Plus cela change...

Pierre Vandevenne

DataRescue SA/NV
pierre@datarescue.com

Nous nous trouvons à un moment important dans l'histoire de l'informatique. Les réseaux domestiques deviennent plus variés, plus complexes et plus présents sur l'Internet que les réseaux professionnels d'il y a dix ans. Ces configurations placées entre les mains d'utilisateurs privés deviennent de plus en plus souvent des points d'entrées, directs ou indirects, dans les réseaux des sociétés qui les emploient.

Dans ce contexte, avant de faire le grand bond, où tout ou presque est ou sera connecté à tout ou n'importe quoi, le « Principe de Précaution » voudrait que l'aspect sécurité soit parfaitement maîtrisé. Ou alors, la perfection n'étant pas de ce monde, pouvons-nous peut-être espérer que si, la situation n'est pas idéale, nous avons quand même fait de grands progrès ? Et si le niveau global de sécurité n'avait pas augmenté, vers où nous dirigeons nous ? Commettons nous sans cesse les mêmes erreurs ?

Je souhaite, dans cet article, faire un état des lieux à la fois sérieux et taquin du monde de la sécurité informatique. J'espère vous distraire et, peut-être, susciter une réflexion sur les pratiques et les comportements, parfois automatiques, des professionnels de ce milieu. J'avoue d'emblée une double lâcheté. N'attendez pas de moi de révélations techniques fracassantes, qui permettraient aux censeurs de jouer des ciseaux avec le programme de cette conférence. C'est pourquoi les exemples que j'ai choisi pour illustrer cette présentation ne seront ni trop récents, ni trop controversés. En outre, en tant qu'acteur de ce marché, je dois bien sûr ménager mes clients, qui se trouvent fréquemment dans des camps opposés. Merci de votre compréhension.

Je tiens aussi à vous rassurer d'emblée sur un autre point : contrairement à telle solution finale ou tel système d'exploitation miracle, appelé à résoudre tous les problèmes de sécurité informatique, il n'y a aucun risque de voir les solutions que je propose vous conduire au chômage.

Commençons donc par la question évoquée ci-dessus, et voyons où elle nous mène.

Le niveau de sécurité informatique a-t-il augmenté ou diminué ? Afin de répondre à cette question, nous devons nous intéresser à la notion de mesure du niveau de la sécurité ou de l'insécurité informatique.

1 Mesurer la sécurité ?

Conscients de l'importance de la mesure du niveau de sécurité, de nombreux acteurs se sont attelés à la tâche complexe de la définition de méthodes de mesures. Le prestigieux NIST, par exemple, s'est fendu en 2003 d'un monumental

guide intitulé « Security Metrics Guide for Information Technology Systems »[1]. C'est méthodique et quantifié. C'est théorique et réfléchi. Malheureusement, c'est lourd à mettre en oeuvre : en d'autres termes, c'est un livre de chevet idéal si vous cherchez à occuper une armée de fonctionnaires ou, mieux encore, si vous êtes le consultant qui facture la mise en œuvre des vérifications périodiques qu'il suggère.

Ce document offre des conseils dont la pertinence ne peut que nous étourdir

> « *For example, if a security policy defines a specific password configuration, compliance with this policy could be determined by measuring the percent of passwords that are configured according to the policy.* »*(page 22)*

Au-delà du ridicule intrinsèque de cette phrase, on ne peut s'empêcher d'éprouver un certain sentiment de « déjà-vu ». Par exemple en 1991[2]... En informatique, nous disposons d'un terme plus sérieux pour parler de « déjà-vu », c'est le mot « Motif ». Il a l'avantage d'être très à la mode. Je vais en abuser.

Craquer des mots de passe, c'est un peu le pont-aux-ânes de la sécurité informatique : gratification rapide assurée. Combien d'entre nous ont imprimé de longues listes de comptes d'utilisateurs affligés de sésames vulnérables ? Combien d'entre nous sont repassés six mois plus tard pour suivre l'évolution de la situation ? Combien de réunions, de tours de tables et de factures ?

