ifie
Institut Français de l'Intelligence Economique

Newsletter
n°19

Sommaire

édito

L'IFIE renouvelle la présentation de sa newsletter en choisissant un thème de réflexion par mois décliné en plusieurs rubriques : un article d'actualité, quelques interviews d'experts, et des brèves portant sur les événements en cours.
La problématique retenue pour le mois de mai est celle de la sécurité informatique.
Une réflexion d'actualité puisque Michèle Alliot-Marie, Ministre de l'Intérieur a dévoilé, le 14 février 2008, le nouveau plan d'action du gouvernement en matière de cybercriminalité.
Il est vrai que ces dernières années, les entreprises et les Etats ont pris conscience de leur vulnérabilité. Les notions de sécurité et de défense ont beaucoup évolué en raison notamment de l'explosion des nouvelles technologies, des migrations et des échanges internationaux.
La micro-informatique, en particulier Internet, est devenu le terrain de prédilection des pirates informatiques, des pervers, des virus et des spam en tous genre.
Devant les conséquences, parfois graves, que peuvent provoquer ces actions pour une entreprise ou un Etat, il est utile d'approcher les moyens utilisés par les hackers pour mieux comprendre les actions de défense à mettre en place.

André Added

Agenda

28-29 mai — **I-Expo 2008**
Porte de Versailles - Paris

Organisé par le GFII, l'ADBS et Spat.
Le rendez-vous incontournable pour rencontrer les prestataires en intelligence économique. Des conférences et ateliers pour s'informer sur les avancées des logiciels et les pratiques de l'IE.

Plus d'infos sur www.i-expo.net

29 mai — **Remise du Prix COGENIE 2008**
i-expo - Porte de Versailles

Organisé par le magazine RIE, le prix sera remis à 12h30 à la suite de l'atelier : Le processus collaboratif au sein de la veille.

Plus d'infos sur www.i-expo.net
ou www.riemag.com

10 juin — **Petit-déjeuner de lancement du livre : Les nouveaux territoires de l'IE**
ENA - Paris

Livre collectif et novateur édité en partenariat avec l'ACFCI.

S'inscrire sur le site www.ifie.net

12 juin — **5ème journée franco-suisse de l'intelligence économique et de la veille stratégique**
Neuchâtel - Suisse

Organisé par la Haute école de gestion de Genève, l'IUT de Besançon et la Haute école de gestion Arc.
Thème : La gestion des risques.

Plus d'infos sur le site de l'IFIE, rubrique événement

4 juillet — **1ère Université d'été de l'intelligence économique du CED**
MINEFE - Paris

L'IFIE est partenaire de cet événement de premier ordre, sous le haut partonage d'Alain Juillet. Elle aura pour thème : « La France, les Etats francophones et l'Europe sont - t'ils des marchés conquis?»

Plus d'infos sur le site de l'IFIE, ou contact@ifie.net

ifie Institut Français de l'Intelligence Economique
Newsletter n°19

Bilan 2007 de la Cybercriminalité

Attaques de plus en plus subtiles et diversifiées, tel est le bilan 2007 de la cybercriminalité du CLUSIF, le Club de la Sécurité de l'Information Française. Certes, la fraude aux cartes bancaires et l'espionnage industriel restent des grands classiques. Mais les mondes virtuels, l'exploitation des failles de sites web, la déstabilisation des entreprises voire des Etats sont désormais en ligne de mire.

Association de professionnels indépendante, le CLUSIF [1] a pour but la sécurité de l'information pour les entreprises, de la TPE à la multinationale, ainsi que des collectivités publiques. Le CLUSIF rassemble déjà plus de 300 organisations.
Déjà, en 2006, son bilan relevait le plus important vol de données personnelles connu à l'heure actuelle : la fuite de 94 millions de numéros de cartes bancaires due à une faille informatique des systèmes de TJX [2]. De son côté, le grand courtier américain TD Ameritrade a été victime de pirates basés en Europe de l'Est et en Asie qui ont infiltré 6 millions de dossiers bancaires. Toujours aux États-Unis, un administrateur de bases de données a détourné et revendu plus de 8 millions de dossiers clients.

Les cybers crimes les plus visibles

En 2007, le marché le plus visible reste le « carding » c'est-à-dire le piratage des cartes bancaires avec une technique éprouvée : un petit boîtier électronique, aux mains d'employés de magasins indélicats, copie les cartes à l'insu de leur titulaire. Les données bancaires sont ensuite revendues, notamment sur des forums virtuels. Les gains et le blanchiment d'argent passent par de nombreuses sociétés de ventes virtuelles générant de faux achats mais de vraies transactions. Des entreprises financières spécialisées dans le transfert d'argent, comme la Western Union, permettent également de transférer des fonds à des particuliers. L'année dernière, des hackers français ont été arrêtés dans une affaire internationale de cartes bancaires. La fraude liée au piratage de ces cartes a été chiffrée à 235 millions d'euros, soit 0.07 % des transactions effectuées dans l'Hexagone [3].

