenus d'une stratégie de défense nationale et c'est également celle qui conduit l'Organisation des Nations unies (ONU) à s'appuyer sur le concept de « sécurité humaine ».

Cette extension du champ de la sécurité dans les sociétés modernes n'est pas uniquement conceptuelle, elle traduit également un développement conséquent des missions et des actions. Il n'y a pas uniquement une redéfinition possible des limites du « régalien », il n'y a pas seulement ce que l'État doit faire, il y a aussi ce que l'État peut faire et, corollairement, le constat que ne pouvant pas tout faire il lui incombe de hiérarchiser, de définir ce qui lui revient en propre et ce qu'il peut déléguer.

Ne pouvant tout assumer, il doit partager. De l'État Léviathan à l'État stratège, il y a une évolution qui a profondément changé la société française. L'Etat s'est approprié toutes ces dimensions, car il a mesuré l'importance des enjeux qui caractérisent la sécurité privée lorsqu'elle investit un champ précédemment tenu par des administrations publiques. La création de la délégation interministérielle à la sécurité privée ainsi que la naissance du Conseil national des activités privées de sécurité témoignent de la volonté de l'Etat de ne pas abandonner ses prérogatives naturelles.
Le développement des activités de sécurité privée s'inscrit donc maintenant dans ce débat et lui apporte un éclairage utile.

André-Michel VENTRE
Directeur de l'Institut national des hautes études de la sécurité et de la justice

Résumé de la journée « Article publié dans VeilleMag »

Le 3 Avril 2012, c'est tenu aux salons de la Rose-croix, le GS Day « **Journée Francophone de la sécurité » qui avait pour thème convaincre sans contraindre** » organisé par Marc Jacob.

La journée a débuté par une pièce de théâtre présentant les principales étapes et comportements que traversent les individus et l'entreprise. Basé sur un cas réel, il illustre avant tout les bonnes et mauvaises réactions de salariés confrontés à un vol..

Porté par Eric Doyen, RSSI de Generali et président du Club 27001, Diane Mullenex, avocate, Ichay & Mullenex et Philippe Humeau, consultant en sécurité, Dirigeant NBS System les acteurs amateurs ont rempli avec succès leur mission. Un seul petit regret, le temps pour débattre fut un peu court.

Le **deuxième exposé** a porté sur les sept manières infaillibles de faire condamner son RSSI. avec comme intervenant Thiébaut Devergranne, conseil de la Société Générale et auteur d'un blog professionnel. Rappelant en **première méthode** que de faire de l'Intelligence économique sauvage est le premier moyen de se faire prendre. C'est l'affaire Edf/GreenPeace. **La deuxième méthode** étant de « laisser un sentiment d'impunité, qu'il est parfaitement acceptable de commettre un délit ». Pour Thiébaut Devergranne la défaillance dans l'information juridique et dans l'action sont deux facteurs de risques pour le RSSI. Le manque de sensibilité juridique assorti d'un travail en vase clos, l'absence d'audits extérieurs, le mauvais choix des conseils juridiques et des contrats juridiques rédigés par les DSI sont autant de facteurs de risques qui peuvent mettre en jeu la responsabilité du RSSI.

La **troisième présentation** concernait « Un tableau de bord sécurité comme outil de communication » Olivier Allaire et Sébastien Michaud, Lineon se sont attachés à apporter des éléments de réponse à la question : Comment communiquer avec les partenaires privés et publics qui ne sont pas RSSI.

La **quatrième présentation** était La Fédération des Professionnels des « Tests Intrusifs, 12 ans après », Matthieu Hentzien (HSC) et Olivier Revenu (EdelWeb), FPTI. Née au début des années 90, l'association a eu un renouveau en 2009, suite à une prise de conscience des principaux acteurs. Après l'engouement général pour les tests d'intrusions et les dérives qui ont suivies. Les différents errements comme le dumping des prix et les tensions sur le marché ont donné à l'AFPTI l'impulsion nécessaire pour proposer une « moralisation » et une charte de bonnes pratiques.

Pour clore la journée, la cinquième présentation : « attaques ciblées : quelles évolutions dans la gestion de crises » Gérome Billoil et Frédéric Chollet de Solucom

La présentation s'attachait à l'un des trois risques courus par les entreprises. Les attaques ciblées. Les attaques ciblées se différencient des autres attaques informatiques par la sensibilité des informations visées. Ses auteurs sont mandatés, par un commanditaire, pour vise une entité particulière avec un objectif clair. Ils disposent du temps pour comprendre et analyser l'organisation, préparent des scénarii d'attaques et utilisent tous les moyens internes et externes à leur disposition, simples comme complexes afin d'atteindre leur but.

--- FIN ---