Géostratégie de l'Internet

vendredi 24 juin 2011, par Christophe WOLFHUGEL, Laurent BLOCH

Estonie, Géorgie, WikiLeaks, Tunisie, Egypte… Les démonstrations de la dimension géopolitique d'Internet abondent. Alors que des états-majors de cyber-guerre se mettent en place, le *Diploweb.com* donne la parole à des experts en sécurité informatique.

Les Éditions Eyrolles publient le 23 juin 2011 la troisième édition actualisée du livre *Sécurité informatique, Principes et méthode* de Laurent Bloch et Christophe Wolfhugel. L'éditeur a bien voulu autoriser le *Diploweb.com* à en publier quelques bonnes feuilles, extraites du dernier chapitre du livre, consacré aux questions géostratégiques.

Quelles armes pour la guerre sur Internet ?

L'ARME la plus fréquente à ce jour sur l'Internet est l'attaque par déni de service distribué (*distributed denial of service*, abrégé DDoS). L'attaquant s'assure le contrôle d'un nombre aussi important que possible d'ordinateurs piratés à l'insu de leurs propriétaires et qualifiés de « zombies ». Ce réseau de machines sous contrôle s'appelle un *botnet* [1]. Les machines infectées animent alors un programme qui leur permet de déclencher une action simultanée, comme une avalanche de messages ou de tentatives de connexion. Certains *botnets* comportent plus d'un million de machines et peuvent émettre 14 millions de messages par minute. Peu de services résistent à 100 000 tentatives de connexions réalisées durant la même seconde.

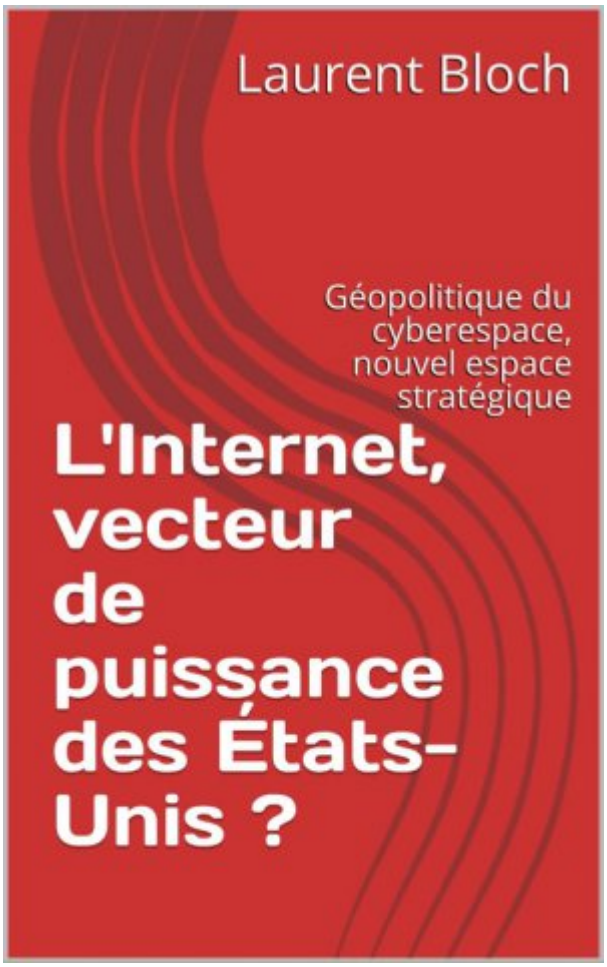
Les logiciels destinés à réaliser de telles attaques sont disponibles sur l'Internet. Leur ergonomie est excellente et il n'est nul besoin d'être un expert en informatique pour les utiliser. Il est aussi possible de louer un botnet, éventuellement par tranches, avec une excellente assistance téléphonique en anglais assurée par un vendeur souvent situé dans la partie orientale de l'ensemble eurasien.

