Colloque ARCSI 2012

La SSI au cœur de l'IE

Metz 23 au 25 mars 2012

Les messages de bienvenue et l'ARCSI

Jean-Marc Laloy, secrétaire général de l'ARCSI et organisateur de ce colloque, remercie les différentes personnalités présentes, celles qui ont permis à ce colloque de se tenir à l'université de Lorraine (en particulier M. Eric WIES), les intervenants, les sponsors (THALES, CASSIDIAN, THEGREENBOW et DICTAO) et les participants.

Le Général Jean-Louis Desvignes, président de l'ARCSI rappelle le cheminement de cette association, qui fête aujourd'hui ses 84 ans. Initialement créée par d'anciens chiffreurs de l'armée de terre, et qui a compté parmi eux Georges Painvin, qui, en décryptant les messages chiffrés de l'armée allemande en 1918 a conduit les alliés vers la victoire, cette association s'est ouverte, avec l'arrivée de l'informatique, aux experts de la sécurité des systèmes d'information puis de l'Information. Elle s'intéresse aujourd'hui non seulement à la cryptographie et à la cryptanalyse, mais aussi aux dangers qui pèsent sur toutes les catégories de systèmes d'information y compris aux infrastructures vitales et aux nouvelles menaces telles que les malwares Stuxnet et Duqu qui peuvent s'attaquer aux systèmes de pilotage industriels. L'ARCSI s'est ouverte récemment aux étrangers en accueillant entre autres, le célèbre historien de la cryptologie David Kahn, citoyen américain et le non moins célèbre Professeur Jean-Jacques Quisquater, sujet Belge, ainsi qu'un passionné d'histoire espagnol.

Le monde de l'économie et celui de la défense qui dépendent fortement de leurs réseaux d'information, nécessitent une capacité de réaction quasi immédiate d'où l'importance de créer des cellules de veille et d'offrir aux systèmes d'Information des capacités de résilience. Aucun pays, surtout s'il est développé, n'est à l'abri d'un Tchernobyl ou d'un Pearl Harbour numérique. L'ARCSI constitue un réservoir de compétences pointues en cyber défense et en cyber sécurité, mais aussi un réservoir d'historiens, et s'ouvre aux juristes.

Une exposition itinérante sera consacrée à la cryptologie au musée des Transmissions de Cesson Sévigné, près de Rennes, dont le président de l'association des amis du musée de tradition de l'arme des transmissions, le Général Jacques Aubert était présent au Colloque. Toutes ces informations sont déjà ou seront bientôt accessibles sur le site Web de l'ARCSI en http://www.arcsi.fr.

Pourquoi le thème de l'Intelligence Economique associé à la sécurité des systèmes d'information a-t-il été choisi pour ce colloque ?

Le Président rappelle les conditions dans lesquelles s'est développée une organisation consacrée à l'Intelligence Economique dans notre pays. Parmi les mésaventures qui interpelèrent les autorités figurent l'échec commercial subi dans la vente de Mirages 2000 de Dassault pour l'armée de l'air finlandaise. Nous nous battions contre le Gripen Suédois ne voulant pas croire que les Finlandais pouvaient s'offrir le F18 américain, tout comme l'alerte donnée par un pilote français qui avait aperçu en 1940 des colonnes de chars allemands avançant vers la frontière des Ardennes n'avait pas été jugée crédible. Le système d'information le mieux conçu est inutile si les décideurs jugent l'information qu'il produit non recevable.
Le comité de la sécurité et de la compétitivité économique créé sous M. Balladur est vite tombé dans l'oubli puis, le domaine de l'IE a fait l'objet d'âpres disputes entre Bercy et la place Beauvau, jusqu'au rapport Carayon qui évoquait la nécessité au niveau gouvernemental de créer une cellule d'Intelligence Economique dépendant du SGDN. C'est ainsi qu'Alain Juillet, qui avait fait carrière dans les milieux du renseignement, s'est vu confier l'organisation d'une équipe d'Intelligence Economique en France, mais sans grands moyens.

Des cursus de formations et des cellules IE furent créées dans les grandes entreprises. Mais il s'en suivit quelques désillusions, les patrons se demandant souvent quel était le retour sur investissement de ces cellules. De nombreux cabinets spécialisés en Intelligence Economique furent ouverts souvent dirigés par d'anciens membres des services de sécurité comme on l'avait observé dans le monde anglo-saxon.

Durant cette même période ont tout de même été créés les pôles de compétitivité qui après des débuts difficiles souvent imputables à une organisation de type usine à gaz, commencent à porter leurs fruits. En septembre 2009, une nouvelle organisation a été mise en place.

L'impression est que les entreprises sensibilisées à l'intelligence économique ont surtout retenu l'aspect collecte de renseignements sur les concurrents alors que la première chose à faire est plutôt de bien gérer l'information que l'entreprise possède déjà : L'expérience et le savoir-faire ont du mal à se transmettre quand l'information ne passe pas entre les services.

Les séniors ne sont pas utilisés au mieux de ce qu'ils pourraient apporter. L'information reste cloisonnée, plutôt que d'être transmise à ceux qui en ont besoin dans l'entreprise. Mais surtout l'information doit être hiérarchisée et celle qui est essentielle, voire vitale doit être protégée et c'est à ce stade qu'entre en jeu la sécurité de l'information, mais les moyens de protection s'avèrent vite coûteux et peu utiles si on ne sait pas ce qu'on doit protéger. Les sociétés doivent s'équiper et s'organiser en proportion de ce qu'elles ont à défendre. Les PME/TPE ne savent pas en général par quel bout prendre la sécurité de leur système d'Information, pourtant elles ne sont pas à l'abri des attaques venant de l'Internet. Une petite entreprise fromagère de l'Aveyron a une probabilité assez faible de subir sur son système d'Information des attaques venant de Chine. Une grande société travaillant dans le domaine aéronautique et spatial, en revanche, se doit de mettre en œuvre des moyens de défense en rapport avec l'importance des enjeux.