Combien se sont posé de meilleures questions ?

- Quel est le nombre de compromissions de systèmes dus à des mots de passe faibles ?
- Si, en informatique, on parle du même problème, en termes identiques, à 12 ans d'intervalle, est-on sur la bonne voie ?
- Quel est le rapport coût bénéfice de ce genre d'opération ?
- Que se passe-t-il vraiment, sous le capot ?

Imaginons par exemple que vous soyez responsable d'un grand hôpital. Administrateur modèle, conscient à la fois des besoins en confidentialité des professions que vous servez et des difficultés de gérer un groupe d'utilisateurs moins intéressés par la sécurité que par l'informatique, vous n'avez évidemment ni le temps, ni les moyens techniques de vérifier en profondeur les détails techniques de la solution que vous allez implémenter. Vous rechercherez une réponse dans la presse ou, éventuellement, parmi les produits « certifiés » utilisés par vos collègues. Votre choix pourrait - qui sait - se porter sur les produits de la société Bardon Data Systems. Bardon Data Systems[3] est une société dont les produits ont été récompensés par la presse, qui offre des interfaces sécurisées simplifiées qui remplacent l'interface classique de Windows. Ils ont reçu la prestigieuse approbation HIPAA (Healt Information Portability and Accountability Act), ce qui ne gache rien.. Surchargé, vous définirez une configuration de base,

[1] NIST Special Publication 800-55, Security Metrics Guide for Information Technology Systems, 2003

[2] Daniel V. Klein, *A Survey of, and Improvements to, Password Security.* Software Engineering Institute, Carnegie Mellon University, Pennsylvania. (February 22, 1991.)

[3] `http://www.bardon.com/`

achèterez votre WinU et distribuerez un mémo décrivant une bonne politique de mots de passe. De temps à autre, si vous êtes vraiment consciencieux, vous vérifierez ou ferez vérifier la compliance de vos utilisateurs.

Avec un peu de chance, vous pourrez rapidement présenter un rapport contenant de jolis graphes, similaires à cet exemple tiré de ce document du NIST et qui fait la fierté légitime de tout responsable sécurité qui se respecte. Oui mais...

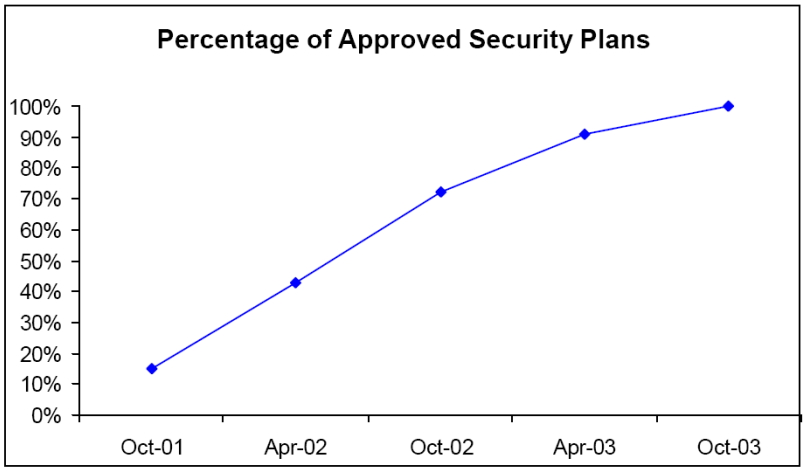

Figure 4-2. IT Security Metric Trend Example

Les « algorithmes » utilisés par Bardon Data Systems sont désastreux[4] : jusqu'à la version 5.0 de leur produit WinU, dont plusieurs centaines de milliers de licences ont été vendues, les mots de passe étaient chiffrés selon la méthode de substitution suivante...

154 – code ascii du caractère = caractère chiffré.

La version 5.1 de WinU a corrigé cette vulnérabilité en remplaçant l'algorithme ci-dessus par celui-ci

code ascii du caractère + 101 = caractère chiffré.

