Forum ATENA

Excellente année 2011!

2011, L'ANNEE DU LIVRE MYTHES ET LEGENDES DES TIC

1er janvier 2011

Collection ATENA

Une réalisation de Forum ATENA avec la collaboration de *(par ordre alphabétique)* **:**

Christian Aghroum, Eric Bourre, Jean-Pierre Cabanel, Jean Christophe Elineau, Franck Franchin, David Grout, Daniel Hagimont, Bruno Hamon, Michel Lanaspèze, Jean Papadopoulo, Gérard Peliks, Sadry Porlon, Philippe Poux, Bruno Rasle, Yvon Rastteter, Nicolas Ruff, Philippe Vacheyrout

Livre collectif sous la direction de Gérard Peliks

Les ajouts depuis la version du 24 décembre sont en bleu

INTRODUCTION

Ce livre collectif de l'association forum ATENA propose une approche originale pour expliquer différentes facettes des **T**echnologies de l'**I**nformation et de la **C**ommunication (**TIC**).

En soulignant les croyances largement partagées mais fausses, Ce livre s'adresse à tous les utilisateurs des **T**echnologies de l'**I**nformation et de la **C**ommunication qui désirent acquérir des connaissances et dominer les problèmes posés par l'Information, les systèmes d'information et les réseaux connectés à l'Internet. Ce livre apporte des réponses à leurs interrogations, leurs doutes, combat les idées fausses mais pourtant largement partagées, et donne des conseils pratiques basés sur nos expériences du terrain. Il aborde non seulement les aspects techniques mais aussi les aspects juridiques, humains et organisationnels qui se posent à tous.

La cible n'est pas une population d'experts. Notre livre s'adresse à un lectorat qui cherche des réponses pratiques à des problèmes concrets sans posséder la compétence pour bien appréhender les informations qu'on trouve dans des livres et des revues spécialisées.

Le fichier PDF de la version la plus récente du livre est en téléchargement libre à partir du Web de Forum ATENA en www.forumatena.org/?q=node/12, rubrique "Mythes et légendes des TIC", en laissant votre adresse e-mail.

Gérard Peliks
Président de l'atelier sécurité de Forum ATENA
Coordinateur de cet ouvrage

SOMMAIRE

1° PARTIE : ASPECTS TECHNOLOGIQUES DES TIC

MYTHES ET LEGENDES DE L'INTERNET

Gérard Peliks, CASSIDIAN
an EADS Company

LES FAUSSES CERTITUDES

L'Internet est tellement ancré dans notre vécu quotidien que comme pour toute chose qui s'est rapidement imposée, il s'est bâti autour de ce phénomène, des croyances devenues certitudes qu'il n'est même pas envisageable de remettre en question sans passer pour quelqu'un qui n'a rien compris à ce qui semble évident à l'homo vulgaris.

Mais ces certitudes ont parfois leur part d'erreurs et peuvent figer le développement de ce moyen irremplaçable de communication qui a bien besoin d'évoluer, peut-être même en changeant de base.

Mieux comprendre l'Internet d'aujourd'hui, en particulier dans ses couches basses est indispensable pour appréhender les travaux qui sont menés actuellement dans des centres de recherche, et qui pourraient bien changer les bases de l'Internet du futur.

MYTHE N° 1 : L'INTERNET BENEFICIE LARGEMENT DE L'INNOVATION

En fait très peu d'innovations ont été réalisées depuis la fin des années 70 dans les couches basses de l'Internet. Comme le système fonctionne, porté par l'augmentation des performances prévue dans les lois de Moore, comme les protocoles sont entérinés par des organismes de standardisation, l'IETF en particulier, ceux qui avaient le pouvoir de faire évoluer l'Internet ont préféré se servir de l'existant pour asseoir leur business. Notons que la standardisation de l'Internet n'est pas le fait d'organismes internationaux de normalisation comme l'ISO, l'UIT ou l'ETSI, et que l'IETF est un organisme essentiellement sous contrôle des Américains.

La recherche et le développement des couches basses de l'Internet ont été laissés à l'abandon car les retombées en revenus immédiats n'ont jamais été perçues de manière évidente et l'aspect économique a primé et écarté l'innovation. Il fallait que l'Internet rapporte de l'argent. Pour cela, il ne fallait surtout pas toucher aux couches basses qui devaient rester stables.

Certes, côté applicatif, il y a eu de grandes innovations, comme bien sûr le Web, aujourd'hui participatif et demain sémantique, comme les nouveaux usages : musique, vidéo, films, P2P, ToIP, forums. Il y en aura de nombreux autres à peine croyables aujourd'hui, comme la 3D et la réalité augmentée... Mais justement, ces avancées peuvent difficilement reposer sur des couches basses qui n'ont pas évolué en rapport avec ce que réclament les nouvelles applications, en sécurité, en mobilité, en sans-fils, en multihoming (connexion à plusieurs réseaux).

MYTHE N° 2 : L'INTERNET EST UN RESEAU QUI APPARTIENT A TOUT LE MONDE

Ça c'est un mythe tellement répandu que l'accès à la toile, l'envoi des courriels, les forums de discussion sont devenus aussi naturels que l'air qu'on respire et qui appartient à tous, comme semble l'être l'Internet, abonnement à un fournisseur de services mis à part. Et pourtant

l'Internet est loin d'être neutre. Il "appartient" à l'ICANN (Internet Corporation for Assigned Names and Numbers). En effet, l'ICANN gère l'espace d'adressage du sommet de la hiérarchie des noms de domaines de l'Internet, et ses serveurs de noms de domaines racines, ce qui en fait de facto son véritable propriétaire car qui détient le nommage détient le pouvoir.

Créé en 1998, l'ICANN est une organisation de droit privé, plus précisément de droit californien. Vinton Cerf, un des intervenants de notre grand événement sur le futur de l'Internet du mois de janvier en avait été le président durant près d'une dizaine d'années. Il est vrai que ces derniers temps, la gouvernance de l'ICANN est devenue un peu moins américaine, mais à peine moins. On dit que le président des Etats-Unis dispose (ou disposera) d'un gros bouton rouge, pour désactiver l'Internet mondial en cas de cyber attaque grave sur son pays. D'ailleurs les Etats-Unis avaient déconnecté pendant un certain temps le domaine de l'Irak du reste de l'Internet. Aucun autre pays ne pourrait en faire autant.

Les Chinois ont déjà pris leurs distances par rapport à ce qu'on appelle encore communément "l'Internet" (au singulier), en constituant leur propre Internet indépendant de celui du reste du monde. Les Iraniens penseraient sérieusement à faire de même. Ces dissidences pourraient faire effet domino, ne serait-ce que pour prendre en compte des alphabets non latins, des lettres accentuées ou une philologie non américaine. On parlera alors non pas de l'Internet mais "des" internets, tout ceci pour une question d'adressage et de gestion des noms de domaines !

MYTHE N° 3 : L'INTERNET EST ISSU DU RESEAU ARPANET

Ce n'est pas faux. L'Internet a beaucoup bénéficié des travaux réalisés pour le réseau ARPANET et en particulier du développement des protocoles IP et des protocoles au dessus (TCP, UDP, ICMP, FTP, SMTP, HTTP …).

Toutefois si on mène une recherche en paternité de l'Internet, on peut remonter plus loin, jusqu'aux travaux autour du projet CYCLADES de l'IRIA (qui allait devenir l'INRIA) et de l'idée du datagramme, objet logiciel qui permet de travailler en mode sans connexion. A la tête du projet CYCLADES, il y avait le Français Louis Pouzin, à qui revient le titre d'inventeur de l'Internet. Mais dans la France des années 70, sous la présidence de Giscard, les PTT avaient imposé le circuit virtuel (mode avec connexion) qui allait donner X25 puis ATM.

Et c'est ainsi qu'une idée française, un mode sans connexion, ne s'est pas concrétisée en France et que les Etats-Unis sont devenus les maîtres incontestés de l'Internet.

MYTHE N° 4 : LE ROUTAGE DE L'INTERNET EST DECENTRALISE

Décentralisé comme le routage du téléphone ou du GSM ? On voudrait bien que ce soit vrai mais c'est loin d'être le cas. Si on prenait une image, utiliser le routage de l'Internet, c'est comme si on demandait à un facteur de distribuer le courrier, mettons rue de Vaugirard. Mais le premier immeuble de cette rue ne serait pas le "1 rue de Vaugirard", mais le "232 boulevard Eisenhower", en face ce ne serait pas le "2 rue de Vaugirard" mais le 12 avenue Mao Tse Toung, et ainsi de suite.

Vous voyez le surcroit de travail pour le pauvre facteur obligé de consulter un répertoire qui fait la liaison entre l'implantation de l'immeuble dans la rue et son adresse ? Et pour les

employés du centre de tri postal, quel cauchemar pour classer le courrier ! Il faut donc des répertoires (serveurs DNS).

Tout ceci suite à de mauvaises options dans l'attribution des adresses IP, dans le nommage des domaines et dans la répartition des tâches entre les couches IP et TCP. Mais c'est ainsi que fonctionne le routage sur l'Internet car la plupart des routes sont statiques.

Chaque message, chaque fichier est découpé en datagrammes et chaque datagramme qui connaît son adresse de destination (contenue dans le champ IP) est acheminé de proche en proche, via des routeurs, dans les réseaux connectés. Et chaque routeur doit connaître vers quel routeur de proximité transmettre le datagramme qui ne lui est pas destiné, en fonction des routes qu'il connait et de celles qu'on lui fait connaître.

Ceci entraine une explosion en taille des tables de routage, des performances dégradées car les routeurs arrivent à la limite de leur capacité de calcul et le problème va vite devenir insoluble.

MYTHE N° 5 :
L'ADRESSE IP IDENTIFIE UN ORDINATEUR

Ça vous semble évident ? Et bien non, l'adresse IP identifie le contrôleur réseau par lequel votre ordinateur se connecte à l'Internet ou à un Intranet. On aurait bien voulu qu'une adresse IP indique qui en est le possesseur, ou au moins l'ordinateur qui possède cette adresse si ce n'est qui est l'utilisateur de cet ordinateur, à quel endroit se trouve cet ordinateur et quelle est sa fonction. On est loin du compte.

Tous ces renseignements (qui, où, quoi), ne peuvent être donnés qu'en rajoutant constamment des rustines au dessus de la couche IP de l'Internet.

Comme l'a fait remarquer le professeur Kavé Salamatian de l'Université du Jura, l'Internet bien conçu il y a quarante ans pour un nombre très petit de nœuds, à ses début dans le projet ARPANET, avait une couche IP fine et élégante, mais elle s'est très vite engraissée et présente aujourd'hui de grosses poignées d'amour qui sont IPsec, NAT, Diffserv, Mcast...

Un poids trop élevé et un corps trop potelé, tous les nutritionnistes vous le diront, ce n'est pas bon pour la santé.

MYTHE N° 6 :
L'IPV6 VA RESOUDRE TOUS LES PROBLEMES EVOQUES

L'IPv6, nouveau protocole de l'Internet, résout le problème du nombre d'adresses IP devenu très insuffisant, avec l'IPv4, pour satisfaire aux exigences de la demande pour les objets communicants, pour les voitures électriques, pour la grille électrique et d'une manière générale pour l'explosion du nombre d'utilisateurs. Un utilisateur, en particulier pour la mobilité a besoin aujourd'hui de nombreuses adresses IP. Et les objets intelligents communicants, les étiquettes RFID vont encore faire exploser ce nombre d'adresses nécessaires.

L'IPv6 ajoute également des solutions pour assurer la sécurité, la qualité de service, la mobilité et la diffusion en multicast (un émetteur et plusieurs récepteurs).

Mais l'IPv6 conserve la philosophie de l'IPv4, en particulier celle du mode sans connexion et la notion de "best effort".

Si l'IPv6 n'est pas la solution, faut-il faire table rase de l'existant et repartir à zéro, et non de protocoles couverts de rustines, et de protocoles qui s'empilent et parfois coexistent mal entre eux, comme le préconisent plusieurs chercheurs, tels John Day et Louis Pouzin qui ont été à la base de l'Internet ?

LE POST-IP

En conclusion de ces mythes et des réponses qu'on peut apporter pour démystifier le phénomène, John Day propose, par exemple, un nouveau socle pour l'Internet, non plus bâti sur les couches IP mais sur un modèle de communication interprocessus (Inter Process Communications : IPC) récursif : les protocoles RINA qu'il décrit dans son livre "Patterns in Network Architecture, a return to fundamentals"

Dans ce nouveau principe, qui est une technologie de rupture par rapport à l'existant, le réseau n'est plus un moyen de transporter les données mais un mécanisme d'échange entre processus qui transportent les données. Seuls les processus accèdent aux données qu'ils transportent. L'extérieur n'a pas accès aux adresses internes, ce qui rend difficiles les attaques classiques, basées sur la connaissance des adresses IP vulnérables, pour compromettre les données et renforce la sécurité.

Si le mode avec connexion et le mode sans connexion se rencontrent pour assurer un transport de l'information sûr et performant, dans une architecture où les IPC remplaceront le modèle en couches, et se dupliqueront de manière récursive pour s'adapter aux réseaux physiques, il est certain que l'Internet du futur pourra reposer sur un socle plus solide que celui sur lequel repose l'Internet d'aujourd'hui.

MYTHES ET LEGENDES DE LA SECURITE DE L'INFORMATION

Gérard Peliks, CASSIDIAN
an EADS Company

LES AGRESSIONS, ÇA N'ARRIVE PAS QU'AUX AUTRES

Bien calé dans votre fauteuil, vous lisez votre messagerie, parfois vous participez aux forums sur les vulnérabilités et les menaces pouvant peser sur votre système d'information, et de temps en temps vous prenez connaissance des dernières alertes des CERT.

Oui, bien des gens n'ont pas de chance de se faire ainsi agresser. Mais pas vous ! Parmi les dizaines de milliers de logiciels malfaisants qui tournent en permanence sur les réseaux, guettant la moindre faille autour de votre PC, comment faites-vous pour toujours passer au travers ? Qu'il est merveilleux, ce sentiment de sécurité qui entoure votre Information ! Sentiment de bien-être encore accru par l'assurance que les contre-mesures que vous avez mises en œuvre, en particulier votre antivirus et votre firewall personnel vous garantissent de ne jamais être concernés par les horreurs qui se passent chez les autres !

Mais la réalité est que la sécurité de l'Information, avec laquelle vous vivez en apparence, est un mythe ! L'insécurité est l'état normal et, comme vos voisins, vous subissez aussi des agressions et parfois celles-ci passent et font des dégâts.

Le véritable danger d'ailleurs n'est pas tellement au niveau des menaces qui vous environnent mais se situe entre votre chaise et votre clavier. Le véritable danger, pesant sur votre information, c'est vous, si vous ne mesurez pas combien est dangereux le monde qui vous entoure.

MYTHE N° 1 : IL EXISTE DES HAVRES DE PAIX SUR L'INTERNET

Les virus, les vers, les chevaux de Troie, concernent les utilisateurs des PC sous Windows. Votre PC tourne sur une distribution de Linux (Ubuntu, Mandriva ?) et donc les virus ne sont pas dirigés contre vous, puisque sous Linux il n'y en a pas ? Erreur, il existe des logiciels malfaisants sous Linux aussi.

Alors, tournons nous vers les MAC puisque là au moins nous sommes tranquilles ? Erreur, il existe aussi des logiciels malfaisants dédiés aux MAC. Mais votre Smartphone n'est pas sous Windows et ce n'est pas un MAC ? Vous avez raison sur ce point mais c'est aussi un mythe qu'il n'y a pas de logiciels malfaisants pour Smartphones, et plus il y aura de PC sous Linux, plus il y aura de MAC, plus il y aura de smartphones et de eBooks, plus il y aura de virus qui les prendront pour cible. Et ce n'est pas tout.

L'imprimante de votre entreprise n'est pas plus à l'abri que le sont vos postes de travail. Une imprimante en réseau est, comme tout serveur, un nœud sur l'Intranet et comme tout nœud d'un réseau, elle est menacée dans son fonctionnement tout d'abord. Que diriez-vous si votre imprimante, dès qu'elle est alimentée, imprimait à longueur de journée, rame après rame, parce qu'elle serait victime d'une campagne de spam que vous ne pouvez arrêter qu'en payant une rançon ? Le chantage visant une entreprise est un marché qui commence à devenir florissant, et qui pourrait bien un jour se généraliser.

Votre imprimante pose de plus un problème côté confidentialité des informations qu'elle a imprimées. Non ce n'est pas parce qu'une main inavouable récupère systématiquement, avant vous, sur votre imprimante, les informations confidentielles que vous venez d'imprimer, encore que ça peut arriver. Ce n'est pas non plus que vous ne vous méfiez pas assez du spool. Votre imprimante a un disque dur dans lequel les impressions sont stockées. Et quand vous restituez votre imprimante à la société qui vous l'a louée, pour vous équiper d'une imprimante plus moderne ou mieux adaptée, vos informations résident toujours sur son disque dur. Et voilà comment, des informations confidentielles depuis longtemps stockées sur une imprimante, alors que ses utilisateurs n'en avaient pas conscience, changent de main.

On a aussi beaucoup parlé des dangers que font courir les documents de la suite Office de Microsoft, suite aux macrovirus qui présentent effectivement un réel danger. Heureusement, la transmission de documents au format PDF est la solution ? Elle ne l'est plus. Les fichiers PDF, qui peuvent être aussi contaminés, représentent aujourd'hui un des trois principaux vecteurs d'infection.

Alors vers quoi vous tourner ? Sur 360 degrés, vous êtes menacés. Il faut apprendre à vivre dangereusement et comme il n'est pas possible d'éliminer tout danger, il faut chercher à le réduire à un niveau acceptable. C'est ce qu'on appelle le risque résiduel, qu'il faut savoir accepter et gérer.

MYTHE N° 2 :
LES EXECUTABLES EN ".EXE", VOILA LE DANGER !

Au début, il y avait les virus, constitués d'instructions qui s'accolent à un programme exécutable. Le virus libère sa charge létale quand le programme, auquel il est accolé, s'exécute. Si vous ne lancez pas l'exécutable contaminé, le virus reste inactif. Et comme le virus modifie la taille de l'exécutable, en fonction du contenu et de la taille de ses instructions, la modification qui est la signature du virus, une fois connue, peut être éradiquée de l'exécutable pour le faire revenir à son état sain. C'est ainsi que procèdent les anti-virus. Contrairement à ce qu'on croit généralement, les virus ne se dupliquent pas. L'infection ne peut se répandre que si on transmet l'exécutable contaminé, par exemple en attachement à un e-mail.

Mais Il existe une autre famille de logiciels malfaisants, les vers (worms en anglais) qui eux ne sont pas attachés à un exécutable. Ils sont eux-mêmes des exécutables autonomes et ils investissent votre PC en passant, à travers le réseau, par une faille non couverte affectant un des logiciels que vous utilisez. Une fois installés chez vous, ils se dupliquent et, toujours par le réseau, se répandent un peu partout chez les autres utilisateurs. On pourrait juste vous reprocher d'être connectés !

Les vers forment une famille bien plus nombreuse et bien plus dangereuse que les virus, et c'est pourquoi, croire que n'exécuter que des fichiers ".exe", ".zip" ou autres fichiers avec du code exécutable de confiance, pour ne pas être infecté, est un mythe.

Croire que la messagerie est le seul vecteur d'infection avec les fichiers exécutables attachés aux messages que vous recevez est aussi un mythe. Le vecteur principal d'infection aujourd'hui est le Web.

Il suffit de naviguer sur des pages Web contaminées et vous récoltez des programmes malfaisants contenus dans des pages que votre navigateur télécharge avant de les interpréter. Une page Web, apparemment anodine, peut contenir beaucoup d'éléments exécutables, comme des applets Java, des ActiveX, des codes JavaScript, des Flashs … Les cybercriminels piègent des sites, même les plus honnêtes, surtout les plus lus. C'est ce qu'on appelle l'infection "drive by download" très répandue. Aujourd'hui le Web devance la messagerie

comme premier vecteur d'infection et. Les fichiers PDF viennent juste après la messagerie dans le classement des éléments dangereux.

MYTHE N° 3 :
LES CYBERCRIMINELS VEULENT DETRUIRE VOTRE SYSTEME D'INFORMATION

Attaquer les systèmes d'information pour éprouver la délicieuse poussée d'adrénaline qui vient avec l'agression du système d'information d'une entreprise, si possible grande et connue, pour le détruire et en entendre ensuite parler; attaquer les réseaux pour prouver qu'après tout on n'est pas incompétent, et les plaintes que poussera l'entreprise en seront une preuve éclatante, c'est du passé et ce type d'attaques ludiques est devenu un mythe, sauf si une cyberguerre se déclenche ou si le cyberterrorisme frappe, ce qui est un autre problème.

Aujourd'hui les cybercriminels attaquent le réseau pour un motif tout aussi inavouable que pour le détruire et leurs attaques sont plus feutrées. Ils mènent leurs attaques pour gagner de l'argent facilement et sans prendre trop de risques. Il est moins périlleux en effet d'attaquer les coffres virtuels d'une banque située à 10 000 km de distance, par l'Internet, depuis un pays où la législation concernant le cybercrime est quasi inexistante, en utilisant un PC et une connexion haut débit, que d'utiliser un camion bélier, un fusil à pompe et un chalumeau, sur place.

Attaquer pour des raisons pécuniaires change les attaquants, les attaques et les cibles. Les attaquants sont souvent des groupes de cybercriminels, parfois sans compétence informatique particulière, mais utilisant des outils conviviaux qu'on trouve dans l'underground de l'Internet, les "kiddies tools". Vous y trouvez même des kits "prêts à l'emploi".

Ces attaques sont silencieuses et les vecteurs d'infection, comme chevaux de Troie et bots spécialisés s'insèrent sans dégâts visibles dans les systèmes d'information des victimes ciblées. Aux virus dévastateurs succèdent les familles de chevaux de Troie, qui sont des bots, pour relayer les attaques, et des vers qui ne veulent surtout aucun mal à votre outil de travail et à vos informations, seulement à vos comptes bancaires. Bien au contraire, ils ont intérêt à ce que tout marche parfaitement chez vous. Mais tapis au fond de votre disque dur, ils observent. Les logiciels malfaisants attendent leur heure…

Et quand vous saisissez l'adresse Web de votre établissement bancaire, alors ils se réveillent et captent l'information que vous entrez : login, mot de passe, numéro de compte, date d'expiration de votre carte de crédit, tout est intercepté et envoyé au cybercriminel. Et ainsi le marché du renseignement sur les victimes potentielles est alimenté et rapporte gros. Il existe des keyloggers qui vont chercher l'information au niveau des touches du clavier que vous utilisez.

Vous pouvez certes chiffrer votre information sur votre PC, mais ce que vous tapez sur les touches de votre clavier, c'est de l'information en clair. La question hélas ne sera pas, avec la généralisation de la cybercriminalité, de savoir si vous avez ou pas un cheval de Troie dans votre système d'information, mais plutôt combien vous en avez, qui se battent en duel pour être peu nombreux à bénéficier de vos ressources informatiques.

MYTHE N° 4 :
LA SECURITE DE L'INFORMATION EST UN CENTRE DE COUT

Bien entendu s'équiper des matériels et logiciels indispensables, s'entourer d'experts sécurité compétents a un coût. Maintenir et bien gérer le système, établir des tableaux de bord conformément à sa politique de sécurité, et aux standards, exploiter les résultats des

évènements, des vulnérabilités, des non-conformités n'est pas une tâche anodine et mobilise des ressources humaines et pécuniaires.

Le coût de la sécurité pèse en général sur le budget informatique, et constitue parfois, hélas pour les victimes futures, une variable d'ajustement des budgets, surtout en temps de crise.

Mais l'insécurité a-t-elle un coût ? Si une entreprise victime d'une agression qui lui a fait perdre son fichier clients, l'historique de ses commandes, ses secrets de fabrication, son image de marque, et entaché la moralité de ses dirigeants, est appelée à disparaître à court terme après une attaque réussie, le coût de l'insécurité sera supporté par l'ensemble de l'entreprise, quand celle-ci devra fermer ses portes.

Mais si vous croyez que la sécurité est trop chère… essayez l'insécurité" ☺

MYTHE N° 5 :
LES ATTAQUES VIENNENT DE L'EXTERIEUR

Le côté obscur de la force qui pèse sur votre information peut certes venir de l'extérieur où une cohorte d'individus malfaisants menace vos finances et vos ressources. Ca ce n'est pas un mythe. Mais le mythe serait de croire que les méchants sont toujours à l'extérieur.

Le firewall qui isole votre réseau en bâtissant un périmètre de sécurité autour de votre système d'information et filtre tout ce qui sort et ce qui entre conformément à votre politique de sécurité est indispensable. Mais il ne sait pas ce qui se passe dans votre Intranet.

Les systèmes d'information aujourd'hui ne sont plus des places fortes qui doivent être entourées d'un rempart imprenable. Ils se rapprochent plus de pays avec des frontières, des ports mais aussi des aéroports d'où l'on peut pénétrer sans passer par les frontières. Sans compter, pour le criminel, la possibilité d'être parachuté près d'un endroit sensible. Il faut donc sécuriser plus que le périmètre de sécurité extérieur de votre entreprise. C'est d'autant plus vrai avec les technologies sans fils, le Peer to Peer, le Cloud Computing, qui, s'ils rendent des services indiscutables, n'en ouvrent pas moins des brèches dans le périmètre de sécurité d'une entreprise. Il faut aussi mettre des contre-mesures à l'intérieur de votre réseau d'entreprise.

Les employés sont-ils des méchants quand l'occasion fait le larron ? Pas tous, bien sûr, mais il faut garder à l'esprit qu'au moins 60% des attaques réussies, ont pour origine l'intérieur de l'entreprise, ou au moins des complicités dans l'entreprise.

MYTHE N° 6 :
LE CYBERMONDE EST UN ESPACE DE NON DROIT

La multiplication des attaques, largement plus médiatisée que les peines qui pourtant frappent les attaquants qui se font prendre, peut laisser penser que le cyber monde est un espace de non-droit où les malveillants, les maîtres chanteurs, les indélicats peuvent œuvrer en toute impunité et leurs victimes se faire agresser ou plumer sans recours. Il n'en est rien.

Mais comme l'Internet ne connaît pas de frontières, il n'est pas toujours évident de déterminer quelle juridiction s'applique. Droit du sol où le serveur Web malveillant réside ? Nationalités des agresseurs ? Nationalités des victimes ? Pays où se passe l'agression ? En France, l'article 113-2 du nouveau code pénal répond en partie à ces questions. Il s'appuie sur le principe de territorialité, établit que « *l'infraction est supposée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire* ».

Nous allons évoquer ici seulement des lois qui s'appliquent en France. N'étant pas juriste, je n'entrerai pas dans les détails. Chaque pays a ses propres lois et ses accords croisés avec d'autres pays ou communautés de pays et bien sûr les agresseurs avertis lancent de

préférence leurs attaques à partir de pays où la législation est très floue et l'extradition difficile. C'est bien sûr aussi dans ces mêmes pays que sont hébergés souvent les serveurs délictueux et les maîtres des Botnets.

En France, contrairement à ce qu'on peut croire, le cybercrime est encadré. Des lois existent et la jurisprudence commence à s'étoffer. D'ailleurs, plusieurs lois datant d'avant même la généralisation de l'utilisation de l'Internet sont applicables, telles la loi dites Godfrain, du 5 janvier 1985, articles L.323-1 et suivants du Nouveau Code pénal qui punit les *atteintes au système de traitement automatisé de données* et prévoit des amendes et des peines de prison même si aucune incidence directe n'a perturbé le système pénétré.

Mais le système judiciaire ne peut intervenir que si la victime ne tait pas le délit commis par l'attaquant et le préjudice subi et que si elle porte plainte.

Avec la volatilité des preuves, la difficulté de les tracer, l'anonymat facile, l'absence de frontières et une présence policière limitée, le cybermonde réunit tous les ingrédients pour être le théâtre d'un crime parfait, à moins que les victimes ne réagissent efficacement.

Si vous vous apercevez que vous avez été attaqués et avez subi des préjudices mais si vous ne portez pas plainte, l'agresseur ne sera sûrement pas inquiété. Si par contre vous portez plainte auprès de l'autorité compétente, il reste une petite chance pour que l'agresseur soit inquiété et cesse de s'attaquer à vous et aux autres. Comme avec l'Internet nous sommes tous liés, améliorer sa sécurité, c'est aussi améliorer la sécurité des autres.

Un web de signalement des infractions a été mis en place par le Ministère de l'intérieur, n'hésitez pas à l'utiliser, c'est ainsi que la vie peut devenir plus dure pour les cybercriminels :

www.internet-signalement.gouv.fr

MYTHES ET LEGENDES DE LA NAVIGATION SUR L'INTERNET

Michel Lanaspèze, SOPHOS

Vous pensez être bien protégé lorsque vous naviguez sur Internet ? Avec une nouvelle page infectée toutes les deux secondes, il est pourtant quasiment impossible de disposer d'une sécurité permanente sur le Web, même en étant parfaitement informé ou conscient des risques potentiels.

Posez-vous juste les questions suivantes :

Pratiquez-vous une navigation prudente sur le Web ? Evitez-vous les sites à risque ? Utilisez-vous un navigateur sécurisé ? Savez-vous reconnaître lorsqu'un site présente un risque quelconque ? Limitez-vous la navigation pendant les heures de travail ? Avez-vous mis en place une politique stricte d'accès à Internet ?

Si répondez "oui" à l'une de ces questions, alors nous vous recommandons vivement de lire la suite. Vous pourriez être la victime de préjugés sur la sécurité d'Internet. Mais ne vous inquiétez pas, vous n'êtes pas seul. Ces dernières années ont vu beaucoup de désinformations circuler sur les risques du Web, leurs effets potentiels et ce qu'il faut faire pour s'en protéger.

MYTHE N° 1 :
LE WEB EST SUR CAR JE N'AI JAMAIS ETE INFECTE PAR DU MALWARE EN NAVIGUANT SUR LE WEB

Si vous faites partie des rares internautes à ne pas encore avoir pris conscience du danger, il est malheureusement assez probable que vous ayez déjà été infecté sans le savoir.

En effet, depuis plusieurs années déjà, la navigation Web est devenue le principal vecteur d'infection par des malwares. Une nouvelle page Web est compromise toutes les deux secondes pour être transformée en page Web infectieuse. De plus, la majorité du spam qui arrive dans vos boîtes aux lettres électroniques essaie de vous diriger vers une de ces pages Web infectieuses, un site Web contrefait (attaque par hameçonnage ou « phishing ») ou des sites de vente en ligne douteux.

Comme l'écrasante majorité des infections est silencieuse, les internautes sont rarement conscients d'avoir été infectés quand ils ne bénéficient d'aucun système de protection. Généralement, les attaques de malware sur le Web sont conçues pour dérober des mots de passe et des informations personnelles, ou pour utiliser votre poste à votre insu comme plate-forme de distribution de spam, de malwares ou de contenu inapproprié.

MYTHE N° 2 :
SEULS LES SITES A CARACTERE PORNOGRAPHIQUE, JEUX D'ARGENT ET AUTRES SITES "SUSPECTS" PRESENTENT UN DANGER

Plus de 80 % des sites hébergeant du malware sont en fait des sites dits de confiance qui ont été piratés. Les internautes les consultent quotidiennement sans savoir qu'ils ont été piratés pour distribuer des malwares.

Pourquoi ? Parce qu'ils sont populaires, ces sites attirent un fort trafic et permettent de distribuer du malware aux visiteurs à leur insu et en grande quantité.

Même s'il est avéré que certaines catégories de sites sont considérablement plus affectées que d'autres, les sites d'entreprises réputées sont susceptibles d'être infectés. Il suffit pour cela d'une page Web mal codée ou d'une nouvelle vulnérabilité du serveur Web non corrigée pour ouvrir la porte aux pirates.

Il est donc essentiel que les internautes restent vigilants, même quand ils limitent leur navigation à des sites de confiance.

MYTHE N° 3 :
AU MOINS, LES RESEAUX SOCIAUX SONT-ILS SURS PUISQUE JE M'Y RETROUVE ENTRE AMIS.

C'est un mythe qu'il faut combattre de toute urgence, pour que les internautes ne baissent pas la garde quand ils socialisent sur ces nouveaux espaces d'échanges.

En effet, les réseaux sociaux sont rapidement devenus le nouveau champ d'action privilégié des pirates informatiques et autres cybercriminels. Il n'y a rien d'étonnant à cela, les attaques informatique de masse suivant leurs victimes potentielles là où elles se retrouvent en nombre. Qui plus est, ce nouvel espace représente une cible de choix car les internautes s'y sentent en confiance, étant en principe entourés d'amis.

Les pirates sont ainsi passés experts dans le vol de comptes et mots de passe de réseaux sociaux, qu'ils utilisent pour infecter et arnaquer les cercles d'amis. Un moyen relativement simple utilisé par les pirates pour récupérer ces informations de comptes consiste à envoyer des messages de spam vous enjoignant de vous connecter de toute urgence sur votre réseau social préféré, prétextant la nécessité d'une supposée mise à jour ou d'une vérification administrative. Le lien qui vous sera proposé n'est autre qu'une version contrefaite de la page d'accès au réseau social, créée dans le seul but de voler votre compte et votre mot de passe. Une fois en possession d'un accès à votre compte, le pirate s'empressera de modifier votre mur ou d'ajouter des messages invitant vos amis à cliquer sur un lien intéressant, qui n'est autre qu'une page infectieuse ou un site d'arnaque.

L'intérêt croissant des pirates pour les réseaux sociaux les a mené à créer des malwares spécialisés, tels que la célèbre famille Koobface. Les malwares de cette famille sont si sophistiqués qu'ils sont capables de créer automatiquement un compte Facebook, de l'activer en confirmant le courriel envoyé à une adresse Gmail (qu'ils auront pris soin de créer auparavant automatiquement), de devenir amis avec des inconnus inscrits sur le site, de rejoindre des groupes Facebook et de diffuser des messages sur les murs de ses amis, prétendant diriger vers des vidéos sexy contenant en réalité du malware. De plus, il cherche à assurer sa discrétion en restreignant le nombre de nouveaux amis qu'il accepte par jour. Au départ limité à Facebook, dont il a d'ailleurs tiré son nom, Koobface a depuis élargi sa cible en visant un grand éventail de sites. Apparue en 2008, cette famille ne cesse de se raffiner et se diversifier, faisant preuve d'une longévité tout à fait exceptionnelle dans le monde des malwares, ce qui illustre l'engouement des pirates pour les réseaux sociaux.

MYTHE N° 4 :
VOUS NE POUVEZ ETRE INFECTE QU'EN TELECHARGEANT DES FICHIERS

La plupart des infections par malwares se produisent aujourd'hui par téléchargement passif, qui ne requiert aucune action de la part de l'internaute si ce n'est le simple fait de visiter un site.

Les pirates injectent du code malveillant dans le contenu de leur page web, qui se télécharge et s'exécute automatiquement dans le navigateur comme une sous-fenêtre de visualisation de la page Web.

Un bon exemple de ce type d'attaque est fourni par la famille Gumblar. Cette famille de malwares a représenté jusqu'à 40% de toutes les infections de sites Web. Après une éclipse en fin d'année 2009, elle est revenu sur le devant de la scène début 2010. Il s'agit d'un code JavaScript malveillant infecté au sein de sites web légitimes, dans le but de rediriger les visiteurs vers des sites web contrôlés par les pirates, qui tentent d'exploiter des vulnérabilités d'Acrobat Reader et de Flash/Shockwave pour infecter le système. C'est un type d'attaque par téléchargement passif auquel appartient également la célèbre injection iFrame.

MYTHE N° 5 :
SEULS LES UTILISATEURS NAÏFS SE FONT INFECTER PAR DES VIRUS ET DES MALWARES

Comme mentionné précédemment, la plupart des infections s'effectuant par téléchargement passif, l'infection n'a donc rien à voir avec les compétences informatiques de l'utilisateur. En réalité, dès lors que vous visitez des sites Internet, le risque existe.

Ces malwares sont très souvent créés à partir de kits de code malveillant professionnel, commercialisés et vendus aux pirates, qui les utilisent pour exploiter les failles dans le navigateur, le système d'exploitation et les plug-ins et infecter les systèmes. Encore une fois, cela s'effectue de manière totalement invisible aux yeux de l'utilisateur qui visite simplement un site piraté.

Un système parfaitement tenu à jour des derniers correctifs de sécurité contre les vulnérabilités connues du système d'exploitation, du navigateur, de ses plug-ins et des applications Web présente cependant un défi certain pour les pirates. Ils peuvent néanmoins toujours s'appuyer sur les vulnérabilités non corrigées ou, plus simplement, la naïveté de certains utilisateurs face aux attaques par « ingénierie sociale ».