L'objectif de ce colloque est précisément la sensibilisation aux dangers d'un usage des technologies de l'information et de la communication mal maîtrisé. Après en avoir cité quelques uns, le général Desvignes cède la parole à **M. Richard Vignon**, Préfet délégué pour la sécurité et la zone de défense Est, auprès du Préfet de la Région Lorraine.

Les zones de défense et de sécurité

M. Richard Vignon, Préfet délégué pour la sécurité et la zone de défense Est, auprès du Préfet de la Région Lorraine, salue l'initiative prise par l'ARCSI d'organiser, en partenariat avec l'Université de Lorraine, un séminaire sur un des sujets phares de la défense et la sécurité nationale, dans son volet de protection de l'intelligence économique, sujet hautement stratégique.

Il marque que l'État est aujourd'hui collectivement investi aux côtés des acteurs de l'économie pour les aider à se protéger et se développer.

Avant d'en venir à la sécurité des systèmes d'information, le cœur du sujet, il tient à élargir le périmètre au dispositif global de la défense et de la sécurité de notre pays.

Quatre ans après la parution du Livre Blanc, nous observons que les grandes tendances retenues se sont dans une large mesure confirmées, donnant toute leur pertinence aux orientations fixées en 2008.

L'accélération de la mondialisation en est l'axe principal, qui influence les relations et la sécurité nationales. Ainsi le contexte international reste marqué par des vulnérabilités qui pèsent sur la sécurité et la stabilité mondiale. Le risque de violence armée s'élargit avec un risque accru de conflits infra et même inter-étatiques.

Parallèlement, les menaces identifiées par le Livre Blanc continuent de peser sur notre sécurité nationale, se sont confirmées : risques naturels, risques sanitaires, risques technologiques, criminalité organisée, et bien sûr, cyber-menace.

Il n'en demeure pas moins que le contexte international et stratégique connaît toujours des évolutions profondes et quelques fois inattendues : la crise économique mondiale et les révolutions du printemps arabe en sont les exemples les plus pertinents. C'est dans ce contexte que toutes les nations industrialisées sont amenées à réfléchir sur la viabilité et la sécurité de leurs installations et sur la protection de leur patrimoine économique.

Lutter contre les différentes menaces pouvant porter atteinte aux populations ou à l'activité économique d'une région, voire de la nation, est une responsabilité fondamentale des pouvoirs publics. Cette responsabilité implique de disposer de moyens de prévention et de réponse adaptés, et d'une organisation humaine efficace. Une fois l'analyse des risques effectuée, il convient de mettre en œuvre des programmes de recherche et de développement en solutions de sécurité.

A l'échelle déconcentrée, la zone de défense et de sécurité est partie prenante du dispositif, dans son rôle de coordination des actions départementales et régionales, y compris pour l'intelligence économique. Parmi les sept zones de défense et de sécurité de France, la zone de défense EST est composée de cinq régions administratives, réunissant au total 18 départements.

Son rôle est de préparer et mettre en œuvre les plans gouvernementaux. Elle dispose pour ces missions d'un État-Major Interministériel de Zone. En matière d'intelligence économique, une section est plus particulièrement chargée des Secteurs d'Activité d'Importance Vitale, tels que l'énergie, les transports, les télécommunications, les installations militaires, les grands acteurs économiques. On dénombre en zone EST 180 Points d'Importance Vitale, répondant à des obligations de sécurité inscrites dans les plans se sécurité opérateur, les plans particuliers de protection et les plans de protection externe.

En zone EST, des vulnérabilités particulières ont été relevées au cours de visites dynamiques des sites ; elles ont fait l'objet de rapports classés «confidentiels défense». Nos services constatent que ces vulnérabilités touchent de plus en plus la sécurité des systèmes d'informations.

En effet, la cyber-menace fait partie aujourd'hui des points essentiels pouvant altérer l'économie d'un pays ou d'un grand opérateur.

Les actions de cybercriminalité sont aujourd'hui très répandues : 14 internautes à la seconde sont victimes de cybercriminalité, soit un million par jour. Cela représente un coût mondial estimé à 388 milliards de dollars (très

proche de la valeur totale du trafic de drogues estimé à 411 milliards de dollars).

La sécurité des systèmes d'information, véritables centres nerveux de notre société, est devenue un enjeu majeur. Tous les secteurs d'activités, qu'ils soient étatiques, industriels, financiers ou commerciaux, sont de plus en plus tributaires des technologies et des réseaux de communications électroniques. Ils seraient très fortement affectés en cas de dysfonctionnements graves.

Face à cette menace croissante et toujours plus insidieuse, le Livre Blanc sur la défense et la sécurité nationale a souligné la nécessité de doter notre pays d'une capacité de défense informatique active, apte à détecter et contrer les attaques. Il a recommandé que soit créée une agence nationale de la sécurité des systèmes d'information.

La création le 7 juillet 2009 de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est une étape marquante dans la mise en place progressive d'une capacité de protection renforcée des systèmes d'information sensibles français.

L'ANSSI assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. A ce titre elle est chargée de proposer les règles à appliquer pour la protection des systèmes de l'État et de vérifier l'application des mesures adoptées.

