

S curit  : La Cyberguerre, le retard fran ais !

S curit 

Post  par : JPilo

Publi e le : 19/9/2011 14:00:00

Aujourd hui l informatique est partout et les syst mes qui  contr lent nos moindres faits et gestes omnipr sents. L explosion des r seaux ne  concerne plus seulement les ordinateurs.

Elle touche   tous les aspects de la vie comme les  « objets  » embarqu s dans nos poches et demain probablement   les industriels y travaillent d j    les appareils m dicaux embarqu s communicants comme par exemple le pacemaker connectable   Internet.

C est une mutation sans pr c dent. La soci t  num rique est en marche et nul retour en arri re n est possible ni m me envisageable. La s curit  des infrastructures pose de ce fait un d fi majeur. Tant pour les Etats et les administrations que pour les entreprises. D autant que, quoiqu en disent les d cideurs, en particulier en France, les sp cialistes en s curit  sont devenus une denr e rare et courtis s au niveau mondial. Le retard de notre pays dans ce domaine est patent.



Prenons le secteur hautement strat gique qu est la D fense du pays.

Les besoins sont estim s   250 ing nieurs par an pendant 5 ans rien que pour le Minist re de la D fense, et l Agence Nationale de la S curit  des Syst mes d Information (ANSSI). 1 250 sp cialistes, c est bien plus que la capacit  actuelle de formation de l ensemble des  coles d informatique ! Or, cette situation de p nurie ne va pas s am liorer pour au moins deux raisons. La premi re tient   ce que d autres minist res, notamment le Minist re de la Sant , mais aussi des entreprises commencent   prendre s rieusement conscience de l enjeu de la s curit  informatique.

La seconde   l intrusion des grandes soci t s am ricaines, telles que Google, Apple , qui commencent   chasser et   piller des soci t s   on peut citer HSC Consulting ou Sogeti   incapables de rivaliser avec les salaires propos s. D o ¹ une h morragie inqui tante de ressources rares et tout cela dans un environnement o ¹ les attaques vont croissant et gagnent en sophistication. C est le cas, en particulier, depuis la fin de l ann e 2009. Elles ont vis  des Etats (Estonie, Zimbabwe, Iran, France ), des organismes supranationaux (OTAN, Communaut  Europ enne, organisation du G-20 ), des soci t s

importantes (Siemens, Maersk, MasterCard) et, pour certaines d'entre elles travaillant dans le domaine des hautes technologies liÃ©es Ã la sÃ©curitÃ© (RSA Labs, HB Gary, RealTek, Comodo). C'est bien de mettre de l'informatique et des rÃ©seaux partout (mÃame ils n'ont rien Ã faire) mais encore faut-il avoir des gens compÃ©tents et de confiance pour faire tourner tout cela.

Que faire pour pallier la pÃ©nurie et sÃ©curiser nos systÃmes d'information ?

En allant chercher les ressources il y en a. Chez les hackers qu'on a tendance Ã diaboliser il y a des excÃs. Pourquoi ? Parce qu'on ne les comprend pas. Il est donc essentiel de rappeler ce que le terme « hacker » recouvre. Contrairement Ã l'idÃe rÃeue et malheureusement vÃhiculÃe Ã surtout en Europe ce terme ne dÃsigne en aucun cas une personne dotÃe de mauvaises intentions, contrairement au pirate informatique. **Le terme de hacker dÃsigne toute personne capable d'analyser en profondeur un systÃme** que ce systÃme soit technique comme un ordinateur ou un tÃlÃphone, mais Ãgalement humain, social, lÃgislatif de sorte Ã en comprendre les mÃcanismes les plus intimes, en privilÃgiant le rÃsultat sur la mÃthode (contrairement souvent Ã l'approche acadÃmique).