Une des attaques les plus en vogue consiste à proposer les services d'un faux antivirus. En naviguant ainsi sur une page Web compromise, l'internaute sera d'abord soumis, en général, à une première tentative d'infection silencieuse par l'intermédiaire d'une faille de sécurité éventuelle. Si cette attaque échoue, le malware passe alors au « plan B », celui du faux antivirus. Pour cela, il ouvre des fenêtres présentant à s'y méprendre l'aspect d'un antivirus ordinaire, mais de marque inconnue, qui va après quelques secondes déclarer avoir détecté plusieurs virus. Il vous proposera alors de désinfecter gratuitement votre ordinateur, en vous demandant de valider son activation. En cliquant sur « oui », vous donnez en réalité l'autorisation à un malware de s'installer sur votre système. En guise de « cerise sur le gâteau », beaucoup de ces faux antivirus vous proposeront ensuite d'acheter une licence illimitée à prix cassé, qui n'aura d'autre but que de récupérer votre numéro de carte de crédit !

Dans ces cas d'attaque par ingénierie sociale, il est effectivement recommandé d'être constamment sur ses gardes et ne pas pêcher par naïveté.

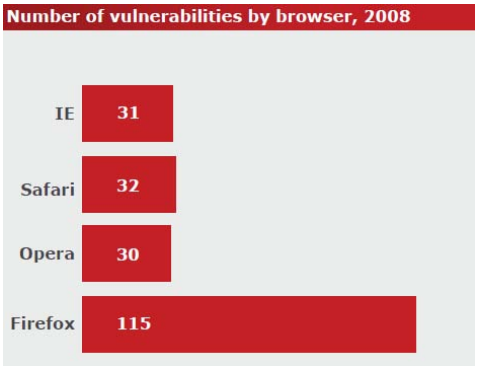
MYTHE N° 6 :
FIREFOX EST PLUS SUR QU'INTERNET EXPLORER

Tous les navigateurs sont exposés de façon identique aux risques car ils constituent tous un environnement d'exécution de JavaScript, qui est le langage de programmation employé pour Internet.

C'est pourquoi tous les auteurs de malwares l'utilisent pour initier des attaques. De plus, de nombreuses failles exploitent les plug-ins, tels que le logiciel Acrobat Reader, qui fonctionnent avec tous les navigateurs.

Bien que les navigateurs les plus utilisés sont plus connus pour leurs failles sans correctifs, ce sont les failles qui ne font pas parler d'elles qui devraient vous alerter le plus. En réalité, il n'existe aucun navigateur sûr.

Quant à Firefox, une étude réalisée par la société de recherche en sécurité Secunia portant sur le nombre de failles des navigateurs en 2008, a montré qu'il n'occupait pas nécessairement la première place des navigateurs les plus sûrs, et de loin.



Source : http://secunia.com/gfx/Secunia2008Report.pdf

D'une manière générale, quel que soit le navigateur que vous utilisez, il est essentiel de le tenir parfaitement à jour des plus récents correctifs de sécurité.

Ceci présente un défi particulier en entreprise, où nombre d'utilisateurs souhaiteraient utiliser leur navigateur préféré, quitte à importer une version mal corrigée d'un navigateur. Il faut rappeler aux internautes qu'un des premiers bénéfices que leur peut apporter leur entreprise est une navigation sûre, et qu'à ce titre il est non seulement légitime mais dans leur propre intérêt que l'entreprise contrôle les versions des navigateurs utilisés sur son réseau.

MYTHE N° 7 :
LORSQUE L'ICONE DE VERROUILLAGE APPARAIT DANS LE NAVIGATEUR, JE SUIS EN SECURITE

L'icône de verrouillage indique la présence d'une connexion chiffrée SSL entre le navigateur et le serveur afin de protéger contre l'interception des informations sensibles personnelles. Mais il n'apporte aucune sécurité contre les malwares.

En fait, c'est même le contraire.

En effet, la plupart des produits de sécurité Web ignorent complètement les connexions chiffrées : c'est donc le parfait vecteur pour infiltrer du malware sur un poste.

De plus, certains malwares peuvent exploiter des vulnérabilités pour imiter des certificats SSL, donnant ainsi aux utilisateurs l'impression d'être sécurisés, ou activer des connexions détournées vers de faux sites bancaires. De nombreux cas récents illustrent comment les pirates créent des techniques sophistiquées de phishing qui permettent de reproduire des sites complets de banque en ligne, avec cartes de crédit et comptes PayPal, via l'imitation de certificats SSL, extrêmement difficiles à identifier pour l'utilisateur moyen. Ces méthodes engendrent des risques de sécurité de plus en plus élevés.

MYTHE N° 8 :
NOUS CONTROLONS L'UTILISATION DU WEB ET NOS UTILISATEURS NE PEUVENT PAS CONTOURNER NOTRE POLITIQUE

Beaucoup d'internautes sont passés maîtres dans l'utilisation de « proxies anonymes » pour contourner la politique de filtrage Internet et consulter les sites Web de leur choix. D'abord popularisés dans les milieux étudiants, les proxies anonymes sont nombreux et facilement accessibles par les utilisateurs. Chaque jour, des centaines de proxies anonymes sont conçus et mis en ligne dans le but de contrer les barrages de sécurité des entreprises et les utilisateurs les plus sophistiqués établissent même leur propre proxy privé à la maison pour pouvoir naviguer sur le Web en toute liberté et échapper à tout contrôle.

Si vous avez tendance à minimiser le problème, il vous suffit de consulter les très nombreuses pages proposant des moyens d'éviter le filtrage Internet sur Google pour vous rendre compte de l'ampleur du phénomène.

Il est donc fortement recommandé de mettre en place des solutions de protection permettant d'éviter le contournement des politiques de sécurité par des proxies anonymes.

MYTHE N° 9 :
DE TOUTE MANIERE, NOUS NE POUVONS RIEN CONTROLER QUAND LES CONNEXIONS SONT CHIFFREES PAR HTTPS

Les connexions chiffrées présentent un défi particulier car dans ce cas, il n'est pas possible de vérifier que des malwares ne sont pas introduits dans l'entreprise ou que des informations sensibles, comme des informations à caractère personnel au sens de la CNIL, ne sont pas diffusées hors de toute légitimité.

De nombreuses solutions de protection de la navigation Web permettent cependant de filtrer le trafic HTTPS. Généralement installées en passerelle, elles n'autorisent l'établissement de connexions HTTPS qu'à condition de leur donner un droit de regard pour appliquer les politiques de sécurité de l'entreprise.

Bien entendu, ce type de filtrage doit être déclaré explicitement dans la charte des politiques de sécurité de l'entreprise, revue et validée par les représentants du personnels et acceptée explicitement par les employés eux même. Ce filtrage exclue en général les connexions vers certains sites, comme ceux d'établissement bancaires et financiers reconnus, afin de préserver la confidentialité complète et légitime de certaines communications.

Il est bon de rappeler que si l'utilisation d'Internet pour des motifs personnels est tolérée en entreprise, elle reste soumise aux politiques de sécurité définies par l'entreprise, qui s'attachent à défendre aussi bien les propriétés intellectuelles de l'entreprise, les droits collectifs des individus comme définis par la CNIL et le droit des employés à pouvoir naviguer sur le Web en toute sécurité.

MYTHE N° 10 :
LA PROTECTION DU WEB SUPPOSE UN COMPROMIS ENTRE SECURITE ET LIBERTE

Internet est devenu un outil indispensable pour les entreprises. Mais que ce soit Facebook pour les ressources humaines ou Twitter pour les relations publiques, il n'y a pas de compromis à faire entre liberté d'accès et sécurité.

Une bonne solution de sécurité doit permettre d'accéder aux sites dont vos utilisateurs ont besoin dans le cadre de leur travail, tout en maintenant l'entreprise sécurisée.

Même quand l'entreprise décide d'applique des restrictions sur les types de sites accessibles, il faut toujours garder à l'esprit que pour les utilisateurs, la première des libertés consiste à pouvoir naviguer sur le Web en toute sécurité.

CONCLUSION

Comme dans tous les autres domaines de la sécurité informatique, l'éducation des utilisateurs représente la première protection contre les menaces. A ce titre, il est essentiel que les internautes prennent pleinement conscience des dangers qui les guettent, afin de se tenir sur leurs gardes et de ne pas se précipiter dans les pièges, parfois grossiers, qui leur sont tendus.

Il est également bon de rappeler la nécessité d'une bonne hygiène de son ordinateur, qui commence par l'installation régulière des derniers correctifs de sécurité, aussi bien sur le système d'exploitation que sur les applications Web, et par la mise en place d'une protection anti-malware parfaitement mise à jour, qui bénéficie si possible d'une fonction de blocage de l'accès aux pages Web malveillantes. En entreprise, cette protection sur les postes de travail sera en outre complétée par une protection au niveau de la passerelle Internet.

MYTHES ET LEGENDES DES RISQUES DE CYBERGUERRE SUR LES INFRASTRUCTURES VITALES

Franck Franchin, FRANCE TELECOM

MYTHE N° 1 :
LES SYSTEMES CRITIQUES SONT PROTEGES DES ATTAQUES GRACE A LEUR REDONDANCE

Dans de nombreux secteurs d'activité industrielle, 2 ou 3 fournisseurs se partagent désormais le marché des systèmes de supervision, de commande et de contrôle (les fameux SCADA), sous forme d'un duopole ou d'un oligopole. Cela entraine que la redondance des systèmes à caractère critique est souvent assurée par le même logiciel ou le même matériel, simplement dupliqués, afin de permettre une redondance à froid ou à chaud.

Que se passe-t-il donc si un système est attaqué ? On peut scénariser une attaque en cinq phases :

- Phase préparatoire de reconnaissance, infiltration et renseignement – ouverture des accès nécessaires à l'attaque
- Phase d'attaque
- Découverte de l'attaque par la victime
- Mesure de défense
- Forensique et post-mortem

Lorsque l'attaque est découverte, la victime peut adopter plusieurs stratégies : arrêter totalement le système et/ou le processus concerné ou basculer sur le système de secours. Grande question : est-ce que le système de secours a été compromis ?

Dans un avion, les commandes de vols vitales sont doublées, via des technologies différentes : câbles électriques, fibres optiques, circuits hydrauliques et passent par des chemins physiques différents. Il existe aussi des modes dégradés lorsque la redondance des systèmes est trop complexe ou trop couteuse à implémenter.

Avec un système informatique, comment s'assurer d'une vraie redondance quand le système d'exploitation est du même fournisseur, voire de la même version, sans même parler du même logiciel métier. Comment être sûr que le système de secours est vraiment 'isofonctionnel' (et donc mis à jour comme le système 'en production') ?

Si on prend comme référence la fameuse affaire Stuxnet, la préconisation de Siemens une fois l'attaque connue fut... de ne surtout toucher à rien et surtout de ne pas changer le mot de passe qui était codé en dur dans les programmes ! Le remède risquait d'être plus grave que la maladie. Rappelons qu'on parle pourtant de systèmes à plusieurs millions d'euros qui régulent et pilotent des centrales nucléaires, des usines chimiques et autres activités à risque.

Il y a donc redondance et redondance. Quand on implémente la redondance de deux baies de disques durs amenées à stocker des données très sensibles, on utilise des processus logiques et physiques de redondance à froid et à chaud (les fameux disques durs hot plug ou les modes de stockage de type RAID) mais on s'assure aussi que les disques durs eux-mêmes ne proviennent pas du même fabricant pour chaque baie. Et si ce n'est pas possible, on prend des lots fabriqués à des dates différentes pour ne pas risquer un même défaut de fabrication.

Il est beaucoup plus difficile d'appliquer cette saine philosophie dans le monde informatique des logiciels.

Un exemple très simple : imaginez que vous soyez journaliste, que votre outil critique soit votre traitement de texte et que vos missions nécessitent une disponibilité de votre outil à 100%. La solution pour s'affranchir des failles ou des attaques informatiques consisterait à avoir un ordinateur PC sous Windows et un autre ordinateur Apple sous MacOS. Au niveau logiciel, vous pourriez avoir un OpenOffice d'un côté et un Microsoft Word de l'autre. Cela fonctionnerait très bien tant que le journal pour lequel vous travaillez n'ait pas choisi d'implémenter des macros spécifiques Word qui n'existent pas sous OpenOffice. La solution serait alors d'être iso-outil et d'avoir Word sur les deux machines. Sauf que Word sous Windows et Word sous MacOS ne sont pas totalement iso-fontionnels, voire compatibles (selon l'éditeur, cela serait corrigé dans la version 2012). La seule solution définitive serait alors d'avoir deux ordinateurs PC avec Word sous Windows, l'un sous Windows Seven, l'autre sous Windows XP, par exemple. En espérant que les macros se comportent exactement de la même manière sous les deux systèmes exploitation.

Hélas, le choix est encore plus limité pour les systèmes de supervision, de commande et de contrôle en milieu industriel de type SCADA. La solution retenue pour la redondance est donc très souvent une copie synchronisée du système en production, avec bascule des données, voire des données de session. La meilleure façon d'avoir deux systèmes aux vulnérabilités strictement identiques.

Cela signifie que la meilleure redondance reste souvent la décision et l'arbitrage humain. Encore faut-il que l'attaque ait été décelée à temps. Dans l'exemple précédent de Stuxnet, l'attaque modifiait certains paramètres bien particuliers de processus industriels très complexes. Seules les victimes savent aujourd'hui réellement le temps qu'a duré l'attaque avant qu'elles ne s'en soient aperçu. Certaines centrifugeuses iraniennes ont eu des baisses de rendement inexpliquées bien avant qu'on évoque du bout des lèvres l'éventualité de Stuxnet…

MYTHE N° 2 : INTERNET EST UNE INFRASTRUCTURE CRITIQUE PRIMORDIALE

Lorsqu'on se demande si l'Internet est une infrastructure critique primordiale, la grande question à se poser est sans aucun doute : *peut-on vivre sans* ?

Bien évidemment, l'Internet a pris une si grande importance dans nos vies professionnelles ou personnelles quotidiennes, qu'il est difficile d'imaginer devoir ou pouvoir s'en passer. Tout comme il semble impensable qu'une économie ou qu'un État puisse fonctionner sans lui.

D'ailleurs, l'Histoire récente des conflits politiques ou militaires entre certains pays de l'ancien Bloc de l'Est nous rappelle que l'attaque des réseaux et des services de communication fait bien partie de la doctrine militaire et des actions de désorganisation propres à la préparation de toute velléité plus ou moins belliqueuse.

Toutefois, une simple taxinomie des services vraiment vitaux au fonctionnement d'un État, c'est à dire à sa capacité à assurer ses fonctions régaliennes, nous oblige à négliger quelque peu le grand Internet. Rappelons ici quelles sont les grandes fonctions régaliennes d'une démocratie :

- Frapper la monnaie (et gérer et protéger la devise du pays)
- Définir le droit et rendre la justice
- Assurer la sécurité du territoire et des citoyens

Au niveau du citoyen, de l'être humain, les besoins réellement vitaux sont :

- S'alimenter (eau et nourriture)
- Accéder aux soins nécessaires (médecine générale, petite et grosse chirurgie, médicaments)
- Disposer d'un hébergement convenable (chauffage, lieux d'aisance)

Le lecteur notera d'ailleurs qu'une certaine partie de l'Humanité n'a pas la chance de se poser ces questions car elle ne dispose pas, sur une base quotidienne, de ce niveau de base que nous considérons comme 'vital'…

La question est donc de savoir dans les six points précédents quels seraient les impacts d'une indisponibilité de l'Internet, que ce soit suite à des attaques physiques ou logiques ou que ce soit par défaillance du réseau énergétique.

En terme de sécurité des personnes et des biens, les services de l'État (police, gendarmerie, pompiers, armées) disposent des moyens de communication nécessaires, même si certains services ont succombé aux charmes de la VoIP. Habitués aux situations de crise, ils savent mettre en place des réseaux de secours si nécessaire. Le risque résiderait éventuellement sur les incompatibilités de certains réseaux entre eux.

En terme de distribution de l'électricité et de l'eau courante, certains systèmes de supervision et de contrôle sont connectés via l'Internet. Cela peut donc poser problème. Toutefois, les fonctions critiques peuvent être assurées soient de manière autonome, soient à travers des réseaux qu'on peut qualifier de privatifs.

En terme de distribution d'eau potable et de nourriture, il est vrai que les échanges commerciaux et logistiques sont désormais basés sur des procédures automatisées de type EDI/XML et que la plupart des réseaux de négoce passent par l'Internet, sous VPN ou non. Toutefois, il serait assez facile de passer en mode dégradé, à partir du moment où les parties prenantes disposeraient des moyens de communication adéquats et que les carburants, nécessaires au transport routier, ne viendraient pas à manquer. Ces contraintes sont assez bien identifiées et prises en compte dans la plupart des plans de crises étatiques.

Restent les services de santé au sens large. Leur criticité et leurs vulnérabilités sont très variables. Toutefois, à partir du moment où l'accès à l'énergie (chauffage et électricité) est maintenu et que les communications d'urgence sont assurées, les prestations d'urgence peuvent être maintenues dans leur très grande majorité, de manière indépendant de l'Internet.

Au risque de surprendre, le seul impact réellement majeur me semble être celui pouvant toucher la distribution d'argent liquide et le paiement par carte. Il convient de ne pas minimiser cet aspect qui pourrait être risque de grand désordre, voire de panique, pour les populations civiles. La plupart d'entre nous, dans nombre de pays occidentaux, ont l'habitude de ne pas avoir plus de 100 euros d'argent liquide sur eux, ce qui serait insuffisant en cas de crise impactant le réseau bancaire pendant plus d'une semaine.

Pour conclure, mon propos n'est pas de minorer les impacts graves et évidents qu'aurait une défaillance de l'Internet sur notre économie mais de la relativiser sur notre vie quotidienne. Il ne s'agirait pas d'une crise humaine à grande échelle. Une grève des transports routiers ou une grève du raffinage de carburant serait bien plus grave et coûteuse.

MYTHE N° 3 :
NOUS AURONS UN PEARL-HABOR DIGITAL DANS LES DIX PROCHAINES ANNEES

Cette phrase est extraite d'une audition d'expert devant le Sénat américain en 1998. Déjà en 1993, John Arquilla et David Ronfeld faisaient trembler les Etats-Unis en annonçant la cyberguerre prochaine.

Que s'est-il passé depuis ? Des événements bien plus graves qu'un Pearl Harbor numérique: l'affaire Madoff, la crise des surprimes, le dépôt de bilan virtuel des PIGs, la Corée du Nord qui joue avec le feu. Qu'en penser ?

Tout d'abord, il y a une grande différence en terme de doctrines et d'impacts entre un Pearl-Habor numérique et une cyberguerre (voir Mythe N°5).

Les ardents défenseurs de ce mythe ont avancé plusieurs arguments au fil des ans. Dans un premier temps, il y a 10-15 ans environ, le monde devait redouter qu'une bande de méchants génies de l'informatique, ultralibertaires, altermondialistes, pirates ou terroristes, s'en prenne à nos infrastructures vitales : transport, hôpitaux, centrales nucléaires, trafic aérien, etc.

Aujourd'hui, ce sont des Etats qui cyber-combattent de manière directe ou indirecte (Russie-Georgie, Russes-Estonie) ou des Etats contre des entreprises (Chinois/Chine contre Google).

Le problème est probablement ailleurs. Les Etats-Unis vont dépenser entre 50 et 75 milliards de dollars pendant la période 2010-2015 pour leur doctrine de cyberguerre. Une manne inespérée pour les Boeing, Northrop, Lockheed et autre Thalès. Des rapports alarmistes fleurissent dans les différents cercles de lobbying européens et américains, tous financés directement ou indirectement par des tierces parties qui ont des intérêts à cette cyberprogagande.

Nous sommes dans le domaine du fantasme, quelque fois entretenu par des journalistes en manque d'un bon papier. Les réseaux du Pentagone sont attaqués des centaines de fois par jour et si on en croit Siemens, seule une petite vingtaine de systèmes Scada ont été concernés par Stuxnet et de toute façon sans impact particulier (sic).

A ce jour, le seul Pearl-Harbor réellement numérique fut probablement WikiLeaks. Et tous les moyens financiers, juridiques, diplomatiques, policiers et militaires des Etats concernés n'ont pu y mettre réellement fin, à l'heure où j'écris cette phrase (Décembre 2010).

MYTHE N° 4 :
LE CYBER-TERRORISME EST UNE MENACE IMPORTANTE

Quand on lit la presse ou les documents gouvernementaux d'origine anglo-saxonne, et particulièrement en provenance des Etats-Unis, on frémit à la simple allusion de la possible éventualité d'un acte de cyber-terrorisme. A la défense de nos amis américains, il y aura toujours un avant et un après 9/11. Il est difficile pour nous européens de comprendre vraiment à quel point cette tragédie les a touchés au plus profond de leurs âmes et de leurs certitudes. Il convient donc de comprendre que leurs réactions étatiques,

qui nous paraissent parfois endémiques ou disproportionnées, sont tout à fait normales, et légitimes, dans leur esprit.

Cela étant dit et reconnu, quel est le risque réel d'une menace cyber-terroriste ? Au risque de surprendre, je dirais pratiquement aucun. Non pas que je souhaite minimiser ce risque ou cette menace, mais simplement parce que je suis convaincu que les-dits terroristes disposent de moyens bien plus efficaces (si le lecteur me permet cette expression) pour arriver à leurs fins.

Le Dr. Dorothy Denning a donné en 2007 la définition suivante pour le cyber-terrorisme :

"...the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objections. Further, ***to qualify as cyberterrorism, an attack should result in violence against persons or property, or at the least cause enough harm to generate fear****. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples."*

La notion de 'génération de terreur' est très importante dans la doctrine de la plupart des terroristes. Je me permettrais de rajouter à la définition précédente que l'acte terroriste doit être en soit un acte de communication, qui marque les esprits, qui permet de faire les gros titres des médias pendant plusieurs jours, plusieurs semaines.

La plupart des réseaux terroristes ont deux objectifs principaux :

- Développer leur réseau de soutien et assurer le financement de leurs activités
- Creuser le fossé culturel, politique, émotionnel entre leurs partisans (ce que j'appelle les identitaires) et le reste du monde (les oppresseurs et les victimes potentielles...)

On est très proche de l'esprit des sectes.

Dans cet esprit, tout acte terroriste doit répondre de manière directe ou indirecte à ces objectifs.

Une erreur courante consiste à croire que les terroristes sont des gens irrationnels. Bien au contraire, un terroriste agit en général de manière très pragmatique et très logique. Simplement, c'est sa logique propre que nous avons du mal à comprendre, en particulier car nous refusons son mode de pensée. Un terroriste pense toujours que son action est légitime par rapport à son référentiel de pensée et/ou de croyance. Il n'a pas à justifier ses crimes car il ne se considère pas comme un criminel. Selon ses propres référentiels, c'est lui qui est la victime, le martyr, le héros.

Les organisations terroristes sont de grands utilisateurs du cyberespace. Tout d'abord, ils ont rapidement pris conscience de l'énorme capacité de l'Internet, de cet espace de 'liberté de pensée et d'expression', comme outil de propagande, de recrutement et de financement (directement ou indirectement via la cybercriminalité). On a pu découvrir dans certaines affaires que ces organisations maîtrisaient parfaitement les outils et les méthodes d'anonymisation, d'offuscation, de déni de service distribué (DDoS) et de chiffrement. On sait aussi que les plus importantes d'entre elles ont mis en place depuis plusieurs années des cellules spécialisées, à l'image de nos armées.

Ces organisations ont donc tout à fait les capacités techniques, financières et logistiques pour mener avec succès des actions et des attaques dans le cyber-espace. Quand on voit qu'une poignée de script-kiddies, défenseurs des idées libertaires de WikiLeaks, ont pu mettre à mal pendant des heures des sites bancaires comme PostFinance.ch ou Paypal, on peut aisément imaginer ce que des terroristes déterminés pourraient faire pour nuire à des intérêts vitaux des Etats cibles. Et pourtant, aucune attaque cyber-terroriste importante n'a été révélée à ce jour.

J'oserais plusieurs explications possibles.

Tout d'abord, en reprenant la définition ci-dessus, quels seraient les points d'emploi d'un acte cyber-terroriste qui concernerait les infrastructures vitales et qui serait générateur d'extrême violence et/ou d'extrême terreur. Quelques exemples viennent immédiatement à l'esprit : hacking d'un réseau de distribution d'eau, d'une centrale nucléaire, d'un réseau de contrôle ferroviaire. Mon sentiment est que le résultat serait bien faible par rapport aux moyens engagés grâce aux contrôles, aux régulations et au facteur humain qui, pour une fois, serait à notre avantage. Si on veut s'attaquer à un réseau d'eau, il est bien plus facile d'introduire des produits nocifs en aval des systèmes de capteurs, d'analyse et de protection…Si on veut mettre en danger une centrale nucléaire, il est bien plus facile de le faire de l'intérieur, voire de l'attaquer avec un commando suicide. Les récentes attaques de bases ultra-sécurisées en Afghanistan en donnent un triste exemple. Bref, le coût d'opportunité serait disproportionné par rapport à d'autres attaques possibles.

Ce n'est clairement pas un objectif prioritaire actuel des organisations terroristes alors qu'elles disposent d'armées de martyrs prêts à se faire sauter pour leur cause (je refuse d'utiliser le terme de Kamikaze par respect vis à vis de ces héros japonais).

Toutefois, mon analyse des doctrines terroristes actuelles me conduit à suggérer un risque différent : celui d'une attaque cyber-terroriste de nos infrastructures vitales comme partie d'un plan d'action coordonné plus global. Par exemple :

- Pour 'fixer' les organisations gouvernementales
- Pour désorganiser l'Etat et les populations
- Pour amplifier l'acte terroriste 'physique' principal.

Ce livre n'a cependant point le propos de définir ni de proposer des scénarios d'attaques terroristes et c'est pourquoi je n'irai pas plus loin dans les détails.

Gageons que les plus hautes autorités sont conscientes de ces risques et que des scénarios, des exercices et des plans de crise sont déjà opérationnels.

MYTHE N° 5 :
LA GUERRE DE TROIE N'AURA PAS LIEU

Au contraire des raisonnements présentés dans les 4 mythes précédents, je serai hélas bien moins optimiste pour ce Mythe N°5.

Toutes les armées et les gouvernements du monde se préparent depuis presque 10 ans à la guerre cybernétique. La question n'est pas de savoir désormais *pourquoi* ou *comment* mais *quand*.

Récemment, début 2010, Mike McConnell, ancien directeur de la NSA, avançait même que les Etats-Unis étaient en train de perdre cette fameuse cyberguerre.

D'ailleurs, sémantiquement parlant, cette Guerre de Troie numérique a déjà eu lieu. Quand le Hezbollah a piraté les flux vidéos des drones israéliens, ou quand des russes ont attaqué les réseaux bancaires et media de l'Estonie, c'étaient des actes de cyberguerre ou de cyberguerilla. Sans parler du détournement du trafic de l'Internet mondial pendant 18 minutes via la Chine, suite à une 'erreur' malencontreuse de China Telecom.

Il est intéressant de noter qu'en matière de cyberguerre, certains pays ont mis en place des unités opérationnelles offensives avant même de parler leur propre politique de défense.

Pour les experts en sécurité, ce qui fait froid dans le dos, ce n'est pas tant la débauche de moyens militaires ou privés qui semblent se préparer au pire, mais plutôt les discours de certains politiques qui clament haut et fort que leurs pays sont bien protégés et à l'abri de toute cyberattaque.

Il est bien connu que la meilleure façon de minimiser ses faiblesses, c'est de les clamer haut et fort publiquement en les considérant comme des forces !

MYTHES ET LEGENDES DES VULNERABILITES LOGICIELLES

Nicolas Ruff, EADS Innovation Works

MYTHE N° 1 :
TROUVER DES VULNERABILITES , C'EST COMPLIQUE (RESERVE AUX EXPERTS)

Dans le domaine des failles de sécurité, il y a bien deux compétences disjointes (souvent détenues par des personnes différentes d'ailleurs): la découverte des failles, et la transformation des failles en attaques (appelée *exploitation* ou simplement *exploit* dans le jargon).

Si la deuxième compétence reste et restera réservée aux experts techniques, il est au contraire à la portée de n'importe qui de découvrir des failles.

Vous avez reçu un document endommagé qui fait "planter" Word ? Vous avez peut-être entre les mains une bombe !

Vous avez rempli un formulaire en ligne et le serveur vous a retourné un message incompréhensible car vous avez un guillemet simple (') dans votre nom de famille ou dans votre mot de passe ? Vous avez peut-être trouvé un moyen de compromettre à distance le serveur !

En pratique, quiconque a pratiqué l'audit de sécurité pendant quelques années a forcément découvert des vulnérabilités dans des dizaines de logiciels pourtant largement utilisés. Il y a un fossé entre le sentiment de sécurité des utilisateurs (souvent béats devant la technologie), et la sécurité effective de leurs applications.

COROLAIRE: UN LOGICIEL QUI N'A AUCUNE VULNERABILITE CONNUE EST "SUR"

Archifaux ! Un logiciel qui n'a aucune vulnérabilité connue n'a jamais été audité sérieusement et/ou son éditeur n'a pas de processus sérieux de gestion des vulnérabilités (ce qui inclut correction et communication).

MYTHE N° 2 :
MAINTENANT QUE LA SECURITE EST DEVENUE UN ENJEU IMPORTANT POUR LES EDITEURS, LE NOMBRE DE VULNERABILITES VA DIMINUER

Il est certain que la sécurité informatique n'a jamais bénéficié d'autant de couverture médiatique (n'allons pas jusqu'à dire de moyens :). Pourtant le nombre de nouvelles vulnérabilités ne baisse pas - il a même plutôt tendance à augmenter !

La raison ? C'est que la plupart des "gros" logiciels que nous utilisons actuellement a été développée il y a fort longtemps, dans un monde très différent du nôtre. Un monde où les quelques personnes interconnectées l'étaient via RNIS, et où la principale menace était la disquette. Pour des raisons de coût et de compatibilité, ces logiciels ne sont pas prêts d'être réécrits.

Et en ce qui concerne les nouveaux logiciels qui sont développés actuellement ? Ils le sont par des stagiaires ou des sous-traitants *offshore*, qui reproduisent exactement les mêmes erreurs qu'il y a 30 ans !

MYTHE N° 3 :
TOUT LE MONDE EST TRES CONCERNE PAR LA DECOUVERTE DE VULNERABILITES CRITIQUES

On pourrait penser que la découverte d'une vulnérabilité critique dans un logiciel est un évènement sérieux qui va impliquer toutes les parties prenantes.

Pourtant l'utilisateur (ou le client, s'il ne s'agit pas d'un logiciel gratuit) ne peut pour ainsi dire rien faire : il doit attendre le correctif de l'éditeur.

L'éditeur quant à lui dispose de ressources et de connaissances en sécurité limitées (c'est pour cela que ses produits sont vulnérables ;). Il va donc au choix : minimiser la portée de la découverte, intégrer le correctif dans une future maintenance, ou proposer un correctif spécifique (parfois payant) au client.

Quant aux autres utilisateurs du logiciel, ils sont rarement prévenus : les éditeurs n'aiment pas trop qu'on parle de leurs failles sur la place publique.

Et ceci dans le meilleur des cas, car parfois l'auditeur (ou son client) sont poursuivis en justice par l'éditeur du logiciel pour violation de licence !

MYTHE N° 4 :
CORRIGER LES VULNERABILITES AMELIORE LA SECURITE DES SYSTEMES

Cela pourrait être vrai dans un monde où tous les systèmes sont mis à jour en temps réel. Malheureusement la plupart des systèmes du monde "réel" sont mis à jour entre 24h et … jamais !

Ceci est particulièrement vrai dans le domaine des systèmes embarqués (sans parler de SCADA). On peut considérer par exemple que l'énorme majorité des téléphones portables n'est pas mise à jour après sa commercialisation. Un téléphone sous Android restera donc vulnérable à toute faille affectant le noyau Linux et/ou le navigateur Chrome après sa sortie.

A contrario, il faut souvent moins de 24h à un attaquant motivé pour produire une attaque à partir d'un correctif de sécurité. Sans parler de l'auteur initial de la découverte, qui est libre de l'exploiter à loisir tant que le correctif n'est pas disponible, ce qui prend parfois des années !

Ce problème a déjà été retourné dans tous les sens - et il n'admet pas de solution satisfaisante pour toutes les parties. Il est impossible de ne pas mettre au courant les clients des failles sans en informer également les pirates.

MYTHE N° 5 :
IL EXISTERA UN JOUR DES LOGICIELS GRAND PUBLIC INVULNERABLES

Est-ce que nos enfants (ou nos petits-enfants) pourront utiliser un jour un "système de traitement automatisé de données" (quel qu'il soit) en toute fiabilité ? Probablement pas. D'ailleurs c'est plutôt l'inverse qui est en train de se produire: aujourd'hui, la "panne informatique" est invoquée pour justifier à peu près toutes les erreurs et tous les dysfonctionnements.

La réduction des coûts à outrance, la déqualification des métiers techniques comme l'ingénierie logicielle, la course à l'immédiateté (et la culture du "patch" qui l'accompagne) ont tendance à diminuer la qualité de la production logicielle.

A titre anecdotique, on peut citer l'exemple des jeux vidéo dont la version vendue en magasin est non fonctionnelle - les éditeurs ayant mis à profit le temps de pressage et de distribution des CD-ROM pour finir le développement du logiciel, et fournir le tout sous forme d'un patch à télécharger.

Sans parler évidemment des vulnérabilités qui sont introduites volontairement par l'éditeur (aussi appelées backdoors), souvent dans le but de faciliter le support client … Vous avez oublié votre mot de passe de 30 caractères ? Pas de problème, le technicien saura vous dépanner !

On peut donc conclure sur une note positive en affirmant que la recherche de vulnérabilités logicielles a de beaux jours devant elle !

MYTHES ET LEGENDES DES VERS, VIRUS ET TROJANS

David Grout, McAfee

MYTHE N° 1 :
LES EDITEURS D'ANTIVIRUS ECRIVENT EUX-MEMES LES CODES MALVEILLANTS:

Dès que je suis arrivé dans ce domaine en 2003 ce fut la première remarque de l'un de mes clients… « Mais c'est vous qui générez tous ces codes pour vous mettre en valeur à travers vos protections et nous vendre vos solutions ». Vaste question, que d'interrogations, serait-ce possible ?… Une investigation devenait alors nécessaire. Après quelques recherches sur l'Internet je me rendis compte que les vers les plus répandus de cette époque l'étaient en fait à travers des codes générés par des scripts Kiddies (nous en reparlerons dans un prochain mythe). 7 années plus tard en 2010 l'ensemble de mes interrogations sur le sujet est levé et sans ambiguïtés, en effet les laboratoires d'un éditeur de sécurité reçoivent en moyenne 1000 nouveaux codes malveillants par heure.

On comprend aisément deux choses, les éditeurs de sécurité n'ont pas besoin de se faire de la publicité, le mal est réel, et de plus le volume est si considérable que les entreprises d'aujourd'hui n'auraient même pas la capacité humaine de générer tous ces codes.

Pour conclure, il est sur qu'aujourd'hui l'écriture de codes de malveillants n'est pas fait par les éditeurs de sécurité, ils ont déjà un travail herculéen à les contrecarrer.

MYTHE N° 2 :
LES CODES MALVEILLANTS SONT ENFANTINS A GENERER :

Cette phrase est la citation préférée de tous les « geeks » en élaboration de codes malveillants, autrefois appelés les scripts kiddies terme qui était au départ plutôt péjoratif dans la communauté mais que j'emploierai plus pour englober les personnes et les utilitaires permettant à n'importe quelle personne de générer par lui-même un code malveillant.

Malheureusement nous sommes passés depuis quelques années dans une autre dimension de la sécurité et de la malveillance, car aujourd'hui l'argent est le vecteur premier de reconnaissance. Finie l'époque ou l'on souhaitait juste défigurer un site Internet et y mettre son nom pour, comme disent les enfants, montrer que « l'on est cap de le faire ». Aujourd'hui même si ce type d'attaque existe toujours, il est aisément contré par des dispositifs de sécurité de « base » comme les antivirus, firewall.

Depuis quelques années la génération de codes malveillants se complexifie et est le fruit d'équipes complètes de personnes présentant des compétences multiples et très pointues dans différents domaines. Il existe même à ce jour des entreprises dédiées à l'écriture de codes malveillants (avec un SAV oui oui !!!), nous sommes passés de la reconnaissance d'un nom à la reconnaissance financière.

Les dernières attaques en dates appelées aussi APT (Advanced Persistent Threats) telles que Aurora ; Stuxnet le démontrent. Le code malveillant est devenu aujourd'hui une chose extrêmement complexe motivée par le plus vieux moteur du monde : l'Argent. Il ne faut pas oublier aussi l'utilisation de cette menace, ou de cette arme qu'est le code malveillant à un niveau étatique. Aujourd'hui la démobilisation d'un pays par un malware serait-elle possible : Die Hard 4 est-il si loin de nous ?….