Ces mesures sont ensuite déclinées au sein de chaque ministère, en tenant compte de leurs spécificités. Le Ministère de l'Intérieur est très impliqué dans la politique publique d'intelligence économique :

- il est membre du comité directeur de l'intelligence économique : ce comité fixe les priorités d'action du délégué interministériel de l'Intelligence économique, représenté aujourd'hui par Philippe RAMON
- deux hauts fonctionnaires du ministère assistent Olivier BUQUEN, le délégué interministériel, dans ses travaux
- plusieurs directions du ministère (DCRI, DGGN, DSCP) ont un rôle à jouer, décrit par une circulaire du 1er juin 2010
- le Haut Fonctionnaire de Défense est quant à lui chargé d'animer la politique d'intelligence économique au niveau territorial.

Les préfets de département ont en charge de prévenir toute tentative d'intrusion dans les serveurs informatiques des préfectures et de la police nationale. Le réseau des préfets de région est responsable de la mise en œuvre au plan local :

- la veille stratégique et le soutien à la compétitivité relèvent en priorité des compétences des DIRECCTE qui disposent localement de chargés de mission dédiés,
- un coordonnateur régional (Sous Préfet) est par ailleurs désigné pour animer le réseau régional

Concernant la sécurité économique, la Direction Centrale du Renseignement Intérieur est l'une des pierres angulaires du dispositif. Ses missions consistent dans la lutte contre toutes les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la nation.

Elle contribue notamment à la surveillance des communications électroniques et radioélectriques susceptibles de porter atteinte à la sûreté de l'État ainsi qu'à la lutte, en ce domaine, contre la criminalité liée aux technologies de l'information et de la communication.

Les autres services de la Police Nationale, notamment ceux de la sécurité publique en charge de l'information générale; ainsi que ceux de la Gendarmerie Nationale, disposent d'une capacité importante de collecte d'informations sur la vie interne et l'environnement des entreprises dans leurs zones de compétences. Leurs maillages permettent d'évaluer les vulnérabilités de ces entreprises et de sensibiliser les opérateurs afin de préserver leur patrimoine et améliorer leur résilience.

Comme nous le voyons, et comme Monsieur le Préfet délégué Richard Vignon l'énonçait en introduction, les grandes tendances retenues par le Livre Blanc se sont dans une large mesure confirmées.

Mais les services du SGDSN, sous l'impulsion du Premier Ministre, engagent actuellement un exercice de révision de la stratégie mise en place au travers du Livre Blanc, afin de nous permettre de tirer les conclusions des actions menées jusqu'à présent et de confirmer notre démarche de prévention et de défense.

Cette révision devra prendre en compte les grandes évolutions de nos sociétés, qui impacteront nécessairement les approches d'intelligence économique et de protection des systèmes d'information.

La SSI au cœur de l'IE

M. Philippe Ramon, adjoint du délégué interministériel à l'Intelligence économique, chef du pôle Sécurité économique et affaires intérieures, présente l'historique de l'Intelligence Economique en France.

Née de l'activité de Rémy Pautrat, au sein du SGDN suite au rapport Martre au milieu des années 1990, l'Intelligence Economique a tracé son chemin en France, avec en particulier Alain Juillet, qui exerça la fonction de Haut Responsable pour l'Intelligence Economique en France auprès du premier Ministre.

Il faut souligner qu'en cas d'attaque délibérée sur les fichiers clients, de défiguration de sites Web, de falsification de fichiers, ou de destruction de données, trop souvent les petites entreprises n'ont pas pu détecter la concrétisation de la menace à laquelle est ont été confrontées avant que les dégâts ne soient visibles. Un colloque tel que celui de l'ARCSI est vraiment nécessaire pour prévenir sur l'existence des nouvelles menaces, pour sensibiliser et pour compléter l'information que nul ne doit ignorer.

M. René MENOT de l'Observatoire Zonal SSI (OZSSI), chef du Pôle Sécurité des Systèmes d'Information et délégué de l'Observatoire Zonal de la Sécurité des Systèmes d'Information de la zone de défense et de sécurité Est, nous présente l'OZSSI situé à METZ.

Le livre blanc en 2008 a préconisé la mise en place d'observatoires zonaux dans toutes les zones de défense. Dès sa création en 2009, l'ANSSI a assuré des actions de formation sur la sécurité des systèmes d'Information dans toutes ces zones de défense et chez les opérateurs d'importance vitale.

Aujourd'hui on constate une décroissance du nombre de virus, mais nette augmentation de l'ingénierie sociale. En mars 1999 a été créée une organisation qui regroupait à ses débuts des services déconcentrés de quelques ministères dans la zone Est. Cet OZSSI, issu des travaux du SGDSN existe donc depuis 13 ans, a mené 14 réunions plénières et délivré 1660 hommes-jours de formation. Il a effectué des exercices de cyberdéfense avec l'ANSSI et mené des campagnes de sensibilisation, et d'audits de la sécurité des systèmes d'information, en particulier en soutient des pôles de compétitivité de la Région Lorraine.

L'OZSSI de la zone Est évalue à plus de 1000, le nombre de contacts qu'on lui adresse chaque année pour répondre aux questions, pour soutenir la rédaction de clauses techniques des projets informatiques. René Menot rencontre souvent les correspondants sur le terrain et remonte des informations vers l'ANSSI. Une enquête semestrielle fait remonter les attentes, en particulier en matière de formation. Actuellement les formations en Infogérance et concernant le Cloud Computing sont très demandées, ainsi que des formations spécifiques sur des retours d'expérience concernant des attaques virales et des attaques sur les réseaux.

L'ANSSI écrit des directives mais chaque ministère est libre de ses orientations. La première mission que René Menot a donnée à cet OZSSI est la détection des incidents, et de la mise en relief de l'image globale de la protection des systèmes d'information de ce territoire. Un portail Web est là pour tracer les actions, mettre en commun les expertises, sensibiliser les utilisateurs. Des analyses réseaux et codes informatiques peuvent permettre de détecter si les systèmes sont vulnérables et donnent des conseils pour les mettre à niveau.