Est-ce une mauvaise blague ? Non, juste un exemple parmi des centaines, que je n'ai sélectionné que pour sa simplicité et son innocuité – il y a peu de chance qu'un représentant de la société Bardon Data Systems se trouve parmi nous aujourd'hui, m'assigne en justice pour avoir dénigré ses produits. C'est que la certification HIPAA est censée être sérieuse et que craquer ce genre de chose, en 2006, peut signifier une lourde amende ou même la prison.

[4] `http://www.securiteam.com/windowsntfocus/5HP0L152BA.html`

Quelle est l'utilité réelle, pour notre pauvre administrateur, de la vérification de la compliance à une politique de mot de passe si la « technologie » sous-jacente est si faible ? Nous rencontrons ici, d'un coup, 5 motifs

- L'utilisateur normal est incapable de juger de la validité de la technologie sous-jacente.
- La technologie sous-jacente, quelle que soit l'élégance avec laquelle elle a été emballée, craque « au niveau de l'octet », au plus bas niveau.
- Les sociétés commerciales qui ne sont pas soumises à un contrôle efficace sont fort tentées d'être incompétentes ou malhonnêtes.
- Les certifications sont peu fiables ; souvent en raison du manque de compétence des certificateurs.
- Les lois peuvent servir à empêcher l'expression des quatre motifs précédents.

Le cas, plus fameux, de Dmitry Sklyarov est, sous bien des aspects, similaire. Imaginons que notre administrateur, conscient des limites de sa politique de sécurisation, ait simplement souhaité sécuriser les documents les plus importants de ses utilisateurs. Parmi les produits qu'il pourrait avoir achetés, en les payants parfois très cher, on trouve des produits qui se contentent de boucles XOR avec la chaîne « encrypted », chiffrent tous les documents avec une clé unique ou encore stockent simplement la clé de chiffrement, en clair, dans le document lui-même[5]. Le problème est ancien et récurrent[6]. On pourrait résumer l'évolution de la façon suivante

Avant 2000 : beaucoup de programmes de « sécurité » sont faibles. En parler provoque une réaction embarrassée de l'éditeur qui assure avoir amélioré ses nouvelles versions.

Après 2000 : les programmes de sécurité restent faibles. Décrire leurs vulnérabilités suscite les premières réactions légales musclées. Prévoir un budget légal important. Compter sur le support de l'opinion publique.

En 2006 : dans le cadre légal actuel, démontrer la faiblesse d'un programme de « sécurité » est simplement devenu trop dangereux. On n'en parle donc plus. Gageons que d'éventuelles statistiques de solidité donneraient l'impression d'une nette amélioration des programmes...

Passons rapidement sur le reste du document du NIST, consacré en grande partie à des suggestions lourdes, voire impossibles à mettre en oeuvre, et qui ignorent complètement soit la réalité sous-jacente, soit la vitesse d'évolution des technologies.

La question initiale, qui concernait simplement la mesure de la sécurité, nous a vite conduit sur d'autres chemins intéressants.

2 Et les commerciaux dans tous cela ?

Certains d'entre-vous pensent peut-être que ce que nous venons d'entendre relève de la bureaucratie et qu'il vaut mieux se tourner vers le secteur privé, plus réactif et peut-être plus informé, pour obtenir une évaluation pertinente.

[5] `http://www.cs.cmu.edu/~dst/Adobe/Gallery/ds-defcon/sld001.htm`

[6] post personnel sur alt.security le 21 Mars 1997

2.1 Niveaux d'alertes

Il y a par exemple les niveaux d'alertes auxquels les éditeurs d'anti-virus nous ont habitué. Si l'on note une certaine responsabilisation à ce niveau – plus personne n'oserait en 2006 nous refaire le coup de « Michelangelo », « Hare Krishna », « Palm Trojan » (motif : honnêteté spontanée des sociétés commerciales...) - on a le droit de penser que ces codes colorés relèvent plus du marketing que de la statistique utile. De nos jours, un administrateur de serveur de courrier électronique tant soit peu fréquenté est, de toute façon, très rapidement au courant du niveau d'alerte qui le concerne. Passons.