MYTHE N° 3 :
C'EST SUR LES PC SOUS WINDOWS QUE LES VIRUS ATTAQUENT

Un mythe qui nous tient, je dirais même qui nous colle … Et oui les virus attaquent Windows mais pas seulement. Le concept aujourd'hui d'une attaque malware est de gagner de l'argent, alors pourquoi Windows ? Tout simplement parce que la part de marché de cet OS est la plus conséquente donc potentiellement les cibles offertes par Windows sont les plus nombreuses.

Mais aujourd'hui avec l'évolution et l'ouverture des plateformes on voit des virus sur MAC, sur Linux et encore plus aujourd'hui sur IOS (Apple OS). Une chose est sûre : la seule motivation et le seul vecteur est l'argent, alors plus un OS est utilisé par des populations sensibles en entreprises plus ces OS seront visés. Il y a fort à parier que 2011 sera l'année du mobile et ce dans tous les sens du terme.

Dernier élément qui casse définitivement ce mythe, parmi les attaques ciblées à des fins financières mais aussi politiques, les malwares visent aussi des OS inconnu du grand public : SCADA avec l'attaque Stuxnet en est un.

Donc pour conclure, aucun OS n'est à l'abris et au vue du peu de couverture que les entreprises consacrent à des environnements « non standards » comme Linux ou MAC, il est sûr que si j'étais un hacker, mon choix de cible primaire serait vite fait …

MYTHE N° 4 :
UNE MISE A JOUR DE LA BASE ANTIVIRALE PAR SEMAINE ET JE SUIS TRANQUILLE

Commençons par quelques chiffres : En 2003 l'éditeur pour lequel je travaille annonçait que nous franchissions la barre mythique des 200 000 souches virales couvertes par les signatures antivirales. Aujourd'hui ce chiffre est atteint tous les 4 jours… Oui, oui vous lisez bien, aujourd'hui une base de signatures couvre 42 millions de souches et augmente en moyenne de 50 000 échantillons par jour.

Alors oui, on peut se mettre à jour toute les semaines le risque n'est que de 350 000 infections potentielles. Aujourd'hui il est clair que le niveau de mise à jour se doit d'être continu. Cependant les éditeurs sont confrontés à une problématique que n'ont pas les hackers, le risque de "faux positif". En effet, un faux positif, ou une détection erronée d'un fichier sain, peut avoir des conséquences désastreuses, c'est pour cela que les firmes antivirus sont contraintes à des tests de qualifications et qualités multiples avant la publication de leurs signatures.

La solution aujourd'hui est complexe mais le marché va vers la sécurité à travers des signatures pour une base validée et testée à laquelle s'ajoute une approche « In the Cloud » ou en temps réel en cas de suspicion forte sur un fichier, même si celui-ci n'est pas détecté par la signature classique. Mais il faut retenir que même si ce type de protection tend vers une couverture complète, elle ne reste néanmoins qu'une protection réactive. L'avenir de la protection se situe aujourd'hui dans la pro activité et surtout la prédictibilité, un énorme challenge …

En attendant mettez vous à jour antivirale le plus souvent possible, voici un mythe qui n'en n'est pas un !

MYTHE N° 5 :
IL NE SE PASSE RIEN DE SPECIAL SUR MA MACHINE C'EST DONC QUE TOUT VA BIEN

Une veille croyance du monde de l'informatique est que si rien ne se passe d'étrange c'est que tout va bien … Je dirais que cela n'est pas faux dans 95% des cas, mais que se passe t'il dans les 5% restant ?

Vous allez vous dire, mais il est parano celui là ? Il voit des malwares partout ! Vous n'avez pas tort, mais aujourd'hui il existe une catégorie de malware encore mal perçue par les utilisateurs, les Trojans (ou chevaux de Troie) qui veulent récupérer de l'argent de manière silencieuse.

Le concept n'est plus comme dans le cas de virus massif, de faire tomber une machine (ex : conficker) ou de créer un réseau de robots qui ciblera des sites web pour les faire tomber, mais un concept vraiment différent. L'idée globale est pour l'assaillant de venir s'inviter sur le poste de sa cible sans que celle-ci s'en aperçoive, à travers l'utilisation de rootkits par exemple.

Ensuite le jeu est de faire évoluer son code de manière sensible afin de ne jamais alerter les outils de protections locaux, puis une fois le virus installé et actif , d'ouvrir une porte entre la machine attaquée et l'Internet (Backdoor). Lorsque ces étapes sont réalisées alors l'assaillant commence à lancer des commandes et à récupérer de l'information : captures d'écran, fichiers sensibles … et ceci en petits morceaux afin de ne jamais éveiller le doute…

Si vous venez de lancer votre gestionnaire de tâches, votre "regedit" et que vous recherchez des traces c'est que vous aussi vous êtes devenu paranoïaque…

Mais si il ne se passe rien sur votre machine, alors peut-être qu'il ne se passe réellement rien ?…

MYTHES ET LEGENDES DU CHIFFREMENT

Gérard Peliks, CASSIDIAN
an EADS Company

QUELQUES MOTS A MAITRISER QUAND ON PARLE DE CRYPTOLOGIE

La cryptologie, science des messages cachés, se divise en deux disciplines antagonistes, la cryptographie et la cryptanalyse.

La cryptographie est l'art de transformer un message en clair, en un message incompréhensible. Pour cela le message en clair est traité par un algorithme (un programme) et une clé de chiffrement (un ensemble de bits). La cryptographie est aussi l'art, connaissant l'algorithme et une clé, de retrouver le message en clair à partir du message caché. On parle de "chiffrer" et de "déchiffrer" le message. C'est le chiffre de défense : on cache l'information sauf à celui qui est en droit d'en prendre connaissance.

Mais si on connait le message chiffré sans connaitre la clé pour déchiffrer le message, il est parfois, par calcul, quand même possible d'obtenir le message en clair. C'est la cryptanalyse. On parle alors de "décrypter" le message chiffré. C'est le chiffre d'attaque : on essaie de récupérer un message chiffré alors qu'on n'en est pas le destinataire.

Ceci étant posé, que signifie "crypter" un message ? Cela ne signifie rien et le mot crypter est à bannir du vocabulaire de la cryptologie.

La cryptologie à l'ère numérique est un combat entre les cryptographes qui élaborent des algorithmes toujours plus difficilement cassables, et qui se basent sur des clés toujours plus longues, et les cryptanalystes qui élaborent des méthodes toujours plus efficaces pour retrouver le message en clair sans utiliser la clé.

Par exemple, à l'aire pré-numérique, Scherbius qui avait conçu la première machine Enigma dans les années 1920 était un cryptographe. Les Anglais du Bletchley Parc, durant la seconde guerre mondiale, qui décryptaient les messages, que les Allemands chiffraient avec cette machine, étaient des cryptanalystes.

MYTHE N°1 :
LE SECRET DU CHIFFREMENT EST DANS L'ALGORITHME

Non, contrairement à ce qu'on pense généralement, le programme de traitement (l'algorithme) qui transforme, en utilisant une clé de chiffrement, un fichier en clair en un fichier chiffré, n'est ni confidentiel défense, ni même un secret industriel, tout du moins dans un contexte où ce principe a été compris.

Le secret réside dans une clé qui sert à chiffrer un fichier, cas de la signature électronique ou du chiffrement symétrique, ou à déchiffrer ce fichier, cas du chiffrement asymétrique.

Kerckhoffs, à la fin du 19eme siècle avait déjà énoncé ce principe : "le secret du chiffrement ne doit résider que sur le secret de la clé". L'algorithme peut être public.

Et mieux, si l'algorithme est un standard comme par exemple l'AES ou le RSA, une communauté importante d'experts peut essayer de le casser, signale ses failles qui sont alors corrigées, et avec le temps, le code d'implémentation de cet algorithme ne présente plus de vulnérabilité évidente, connue.

Si le code d'implémentation de l'algorithme de chiffrement est jalousement gardé, alors seuls ceux qui ont le droit d'en connaître, donc un nombre infime d'experts par rapport à ceux qui

composent la communauté sur le net, peuvent corriger d'éventuelles erreurs. De plus, quand les experts qui connaissent les méandres d'un algorithme confidentiel ne sont plus disponibles, la connaissance a disparue et la maintenance ne peut plus se faire.

Avec un algorithme public, c'est au niveau de la clé que le secret réside. L'algorithme utilise diverses parties de la clé pour effectuer les transformations qui aboutissent au chiffrement ou au déchiffrement du message. Sans la connaissance de la clé, il est difficile de savoir comment se comporte l'algorithme, donc il est difficile, à partir du message chiffré, de reconstituer le message en clair.

Il existe néanmoins des chiffrements qui reposent sur le secret de l'algorithme. Mais ni Kerckhoffs, ni les cryptologues d'aujourd'hui ne trouvent que c'est une bonne idée et conseillent d'utiliser plutôt les algorithmes standards et éprouvés, et de plus soutenus par la communauté du chiffre.

MYTHE N° 2 :
ON CHIFFRE AVEC SA CLE PRIVEE

Mythe ou réalité, cela dépend.

Pour comprendre ce qui suit et pourquoi le chiffrement qui utilise une clé privée est un mythe, cela nécessite des explications sur les deux méthodes de chiffrement. Le chiffrement symétrique et le chiffrement asymétrique.

Dans le chiffrement symétrique, on chiffre une information en utilisant une clé et un algorithme de chiffrement symétrique tels que le 3DES ou l'AES. On déchiffre avec le même algorithme et la même clé. La clé de chiffrement, dite "clé secrète", est la même que la clé de déchiffrement, c'est pourquoi ce type de chiffrement est dit symétrique. En utilisant la même clé, un coup on chiffre, un coup on déchiffre.

Mais un problème se pose. Celui qui chiffre génère la clé de chiffrement symétrique (la clé secrète), mais comment celui qui va déchiffrer, si ce n'est pas la même personne que celui qui a chiffré, va-t-il entrer en possession de cette clé, qui doit bien sûr rester secrète pendant le transfert ? L'autre gros problème est la multiplication des clés secrètes si on se met à chiffrer et déchiffrer entre un nombre élevé de destinataires. Le chiffrement symétrique est pratique et de plus très rapide, mais suite à la difficulté de transmettre la clé et suite à la multiplication des clés qu'il impose, il est difficilement utilisable en l'état.

Le chiffrement asymétrique met en jeu deux clés mathématiquement liées. Une clé privée qui est un secret et une clé publique dont tout le monde peut prendre connaissance. Quand on chiffre avec un algorithme de chiffrement asymétrique comme le RSA, et avec une des deux clés, on déchiffre avec le même algorithme et avec l'autre clé. Dernier postulat : connaissant la clé publique, il est évidemment très difficile de retrouver la clé privée correspondante.

Vous conservez votre clé privée, de manière idéale sur un token USB ou une carte à puce protégée par un code PIN, et vous donnez à tous ceux qui en ont besoin votre clé publique correspondante, ou alors vous dites où aller la chercher.

Avec quoi chiffrez-vous votre information pour la garder confidentielle ? Avec votre clé privée ? Non bien sûr, réfléchissez. Si vous chiffrez avec votre clé privée, tous ceux qui ont votre clé publique pourront déchiffrer votre information, donc il aura été inutile de la chiffrer et la confidentialité espérée ne sera qu'illusoire.

Mais tout de même, une signature RSA est le chiffrement par la clé privée d'une information. Ici le but n'est pas la confidentialité, mais l'authentification: tout porteur de la clé publique doit pouvoir déchiffrer cette information pour l'authentifier comme venant du porteur, unique, de la clé privée.

MYTHE N° 3 :
ON CHIFFRE AVEC UNE CLE PUBLIQUE

Nous avons vu que ce n'est pas avec votre clé privée que vous chiffrez votre information, sinon tout le monde pourrait la déchiffrer.

Alors si ce n'est pas avec votre clé privée, c'est forcément avec l'autre clé, votre clé publique ? Et bien non ! Si vous chiffriez avec votre clé publique, comme personne d'autre que vous n'est censé posséder votre clé privée, pour déchiffrer, à moins que vous chiffrez vos informations pour, seulement vous-même les déchiffrer, ce ne peut être avec votre clé publique. Alors si ce n'est avec votre clé publique, ce pourrait être avec la clé publique de celui à qui vous voulez envoyer votre information chiffrée ?

En effet, comme vous trouvez cette clé publique dans le certificat de celui à qui vous voulez envoyer l'information chiffrée, et comme ce certificat est signé par une autorité de confiance, vous êtes sûr que c'est vraiment la clé publique de votre correspondant, car lui seul possède la clé privée correspondante avec laquelle il va déchiffrer l'information que vous avez chiffrée. Donc tout va bien et c'est comme ça qu'il faut faire ?

Et bien non !

Le chiffrement asymétrique présente un gros handicap : il est cent à mille fois plus lent que le chiffrement symétrique. Cela est du à ses algorithmes qui sont plus complexes. Si déchiffrer une vidéo prend 5 minutes en chiffrement symétrique et plusieurs heures en chiffrement asymétrique, vous aurez vite choisi quel chiffrement vous désirez utiliser.

Ce n'est donc pas non plus avec la clé publique de votre destinataire que vous allez chiffrer votre information, mais avec une clé secrète symétrique que vous générez. Et cette clé secrète, vous la chiffrez avec la clé publique de votre destinataire. Vous lui envoyez cette clé de chiffrement symétrique ainsi chiffrée. La clé de chiffrement symétrique reste confidentielle durant le transfert puisqu'elle ne peut être déchiffrée que par le destinataire qui seul possède sa clé privée. Avec sa clé privée le destinataire déchiffre la clé secrète, et avec cette clé secrète, il déchiffre l'information qui avait été chiffrée avec cette même clé secrète, par chiffrement symétrique.

En résumé, ce n'est pas avec une clé publique qu'on chiffre une information, mais avec une clé secrète symétrique. La clé publique ne servant ici qu'à chiffrer la clé secrète, par chiffrement asymétrique, et la clé secrète sera ensuite déchiffrée par la clé privée du destinataire.

MYTHE N° 4 :
LE CHIFFREMENT QUANTIQUE, ARME ABSOLUE, DES AUJOURD'HUI

Basé non plus sur des calculs mathématiques mais sur la physique des particules, le chiffrement quantique causera une rupture technologique, dans le monde des cryptographes et des cryptanalystes, c'est dire que leur combat va prendre une dimension nouvelle.

Le calcul quantique permet d'effectuer en parallèle une énorme quantité d'opérations qui s'opérait en série avec les calculateurs classiques. Les ordinateurs vont pouvoir résoudre rapidement les problèmes quasiment insurmontables avec les moyens conventionnels tels que la décomposition d'un grand nombre en facteurs premiers, base du RSA, ou le problème du logarithme discret, base du chiffrement par courbes elliptiques.

Nous n'entrons pas ici dans les détails, mais retenez que le cassage de clés par force brute, c'est-à-dire la recherche de toutes les combinaisons possibles de clés pour arriver à retrouver

un message en clair à partir d'un message chiffré, deviendra possible, dans un temps acceptable.

Mais aujourd'hui les ordinateurs quantiques ont un gros défaut : ils n'existent pas, sauf dans les romans de science fiction ou alors à titre expérimental, ils en sont à leurs premiers balbutiements dans des laboratoires de recherche.

Les cryptographes ont ainsi encore des années de tranquillité devant eux. De plus, ils peuvent utiliser la mécanique quantique, et nous ne parlons plus d'ordinateurs quantiques, pour échanger une clé de chiffrement de manière sûre, ce qui était jusque là le gros problème à résoudre pour le chiffrement symétrique.

La mécanique quantique dit qu'un photon tourne autour d'un axe qui est orienté dans une direction qu'on peut lui imposer en jouant sur un champ magnétique. On connait d'autre part la probabilité que ce photon traverse ou pas un filtre à particules, en fonction de l'angle que fait ce filtre par rapport à l'orientation de l'axe du spin du photon qui essaie de le traverser.

Et merveille des merveilles, pour un cryptographe, si une tierce personne observe le spin d'un photon, son orientation est modifiée. Celui qui reçoit la clé s'aperçoit d'une incohérence avec ce que devait être l'état du photon quand celui-ci a été envoyé.

Cette propriété est utilisée pour échanger la clé de chiffrement de manière sûre, car si un espion entre dans la boucle et observe, la clé envoyée est invalidée et on en essaie une autre.

Le calculateur quantique qui résout les problèmes difficilement traités par les ordinateurs actuels et qui cassent les clés dont la taille rendait jusqu'ici ce cassage impossible ou trop coûteux en temps et en ressources est encore un mythe qui va durer quelque temps avant de devenir réalité.

Par contre l'échange sécurisé de clés de chiffrement, qui utilise la mécanique quantique, a dès aujourd'hui des applications, en particulier dans le domaine des télécoms.

MYTHE N° 5 :
LE CHIFFREMENT SEUL MOYEN D'ASSURER LA CONFIDENTIALITE

Une façon d'assurer la confidentialité d'une information est de la chiffrer. Mais il existe un autre moyen, plus pernicieux : cacher cette information, dans son contenant. C'est la science de la stéganographie, aussi vieille que la cryptologie, sinon plus.

Avec la stéganographie, l'information à cacher est en clair (ou chiffrée), mais on ne se doute pas de sa présence. Un exemple physique simple est l'utilisation de l'encre sympathique qui rend invisible un message, sauf quand on chauffe son support. Plus technique, des micropoints peuvent dissimuler une information en la rendant microscopique.

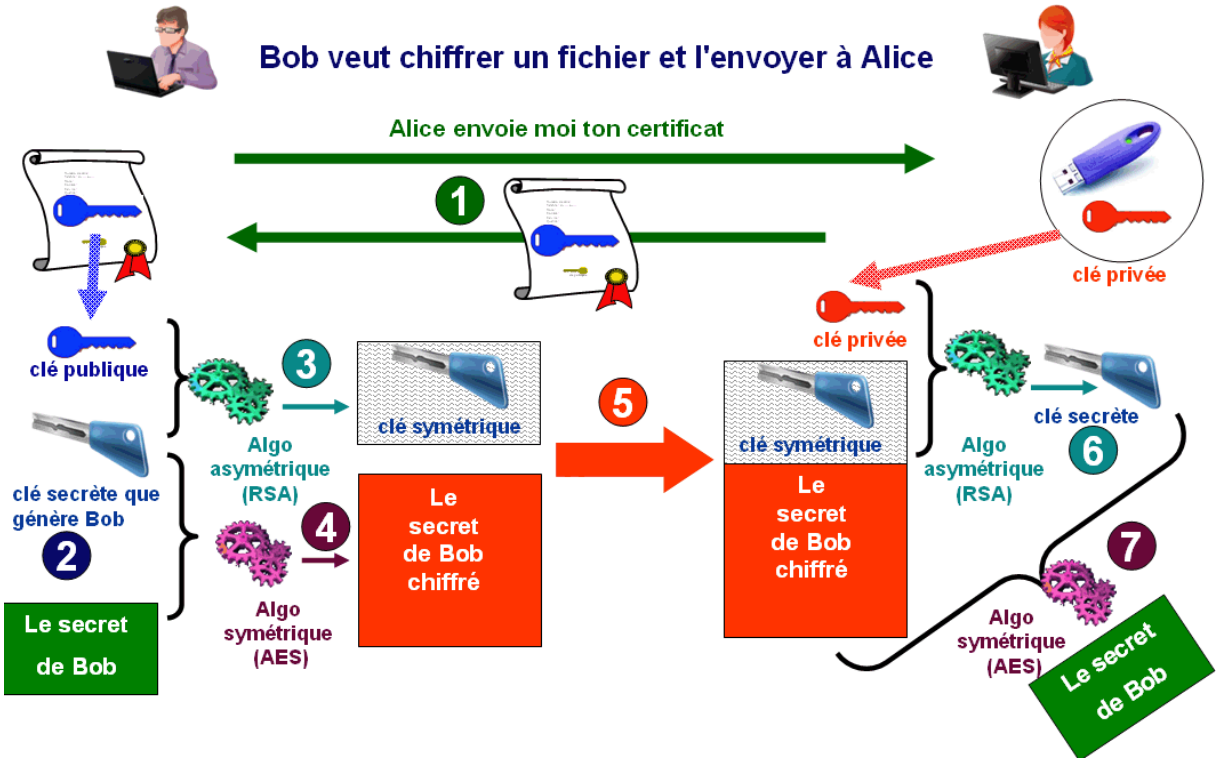
Autre exemple, dans une vidéo de vacances, suivant que vous portiez un chapeau de paille ou un béret basque, ça peut signifier quelque chose à quelqu'un que vous avez mis au parfum de la vraie signification de votre couvre-chef, mais pas pour le commun des mortels.

Une application numérique de la stéganographie est de jouer sur le dernier bit de chaque pixel d'une image, pour cacher un message dans l'ensemble de ces bits. L'œil ne remarque pas les modifications de teintes ou de niveaux de gris de l'image, mais avec le programme approprié, l'image révèle ses messages cachés.

Face à un message chiffré, le cryptanalyste pensera que le message dissimule un secret et a donc de la valeur et il tentera de le décrypter. L'avantage de la stéganographie est que si le message est simplement invisible dans son support visible, qu'il soit chiffré ou en clair, personne n'aura l'idée d'aller le chercher sauf son destinataire qui saura que, dans un fichier anodin, se trouve le message secret.

LES MECANISMES DU CHIFFREMENT

Principe [1] :



Bob chiffre un fichier et l'envoie à Alice. Les exemples sur le chiffrement font toujours intervenir Bob et Alice. Dans la réalité, se sont-ils connus vraiment et échangés des informations chiffrées ? Peut-être est-ce aussi un mythe ☺ ?

Comme l'a dit Albert Einstein « il faut rendre les choses complexes aussi simples que possible mais il ne faut pas les rendre plus simples que possible ». Il est sûr que la crypto est complexe, ça ce n'est pas un mythe.

Allons y ensemble, je vous guide dans l'utilisation des diverses clés et algorithmes divers qui interviennent dans l'échange d'un fichier chiffré.

Bob demande à Alice son certificat. Alice le lui envoie. Bob vérifie le certificat d'Alice, qui est l'autorité qui l'a signé, ses dates de validité, et s'il l'accepte en tire la clé publique d'Alice, pour l'utiliser dans un algorithme asymétrique, comme le RSA.

Bob génère une clé secrète avec laquelle il chiffrera son message confidentiel par un algorithme de chiffrement symétrique, comme l'AES.

Avec la clé publique d'Alice, Bob chiffre sa clé secrète qu'il vient de générer, en utilisant un chiffrement asymétrique, comme le RSA.

Avec sa clé secrète, Bob chiffre son message, en utilisant un chiffrement symétrique, comme l'AES.

Bob envoie à Alice, le message qui a été chiffré par sa clé secrète et un algorithme symétrique comme l'AES, et joint sa clé secrète qui a été chiffrée par la clé publique d'Alice et un algorithme asymétrique comme le RSA.

[1] *Crédit Pictogrammes Aastra*

Avec sa clé privée contenue dans son token USB, Alice déchiffre la clé secrète, générée par Bob et chiffrée avec la clé publique d'Alice.

Et avec cette clé secrète et un algorithme symétrique, comme l'AES, Alice déchiffre le message envoyé par Bob.

La clé secrète intervenant dans le chiffrement symétrique utilisée pour chiffrer et déchiffrer le message secret a ainsi été envoyée par Bob à Alice en toute sécurité.

MYTHES ET LEGENDES DES MATHEMATIQUES DE LA CRYPTOGRAPHIE

Eric Bourre, CASSIDIAN

MYTHE N°1 :
LES FAILLES CRYPTOLOGIQUES SONT DUES A DES MATHEMATIQUES PAS ASSEZ SOLIDES

Penser que des failles cryptologiques seraient dues à des problèmes mathématiques est une idée fausse.

POUR LA CRYPTOGRAPHIE A CLE SECRETE (SYMETRIQUE) :

Les algorithmes de chiffrement utilisés aujourd'hui sont l'AES ou le 3DES. L'AES n'a pour l'instant pas été cassé et la recherche exhaustive (force brute) demeure la seule solution pour retrouver la clé de chiffrement.

Les standards sont conçus de manière à ce que les attaques classiques, comme la cryptanalyse linéaire ou différentielle, soient très difficiles voir impossibles à réaliser.

Si l'on considère l'attaque par force brute pour trouver la clé secrète comme la seule possible, il faut essayer toutes les possibilités.

Si la clé utilisée est de longueur 256 bits, il faudra essayer 2^{256} combinaisons (soit environ 1 million de milliard de milliard de milliard de milliard de milliard de milliard de milliard de milliard de combinaisons), ce qui représente un nombre qui dépassera toujours la puissance de calcul qui peut être mise en place. Cela équivaudrait pratiquement à compter un à un tous les atomes qu'on estime composer l'univers (environ 2^{270} atomes) ! Cela rend en fait inconcevable le déchiffrement. Nous verrons toutefois dans le mythe n°4 pourquoi ce niveau de sécurité est la plupart du temps interdit.

POUR LA CRYPTOGRAPHIE A CLE PUBLIQUE (ASYMETRIQUE) :

Elle se base sur des fonctions à sens unique.

Les fonctions à sens uniques sont des fonctions difficilement inversibles à moins d'en connaître la brèche, la brèche étant la clé privée. C'est à dire qu'un message chiffré sera difficilement déchiffrable si l'on ne connaît pas la clé privée, correspondant à la clé publique qui l'a chiffré.

Bien sûr le terme "difficilement déchiffrable" s'exprime et se quantifie de façon mathématique. En cryptologie, ces problèmes 'difficilement déchiffrables" sont de complexité exponentielle par rapport à la taille des clés.

Pour RSA doubler la taille d'une clé ne rend pas le problème 2 fois plus difficile mais plus de 1000 fois plus difficile à résoudre. Il serait possible de choisir des clés assez grandes pour rendre toute attaque veine.

Mais alors pourquoi ne choisissons-nous pas des tailles de clés plus grande?

Cela est du au fait que le temps de déchiffrement (ou de signature) augmente plus que linéairement en fonction de la taille de la clé. Ainsi doubler la taille des clés rend le déchiffrement/ signature entre 6 et 7 fois plus lent, donc 6 à 7 fois plus coûteux !!

Plus la taille de la clé est grande, plus le coût associé aux opérations cryptographiques sera grand.

Le tout est donc de trouver un juste milieu entre la sécurité nécessaire (qui dépend des puissances machines existantes) et son coût. Il existe des recommandations liées à la taille de clés pour un algorithme de chiffrement choisi (jusqu'en 2010 : 1024 bits, jusqu'en 2030 : 2048, puis ensuite 3072). Cela est valable, tant que l'on ne trouve pas de meilleur algorithme de déchiffrement que le RSA.

Pour résumer, les failles des systèmes cryptographiques tiennent donc à :

- des failles sur les protocoles, ou algorithmes mis en place (ex : le WEP) ;
- des données, en entrée des problèmes trop faibles, comme des tailles de clés trop faibles ;
- des langages de programmation, faille systèmes ;
- des composants physiques ou logiciels qui utilisent des clés (rayonnement des cartes à puce....).

Mais les problèmes mathématiques eux sont solides.

MYTHE N°2 :
ON ME DIT QUE L'ALGORITHME RSA SE CASSE DEUX FOIS PLUS FACILEMENT, NOUS DEVONS ALORS DOUBLER LA TAILLE DES CLEFS

Comme je l'ai indiqué dans le mythe précédent, la complexité du problème RSA n'est pas linéaire en fonction d'une taille de clé.

Si l'on double la taille de la clé RSA, on rend l'attaque par force brute plus de 1000 fois plus longue pour aboutir. De façon pratique, si on trouvait un algorithme qui casse RSA deux fois plus rapidement, il suffirait de choisir des clés avec seulement quelques bits supplémentaires.

L'INRIA en 2009 a réussi à casser une clé RSA de 768 bits. Pour casser une clé d'environ 1536 bits, l'INRIA aurait besoin d'une puissance de calcul 1000 fois supérieure (sachant que cet institut possédait déjà des supercalculateurs calculant en parallèle pour réaliser ce cassage). La croissance de la difficulté de cassage de clé augmente beaucoup plus vite que la taille des clés.

Nous pouvons aujourd'hui penser que les clés de taille 2048 bits ont de beaux jours devant elles.

MYTHE N°3 :
LA MONTEE EN PUISSANCE DE CALCUL PERMETTRA DE RESOUDRE DES PROBLEMES COMPLEXES

Penchons nous sur la loi de Moore un instant.

Elle stipule que la puissance machine double chaque année (on a constaté qu'elle doublait réellement tous les 18 mois). Cela veut dire que la puissance machine augmente de façon exponentielle. On pourrait alors penser que ces améliorations pourraient résoudre des problèmes complexes (solutions exponentielles). Toutefois cette loi ne peut durer car la croissance exponentielle s'essouffle inévitablement très rapidement. En fait ce qui va bloquer ce développement est le fait que le coût des chaînes de production, permettant de créer les processeurs plus puissant, est lui aussi exponentiel (à tel point que même des géants comme IBM et Siemens, pourtant concurrents, ont dû grouper leurs investissements pour arriver à suivre le mouvement). On est donc proche de la fin de la loi de Moore.

Sauf une découverte d'autres lois physiques comme l'utilisation du calcul quantique pourrait permettre à la loi de Moore de se vérifier durablement. Mais rien n'est plus hypothétique car

le calcul quantique réclamerait apparemment une énergie exponentielle pour être mise en application. Sans découverte physique majeure, il y aura toujours des tailles de clés intouchables face à toute puissance de calcul que l'homme pourra mettre en place.

MYTHES ET LEGENDES DE LA SIGNATURE ELECTRONIQUE

Gérard Peliks, CASSIDIAN
an EADS Company

LA SIGNATURE ELECTRONIQUE, CE QU'ELLE N'EST PAS

Avec la généralisation des accès par l'Internet et la dématérialisation des documents, un jour viendra où la signature électronique va reléguer la signature papier au rang de curiosité du passé.

Aujourd'hui cette technologie, qui authentifie un document et en prouve l'intégrité, est mal connue, et dans le vécu quotidien, on utilise la signature électronique sans trop se poser de questions ou si on s'en pose, on apporte souvent de mauvaises réponses. C'est en particulier le cas sur l'utilité du certificat, objet de bien d'interprétations erronées.

Comme la signature manuscrite, la signature électronique permet à celui qui consulte un document signé d'authentifier le signataire. Mais la signature électronique, c'est encore autre chose.

Non, la signature électronique n'est pas la copie d'une petite partie d'un écran contenant une signature manuscrite, qu'on aurait coupée puis collée au bas d'un document Word. Cette manipulation s'appelle simplement du traitement d'image et n'a aucune valeur car on peut après tout placer ainsi n'importe quelle signature sur n'importe quel document. Il est alors trompeur d'établir une relation entre le document et la signature, même si celle-ci était, en toute honnêteté, déjà dans le document initial scanné.

La signature électronique n'est pas d'avantage ce que vous saisissez en apposant votre paraphe sur une tablette digitale et qui ajoute directement votre signature manuscrite au document que vous signez, comme un contrat de location de voiture, par exemple. Cela s'appelle la signature numérique et fait l'objet de lois spécifiques.

La signature électronique consiste en un petit fichier chiffré, accolé à un document, qui prouve en faisant appel à divers algorithmes et clés de chiffrement que le document a bien pour origine celui qui l'a signé (authenticité) et n'a pas été modifié depuis sa signature (intégrité). Le destinataire, par son logiciel de traitement du document signé, ou manuellement, peut en vérifier l'authenticité et l'intégrité. De plus, le signataire ne pourra pas prétendre ne pas avoir eu connaissance de son document signé (non répudiation).

Nous évoquons dans ce document les mythes et les légendes qui tournent autour de la signature électronique, et nous apportons des réponses. A la fin du document, vous trouverez des explications techniques plus détaillées sur les mécanismes qui interviennent dans l'établissement d'une signature électronique et sur la vérification du document signé.

MYTHE N° 1 : ON SIGNE PAR SON CERTIFICAT ELECTRONIQUE

Un certificat électronique ne sert en aucun cas à signer un document qu'on émet. Il intervient dans la vérification de la signature d'un document qu'on reçoit ou qu'on consulte.

Votre certificat personnel ne vous est d'aucune utilité pour signer un document ou pour vérifier la signature d'un document que vous recevez. Pour effectuer cette vérification, vous avez besoin, non pas de votre certificat mais du certificat de celui qui a signé le document.

En annexe, vous trouverez des explications techniques qui vous permettront de mieux saisir les mécanismes.

Un certificat prouve que quelqu'un, qui en est le propriétaire, possède aussi une clé de chiffrement privée qui lui est propre et qu'il a utilisée pour signer son document. Grace à ce certificat le destinataire du document pourra vérifier que ce document a bien été signé par celui dont il a le certificat.

Un certificat contient une clé, dite "clé publique", mathématiquement liée à une deuxième clé, dite "clé privée".

Si vous chiffrez un élément du document avec votre clé privée, cet élément ne pourra être déchiffré qu'avec votre clé publique correspondante, qui se trouve dans votre certificat que vous remettez au destinataire du document. Inutile de prendre des précautions pour transférer votre certificat, celui-ci ne contient aucune donnée confidentielle.

Votre certificat est lui-même signé par une autorité de confiance, qui utilise bien sûr le même mécanisme, pour prouver que la clé publique trouvée dans le certificat est bien la vôtre, c'est-à-dire correspond bien à la clé privée que vous possédez et avec laquelle vous avez signé le document.

Vous signez votre document avec votre clé privée, le destinataire de votre document signé vérifie votre signature avec votre clé publique.

L'élément chiffré puis déchiffré qui a servi à établir qui a signé le document est une "empreinte", ou anglais un "hash" et en bon français un "condensat".

On ne signe donc pas avec un certificat électronique, ni avec la clé publique qu'on trouve dans le certificat, mais avec sa clé privée.

MYTHE N° 2 :
LE CERTIFICAT EST CONFIDENTIEL ET IL FAUT LE PROTEGER

Non, un certificat n'est pas confidentiel, c'est un fichier tout à fait visible et public, destiné à être lu et utilisé par n'importe qui. Le certificat ne contient aucune donnée confidentielle, tout son contenu est en clair, mis à part l'élément chiffré dont nous avons parlé au mythe no 1.

Le certificat est par contre, lui-même, signé électroniquement par une autorité de confiance qui en atteste l'authenticité et l'intégrité. Si vous modifiez ne serait-ce qu'une virgule dans le certificat, cette modification apparaîtra au logiciel de traitement du certificat comme n'étant plus signé par l'autorité de confiance que ce certificat indique.

Le certificat contient une clé de chiffrement publique, qui correspond à la clé privée possédée également par le propriétaire du certificat. Comme le nom des clés l'indique, la clé publique trouvée dans le certificat est publique et donc n'est pas confidentielle.

Seule la clé privée correspondant à la clé publique est confidentielle, et son propriétaire ne doit jamais la dévoiler. La clé privée n'est bien évidemment pas dans le certificat mais, dans le cas idéal, sur un support amovible, tel qu'un token USB protégé par un code PIN.

Le certificat est lui-même signé par une autorité de confiance qui a chiffré un élément du certificat (l'empreinte du certificat qui est l'élément dont nous avons parlé au mythe no 1). Vous possédez le certificat de l'autorité de confiance, contenant sa clé publique (attention, c'est un deuxième certificat, celui de l'autorité de confiance).

L'empreinte chiffrée du certificat peut être alors déchiffrée, par vous, à l'aide de la clé publique de l'autorité de confiance et ainsi vous êtes sûr de l'authenticité et de l'intégrité du certificat qui est attestée par l'autorité de confiance.

Mais si ne possédez pas le certificat de l'autorité de confiance ? Alors vous ne pouvez pas vérifier la validité (authenticité et intégrité) du certificat que cette autorité a signé. Rassurez-vous, vos logiciels connaissent déjà les certificats de nombreuses autorités de confiance, et ceux qui vérifient les signatures électroniques, savent vous demander d'ajouter, aux certificats des autorités que vous connaissez déjà, le certificat de telle autorité de confiance, et vous indiquent en général d'où le télécharger.

MYTHE N° 3 :
UNE SIGNATURE ELECTRONIQUE EN VAUT UNE AUTRE

Bien entendu, nous ne parlons pas ici de l'identité de celui qui signe. Il est sûr qu'un document signé par un notaire ou par une autorité officielle a plus de valeur devant la loi qu'un document signé par un inconnu. Nous parlons ici de la validité d'une signature, qui que soit le signataire. En d'autres termes nous parlons de l'adéquation entre le signataire et sa signature.

Il existe différents niveaux de confiance pour les signatures parce qu'il existe différents niveaux de confiance pour les certificats. Tout dépend qui en établit la validité et comment les certificats ont été obtenus.