Les aspects juridiques de la protection de l'Information

Maitre Isabelle LANDREAU, avocate au barreau de Paris, spécialisée en nouvelles technologies et droit de l'entreprise traite du sujet "La cyber surveillance, quelle sécurité en interne et en externe pour l'entreprise ?".

Isabelle Landreau évoque comme actualité brûlante le RNCPF, Répertoire National Commun de la Protection Sociale, méga fichier de collecte d'informations qui aurait du être mis en place pour aider à la répression des fraudes mais qui vient d'être jugé non acceptable par le Conseil Constitutionnel car son existence a été jugée être disproportionnée par rapport aux buts recherchés. Elle évoque aussi la manière dont Mohamed Merah, l'assassin de Toulouse et de Montauban a été repéré grâce à une adresse IP laissée sur l'Internet durant les transactions autour de son scooter. La DCRI et la police judiciaire ont pu ainsi l'identifier et le localiser.

L'Internet représente un atout pour notre pays. Il a créé 700 000 emplois en 15 ans mais 5000 sociétés françaises subissent chaque année des attaques avérées. Et ce chiffre est en croissance moyenne de 17% par an.

La question est bien de savoir ce qu'on veut protéger. Il y a bien sûr les données confidentielles, dont la protection se base sur une loi de 1978. Ces données sont celles qui intéressent la défense nationale, le nucléaire et l'innovation. Il y a aussi les données intéressant le secret des affaires : données marketing, chiffres d'affaires, plans de développement, salaires, toutes informations pour lesquelles le chef d'entreprise doit limiter les accès.

La cybersurveillance en entreprise concerne aussi bien sûr les employés qui ont une obligation de loyauté envers leur employeur et ceci doit être écrit dans leur contrat de travail. Face à cela, l'article 9 du code civil impose le respect de la vie privée, et instaure une bulle de confidentialité autour de la vie personnelle de l'employé.

Isabelle Landreau apporte des réponses à des questions fréquemment posées telles que :

- Peut-on pratiquer le jeu en ligne à partir de son bureau ? : La réponse est non, l'utilisation des moyens informatiques de l'entreprise durant le temps de travail, pour de telles pratiques, peut constituer une faute grave.
- Peut-on consulter des sites pornos ? : La réponse est non, pas pendant les heures de travail. On ne peut interdire au salarié toutefois l'utilisation de son poste de travail pour accéder à des sites qui ne sont pas des sites utiles à l'exécution de ses tâches professionnelles, mais les limitations doivent être précisées dans le contrat de travail : pourcentage du temps admis, liste de types de sites autorisés...
- Peut-on dénigrer son supérieur hiérarchique ? : Non, pas à partir de son poste de travail, durant le temps de travail. Mais à l'extérieur de l'entreprise, s'en prendre à une personne de l'entreprise est autorisé, puisque c'est dans la sphère privée, mais attention aux conséquences si un délit de diffamation est constitué. Par rapport à la personne morale de l'entreprise, même en dehors du cadre de l'entreprise, le devoir de loyauté demeure.
- Peut-on participer à des Forums de discussion ? : La réponse est non si la finalité est de dénigrer son employeur. En France, on évalue à 27% les entreprises qui contrôlent l'usage des réseaux sociaux par leurs employés. Une entreprise sur deux a constaté des dérapages, une entreprise sur trois bloque l'accès aux réseaux sociaux, mais, pour cela, une autorisation de la CNIL est indispensable, sinon la mesure pourra être annulée, et les employés ne pourront être poursuivis.

L'article 1384 du code civil précise que l'employeur est responsable des faits commis par ses employés (responsabilité des commettants). Il convient de définir les règles d'usage de l'Internet en entreprise et écrire précisément qui a le droit de faire quoi, qui est le responsable de tel traitement des données et quelles sanctions seront pratiquées contre les contrevenants, avant l'application éventuelle des règles générales qui sont prévues par le droit du travail.

L'employeur a une obligation de transparence et de proportionnalité dans les mesures prises pour protéger l'information de son entreprise. Il doit informer les employés des contrôles mis en place pour accompagner leur vie professionnelle sur les lieux de travail. Par exemple, contrôler si les appels téléphoniques sont professionnels ou personnels et demander le remboursement des appels personnels est possible si les conditions légales sont remplies.

La proportionnalité indique que les moyens de contrôle mis en œuvre pour réprimer les abus restent en rapport avec ce qu'on veut contrôler. Le méga fichier de récolte des informations pour lutter contre les fraudes à la carte vitale, et qui aurait contrôlé 70 millions de personnes, a été ainsi jugé illégal. Les correspondances privées des employés sont inviolables. L'employeur ne peut ni les lire, ni les diffuser. Pour cela il convient d'installer une solution de marquage et de tout consigner dans une charte de confidentialité.

Par contre ni l'employeur, ni l'employé ne peuvent s'opposer à des écoutes, si elles sont légales. Si l'employé bénéficie d'un téléphone portable d'entreprise, le périmètre et les conditions de son utilisation doivent être précisées dans son contrat de travail.

La cybersurveillance externe s'exerce pour protéger les STAD (Systèmes de Traitements Automatiques des Données). Les atteintes aux STAD peuvent constituer des délits relevant du droit pénal et punis d'une peine maximale de 4 ans de prison et 50 000 euros d'amende.

Isabelle Landreau cite plusieurs affaires. Celle de l'EDF qui s'est introduite dans le système d'Information de Greenpeace France et qui a été condamnée pour cela par le tribunal de Nanterre à une amende de 1,5 millions d'euros pour accès et maintient frauduleux dans le STAD de Greenpeace.