3 Mesure Commerciale de Securité

Le « Security Metrics Consortium » lancé à grand renfort d'annonces de presse[7] au début de 2004 par la société Foundstone s'était donné le but louable de mettre de l'ordre au pays des « security metrics ». Il devait regrouper des CSO/CISO de premier plan et, enfin, répondre de façon indépendante et neutre

[7] `http://www.eweek.com/article2/02C18952C15384102C00.asp` et `http://www.foundstone.com/company/pressrelease_template.htm?indexid=115`

aux interrogations légitimes des responsables de la sécurité informatique. Le « Security Metrics Consortium » avait-il des réponses à nous apporter ? Nous ne le saurons malheureusement pas.

4 Statistiques d'incidents

Il est généralement admis, dans le monde de la sécurité informatique, qu'on ne peut se fier aux rapports d'accidents informatiques spontanément signalés par les sociétés qui en sont victimes. Les cadavres, au placard ! (motif : honnêteté des sociétés commerciales...)

C'est pourtant, effet secondaire inattendu de notre excursion dans les méthodes de mesure de la sécurité informatique, de ce côté que vient notre premier élément positif : une loi bien informée comme le **California Security Breach Information Act**[8] peut aider les sociétés commerciales à rester dans le droit chemin. C'est ainsi qu'on s'est aperçu que CardSystems[9], un centre d'autorisations de cartes de crédit majeur, n'utilisait aucun chiffrement pour ses communications sensibles. La loi les a forcés à révéler l'attaque dont ils avaient été victime mais aussi à préserver toute la documentation dont ils disposaient sur l'incident. Ils n'avaient « perdu » que les caractéristiques de 40 millions de cartes de crédits... Cette loi, qui engage clairement la responsabilité des sociétés commerciales, a suscité une réaction unanimement décrite comme salutaire. Nous y reviendrons.

5 Système D : le sondage

Une autre méthode d'estimation du niveau de sécurité informatique, c'est le sondage des professionnels. Qui pense que le niveau de sécurité informatique est meilleur aujourd'hui qu'il y a cinq ou dix ans ? Si vous pensez, comme moi, que la situation ne s'est pas améliorée, malgré les quelques 27 milliards de dollars dépensés en 2004 dans le secteur, (qui affiche des taux de croissance de 20% par an), il est légitime de se demander quelle malédiction frappe notre secteur, qui l'empêche d'afficher des progrès similaires, par exemple, à ceux de la sécurité routière.

Il y a malheureusement un ensemble de facteurs face auxquels nous sommes presque impuissants.

6 La prouvabilité des programmes

Les programmes ne sont pas prouvables. De façon générale et de façon particulière, quel que soit le niveau auquel l'on se place[10]. Une anecdote illustre

[8] California Security Breach Information Act (SB-1386)

[9] `http://www.computerworld.com/securitytopics/security/story/0,10801,102646,00.html`

[10] `http://www.acm.org/classics/sep95/`

l'ignorance de ces principes. Un soir de 2001, un de nos clients téléphone pour nous proposer une collaboration technique avec sa prestigieuse institution universitaire : son but est simple. Le marché est, en théorie, profitable aux deux parties.

« *Nous allons commencer par déterminer l'intention hostile d'un morceau arbitraire de code. Vous nous aidez techniquement à implémenter ces heuristiques sous forme de plugin pour votre produit* »

Nous rencontrons un nouveau motif du monde de la sécurité informatique - l'ignorance de principes théoriques fondamentaux – et un motif connu : l'ignorance pratique, de tous les petits détails qui, au niveau de l'octet, peuvent gâcher la fête.

Mon correspondant s'est étonné, offusqué même, de mon manque d'intérêt. En 2005, il travaillait toujours sur le problème et nous a offert une nouvelle collaboration, rémunérée cette fois, que nous avons refusé.