Les mondes virtuels en ligne de mire

D'après le CLUSIF, ce genre de vol ne suffit plus au bonheur des pirates. Les attaques sont nettement plus diversifiées. D'ici à 2011, 80% des internautes vivraient une seconde vie dans un univers virtuel [4]. Ces nouveaux mondes, réseaux utiles d'échanges personnels ou professionnels, deviennent des cibles de choix pour les impostures, les mauvaises rencontres et les vols d'identité, qui eux, ne sont pas virtuels. Les millions d'inscrits dans ces réseaux courent des risques d'autant plus importants que les données personnelles sont très précises et abondantes.
De même, le développement exponentiel des jeux en ligne multi-joueurs appâte le malfrat. World of Warcraft, (WoW) suit ainsi une pente quasi verticale avec plus de 9 millions d'inscrits entre octobre 2004 et août 2007, soit 2 millions d'abonnés tous les six mois ! Sur Second Life, 1,5 million de dollars changent de main chaque jour. Des chiffres pourtant dérisoires par rapport à la Corée qui compte 60 millions d'inscrits !
Dans ces mondes où chaque joueur crée son personnage, gagner et dépenser de l'argent sont les deux activités essentielles. De quoi susciter de nouveaux appétits pour les vols d'identifiants et leur exploitation : chevaux de Troie, virus, Phishing [5], bots [6] et exploitation d'individus [7].
Un bel exemple de Phishing : en copiant un site, un adolescent hollandais de 17 ans a récupéré l'identité de joueurs, volant des meubles virtuels pour 4000€, ceux-ci bien réels !

Une nouvelle forme de déstabilisation : l'attaque en réputation

CastleCops, une organisation américaine très efficace pour lutter contre les logiciels malveillants, a été l'objet d'une attaque particulièrement virulente [8].
L'ampleur des moyens mis en œuvre témoigne d'ailleurs de la crainte qu'inspire ce genre d'entreprise aux malfrats.
CastleCops a été mitraillé durant près d'un mois de DDoS, Déni Distribué de Service [9] : des milliers de machines zombies empêchaient toute connexion au site.
Vite maîtrisés, les pirates ont choisi une stratégie plus subtile. Après avoir mis la main sur des comptes PayPal,

1- Bilan 2007, livré en janvier 2008. Source: www.clusif.asso.fr.

2- TJX est un groupe nord-américain détenant plusieurs chaînes de distribution. Au Canada : HomeSense et Winners, Aux Etats-Unis : AJ Wright, Bob's Stores, HomeGoods, Marshalls et TJ Maxx. Au Royaume-Uni, TK Maxx.

3- www.zataz.com/news/14292/carding-credit-card

4- D'après Gartner, firme américaine de consulting

5- Le phishing, ou hameçonnage, permet aux pirates informatiques de récupérer des informations. Un mail usurpant l'identité d'une entreprise invite l'internaute à se connecter pour mettre à jour les informations le concernant.

6- Bot, diminutif de robot désigne un personnage contrôlé par l'ordinateur. Il simule le comportement d'un joueur humain.

7- L'exploitation d'individus par le « gold farming » consiste à récolter un maximum d'argent virtuel ou d'objets dans un jeu multijoueur, pour ensuite procéder à un échange contre de l'argent réel. Tout comme dans l'industrie textile asiatique, de grands fournisseurs mondiaux de services pour les joueurs exploitent des adolescents pour récolter de l'argent virtuel. Ils travaillent 12 heures par jour, 7 jours sur 7, payés 25 cents de l'heure.

8- Le programme de CastleCops aurait empêché l'année dernière la perte de plus de 150 millions de dollars,

9- Surcharge de serveur informatique

les malfrats reversaient à CastleCops l'argent volé sous forme de faux dons allant de 1 à 2800 dollars. Cette attaque en réputation a fait coup triple : colère des internautes, soupçons égarés, image ternie.
Mais avec l'aide de la Police judiciaire fédérale (FBI) et de PayPal, cette attaque s'est retournée contre les escrocs. CastleCops a en effet collecté une masse d'informations sur les criminels qui, depuis, sont poursuivis.

Cyber guerres

On peut également imaginer que les attaques en réputation déstabilisent l'économie d'un pays.
Le 24 février 2007, les Argentins apprenaient par la presse que 1000 stations services étaient privées de livraison de combustible. Un hacker les aurait effacées du site internet du secrétariat à l'Énergie. Répercutée en boucle par les médias et dans les sites web, l'information, « la distribution nationale d'essence paralysée par un pirate », n'a fait qu'accroitre la panique des automobilistes et des autorités. Vérification faite, il n'y a eu ni piratage, ni erreur, mais effacement volontaire parce que ces stations n'étaient pas réglementaires. Mais la rumeur est tenace…. Et semble être tombée à pic. En remontant à la source, on s'aperçoit en effet que la presse a été informée par la Fédération des entreprises de combustibles de la République Argentine, la FECRA, laquelle est en conflit avec les autorités. Les professionnels du secteur avaient, peu avant, fait état de leur projet d'une action de force auprès du Secrétariat à l'énergie.
Le 27 avril dernier, les sites officiels estoniens ont été victimes d'attaques de dénis de service empêchant toute connexion. Faut-il y voir la main du Kremlin? L'offensive, dangereuse pour le pays, a été menée après avoir décidé d'abattre un monument à la gloire de l'armée rouge…