Autre exemple, la société Elypsal qui voulait acquérir le portail internet Netpass.net (divertissement à caractère pornographique) de la société 3Wimedia, a menacé cette dernière de l'attaquer en déni de service si 3Wimedia n'acceptait pas cette demande d'achat. 3Wimedia a refusé et a été attaquée en déni de service. Son portail a connu une interruption de service de plusieurs jours. L'affaire ayant été portée en justice, le Tribunal de Grande Instance de Paris a condamné le gérant d'Elypsal à payer 5000 euros d'amende, et la société Elypsal a été condamnée à payer à la société 3Wimedia, 9600 € de dédommagement pour mobilisation de ses ressources humaines et 3000 € en réparation pour l'atteinte à son image.

Le vol de donnée est puni par l'article 321-1 du code pénal d'une amende de 375000 euros et de 5 ans de prison (peines maximales), mais seulement si la faute est intentionnelle. Le délit de recel de données volée n'existe pas puisqu'on ne peut voler que ce qui est matériel. Suite aux affaires Renault et Michelin, le député Bernard Carayon a soumis au vote de l'Assemblée Nationale en janvier 2011, une proposition de nouveau délit : le recel de données informatiques, et la reconnaissance comme un délit de la divulgation du secret des affaires. Cette loi pourra protéger les brevets, l'innovation, le savoir-faire. Cette proposition de loi est actuellement en attente de vote au Sénat.

Les Etats Unis ont voté une loi fédérale, dès 1996, le "Cohen Act" qui réprime le vol de secrets d'affaires d'une peine de 5 ans de prison et de 5 millions de dollars d'amende. Les peines proposées par Bernard Carayon sont très inférieurs à celles du Cohen Act.

Le Patriot Act aux Etats Unis leur confère t'il le droit aux autorités américaines de tout faire pour des raisons de sécurité nationale ? Non, l'ère George Bush est terminée. Il y a maintenant connivence entre les juges et les entreprises pour adoucir les contours du Patriot Act. De toute manière, sur les aspects sécurité de l'Information, la loi Sarbanes Oxley est plus importante que le Patriot Act.

Une question est posée pour savoir si en France, une adresse IP est une donnée à caractère personnel. La question aujourd'hui n'est pas tranchée. La cour d'appel d'Aix en Provence a répondu par l'affirmative, mais la cour de cassation a répondu par la négative. Une adresse IP caractérise bien sûr techniquement non pas une personne derrière un clavier mais le contrôleur réseau du moyen d'accès à l'Internet. Toutefois, dans l'affaire Mohamed Merah, l'adresse IP utilisée par sa mère a permis à la DCRI et à la police judicaire, par recoupements, de coincer l'assassin.

Le BYOD (Bring Your Own Device) fait interférer la sphère professionnelle et la sphère privée. La charte de sécurité de l'entreprise doit intégrer ce nouveau phénomène, s'il est mis en œuvre, mais la jurisprudence n'est pas encore étoffée dans le domaine.

Le RSSI est-il responsable des délits commis par les employés de son entreprise ? C'est le contrat qui décide, et il doit stipuler quels sont les moyens dont il dispose. C'est tout le problème des relations qui lient "le maitre et les commettants".

Les chercheurs sont parmi nous

Jean-Yves Marion, professeur à l'École des Mines de Nancy, responsable du laboratoire de haute sécurité du LORIA présente son laboratoire (Laboratoire lorrain de recherche en informatique et ses applications).

Le LORIA est un grand laboratoire de recherche avec 400 personnes dont 160 chercheurs permanents. 25 chercheurs font des travaux sur la sécurité informatique et mènent des études théoriques amonts ou plus concrètes sur la virologie informatique. Les recherches portent sur

la vérification formelle de protocoles, sur les primitives crypto et les systèmes de chiffrement appliqués à la signature numérique, sur le monitoring réseau pour détecter des attaques sur la voix sous IP, le P2P, et faire avancer la traque des pédophiles.

Ils disposent d'un laboratoire haute sécurité pour mener ce genre de recherches, en liaison avec l'ANSSI et la DGA, et décortiquer des attaques visant par exemple le vote par Internet, les réseaux sociaux, le P2P. Ce laboratoire travaille sur l'analyse morphologique des virus.

Pierrick Gaudry, directeur de recherche au CNRS, responsable de l'équipe CARAMEL du LORIA, travaille sur la théorie algorithmique des nombres appliquée à la cryptographie à clef publique.

Il évoque la factorisation de grands nombres sur laquelle est basé le RSA et qui ne permet pas de déduire une clé privée de la connaissance de la clé publique correspondante. Cette sécurité repose sur la difficulté présumée de la factorisation d'entiers de taille suffisante.

Avec le RSA, une carte bancaire insérée dans un terminal de paiement prouve son identité au terminal. L'utilisateur prouve que la carte bancaire est la sienne en entrant un code PIN. Mais la signature électronique pose une ambiguïté car elle est utilisée pour deux fonctions distinctes : D'abord pour l'authentification, ce qui est bien sa finalité, mais aussi pour engager la responsabilité de celui qui signe, et en fait ces deux notions proches, s'authentifier et s'engager, ne doivent cependant pas forcément être associées.

Pierrick Gaudry rappelle que dès 1995, des nombres entiers de 120 bits pouvaient être factorisés. Aujourd'hui on parvient à factoriser des nombres de 768 bits et la factorisation des grands nombres entiers reste toujours un des grand défit du siècle. D'un point de vue sécurité, le Web http://www.keylength.com/fr donne des conseils sur les longueurs de clés minimales à utiliser.