Il y a également différents niveaux de confiance à accorder aux certificats suivant les algorithmes de chiffrement et de calcul d'empreinte utilisés et la longueur des clés de chiffrement. L'algorithme de calcul d'empreinte recommandé aujourd'hui est le SHA2 et la longueur des clés pour le chiffrement asymétrique RSA est de 2048 bits.

La première chose qu'on regarde dans un certificat est l'autorité de confiance qui l'a signé. Si le destinataire a confiance en cette autorité, le certificat peut être utilisé pour en tirer la clé publique qu'il contient afin de vérifier qui a signé le document. Si le destinataire ne fait pas confiance en l'autorité qui a signé le certificat, il ne fera pas confiance en la signature du document.

Les autorités de confiance n'ont de sens que par la confiance qu'elles inspirent à leurs clients qui achètent leurs certificats (et avec chaque certificat la clé privée qui correspond à la clé publique que le certificat contient.

Cette confiance peut être accordée par exemple aux certificats signés par une autorité de confiance de même nationalité que le destinataire du document signé, ou alors à une autorité de confiance reconnue par beaucoup d'état comme Verisign qui est une autorité américaine.

Et surtout, il est important de connaître comment un certificat a été décerné à son propriétaire. Le certificat et la clé privée ont pu être achetés par courriel, à travers l'Internet, juste en fournissant une adresse et en le payant. A l'autre bout de l'échelle, le certificat, et sa clé privée associée ont pu être décernés par une autorité de confiance qui convoque l'utilisateur et s'assure de son authenticité, avant de lui remettre sa clé privée et le certificat qui contient sa clé publique.

On distingue plusieurs classes de certificats. Un certificat s'il est obtenu sans formalités, pourvu qu'on le paye, est un certificat qui n'est pas de la même classe qu'un certificat obtenu après déplacement et authentification forte de l'utilisateur. En France, seuls les documents signés et vérifiés avec des certificats à partir d'une certaine classe ont même valeur juridique que les documents qui présentent une signature manuscrite.

MYTHE N° 4 :
SIGNER, C'EST CHIFFRER ET CHIFFRER C'EST SIGNER

Non, signer n'est pas chiffrer. Il y a des documents signés et des documents chiffrés. Il y a aussi des documents à la fois signés et chiffrés. En fait la signature et le chiffrement sont deux fonctions différentes avec des buts différents. Le chiffrement assure la confidentialité alors que la signature assure l'authenticité et l'intégrité du document sur laquelle elle porte. Un document peut être signé mais être en clair.

La signature du document, d'un point de vue technique fait appel à un calcul d'empreinte, puis cette empreinte est chiffrée par chiffrement asymétrique. De même la vérification de la signature du document fait appel aussi au chiffrement asymétrique pour déchiffrer l'empreinte avec la clé publique correspondant à la clé privée.

Mais seule l'empreinte du document est chiffrée ou déchiffrée, le document lui peut ne pas être chiffré. La signature électronique n'assure pas la confidentialité du document.

A l'opposé, rien ne prouve qu'un document chiffré l'ait été par son propriétaire et qu'il n'ait pas été modifié par une tierce personne.

MYTHE N° 5 :
UNE SIGNATURE ELECTRONIQUE, C'EST POUR LA VIE

La signature n'est vérifiable que durant la période de validité du certificat.

Outre la clé publique, le certificat contient la date à partir de laquelle il commence à être valable et la date à partir de laquelle il ne sera plus valable. Comme le certificat est lui-même signé par une autorité de confiance, si on falsifie ces dates, cela se remarque. Les logiciels de vérification des signatures tiennent compte de ces dates.

Il existe également des listes de révocation de certificats. Si le certificat du signataire a été révoqué, le logiciel de traitement de signature électronique refusera de considérer la signature du document comme valable, même si le certificat est encore dans ses dates de validité.

Une signature électronique n'est donc vérifiable, par logiciel, que durant la période de validité du certificat qui possède la clé publique avec laquelle on le vérifie.

Mais si le document a été signé alors que le certificat pour vérifier la signature était encore valable ? Bien entendu, même quand le certificat a expiré ou a été révoqué, la signature peut être tout de même recevable par un être humain qui prend de la hauteur par rapport à un logiciel de traitement de signatures électroniques, qui agit mais n'interprète pas.

C'est le même cas qui se pose si un contrat a été signé par un employé qui était dans une entreprise au moment de la signature, et l'a quittée depuis.

LES MECANISMES DE LA SIGNATURE ELECTRONIQUE

Pour comprendre le mécanisme de la signature électronique, il faut connaître deux mécanismes qui sont le calcul d'empreinte et le chiffrement asymétrique.

Le calcul d'empreinte consiste à calculer, à partir d'une chaine de caractères de longueur quelconque, un ensemble de bits (l'empreinte) dont le nombre fixe est déterminé par l'algorithme de calcul d'empreinte. C'est par exemple 128 bits pour le MD5 et 160 bits pour le SHA1. Si la chaine de caractère de longueur variable subit la moindre modification, son empreinte produite sera différente. Un document est donc caractérisé par son empreinte.

Le chiffrement asymétrique fait intervenir deux clés. L'une pour chiffrer, l'autre pour déchiffrer. L'une des clés est privée et doit être gardée secrète par son propriétaire, l'autre est publique et son propriétaire peut la donner à tout le monde. Cette clé publique est placée

dans un certificat électronique qui atteste qu'elle correspond bien à la clé privée détenue par le propriétaire des deux clés.

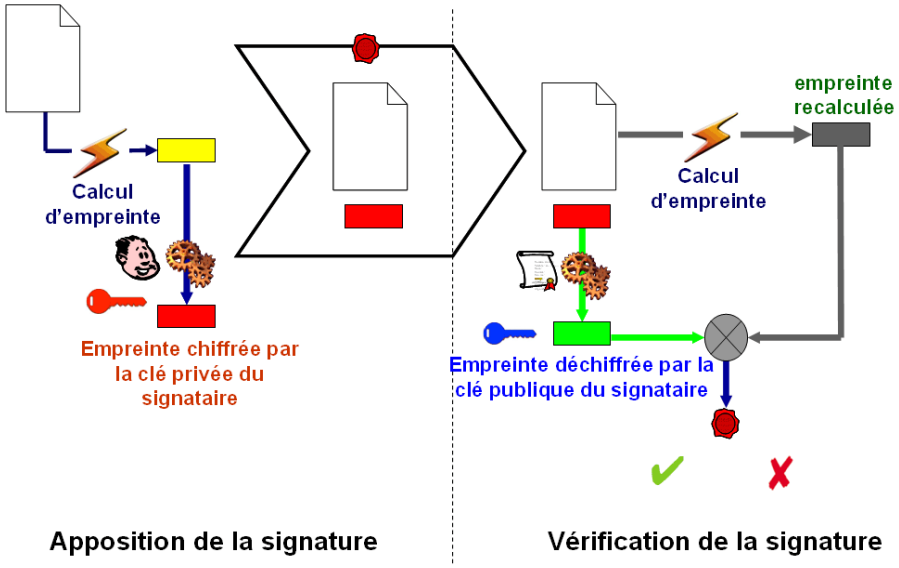
La clé publique est contenue dans un certificat qui est signé par une autorité de confiance. Bien entendu, connaissant la clé publique, il n'est pas possible d'en déduire la clé privée. Quand on chiffre avec l'une des clés, on ne peut déchiffrer qu'avec l'autre. Dans la signature électronique, c'est la clé privée qui est utilisée pour chiffrer et la clé publique pour déchiffrer. Dans le chiffrement asymétrique d'un document, c'est l'inverse.

Le signataire calcule l'empreinte du document à signer et la chiffre avec sa clé privée. Il joint l'empreinte chiffrée au document qui est alors signé.

Ceux qui vérifient la signature du document ont besoin de la clé publique de celui qui l'a signé, donc du certificat qui la contient. Ils déchiffrent grâce à la clé publique l'empreinte chiffrée. Ils recalculent, à partir du document reçu, l'empreinte de ce document. Si l'empreinte déchiffrée est la même que l'empreinte recalculée, la signature est prouvée.

Le document est authentique car son empreinte n'a pu être chiffrée que par celui qui détient la clé privée. Le document signé est intègre puisque le calcul de l'empreinte du document signé est identique au calcul d'empreinte du document avant sa signature.

Principe :



Terminons cette exploration en soulignant un arrêt de la Cour de Cassation qui par un arrêt du 30 septembre 2010 rappelle les formes impératives que doit revêtir un échange électronique pour acquérir une force probatoire et une valeur juridique donnant ainsi son importance à cette technologie : " Sans signature électronique garantissant identité du signataire et intégrité du message, le courriel n'a pas plus de valeur juridique qu'une lettre anonyme faite de collages de caractères découpés dans les journaux".

MYTHES ET LEGENDES DE L'IDENTITE NUMERIQUE

Philippe Vacheyrout, CAPUCINE

La notion d'identité numérique apparait dans la loi Informatique fichiers et liberté de 1978 et le concept s'est imposé progressivement au fil des pratiques d'identification et d'authentification, notamment dans le cadre des procédures administratives et de la mise au point de processus de signature numérique.

Par ailleurs, l'utilisation du Web dans une perspective participative, le développement des réseaux sociaux ont permis l'émergence d'autres problématiques qui y sont liées.

On en arrive donc à l'utilisation du même terme dans deux contextes différents :

- L'identité numérique perçue en termes d'image de l'individu au sens social du terme, c'est-à-dire l'e-réputation.
- L'identité numérique en tant que support de procédures légales, recouvrant la notion d'identification et de possibilité d'authentification de documents à valeur probante, reliés à l'identité au sens légal du terme (authenticité). C'est dans ce sens là que nous l'envisagerons sous le terme de Cyber Identité en liaison avec les labels SuisseID, IDéNum et les cartes Nationales d'Identités Electroniques.

Techniquement, l'identité numérique se définit comme un « lien technologique entre une entité réelle et une entité virtuelle ». (voir Wikipedia)

MYTHE N° 1 : L'IDENTITE NUMERIQUE EST UNIQUE :

Ceci est à la fois vrai et faux.

L'entité réelle en cause étant l'individu, elle est unique malgré la diversité des moyens employés pour l'authentifier. Par contre, l'entité virtuelle, en tant que profil utilisateur (Avatar) : national, familial, professionnel, médical, juridique, consommateur, etc. - est multiple avec les données qui s'y attachent et qui ne sont pas nécessairement toutes les mêmes. Dans les deux cas l'individu doit pouvoir bénéficier de l'application de la loi Informatique et liberté et des recommandations diverses qui l'accompagnent :

- Anonymat
- Droit à l'oubli
- Protection des données personnelles
- Propriété intellectuelle
- Traçabilité des données
- Maitrise de son Identité Numérique au niveau international

En ce qui concerne les dispositifs, divers processus, méthodes, sont possibles. Plusieurs niveaux de certification existent, les autorités de certifications peuvent être privées ou publiques. Il en résulte une multitude de moyens et même de façons d'en aborder le concept.

En ce sens il est possible de parler de multiplicité des identités virtuelles, du simple pseudonyme à usage ciblé à l'identité certifiée à travers un acte authentique

Il en est de même des procédés, du couple login/ mot de passe au système basé sur des données biométriques dont le plus extrême serait l'ADN, en passant par les systèmes de

certificats. Il convient de protéger cet identifiant par les dispositifs disponibles sur le marche (PKI, IGCP 2.0, OTP, SSO, Token etc.)

MYTHE N° 2 :
L'IDENTITE NUMERIQUE RELEVE DE L'AUTORITE REGALIENNE.

Les gouvernements délèguent à des tiers certificateurs le soin d'établir l'identité nationale par le biais d'une identité numérique (Carte bancaire, clé USB, mot de passe dynamique etc…)

De plus toute identité numérique n'est pas utilisée dans un cadre nécessitant une identification certaine (Cartes prépayées)

Il est possible de mettre en place des «cyber- identités » destinées à retracer une activité tout en permettant un certain anonymat – sous réserve des possibilités d'identification dans un cadre règlementé, par exemple à travers la possibilité d'indiquer simplement l'hébergeur dans le cas de blogs individuels. Cette Cyber Identité permet à l'utilisateur de conserver l'anonymat, assurer la protection de ses données personnelles et de préserver la propriété intellectuelle, mais elle n'est pas dépendante de l'autorité régalienne.

MYTHE N° 3 :
IDENTIFICATION ET AUTHENTIFICATION C'EST PAREIL.

L'identification repose sur les informations associées à un objet ou un humain dans un contexte donné pour le distinguer. Il s'agit de disposer des informations nécessaires pour déterminer que l'individu est bien, selon les données que l'on possède, celui qu'il prétend être. Elle s'applique à l'individu.

L'authentification consiste à s'assurer de l'authenticité, l'intégrité et la non-répudiation des informations fournies. Il peut s'agir des informations fournies pour l'identification ou de tout autre processus ou document. Elle s'applique à l'objet et non à l'individu.

MYTHE N° 4 :
LA SECURITE EST GARANTIE PAR LES REFERENTIELS DE SECURISATION ET D'INTEROPERABILITE (RGS [2]- RGI [3])

Selon le Référentiel Général de Sécurité :

« L'objectif du RGS n'est pas d'imposer une technologie, une architecture ou une solution technique, ni même les fonctions se sécurité décrites dans le RGS »

Le socle de sécurisation IAS (Identification, Authentification, Signature) sur lequel s'appuient les rapports de certification [4] pour les Carte d'Identité Électronique ne peut pas fonctionner, dans la mesure où les identifiants biométriques sont des données statiques numérisables et reproductibles. Il est donc possible, partant d'une fausse identité authentifiée, d'aboutir à une signature techniquement valide mais fausse.

---

[2] *Le référentiel RGS peut être trouvé sur le site : http://www.ssi.gouv.fr/IMG/pdf/RGSv1-0.pdf*

[3] *Voir le référentiel sur le site : https://www.ateliers.modernisation.gouv.fr/ministeres/domaines_d_expertise/architecture_fonctio/public/rgi/referentiel_general1617/downloadFile/file/Referentiel%20General%20Interoperabilite%20Volet%20Technique%20V0.90.pdf*

[4] *Voir sur le site du gouvernement : http://www.ssi.gouv.fr/IMG/certificat/anssi-cc_2009-56fr.pdf*

En inversant les deux facteurs, le socle AIS permet à l'utilisateur de délivrer son identité dans un environnement authentifie avec une adresse ID (label IDéNum [5] pour la France) constituant un intranet ou réseau de confiance numérique qui rejoint le post-IP et la proposition de John DAY en y associant l'ID (SuisseID, IDéNum, CapucineID etc .). Ce dernier est compatible avec le RGS puisqu'il est précisé :

« En revanche lorsqu'une autorité de certification juge nécessaire, à l'issue d'une analyse de risque, de mettre en œuvre les fonctions de sécurité qui sont prévues dans le RGS, elle doit alors respecter les règles correspondantes ».

MYTHE N° 5 : LA GOUVERNANCE DE L'INTERNET RELEVE D'UNE ORGANISATION CENTRALISEE

La Gouvernance de l'Internet ne se limite pas à une question d'adressage et la gestion des noms de domaine. L'objet de l'ICANN précise « Les autres questions concernant les internautes, telles que les règles relatives aux transactions financières, les contrôles de contenus sur l'Internet, les messages électroniques à caractère commercial non sollicité (*spam*) et la protection des données n'entrent pas dans le cadre des responsabilités de coordination technique de l'ICANN »

Les autres questions relèvent donc des Internautes, en complément du réseau constitué par la gestion des DNS avec des adresses IP il convient de créer un réseau de fédération d'Identité à l'instar de Shibboleth (qui est un mécanisme de propagation d'identités, développé par le consortium Internet [6], qui regroupe 207 universités et centres de recherches). Cette notion associée avec des adresses ID, à l'instar d'un réseau OpenID+ sécurisé, associés aux réseaux des Internets, pourrait constituer une gouvernance de l'Internet qui relèverait alors de plusieurs organisations centralisées sur la base de « critères communs » évoqués précédemment, définis dans le Web sémantique.

Il revient donc à chaque usager de s'assurer du bon usage des TIC en réseau sécurisé pour participer à la gouvernance mondiale dans le cadre du Forum pour la Gouvernance de l'Internet [7] et construire la Société de l'Information du XXIème siècle, en tirant parti des Technologie du Relationnel notamment avec les environnements 3D, pour partir de la réalité augmentée, vers un futur augmenté.

EN CONCLUSION : INTERNET EST LA PIRE ET LA MEILLEURE DES CHOSES

Cette formule fourre-tout n'est pas un argument mais est largement utilisée par les détracteurs d'Internet. Une formule ne fait pas la réalité et, si nous avons pu observer ce que pouvaient être les pires facettes d'Internet, à l'instar du « Le meilleur des mondes [8]» de Aldous Huxley. Reste à expérimenter ce que pourrait être un monde meilleur entre le « Big Brother » de George Orwell [9] et la « Big Society » de David Cameron , le premier ministre britannique, pour mieux responsabiliser les citoyens dans les collectivités locales afin de construire un réseau vertueux d'économie sociale et solidaire avec une démarche d'entrepreneuriat social, pour un développement soutenable.

---

[5] *Voir annonce IDéNum : http://www.gouvernement.fr/gouvernement/label-idenum-plus-de-securite-et-plus-de-facilite-pour-l-usage-des-services-sur-interne*

[6] *Voir la définition de ce concept sur Wikipédia sur http://fr.wikipedia.org/wiki/Internet2*

[7] *Site du Forum : http://www.intgovforum.org/cms*

[8] *Voir la page de Wikipedia http://fr.wikipedia.org/wiki/Le_Meilleur_des_mondes*

[9] *Pour en savoir plus, voir la page de Wikipedia : http://fr.wikipedia.org/wiki/George_Orwell*

MYTHES ET LEGENDES DES SYSTEMES DE CLOUD

Professeur Jean-Pierre Cabanel, INP / ENSEEIHT, membre de l'IRIT
Professeur Daniel Hagimont, INP / ENSEEIHT, membre de l'IRIT

Face à l'augmentation continuelle des coûts de mise en place et de maintenance des systèmes informatiques, les entreprises externalisent de plus en plus leurs services informatiques et confient leur gestion à des entreprises spécialisées (que nous appelons fournisseurs). L'intérêt principal réside dans le fait que le client de ces fournisseurs ne paie que pour les services effectivement consommés, alors qu'une gestion de ces services par le client ne serait pas complètement amortie, en particulier lorsque les besoins du client varient. Le « Cloud Computing » se situe dans cette orientation récente.

Devant le manque de consensus sur la définition de la notion de « Cloud Computing », reprenons celle de CISCO : "Cloud Computing is an IT ressources and services that are abstracted from the underlying infrastructure and provided on-demand and at scale in a multitenant environment".

Il s'agit donc de fournir aux clients (des entreprises) des services à la demande, illusion de l'infinité des ressources et enfin d'utiliser les mêmes ressources (mutualisation) pour tous les clients.

Cette stratégie offre plusieurs avantages parmi lesquels :

- Réduction des coûts pour le client. Il n'a plus besoin de gérer sa propre infrastructure et il est facturé en fonction de l'utilisation des services du Cloud.
- Flexibilité pour le client. Il peut augmenter la capacité de son infrastructure sans investissements majeurs, les ressources du Cloud étant allouées dynamiquement à la demande.
- Moins de gaspillage. Les infrastructures gérées chez les clients sont souvent sous-utilisées, alors que l'infrastructure d'un Cloud mutualise un ensemble de ressources pour un grand nombre de clients, ce qui permet d'augmenter le taux moyen d'utilisation des ressources.

Un exemple privilégié de mesure de ce gaspillage est la consommation électrique des infrastructures.

MYTHE N° 1 :
LE CLOUD EST JUSTE CE QU'ON APPELAIT AVANT LE "TIME SHARING" : LES APPLICATIONS NE SONT PLUS HEBERGEES CHEZ SOI ET ON NE PAYE QUE CE QUE L'ON CONSOMME

Le Cloud, c'est un peu plus compliqué. Les utilisateurs potentiels d'un Cloud se regroupent en 3 catégories : administrateur du Cloud, administrateur du client et utilisateur final.

L'administrateur du Cloud est responsable de l'administration des ressources matérielles et logicielles du Cloud. Il est notamment responsable de la gestion de la capacité d'hébergement du Cloud. Le Cloud doit donc fournir à son administrateur des services d'administration lui permettant de gérer les ressources matérielles et logicielles mises à disposition des clients.

Quant à l'administrateur du client, il utilise les ressources fournies par le « Cloud « pour gérer les applications finales du client. Il n'a pas une vue globale de l'environnement du Cloud,

mais seulement des ressources mises à la disposition du client et des applications gérées avec ces ressources.

En fonction du niveau de service fourni par le Cloud, on identifie 3 scénarios d'utilisation du Cloud :

- **Infrastructure as a Service (IaaS)** : Il s'agit du niveau le plus bas. Le Cloud fournit des ressources matérielles à ses clients (capacité de traitement, de stockage ...). Ces ressources matérielles peuvent être fournies directement au client (l'unité d'allocation est alors généralement une machine équipée d'un système d'exploitation) ou être virtualisées (l'unité d'allocation est alors généralement une machine virtuelle, plusieurs machines virtuelles pouvant s'exécuter sur une même machine physique) pour une gestion plus fine des ressources physiques. Pour ce niveau, le Cloud fournit un ensemble d'API permettant à l'administrateur du client d'utiliser un ensemble de ressources. L'administrateur du client a alors la responsabilité d'utiliser ces ressources (machines physiques ou virtuelles) pour y installer et gérer les applications utilisées par le client.
- **Platform as a Service (PaaS) :** Il s'agit d'un niveau intermédiaire dans lequel le Cloud ne fournit pas que des machines et leurs systèmes d'exploitation, mais également des logiciels appelés plateformes applicatives. Ces plateformes sont des environnements d'exécution pour les applications finales comme par exemple : les serveurs d'applications dans une architecture JEE. Ces plateformes applicatives sont maintenues par l'administrateur du Cloud, mais l'administrateur du client a la charge d'administrer les applications finales du client sur ces plateformes applicatives.
- **Software as a Service (SaaS)** : Il s'agit du niveau le plus haut dans lequel le Cloud fournit directement les applications finales à ses clients. L'administrateur du Cloud administre les applications finales et le rôle de l'administrateur du client est quasiment nul. Il est important de souligner qu'un Cloud de niveau SaaS peut être implanté par un acteur en s'appuyant sur un Cloud de niveau PaaS géré par un autre acteur, lui même implanté sur un Cloud IaaS.

MYTHE N° 2 : LE CLOUD COMPUTING EST UNE REVOLUTION TECHNOLOGIQUE

On peut penser que le « Cloud Computing » est une révolution technologique, mais non, c'est une orientation vers un mode de gestion des infrastructures informatiques des entreprises.

En adoptant cette orientation, on retrouve tout les problèmes classiquement adressés dans les infrastructures actuelles, et notamment :

- **La tolérance aux pannes**. Un service géré dans un Cloud soit tolérer les pannes dans le sens où il faut assurer la cohérence de l'état du service en cas de panne ainsi que sa disponibilité pour les usagers. La disponibilité peut être plus difficile à assurer du fait que les services sont déportés dans le Cloud et qu'une indisponibilité de la connexion entre le client et le Cloud peut lourdement affecter la disponibilité du service.
- **La sécurité.** Un service géré dans un Cloud doit résister à des utilisations malveillantes. La sécurité peut être délicate à assurer du fait que le Cloud peut héberger des applications pour le compte de différents utilisateurs (ce qui n'est pas le cas pour une infrastructure interne à l'entreprise cliente). De plus, l'utilisation d'un service nécessite une communication entre le client et le Cloud, ce qui peut constituer un talon d'Achille pour la sécurité.

- **L'interopérabilité et la portabilité.** Les clients des « Clouds » auront vite envie de pouvoir migrer des services d'un Cloud à un autre, ce qui nécessitera l'établissement de standards permettant de tels échanges.

Un problème apparaît toutefois plus crucial dans le domaine du Cloud Computing. Comme on l'a vu précédemment, l'organisation d'un Cloud implique deux administrateurs : l'administrateur du Cloud et l'administrateur du client. L'administrateur du Cloud doit déployer des logiciels (systèmes d'exploitation, machines virtuelles, plateformes applicatives ou logiciels pour l'utilisateur final) sur des machines physiques et les gérer à l'exécution (migration, répartition de la charge) afin d'assurer la qualité de service à ses clients.

L'administrateur du client doit effectuer les mêmes tâches d'administration dans le cas des scenarios PaaS et IaaS. Ces tâches d'administration ne peuvent être effectuées manuellement et une tendance générale est de fournir des environnements d'administration autonomes visant à automatiser au maximum ces tâches (on parle également plus généralement « d'autonomic computing ». Ces environnements d'administration autonome fournissent des formalismes permettant de décrire les actions à effectuer pour déployer des applications et les reconfigurer dynamiquement pour prendre en compte les conditions à l'exécution.

Il existe principalement trois types de système de Cloud et les problèmes de sécurité sont différents suivant la structure utilisée.

1. **Les systèmes privés** propres à un grand compte, avec si nécessaire quelques sous-traitants
2. **Les systèmes partagés** par plusieurs grands comptes
3. **Les systèmes publics**, ouverts à tout le monde

Un système de type Cloud se décompose en plusieurs parties :

- Des postes clients indépendants
- Un système de communication entre le poste client et le système.
- Des bâtiments qui abritent les ordinateurs Cloud
- Des ordinateurs, systèmes d'exploitation et logiciels du Cloud

Chacun des ces éléments est un des maillons de la chaine sécuritaire du système et impacte sur les paramètres suivants :

- Confidentialité
- Authentification
- Déni de service
- Pollution, destruction

La problématique de la sécurité d'un système de Cloud relève d'une tache ardue, et les protections envisagées vont diminuer la potentialité de généralisation d'utilisation de Cloud multiples pour un même client.

De manière induite, la problématique juridique est, elle aussi, très difficile : Qui va être responsable des aléas direct ou indirect qui surviendront ? Comment obtenir la réalité sur les causes des situations ?

Il y a quelques années, les constructeurs de « main frame », DEC, BULL, IBM etc., exploitaient des systèmes identiques au Cloud avec sur le plan sécuritaire plusieurs différences essentielles :

- Très souvent, les clients du point central, appartenaient à une même entité juridique: une banque, une industrie etc.

- Les systèmes de communications utilisés n'étaient pas l'Internet, ils permettaient un contrôle suffisant : lignes et réseaux spécifiques et propriétaires.
- La protection des ressources et la recherche des causes d'aléas étaient simplifiées, une seule entité juridique cliente et des systèmes de communication propriétaires des fournisseurs de « Main Frame » ou centre de ressources informatiques.

La nouvelle approche, modifie l'environnement précédemment présenté : clients avec des entités juridiques multiples, même si ces clients sont connus et identifiables à priori, et utilisation de moyens de communication ouverts et incontrôlables : l'Internet.

MYTHE N° 3 :
LE CLOUD PRIVE D'UN GRAND COMPTE EST COMPLETEMENT SECURISE

Dans les systèmes privés propriétaires d'un grand compte, ce type d'utilisation (très proche des PKI intra entreprise), le système est installé sur le site de l'entreprise et les risques sécuritaires sont minimisés. Ils relèvent de la protection des communications dans l'entreprise (internationales) et du contrôle des personnes et des systèmes dédiés au Cloud. Le responsable vis-à-vis des utilisateurs est alors le service informatique qui gère les services de Cloud. Sommes-nous face à un système qui possède un haut niveau de sécurité ?

Et bien cela n'est pas si clair, il est encore nécessaire de contrôler, les chemins utilisés par l'information afin que des copies illicites ne soient réalisées, de s'assurer de la pérennité du fournisseur du service, afin de ne pas perdre de l'information et ainsi désorganiser l'entreprise, contrôler les communications, etc.

Avec les systèmes réservés à plusieurs grands comptes, nous sommes en présence de la structure la plus exposée aux problèmes sécuritaires. En effet le site physique du Cloud n'est pas sous contrôle de l'entreprise mais contient des informations confidentielles de plusieurs entreprises.

MYTHE N° 4 :
LES INFORMATIONS STOCKEES SUR UN CLOUD PARTAGE SONT PROTEGEES, PAR CONTRAT, DES VIRUS, VERS ET AUTRES ATTAQUES

Les postes clients du système Cloud, utilisent sûrement des supports magnétiques amovibles, (il existe très peu d'application fermée) ou bien le poste client est utilisé pour d'autres travaux, ou dans le cas pire, le poste client est connecté à l'Internet de temps en temps.

Pensez-vous alors que les filtres anti virus du Cloud vont protéger les informations des entreprises clientes ? Et bien non ! En réalité ces filtres possèdent une efficacité toute relative et cela conduit au risque de pollution du Cloud par les virus et autres programmes malveillants positionnés par un client et ainsi polluer ou détruire des informations des entreprises clientes du Cloud

Vous imaginez peut-être, que les données des entreprises peuvent être séparées physiquement sur des machines différentes avec des accès réseaux différents ? Et bien non ! La réalité économique de ces systèmes oblige à mettre en commun les ressources afin de diminuer les coûts pour les clients.

Un fournisseur de systèmes de Cloud peut-il garantir par contrat la non destruction ou pollution des données stockées ? Les notions de virus et vers sont elles assimilées aux forces majeures : nature, guerre etc. ? La pérennité du fournisseur est-elle prise en compte par des clauses spécifiques ? Il semble que si l'on désire garder des coûts acceptables de service de Cloud, il soit très difficile de garantir de telles contraintes.

Pensez vous qu'il est possible, de détecter le client responsable d'une pollution ? Quelles sont les responsabilités partagées du Cloud et du client pollueur ?

Dans un environnement semi ouvert (les clients sont connus), la technique actuelle ne permet pas de protéger de la pollution un site de Cloud, de plus, cette dernière, peut être engendrée par un poste client, qui ne connait pas obligatoirement son propre état de pollution. Il est donc très difficile de remonter au client initial, et les autres clients du Cloud sont alors en droit de se retourner vers le propriétaire du Cloud dans le cas de pollution de leurs données.

De plus des postes clients peuvent eux-mêmes être pollués, par un Cloud pollué par un autre client. Cela montre l'interaction informatique entre des entreprises qui ne se connaissent peut être pas,

Peut être pensez vous que si vous participez à un Cloud, le fournisseur vous garantit un cloisonnement informatique étanche ? Et bien non ! Votre entreprise (vos postes connectés au Cloud) devient une partie de la toile tissée par le Cloud et votre informatique est alors assujettie aux aléas d'autres entreprises.

C'est un des problèmes très important lié au système de type Cloud.

MYTHE N° 5 :
SI VOUS QUITTEZ VOTRE FOURNISSEUR, VOTRE CONTRAT GARANTIT LA CONFIDENTIALITE ET LA RESTITUTION DE VOS INFORMATIONS ET LEUR DESTRUCTION

En dehors des problèmes de confidentialité et d'authentification relatifs aux communications électroniques entre plusieurs sites, les informations (confidentielles ou non) des clients sont stockées chez un tiers. Il se pose alors le problème de la confiance dans le tiers par rapport aux problèmes suivants :

- Accès à des informations de clients par des employés du tiers (espionnage).
- Pénétration du site par autrui qui est ou non un client. (usurpation d'identité)

Même si les informations sont chiffrées sur les machines du Cloud, le chiffrement est propriétaire (algorithme et clef) du Cloud et pas de chaque client. Un chiffrement propre à chaque client avec des clefs différentes pour chaque envoi, minimise les risques d'indiscrétion, mais complique la gestion du Cloud et ouvre la porte à d'autres problèmes.

Comment pensez-vous accorder votre confiance à un fournisseur de service de Cloud ? Quel niveau d'informations confidentielles êtes-vous prêt à confier à autrui ? Pensez vous que par contrat le fournisseur de Cloud va vous garantir la non divulgation en interne, ou par accès extérieur, des informations stockées ?

Ces questions montrent la difficulté d'accorder sa confiance à un fournisseur de service de Cloud, que vous ne contrôlez pas.

Vous pouvez aussi penser à changer de fournisseur de Cloud ou vous pouvez vous retrouver face à la disparition de votre fournisseur.

Alors se pose la question de la récupération de vos données et de l'effacement des informations des supports magnétiques utilisés. Pensez-vous que par contrat, votre fournisseur va vous garantir l'effacement de vos informations, c'est-à-dire la destruction des supports magnétiques ? Il semble peu vraisemblable que vous obteniez cette clause dans votre contrat.

Les systèmes ouverts au public ne peuvent correspondre au monde industriel, y compris aux PME/PMI. Les dangers sont très importants, ils correspondent à ceux relatifs au réseau internet. Aucun contrat ne pourra garantir la sécurité des informations, donc ils ne peuvent être utilisés que pour des informations ou traitement non confidentiels.

Comme les puissances de calcul, les volumes de stockage, les prix des logiciels continuent de s'améliorer, on peut se demander si le grand public nécessite ce type d'offre.

MYTHE N° 6 :
AVEC UN SERVICE DE CLOUD, JE N'AI PLUS BESOIN DE ME PREOCCUPER DE MA SECURITE ET DE LA DISPONIBILITE DES SERVICES, ET MON CONTRAT COUVRIRA LES RISQUES INFORMATIQUES ENGENDRES

Comme tout problème de sécurité, la problématique de l'utilisation de systèmes de type Cloud peut être formalisée par les deux idées antinomiques suivantes :

D'un coté les diminutions de coût engendrées par la mise en commun et la meilleure utilisation des ressources informatiques et, d'un autre coté une augmentation importante des risques d'espionnage, pollution etc. dans le monde informatique.

Avec un service de Cloud Computing, les problèmes de sécurité sont très fortement amplifiés : destruction, pollution, confidentialité etc., et la disponibilité des ressources est assujettie au fonctionnement du réseau. Il est plus facile de sécuriser des informations dans son entreprise que sur un système non propriétaire partagé et utilisable à travers un réseau.

Il est clair, que pour des entreprises stratégiques de taille importante, la notion de Cloud ne peut exister que dans le périmètre de l'entreprise, le Cloud est physiquement installé sur un des sites et les clients appartiennent à un même environnement. C'est une vieille utilisation, même si l'exploitation des calculateurs est confiée à un tiers qui peut être le fournisseur de système Cloud.

Pour des entreprises (PME-PMI) stratégiques, un vrai problème se pose, et l'analyse entre la perte financière engendrée par la copie (espionnage ou destruction) de document, et le gain obtenu par la diminution des coûts journaliers de l'informatique, est très difficile à évaluer et dépend de nombreux facteurs.

L'utilisation des systèmes de Cloud ouverts et gérés par des tiers devient alors limitée à des applications dont le niveau de confidentialité est faible, dans le monde industriel, la dernière molécule, le dernier programme etc. ne se partage pas, et les informations relatives à la comptabilité client sont protégées.

L'utilisation de système de type Cloud pose le problème de la confiance vis-à-vis du fournisseur du Cloud, mais aussi vis-à-vis de ses clients, il manque un gendarme.

Pensez-vous vraiment confier vos informations confidentielles à un tiers, et pensez vous que votre contrat couvrira les risques informatiques engendrés ? L'informatique évolue, les types d'attaques aussi, et un contrat signé à une date, ne peut envisager les évolutions dans les années suivantes.

QUELQUES PLATEFORMES EXISTANTES

Plusieurs plateformes ont émergé dans le domaine du Cloud Computing. Parmi les plus connues, nous pouvons citer :

- **Amazon Elastic Compute Cloud** (EC2) : il s'agit d'une plateforme de type IaaS basée sur les machines virtuelles Linux. EC2 fournit une plateforme de création de machines virtuelles personalisées (AMI pour Amazon Machine Image) et d'exécution de ces machines virtuelles.
- **Google App Engine** : il s'agit d'une plateforme de type PaaS de développement et d'exécution d'applications web. Une quantité de ressources minimum est allouée par la plateforme et peut évoluer en fonction des demandes de l'application.

- **Microsoft Live Mesh** : il s'agit d'une plateforme de type SaaS de stockage d'applications et de données. Elle assure la disponibilité et la synchronisation des données entre tous les équipements du client.

Ces quelques exemples montrent l'implication des grands acteurs. Si le Cloud Computing est plus une orientation stratégique et architecturale qu'une révolution technologique, il est clair que cette orientation risque de bouleverser les infrastructures informatiques de nos entreprises.

MYTHES ET LEGENDES DES TECHNOLOGIES VOCALES

Philippe Poux, VocalNews.info et VocalExpo.com

Reconnaissance automatique et synthèse de la parole sont nées sous l'impulsion de quelques chercheurs, autour du Professeur Jelinek, dans les laboratoires IBM.

Rapidement ce qui semblait aisé en traitement informatisé du signal s'est avéré mathématiquement complexe, gourmand en puissance de calcul … démontrant ainsi que notre cerveau est nettement plus efficace qu'un simple calculateur.