Espionnage industriel

De son côté, l'espionnage industriel empire d'année en année, avec la particularité d'être souvent le fait des salariés. Chez McLaren et Ferrari, plusieurs centaines de mails et de SMS ont été échangés entre deux responsables techniques. Reconnue coupable d'espionnage, McLaren s'en est sorti avec une amende record de 100 millions de dollars, l'exclusion du championnat du monde des constructeurs et une image ternie.
Lors d'une 2ème affaire, c'est au tour de Mac Laren d'accuser Renault.Un de ses anciens cadres, embauché chez son concurrent, aurait communiqué des documents confidentiels.
De même, un ancien chercheur chimiste de DuPont a téléchargé 22000 résumés et 16000 documents contenant des secrets de fabrication, pendant qu'un ex-employé de Duracell engrangeait des documents de recherche sur les piles AA pour les vendre au plus offrant.

Des attaques très sophistiquées

Près de deux tiers de pages web seraient infectées par la technique de l'Ifram. Ce procédé consiste à insérer dans un page web légitime un autre page web malveillante. Les pages contaminées redirigent discrètement les visiteurs sur un site web piraté, lequel infecte les ordinateurs des malheureux internautes connectés.
Une attaque menée sur des sites italiens a infecté plus de 1000 pages de sites légitimes: mairies, agences pour l'emploi, offices de tourisme… Une grande partie des pages étaient hébergées par l'un des grands fournisseurs de services Internet italiens.
Vendus entre 400 et 1000 dollars, les outils de piratages sont simples à installer et redoutablement efficaces. MPack développé par un groupe russe implante des Iframe piégés dans un serveur web afin d'infecter automatiquement les visiteurs. N404 a infiltré le site de la Bank of India en août 2007. NeoSploit celui de Monster.com.
Plus vicieux sont les réseaux «Botnet», l'arme de choix des cybercriminels. Il s'agit d'un réseau d'ordinateurs zombies contrôlés par des pirates informatiques à l'insu de leur utilisateur. StormWorm apparu en janvier 2007 s'est propagé par mail, en invitant l'utilisateur à se connecter sur un site piégé pour lui voler ses données personnelles. Salué par un attrayant «Remember me ?» l'internaute reçoit un message chargé d'un virus troyen. En quelques jours, des milliers d'ordinateurs peuvent être sous contrôle.
Il serait possible de louer un réseau Botnet de 1 500 000 PC pour la modique somme de 350$ par semaine ! De quoi conduire en toute impunité une campagne de spam contre de grandes entreprises en noyant leurs serveurs de messagerie par l'envoi automatique de mails innombrables.
Une faille du système actuel permet à certaines entreprises de faire commerce de noms de domaines non utilisés (Domain Tasting). L'acheteur d'un nom de domaine peut l'utiliser gratuitement car il dispose d'une période de rétractation de cinq jours. De juillet 2005 à mars 2007, on est ainsi passé de 20 millions à 60 millions d'essais gratuits ayant certainement servi à commettre des actions frauduleuses. Basé à Saint Petersbourg connu pour son hébergement d'activités criminelles: pornographie infantile, hameçonnage, envoi de messages indésirables, The Russian business Network RBN, comptabilisait, en octobre 2007, un million de sites, plusieurs millions d'adresses disponibles et 4 millions de visiteurs par mois.

Une prévention indispensable

Ce phénomène exponentiel de cybercriminalité sur Internet appelle la réponse institutionnelle. La prévention et la coopération internationale sont plus que jamais nécessaires. En France, les structures existent et doivent être contactées en cas d'attaques: la direction générale de la police nationale, la direction générale de la gendarmerie nationale, la Préfecture de police.
Ne rien dire laisse les criminels impunis !

Agnès Jauréguibéhère - ifie

Interview

La banque confrontée au piratage informatique

Chargé de la sécurité d'une grande banque française, Éric Detoisien analyse les risques, les techniques d'attaques, et les défenses spécifiques de son champ d'activité et de responsabilité.

A quels risques spécifiques se heurtent les établissements bancaires ?