A une question posée par Jean-Marc Laloy sur les calculateurs quantiques qui pourraient plus rapidement factoriser les grands nombre, Pierrick Gaudry répond qu'aujourd'hui les ordinateurs quantiques n'existent pas. IBM prévoit dans sa publicité l'existence de tels calculateurs mais pas avant une quinzaine d'années et c'est encore à voir. Par contre il y a aujourd'hui des recherches qui se font sur les clés publiques "post quantiques".

Jean-Yves Marion nous présente le laboratoire de haute sécurité du Loria, et nous parle du virus Stuxnet, et comment un virus parvient à compromettre des données. Tout commence par un travail d'approche avec les techniques de l'ingénierie sociale, pour connaître les goûts de la victime. Puis il reçoit une clé USB avec des fichiers correspondant à ses goûts. Bien entendu ces fichiers sont infectés. Le malware que le fichier infecté contient va passer par une vulnérabilité d'un programme, et tout programme présente des vulnérabilités. Après la phase de pénétration, il y a la phase d'invasion où il investit le réseau et ses serveurs. Stuxnet utilisait 4 ou 5 vulnérabilités et pas toutes connues (vulnérabilités "0day") pour prendre le contrôle d'un PC sous Windows. Ensuite le malware s'installe dans la durée et lance sa charge létale. Stuxnet visait les contrôleurs Siemens d'un certain type, précisément celui qui contrôlait la vitesse des centrifugeuses de l'usine d'enrichissement de l'uranium, à Natanz en Iran. Le virus pouvait aussi communiquer avec l'extérieur pour se mettre à jour et charger de nouvelles fonctionnalités.

Stuxnet est un virus particulièrement bien conçu. Le développement de ce virus a du demander six mois avec 5 à 6 experts pour le concevoir. De plus il utilise des signatures numériques usurpées à Taïwan pour faire croire au système qu'il va infecter, que ses composantes sont légales et d'origine. La première attaque a été déclenchée en juin 2009, elle a fait rage en mars/avril 2010 et n'a été isolée qu'en juillet 2010.

Un tel virus pourrait s'attaquer à tous système SCADA (Supervisary Control and Data Architecture), et perturber la distribution d'électricité ou autres systèmes industriels. Les moyens de défenses classiques sont inefficaces devant de telles attaques.

Le virus Duqu, de la même souche virale que Stuxnet, prend le contrôle de PC pour en subtiliser de l'information qu'il chiffre et place dans un fichier jpeg avant de l'envoyer, par la messagerie du système infecté, au destinataire. Ce virus a été découvert début juin 2010.

Les sensibilisations de la gendarmerie nationale

Le commandant Rémy FEVRIER de la Gendarmerie Nationale, chargé de mission Intelligence Economique et Sécurité des SI à l'Etat-major de la Région de Gendarmerie Nord-Pas-de-Calais nous présente les actions de sensibilisation à la protection de l'Information et à l'intelligence économique qu'il mène avec la gendarmerie nationale en particulier en direction des PME.

96% des entreprises en France comptent moins de vingt salariés. Une grande majorité d'entre elles ne prend pas les précautions indispensables pour sécuriser leurs informations. Sensibiliser l'ensemble des entreprises demeure donc une gageure. S'il peut exister une certaine méfiance entre les PME et les grands groupes en matière de partage de l'information, les collectivités territoriales constituent un des vecteurs majeurs susceptible de favoriser une collaboration plus étroite entre les différents acteurs économiques locaux.

Pourtant, les petites sociétés sont aussi la cible d'attaques numérique. Le commandant Février cite ainsi le cas d'une petite société du sud de la France et employant une quarantaine d'employés, victime d'une campagne de dénigrement massive via Internet, bien que son activité soit limité à la production de fruits. Cet exemple montre que, contrairement, à une opinion généralement répandue, ce ne sont plus ni la taille ni le secteur d'activité de l'entreprise qui en font une cible, mais plutôt son niveau de compétitivité et sa performance.

Avant la chute du « rideau de Fer », on peut globalement considérer qu'une quinzaine de pays occidentaux (Japon compris…), se partageaient l'essentiel de la croissance mondiale : ils sont aujourd'hui 150. Nous avons donc changé d'ère en matière de compétition économique et pour faire face à ces mutations majeures, certaines entreprises sont de plus en plus tentées d'avoir recours à des procédés bien éloignés de l'idéal concurrentiel (déstabilisation d'entreprise, rumeurs, désinformations…)

Bien que certains pays étrangers mènent depuis longtemps des politiques structurées de récupération de données économiques stratégiques, force est de constater que plus de la moitié des vols d'informations stratégiques (60%), sont le fait d'une concurrence strictement hexagonale.

Au vu de l'expérience acquise par la Gendarmerie Nationale, on constate que la plupart des PME sécurisent mal leurs informations stratégiques. Ainsi, sans même chercher à pénétrer le SI d'une entreprise, la simple récupération des feuilles de « paperboard » usagées permet la plupart du temps d'avoir accès à de nombreuses informations confidentielles vitales pour la pérennité de l'organisation (plan stratégique de lancement d'un produit, projet de fusion-acquisition ou d'OPA, domaines d'investissements…).

Parallèlement à un développement croissant de l'ingénierie sociale, certaines organisations de type mafieuses se sont spécialisées dans l'usurpation d'identité numérique ou le vol d'informations via Internet. En effet, celles-ci misent sur une coordination judiciaire internationale encore insuffisante pour commettre des délits encore bien moins sévèrement réprimés qu'un vol qualifié ou *à fortiori*, qu'une attaque à main armée.