7 L'utilisation du C et du C++

On peut se demander quel serait l'aspect du paysage de la sécurité informatique si le C et le C++ n'avaient pas été inventés. Beaucoup de choses ont été écrites sur le sujet et sur les vulnérabilités associées à une certaine pratique de ces langages. Des efforts très importants ont été consentis et commencent à porter leurs fruits. Hélas, l'héritage est très lourd et c'est cette énorme quantité de code laissée en héritage qui continuera de poser problème.

8 La complexité croissante

L'immense diversité des applications et appareils déployés, la complexité sans cesse croissante des protocoles et des standards, restent évidemment des obstacles majeurs à l'amélioration du paysage sécuritaire. Il n'est pas possible d'être un hyper-spécialiste des algorithmes cryptographiques, de la rétro-ingéniérie de leurs implémentations, de TCP/IP, des détails de l'uPnP, la sécurisation d'un serveur Exchange, etc...

9 L'éducation de l'utilisateur

Nous savons aujourd'hui que l'éducation de l'utilisateur est une tâche insurmontable. Dans les domaines qui n'ont pas ou peu changé, tels la gestion des mots de passe, il est clair que les nombreuses campagnes d'éducation n'ont eu que peu d'effet. Dans les domaines très changeants, on a à peine terminé une explication qu'elle ne s'applique plus. (phishing, sécurité wireless)

Heureusement, certains des facteurs responsables de l'environnement précaire actuel sont à notre portée. Commençons par mettre de l'ordre dans notre propre jardin et penchons-nous sur l'attitude des chercheurs en sécurité informatique.

10 Le chercheur et le « Cool factor ».

L'utilisation par IBM de réseaux neuronaux pour la détection des virus de secteur de démarrage et la publication des résultats de cette recherche[11] dans la revue IEEE Expert reste pour moi un cas d'école

- le problème était d'une portée minime.
- les solutions existantes étaient suffisantes techniquement.
- des solutions non techniques raisonnables existaient.

Le monde de la sécurité informatique est plein d'individus talentueux et enthousiastes, qui s'amusent à inventer et cherchent, c'est bien naturel, à attirer l'attention. Le spectaculaire devance souvent l'outil. L'outil précède parfois le problème. C'est bien, mais ce n'est en général pas la solution optimale et cela gaspille le talent. Une approche plus méthodique, moins médiatique, comme celle de l'équipe du Wisconsin Safety Analyzer[12] devrait jouer le rôle de modèle. Essayons d'y penser chaque fois que nous apportons une solution très « Cool » à un problème de sécurité informatique.

11 Le chercheur et l'hypocrisie.

En 1996, le « Little Black Book of Computer Viruses » défrayait la chronique. A l'époque, l'aura « virus » était bien plus fort qu'aujourd'hui. Quand les bulgares ne jouaient pas du parapluie dans les rues de Londres, leurs méchants génies travaillaient à la perte du monde occidental.

The Bulgarian Dark Avenger writes viruses. Much like Hannibal Lecter, he is clever - and cunningly dangerous. (Sarah Gordon – IBM)

En 2006, un des livres de sécurité informatique les plus lu se consacre exclusivement à la construction de rootkits. Est-il vraiment nécessaire, dans ce genre d'ouvrage, d'expliquer au lecteur qu'il est intéressant de créer des sous-répertoires pour gérer des projets d'une certaine ampleur ? Guider pas à pas un public paresseux dans la réalisation d'outils dangereux est-il une attitude responsable à moyen ou long terme ? Question intéressante : pourquoi la justice, pourtant moins aggressive à l'époque, avait-elle souhaité interdire le « black book » alors que le livre consacré aux « rootkit » ne suscite aucune réaction ? (nouveau motif : les buts des sociétés commerciales ont-ils un impact sur la genèse et l'utilisation des lois ?)