Avec des algorithmes basés sur les modèles de Markov, et l'augmentation régulière de la puissance de calcul des processeurs, ces technologies de la parole sont devenues réalité. On a vu alors des variantes dégradées envahir nos téléphones mobiles et d'autres les serveurs vocaux interactifs, avec plus ou moins de bonheur, laissant le champ libre à plusieurs idées reçues.

MYTHE N° 1 :
LES CLIENTS N'AIMENT PAS PARLER A UN ORDINATEUR

La plupart des responsables de relation client pensent instinctivement déplaire à leurs clients en leur proposant ces technologies, sans étayer leur point de vue sur la moindre étude ou analyse. Et en oubliant que le premier souhait d'un client qui appelle … c'est d'obtenir une réponse. Le mode d'interaction importe peu.

En corollaire, on entend souvent que les technologies de la parole déshumanisent la relation client … rien n'est dit de tel concernant le site web ou les scripts contraignants imposés aux téléacteurs ;-)

Alors, basons-nous sur quelques faits démontrés. L'étude Forrester de début 2010 a montré que les consommateurs notent mieux les systèmes automatisés que les agents pour certaines interactions … car ces derniers sont tellement enfermés dans des scripts qu'ils répondent moins bien qu'un SVI. Le sondage a également révélé que les systèmes téléphoniques automatisés sont un attendus et acceptés comme service par 82 % des clients.

Par ailleurs l'impression désagréable de nombre de services vocaux vient de leur ergonomie déficiente. En effet, pourquoi faire confirmer les demandes lorsque l'on sait que le moteur de reconnaissance est bon dans 96% des cas ? C'est ce qu'a très bien compris Air France avec son service 3654, qui remercie à chaque information client et passe à la phase suivante.

L'étude BVA Service Client 2010 montre que la satisfaction client est de 79% avec un email et 75% au téléphone, contre 93% en face à face …

MYTHE N° 2 :
LES HUMAINS SONT PLUS EFFICACES

Rien ne vaut un être humain, que ce soit pour écouter, comprendre, ou entrer en empathie. Les prescripteurs comme les chercheurs dévoués aux technologies vocales ne cherchent pas à remplacer l'humain, seulement à l'accompagner, l'aider. Et les questions complexes sont plus du ressort de l'intelligence humaine, l'artificielle restant encore plus limitée que la reconnaissance de la parole.

Mais une fois ces jalons posés, force est de constater que si l'humain est plus efficace que l'ordinateur, c'est aussi une denrée rare et chère. Les entreprises continuent de considérer les centres de contacts comme des centres de coût et non de véritable relation client, aussi ils limitent le nombre des opérateurs. Au détriment de leurs clients.

MYTHE N° 3 :
INTERNET REMPLACE LES SERVICES VOCAUX

Les SVI auraient été un moyen de proposer du renseignement et self service avec le téléphone, Internet supplée donc à tous ces besoins. Ce point de vue se tient à un détail près, l'émergence de l'autre phénoménale révolution de ces dernières années, le Mobile.

Les usages ont profondément évolué, le mobile est nettement plus présent que l'accès internet et la convergence ne fera qu'accélérer la prédominance du Mobile.

C'est ce qu'ont très bien compris Larry Page et Sergei Brin, les fondateurs de Google, en expliquant fin 2008 qu'il leur fallait devenir aussi les leaders de la recherche d'information sur ces appareils et que l'interaction la plus naturelle était … la voix !

Ils ont alors créé un département entier pour développer leurs moteurs vocaux, lancé un service gratuit d'annuaire pages jaunes (1-800-GOOG-411) afin d'appréhender les comportements et d'affiner leurs modèles. Ce service a tellement bien fonctionné qu'ils proposent maintenant leurs premières applications vocales pour smartphones avec une qualité étonnante. Maintenant qu'il a rempli sa mission, le service 411 a été fermé …

MYTHE N° 4 :
LA RECONNAISSANCE VOCALE EST MORTE

Certaines technologies prennent moins de temps pour devenir matures. Aussi, certains analystes, constatant que les taux d'erreur réduisent lentement, que la parole n'a pas encore envahi tous nos appareils, en déduisent la mort de cette technologie.

Et il est vrai que la plupart des recherches en intelligence artificielle ont pris beaucoup de temps. Plus que prévu, pensé, rêvé … Car l'intelligence humaine est beaucoup plus complexe que ne le supposaient certains chercheurs. Ce n'est pas une raison pour jeter aux orties les systèmes experts, réseaux neuronaux et autres avancées.

Enfin, on verra rapidement que des usages simples de la reconnaissance de la parole dans des mobiles arrivent et rendent de véritables services. Il suffit de voir le succès de ces applications sur l'AppStore de l'iPhone ou sur Android.

MYTHES ET LEGENDES DU CALCUL INTENSIF

Jean Papadopoulo, JP ETUDES & CONSEIL

« Calcul intensif » est le terme utilisé ces dernières années pour désigner le terme anglophone de « High Performance Computing » ou HPC, ce dernier ayant lui-même évincé celui de « Supercomputing ». Historiquement, les matériels et logiciels classés dans cette catégorie étaient dédiés à des applications scientifiques et techniques, telles la mécanique des fluides, la météorologie et la climatologie, la thermodynamique, etc… Les trois caractéristiques les plus significatives du calcul intensif étaient : les performances de l'arithmétique flottante (ce qui justifie que le classement des solutions proposées se fait généralement à l'aune des opérations flottantes par seconde ou « FLOPS » consacré par le classement « TOP500 », actuellement dans la zone « petaflopique ») ; l'importance du calcul vectoriel (liée à la nature des problèmes à résoudre) ; et le débit mémoire (lié au volume des données traitées). L'évolution des matériels ces dernières années, tel que nous le décrirons dans la suite, a légèrement modifié cette définition. En effet, les mêmes systèmes permettent aujourd'hui d'aborder des applications différentes, telle la recherche de séquences génétiques qui n'utilise pas le calcul flottant, ou la fouille de données et l'informatique décisionnelle qu'on aurait plutôt tendance à classer comme application de gestion.

MYTHE N° 1 : LE CALCUL INTENSIF EST A L'INFORMATIQUE CE QUE LA F1 EST A LA VOITURE DE MR TOUTLEMONDE

Cette comparaison était tout à fait de mise pratiquement jusqu'à la fin du 20ème siècle : les ordinateurs qui possédaient les caractéristiques voulues étaient terriblement onéreux, basés sur des architectures propriétaires et parfois « exotiques », peu compatibles entre les différents constructeurs, bénéficiant de peu de logiciels, souvent développés en interne et également chers. L'excellence dans ce domaine était gage de prestige et d'image, mais aucun des acteurs en place n'était économiquement viable et, pour tout dire, aucun n'aurait survécu sans des subventions substantielles de la part des pouvoirs publics. Par suite, les coûts de possession et d'utilisation étaient tels que peu de domaines scientifiques et techniques pouvaient justifier un retour sur investissement suffisant pour recourir au calcul intensif.

Toutefois, les choses ont véritablement commencé à changer dès le milieu des années 90, dans la brèche ouverte par l'informatique de gestion. Cette dernière a en effet atteint un haut niveau de standardisation, par le jeu d'instructions d'abord, le X86-64 s'octroyant un quasi monopole dans le domaine ; par l'architecture système multiprocesseur (SMP comme Symmetrical Multi-Processor) que l'on retrouve aujourd'hui au niveau du chip même ; au niveau du système d'exploitation enfin, Windows et Linux ayant relégué le reste dans des niches de faible diffusion. La domination de l'architecture X86-64 a mis beaucoup plus de temps à s'établir dans le calcul intensif, car la montée en puissance de ce jeu d'instruction s'est étalée sur une vingtaine d'années pour rattraper ses concurrents propriétaires les plus avancés, surtout concernant les performances de l'arithmétique flottante. De plus, la grande majorité des applications de calcul intensif requièrent plus de puissance que ne peut délivrer un seul processeur, ni même un système multiprocesseur qu'utilise avec succès l'informatique de gestion. Ainsi, les quinze dernières années ont vu l'émergence des clusters de SMP en tant que plate-forme de prédilection pour le HPC. L'interconnexion de ces briques de grande diffusion a bénéficié du très haut niveau de standardisation dans le domaine des réseaux par

l'utilisation d'InfiniBand et Ethernet. Ceci est d'autant plus vrai depuis l'adoption récente de la spécification RoCE (RDMA over Converged Ethernet) qui apporte à Ethernet le seul attribut qui lui manquait pour jouer ce rôle, à savoir une faible latence des messages. Pour compléter le tableau, l'utilisation de Linux (sans minimiser les efforts de Microsoft avec Windows HPC Server) et le standard de communication par message MPI (message Passing Interface) ont transformé les perspectives offertes aux développeurs d'applications qui ne sont plus confrontés à une multitude de plates-formes incompatibles avec tout ce que cela implique de coûts d'adaptation et maintenance de versions multiples.

Le résultat net de cette évolution est que l'industrie du calcul intensif est passée d'une période élitiste vers une standardisation poussée, la transformant ainsi d'un marché de niche en marché de grande diffusion, garant d'économies d'échelle et moteur de sa démocratisation. Et si le célébrissime TOP500 continue de susciter des luttes intenses de prestige, il ne représente aujourd'hui que le haut d'une pyramide dont la base s'étoffe et attire des utilisateurs qui n'aurait pas imaginé y recourir il y a encore quelques années.

MYTHE N° 2 :
LE CALCUL INTENSIF EST LA CHASSE GARDEE DES AMERICAINS ET DES JAPONAIS

Encore une idée reçue qui s'explique par l'histoire telle que nous l'avons esquissée ci-dessus. En effet, le modèle initial de l'industrie du calcul intensif le plaçait d'office comme une activité extrêmement onéreuse et tributaire d'aides importantes. Dans ce contexte, seuls les Etats-Unis ont eu les moyens et la volonté politique de subventionner son développement de façon suivie et relativement cohérente. Dans les années 80, le Japon avait bâti une stratégie ambitieuse dans tous les domaines de l'informatique et s'est lancé dans le développement d'ordinateurs vectoriels qui pendant un certain temps a menacé le quasi monopole américain. Avec la prise de pouvoir du modèle « cluster de SMP », basé sur l'intégration d'éléments de grande diffusion largement accessible, la barrière d'entrée dans ce domaine s'est singulièrement abaissée. Cette redistribution met l'industrie du calcul intensif à la portée de nombreux pays qui ont le savoir faire d'intégration de matériel et logiciel à grande échelle. Ainsi, selon le dernier classement TOP500, le système le plus puissant au monde est actuellement chinois. Bull, vénérable société française qui périclitait lentement, a trouvé son salut en développant des systèmes de calcul intensif. Le plus puissant ordinateur en Europe, Tera100, installé au CEA/DAM en est un exemple, et le système « Curie » acheté par le GENCI portera également les couleurs de Bull. Les années à venir verront d'autres entrants, russes, indiens ou autres encore.

Reste qu'en termes de puissance de calcul installée, les Etats-Unis sont toujours loin devant avec plus de la moitié du total général. Ceci reflète la tradition de l'utilisation de cet outil, largement explicable par le poids du passé. Mais la croissance considérable des infrastructures mises en place en Chine en si peu de temps, le rattrapage opéré par l'Europe et plus particulièrement la France avec notamment l'initiative PRACE laissent augurer un avenir plus équilibré.

MYTHE N° 3 :
SEULES LES (TRES) GRANDES ENTREPRISES OU ORGANISMES PUBLICS Y ONT ACCES

Avec la démocratisation du calcul intensif, ce mythe appartient également au passé. Nous avons mentionné précédemment l'importance du coût de possession et d'opération de l'outil informatique pour justifier ou non son emploi. L'autre élément de taille à considérer est l'apparition de logiciels de simulation de plus en plus performants et accessibles. La simulation est devenue, pour reprendre une très belle expression d'un rapport américain, le

troisième pilier de la science, avec la théorie et l'expérimentation. La modélisation permet de prévoir les performances et le comportement d'un produit avant même de l'avoir construit. On connaît ainsi les gains qu'apporte la simulation aux industries du transport ou du bâtiment, évitant les coûteux prototypes ou tests destructifs. Mais ces techniques trouvent leur voie un peu partout, même dans des PMEs où on a du mal à le deviner. De nombreuses anecdotes sont connues, telle la coopérative agricole qui a recouru à la simulation sur une plate-forme de calcul intensif pour concevoir l'emballage utilisé pour sa production de pêches…

MYTHE N° 4 :
L'AVENIR DU CALCUL INTENSIF PASSE PAR L'UTILISATION DES GPGPU

La désaffection des calculateurs vectoriels au profit des architectures parallèles basées sur l'intégration d'éléments de grande diffusion a tout de même laissé un vide pour certains types d'applications qui n'arrivent à exploiter qu'une partie de la puissance théorique maximale, l'exemple classique étant les prévisions météorologiques qui ont été les derniers défenseurs des machines vectorielles. Depuis plusieurs années se pose périodiquement la question comment « augmenter » les architectures clusters pour améliorer le traitement vectoriel. Rapidement les différentes options envisagées se sont cristallisées sur l'emploi opportuniste de cartes dérivées des contrôleurs graphiques de PC qui ont été baptisées GPGPU (General Purpose Graphical Processor Unit). Cette évolution technologique apporte aujourd'hui, il est vrai, des résultats spectaculaires dans le haut de la pyramide (cf. résultats publiés dans le dernier TOP500 sur le célébrissime benchmark Linpack). Cependant, malgré les efforts intenses de la recherche, il est encore très difficile d'obtenir des améliorations équivalentes dans l'application lambda d'un utilisateur. On peut également observer le manque de standard universellement accepté, ce qui nous paraît justement aller à l'encontre de l'objectif de plates-formes de grande diffusion et de portabilité des applications.

Si la direction est clairement perçue par les principaux acteurs de l'industrie, des implémentations divergentes s'affrontent actuellement. NVIDIA, le plus populaire actuellement, propose sa solution Fermi qui est basée sur une connexion lâche (PCI Express) avec les cœurs des processeurs, ce qui implique une évaluation délicate entre les gains du temps des calculs déportés par rapport au temps perdu pour la communication entre processeurs et coprocesseurs. AMD vient d'annoncer la sortie prochaine de sa technologie « Fusion » qui rassemble sur un seul chip CPU et GPU, dont on peut espérer justement une réduction drastique des temps de communication entre les deux. Intel, enfin, a annoncé à ISC'10 « Knights Corner », une réorientation du projet Larrabee (initialement annoncé comme processeur graphique) visant à en faire un élément clé dans les systèmes dédiés au calcul intensif. Il est clair que le concept décantera dans les années à venir, mais à notre avis, ce n'est que lorsque cette accélération sera disponible avec un couplage fort au(x) CPU(s) qu'elle pourra être considérée comme susceptible de devenir un standard pour produits de diffusion de masse. Une analogie peut être établie à ce sujet avec les opérations sur nombres flottants qui ont un certain temps été confiées à des coprocesseurs avant de devenir partie intégrante du CPU. NVIDIA avec CUDA et AMD avec OpenCL ont pris un peu d'avance, mais l'issue de la bataille à venir est loin d'être jouée.

MYTHE N° 5 :
LE « CLOUD COMPUTING » SERA LA SOLUTION PRIVILEGIEE POUR ABORDER LE CALCUL INTENSIF

Peut-être…. Les phénomènes de mode sont tenaces, en particulier en informatique. Depuis que la bureautique et la gestion ont commencé à être accessibles comme services (signe

tangible de la maturité de l'industrie) à différents niveau (infrastructure, plate-forme, application), beaucoup prédisent que le calcul intensif suivra le même chemin. Si de nombreux arguments peuvent appuyer cette prophétie (économie d'échelle et efficacité des grands centres –en quelque sorte le retour de la célèbre loi de Grosch- ; mutualisation des prix de licences, administration, maintenance ; coopération et collaboration facilitées), les différences avec le calcul intensif subsistent. La (re)concentration des serveurs issus du « downsizing » des années 80-90 a résulté de la montée continue en puissance des microprocesseurs, ce qui a déclenché la propagation des techniques de virtualisation, un seul système étant capable de se charger de multiples tâches. Comme nous l'avons mentionné précédemment, le calcul intensif nécessite au contraire l'utilisation parallèle de plusieurs systèmes. Le parallélisme en gestion est « automatique », la charge se répartissant entre les ressources de calcul partageant la même mémoire, alors que le parallélisme entre les nœuds d'un cluster est explicite et nécessite une analyse précise garantissant la proximité des traitements et des données utilisées. A titre d'exemple, mentionnons qu'il y a quelques années certains promettaient la disparition des grands centres de calcul au profit des grilles, il n'en a rien été.

Notre conviction est que seules les tâches les moins exigeantes pourront être servies par le modèle du « cloud computing ». Cela conviendra vraisemblablement bien aux PMEs, et c'est déjà un progrès très notable.

MYTHES ET LEGENDES DU PCA / PRA[10]

Bruno Hamon, MIRCA

Construire un PCA c'est conduire un projet d'entreprise, transversal et multidisciplinaire.

Son ardent objectif consiste à préparer l'entreprise à faire face à un sinistre, pour assurer sa survie. La construction du PCA impose la production d'un plan d'actions détaillé sur ce qu'il faudra faire si le sinistre survient.

Construire le PCA, revient donc à adapter l'organisation d'une entreprise pour atteindre l'objectif de continuité, lui-même orienté vers la satisfaction de ses clients.

Pour réussir cet ambitieux projet, vous devez déjouer les pièges et les mythes qui sont nombreux et dont certains ont la vie dure.

MYTHE N° 1 : JE N'AI BESOIN DE PERSONNE POUR CONSTRUIRE MON PCA

En aucun cas !

Comme tout projet transverse, vous devez susciter l'adhésion de tous. Il faut mobiliser dès la construction du PCA la direction générale, seule autorité pour le légitimer. Cette adhésion, c'est celle que l'Entreprise attend de ses collaborateurs au moment du sinistre. Dès le projet de mise en place du PCA, vous devez communiquer vos objectifs de résultats et de délais.

Il faut éviter les cathédrales technologiques et les effets tunnels tout comme il est nécessaire de fixer des objectifs atteignables. Redémarrer toutes vos activités sous 2 heures, ce n'est pas un objectif réaliste, et c'est rarement ce dont vous avez besoin. Le PCA dans l'entreprise, c'est l'affaire de tous

MYTHE N° 2 : JE VAIS D'ABORD TRAITER L'INFORMATION DANS MON PCA

Surtout pas

Il faut tout d'abord mobiliser vos directions Métier, seules compétentes pour définir les objectifs opérationnels à atteindre au moment du redémarrage, et en déduire les moyens et les outils nécessaires. Ce n'est qu'après que vous pourrez mobiliser vos fonctions support, dont la fonction informatique, en répondant précisément aux besoins des directions Métier.

Il n'y a pas de belle infrastructure technique : il n'y a que celle qui répond aux besoins des opérationnels métier, dans les délais et là où elle est attendue.

MYTHE N° 3 : JE N'AI PAS BESOIN DE TESTER MON PCA

Grave erreur !

Dans un PCA, il n'y a ni héros, ni exploit personnel, ni improvisation subtile de dernière minute.

Les improvisations de dernière minute sont rarement géniales.

[10] *Plan de Continuité d'Activité / Plan de Reprise d'Activité*

Quand votre PCA est défini, documenté, et que tous ont été entraînés à son exécution, il faut alors mobiliser toute l'Entreprise sur l'objectif des tests du PCA.

Seuls ces tests permettent d'établir avec certitude que votre PCA est opérationnel.

Pour les deux volets du PCA souvent désignés par le PCO (Plan de Continuité Opérationnel qui traite l'angle Métier) et le PCI (Plan de Continuité Informatique qui lui traite de la partie technique), il est fortement recommandé de procéder régulièrement à des « tests unitaires » (une seule procédure) mais aussi réaliser des « tests de bout en bout » (enchainement de l'ensemble des procédures)

MYTHE N° 4 :
UN PCA, ÇA COUTE LES YEUX DE LA TETE

Fausse idée !

La mise en place d'un PCA est une nécessité que l'on rend accessible en ajustant la démarche aux enjeux d'une entreprise tout en faisant preuve de pragmatisme et du souci de la maîtrise de l'investissement.

Par conséquent, un projet PCA doit être adapté au contexte de l'entreprise qu'il va toucher ; la prévention doit être privilégiée, dans certain cas l'externalisation du secours peut également permettre à l'entreprise de ne se concentrer que sur son cœur de métier. Par ailleurs, on a pu constater ces dernières années que les coûts des solutions techniques avaient drastiquement baissé ; dans certain cas la solution technique peut répondre aux chocs extrêmes mais aussi aux problèmes de disponibilité du quotidien. Enfin, notons qu'un PCA peut commencer par une simple clé USB !

MYTHE N° 5 :
UN PCA EST UN PROJET SANS RETOUR D'INVESTISSEMENT

Autre fausse idée !

Décider de mettre en place un PCA ressemble, à peu de choses près, à la signature d'un contrat d'assurance.

De fait, la question à se poser alors n'est pas tant « Avons-nous besoin d'un PCA ? » que

« Jusqu'à quel point avons-nous besoin de définir les mesures de continuité d'activité de notre organisation ».

Cette approche spécifique privilégie donc l'adéquation des mesures aux enjeux d'une entreprise et doit garantir un retour sur investissement par construction.

Dans tous les cas de figure, les bénéfices attendus doivent s'ajuster aux risques encourus.

MYTHE N° 6 :
UN PCA N'EST BON QUE POUR LES GRANDS COMPTES

Encore une idée fausse!

Une PME reste plus sensible aux risques de choc extrême car elle réside souvent sur un seul et même site. Autrement dit, son bassin commercial est souvent régional et son assise financière demeure plus fragile. Très rares sont les cas où les PME peuvent compter à la fois sur le recouvrement des fonctions-clés mais également sur une concentration de leurs ressources vitales.

Par conséquent, une PME peut moins se permettre de laisser les sinistres décider de son avenir en comparaison avec ses principaux et gros concurrents qui eux sont généralement assis sur plusieurs sites/continents ou adossés à des groupes/investisseurs puissants.

Dans tous les cas, il est important de bien calibrer l'organisation de crise et le dispositif du PCA.

Ces deux aspects doivent être aussi souples et agiles que la PME.

MYTHE N° 7 : MON PCA EST ACHEVE ET TESTE : LE TRAVAIL EST TERMINE

Malheureusement non, il ne fait que continuer !

La vie de l'Entreprise continue, et vous devez adapter les processus de décision de l'Entreprise pour qu'ils « pensent PCA » : un nouvel embauché, un nouveau client, un nouveau fournisseur, un nouveau produit, un nouveau contrat, un nouveau règlement, un nouveau site de production, une nouvelle agence commerciale, une croissance externe, et, bien entendu, un nouvel outil informatique : autant de changements à traduire sur votre PCA, pour le maintenir à jour et opérationnel.

C'est ce que l'on appelle le Maintien en Condition Opérationnelle (MCO) du PCA qui doit prendre en compte toutes les évolutions et mises à jour de votre PCA au sein de votre organisation.

CONCLUSION

Toute décision de mise en place d'un PCA exige une volonté affirmée, demande du temps et de l'énergie, suppose un budget en conséquence. Le PCA impose également un suivi permanent, requiert un pilote motive, disponible, rigoureux et méthodique. D'un autre côté, le PCA va devenir à terme un élément commercial différenciateur : il est un moyen et non une finalité.

MYTHES ET LEGENDES DES LOGICIELS LIBRES

Jean Christophe Elineau, président du pôle AQUINETIC
Yvon Rastteter, ARTS.SOFT

MYTHE N° 1 :
LE LOGICIEL LIBRE EST GRATUIT

Un des contre-sens les plus courants dans la thématique « Logiciels Libres » consiste effectivement à dire qu'un logiciel libre est un logiciel gratuit.

Il faut savoir qu'un logiciel libre n'est pas forcément gratuit même si pour la plupart d'entre eux, c'est effectivement le cas. Ces logiciels sont alors téléchargeables sur de nombreux sites internet, spécialisés notamment. La confusion vient de fait que la langue anglaise utilise l'expression « Free Software » pour ce que nous appelons nous, « logiciel libre ». Or, en anglais, « free » peut aussi bien signifier « libre » que « gratuit ». Le terme « Free Software est donc très souvent mal interprété.

Il existe autour du logiciel libre, plusieurs modèles économiques et certains d'entre eux permettent notamment de vendre des logiciels libres (modèle de la double licence notamment ou l'éditeur peut alors proposer une version communautaire gratuite mais aussi une version professionnelle payant). C'est par exemple notamment le cas pour la solution trixbox, solution libre de téléphonie à base d'Asterisk.

Des versions payantes, destinées à des entreprises, sont commercialisées par des éditeurs, avec support technique et documentation complète. La société Red Hat, société américaine fournit par exemple son produit « Red Hat Enterprise Linux » en basant sur des services avec vente de maintenance, formations …

Vous trouverez en conclusion de la thématique, un document de l'APRIL (Association française ayant pour objet la promotion et la défense du logiciel libre) ayant pour intitulé « le logiciel libre, comment ca marche ? ». Il permet de mieux comprendre le concept que nous défendons.

MYTHE N° 2 :
LE LOGICIEL LIBRE DETRUIT LA VALEUR AJOUTEE DE L'INDUSTRIE DU LOGICIEL

La valeur ajoutée de l'industrie du logiciel porte sur la vente des progiciels d'une part et les services associés à l'adaptation, l'exploitation, la maintenance et des logiciels d'autre part. L'analyse du prix de revient d'un progiciel fait apparaître des frais importants concernant le marketing et un coût de développement réparti entre le nombre de licences vendues qui est d'autant plus faible que le nombre de licences est important.

On est dans un modèle économique qui vise à créer de la rareté alors que le coût marginal pour produire une nouvelle version du logiciel est quasiment nul.

Cette rareté créée profite à tous les acteurs de la filière : l'éditeur du progiciel et la société de service qui le revend à un client. Les marges peuvent être importantes, surtout dans les domaines ou un progiciel est dans une situation de quasi-monopole.

L'intérêt des consommateurs, particuliers ou entreprises, est de faire baisser le prix de ce progiciel. Ceci est possible lorsqu'un éditeur produit un logiciel offrant les mêmes fonctionnalités, mais sous forme de logiciel libre. Il se rémunère alors sur le service offert à l'utilisateur ou sur le service de haut niveau offert à un intégrateur.

D'autre part, la forme de marketing viral, de bouche à oreille, effectué dans l'écosystème du logiciel libre est beaucoup moins coûteux que le marketing classique.

Tous les postes de la chaîne de valeur s'en trouvent ainsi réduits. Parler de destruction de valeur, c'est adopter le parti qui exploite la rente du système économique propriétaire.

Prendre le parti de l'utilisateur consiste à dire que, dans une économie numérique ouverte et concurrentielle, le coût d'un logiciel doit refléter sa réalité économique : la rareté ne s'applique pas puisque le coût de production marginal est quasiment nul.

Il est d'ailleurs intéressant d'observer que tous les acteurs du logiciel propriétaire s'appuient sur des briques en logiciel libre efficaces et performantes pour réduire leur coût de production. Il est donc inéluctable que la part des logiciels libres va croître dans le contexte de l'économie numérique.

MYTHE N° 3 :
UN LOGICIEL PROPRIETAIRE EST DE MEILLEURE QUALITE QU'UN LOGICIEL LIBRE

A faire

MYTHE N° 4 :
UN LOGICIEL LIBRE N'EST PAS SOUMIS A UNE LICENCE

Voilà sans doute un des aspects les plus intéressants de la thématique : "Ce logiciel est libre donc il n'est pas soumis à licence". Mais non, le logiciel libre est lui aussi soumis à licence. On en dénombre entre trente et cinquante environ (selon classification). Ces licences sont beaucoup moins restrictives que les licences propriétaires mais elles permettent d'offrir un certain nombre de garanties aux créateurs de programmes.

Selon WikiPedia (l'encyclopédie libre), « Une licence libre est un contrat juridique qui confère à toute personne morale ou physique, en tout en temps et tout lieu, les quatre possibilités suivantes sur une œuvre :

- La possibilité d'utiliser l'œuvre, pour tous les usages ;
- La possibilité d'étudier l'œuvre ;
- La possibilité de redistribuer des copies de l'œuvre ;
- La possibilité de modifier l'œuvre et de publier ses modifications ».

On notera donc surtout la possibilité de modifier l'œuvre mais aussi l'obligation de publier les modifications. Le contributeur devient ainsi co-auteur. C'est en fait la pleine expression du droit d'auteur qui peut prendre ainsi une forme collective.

Parmi ces licences, on retiendra notamment la licence GNU GPL (GNU General Public licence, fixant les conditions légales de distribution des logiciels libres du projet GNU) ou bien encore la licence CeCILL (CEA CNRS INRIA Logiciel libre).

Le non respect de ces licences peut entrainer des poursuites judiciaires. Ce fut le cas en 2009 quand la Cour d'Appel de Paris qui sanctionna une société n'ayant pas respecté les principes de la licence GNU GPL.

MYTHE N° 5 :
LE LOGICIEL LIBRE N'EST PAS PROFESSIONNEL

Ou dit autrement : c'est une affaire de bidouilleurs qui travaillent en perruque en volant les heures de travail à leur employeur.

L'extension de l'utilisation de modules écrits diffusés et maintenus en logiciel libre prouve que ce n'est pas vrai. Le nombre croissant d'éditeurs propriétaires qui incorporent des

modules en "logiciel libre" dans leurs produits, voire les recomposent entièrement avec ces produits prouvent que ces produits sont professionnels.

Les éditeurs propriétaires ont intérêt à accréditer cette idée pour mieux vendre leurs produits.

Ils s'appuient sur le préjugé comme quoi quelque chose qui est gratuit n'est pas de bonne qualité et sur le sérieux et la solidité de leurs moyens pour la maintenance.

Il est vrai cependant que, dans certains domaines, les éditeurs et intégrateurs de logiciel libre n'ont pas atteint la taille suffisante pour pénétrer des marchés maîtrisés depuis des dizaines d'années par les fournisseurs propriétaires.

Les produits du logiciel libre se sont implantés dans les domaines émergents, celui par exemple des serveurs Web. Ils peinent à s'imposer dans des domaines comme la téléphonie ou les acteurs « historiques » dominent le marché depuis des dizaines d'années et où un offreur comme Cisco a acquis une monopole mondial par la vente de ses routeurs et a pu considérablement investir pour s'implanter sur la téléphonie et concurrencer les fournisseurs historiques.

C'est question de taille et de croissance pour atteindre la taille critique. Cependant atteindre une grande taille n'est pas nécessaire pour s'imposer sur le plan mondial.

C'est le cas de sociétés comme Talend, ExoPlatform. Même Redhat reste une société de petite taille par rapport aux grands. Reste l'évolution actuelle qui voit des gris éditeurs racheter des éditeurs en logiciel libre, comme MySQL par SUN puis Oracle, mais c'est une autre problématique. Ces éditeurs de logiciel libre font justement l'objet de convoitise à cause de leur professionnalisme !.

MYTHE N° 6 :
UN LOGICIEL LIBRE N'EST PAS, OU EST MAL, DOCUMENTE

Autre mythe concernant les logiciels libres : nos amis, gentils programmeurs de solutions libres ne prennent pas le temps de rédiger des documentations techniques complètes, ni de les traduire.

Ce n'est absolument pas le cas et bien au contraire la plupart des logiciels libres sont aujourd'hui particulièrement bien documentés.

Prenons par exemple, les documentations concernant certains systèmes d'exploitation comme Ubuntu, Fedora ou autres... Les documentations proposées avec ces logiciels, n'ont véritablement rien à envier aux documentations fournies avec certains systèmes d'exploitation propriétaires. Des sites spécialisés sont même créés sur cette thématique (ex : http://doc.fedora-fr.org/).

Il existe aussi des projets comme Traduc.org qui « rassemble et soutient les projets d'adaptation française des documents et logiciels de l'informatique libre » en réunissant des traducteurs volontaires pour les projets libres.

Tout ce travail peut être, bien entendu protégé notamment par la Licence de documentation libre GNU, dont l'objet est de protéger la diffusion de contenu libre.

EN COMPLEMENT :

Les Rencontres Mondiales du Logiciel Libre (R.M.L.L) rassemblent chaque année les contributeurs du logiciel libre ainsi qu'un public généraliste de plus en plus nombreux. L'organisation des R.M.L.L. est attribuée par un comité rassemblant les organisateurs précédant de l'événement, à un G.U.L.L. (Groupe d'Utilisateurs de Logiciels Libres)

Créée en 2000 par l'A.B.U.L. (Association Bordelaise des Utilisateurs de Logiciels Libres (A.B.U.L.), cette manifestation a depuis 10 ans, sillonné l'hexagone. Ainsi, les éditions précédentes se sont elles donc déroulées successivement à Bordeaux (2000, 2001, 2002, 2004 et 2010), à Metz (2003), à Dijon (2005), à Vandoeuvre les Nancy (2006), à Amiens (2007), Mont de Marsan (2008) et Nantes (2009).

Pour 2011, la manifestation prendra racine dans une ville symbolique pour l'Europe, en l'occurrence Strasbourg. Mais plus intéressant encore, 2012 semble être parti pour être l'année de l'exportation de l'événement en dehors de la France pour la première fois car c'est la ville de Liège en Belgique qui a retenue l'attention du comité de sélection.

Mais intéressons nous d'un peu plus près au public qui fréquente l'événement et notamment aux pays représentés. En 2008 à Mont de Marsan, ce ne sont pas moins de quarante pays qui étaient ainsi présents pendant les cinq premiers jours du mois de juillet. : Espagne, Allemagne, Angleterre, Pays-Bas, Irlande, Suisse, Venezuela, Canada, Etats Unis, Russie, Asie et de nombreux pays Africains (et ceci malgré les conditions d'obtention des visas particulièrement difficiles). Je m'excuse par avance auprès des pays que j'oublierais dans cette liste à la Prévert.

Cette diversité permet donc des rencontres particulièrement enrichissantes mais justifie surtout l'appellation de Rencontres MONDIALES.

Document de l'**APRIL** (Association française ayant pour objet la promotion et la défense du logiciel libre)

MYTHES ET LEGENDES DE LA CERTIFICATION CRITERES COMMUNS

Gérard Peliks, CASSIDIAN
an EADS Company

LA CONFIANCE OBJECTIVE EN UNE SOLUTION DE SECURITE

L'Information que vous détenez est sans doute protégée par des solutions de sécurité. Mais ces solutions sur lesquelles réside votre confiance, sont-elles sécurisées ?

Un logiciel de sécurité n'en reste pas moins un logiciel et comme toute œuvre de l'esprit humain, il peut être entaché d'erreurs de programmation, ou d'implémentation, qui sont autant de vulnérabilités ouvertes aux attaques que le logiciel est censé contrer. Il en est de même pour les cartes à puce et pour les logiciels embarqués.

Qu'est ce qui pourrait alors motiver la confiance que vous accordez à un logiciel de sécurité ? Serait-ce parce que votre voisin n'a pas eu de problèmes avec la même solution ? Est-ce la notoriété que le produit rencontre sur le marché ? Seraient-ce les sirènes d'un constructeur qui vous affirme que son produit est le meilleur ? Non, tout ceci n'est que confiance suggérée…

Une confiance objective peut-elle s'établir ? Oui, un certain niveau de confiance objective reste possible si la solution de sécurité a été soumise à des essais normalisés, conduits par un organisme indépendant, étroitement surveillé, et si un organisme officiel reconnu au plan international, quand les tests ont donné un résultat satisfaisant, appose sa signature sur l'attestation de certification. Et bien sûr chaque solution de même type doit passer les mêmes tests. C'est l'un des buts de la norme des Critères Communs (ISO/IEC 15408) conçue à la fin des années 1990 et qui évolue. Mais ces résolutions cachent bien des mythes et légendes, en voici quelques uns.

MYTHE N° 1 : MA SOCIETE EST CERTIFIEE "CRITERES COMMUNS"

Non, la certification Critères Communs ne s'applique en aucun cas à un organisme. Elle ne peut être attachée qu'à une solution de sécurité. Si un produit qui a obtenu cette certification n'est plus commercialisé par le même éditeur, suite par exemple à un rachat de technologie ou suite à un rachat de l'éditeur qui a créé le produit, le produit n'en demeure pas moins certifié Critères Communs pour la version qui a obtenu cette certification.