De nombreux dirigeants d'entreprise ne prennent pas suffisamment en compte les risques de pertes ou de vols d'informations. Ces derniers considèrent, par exemple, qu'un wagon de train ou qu'un hall d'aéroport ne sont que le prolongement de leur bureau. Or, comment être certains que d'autres voyageurs ne sont pas des concurrents potentiels ? On peut citer, à ce propos, le cas d'une entreprise ayant envoyé plusieurs de ses cadres, faire des allers-retours en TGV la veille d'un salon international durant lequel l'ensemble des principaux acteurs mondiaux de son secteur d'activité étaient présents : la récolte fut inespérée

Le conseiller à la sécurité nationale américain a récemment admis, pour la première fois, que les menaces numériques constituaient le principal danger pour les Etats-Unis, devant les attaques terroristes… La délinquance informatique va continuer à croitre. De même que la défiguration d'un site Web ne pose pas de problèmes particuliers, la déstabilisation d'un produit peut entamer la crédibilité d'une société. Ainsi, un simple « post » sur un site fréquenté peut avoir des répercussions directes sur le niveau de vente d'un produit…

Deux autres dangers sont enfin à relever : d'une part les risques inhérents aux contrôles douaniers lors de voyages à l'étranger (plusieurs cas de vols de données contenus dans des disques durs de cadres supérieurs ont été recensés) et d'autre part l'ensemble des risques liés au vol d'un disque dur de photocopieur, rendu d'autant plus problématique qu'aujourd'hui ces derniers sont de plus en plus multi usages et font également office d'imprimante, de scanner ou encore de fax…

Jean-Louis Desvignes précise que durant la guerre froide, durant 6 à 8 ans, toutes les dépêches entre l'ambassade de France à Moscou et Paris étaient régulièrement lues par le KGB.

Les saynètes commentées de Philippe Wolf

M. Philippe WOLF Conseiller du Directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et qui fut Directeur du Centre de formation à la sécurité des systèmes d'information (CFSSI) de cette agence, nous présente des saynètes, réalisées en 2005, intitulées "Bienvenue dans la SSI". Il nous commente pour chacune d'elles la réalité des cybermenaces en 2012.

Le premier film est sur un boitier équipé d'un logiciel furtif pour aspirer de l'information, qu'une femme de ménage place sur un PC pendant l'absence de son propriétaire sorti quelques minutes prendre un café en laissant son poste sans surveillance.

Le deuxième tourne autour de la corruption, le troisième avec pour titre "piège sur l'Internet" porte sur l'insécurité des smartphones, le quatrième "des souris et des virus" montre comment on vole une information et le dernier montre que même les malwares sont signés.

En commentaire, Philippe Wolf conseille d'écouter le discours de Patrick Pailloux prononcé aux assises de la sécurité, au sujet de l'hygiène informatique, et demande de méditer sur le Wysinwyg (What You See Is Not What You Get).

L'université de Lorraine et le CLUSIR Est

M. Éric WIES, Membre du conseil d'administration du CLUSIF et représentant du CLUSIR – Est, responsable informatique de l'Unité de Formation de Recherche en Mathématiques Informatiques, Mécanique et Automatique de l'Université de Lorraine, parle de la fuite d'information.

Il n'est pas possible de détecter toutes les failles, celles des PC mais aussi celles des tablettes et des smartphones. De toute manière, détecter une faille c'est bien mais appliquer un correctif, c'est mieux.

Les menaces portent sur la perte de données, sur l'intrusion dans les réseaux d'entreprises et il n'est pas toujours besoin pour cela d'attaque le système d'authentification par force bute. Si on a besoin de connaître un mot de passe, il suffit parfois de le demander gentiment.

Des contre-mesures existent en particulier de chiffrement des informations. Eric Wies donne plusieurs exemples

croustillants, comme la Cour d'appel de Metz qui avait établit un portique d'accès. Mais le personnel ne passait pas par le portique, les hackers non plus. Un étudiant s'est plaint que sa clé USB ne marchait pas. Pour l'aider le service support a essayé sa clé sur un autre PC, elle ne marchait pas. Il l'a essayée alors sur le PC d'administrateur, avec tous les privilèges. Le ver que contenait cette clé s'est repandu sur tout le réseau.

Des vidéos d'Action Discrète sont passées. Des comédiens, par caméra invisible filment des tentatives pour pénétrer les locaux de grands journaux et tout enregistrer.

L'une dans les bureaux de Libération, sous prétextes de filmer les locaux à destination de "Google Inside". Tout comme Google Street, le but était de rendre visible sur l'Internet, la cartographie de l'intérieur des bureaux. Ca avait l'air de très bien fonctionner. Le personnel avait l'air tout fier qu'on prenne en film leurs locaux. Une employée, leur dit même "voulez-vous que je quitte mon bureau pour vous laisser filmer ?", la réponse est "oui, ce serait mieux ;-)).

Dans une autre, les comédiens se font passer pour des agents de la DCRI annonçant qu'il venait tout simplement poser des caméras pour contrer des journalistes peu scrupuleux, et on les laisse faire.

Dans une autre, au Nouvel Observateur, sous couvert de pratiquer des tests hygrométriques, les acteurs posent des caméras un peu partout dans les locaux. Là le personnel s'en étonne, l'un des comique dit alors à l'autre "Allez, on n'insiste pas, on décroche !".

Enfin la cerise sur le gâteau, déguisés en Pères Noël, les comiques investissent le journal Marianne pour déposer en cadeau pour le personnel des arbres de Noël en fait bourré de micros et de caméras et font également de petits cadeaux : des clés USB "dernière génération" et ils précisent même que ces clé peuvent dupliquer l'intégralité d'un disque dur en une seconde, et les comiques le prouvent en branchant leur propre clé USB sur les ordinateurs du personnel.

Si le personnel est si naïf et si facile à influencer, que faire pour éviter la fuite d'information sensible en dehors de l'entreprise ? Le mieux est de sensibiliser dès le plus jeune âge, dans les lycées et collèges.