12 Le chercheur et la technologie.

La technologie ne fonctionne pas ? Ajoutons de la technologie ! Une réaction bien naturelle, face à un problème technologique, est d'apporter une réponse technologique : le logiciel « **BlackIce** » fut un des premiers systèmes de pare-feu/IDS personnel. Malheureusement, Black Ice lui-même est devenu la source

[11] `http://www.research.ibm.com/antivirus/SciPapers/Tesauro/NeuralNets.html`
[12] `http://www.cs.wisc.edu/wisa/`

d'incidents[13] et, à l'autopsie, les utilisateurs qui ne l'ont pas installé mais qui lui ont préféré des mesures d'hygiène simple ont gagné au change. Au début des années 2000, la mode était à l'installation de doubles firewalls : CodeRed, imprévu, est tranquillement passé au travers des doubles configurations. Parfois, souvent, il faut simplifier. (motif : une vulnérabilité est corrigée par une nouvelle couche logicielle, elle-même vulnérable)

13 Le chercheur, l'attrait de la gloire et la confusion des termes.

Le « rootkit » de Sony est un cas d'école récent. Selon les définitions existantes avant l'incident, il ne s'agissait clairement pas d'un rootkit, mais bien d'une méthode de protection, malpolie, dangereuse, irritante comme on en trouve dans les jeux vidéos[14]. Mark Russinovich l'a initialement qualifiée de « rootkit like method ». Très vite, on a assisté à une dérive du sens des mots. On a résumé en « rootkit ». Sony passé en mode contrôle de dommage, a offert une méthode lourde et vulnérable de désinstallation. Bien entendu, un « chercheur » a montré la possibilité d'exploiter cette méthode de désinstallation, pour faire n'importe quoi, et éventuellement installer un virus. Le rootkit Sony qui n'en était pas un est devenu « le virus Sony »... Mais déjà, on commençait à parler du « rootkit Symantec »

Ces glissements de sens sont dangereux. Certes, prompts à susciter l'attention des médias et la mobilisation populaire, ils offrent l'illusion d'une victoire rapide sur une « méchante » société commerciale (motif : l'honnêteté spontanée des sociétés commerciales). Mais le KO ainsi obtenu n'est pas nécessairement suivi d'effets durables : Sony n'a pas vraiment retiré les disques protégés du marché. Ensuite, comme Symantec l'a appris, la dérive de sens peut avoir des effets de bord inattendus.

Enfin, ils contribuent, chez les décideurs qui n'ont ni le temps ni les moyens de creuser le sujet, à entretenir le climat de confusion qui aide à la genèse de mauvaises lois. L'avis de Schneier sur le sujet, que je ne partage pas mais qui est intéressant, illustre clairement la confusion et le malaise.[15]

L'important n'était pas de gifler Sony, l'important était de poser fondamentalement la question de ce que ces sociétés peuvent se permettre et, éventuellement, de légiférer. Une bonne loi comme le « California Security Breach Information Act », nous l'avons vu, peut responsabiliser les sociétés commerciales sans les étouffer.

L'appel de la gloire a entraîné une surenchère qui a rapidement masqué les vrais enjeux : nous avons manqué une opportunité. Ce n'est pas un cas isolé.

---

[13] `http://isc.sans.org/diary.php?date=2004-03-20`

[14] `http://www.bookofhook.com/Article/GameDevelopment/TheCopyProtectionDilemma.html`

[15] `http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html`

14 Le chercheur qui casse pour casser.

Gardons toujours à l'esprit qu'il est plus facile de casser un programme ou un système que de le construire. Cette vérité inévitable devrait inciter beaucoup d'entre-nous à un peu plus de mesure et de modestie. L'impression que le « super-hacker » médiatisé est plus fort que le pauvre programmeur anonyme est, dans la très vaste majorité des cas, totalement fausse. Ce distingo est évident pour les spécialistes, mais pas toujours pour les médias...

Quittons maintenant notre chercheur pour nous intéresser au rôle des sociétés commerciales...

15 Attitude des sociétés commerciales

Affirmons le sans hésiter : rien ne pousse la société commerciale à l'honnêteté spontanée. Croire que les lois du marché sont des moteurs puissants de vertu relève de la naïveté (SUV Ford, Vioxx, Cartes Bancaires...) ou du Bushianisme. L'attitude des sociétés de sécurité informatique ne fait pas exception à la règle : pour ces sociétés, l'unité de péché se mesure en octets ce qui permet de cacher des cimetières entiers dans de petits placards. De l'affaire Michelangelo aux affirmations qu'aucune exploitation des failles WMF n'était connue. De la vente de boucles XOR à cinq mille dollars en passant par les campagnes de pub carrément mensongères (Oracle[16], [17]) on pourrait facilement consacrer une conférence comme celle-ci à la liste de ces exactions.