Le sérieux affirmé par un organisme vis-à-vis de la sécurité, en d'autres termes vis à vis de la gestion de la sécurité de son propre système d'information, peut être certifié par rapport à d'autres normes comme celles de la famille ISO 2700x, en particulier par l'ISO 27001 qui est à la sécurité d'un système d'information, ce que l'ISO 9001 est à la qualité. Pour obtenir la certification ISO 27001, l'organisme doit gravir une pente qui le conduit à plus de sécurité en adoptant le modèle dit "roue de Deming". A chaque tour de la roue de Deming, les étapes "Plan, Do, Check, Act" se succèdent et la société mesure l'écart entre ce qui devrait être et ce qui est réellement, pour réduire cet écart. Cette ascension de la roue de Deming qui gravit une pente, conduit l'organisation à obtenir, puis à maintenir, sa certification ISO 27001. Mais cela est une autre facette de la sécurité et ne porte pas sur la certification d'un produit ou d'une solution intégrée de sécurité, donc sur la certification Critères Communs, objet de cet article.

Une société qui propose des services, mais aucun produit, peut être certifiée ISO 27001 et un constructeur ou éditeur de logiciels de sécurité qui n'est pas certifié ISO 27001 peut faire certifier ses produits "Critères Communs". Mais souvent il y a confusion entre ces normes.

La certification Critères Communs peut d'ailleurs s'appliquer également à des solutions comme des IPBX (autocommutateurs téléphoniques sur protocole IP) ou à des systèmes d'exploitation pour contrôler et affirmer dans le détail la robustesse c'est à dire l'exactitude des annonces de sécurité, et répondre à des questions comme : les protections sont-elles efficaces face aux menaces ?

MYTHE N° 2 :
LA CERTIFICATION CRITERES COMMUNS PORTE SUR L'ENSEMBLE D'UN PRODUIT

C'est un mythe de croire qu'un pare-feu (firewall), par exemple, certifié Critères Communs l'est sur l'ensemble de ses fonctionnalités, quelle que soit sa version et ses conditions d'emploi. La certification Critères Communs porte sur une version précise d'un produit, qui tourne sur une version précise d'un système d'exploitation ; le tout dans un environnement qui doit respecter un certain nombre d'hypothèses spécifiées dans le document « Cible de Sécurité ». Quand le pare-feu, ou autre logiciel, est proposé déjà intégré sur un calculateur (une Appliance), la certification porte seulement sur certains des modèles de cet Appliance. Et quand l'Appliance comporte un pare-feu, un antivirus et un antispam, ni l'antivirus, ni l'antispam ne sont, le plus souvent, couverts par la cible de sécurité.

Tout ceci est écrit sur l'attestation remise avec la certification, encore faut-il la lire attentivement. Il ne serait pas très honnête, par exemple, pour un éditeur, d'affirmer "mon Appliance de sécurité a obtenu la certification Critères Communs au niveau EAL3+ (en insistant toujours sur le "+" !) alors que cette certification a été obtenue sur une version déjà ancienne de cette Appliance et qui n'est plus commercialisée, et peut-être sur un autre système d'exploitation que celui proposé à la vente. La sécurité du produit n'a pas forcément régressé depuis l'obtention de sa version certifiée, mais rien ne le prouve.

Un programme de maintenance de la certification de la solution existe, qui établit la non régression de la sécurité du produit sur la surface testée (la cible de sécurité) à chaque nouvelle version, ou après chaque action de maintenance majeure; mais l'éditeur a-t-il souscrit à ce programme ?

MYTHE N° 3 :
DEUX PRODUITS DE MEME TYPE, CERTIFIES CRITERES COMMUNS, SONT COMPARABLES

Il est certain que l'un des buts principaux des Critères Communs a été de permettre la comparaison, côté sécurité, entre des produits de même type, par exemple des pare-feux, des réseaux virtuels chiffrés (VPN) ou des produits de chiffrement sur disque. Les certifications précédentes, comme l'Orange Book aux USA ou les ITSEC en Europe n'avaient pas intégré cette possibilité, et c'est en quoi les Critères Communs se démarquent principalement des autres certifications de produits. Mais affirmer que deux produits de même type, certifiés Critères Communs à un même niveau, par exemple deux pare-feux certifiés Critères Communs EAL3+, sont comparables, peut être un mythe si on ne sait pas exactement ce que la certification recouvre pour chacun d'eux.

Une certification porte sur une certaine surface de fonctionnalités du produit, et sur certaines menaces que le produit doit contrôler. Tout ceci est consigné dans un document appelé la "cible de sécurité" (ST : Security Target). Deux outils de chiffrement sur disque certifiés EAL4+, chacun sur des cibles de sécurité différentes, ne sont assurément pas comparables. Avant de commencer une démarche de tests, le commanditaire doit faire accepter la cible de

sécurité par l'organisme officiel qui signera le certificat. En France, l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) est cet organisme. L'ANSSI, qui est rattachée au Premier Ministre, engage son sérieux par sa signature, et la confiance que porte un utilisateur dans un produit certifié dépend bien sûr de la confiance qu'inspire l'ANSSI

De plus, pour éviter que le commanditaire de la certification n'opère un savant découpage en dentelles de la cible de sécurité afin de n'y inclure que les fonctionnalités qu'il juge devoir réussir les tests sans problème, il a été introduit la notion de "Profil de Protection" (PP). Si des profils de protection existent, l'ANSSI peut exiger que le périmètre proposé à la certification respecte les exigences spécifiées dans ces documents. Ainsi deux produits de même type, peuvent présenter une cible minimale commune, mais bien sûr un constructeur peut faire certifier une cible plus étendue que celle constituée par l'ensemble des profils de protection exigés, afin de se démarquer de ses concurrents. Les produits ne sont alors plus comparables.

MYTHE N° 4 :
DANS EALX+, LE "+" EST LE PRINCIPAL FACTEUR DE QUALITE

Le niveau d'assurance (aussi communément appelé "niveau d'évaluation" ou "niveau de certification") définit la liste des contrôles qui doivent être réalisés sur le produit et son environnement de développement. Choisir un niveau d'évaluation, par exemple le niveau EAL4 (Evaluation Assurance Level de niveau 4) signifie sélectionner un paquet standard de contrôles tel que définit dans les Critères Communs. Les Critères Communs définissent 7 paquets de EAL1 à EAL7 comportant un nombre croissant de contrôles à réaliser. Mais les Critères Communs offrent aussi la possibilité aux commanditaires des évaluations de demander des contrôles supplémentaires, par exemple qui seraient requis pour des paquets EAL supérieurs. Cet ajout est nommé une "augmentation" du paquet standard EAL. Si la terminologie officielle impose de détailler dans le certificat la liste des augmentations, les fournisseurs de produits se contentent souvent d'un "+".

Ce que recouvre le "+" est parfois négligeable par rapport à ce que recouvre le paquet imposé par le niveau de certification choisi. Hors souvent l'acheteur est plus impressionné par le "+" que par le niveau de certification et ainsi se constitue le mythe du +, qui n'est pas le vrai différentiateur de qualité d'une certification Critères Communs. Mais le "+" peut tout de même recouvrir des éléments significatifs, comme les tâches d'assurance liées à la correction des défauts, ce qui intéresse directement l'acheteur.

MYTHE N° 5 :
UN CERTIFICAT CRITERES COMMUNS A UNE DATE DE PEREMPTION

Oui et Non. Comme nous l'avons indiqué auparavant, un certificat ne s'applique qu'à une version précise d'un produit. Il atteste qu'à la date de signature du certificat, le produit a passé avec succès tous les tests spécifiés dans sa cible de sécurité. Dans l'absolu, cette attestation n'a pas de raison d'être invalidée. En revanche, une personne qui souhaiterait utiliser ce certificat doit se poser la question suivante : vu les évolutions des techniques d'attaque depuis la signature de ce certificat, le produit ne risque-t-il pas aujourd'hui ou demain de ne plus passer la certification ? La ligne Maginot aurait sans doute obtenu la certification Critères Communs … avant 1940.

L'ANSSI propose un programme de « Surveillance » qui revient à mettre à jour régulièrement les résultats des tests. Si cette surveillance est bien adaptée à des produits matériels qui n'évoluent pas, elle l'est moins pour des logiciels en constante évolution. En

effet, il faudrait alors se poser la question : si la version précédente du produit a passé avec succès l'évaluation il y a quelques mois, qu'en est-il de la nouvelle version aujourd'hui ?

Pour répondre à cette question, l'ANSSI propose deux solutions :

- fournir un rapport de maintenance qui, sur la base d'une analyse d'impact réalisée par le développeur, estime un niveau de "certificabilité" de la nouvelle version,
- faire réaliser par un CESTI une réévaluation de la nouvelle version du produit avec réutilisation au maximum des travaux déjà réalisés sur la version antérieure.

MYTHE N° 6 :
UNE CERTIFICATION CRITERES COMMUNS OBTENUE DANS UN DES PAYS CERTIFICATEURS EST AUTOMATIQUEMENT RECONNUE DANS TOUS LES PAYS

Les pays qui possèdent des centres de tests des produits et aussi des organismes officiels qui délivrent et maintiennent les certificats obtenus sont en nombre très limité. Seuls ces pays peuvent être des centres de certification. Un commanditaire qui veut faire certifier une solution de sécurité doit écrire la cible de sécurité sur laquelle portera la certification et la faire accepter par l'organisme officiel d'un des pays certificateurs, même s'il n'y réside pas. Les tests ayant donné un résultat satisfaisant, l'organisme officiel signera le certificat. La certification obtenue dans un des pays certificateurs est reconnue, en théorie, dans tous les pays.

Mais cela n'est vrai que jusqu'au niveau de certification EAL4. Au-delà, cela peut être un mythe. A partir du niveau de certification EAL5, une certification obtenue dans un des pays de la Communauté Européenne n'est reconnue que dans certains des pays de cette Communauté, et seulement aujourd'hui pour les "microcontrôleurs sécurisés et produits similaires". Cette certification Critères Communs au-delà du niveau EAL4 ne sera pas reconnue, aujourd'hui, par les USA. De même, une certification à partir du niveau EAL5 obtenue aux USA n'est pas reconnue dans les pays de la Communauté Européenne. Tout est question d'accords mutuels entre les organismes d'état de chacun des pays (CCRA, SOG-IS) et ces accords évoluent avec le temps.

MYTHE N° 7 :
UN NIVEAU DE CERTIFICATION EVALUE LES FONCTIONNALITES DE SECURITE D'UN PRODUIT

C'est ce qu'on pense généralement mais c'est une idée fausse. Le niveau EALx (Evaluation Assurance Level niveau "x") indique non pas l'étendue des fonctionnalités de sécurité soumises aux tests – c'est la cible de sécurité (ST) qui l'indique - mais la liste des contrôles qui doivent être réalisés sur ces fonctionnalités.

La documentation Critères Communs est constituée de trois volumes. Le deuxième volume est un catalogue de composants fonctionnels qui doivent être utilisés pour spécifier, dans le document Cible de Sécurité, les fonctionnalités de sécurité à évaluer. Une fois la cible de sécurité acceptée par l'organisme officiel (l'ANSSI en France), le niveau de certification sélectionné va définir la manière dont vont se dérouler les tests sur les fonctionnalités de la cible. Cette manière est définie par les composants d'assurance décrits dans le volume 3 des Critères Communs.

Ce niveau peut représenter une évaluation en boîte noire (EAL1) qui consiste à vérifier que le produit se comporte comme l'indique sa Cible de sécurité et sa documentation, ou en boîte blanche, à partir du niveau EAL2 où on commence à regarder comment le produit est conçu. La fourniture d'une partie des sources peut être exigée à partir du niveau EAL4.

A partir du niveau EAL5, les Critères Communs demandent à l'évaluateur de vérifier si le développeur a utilisé des méthodes semi-formelles ou formelles lors de la conception du produit pour la politique de sécurité (EAL5), pour la conception détaillée EAL6), pour la vérification du code (EAL7).

MYTHE N° 8 :
UNE SOLUTION DE SECURITE DOIT ETRE CERTIFIEE CRITERES COMMUNS POUR ENTRER DANS LE CATALOGUE DE L'ADMINISTRATION FRANÇAISE

Comme la démarche pour obtenir une certification Critères Communs dure plusieurs mois et coûte cher, y compris par les ressources internes du commanditaire qu'elle mobilise, peu de PME peuvent se permettre de réunir ce budget.

Pour permettre à tous de faire certifier un produit de sécurité, et même pour que les logiciels libres puissent obtenir une certification, l'ANSSI a conçu une certification plus légère : la CSPN (Certification de Sécurité de Premier Niveau).

En 25 jours de travaux (coûts limités), 35 jours si le produit comporte des mécanismes cryptographiques, une organisation peut faire évaluer son produit pour obtenir la certification CSPN. Bien entendu, la solution de sécurité peut ne pas obtenir cette évaluation à l'issue des 25 ou 35 jours mais les coûts sont limités et connus d'avance.

Pour entrer dans le catalogue des solutions de sécurité des administrations française, le produit certifié doit être également qualifié. La qualification implique une vérification par l'ANSSI que la cible de sécurité est conforme à des profils d'exigences et correspond aux besoins des administrations.

Trois niveaux de qualifications sont définis : élémentaire, standard, et renforcé. La qualification élémentaire implique une certification CSPN, les deux autres une certification Critères Communs. Il est donc faux d'affirmer qu'une solution de sécurité qui n'a pas la certification Critères Communs ne peut être vendue aux administrations.

Un logiciel libre peut ainsi trouver un commanditaire dans son club d'utilisateurs pour être évalué CSPN et entrer dans le catalogue des solutions de sécurité des administrations. TrueCrypt par exemple est certifié CSPN. Attention, la certification CSPN qui est purement française n'est reconnue qu'en France.

MYTHE N° 9 :
EN FRANCE, C'EST L'ANSSI QUI CONDUIT LES TESTS D'EVALUATION

Non, l'ANSSI n'intervient que dans la supervision le contrôle de la conformité des actions d'évaluations de sécurité effectuées par des laboratoires, et l'analyse du rapport d'évaluation, donnant ou non lieu à la délivrance du certificat Critères Communs ou CSPN. L'ANSSI publie les résultats sur son site Web.

Les tests d'évaluation sont menés par une société d'experts qui réalise les tests sur la base du document cible de sécurité écrit par le commanditaire et qui constitue son cahier des charges. Ces sociétés d'experts s'appellent des CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information). Il existe en France deux CESTI habilités à mener les tests d'évaluation Critères Communs pour les logiciels et trois CESTI habilités à mener des tests pour les logiciels embarqués et les cartes à puces. Le CESTI est l'interface obligée entre le commanditaire et l'ANSSI qui signe le certificat au vue des rapports techniques délivrés par le CESTI. Toutefois, si la solution de sécurité comporte des mécanismes cryptographiques, l'ANSSI peut mener des analyses complémentaires sur ces mécanismes.

POUR EN SAVOIR PLUS :

www.ssi.gouv.fr/site_rubrique71.html
www.commoncriteriaportal.org/

2° PARTIE : ASPECTS JURIDIQUES DES TIC

MYTHES ET LEGENDES DE L'IMPUNITE JURIDIQUE, DE L'ARGENT FACILE ET DE LA SURVEILLANCE TOTALE

Christian Aghroum
Ancien chef de l'OCLCTIC
Directeur de la sécurité d'un groupe international suisse

Mais que fait la police ? On a souvent l'impression que le policier et le gendarme sont seulement là pour nous verbaliser au bord des routes ... rassurez vous, ils veillent aussi sur les autoroutes de l'information ...

MYTHE N° 1 :
INTERNET PERMET AUX DELINQUANTS D'ECHAPPER AUX POURSUITES.

Faux, il n'est pas nécessaire de connaître à priori l'auteur ou le suspect des faits commis. Rien n'interdit d'ouvrir une enquête contre personne inconnue, contre X... dit-on, dès lors que l'auteur des faits est inconnu. Il faut cependant reconnaître que la cybercriminalité profite de tous les atouts accordés à la criminalité moderne : un caractère organisé, transfrontalier, complété par l'utilisation de technologies toujours nouvelles, dont n'auraient pu bénéficier que les services secrets il y a à peine deux décennies. La cryptologie, la miniaturisation ne serait-ce que des caméras et appareils photos, des microphones, la simplification des outils de transmission sont autant d'élément de progrès dont les criminels ont rapidement su tirer profit. Enfin, la capacité à disséminer rapidement une information sur la planète entière permet au criminel de tout poil d'élargir considérablement le panel de ses victimes possibles. On pêche avec un immense filet aux mailles très serrées ...

La collaboration entre services de police et autorités judiciaires progresse aussi en matière de lutte contre la cybercriminalité, tout particulièrement grâce à un texte fondateur, la convention de Budapest du 23 novembre 2001.

Alors bien sûr, dans le lot, échappent quelques délinquants, aidés par l'hébergement de leurs activités dans des pays corrompus aux législations défaillantes voire inexistantes. Il n'en reste pas moins vrai que les progrès techniques profitent aussi à la justice. Les services de police se spécialisent et se dotent d'outils performants, la justice se forme et s'adapte. Les cyberpatrouilleurs veillent dorénavant.

L'action pénale ne peut être efficace par contre qu'avec l'aide de la victime qui prendra soin de déposer plainte et de fournir très rapidement et sans hésitation tous les éléments en sa possession. Cela permettra des constatations exhaustives et une meilleure connaissance de l'environnement victimiologique, seules garanties d'une enquête ancrée sur de bonnes bases.

MYTHE N° 2 :
LA POLICE ET LA JUSTICE ONT TOUJOURS UN TEMPS DE RETARD.

Voilà une approche bien rapide et faisant fi de la réalité pragmatique du terrain. Le temps de la justice ne peut pas être celui de l'infraction si l'on veut que la justice demeure objective et impartiale. Police et justice sont ancrées dans le temps de l'action, déclenchée avant tout par leur information. Si nul ne se plaint, si aucune information ne filtre, il ne peut y avoir d'action pénale. Combien d'entreprises refusent de déposer plainte de peur d'une perte d'image, combien de particuliers ont honte d'avoir été si naïfs à postériori ...

Il faut cependant admettre que les approches traditionnelles volent en éclat face à la cybercriminalité : souveraineté nationale, espace frontalier, asymétrie des législations sont autant de frein à une action efficace. Cela n'empêche pas, à force de pugnacité, d'obtenir des succès réguliers grâce à une coopération policière et judiciaire forte et voulue par tous, dès lors que les intérêts individuels ne supplantent pas l'intérêt public.

Enfin, l'apport des services de renseignement en amont de la commission de l'infraction doit demeurer discret, leur permettre d'être efficaces ; il n'en est pas moins indispensable.

MYTHE N° 3 :
EN FRANCE, POLICE ET JUSTICE N'ONT PAS LES COMPETENCES NECESSAIRES.

Encore un lieu commun sans fondement. Depuis la fin des années 80, des unités de police et de gendarmerie se sont progressivement spécialisées, pour permettre à l'heure actuelle la présence sur l'ensemble du territoire national de spécialistes dits "NTECH" pour la gendarmerie nationale (enquêteurs spécialisés en nouvelles technologies) et "ICC" (investigateurs en cyber criminalité) pour la police nationale, nonobstant les cyber correspondants des deux forces placés au plus près des besoins dans les brigades de gendarmerie et commissariat de police. Les douanes concourent à la cyber protection de la France dans la lutte contre les contrefaçons et produits illégalement importés.

La justice forme dès l'Ecole Nationale de la Magistrature ses magistrats et complète leur mise à niveau par des formations spécialisées.

La CNIL participe au dispositif en encadrant les activités de tous et limitant les abus vite tentants en la matière.

La France est enfin dotée d'un arsenal juridique à jour et régulièrement actualisé (la LOPPSI II devrait apporter une dernière touche d'actualité). Cette ossature juridique existe depuis ... 1978 et la loi "informatique et libertés" plaçant la France dans le peloton de tête des précurseurs en matière de lutte contre la cybercriminalité et de protection de ses concitoyens.

MYTHE N° 4 :
L'ARGENT EST FACILE A GAGNER SUR INTERNET.

Quel argent ?

L'argent propre : comme toute activité humaine, le créatif, innovateur, consciencieux, et travailleur peut gagner sa vie au prix des efforts qu'il mettra à la bonne avancée de son entreprise. Encore que sans idée novatrice, sans un entourage compétent, sans l'appui d'un banquier, il est dur d'imaginer que l'argent puisse miraculeusement couler par le biais de connexions diverses vers un compte bancaire en ligne.

L'argent sale : lui pourra plus facilement alimenter les caisses de votre organisation dès lors que sans scrupules vous envisagez de voler, infiltrer, escroquer, trahir la confiance de votre prochain. Bienvenue dans le monde des criminels peuplé de trahisons, de dénonciations, de surveillances par les services de police, d'années de prison, de saisie complète de vos biens considérés à juste titre comme des avoirs criminels. Au résultat, loin des clichés cyberromantiques véhiculant de modernes Robin des Bois, de richissimes magnats enrichis rapidement par quelques magouilles sans risques physiques sortes de Spaggiari à la mode cyber, vieillissent le lot des criminels usés par les années de prison, désociabilisés et bannis.

MYTHE N° 5 :
BLANCHIR ET CACHER SON ARGENT EST A LA PORTEE DE TOUS SUR INTERNET.

Ce n'est déjà pas à la portée de tous les délinquants, il est dur d'imaginer que cela puisse être à la portée des honnêtes gens ... qui de toutes façons deviendraient alors délinquants ... Des affaires récentes ont également démontré que la fragilité de certains systèmes d'information conduit aussi les pays réputés pour leur discrétion bancaire à revoir leur position et permet aux services de l'Etat de récupérer quelques listes de citoyens indélicats envers leur système fiscal, au moins ...

MYTHE N° 6 :
INTERNET EST ENTIEREMENT SOUS LA SURVEILLANCE DES ETATS UNIS ET DE LA PLUPART DES PAYS.

Bien sûr qu'il est possible de surveiller internet, comme il l'est des communications en général. Cependant, la surveillance exercée par les services de renseignement ou par les services judiciaires ne saurait être exhaustive. Au delà des contraintes légales, de la déontologie et de l'éthique des forces en charge de son exercice, cette surveillance totale ne peut de toute façon l'être, faute de temps et de moyens tout simplement. On est encore loin de "Big Brother" fort heureusement. La surveillance s'exerce en destination de cibles préalablement repérées grâce à toutes les méthodes existantes dont les plus traditionnelles sont les plus efficaces. La source, l'informateur, l'aviseur, ou quelque soit le terme par lequel on le désigne, sera toujours le meilleur point de départ d'une enquête dès lors recoupée par des surveillances physiques et techniques.

Le contrôle d'accès à internet est par contre opéré dans de nombreux pays dont la proximité à la démocratie est aussi lointain que l'âge de pierre l'est au cyber espace. Ce filtrage est la forme moderne de la censure par ailleurs exercée sur tous les médias au sein de ces dictatures déclarées ou non.

"Big brother is watching you !". Laissons ce cauchemar à Orwell mais gardons cet avertissement à l'oreille ; qu'il nous permette de nous prémunir de toute dérive vers laquelle nous conduirait une technique totalement débridée.

MYTHE N° 7 :
ON PEUT TOUT DIRE ET TOUT FAIRE SUR INTERNET, C'EST UN TOTAL ESPACE DE LIBERTE.

Internet n'appartient plus aux seuls internautes, Internet est devenu un espace public ! Dès lors, il doit être soumis aux mêmes règles que tout espace de communication. La loi encadre pour le bien de tous l'expression publique : on peut penser ce que l'on veut, s'exprimer tant que l'on veut, dès lors que l'on respecte son prochain. Ainsi, l'injure, la diffamation, la propagation de fausses nouvelles, l'incitation à la haine raciale, l'excitation à la débauche sont autant de formes d'expressions déviantes, insupportables aux règles d'une vie courtoise et paisible en société et ne permettent ni à la tolérance et ni au respect de l'autre de s'exprimer. Il en est de même pour internet, les mêmes infractions sont tout aussi détestables, détectables et poursuivables.

Une étape mériterait d'être franchie, celle de la création d'un droit international de l'internet au même titre qu'il existe un droit de l'espace aérien ou de l'espace maritime. Nul doute qu'il simplifierait la circulation, l'installation et l'expression de tous. A condition de trouver outre l'ICANN et la convention de Budapest un nouveau leader et un outil légal plus universel encore ... auprès de l'O.N.U. peut-être ?

MYTHE N° 8 :
IL N'Y A QUE LES NAÏFS QUI SE FONT AVOIR SUR INTERNET.

Faux ... si le caractère naïf des victimes de phishing ou d'escroquerie à la nigériane est souvent mis en avant, c'est mal connaître la malignité des cyberdélinquants et leurs capacités à mettre en place des dispositifs d'ingénierie sociale de plus en plus ingénieux. Même les plus attentifs peuvent si faire prendre par négligence, fatigue ou du fait d'une trop grande confiance dans des dispositifs techniques qui même mis à jour à temps sont parfois détournés par une technique nouvelle. Enfin, chacun a ses petites faiblesses, ses penchants, ses passions qui le conduiront à répondre trop rapidement à un mail alléchant, une publicité plus vraie que nature, un appel à la charité bien ciblé ; une seule parade : faire preuve de bon sens, prendre le temps nécessaire à la réflexion et à l'interrogation, les sites d'aide et de prévention sont à cet égard suffisamment nombreux.

MYTHE N° 9 :
SIGNALER LES FAITS NE SERT A RIEN.

Bien sûr que si, signaler des faits apparemment illégaux relevés sur internet procède du civisme et de l'esprit d'entraide de son prochain. Il ne s'agit en rien de délation ! Si je suis témoin d'un accident de la route et que le chauffard s'enfuit en laissant une victime agonisante sur le bord de la chaussée, je préviens police et services de secours. De la même manière, si je détecte incidemment un site pédopornographe ou d'escroqueries sur internet, je le signale auprès du service créé à cet effet sur le site www.internet-signalement.fr, même anonymement. L'information sera vérifiée, qualifiée pénalement et adressée en France ou à l'étranger vers le service de police, de douanes, de répression des fraudes compétent. En quelques clics de souris, j'aurais aidé à protéger les enfants de mes voisins ou épargner à quelqu'un de se faire arnaquer par un escroc sans scrupules ...

De même est-il vain de croire que de petites infractions, pour lesquelles on a déposé plainte et qui ne sont pas poursuivies, demeurent lettres mortes. C'est à travers le recoupement de ces informations que les services de police décèlent des organisations criminelles transnationales et activent leurs homologues étrangers. Une victime à 100 euros ne motivera pas un service à l'étranger, 10 000 victimes des mêmes faits permettront de déclencher une opération internationale. Alors consolons nous, si malheureusement notre cas n'est pas résolu, la plainte ou le signalement du fait permettra certainement d'en prévenir de nombreux autres.

MYTHE N° 10 :
LE PARTENARIAT PUBLIC PRIVE EST UN SERPENT DE MER.

Le PPP est bien souvent cité, rarement décrit, ce qui laisse penser à la Belle Arlésienne. Pourtant, dans le cadre de la lutte contre la cybercriminalité, le partenariat public privé est une réalité quotidienne. L'enquête de police est de plus en plus une enquête de traçabilité dans laquelle sur la base de constatations, les services cherchent des traces physiques, biologiques, techniques et technologiques. La plupart de ces traces numériques sont détenues par d'autres que l'Etat : banques, fournisseurs d'accès, opérateurs de téléphonie, fournisseurs d'accès ... Les services de l'Etat en quête de vérité sont dépendants de partenaires privés qu'il faut alors requérir selon les formes légales. Il devient donc incontournables pour les uns et les autres de mieux se connaître : comment rechercher ce qu'on ne connaît pas, comment répondre avec pertinence et célérité à un interlocuteur inconnu ou envers lequel on a de la défiance, comment conjuguer impératifs de service public, continuité, horaires et contraintes financières, reports de charges et impératifs légaux de stockage de l'information ... Toutes ces

questions trouvent réponse dans une connaissance mutuelle basée sur la découverte et la confiance mutuelle encadrée.

Le guide des bonnes pratiques voté et publié par le Conseil de l'Europe[11] suivi de celui de la Commission Européenne[12] sont des avancées juridiques considérables. Signal-Spam est une organisation publique-privée, dont la compétence et l'efficacité dans la lutte contre le spam ne sont plus à démontrer.

Un regret : l'absence d'un véritable dispositif interministériel calqué sur la mission interministérielle de lutte contre la drogue et la toxicomanie qui permettrait d'organiser de manière cohérente la synthèse des actions des différentes entités publiques et privées dans un effort commun et concerté. Ce rôle n'est pas celui de l'ANSSI ne celui de la CNIL et n'a pu être tenu par le forum des droits de l'internet. La MILC, mission interministérielle de lutte contre la cybercriminalité, dotée d'un budget et d'une autorité réglementaire, répondant directement au Premier Ministre, pourrait efficacement fonctionner sous la présidence d'un Monsieur ou d'une Madame "Cyber" charismatique et reconnu(e).

[11] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/Reports-Presentations/567%20prov-d-%20guidelines%20provisional2%20_3%20April%202008_FRENCHrev.pdf

[12] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/fr/jha/103548.pdf

MYTHES ET LEGENDES DU DROIT DE LA COMMUNICATION SUR L'INTERNET

Sadry Porlon
Avocat au Barreau de Paris

Le droit de la presse, dont la pierre angulaire reste la loi 29 juillet 1881, a été suivi par la création d'un droit plus large dit de la communication après l'apparition de la télévision, de la radio et plus récemment d'internet.

Ce droit de la communication qui, de prime abord, semble abordable, est en réalité un droit des plus techniques au sein duquel un formalisme des plus stricts doit être respecté pour envisager intenter avec succès une action devant les tribunaux ou encore faire valoir ses droits devant le responsable d'un site internet.

Il convient, en effet, de savoir distinguer la diffamation, de l'injure, du dénigrement ou encore de la simple atteinte à la vie privée pour être certain de voir ses demandes accueillies valablement par les juges.

L'apparition d'internet, sans pour autant avoir révolutionné le droit de la communication, a nécessité la mise en place des textes spécifiques contenus, pour la plupart, dans la loi du 24 juin 2004 dite Loi de Confiance dans l'Économie Numérique.

De nombreuses idées reçues sont diffusées autour du droit de la communication quand il touche à internet.

Gros plan sur certaines d'entre elles…

MYTHE N° 1 :
UNE INJURE OU UNE DIFFAMATION DONT ON EST VICTIME SUR INTERNET EST SUSCEPTIBLE D'UNE ACTION DEVANT LES TRIBUNAUX TANT QUE LE MESSAGE EST VISIBLE SUR LE SITE LITIGIEUX

A la fin des années 1990, la doctrine s'est penchée sur la question de savoir si les infractions de presse commises sur internet devaient ou non présenter une spécificité d'ordre procédural par rapport aux infractions propres à la presse écrite.

Elle s'est demandée si ces infractions devaient être considérées comme continues, lesquelles subsistent tant que les messages sont accessibles et ne font courir le délai de prescription qu'à compter de la date de leur suppression, ou comme « instantanées », ce délai démarrant alors dès la date de la mise en ligne, constitutive du fait de publication.

La Cour de cassation a posé, après quelques hésitations jurisprudentielles, que « lorsque des poursuites pour l'une des infractions prévues par la loi de 1881 sont engagées à raison de la diffusion, sur le réseau internet, d'un message figurant sur un site, le point de départ du délai de prescription de l'action publique prévu par l'article 65 de la loi du 29 juillet 1881 doit être fixé à la date du premier acte de publication ; que cette date est celle à laquelle le message a été mis pour la première fois à la disposition des utilisateurs ». (Cass. crim., 27 nov. 2001, C. : Comm. com. électr. 2002, comm. 32, obs. A. Lepage ; Légipresse 2002, n° 189, III, p. 26 et 27).

Dès lors, il faut donc considérer que sur internet, comme en matière de presse écrite, le délai de prescription commence à courir à compter du premier jour de la publication et que le fait que le message demeure accessible ou disponible n'y change rien.

Ce principe, qui peut paraître injuste à bien des égards, oblige celui qui s'interroge sur le bien fondé d'une action pour diffamation ou pour injure, suite à la découverte sur internet de propos litigieux, à s'assurer préalablement que le message a bien été publié moins de trois mois avant.

L'article 6-V de la loi de la Loi de Confiance dans l'Économie numérique du 21 juin 2004 renvoie, en effet, aux dispositions de l'article 65 de la loi de 1881 qui prévoit que ce délai de prescription est de trois mois à compter de la date de la publication.

Par ailleurs, depuis une loi n° 2004-204 du 9 mars 2004, le délai de prescription des infractions à caractère raciste (exemples : provocation à la discrimination ou à la haine raciale, diffamation raciale, injure raciale) est d'un an. Ce délai s'applique également à Internet.

MYTHE N° 2 :
IL FAUT AVOIR ETE INJURIE, DIFFAME OU DENIGRE POUR POUVOIR OBTENIR UN DROIT DE REPONSE AUPRES DU SITE INTERNET A L'ORIGINE DE L'INFRACTION

Le droit de réponse à un caractère général et absolu. Cela implique donc qu'il n'est pas subordonné à la preuve que les propos auxquels il répond soient motivés par une intention de nuire de la part de son auteur.

L'article 6, IV alinéa 1 de la loi du 21 juin 2004 dispose en effet que :

« Toute personne nommée ou désignée dans un service de communication au public en ligne dispose d'un droit de réponse, sans préjudice des demandes de correction ou de suppression du message qu'elle peut adresser au service (…) ».

Il suffit donc d'avoir été nommée ou désignée sur internet pour pouvoir prétendre à un droit de réponse auprès du directeur de publication du site.

Dans l'absolu, même un article flatteur et complètement exact est susceptible de provoquer un droit de réponse des plus valables de la part de la personne nommée ou désignée dans l'article ou le message disponible sur internet.

Une disposition des plus utiles pour une personne physique ou morale qui, ne trouvant pas la matière suffisante à une action pour diffamation ou pour injure aurait, par cet intermédiaire, l'occasion de donner son point de vue et sa version des faits en réplique à l'article ou un message litigieux.

MYTHE N° 3 :
IL FAUT AVOIR ETE INJURIE, DIFFAME OU DENIGRE POUR POUVOIR OBTENIR UN DROIT DE REPONSE AUPRES DE LA TELEVISION OU DE LA RADIO A L'ORIGINE DE L'INFRACTION

Tout dépendra en réalité du moyen de diffusion de cette télévision ou de cette radio.

Il faut savoir que la réglementation du droit de réponse dans les services de communication audiovisuelle (c'est à dire à la télévision ou à la radio) est extérieure à la loi du 29 juillet 1881.

Le droit de réponse spécifique à la presse écrite n'a donc pas été, contrairement à internet, directement transposé en matière audiovisuelle.

Le droit de réponse à la radio ou à la télévision est subordonné à la démonstration « d'imputations susceptibles de porter atteinte à l'honneur ou à la réputation d'une personne ».

L'article 6 de la loi du 29 juillet 1982 dispose que : « Toute personne physique ou morale dispose d'un droit de réponse dans le cas où des imputations susceptibles de porter atteinte à

son honneur ou à sa réputation auraient été diffusées dans le cadre d'une activité de communication audiovisuelle (…)

Il existe néanmoins une exception à ce principe.

Dans le cas de ce qu'on appelle une web télé ou d'une web radio (médias diffusés exclusivement sur internet), la réglementation relative au droit de réponse redevient celle prévue à l'article 6 IV de la loi du 21 juin 2004, ce qui implique que tout message désignant une personne peut être à l'origine d'un droit de réponse ; quelle que soit sa teneur.

MYTHE N° 4 :

DEMANDER UN DROIT DE REPONSE A L'EDITEUR D'UN SITE INTERNET ET L'OBTENIR EMPECHE TOUTE ACTION DEVANT LES TRIBUNAUX CONTRE L'AUTEUR DES PROPOS.

Les actions pour diffamation ou pour injure sont indépendantes de l'exercice du droit de réponse.

Une personne peut donc légitimement solliciter un droit de réponse en engageant simultanément une action devant les tribunaux contre l'auteur du message diffusé sur internet.

MYTHE N° 5 :

LE FAIT QUE L'AUTEUR D'UN MESSAGE DIFFAMATOIRE OU INJURIEUX SE SOIT EXCUSE PUBLIQUEMENT SUITE A LA DIFFUSION DU PROPOS LUI PERMETTRA D'ECHAPPER A UNE SANCTION EN CAS D'ACTION DEVANT LES TRIBUNAUX.

Le repentir actif, c'est-à-dire l'action qui consiste pour l'auteur d'un message injurieux ou diffamatoire à présenter ses excuses publiques ou à publier un rectificatif, ne supprime pas l'intention coupable.

La personne directement visée par les propos litigieux pourra toujours agir et obtenir la condamnation de son auteur.

MYTHE N° 6 :

LE FAIT POUR L'EDITEUR D'UN SITE INTERNET DE NE PAS AVOIR MIS A DISPOSITION DES INTERNAUTES UN CERTAIN NOMBRE D'ELEMENTS D'IDENTIFICATION COMME, POUR LES PERSONNES PHYSIQUES, (SON NOM, SON PRENOM, SON DOMICILE) OU POUR LES PERSONNES MORALES (SA DENOMINATION, SA RAISON SOCIALE OU ENCORE SON SIEGE SOCIAL) NE PEUT PAS LUI VALOIR UNE CONDAMNATION DEVANT LES TRIBUNAUX.