La sécurité physique

En préambule, le **Colonel Jean MORNARD**, directeur régional de la protection et de la sécurité de la défense de la région Est, a présenté à grands traits son service. Outil à la disposition du ministre de la défense pour la protection des capacités de la défense, la Direction de la protection et de la sécurité de la défense (DPSD) inscrit au nombre de ses priorités de premier rang la protection du patrimoine industriel et technologique des 2 000 entreprises sous contrat avec le ministère de la défense.

Dans ce cadre, elle réalise des actions d'information, de sensibilisation, d'audit et de conseil en mettant l'accent sur la connaissance et l'application de la règlementation relative à la protection des informations sensibles. Pour l'exécution de ses missions, la direction régionale de Metz dispose d'un réseau de cinq postes répartis dans les capitales des cinq régions économiques de l'Est de la France (Alsace, Bourgogne, Champagne Ardennes, Franche-Comté et Lorraine).

Partie constitutive de son action au profit des entreprises, la protection physique constitue une expertise spécifique de la DPSD. Centrée sur l'infrastructure et l'équipement matériel des implantations à protéger, elle touche également à l'ensemble des domaines permettant le stockage, le transport et l'utilisation des informations sensibles et implique une attention particulière portée au facteur humain, qui occupe le centre des raisonnements et des actions. Ensemble cohérent de mesures d'ordre pratique, la protection physique débute par l'identification précise de l'objet à protéger, processus relevant de l'entreprise elle-même et à partir duquel seront définies les mesures concrètes à appliquer pour la conception ou la modification des zones concernée, leur équipement en moyens adaptés et la gestion des accès et de la circulation des données classifiées.

Au plan pratique, l'économie générale du système de protection physique doit prévoir une répartition différenciée et progressive des moyens entre les trois cercles successifs du dispositif à mettre en place. A la périphérie (1er cercle) de l'implantation (enceinte extérieure), priorité sera donnée à la détection, le freinage relevant plutôt de la périmétrie (2ème cercle) de l'emprise (murs extérieurs du ou des bâtiments à protéger) et l'interdiction d'accès se concentrant sur les locaux intérieurs (3ème cercle) abritant le patrimoine à protéger. Quels que soient les solutions matérielles et techniques adoptées, ils s'inscriront dans une succession d'effets combinant la détection de la tentative d'intrusion (caméras, détecteurs volumétriques ou de chocs, alarmes, etc.), le freinage de la progression (grillages, barreaux, murs, armoires fortes, etc.) et l'intervention sur les lieux (société de gardiennage, police). Le dispositif devra par ailleurs être entretenu et testé régulièrement.

Au-delà de cette organisation conceptuelle et technique, le facteur humain demeure l'élément décisif. Aucune politique ou mesure technique de protection ne peut être efficace sans la participation active et raisonnée des personnels de l'entité concernée. Une chaine de responsabilité claire et connue de tous est un préalable indispensable. De même, la sensibilisation régulière et adaptée de chaque catégorie de collaborateurs susceptibles de détenir ou d'accéder au patrimoine sensible est nécessaire, en particulier en ce qui concerne les cadres destinés à entretenir des contacts extérieurs. En outre, la gestion des accès (filtrage, identification, accompagnement) par des personnes extérieures (visiteurs, stagiaires, sous-traitants, etc.) ne doit pas être négligée.

L'ensemble de ces dispositions n'aura de valeur que si leur rapport coût/efficacité demeure acceptable par l'entreprise (an prenant en compte le coût d'une éventuelle intrusion réussie).

Les démonstrations des experts de l'ARCSI

Un brillant expert de l'ARCSI mène la danse pour prouver qu'il y a toujours moyen de contourner les moyens mis en œuvre pour assurer la sécurité de l'information.

Une petite puce programmable (Teensy ou mieux Teensy++) à mettre dans une clé USB ou une souris permet de lancer automatiquement un programme exécutable qui se situe sur la clé.

Stéphan Leberre, autre brillant expert de l'ARCSI, précise qu'un PC dont le disque est entièrement chiffré (par exemple par Truecrypt mais dont la partition est ouverte peut être l'objet d'une attaque. Dans sa mémoire vive, les clés AES gardent une forte entropie. Si on recueille la RAM du PC, durant quelques secondes, les informations sont conservées dans la mémoire. Si on refroidit la RAM, par exemple avec une bombe pour nettoyer l'écran et en soufflant dessus pour faire baisser la température, on peut espérer conserver les données en mémoire vive durant une heure.

Donc le PC volé et la mémoire vive conservée, on peut utiliser passware qui donne la mémoire image de la RAM, le fichier qui contient la partition mémoire déchiffrée. Avec Passware, on récupère les clés de chiffrement dans la RAM, et ... on peut déchiffrer le disque.

Donc, par soucis de précaution, faut-il obliger les utilisateurs à éteindre leur poste de travail pour altérer leur RAM, dès qu'ils ne s'en servent plus ? C'est le meilleur moyen de se mettre tous les utilisateurs à dos ;-)

Il nous est démontré ensuite l'utilisation de l'outil "Havij" qui réalise des injections SQL dans les applications Web. On peut récupérer le couple utilisateur/mot de passe. Le mot de passe est haché mais une requête à google et on peut espérer obtenir le password en clair à partir de son empreinte qui est le paramètre qu'on entre dans Google (ou dans un autre moteur de recherche). Si le compte était celui de l'administrateur, banco pour le mot de passe !

La journée bien remplie s'achève. Rendez-vous pour le 8eme colloque de l'ARCSI (à Toulouse ?).

Gérard Peliks
Membre de l'ARCSI
Expert sécurité
Cassidian Cyber Security