Deux cibles différentes engendrent deux risques distincts. L'activité de la banque et les clients de la banque.
Comme toute entreprise, des personnes malveillantes essayent d'attaquer les serveurs ou les collaborateurs. Les serveurs, pour récupérer de l'information ou modifier un site. Pirater un site bancaire permettrait de pirater les personnes qui s'y connectent. Très professionnalisées, les attaques sont furtives et invisibles pour durer plus longtemps et être plus efficaces. La sécurité à 100% n'existe pas, mais la protection des serveurs bancaires est aujourd'hui, optimale. Sans commune mesure avec un utilisateur privé. Les serveurs exposés sur Internet se situent dans des zones sécurisées, complètement isolées des autres. Pour être efficace, il faudrait arriver à pirater toute une série d'ordinateurs, ce qui est compliqué. En revanche, il serait plus facile d'attaquer directement les collaborateurs par l'envoi de spam et de mails qui les inciteraient à cliquer sur des liens les orientant vers des sites web malveillants. Lesquels exploiteront des failles propres aux logiciels des utilisateurs. Si un poste d'utilisateur est piraté, l'attaquant aura accès aux mêmes informations et aux mêmes droits que l'utilisateur piraté. En cas d'accès prioritaires à des logiciels de virement, on pourrait imaginer le pire… Cependant, la sécurité en interne est maxima.

Éric DETOISIEN est un expert en sécurité informatique, actuellement responsable sécurité informatique pour une grande banque française. Ses expériences précédentes dans le milieu professionnel de la sécurité des systèmes d'information l'ont conduit à mener des missions d'audit, de test d'intrusion, de conception d'architecture sécurisée et de formation.

Il est, en outre, l'auteur de plusieurs articles (MISC, Banque & Informatique, Linux Mag,..) et conférences (Black Hat, JSSI, SSTIC, Salon Juridique, ...)

Quelle est la défense mise en place ?

La défense se fait en profondeur avec trois niveaux de protections. 1. Protection de l'utilisateur qui n'a pas tous les droits, mais seulement celui d'utiliser les applications et les fichiers nécessaires à son activité. 2. Protection du poste grâce aux antivirus et mises à jour qui évitent l'exploitation des failles. 3. Protection périmétrique avec des zones de confidentialité différentes. Les accès à la messagerie ou à Internet sont filtrés. D'excellents logiciels munis de « black list » filtrent des millions de sites malveillants. Des antivirus analysent le flux entre Internet et le poste d'utilisateur pour repérer les logiciels porteurs de chevaux de Troie. Dès la détection, le blocage est immédiat.
En résumé, on prévient l'attaque. Si elle parvient à s'infiltrer dans un poste, elle est détectée. Et, au pire, en cas d'installation d'un cheval de Troie, celui-ci ne pourra communiquer avec l'extérieur pour sortir de l'information et finira pas être aussi détecté et supprimé.
Ces trois niveaux font l'objet de mises à jour régulières. En cas de nouvelles menaces, soit les produits s'adaptent soit nous adaptons l'architecture. Ce ne sont pas des dispositifs à renouveler tous les trois mois mais dès lors qu'ils sont bien conçus, la défense est efficace.

Et les clients de la banque ?

S'attaquer à une banque, on l'a vu, est compliqué et demande des ressources. Le 2ème risque ce sont donc ses clients. Des centaines de milliers de personnes sont chez eux avec un ordinateur banal et une protection minima. Pour pirater ces ordinateurs, les malveillants développent des programmes industrialisés et automatisés. Le principe est simple : pirater un site quelconque, sur lequel sont installés de petits programmes. Les personnes connectées sur ce site vont être infectées. Sans protection particulière, l'attaque est aisée. Le cheval de Troie « écoute » et récupère ce que fait l'utilisateur: par exemple, login, mot de passe. Il peut détecter si l'utilisateur est sur un site bancaire ou sur une messagerie. Ces informations sont récupérées et envoyées à des serveurs de contrôle où elles sont traitées. Grâce aux login-mots de passe, les pirates vont pouvoir vider les comptes des clients vers « des comptes de mule », c'est-à-dire des intermédiaires. Intermédiaires indispensables, puisque les pirates sont le plus souvent basés à l'étranger. Ils sont recrutés par des mails leur faisant miroiter un job bien rémunéré. L'argent des comptes clients versés sur les comptes mules sera converti en espèces et envoyé par exemple, via Western Union aux pirates. La majeure partie de ces mules est suffisamment naïve pour accepter ce job. Quand le client porte plainte, la police intervient, récupère les éléments, et chez qui va-t-elle? La mule. Entre temps l'argent s'est envolé. Certes des enquêtes ont lieu, mais compliquées du fait de l'externalisation des pirates.

Comment agir ?

En mettant en œuvre des moyens d'authentification

beaucoup plus forts qu'un simple login-mot de passe, authentifiant statique, qui, s'il est volé, peut être utilisé n'importe quand, n'importe où.
Un système d'authentification forte se base sur plusieurs critères. Ce que l'on connaît : un mot de passe par exemple. Ce que l'on possède : une carte à puce par exemple. Ce que l'on est : des éléments de biométrie. En retenant déjà les deux premiers éléments, l'authentification est forte. Sans le code, la carte est inexploitable et inversement. Un autre système de protection, le mot de passe à usage unique : une petite calculette génère un numéro automatique, mot de passe utilisable une seule fois. Sans cette calculette, le login volé est inutilisable.