Le non-respect des obligations prévues à l'article 6-III-1 de la loi du 21 juin 2004 est « puni d'un an d'emprisonnement et de 75 000 euros d'amende ». (Article 6-VI-2 de la loi du 21 juin 2004).

Les personnes morales peuvent se voir interdire d'exercer leur activité « pour une durée de cinq ans au plus ». (L. 131-38 et L. 131-39 du Code pénal).

L'article 6-III-2 prévoit une exception notamment pour les blogueurs anonymes qui exercent cette activité à titre non professionnel.

Cet article pose, en effet, que « les personnes éditant à titre non professionnel un service de communication au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale » de leur fournisseur d'hébergement, « sous réserve de lui avoir communiqué les éléments d'identification personnelle » exigés des éditeurs de services agissant à titre professionnel.

C'est d'ailleurs cette distinction entre les obligations d'identification auxquelles sont tenus les éditeurs professionnels et les éditeurs non professionnels de services en ligne qui a motivé la fameuse proposition de loi en date du 3 mai 2010 du Sénateur Jean-Louis Masson, laquelle tendait « à faciliter l'identification des éditeurs de sites de communication en ligne et en particulier des « blogueurs » professionnels et non professionnels ».

MYTHE N° 7 :
IL EST POSSIBLE DE REPRODUIRE INTEGRALEMENT L'ARTICLE D'UN AUTEUR SUR SON SITE A CONDITION DE CITER SON NOM ET LA SOURCE DE L'ARTICLE.

L'article L. 122-4 du Code de la propriété intellectuelle dispose que :

« Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droits est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque. »

L'article L. 335-2 alinéa 3 du Code de la propriété intellectuelle ajoute que :

« Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon, et toute contrefaçon est un délit ».

Il s'agit d'un délit puni de trois ans d'emprisonnement et de 300.000 euros d'amende.

L'article L. 122-5 du Code de la propriété intellectuelle prévoit néanmoins une exception dans le cas où il s'agit d'une courte citation de l'article.

La courte citation s'évaluera par rapport aux dimensions de l'œuvre citée, mais aussi de celle de l'œuvre citante. Cette citation devra être justifiée par certaines finalités (critique, polémique, pédagogique, scientifique ou d'information) de l'œuvre d'origine.

Elle devra également être intégrée à une œuvre ayant une autonomie propre en dehors des citations.

MYTHE N° 8 :
LE FAIT DE REPRODUIRE UNE ŒUVRE OU UN CONTENU SUR UN SITE INTERNET A VOCATION NON COMMERCIALE PERMET D'ECHAPPER A UNE CONDAMNATION POUR CONTREFAÇON.

Malgré une forte croyance chez l'internet lambda, la loi n'a jamais entendu faire de distinction l'éditeur d'un site qui reproduit l'œuvre d'un tiers sans autorisation et dans un but commercial et celui qui le fait dans un but non commercial.

Les deux sont, dès lors, potentiellement condamnables pour contrefaçon à ce titre tant sur le plan pénal que sur le plan civil.

CONCLUSION

Ces quelques exemples contribuent à illustrer le fossé qui existe entre la perception qu'à l'internaute lambda d'un internet dans lequel régnerait le vide juridique et la réalité dans laquelle ce média n'a finalement eu que peu de mal à se voir appliquer des règles datant du XIXème siècle.

Les contentieux sans cesse croissants générés par quelques uns des millions de messages diffusés quotidiennement sur les blogs, les forums de discussion ou encore à travers les réseaux sociaux comme Facebook ou Twitter, sont d'ailleurs là pour en témoigner.

MYTHES ET LEGENDES DES TELECHARGEMENT ILLEGAUX

Sadry Porlon
Avocat au Barreau de Paris

La loi du 12 juin 2009 favorisant la diffusion et la protection de la création (dite HADOPI 1), puis celle du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet (dite HADOPI 2) ont conduit d'une part, à la création de la HADOPI, Haute autorité pour la diffusion des œuvres et la protection des œuvres, à celle de création d'une obligation pour le titulaire de l'accès à l'internet ne soit pas utilisé à des fins de contrefaçon, sorte d'obligation de sécurisation de l'accès à l'internet à la charge de l'abonné, faute de quoi il s'exposera notamment à la contravention de négligence caractérisée, et d'autre part à adapter le dispositif pénal applicable aux contrefaçons commises sur internet.

Quelques idées reçues existent encore sur le téléchargement illégal en général et sur HADOPI en particulier…

MYTHE N°1 :
L'EXCEPTION POUR COPIE PRIVEE PERMET A CELUI QUI TELECHARGE UNE ŒUVRE SUR INTERNET SANS AUTORISATION DE NE PAS ETRE CONDAMNE DEVANT LES TRIBUNAUX S'IL DEMONTRE QUE LADITE COPIE A FAIT L'OBJET D'UNE UTILISATION STRICTEMENT PRIVEE

L'article L. 122-5 du Code de la propriété intellectuelle prévoit qu'il est possible de copier une œuvre pour un usage privé.

L'article L. 122-5 alinéa 2 refuse, en effet, la possibilité à l'auteur de l'œuvre d'interdire « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective (…) ».

L'exception affirmée par le Code de propriété intellectuelle ne distingue pas selon les supports.

Mieux, il n'est nulle part exigé que le copiste se doive de disposer de l'œuvre originale pour en faire la copie. L'article L 122-5 du Code de la propriété intellectuelle qui accorde à l'utilisateur un droit à la copie privée ne distingue pas non plus selon que la copie soit légale ou pas ou encore que l'utilisateur possède l'original dont il fait la copie.

La question de savoir si l'exception de copie privée trouve ou non à s'appliquer dans le cas d'une copie d'œuvres téléchargées sur internet, notamment via logiciel peer to peer, a donc longtemps été, de ce fait, l'objet d'une vive controverse doctrinale et jurisprudentielle.

Des opinions défavorables à la prise en compte de l'exception pour copie privée en cas de téléchargement sans autorisation se sont développées à partir de l'idée selon laquelle la copie réalisée à partir d'un exemplaire contrefaisant est elle-même contaminée par ce caractère illicite et ne peut donc pas être couverte par l'exception pour copie privée.

La jurisprudence est venue depuis clarifier quelque peu la situation.

Dans une affaire qui a fait beaucoup parler, un étudiant avait gravé près de 500 films sur cédéroms ; films qu'il avait, notamment, auparavant téléchargés sur Internet. Poursuivi

devant les tribunaux pour contrefaçon de droit d'auteur par la majeure partie de l'industrie cinématographique mondiale, il a tenté de se prévaloir de l'exception pour copie privée.

En premier instance, le Tribunal correctionnel de Rodez a conclu, le 13 octobre 2004, à l'absence de contrefaçon, ce qu'à confirmé la Cour d'Appel de Montpellier, dans un arrêt en date du 10 mars 2005, sans pour autant se prononcer sur le caractère licite ou illicite de la source des copies.

La Cour de Cassation est venu casser l'arrêt précité en retenant notamment que :

« Attendu que, pour confirmer le jugement entrepris, l'arrêt retient qu'aux termes des articles L 122-3, L 122-4 et L 122-5 du code de la propriété intellectuelle, lorsqu'une œuvre a été divulguée, l'auteur ne peut interdire les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective ; que les juges ajoutent que le prévenu a déclaré avoir effectué les copies uniquement pour un usage privé et qu'il n'est démontré aucun usage à titre collectif ;

Mais attendu qu'en se déterminant ainsi, sans s'expliquer sur les circonstances dans lesquelles les œuvres avaient été mises à disposition du prévenu et sans répondre aux conclusions des parties civiles qui faisaient valoir que l'exception de copie privée prévue par l'article L 122-5, 2°, du code de la propriété intellectuelle, en ce qu'elle constitue une dérogation au monopole de l'auteur sur son œuvre, suppose, pour pouvoir être retenue que sa source soit licite et nécessairement exempte de toute atteinte aux prérogatives des titulaires de droits sur l'œuvre concernée, la cour d'appel n'a pas justifié sa décision ; ».

Dès lors, il n'est donc pas possible de prétexter valablement de l'exception pour copie privée pour télécharger, sans autorisation, des œuvres sur internet.

MYTHE N°2 :
DEPUIS LES LOIS HADOPI, LE TELECHARGEMENT ILLEGAL D'UNE ŒUVRE SUR INTERNET NE PEUT PLUS ETRE SANCTIONNE « QUE » PAR UNE SUSPENSION D'INTERNET PENDANT UN MOIS MAXIMUM ET D'UNE AMENDE NE DEPASSANT PAS 1500 EUROS.

Un décret du 25 juin 2010, pris en application de la loi HADOPI 2 est venu définir ce qu'est la contravention de négligence caractérisée tout en précisant la caractérisation de ce manquement et les sanctions encourues par l'abonné.

L'article R. 335-5 du Code de la propriété intellectuelle dispose désormais que :

« I.-Constitue une négligence caractérisée, punie de l'amende prévue pour les contraventions de la cinquième classe, le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne, lorsque se trouvent réunies les conditions prévues au II :

1. Soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ;
2. Soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.

II.-Les dispositions du I ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes :

1. En application de l'article L. 331-25 et dans les formes prévues par cet article, le titulaire de l'accès s'est vu recommander par la commission de protection des droits de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de reproduction, de représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ;

2. Dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées au 1° du présent II.

III.-Les personnes coupables de la contravention définie au I peuvent, en outre, être condamnées à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un mois, conformément aux dispositions de l'article L. 335-7-1.

L'abonné s'expose donc à ce titre à une contravention de 5ème classe (amende de 1500 euros maximum) ainsi qu'à une peine complémentaire de suspension de l'accès à internet qui ne pourra excéder un mois.

Cependant, le recours à la procédure judiciaire simplifiée de l'ordonnance pénale prévue par la loi HADOPI 2 n'est qu'une possibilité qui vient s'ajouter aux actions civiles et pénales liées à la contrefaçon de droit d'auteur et en aucun un préalable nécessaire à l'engagement de poursuites.

Tout abonné dont l'accès à internet a été utilisé à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits reste, en effet, sous la menace d'une action en contrefaçon de droit d'auteur et des sanctions encourues en matière de contrefaçon soit une peine maximum d'emprisonnement de 3 ans et une amende de 300.000 euros (article L. 335-2 du Code de la propriété intellectuelle).

La loi HADOPI 2 a d'ailleurs apporté des changements en matière de sanctions pénales en précisant qu'une nouvelle possibilité de sanction pénale est donnée au juge lorsque le délit de contrefaçon a été commis par le biais d'un service de communication au public en ligne à savoir celle de prononcer une peine complémentaire de suspension de l'accès à internet pendant une durée maximale d'un an (Article L. 335-7 alinéa 1).

MYTHE N°3 :

SI MON ACCES A INTERNET EST SUSPENDU SUITE A UNE DECISION DU JUGE, IL ME SUFFIT DE SOUSCRIRE IMMEDIATEMENT UN NOUVEL ABONNEMENT

Il est interdit à un abonné dont l'accès à internet aurait été suspendu suite à une décision du juge de se réabonner par un autre moyen.

L'article L. 335-7-1 du Code de la propriété intellectuelle prévoit d'ailleurs que le fait pour la personne condamnée à la peine complémentaire de suspension d'internet de ne pas respecter l'interdiction de souscrire un autre contrat d'abonnement à un service de communication au public en ligne pendant la durée de la suspension est puni d'une amende d'un montant maximal de 3 750 euros.

MYTHE N°4 :

SI LE JUGE DECIDE D'UNE SUSPENSION DE MON ABONNEMENT, JE NE VAIS QUAND MEME PAS ETRE CONTRAINT DE CONTINUER A PAYER CET ABONNEMENT PENDANT LA DUREE DE CETTE SUSPENSION

Dans l'hypothèse d'une suspension d'internet pendant un maximum d'un an au motif qu'une sanction pénale au titre d'une contrefaçon aurait été prononcée par le juge cette suspension de l'accès n'affecte pas, par elle-même, le versement du prix de l'abonnement au fournisseur du service.

L'article L. 121-84 du code de la consommation qui dispose : « Tout projet de modification des conditions contractuelles de fourniture d'un service de communications électroniques est communiqué par le prestataire au consommateur au moins un mois avant son entrée en

vigueur, assorti de l'information selon laquelle ce dernier peut, tant qu'il n'a pas expressément accepté les nouvelles conditions, résilier le contrat sans pénalité de résiliation et sans droit à dédommagement, jusque dans un délai de quatre mois après l'entrée en vigueur de la modification » n'est pas applicable au cours de la période de suspension.

Les frais d'une éventuelle résiliation de l'abonnement au cours de la période de suspension sont supportés par l'abonné.

Pour information, le fait pour une le fournisseur d'accès à internet de ne pas mettre en œuvre la peine de suspension qui lui a été notifiée est également puni d'une amende maximale de 5 000 euros.

MYTHE N°5 :

L'ABONNE QUI REÇOIT DES RECOMMANDATIONS DE LA PART DE LA HADOPI DEVRA ATTENDRE D'ETRE POURSUIVI DEVANT LES TRIBUNAUX POUR FAIRE VALOIR SES DROITS

L'abonné qui reçoit un ou plusieurs avertissements peut directement présenter ses observations à la Commission de protection de la HADOPI et demander des précisions sur le contenu des œuvres et objets protégés concernés par le ou les manquements qui lui sont reprochés.

Il pourra notamment être convoqué ou demandé à être entendu et pourra se faire assister du conseil de son choix.

Si une ordonnance pénale venait à être rendue à son encontre, l'abonné aura également la possibilité de contester la décision rendue, dans un délai de quarante cinq jours à compter de la notification en formant opposition à l'exécution de ladite ordonnance.

Cela a pour conséquence de renvoyer l'affaire devant le tribunal correctionnel pour un débat qui sera, cette fois, contradictoire.

Il reviendra alors à l'abonné de monter, le cas échéant avec l'aide de son conseil, un dossier visant à démontrer, preuves à l'appui, qu'il n'est en aucun cas le responsable des faits qui lui sont directement reprochés et qu'eu égard à l'article 121-1 du Code pénal disposant que : « Nul n'est responsable que de son propre fait », il ne peut être valablement sanctionné.

MYTHE N°6:

EN PRESENCE D'UN TELECHARGEMENT ILLEGAL AVERE, LE JUGE A UNE MARGE DE MANŒUVRE ASSEZ FAIBLE DANS LA FIXATION DE LA DUREE DE LA SUSPENSION DE L'ACCES A INTERNET

L'article L. 335-7-2 du Code de la propriété intellectuelle prévoit que pour prononcer la peine de suspension (peine complémentaire à l'amende de contravention de 5ème catégorie) prévue aux articles L. 335-7 (un an maximum en cas de contrefaçon) et L. 335-7-1 (un mois maximum en cas de négligence caractérisée) et en déterminer la durée, la juridiction prend en compte les circonstances et la gravité de l'infraction ainsi que la personnalité de son auteur, et notamment l'activité professionnelle ou sociale de celui-ci, ainsi que sa situation socio-économique.

Ainsi, cet article permet notamment au juge de tenir compte de la personnalité de l'abonné afin de déterminer la peine complémentaire de suspension d'internet.

On imagine que cela puisse être le cas d'une entreprise pour laquelle le maintien de la connexion à internet est la condition sine qua non du maintien de son activité ou encore d'un particulier qui justifierait que ce média est pour lui une ouverture indispensable sur le monde.

L'article 335-7-2 du Code de la propriété intellectuelle précise d'ailleurs que la durée de la peine prononcée doit concilier la protection des droits de la propriété intellectuelle et le respect du droit de s'exprimer et de communiquer librement, notamment depuis son domicile.

MYTHE N°7 :
C'EST LA HAUTE AUTORITE POUR LA DIFFUSION DES ŒUVRES ET LA PROTECTION DES ŒUVRES QUI COLLECTE, ELLE-MEME, LES ADRESSES IP DES ABONNES DONT L'ACCES A SERVI A TELECHARGER DES ŒUVRES

La HADOPI, saisie en cela par les ayants droits des œuvres, peut constater et établir des procès verbaux de manquements à l'obligation de sécurisation, adresser des avertissements aux abonnés ou encore transmettre au procureur de la République tout fait susceptible de constituer une infraction.

Elle ne collecte pas directement les adresses IP.

Ce sont les organismes assermentés représentant les titulaires des droits (pour l'heure, la société Trident Media Guard - TMG) qui, ayant reçu préalablement les autorisations nécessaires de la CNIL pour effectuer ces démarches, se chargent d'observer les œuvres circulant sur les réseaux et de collecter ce type informations.

La HADOPI se contente de recevoir les saisines des sociétés de perception et de répartition des droits et des organismes de défense professionnelle ayant reçu une autorisation de la CNIL.

Elle peut par la suite obtenir des fournisseurs d'accès à l'internet ou des prestataires d'hébergement, l'identité, l'adresse postale, l'adresse électronique et les coordonnées téléphoniques de l'abonné dont l'accès à l'internet à été utilisé à des fins de contrefaçon et ce sur la base des adresses IP collectées par les sociétés privées mandatées par les ayants droit pour surveiller les réseaux de téléchargement illégal.

La réponse graduée débutera ensuite par l'envoi d'une recommandation ou « avertissement » à l'abonné par le biais d'un courriel et par l'intermédiaire du fournisseur d'accès auprès duquel il a souscrit un abonnement.

Celle-ci prévoit notamment un rappel de l'obligation de sécurisation, la mention de la date et l'heure auxquelles les faits susceptibles de constituer un manquement à l'obligation de sécurisation ont été constatés ainsi que les coordonnées téléphoniques, postales et électroniques où l'abonné peut s'adresser, s'il le souhaite, pour formuler ses observations et obtenir des précisions sur ce qui lui est reproché.

Si dans les six mois suivant cette recommandation l'accès à internet devait à nouveau être utilisé pour « des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits lorsqu'elle est requise », une seconde recommandation pourra lui être adressée par le biais d'une lettre recommandée avec avis de réception ou encore par tout autre moyen permettant d'établir la preuve de la date de présentation de cette recommandation.

La loi HADOPI 1 a imposé à la personne titulaire de l'accès à des services de communication au public en ligne l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits lorsqu'elle est requise.

Si malgré un second avertissement l'accès internet de l'abonné devait de nouveau servir à des fins de contrefaçon de droit d'auteur, la HADOPI pourra remettre son dossier à un juge afin que l'abonné soit, notamment, sanctionné d'une amende et/ou d'une suspension de son accès à internet ou encore transmettre au procureur de la république tout fait susceptible de constituer une infraction.

CONCLUSION

Ces quelques exemples démontrent une fois de plus le fossé qui existe entre le grand public qui associe assez souvent internet gratuité et le législateur qui n'a finalement qu'à de rares exceptions accepté que ce média puisse déroger aux grands principes du droit de la propriété intellectuelle.

MYTHES ET LEGENDES DE LA CONTREFAÇON SUR L'INTERNET

Sadry Porlon
Avocat au Barreau de Paris

Le fléau mondial qu'est la contrefaçon sur internet prend différentes formes. L'une des plus connues, à savoir le téléchargement illégal, ayant été abordée dans un chapitre précédent, nous allons cette fois nous intéresser à quelques unes des actions qu'il est possible d'intenter devant les tribunaux pour faire cesser l'infraction qu'il s'agisse de contrefaçon de droit d'auteur, de marque ou encore de concurrence déloyale (cybersquatting).

MYTHE N°1 : DE SIMPLES IMPRESSIONS D'ECRAN SUFFISENT POUR PROUVER DEVANT LES TRIBUNAUX LA MATERIALITE D'UNE CONTREFAÇON SUR INTERNET

L'article 1315 du Code civil fait peser la charge de la preuve sur le demandeur. En vertu de ce principe fondamental, le juge attend que celui qui intente une action en justice lui apporte la preuve de l'infraction alléguée.

Plusieurs décisions récentes sont venues rappeler que la preuve d'une infraction sur internet, qu'il s'agisse d'une contrefaçon ou encore d'un délit de presse (injure ou diffamation), n'est pas une preuve comme les autres.

Même si la preuve d'un fait juridique (événement susceptible de produire des effets juridiques) peut se faire par tous moyens en vertu de l'article 1348 du Code civil, le juge n'accepte, en effet, pas tous les moyens de preuve qui lui sont présentés quand il s'agit d'une infraction commise sur internet.

Ces moyens de preuve doivent respecter un certain nombre d'exigences pour pouvoir prétendre à une valeur probante aux yeux des juges.

Depuis plusieurs années, il est, en effet, établi que faire constater une infraction sur internet se doit de respecter un formalisme des plus stricts. Le juge impose à l'huissier ou encore à l'Agence de protection des programmes[13] qui se charge du constat, de respecter un certain nombre d'étapes lors son établissement.

Il devra notamment :

- Décrire le matériel grâce auquel le constat est établi (configuration technique)
- Effacer l'historique, les cookies, les répertoires de la mémoire cache de l'ordinateur avant de procéder au cheminement lui permettant d'accéder à la page internet litigieuse.

[13] Même si l'Agence de Protection des Programmes (APP) dispose d'agents assermentés qui ont autorité pour constater la preuve de la matérialité de toute infraction relative à un droit d'auteur, à un droit sur un logiciel, sur la base de données, ou à un droit relatif à un artiste interprète, l'infraction sur internet est souvent constatée par un procès verbal dressé par un huissier de justice.

La Cour d'Appel de Paris, dans un arrêt du 17 novembre 2006, a refusé d'admettre comme preuve un constat d'huissier au motif que l'huissier n'avait pas vidé les caches contenus dans la mémoire du serveur proxy, service offert par le fournisseur d'accès.[14]

- Inscrire le numéro IP de la machine ayant servi à dresser le constat sur son procès verbal dans le but de permettre en cas de contestation « *de vérifier au moyen du journal de connexion du serveur interrogé les pages réellement consultées pendant les opérations de constat* ».[15]
- Décrire le cheminement qu'il a lui-même effectué pour accéder à la page internet contenant l'infraction. Le constat doit « *établir l'existence de liens hypertextes* » dans le but de s'assurer que le cheminement doit pouvoir être effectué par n'importe quel internaute « *sans connaissance de l'organisation du site* ».[16]
- Matérialiser la page internet contenant l'infraction en l'imprimant puis en l'annexant au procès-verbal.

Un jugement du Tribunal de Grande Instance de Mulhouse en date du 7 février 2007[17] a retenu que « *le fait de ne pas avoir cliqué sur le lien et imprimé la page du site rend cette recherche sur internet incomplète et ne permet pas d'apprécier la réalité des griefs invoqués* ».

Toutes ces décisions rappellent l'importance pour le demandeur de disposer d'une preuve respectant des règles strictes et non pas de simples copies d'écran établies par lui-même dans des conditions inconnues, faute de quoi il prendrait le risque de ne pas voir l'action qu'il engagera couronnée de succès.

MYTHE N°2 :
DANS L'HYPOTHESE OU LES INFRACTIONS AURAIENT ETE SUPPRIMEES DU SITE PAR SON EDITEUR, UN SITE D'ARCHIVAGES DE PAGES WEB PERMET DE PALLIER L'ABSENCE DE PREUVE

Parce que les informations disponibles sur internet peuvent être rapidement modifiées et que la preuve de leur présence avant cette modification est souvent difficile à établir, de nombreux contentieux ont vu apparaître des constats internet au sein desquels figuraient des copies de pages de site d'archivages, comme celui du site internet www.archive.org.

Ce type de site permettant d'avoir une représentation « fidèle » de tout ou partie d'un site internet tel qu'il était plusieurs mois, voire plusieurs années auparavant, nombreux sont les demandeurs qui ont tenté de contourner la difficulté de l'absence de preuves « actuelles », en faisant constater par un huissier, la présence de l'infraction sur le site litigieux (par l'entremise du site d'archivage) à une date antérieure à la supposée modification.

La question s'est néanmoins très vite posée de la valeur probante des pages internet constatées par le biais de ce site d'archivage.

La Cour d'Appel de Paris a récemment eu l'occasion de se prononcer sur ce point.

Dans un arrêt en date du 2 juillet 2010, les juges ont retenu qu'aucune force probante ne pouvait être reconnue audit constat, quant au contenu, pendant la période au cours de

[14] *CA Paris, 4è ch., B. 17 nov. 2006, SARL Net Ultra c/AOL, RLDI 2006/22, n°706, obs/ Auroux J.B.*

[15] Tribunal de Grande Instance de Paris, 3ème chambre, 1ère section, Jugement du 4 mars 2003.

[16] Tribunal de Grande Instance de Paris, 3ème chambre, 1ère section, Jugement du 4 mars 2003.

[17] TGI Mulhouse, 1re ch., 7 février 2007, Ste Groupe Bosc c/St MMT

laquelle les actes de contrefaçon auraient été commis au motif que « *le constat a été effectué à partir d'un site d'archivage exploité par un tiers à la procédure, qui est une personne privée sans autorité légale, dont les conditions de fonctionnement sont ignorées* » avant d'ajouter que « *cet outil de recherches n'est pas conçu pour une utilisation légale* » et que « *l'absence de toute interférence dans le cheminement donnant accès aux pages incriminées n'était donc pas garantie* ».

MYTHE N°3 :
LE SEUL MOYEN DE LUTTER EFFICACEMENT CONTRE UN CYBERSQUATTEUR ET DE RECUPERER SON NOM DE DOMAINE CONSISTE A ENGAGER CONTRE LUI UNE ACTION DEVANT LES TRIBUNAUX

Le cybersquatting se définit comme le fait pour une personne d'usurper le signe distinctif d'autrui en l'enregistrant en tant que nom de domaine.

Cette pratique qui existe depuis plus d'une dizaine d'années a évolué au cours du temps.

Ce fléau mondial est désormais combattu en France tant par la voie judiciaire (référé, action au fond) que par la voie de l'arbitrage (procédure UDRP[18], ADR[19], CERDP[20] DCDRP[21], STOP[22], IPDRCP[23], PARL[24], PREDEC[25] et de la médiation.[26]

Les signes distinctifs auxquels il est fréquemment porté atteinte, par le biais d'une réservation de nom de domaine, sont notamment la marque, le nom commercial, la dénomination sociale, l'enseigne, le nom patronymique ou le nom d'une collectivité territoriale.

En France, il est établi que les procédures de référé ne peuvent aboutir, eu égard aux pouvoirs du juge des référés, à un transfert du nom de domaine au bénéfice du requérant. Un arrêt dit Sunshine (Cass. com., 9 juin 2009, n°08-12-904) est, en effet, venu préciser que le transfert d'un nom de domaine ordonné par ledit juge « ne constituait ni une mesure conservatoire, ni une mesure de remise en état » au sens de l'article 809, alinéa 1er du Code de

[18] Uniform Domain Name Dispute Resolution Policy pour les extensions en .com, .net et .org et pour les litiges opposant des noms de domaine et des marques.

[19] Alternative Dispute Resolution pour les extensions en .eu.

[20] Charter Eligibility Dispute Resolution Policy pour les extensions en .aero, .coop et .museum.

[21] DotCoop Dispute Resolution Policy pour l'extension en .coop

[22] *Star-up Trademark Opposition Policy pour l'extension en .biz.*

[23] *pour l'extension en .pro*

[24] Procédure alternative de résolutions des litiges adaptée aux extensions .fr et .re.

[25] Procédure de Règlement de Résolutions des cas de violations manifestes des dispositions du Décret du 6 février 2007.

[26] Pour ce qui concerne le .fr et le .re, l'AFNIC (Association Française pour le nommage Internet en Coopération) délègue au Forum des Droits sur l'Internet, par l'intermédiaire du service mediateurdunet.fr, le règlement extrajudiciaire de litiges entre deux particuliers ou entre un particulier et une entreprise.

procédure civile. Il sera néanmoins possible d'obtenir le gel ou le blocage du nom de domaine dans le cadre d'une action devant le juge des référés.

Il faudra donc, pour obtenir le transfert du nom de domaine, engager une action au fond devant les tribunaux. Il est utile de rappeler que les procédures UDRP ou PARL aboutissent à ce même transfert dans un délai qui excède rarement les quatre mois suivant la saisine.

L'inconvénient principal de ces procédures dites UDRP tient dans le fait qu'elles ne possèdent aucun caractère dissuasif. Même si le transfert du nom de domaine litigieux est ordonné, la décision ne sera pas accompagnée de dommages-intérêts ni même du remboursement des frais de procédure engagés par le demandeur à la charge du défendeur, lesquels restent l'apanage des décisions de justice qui suivent les actions en référé ou au fond engagés devant les tribunaux.

Il convient donc de bien peser le pour et le contre avant de décider de la stratégie à adopter pour faire cesser définitivement un trouble lié à la reprise, par un individu lambda ou par un concurrent, de son signe distinctif dans un nom de domaine.

MYTHE N°4 :

QUAND IL EXISTE UN CONFLIT ENTRE UNE MARQUE ET UN NOM DE DOMAINE ENREGISTRE POSTERIEUREMENT A CETTE MARQUE, IL SUFFIT QUE LE NOM DE DOMAINE SOIT IDENTIQUE OU SIMILAIRE A LA MARQUE POUR QUE LA CONTREFAÇON DE MARQUE SOIT ETABLIE

Quand il existe un conflit entre une marque et un nom de domaine enregistré postérieurement à cette marque, on estime désormais que pour qu'il y ait contrefaçon, il faut un acte consistant à utiliser un signe identique ou similaire pour désigner des produits identiques ou similaires.

La règle de la spécialité, qui existe en matière de marques, a été transposée aux noms de domaine.

Il faut savoir que les juges ont un temps retenu la contrefaçon de marque selon une méthode différente d'identification de la spécialité du nom de domaine. Ils considéraient, en effet, que les noms de domaine avaient pour spécialité les services de communication par réseau informatique (services de communication en ligne ou services assimilés) prévus dans la classe 38 de la classification de Nice.

Ce raisonnement avait pour conséquence de ne pas reconnaître la contrefaçon alors même que les services proposés par le site étaient de la même spécialité que la marque contrefaite, faute pour le titulaire de la marque d'avoir visé dans son dépôt le « service de communication » en ligne de la classe 38.

Inversement, quand la marque visait expressément le « service de communication en ligne » de la classe précitée, les juges retenaient la contrefaçon alors que le site internet utilisant le nom de domaine exploitait des produits ou des services différents.

Un important arrêt dit Locatour (Cass. Com. 13 décembre 2005) est venu préciser clarifier la situation en indiquant qu' : « *Attendu qu'un nom de domaine ne peut contrefaire par reproduction ou par imitation une marque antérieure, peu important que celle-ci soit déposée en classe 38, pour désigner des services de communication télématique, que si les produits et services offerts sur ce site sont soit identiques, soit similaires à ceux visés dans l'enregistrement de la marque et de nature à entraîner un risque de confusion dans l'esprit du public* ».

Il convient désormais se déterminer par rapport aux produits ou services proposés par le site du nom de domaine, et non par référence automatique à la classe 38 pour les noms de domaines.

La spécialité du nom de domaine, en cas de conflit avec une marque, sera liée à la spécialité du site auquel il renvoie.

MYTHE N°5 :
EN CAS DE CONFLIT ENTRE DEUX TITULAIRES DE NOMS DE DOMAINES IDENTIQUES OU SIMILAIRES, L'ANTERIORITE SE DEDUIT DE LA DATE D'ENREGISTREMENT DU NOM DE DOMAINE

Faux : en cas de conflit entre deux noms de domaines, c'est la date de commencement d'exploitation des noms de domaines et non la date d'enregistrement de ces derniers qui compte.

En pratique, cela signifie que le titulaire d'un nom de domaine, qui ne l'aurait pas utilisé pour un site internet, ne pourra pas se prévaloir d'une antériorité valable et d'une action pertinente en concurrence déloyale pour cybersquatting à l'égard d'un réservataire postérieure qui aurait exploité, avant lui, un nom de domaine identique ou similaire dans le cadre d'un site internet.

MYTHE N°6 :
UTILISER UNE PHOTO, UN DESSIN OU L'ŒUVRE D'UN TIERS SANS SON AUTORISATION POUR ILLUSTRER UN BLOG OU UN SITE PERSONNEL N'EST PAS CONDAMNABLE

À l'heure du web 2.0, il devient toujours plus facile de créer un site internet, notamment via l'émergence de blogs tels que wordpress. La tentation est donc assez forte pour les utilisateurs de ces plates-formes d'utiliser des contenus qu'ils ont piochés çà et là sur la toile afin d'illustrer leurs sites.

Ces choix ne sont cependant toujours pas sans conséquence. En effet, un créateur de site web ou un particulier peut être tenté d'utiliser une œuvre sans autorisation en minimisant volontairement l'importance que cet emprunt pourrait avoir sur la suite.

Rappelons à ce propos que la mise en ligne d'une création littéraire ou artistique, quelle qu'elle soit, correspond à un acte de représentation et que le droit commun de la propriété littéraire et artistique s'applique de manière classique à internet.

L'article L. 122-1 du Code de la propriété intellectuelle prévoit en effet que « le droit d'exploitation appartenant à l'auteur comprend le droit de représentation et le droit de reproduction ». Ce sont ces droits lui permettent de tirer profit de l'exploitation de son œuvre.

L'article L. 122-4 du CPI précise que « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants illicite » tandis que l'article L. 335-3 du CPI ajoute qu' « *est (…) un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur* ».

En vertu de ces articles, un auteur peut donc agir contre un créateur de site web ou un simple particulier pour avoir reproduit ou représenté son œuvre sur son site internet sans autorisation et réclamé des dommages-intérêts pour contrefaçon de droit d'auteur au titre du préjudice tant moral que patrimonial qu'il a subi.

Les tribunaux ont été amenés à sanctionner, à plusieurs reprises, des personnes qui avaient, sans autorisation, diffusé des œuvres artistiques sur leur site internet.

Même si dans la pratique, les internautes ne sont pas systématiquement poursuivis pour avoir reproduit une œuvre sans en avoir préalablement demandé l'autorisation à son auteur, le risque encouru mérite qu'il soit également rappelé que les conditions d'utilisation de l'œuvre,

en l'occurrence pour un site à but non-lucratif, n'empêchent en rien que l'atteinte soit constituée.

MYTHE N°7 :

EN CAS DE CONTREFAÇON DE PRODUITS SUR UN SITE E-COMMERCE QUI LES LIVRE A SES CLIENTS A TRAVERS PLUSIEURS PAYS DU MONDE, LE DEMANDEUR PEUT OBTENIR LA REPARATION DU PREJUDICE MONDIAL SUBI EN SAISISSANT LA JURIDICTION FRANÇAISE.

Malgré le fait que le site internet soit disponible depuis n'importe quel pays du monde, le juge français, notamment en matière de contrefaçon, n'est compétent que pour réparer les préjudices subis sur le territoire français.

En France, l'article 46 du Code de Procédure Civile précise que le demandeur peut saisir à son choix, outre la juridiction du lieu où demeure le défendeur (article 42 du Code de Procédure civile) :

- en matière contractuelle, la juridiction du lieu de la livraison effective de la chose ou du lieu de l'exécution de la prestation de service ;
- en matière délictuelle, la juridiction du lieu du fait dommageable ou celle dans le ressort de laquelle le dommage a été subi ;

La contrefaçon étant un délit, le demandeur devra démontrer que le produit a bien été vendu en France pour que le juge français puisse s'estimer compétent.

CONCLUSION :

Ces quelques exemples illustrent l'importance pour le demandeur de bien cerner les enjeux légaux et procéduraux avant d'intenter une action en justice dont l'objectif sera de voir réparé le préjudice subi par la contrefaçon commise sur Internet.

MYTHES ET LEGENDES DU CORRESPONDANT INFORMATIQUE ET LIBERTES

Bruno Rasle
Délégué général de l'AFCDP

Le 6 août 2004, à l'occasion de la transposition de la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, la France s'est dotée d'un dispositif qui dispense de l'obligation de déclaration auprès de la CNIL les responsables de traitements qui ont procédé à la désignation d'un «*détaché à la protection des données à caractère personnel* ».

Cette personne – plus connue sous le nom de CIL (pour Correspondant Informatique & Libertés) – est « *chargée d'assurer, d'une manière indépendante, l'application interne des dispositions nationales* » et « *de tenir un registre des traitements […] garantissant de la sorte que les traitements ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées* ». La fonction a été définie par le décret n°2005-1309 du 20 octobre 2005. Toutes les entités procédant au traitement automatisé de données à caractère personnel sont concernées quelque soit leur secteur, leur statut ou leur taille.

Issue largement d'une pratique allemande, cette mesure a été introduite dans la Loi dite « Informatique et Libertés » sur l'initiative d'Alex Türk, sénateur du Nord et Président de la CNIL. Cette fonction de « délégué à la protection des données à caractère personnel » a été transposée chez plusieurs de nos voisins : Allemagne, Estonie, Luxembourg, Hongrie, Pays-Bas, Slovaquie et Suède.