Un hacker, par dÃfinition, n'hÃsite pas Ã s'Ãcarter de toute forme d'orthodoxie en particulier technique et scientifique pour parvenir Ã ses fins. C'est principalement ce trait de caractÃre qui gÃnÃralement couplÃ Ã un certain anticonformisme, un soupÃon d'autisme et d'esprit quelquefois pÃchu, Ã tort, comme asocial qui dans l'opinion gÃnÃrale fait du hacker une personne peu recommandable. C'est une profonde mÃconnaissance de ce qu'est le mouvement et l'esprit hacker.

Cette mÃconnaissance est toutefois Ã moduler selon les pays et les cultures.

Le monde anglo-saxon, contrairement au monde latin, a toujours manifestÃ un intÃrÃt pragmatique vis-Ã-vis des hackers. C'est Ãgalement le cas de l'Allemagne qui a, depuis les annÃes 80, su intelligemment appuyer sur la communautÃ des hackers allemands et qui, dans le domaine de l'informatique, a su mieux ou moins mal anticiper la pÃnurie gravissime qui s'annonce. Mais ils ont su aussi ne pas sacrifier Ã la compÃtence, les valeurs fondamentales qu'exigent les mÃtiers de la sÃcuritÃ informatique : Ãthique et loyautÃ. Cela passe entre autres choses par une gestion humaine et managÃriale dans les deux sens : si les hackers ont des droits, et notamment celui de la reconnaissance, ils ont aussi des devoirs. Or cela la France ne sait pas le faire : la politique de la main de fer dans un gant de velours lui est totalement ÃtrangÃre.

A cet Ãgard, la France dont la rÃponse au mouvement des hackers a ÃtÃ d'empiler les textes la cÃlÃbre loi Godfrain, devenue plus tard l'article 323 du Code PÃnal, agrÃmentÃ depuis 2003 de nombreux autres textes, tous aussi subtilement inappropriÃs ayant pour nom LSQ, LCEN - accuse un retard catastrophique que l'on peut Ãvaluer Ã au moins 20 ans (par exemple par rapport Ã l'Allemagne).

D'ailleurs il y a absence d'un mouvement hacker digne de ce nom Ã part l'historique mais trÃs actif /tmp/lab et quelques rÃurgences ici et lÃ du groupe 2600. Ce n'est que trÃs rÃcemment (depuis 2009) et encore timidement que la France voit l'organisation de confÃrences de hacking comme iAWACS, HES, HIP; mais toujours avec une extrÃme prudence car on ne sait jamais comment l'article 323 du Code PÃnal sera appliquÃ au final.

A l'Ãtranger les plus grandes confÃrences de hacking comme les plus petites, et le terme n'est pas pÃjoratif sont sponsorisÃes par les trÃs grosses sociÃtÃs de logiciels ou de services (Google, Microsoft, Oracle) et, quelquefois, avec le soutien des Etats (par exemple la cÃlÃbre confÃrence Hack.lu au Luxembourg). Elles sont tout autant frÃquentÃes

majoritairement par les services gouvernementaux et les industriels/sociétés.

C'est la preuve s'il en fallait une que les évolutions majeures se font, aujourd'hui, dans ces conférences et nulle part ailleurs. Phénomène très significatif : depuis quatre ans les avancées majeures en matière de cryptanalyse ne sont plus publiées dans les conférences académiques mais dans les conférences de hacking et en particulier lors de la conférence du CCC (Chaos Computer Club) à Berlin.

En France, on est encore, hélas, dans un monde d'anciens qui administrent mais ne comprennent rien à la technique et les jeunes hackers qui maîtrisent mais n'administrent pas. Cette fracture n'est plus tenable. Sinon, ce qui a commencé comme un mouvement d'humeur risque de se muer en une révolte contre les décideurs dont ni les institutions, ni les entreprises ne sortiront indemnes. Et les victimes seront le pays tout entier, y compris les hackers qui ne peuvent espérer qu'une victoire à la Pyrrhus.

[**Eric Filiol**, Directeur de la recherche de l'École Supérieure, d'Informatique, Electronique, Automatique ([ESIEA](#)).]