Il reste toujours des failles ?

Certes, mais ce qui est important, c'est de se protéger des attaques opportunistes automatisées et des voleurs visant l'industrialisation. Ce qui représente la majorité des attaques actuelles. Depuis, la mise en place d'un système d'authentification fort, il n'existe quasiment plus de problèmes. Mais bien que très efficace, la solution n'est pas infaillible. Tant que l'outil malveillant atteint suffisamment de victimes, il reste rentable. Le jour où tout le monde changera de protection, l'attaque s'adaptera aussi !

En cas de hameçonnage ?

Le Phishing va servir, entre autres, à récupérer un login-mot de passe pour se connecter au site bancaire. Notre réponse est celle de l'authentification forte. Le Phishing entraine aussi la compromission de certaines informations, puisqu'on demande à la victime de rentrer nom, prénom, adresse, n° de carte bleue, code pin, pour exploiter le n° de carte. Là, des systèmes de surveillance avec des sociétés extérieures permettent de détecter le plus tôt possible les attaques de Phishing, pour prévenir les clients touchés et faire fermer le site sur lequel le faux est hébergé.
La plupart des grandes banques ont déjà été visées, directement ou indirectement.

Avez-vous été confronté à des cas de dénis de service ou de chantage aux dénis de service ?

Je n'ai pas de connaissance de cas en France. Si l'on se met à la place de l'attaquant, le chantage est risqué, il est difficile de récupérer une rançon. Mais, c'est envisageable. Aujourd'hui les voleurs ciblent surtout les clients, susceptibles de rapporter de l'argent assez vite avec un niveau de risque faible. Ils font aussi une bonne analyse de risque !

En cas de panne ?

La probabilité d'indisponibilité est nettement supérieure à celle d'attaque : erreur humaine, défaillances matérielles… L'informatique a toujours géré ce type d'incident, cela fait partie des process internes, avec des personnes présentes 24h/24. Il existe beaucoup d'indicateurs, qui permettent de voir si une machine est défaillante, sachant en plus que si un serveur tombe, un autre peut prendre le relais immédiatement. Le temps d'un serveur unique est terminé.

Sensibilisez-vous le personnel ?

Dès lors qu'une personne accède au système d'information, elle est impliquée dans la sécurité.
Des formations sont données pour expliquer la nécessité d'avoir une sécurité du système d'information efficiente et comment chacun peut agir au jour le jour afin de respecter la politique de sécurité.

Trop de sécurité ne nuit-t-elle pas au business ?

Il faut parfois trouver le bon compromis entre sécurité et business, ne pas ralentir le business tout en le protégeant. Un équilibre toujours à parfaire. Personnellement, j'interviens lors de projets bancaires pour faire une analyse de risque, montrer les points de sécurité sur lesquels il faut se focaliser ou relativiser.

Y a-t-il des matériels auxquels vous faite plus confiance que d'autres ?

Je ne suis pas pour les grands débats « Il vaut mieux Microsoft ou UNIX ? ». Il est primordial de bien maîtriser le logiciel utilisé en interne. Un système très sécurisé que personne ne peut utiliser est inefficace. J'ai toujours eu une démarche pragmatique : il faut faire de la sécurité utile. J'ai l'avantage de bien connaître les menaces concrètes, de voir comment se défendre et où le faire en priorité. Ce n'est pas forcément en achetant du matériel sophistiqué qu'on va pouvoir mieux se défendre, il est préférable d'utiliser au mieux le matériel déjà possédé.
Il faut connaître les techniques d'attaques. Je suis un peu sceptique à l'égard de ceux qui pensent pouvoir faire de la sécurité sans bien les connaître.

Avez-vous des difficultés à équilibrer sécurité et protection des données personnelles ?

Nous suivons les directives de la CNIL. Dès lors qu'il y a des données personnelles, l'accès est restreint, de même les informaticiens ont des droits restreints.
Légalement, nous sommes obligés de garder des traces, mais sur une durée limitée. Leur exploitation n'est possible qu'à certaines conditions, dans la mesure du respect de la vie privée. Le droit de les utiliser relève de réquisitions spécifiques, judiciaires par exemple.

Éprouvez-vous des difficultés à vous adapter à la législation en cours ?

La banque est soumise à beaucoup de réglementations et de lois. Celles sur la sécurité sont en général connues et prises en compte avant d'être promulguées. La notion du risque est forte dans les banques, nous savons ce qu'il y a à protéger, et nous le faisons.

Propos recueillis par **Agnès Jauréguibéhère**

Protéger la recherche

Chargé de mission Sécurité des systèmes d'information au CNRS, Robert Langeon coordonne l'action au niveau national. Il explicite ici pourquoi et comment protéger la recherche fondamentale de cet organisme d'Etat.

Vous êtes Chargé de Mission à la sécurité des systèmes d'information. Quelle est la spécificité et l'enjeu de cette mission ?