Le Correspondant Informatique et Libertés a vocation à être un interlocuteur spécialisé en matière de protection de données à caractère personnel, tant pour le responsable des traitements, que dans les rapports de ce dernier avec la CNIL. Le CIL occupe ainsi une place centrale dans le développement maîtrisé des nouvelles technologies de l'information et de la communication.

Au-delà du simple allègement de formalités, le Correspondant à un rôle primordial à jouer pour s'assurer que l'informatique se développera sans danger pour les droits des usagers, des clients et des salariés. C'est aussi pour les responsables des fichiers le moyen de se garantir de nombreux risques vis-à-vis de l'application du droit en vigueur.

Au sens strict de la nouvelle loi et de son décret d'application relatif au correspondant, les missions de ce dernier sont de tenir la liste des traitements et de veiller à l'application de la loi. Mais d'autres missions peuvent être confiées au Correspondant, comme la préparation des demandes d'autorisation, l'élaboration d'une politique de protection des données à caractère personnel, la sensibilisation du personnel aux dispositions de la loi, l'extension de la tenue de la liste aux traitements non dispensés ou encore le contrôle de l'application des règles prédéfinies.

MYTHE N°1 :
LE CORRESPONDANT INFORMATIQUE ET LIBERTES (OU CIL) EST LE REPRESENTANT DE LA CNIL AU SEIN DE L'ORGANISATION QUI L'A DESIGNE.

Le CIL est le plus souvent un collaborateur de l'entité (entreprise, association, collectivité, etc.), recruté spécialement ou désigné parmi le personnel. Bien qu'il soit effectivement l'interlocuteur privilégié de la Commission Nationale Informatique et des Libertés, il n'est en

rien son représentant. Il est financièrement à la charge de l'entité qui l'a désigné et conseille dans ses choix le responsable de traitement au regard de la conformité à la loi Informatique et Libertés et du droit des personnes concernant leurs données à caractère personnel.

Le CIL doit particulièrement veiller à ne pas apparaître comme un *Mister No*, évoquant à la moindre dérive les risques juridiques qui pèsent sur le responsable de traitement. Il doit s'imprégner des objectifs opérationnels poursuivis par les directions métier et – dans la limite de ce que permet le cadre légal – porter conseil pour trouver les équilibres adéquats.

MYTHE N°2 :
LE CORRESPONDANT INFORMATIQUE ET LIBERTES EST NECESSAIREMENT UN EMPLOYE DE L'ORGANISATION.

Dans une limite précisée par le décret d'application n°2005-1309 du 20 octobre 2005 (dans son article 44), certaines entités peuvent désigner une personne étrangère à leur personnel. Lorsque moins de cinquante personnes participent à la mise en œuvre du traitement ou y ont directement accès, l'organisme est libre de désigner un CIL externe. Il peut s'agir d'un consultant spécialisé, d'un avocat, d'un expert comptable, d'une société de conseil en informatique … pour autant que la personne dispose des compétences nécessaires. Sont comptabilisées pour pouvoir procéder ainsi toutes les personnes chargées d'exploiter, de développer et d'assurer la maintenance de l'application, tous les utilisateurs chargés notamment de saisir les données ou de les consulter ainsi que toutes les personnes qui, en raison de leurs fonctions ou pour les besoins du service, accèdent aux données enregistrées.

Lorsque le seuil des cinquante personnes est dépassé, le recours à une personne externe est strictement encadré : le CIL peut être un salarié d'une des entités du groupe de sociétés auquel appartient l'organisme, un salarié du groupement d'intérêt économique dont est membre l'organisme, une personne mandatée à cet effet par un organisme professionnel, une personne mandatée à cet effet par un organisme regroupant des responsables de traitement d'un même secteur d'activité. On parle alors de CIL externe et de CIL mutualisé (comme au sein du Notariat, ou chez les huissiers).

A noter que, parmi les états membres qui ont opté pour la formule du Délégué à la protection des données personnelles, seule la France restreint le champ des possibles. Aucun de nos voisins n'impose un seuil, laissant le responsable de traitement prendre ses responsabilités en choisissant ce qui lui semble correspondre le mieux aux objectifs poursuivis.

MYTHE N°3 :
LE CIL ENDOSSE LES RESPONSABILITES PENALES QUI PESAIENT, AVANT SA DESIGNATION, SUR LE RESPONSABLE DE TRAITEMENT.

Le CIL n'est pas un paratonnerre. Son rôle est de conseiller le responsable de traitement sur les mesures à prendre pour respecter le droit et il n'y a pas de transfert de la responsabilité vers le CIL. Le responsable de traitement conserve la pleine et entière responsabilité vis-à-vis des traitements mis en œuvre et de leur conformité à la loi.

Pour autant on peut imaginer que la responsabilité propre du CIL pourrait être recherchée en cas de complicité d'infraction (par exemple s'il a connaissance d'une non-conformité grave au regard de la loi Informatique et Libertés, commise sciemment par le responsable de traitement ou ses commettants, mais qu'il ne la traite pas), voire de négligence patente.

Si le CIL ne peut être tenu pénalement responsable des manquements de son responsable de traitement, seuls ses propres manquements peuvent lui être imputables. En conclusion, le

risque de mise en cause de la responsabilité du CIL semble très faible, sans être pour autant inexistant.

MYTHE N°4 :
LE CORRESPONDANT INFORMATIQUE ET LIBERTES EST UN SALARIE PROTEGE.

C'est le cas en Allemagne mais pas en France, au sens où on l'entend pour des représentants du personnel ou des délégués syndicaux. Même si la loi Informatique et Libertés précise que le CIL ne peut faire l'objet de sanctions de l'employeur du fait de l'exercice de ses missions, il peut être déchargé en cas de manquements graves dûment constatés et qui lui sont directement imputables au titre de ses fonctions de CIL. Pour assurer l'effectivité de cette protection, la CNIL doit être avertie de toute modification affectant sa fonction.

La décharge du CIL peut être initiée par la CNIL, lorsqu'un manquement grave aux devoirs de ses missions est directement imputable au Correspondant. Après avoir recueilli les observations de ce dernier, la Commission Nationale Informatique et des Libertés peut demander au responsable des traitements de relever le CIL de ses fonctions.

La décharge du CIL à la demande du responsable de traitement ne peut être envisagée qu'en raison de manquements à l'exécution de sa mission par le CIL : Le responsable des traitements doit saisir la CNIL pour avis et informer son Correspondant en même temps, afin que celui-ci puisse présenter ses observations. Les manquements invoqués doivent être directement imputables au Correspondant et relever directement de l'exercice de ses missions telles que définies dans la désignation notifiée à la CNIL.

La CNIL fait alors connaître son avis dans le délai d'un mois.

Ce n'est qu'une fois le CIL mis en mesure d'exposer son point de vue et à l'expiration du délai que la décision de le décharger peut être prise par le responsable des traitements. Pour continuer à bénéficier de la dispense de déclaration, le responsable de traitement doit notifier à la CNIL les coordonnées et fonctions de son nouveau Correspondant. A défaut, le responsable de traitement devra déclarer l'ensemble des traitements exonérés.

MYTHE N°5 :
LE CIL A UNE OBLIGATION DE DENONCER SON EMPLOYEUR OU CLIENT A LA CNIL S'IL CONSTATE DES IRREGULARITES.

Dans son article 49, le décret n°2005-1309 du 20 octobre 2005 dispose que le CIL « *informe le responsable des traitements des manquements constatés avant toute saisine de la Commission nationale de l'informatique et des libertés* ». *L'article 51 précise que « La Commission nationale de l'informatique et des libertés peut être saisie à tout moment par le correspondant à la protection des données à caractère personnel ou le responsable des traitements de toute difficulté rencontrée à l'occasion de l'exercice des missions du correspondant. L'auteur de la saisine doit justifier qu'il en a préalablement informé, selon le cas, le correspondant ou le responsable des traitements* ».

Ce pouvoir de saisine doit donc être utilisé en dernier recours (une fois seulement que toutes les autres voies ont été exploitées, après que le Correspondant a effectué les démarches nécessaires auprès du responsable de traitements et que celles-ci sont demeurées infructueuses) et lorsque cela se justifie réellement, quand le CIL rencontre de notables difficultés dans l'exercice de ses missions, par exemple en l'absence systématique de consultation avant la mise en œuvre de traitements sensibles, ou devant l'impossibilité d'exercer ses fonctions du fait de l'insuffisance des moyens alloués.

Avant d'utiliser ce pouvoir, le CIL et le Responsable de traitement peuvent s'entretenir avec la CNIL, notamment devant certaines difficultés d'application des dispositions législatives et réglementaires.

Si le Correspondant doit utiliser son pouvoir de saisine dans les cas extrêmes, il doit veiller également à ses propres intérêts, car nous avons vu que sa responsabilité propre pourrait être recherchée en cas de complicité d'infraction.

MYTHE N°6 :
SI LE RESPONSABLE DE TRAITEMENT DESIGNE UN CIL, IL EVITE LES CONTROLES SUR PLACE DE LA CNIL ET ECHAPPE A TOUTE SANCTION.

Des entités ayant désigné un CIL ont d'ores et déjà fait l'objet de contrôles sur place. Dans son rapport annuel pour l'année 2009, la CNIL indique même qu'elle compte profiter des prochains contrôles sur place qu'elle va effectuer pour « évaluer l'efficacité des CIL ». La désignation d'un Correspondant n'est donc pas un facteur direct permettant d'échapper aux contrôles et aux éventuelles sanctions. Par contre c'est indubitablement un facteur de réduction de l'exposition à ces risques.

De plus le CIL est à même de préparer son entité à faire l'objet d'une mission de contrôle de la CNIL. L'AFCDP, association qui représente les CIL, a publié un livre blanc qui permet de gérer une telle situation.

MYTHE N°7 :
SI LE RESPONSABLE DE TRAITEMENT DESIGNE UN CIL, IL N'A PLUS AUCUNE FORMALITE A EFFECTUER VIS-A-VIS DE LA CNIL.

Seuls les traitements de données à caractère personnels soumis au régime de la déclaration sont exonérés de formalité en cas de désignation d'un Correspondant Informatique et Libertés. Les traitements soumis à demande d'autorisation ne le sont pas.

Lors de la désignation de son CIL, le responsable de traitement doit indiquer s'il attend également de son Correspondant qu'il apporte son aide dans la préparation des demandes d'autorisation.

Enfin, même si le décret n°2005-1309 du 20 octobre 2005 n'oblige le CIL qu'à mettre dans son registre les traitements exonérés de déclaration, il est recommandé de garder sous son « radar » les traitements bénéficiant de dispense, ne serait-ce que pour vérifier qu'ils restent bien sous ce périmètre.

MYTHE N°8 :
LE CIL EST FORCEMENT UN JURISTE.

Clarifions immédiatement un point : il n'existe pas de « profil » idéal du candidat CIL. Les correspondants actuels viennent d'horizons très divers : informatique, juridique, qualité, contrôle interne, audit, record management, etc.

Actuellement, aucun agrément n'est demandé, aucune exigence de diplôme n'est fixée, la loi prévoit que le Correspondant est « *une personne bénéficiant des qualifications requises pour exercer ses missions* » : l'une des priorités d'un nouveau CIL est donc de compléter ses connaissances.

Les compétences et qualifications du CIL doivent porter tant sur la législation relative à la protection des données à caractère personnel (Informatique & Libertés, LCEN, Code du travail, etc.) que sur l'informatique et les standards technologiques (cybersurveillance, géolocalisation, biométrie, chiffrement, cookie, etc.), sans oublier le domaine d'activité propre du responsable des traitements.

Le Correspondant doit également avoir connaissance des législations particulières au secteur d'activité concerné (commerce électronique, marketing direct, assurances, collectivités territoriales ...) et des règles spécifiques au traitement de certaines données (données

couvertes par exemple par le secret médical ou le secret bancaire). Le CIL doit aussi avoir ou acquérir des compétences en conseil et management pour pouvoir assurer pleinement son rôle d'information et d'audit.

Une qualité est souvent oubliée, celle de communiquant, car il faut garder à l'esprit le facteur organisationnel et humain. Afin de diffuser une culture de protection des données, le CIL doit savoir écouter, sensibiliser, et favoriser les remontées d'informations : Il sera aussi amené dans l'exercice de ses fonctions à permettre un dialogue entre le responsable du traitement, les personnes faisant l'objet du traitement, et la CNIL.

MYTHE N°9 :
LE CIL EST FORCEMENT UN INFORMATICIEN.

D'après les sondages effectués par l'AFCDP auprès de ses membres et les informations divulguées par la CNIL, les informaticiens viennent en première position : plus du tiers des CIL sont de profil informatique (principalement Chefs de projet, RSSI et DBA). La plus forte représentation s'observe au sein des collectivités territoriales et au sein des Universités, dont les CIL sont à plus de 95% des informaticiens.

Mais une nouvelle fois, il n'existe pas de profil idéal pour cette fonction.

Le nom de la loi (Informatique et Libertés) a peut-être assimilé un peut vite, aux yeux des responsables de traitement, la fonction à la seule sphère du système d'information ? Il convient de ne pas oublier que les fichiers sur support papier sont également concernés (comme ceux du périmètre Ressources humaines, par exemple), du moment qu'il existe un ordre permettant un tri ou une entrée sélective.

MYTHE N°10 :
NOUS N'AVONS PAS BESOIN D'UN CIL, NOUS AVONS DEJA UN RSSI.

Si le Responsable de la Sécurité des Systèmes d'Information est chargé de la protection des actifs immatériels de l'entreprise, la mission du CIL est centrée sur la conformité à la loi Informatique et Libertés. Outre le fait que son périmètre d'action est focalisé sur les données à caractère personnel, sa tâche ne se limite pas à s'assurer de leur bonne sécurité, mais s'étend à bien d'autres aspects : information des personnes, tenue du registre des traitements et publicité de celui-ci, organisation des processus de réception et de gestion des demandes de droits d'accès, vérification de l'adéquation des données collectées et de leur durée de conservation au regard de la finalité, etc. En ce qui concerne les données à caractère personnel, le *Privacy By Design* englobe le *Security by Design*.

Mais d'autres missions peuvent être confiées au Correspondant, comme la préparation des demandes d'autorisation de certains traitements auprès de la CNIL (notamment lors de flux transfrontières), l'élaboration d'une politique de protection des données à caractère personnel, la sensibilisation du personnel aux dispositions de la loi, l'extension de la tenue de la liste aux traitements non dispensés ou encore le contrôle de l'application des règles prédéfinies.

MYTHE N°11 :
IL EST IMPOSSIBLE D'ETRE CIL ET RSSI SIMULTANEMENT.

Observons pour commencer que de nombreux RSSI ont été désignés CIL.

Cette simultanéité de pose pas de problèmes particuliers, à réserves prêt. La première provient de l'article 46 du décret n°2005-1309 du 20 octobre 2005 qui précise que « *Le correspondant ne reçoit aucune instruction pour l'exercice de sa mission* » et que « *Les fonctions ou activités*

exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission ». Concernant spécifiquement les mesures de protection des données personnelles, il faut donc s'assurer qu'il n'y a pas un tel conflit : la même personne peut-elle bien, simultanément, être en charge de cette sécurisation et du contrôle de cette bonne sécurisation ?

La seconde réserve porte sur la délicate gestion des relations hiérarchiques. Le CIL exerce ses missions de manière indépendante, dispose d'une autonomie d'action reconnue par tous et est directement rattaché au responsable de traitement à qui il peut apporter conseils, recommandations et alertes si nécessaires. Ces particularités ne sont pas le fait de la plupart des RSSI qui, dans cette mission, rapporte à un supérieur hiérarchique qui n'est pas le responsable de traitement.

Si la fonction est dévolue à un autre professionnel que le RSSI, le CIL contribue à améliorer la politique de sécurité informatique de l'organisation : en cela CIL et RSSI sont des alliés objectifs et ont de nombreux points communs. Outre le fait qu'ils sont parfois perçus à tort comme des « improductifs » et des « empêcheurs de tourner en rond », ils éprouvent les mêmes difficultés pour être impliqués en amont (et non pas la veille de la mise en œuvre d'une nouvelle application), pour faire passer l'idée que « mieux vaut prévenir que guérir », pour sensibiliser utilisateurs et direction, pour faire appliquer les décisions, politiques, charte, et pour valoriser leurs actions (en l'absence d'incident, avions nous réellement besoin de faire des efforts ?).

Cette coopération (qui doit être élargie au *Risk Manager*, aux spécialistes de l'Intelligence économique et à ceux de la Conformité, de l'Audit et de la Déontologie) va se renforcer dans l'éventualité d'une future obligation de notifier les violations aux traitements de données à caractère personnel, envisagé dans le cadre de la révision de la Directive européenne 95/46 CE et à laquelle les Opérateurs et FAI sont tenus dans le cadre de la transposition du Paquet Telecom.

MYTHE N°12 :
IL N'Y A FINALEMENT PAS GRAND AVANTAGE A DESIGNER UN CIL

En matière de protection de données à caractère personnel, la loi, à elle seule, ne suffit pas. La fonction de Correspondant Informatique et Libertés, créée par le décret n°2005-1309 du 20 octobre 2005, est un élément clé de régulation, par la pratique.

Au-delà du simple allègement de formalités, le Correspondant à un rôle primordial à jouer pour s'assurer que l'informatique se développe sans danger pour les droits des usagers, des clients, des patients, des salariés, des citoyens. C'est aussi pour les responsables des traitements le moyen de se garantir de nombreux risques vis-à-vis de l'application du droit en vigueur.

Au sens le plus strict, la fonction de Correspondant exonère de l'obligation de déclaration préalable des traitements les plus courants. Une lecture superficielle de la loi pourrait laisser croire que l'unique portée de la désignation d'un correspondant serait de bénéficier de cet allègement des formalités déclaratives… ce qui représente une économie de quelques timbres.

Ce serait sous-estimer l'aide précieuse que le CIL apporte au responsable du traitement. C'est, pour ce dernier, le moyen de se garantir de nombreux risques vis-à-vis de l'application du droit en vigueur, d'autant que de lourdes sanctions sont encourues en cas de non-respect de ces obligations. Le Correspondant a donc un rôle de conseil et de suivi dans la légalité de déploiement des projets informatiques et, plus largement, de la gestion de données à caractère personnel. Il propose les solutions permettant de concilier protection des libertés

individuelles et intérêt légitime des professionnels. En l'absence de CIL, ces tâches sont souvent négligées alors qu'elles sont essentielles au regard de la protection des droits des personnes.

La désignation d'un Correspondant Informatique et Libertés contribue à réduire les coûts de gestion client (exercice du droit d'accès, gestion des litiges, rationalisation des traitements, suppression des données obsolètes) et permet de développer la collaboration et les synergies entre services (juridique, informatique, marketing, etc.). Enfin, pour les entreprises globales, la désignation d'un CIL s'impose face au *Chief Privacy Officer* des groupes multinationaux. En outre, la désignation d'un Correspondant Informatique et Libertés permet à une organisation de bénéficier d'une relation privilégiée avec la CNIL, qui a mis en place un service qui leur est entièrement consacré.

Le Correspondant, s'il est d'ores et déjà un personnage-clé dans le paysage de la protection des données personnelles, est amené à prendre de l'importance. De plus, que la fonction reste facultative ou qu'elle devienne obligatoire, comme c'est le cas en Allemagne, la désignation d'un CIL va immanquablement être perçue comme un label de qualité et de bonnes pratiques en ce qu'elle rassure le consommateur, l'usager, le collaborateur ou le citoyen : un élément à ne pas négliger quant il s'agit d'instaurer la confiance. Il ne faudrait pas paraître en retard par rapport à ses homologues, confrères et compétiteurs.

MYTHE N°13 : NOUS SOMMES FORCEMENT EN CONFORMITE CAR NOUS AVONS DESIGNE UN CIL

De la même façon qu'une entité qui n'a pas fait le choix de désigner un CIL peut parfaitement être en conformité avec la loi Informatique et Libertés, rien n'assure qu'un organisme qui a désigné un Correspondant Informatique et Libertés est en complète conformité. Encore faut-il que le CIL ait les qualités et connaissances nécessaires, encore faut-il lui donner les moyens de mener à bien ses missions.

Parmi les facteurs d'efficience, on peut citer : une désignation préparée en mode projet, un rattachement au Responsable du traitement ou *a minima* à une personne faisant partie de l'équipe de direction, une certaine « mise en scène » de la désignation pour bien montrer qu'une telle décision est un geste fort, une réelle affectation de moyens (temps alloué à la mission, budget, soutien, formation initiale, veille).

D'une façon générale il faut mieux considérer la conformité comme une démarche que comme un état : la désignation d'un CIL par le responsable de traitement n'est pas un aboutissement, mais bien le début de cette démarche.

CONCLUSION

En quelques années, le CIL s'est imposé comme un personnage-clé dans le paysage de la protection des données personnelles. Son absence ne veut pas dire que l'entité n'a pas déployé tous les efforts nécessaires pour être en conformité, mais la désignation d'un Correspondant rassure le consommateur, l'usager, le collaborateur, le patient ou le citoyen : un élément à ne pas négliger quant il s'agit d'instaurer la confiance.

De plus, que la fonction reste facultative ou qu'elle devienne obligatoire comme c'est déjà le cas en Allemagne et comme la proposition de loi Détraigne-Escoffier (votée au Sénat le 29 mars 2010) le prévoit, la désignation d'un CIL peut être perçue comme un label de qualité et de bonnes pratiques. Dans l'attente, le volontariat donne l'occasion à certaines entités de se démarquer.

La révision de la Directive européenne de 1995, qui a donné naissance à notre loi Informatique et Libertés actuelle et au CIL, est en marche, pour adapter le cadre légal aux

récents développements technologiques comme le *Cloud Computing*, les réseaux sociaux, les applications mobiles et la géolocalisation, le marketing comportemental, les puces RFID, la vidéoprotection, la biométrie ou les nanotechnologies. Dans sa communication du 4 novembre 2011 la Commission européenne introduit de nouvelles contraintes, comme l'*Accountability* (l'obligation, pour le Responsable de traitement de prouver qu'il a pris des mesures pour assurer la conformité), l'analyse d'impact et de risques en amont de tout projet manipulant des données personnelles, la notification des violations aux traitements de données à caractère personnelles, la mise en œuvre du concept de *Privacy By Design* et la désignation d'un délégué à la protection de ces mêmes données.

Pour s'y préparer, les professionnels concernés se sont regroupés au sein d'une association qui les représente, l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel), qui a déjà eu l'occasion de faire connaître ses positions et d'influer sur certaines orientations.

La fonction de correspondant doit être tirée vers le haut. Certains voient le CIL du futur comme un véritable « Commissaire aux données », ou « Commissaire Informatique et Libertés », par analogie avec les commissaires aux comptes. De toute façon, il faut avoir de l'ambition pour ce nouveau métier, passionnant, qui se fonde sur la primauté de la personne comme le dit l'article premier de la Loi Informatique et Libertés : « *L'informatique doit être au service de chaque citoyen […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

GLOSSAIRE

MYTHES ET LEGENDES DE L'INTERNET

ATM : Asynchronous Transfer Mode

ETSI : European Telecommunications Standards

ICANN : Internet Corporation for Assigned Names and Numbers

IETF : Internet Engineering Task Forc

IPsec : Internet Protocol Security

IPv6 : Internet Protocol version 6

ISO : International Organization for Standardization

NAT : Network Address Translation

P2P : Pair-to-Pair

RINA : Recursive Inter-Network Architecture

ToIP : Telephony on IP

UIT : Union internationale des télécommunications

MYTHES ET LEGENDES DE LA SECURITE DE L'INFORMATION

CERT : Computer Emergency Response Team

MYTHES ET LEGENDES DU CHIFFREMENT

3DES : Triple Data Encryption Standard

AES : Advanced Encryption Standard

RSA : Rivest Shamir Adleman, algorithme de cryptographie asymétrique du nom de ses inventeurs

MYTHES ET LEENDES DE LA SIGNATURE ELECTRONIQUE

MD5 : Message Digest 5, fonction de hachage

PIN : Personal Identification Number

SHA1,2,3 : Secure Hash Algorithm

MYTHES ET LEGENDES DE LA CERTIFICATION CRITERES COMMUNS

ANSSI : Agence nationale de la sécurité des systèmes d'information

EALn : Evaluation Assurance Level n

ITSEC : Information Technology Security Evaluation Criteria

VPN : Virtual Private Network

POUR ALLER PLUS LOIN DANS LA CONNAISSANCE DES TIC

Les contributeurs de cet ouvrage collectif ont également écrit, ou participé à l'écriture de livres dans leurs domaines d'expertises. Voici, sans être objectif, loin s'en faut, quelques uns de ces livres qui peuvent vous permettre d'aller plus loin dans la connaissance des TIC.

.

Christian Aghroum :

Auteur de :

- « Les mots pour comprendre la cybersécurité et profiter sereinement d'Internet », collection Dico Dékode, 2010, éditions Lignes de Repères.

Contributeur de :

- « Identification et surveillance des individus ». Editions de la Bibliothèque publique d'information (Centre Pompidou) Juin 2010
- « Cybercriminalité, une guerre perdue ? » Editions Choiseul « Sécurité Globale » Dossier numéro 6 - Hiver 2008
- « La criminalité numérique ».Editions INHES : « Les cahiers de la sécurité » Cahier numéro 6 – Octobre 2008
- « Cybercriminalité et cybersécurité en Europe ». Les Dossiers Européens n°14 April 2008
- « La lutte contre la contrefaçon, enjeux, nouveaux moyens d'action, guide pratique ». Editions du Ministère de l'Economie, Ministère du Budget 1995

Franck Franchin

Auteur de :

- « Le business de la cybercriminalité ». Collection Management et informatique. Editions Hermes Science.

Gérard Peliks

Auteur de :

- « Le World Wide Web*:* Création de serveurs sur Internet ». Éditions. Addison-Wesley France 1995

Contributeur dans les livres collectifs :

- « La sécurité à l'usage des décideurs ». Edition etna France – 2005
- « La sécurité à l'usage des PME et des TPE », collection Ténor – 2006
- « La Sécurité à l'usage des Collectivités locales et territoriales », Forum ATENA – 2009

Bruno Rasle

Co-auteur avec Frédéric Aoun de :

- « Halte au spam ». Editions Eyrolles – 2003

Yvon Rastetter

Auteur de :

- « Le logiciel libre dans les entreprises ». Editions Hermes – 2002
- « La fusion de la téléphonie dans l'internet ». Editions Hermes – 2005
- « Le logiciel libre dans la mondialisation ». Editions Hermes – 2006
- « Le logiciel libre dans les PME ». Editions 2008

Philippe Vacheyrout

Maitre d'œuvre pour :

- «Mediam » le site intranet de la branche maladie de la Sécurité Sociale www.mediam.ext.cnamts.fr/cgi-ameli/aurweb/ACI RCC/MULTI
- « Ameli » le site extranet de la branche maladie de la Sécurité Sociale www.ameli.fr/
- Pionnier de la carte Sésam Vitale www.sesam-vitale.fr/index.asp

Auteur de :

- Contribution de C@pucine.net au Sommet à Tunis 12/2005 www.capucine.net/article.php?id_article=8
- Contribution au Forum sur la Gouvernance de l'Internet à Genève 02/2006 www.capucine.net/article.php?id_article=10
- Charte du « Réseau de Confiance Numérique » Capucine.net *6 www.capucine.net/article.php?id_article=15

A PROPOS DES AUTEURS

Par ordre alphabétique :

Christian Aghroum est diplômé de l'Ecole Nationale Supérieure de la Police et titulaire d'un DESS en "politique et gestion de la sécurité". Responsable central de la sécurité des systèmes d'information de la Direction Centrale de la Police Judiciaire, il a dirigé durant quatre années l'OCLCTIC, l'office de lutte contre la cybercriminalité, jusqu'en juin 2010. Il a représenté la France dans des instances internationales et enseigné à l'ENSP, à l'ISEP et donné des conférences à l'ENA, l'ENM, l'IHEDN et l'INHES. Il vit dorénavant en Suisse où il exerce les fonctions de Chief Security Officer dans une grande entreprise internationale.

chrisagh (at) hotmail.fr

Eric BOURRE est ingénieur IAM au sein du Cyber Security Customer Solutions Centre de EADS où il travaille sur des sujets tels que la PKI, la fédération des identités ou encore le contrôle d'accès.

Diplômé de l'école nationale supérieure d'informatique et de mathématiques appliquées de Grenoble (ENSIMAG), il est également titulaire d'un master en cryptologie et sécurité des systèmes d'information.

eric.bourre (at) cassidian.com

Jean Pierre CABANEL est Professeur à l'Institut National Polytechnique (INP / ENSEEIHT) de Toulouse et membre du laboratoire IRIT (Institut de Recherche en Informatique de Toulouse), équipe Université. Il anime un groupe de recherche sur le futur des télécommunications. Ses travaux récents traitent de l'autonomie des vecteurs aériens et spatiaux.

Jean Pierre Cabanel est Docteur d'état de l'Université Paul Sabatier (Toulouse) en 1982. Il travaille en premier au sein du laboratoire IBM de Yorktown (USA), avant de retrouver les projets « pilotes » de l'INRIA dans le cadre du laboratoire de l'IRIT. Il anime avec le Professeur Guy Pujolle le « Working Group » 6.4 de l'IFIP sur les LAN et PABX et organise plusieurs congrès au sein de Sup Telecom. Paris.

Il travaille ensuite sur la problématique de la sécurité des systèmes de communication : PKI : Private Key Infrastructure, et TPC : Tierce Partie de Confiance.

jeanpierre.cabanel (at) free.fr

Jean Christophe ELINEAU est responsable informatique dans une mutuelle. Président du pôle Aquinetic (pôle Aquitain de compétences en Logiciels Libres) et des Rencontres Mondiales du Logiciel Libre 2008 (Mont de Marsan). Il a fondé en 2005, Landinux, le Groupe d'Utilisateurs de Logiciels Libres (G.U.L.L.) pour le département des Landes.

jc.elineau (at) aquinetic.org

Franck FRANCHIN, travaille à la Direction de la Sécurité Groupe de France Telecom. Spécialiste depuis 20 ans en architectures sécurisées de systèmes civils ou militaires et en cybercriminalité, il est ingénieur diplômé de Supélec et de l'ENSEEIHT et titulaire d'un MBA de l'ESCP. Il mène aussi des recherches sur la résilience des infrastructures vitales dans l'équipe de la Professeure Solange Ghernanouti-Hélie de la Faculté des Hautes Etudes Commerciales de l'Université de Lausanne :

franck.franchin (at) bbox.fr

David GROUT est responsable avant vente chez McAfee

Titulaire d'un master en Informatique eBusiness, il est également titulaire de plusieurs certifications comme CISSP, Comptia Security +.

Il est aujourd'hui à la tête d'une équipe de 5 personnes et gère l'ensemble du marché entreprise en France. Présent dans le domaine de la sécurité depuis plus de 7 ans il intervient aussi lors de séminaires ou de parutions dans la presse informatique :

David_Grout (at) McAfee.com

Daniel HAGIMONT est Professeur à l'Institut National Polytechnique (INP / ENSEEIHT) de Toulouse et membre du laboratoire IRIT (Institut de Recherche en Informatique de Toulouse), où il anime un groupe de recherche autour des systèmes d'exploitation, des systèmes répartis et des intergiciels. Ses travaux plus récents concernent les systèmes d'administration autonomes.

Daniel Hagimont a obtenu un doctorat de l'Institut National Polytechnique de Grenoble en 1993. Après une année postdoctorale à l'Université de Colombie Britannique (Vancouver) en 1994, il a rejoint l'INRIA en 1995 comme Chargé de Recherche. Il a ensuite pris ses fonctions de Professeur en 2005.

daniel.hagimont (at) enseeiht.fr

Bruno HAMON est fondateur et gérant de la société MIRCA, cabinet de conseil en sécurité du patrimoine informationnel.

Avant de créer sa première entreprise EXEDIS, qui a rejoint le Groupe LEXSI, il a travaillé dans de grands groupes (SAGEM, SIEMENS, ZIFF DAVIS). Il a participé au lancement du site RueduCommerce.com. Depuis 2005, il préside au sein de l'AFNOR le groupe de travail œuvrant sur les Plans de Continuité d'Activité.

Il est chargé de cours à l'ISEP (Institut Supérieur d'Electronique de Paris) où il enseigne auprès d'étudiants en MASTER. Avec 30 années d'expériences dans les NTIC, il participe à de nombreuses conférences.

bhamon (at) mirca.fr

Michel LANASPEZE est Directeur Marketing et Communication de Sophos pour l'Europe de l'Ouest.

Diplômé de Télécom Paris (ENST) et du MBA de l'INSEAD, il contribue depuis 1996 à l'élaboration et la diffusion de solutions de sécurité pour le Web et les réseaux au sein de Bull, Evidian, UBIqube puis Sophos, après avoir participé à la conception de solutions d'administration pour SITA/Equant et Atos Origin.

michel.lanaspeze (at) sophos.fr

Jean PAPADOPOULO, Ingénieur en automatismes de l'Institut Supérieur de Mécanique et d'Electricité à Sofia (Bulgarie) est titulaire d'un doctorat sur la conception de circuits séquentiels par ordinateur au CEA Saclay, obtenu à la Faculté de Paris. Il a développé une expertise en architecture et développement de systèmes informatiques de gestion ou scientifiques, microprocesseurs, systèmes d'exploitation, transactionnel et SGBD, calcul hautes performances, stockage, sécurité informatique, doublée d'une connaissance des mécanismes commerciaux, marketing et légaux dont dépend la profitabilité d'une ligne de produits. Il a été Conseiller Relations Industrielles au laboratoire PRiSM de l'Université de Versailles et Coordonnateur du projet ANR PARA (Parallélisme et Amélioration du Rendement des Applications).

jean.papadopoulo (at) gmail.com

Gérard PELIKS est expert sécurité dans le Cyber Security Customer Solutions Centre de EADS.

Il préside l'atelier sécurité de l'association Forum ATENA, participe à la commission sécurité des systèmes d'Information de l'AFNOR et anime un atelier sécurité dans le cadre du Cercle d'Intelligence Économique du Medef de l'Ouest Parisien. Il est membre de l'ARCSI et du Club R2GS.

Gérard Peliks est chargé de cours dans des écoles d'Ingénieurs, sur différentes facettes de la sécurité.

gerard.peliks (at) cassidian.com

Sadry PORLON est avocat au barreau de Paris

Docteur en droit, il est également chargé d'enseignements, au sein d'une école de commerce, notamment, en droit des médias et de la communication, en droit du commerce électronique et du multimédia ainsi qu'en droit des marques.

avocat (at) porlon.net

Philipe POUX est directeur au sein du cabinet Ellipsa

Spécialiste des nouvelles technologies et de la relation client, président de l'atelier Solutions Vocales de Forum Atena, fondateur des salons VocalExpo et MobilePaymentExpo, chargé de cours à l'Ecole Centrale d'Electronique.

philippe (at) vocalexpo.com

Bruno RASLE est Délégué général de l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel). Il a participé à la création de la première entité française dédiée à l'optimisation des réseaux et à la gestion des performances en environnement IP et s'est consacré ensuite à la protection des données stratégiques. Il a été membre du groupe de contact anti-spam mis en place par la DDM (Direction du Développement des Médias, services du Premier ministre). Bruno Rasle est Délégué Général de l'AFCDP (Association qui représente les CIL) et intervient dans le cadre du Mastère Spécialisé « *Management et Protection des Données à caractère personnel* » de l'ISEP (Institut Supérieur d'Electronique de Paris).

bruno.rasle (at) halte-au-spam.com

Yvon Rastteter est fondateur et gérant de la société Arts.Soft, start-up qui conduit des projets trans-disciplinaires dans lesquels coopèrent des artistes, des architectes, des spécialistes des TIC, des enseignants, des formateurs. Il a fait carrière dans de grandes entreprises en France et aux USA. Depuis 2009, il exerce une veille technologique sur le logiciel libre dans l'association Forum Atena.

rasteter (at) free.fr

Nicolas RUFF est chercheur au sein de la société EADS.

Il est l'auteur de nombreuses publications sur la sécurité des technologies Microsoft dans des revues spécialisées telles que MISC. Il dispense régulièrement des formations sur le sujet et participe à des conférences telles que SSTIC, les Microsoft TechDays ou la JSSI de l'OSSIR.

nicolas.ruff (at) eads.net

Philippe VACHEROUT est président de Capucine.net

Entré à la Cnamts en 1975, il est à l'initiative de la création des Centres de traitements électronique inter-caisses et des Centres de traitement informatique de Saint-Etienne, Troyes et Rouen.

La carte à puce citoyenne Capucine est une carte sans contacts, acoustique. Le son émis est différent à chaque fois, donc impossible à décrypter.

phvacheyrout (at) capucine.net