Une bonne loi comme le « California Security Breach Information Act », nous l'avons vu, peut responsabiliser les sociétés commerciales et les inciter à améliorer leurs pratiques.

Une mauvaise loi, comme le sont des pans entiers du DMCA, est continuellement exploitée dans des actions en justice frivoles, pour réduire au silence la personne qui tire la sonnette d'alarme ou pour dissimuler l'incroyable faiblesse de certaines solutions de sécurité informatique.

Il devrait être possible de découvrir et dénoncer l'utilisation de XOR (ou ses variantes) dans les programmes commerciaux sans s'exposer à des poursuites coûteuses. Les sociétés commerciales devraient être freinées dans leur enthousiasme à se livrer à une publicité mensongère.

16 Cadre Légal - Experts indépendants.

Vous avez maintenant compris que je suis un fervent partisan des bonnes lois. Je ne suis pas le seul : l'opinion qu'il faut mettre de l'ordre dans ce « Far West » qu'est l'Internet est de plus en plus souvent entendue. Mais qu'est-ce qu'une bonne loi ? Il est évident qu'il ne m'appartient pas d'en définir les critères mais je suis autorisé à réfléchir.

[16] `http://www.oracle.com/oramag/oracle/02-mar/o22insight.html`
[17] `http://news.com.com/2061-10789_3-5808928.html`

A la racine d'une grande partie des problèmes de sécurité informatique, des pauvres méthodes de chiffrement de la société Bardon aux « rootkit Sony », il y a un ensemble de faits techniques de bas niveau auxquels le public (qui ne sait pas ce qu'est un rootkit – son éducation reste un mirage), la société commerciale (qui, à l'évidence, réagit avec incompétence), et le législateur (qui subit les pressions intéressées de nombreux groupes d'intérêts) ne comprennent pas grand-chose. Si cette ignorance a des aspects positifs puisqu'elle confère à nos connaissances l'utilité qui nous permet de gagner notre pain, elle ne me parait pas une fondation bien solide pour bâtir de bonnes lois.

On me répondra que les « experts » sont là pour éduquer le législateur et le juge, que c'est ce qui se passe dans d'autres disciplines. C'est vrai. Mais en sécurité informatique, un domaine en forte croissance où les salaires sont plus que corrects, l'expert indépendant compétent est un oiseau rare. Très rare.

On m'objectera que les procès dans le domaine médical peuvent aussi tourner à la bataille d'experts. C'est vrai. Mais, dans ce genre de procès, on ne se bat pas sur la définition du terme fibrillation ou sur la nature du paracetamol. Ces termes ont une acception claire. Des organismes de contrôle indépendants ont établi des définitions précises, des recommandations de traitement, etc... En informatique, un expert pourrait impunément prétendre qu'un pancréas fibrille ou que le paracétamol est une hormone stéroïdienne.

Le milieu de la sécurité informatique a besoin d'experts indépendants, en nombre suffisant pour couvrir les multiples facettes de la technologie. Le milieu de la sécurité informatique a besoin d'organismes indépendants, bien dotés, qui s'expriment clairement. Ces structures indépendantes doivent être utilisées pour responsabiliser, par l'intermédiaire de lois bien conçues, les sociétés commerciales qui fournissent des services et des produits informatiques.

Ces experts seraient immunisés contre le « cool factor », les retombées commerciales que la gloire éphémère pourrait apporter à leur employeur. Ils seraient bien formés et reconnaîtraient les motifs que nous avons évoqués au fil de cette présentation.

Pour améliorer fondamentalement la situation de la sécurité informatique, il faudra de bonnes lois.

Pour récolter de bonnes lois, il faut semer la compétence et l'indépendance.