Le type d'organisation de la sécurité des systèmes d'information au CNRS et une des clés de son efficacité : c'est une structure déconcentrée au niveau local et régional avec une coordination forte au niveau national.
La sécurité opérationnelle se réalise à la base, sous la responsabilité des directeurs des unités de recherche (1300 unités au total) qui s'appuient sur des adjoints chargés de la SSI. On retrouve ce type de structure à chacun des autres niveaux, à l'image d'une « fractale » : au niveau régional, le responsable est le délégué qui s'appuie sur un coordinateur ; au niveau national, c'est le Directeur Général du CNRS qui est aidé par un chargé de mission. Le rôle de ce dernier est d'abord d'animer les actions nationales, de coordonner les politiques régionales et de piloter la PSSI (politique de sécurité des systèmes d'information) du CNRS. C'est aussi de fixer et de contrôler les d'objectifs, de réaliser des formations et des réunions de sensibilisation, de diffuser les alertes et avis de sécurité. C'est enfin, avec l'appui d'experts techniques, de constituer un référenciel SSI commun afin d'assurer la cohérence des actions de notre organisme en SSI.
Ce type d'organisation qui établit un équilibre dynamique entre action locale et pilotage national, savant dosage entre liberté créatrice et contrôle directif, est notre mode de travail au CNRS. Il donne dans l'ensemble des résultats satisfaisants.

Le secteur de la recherche semble particulièrement exposé. Quels risques principaux peut-on identifier ?

Il existe plusieurs niveaux d'appréciation du risque. D'abord, du strict point de vue de la recherche. Il y a une hyper compétition de la recherche, les meilleurs chercheurs rejoignent les laboratoires de réputation internationale. Ceux qui ne peuvent maintenir un niveau d'excellence en leur sein, entrent ainsi dans un cercle vicieux dont il est difficile de sortir : plus ils perdent leurs chercheurs les plus « productifs » moins ils peuvent en recruter. Pour les unités du CNRS, maintenir un niveau de recherche internationale est donc un défi permanent ; perdre pied, c'est prendre le risque de ne plus jamais pouvoir remonter à la surface. C'est à cet enjeu majeur que participe la SSI… même si ce rôle n'est pas toujours facile à faire comprendre. En effet, le sentiment « d'avoir perdu quelque chose » après l'attaque de son système d'information n'est pas immédiat (les informations n'ont pas été vraiment volées puisqu'on les possède toujours !), ce n'est que plus tard qu'on s'aperçoit que d'autres publient des articles qu'on voulait publier, que des contrats qu'on croyait acquis n'ont pu être conclus, que des brevets ont été pris sur ses propres résultats de recherches, que son savoir-faire « a été transféré ». Au fil des années, de piratage en pillage, le laboratoire perd ainsi toute compétitivité internationale. L'angélisme (ou l'insouciance) vis-à-vis de la SSI est comme le cholestérol : on peut vivre avec en se croyant en bonne santé… un certain temps, car l'infarctus surviendra inexorablement.
On peut aussi voir les enjeux à l'échelle de la Nation : sans un bon niveau de recherche, notre pays perdra peu à peu son avance technologique ; il deviendra incapables de fabriquer des avions ou de mettre des satellites sur orbite ; nous n'aurons plus d'industrie compétitive. Restera la sous-traitance…
On peut encore voir les enjeux en termes d'éthique de la science. Si nous perdons notre excellence, l'éthique sera fixée par d'autres qui n'auront pas la même approche que la nôtre… et ça ne sera pas forcément un progrès !
On peut enfin placer les enjeux sur le problème de notre capacité de défense…
Bref, on voit que les enjeux sont multiples, mais quelle soit la manière de les aborder, leur importance est évidente.

Quels moyens essentiels mettre en œuvre pour protéger l'information ?

Je ne peux pas être exhaustif. Les laboratoires sont tous différents. Un laboratoire d'archéologie n'aura pas les mêmes besoins de sécurité qu'un laboratoire travaillant dans le domaine nucléaire dont les technologies ne doivent pas tomber entre les mains d'Etats proliférants.
S'il fallait résumer, je dirais que la SSI est la gestion du risque sur l'information : comprendre les enjeux, déterminer les menaces, étudier les vulnérabilités ; enfin, évaluer les risques et prendre les bonnes décisions.

La sécurité n'est jamais définitivement acquise. Sur quels critères s'appuyer pour l'évaluer ? Sont-ils mesurables ?

On peut même dire que la sécurité absolue est une illusion ! Les menaces évoluent continuellement, il faut donc adapter la sécurité en permanence. Dans ces conditions, savoir si les protections qui ont été mises en place sont efficaces est essentiel. Il existe pour cela diverses techniques, mais la plus utilisée est une technique venu du management : les tableaux de bord basés sur des d'indicateurs donnant les écarts entre des objectifs à atteindre et un état réel. Un exemple : nous avons en permanence près du quart de nos effectifs en mission dans le monde. Pour un chercheur, pouvoir toujours se

connecter aux réseaux de son laboratoire, même durant ses déplacements, est vital. Cette communication est sécurisée au maximum, pourtant, parfois des pirates arrivent à casser ces sécurités. Quand cela arrive, il faut le savoir rapidement, prendre tout aussi rapidement les mesures correctives et tirer le bilan des vulnérabilités qui ont permis l'attaque. Nous aurons donc des détecteurs d'intrusions, des alarmes sur actions « non-conformes », des indicateurs d'activité réseaux suspects, etc. qui nous permettrons – en théorie - de réagir dans les meilleurs délais. Pour évaluer notre niveau de sécurité globale, nous ferons des statistiques sur ce type d'attaque, regarderons comment évolue cet indicateur avec le temps et essayerons d'expliquer cette évolution.
C'est l'éternel combat entre la défense et l'attaque. Celle-ci est toujours avantagée par rapport à la défense, qui ne perçoit ses limites qu'à chaque but marqué.

La sécurité et l'insécurité ont un coût. Comment les évaluer ?

Lorsque la sécurité est vue comme simplement la mise en place d'une défense périmétrique, on sait ce qu'elle coûte mais il est en effet difficile de savoir ce qu'elle rapporte (comment savoir si ces défenses sont efficaces ou même si elles sont nécessaires ?)
Avec l'analyse de risque, la démarche est beaucoup plus simple, car elle part des besoins de sécurité et dimensionne les protections à la mesure des enjeux.
Voici l'échelle des risques, telles que nous l'avons fixée :
1er niveau : le risque est insupportable parce qu'il met en jeu l'organisme, voire des vies humaines (par exemple, information sur l'itinéraire d'un chercheur qui se rend dans un pays où l'enlèvement est une fructueuse industrie)
2ème niveau, le risque est grave : tout ce qui porte atteinte à l'image de marque. Les conséquences peuvent mettre plusieurs années à se manifester.
3ème niveau, le risque est important : des pertes finacières moyennes par exemple.
4ème niveau, le risque est supportable : un virus maîtrisé grâce aux sauvegardes.
Dernier niveau, le risque est insignifiant.
Dans cette échelle de 1 à 5 on compare l'effort à faire par rapport à la menace, il ne s'agit pas de comparer des coûts entre eux.

Constatez-vous une augmentation de la criminalité depuis l'émergence des nouvelles technologies ?

Emergées depuis 50 ans, elles se complexifient.
On est face à trois types de délinquance/criminalité. Un premier type, qu'on peut qualifier de « délinquance juvénile », plutôt ludique et « anti-système », elle fait quelques dégâts dans nos systèmes d'information mais ses conséquence sont moindres comparées à celles des deux autres types. Cette délinquance a tendance à se professionnaliser et à évoluer vers celles d'un 2ème et 3ème type. Le 2ème groupe, celui-là mafieux, est en réalité la grande criminalité sur les réseaux « assistée par ordinateur ». Enfin un 3ème groupe possède, quant à lui, des moyens et des compétences étatiques. En regardant leur évolution respective, on peut voir que le milieu des hackers traditionnels (1er groupe) et le 3ème groupe restent à un niveau à peu près constant tandis que le groupe en plein développement est celui des mafieux du net.

La malveillance n'est pas seule en cause. Entre les pannes, les maladresses, les accidents, lesquels sont les plus importants ?

Si la sécurité est bien faite, on peut prévenir les accidents et les maladresses. On est dans le domaine assez classique et rationnel de la gestion des risques. Aujourd'hui, un disque tombe moins en panne qu'il y a dix ans, mais il ne serait pas professionnel d'oublier de faire des sauvegardes qui protègent à peu près contre tous les types de pannes et maladresses...
En revanche, en ce qui concerne la malveillance, on est dans l'irrationnel. Ce n'est plus vraiment du risque, mais de l'incertitude. Le risque se mesure. Le risque d'une panne disque est le temps moyen de son bon fonctionnement. Mais la malveillance ne ressort pas de la probabilité. Souvent, l'occasion fait le larron. Les coûts sont difficilement mesurables. Parfois, le dégât le plus important n'est pas la destruction ou le vol de données, mais l'atteinte à l'image. Comment être pris au sérieux par un industriel avec lequel on coopère s'il apprend que nous protégeons mal les informations qu'il nous confie ? Sans ce sérieux, plus de contrats.

Constatez-vous un certain scepticisme à l'égard des règles de sécurité à mettre en œuvre ? L'ensemble du personnel se sent-il concerné ?

Nous avons fait de grand progrès ces dernières années en comprenant qu'on ne fait pas de sécurité sans le personnel et encore moins contre lui. La sensibilisation et la formation sont les instruments essentiels de la SSI. Plus les personnes sont sensibilisées, plus on peut élever le niveau de sécurité. Mais si ce niveau n'est pas adapté à la sensibilisation, les personnes ne seront pas d'accord avec les mesures prises, elles transgresseront les règles imposées et l'échec est assuré. C'est par une démarche collective que les personnels pourront s'approprier les enjeux, identifier les menaces et valider les mesures de sécurité. Ce travail est sans cesse à recommencer en raison d'une rotation importante du personnel.

Trop de règles ou de procédures ne risquent-elles pas d'appauvrir la créativité ?

C'est un piège dans lequel tombe les néophytes par peur de ne pas en faire assez. Ils ne comprennent pas que

la sécurité a un coût qui n'est pas seulement financier mais est aussi lié à la rigidification de l'organisation. La recherche, c'est l'ouverture ! Elle a besoin de chercheurs, des laboratoires étrangers, de stagiaires... La contrepartie de cette ouverture est la responsabilité.
Responsabiliser les gens est moins paralysant que d'interdire.

Le nouveau champ de la criminalité a été vite exploité. Où se recrutent, à votre avis, les auteurs de malveillance ?

Dans tous les milieux. Même parmi les cadres supérieurs. L'appât du gain est un moteur puissant. Une personne placée à côté d'un coffre fort dont il possède la clé, résistera 2 ans, 5 ans, peut-être 20 ans ; un jour, elle craquera et vous vous demanderez pourquoi… Jérôme Kerviel de la Société Générale est un cas très médiatisé en raison des sommes fabuleuses en jeu. Mais ce type de problème – à une échelle moindre – est plus fréquent qu'on le croit.

Propos recueillis par **Agnès Jauréguibéhère**

Le CNRS en chiffres
Le CNRS emploie environ 30000 personnes : 26100 permanents (11700 chercheurs et 14400 ingénieurs, techniciens et administratifs) et 4000 contractuels. Son budget annuel est d'environ 3 milliards d'euros dont 500 millions de ressources propres. Le CNRS exerce son activité dans tous les domaines de la connaissance à travers 1260 unités de recherche et de service au niveau local, et 19 délégations au niveau régional.
Chiffres 2007

Actus

➲ Michèle Alliot-Marie a présenté le 14 février son plan d'action pour combattre la cybercriminalité et ne pas « laisser le dernier mot aux trafiquants et aux pédophiles ».

Il devrait être examiné par le Parlement après les municipales.
Quelques mesures préconisées :
- Doubler le nombre des cyber-enquêteurs au sein des services de police.
- Sous contrôle du juge, capter à distance, quand elles s'affichent à l'écran d'un pédophile ou d'un terroriste, les données se trouvant dans un ordinateur.
- Perquisitionner à distance
- Evoluer vers la géolocalisation des internautes.
- Introduire le "délit de l'usurpation d'identité sur internet, passible d'un an d'emprisonnement et de 15.000 euros d'amende",
- Créer une "plate-forme européenne d'échanges d'informations", sous l'égide d'Europol.
- Impliquer les fournisseurs d'accès ou les hébergeurs de sites.
- Elaborer "une charte des bonnes pratiques" pour bloquer les sites illicites.

Source : www.interieur.gouv.fr/sections/a_l_interieur/le_ministre/interventions/lutte-cybercriminalite

➲ Paru ce mois-ci : Les nouveaux territoires de l'intelligence économique.

Préfacé par Alain Juillet, haut responsable en charge de l'intelligence économique auprès du Premier ministre, il est édité en partenariat avec l'ACFCI, réseau clé en matière d'intelligence économique.

L'intelligence économique n'a pas vocation à rester cantonnée à l'économie.
Ces outils s'appliquent à la compréhension de l'ensemble du monde : intelligence juridique, intelligence culturelle, intelligence comptable et financière, intelligence culturelle, intelligence humanitaire, intelligence sociale, intelligence sportive...
C'est à la découverte passionnante et à la description approfondie de ces nouveaux territoires que nous entraînent les auteurs, tous experts en leur spécialité respective.

Plus d'infos sur www.ifie.net

➲ Conférence de presse de la FéPIE - Avril 2008

L'IFIE a organisé un déjeuner de presse le 23 avril au Press Club de France en présence de nombreux journalistes représentant toutes les grandes rédactions intéressées par l'Intelligence économique.
Un projet est en effet actuellement en cours pour assimiler les métiers de l'Intelligence Économique à celui des agents de recherche privés (détectives privés). Les principales associations d'Intelligence économique : la FEPIE, Fédération des professionnels de l'Intelligence Économique, le GCIC, Groupement des Compétences pour l'Information et la Compétitivité, la SCIP, Association Française pour la Promotion de l'Intelligence Économique et Concurrentielle, l'ADBS, Association des Professionnels de l'Information et de la Documentation étaient présentes pour exposer les problèmes soulevés, leur action et position commune.

Conférenciers :

Général Jean-Bernard Pinatel, Président de la FéPIE
Patricia Auroy, Présidente du GCIC
Josette Bruffaert-Thomas, Vice-Présidente du SCIP
Paul-Dominique Pomart, Administrateur du SCIP
Claudine Masse, Déléguée générale l'ADBS
André Added, Président de l'IFIE, vice-Président de la FéPIE

Contacter la rédaction : contact@ifie.net