États-majors de cyberguerre

L'un après l'autre, les pays développés se dotent de commandements spécialisés pour la cyberguerre. Depuis mai 2010 c'est le cas du *US Cyber Command* américain. La Corée du Sud a créé le sien en janvier 2010 afin de résister aux attaques en provenance de Corée du Nord et de Chine. Le Royaume-Uni et la Suisse y réfléchissent, ainsi qu'Israël et la Chine, et à un autre niveau l'OTAN. En France, le décret du 11 février 2011 (http://www.ssi.gouv.fr/site_article318.html) a élargi le domaine de compétence de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et jeté les bases de la stratégie française en matière de défense et de sécurité des systèmes d'information. On observera que la création de ces centres de commandement ne permet pas toujours de distinguer ce qui est défensif de ce qui pourrait devenir offensif, ni même ce qui est militaire de ce qui est civil.

Livre édité par Diploweb

. Laurent Bloch, *Internet, vecteur de puissance des Etats-Unis ?* éd. Diploweb 2017, disponible au format Kindle (6,49 euros), et broché imprimé sur papier, sur Amazon.



Estonie et Géorgie

Les procédés d'attaque sur l'Internetont été utilisés contre l'Estonie et la Géorgie.

L'attaque par déni de service de 2007 contre l'Estonie a été revendiquée en 2009 par Konstantin Goloskokov, activiste de l'organisation de jeunesse nationaliste proche du pouvoir russe *Nachi* (« Les Nôtres »). Elle a concerné 130 sites Web estoniens, gouvernementaux ou privés. Il s'agissait essentiellement d'une manœuvre d'intimidation après la décision estonienne de déplacer un monument soviétique commémoratif de la seconde guerre mondiale. L'implication du gouvernement russe n'est pas prouvée. Les dommages ont été estimés à plusieurs dizaines de millions d'euros.

En prélude à la guerre russo-géorgienne de l'été 2008, des sites géorgiens gouvernementaux et privés ont été attaqués de façon continue, à la manière d'une préparation d'artillerie dans une guerre du siècle dernier, piratés et rendus inutilisables. De nombreux observateurs ont émis l'idée que ces attaques étaient trop perfectionnées, massives et bien coordonnées pour être le fait d'internautes indépendants, mais là non plus l'implication du gouvernement russe n'est pas prouvée.

Ross Stapleton-Gray et William Woodcock ont publié dans les Communications of th ACM [2] de mars 2011 un article intitulé National Internet Defense – Small States on the Skirmish Line qui tire les leçons

contrastées de ces événements. L'Estonie a mieux résisté à l'attaque que la Géorgie, et a rétabli plus vite ses communications, parce que ses connexions à l'Internet global étaient multiples et de meilleure qualité que celles de la Géorgie, dont la plupart des liens internationaux passaient par le territoire russe. L'Estonie avait un *Internet Exchange Point* (IXP) sur son territoire, à la différence de la Géorgie. Cela étant dit, l'Estonie était plus dépendante de l'Internet pour son économie et son administration que ne l'était la Géorgie, qui d'autre part, à la différence de l'Estonie, était confrontée à une « vraie » guerre sur le terrain physique.

Les auteurs terminent leur article par une liste de recommandations à l'adresse des petits pays, auxquels il est conseillé de réaliser quelques investissements dans leur infrastructure d'accès à l'Internet afin d'assurer leur indépendance de ce côté-là :

. favoriser la création d'une infrastructure physique robuste, au moyen de la réglementation, de la politique publique et de l'investissement public ;

. assurer la diversité des connexions internationales ;

. susciter la création sur le territoire national d'au moins un Internet Exchange Point (IXP) ;

. assurer la résolution de noms du DNS sur le territoire national par l'installation d'au moins une copie d'un serveur racine ;

. encourager le développement d'une communauté de professionnels du réseau et de sa sécurité, et stimuler ses collaborations locales et internationales.

Le Centre d'excellence OTAN de Tallinn en Estonie a publié un excellent ouvrage sous la plume de Eneken Tikk, Kadri Kaska et Liis Vihul, International Cyber Incidents : Legal Considerations [3].

WikiLeaks

Le problème numéro 1 que doivent résoudre tous ceux qui travaillent dans le domaine de la sécurité informatique, et au premier chef les Responsables de la sécurité des Systèmes d'information (RSSI), est le faible niveau de conscience et de mobilisation des utilisateurs et des responsables à cet égard. Le RSSI est perçu comme un perturbateur, dont les recommandations et les exigences vont accroître, parfois dans des proportions considérables, les coûts et les délais de tous les projets dans lesquels il a réussi à mettre son nez. Comme l'a écrit l'un d'entre eux, c'est « celui qui mange tout seul à la cantine ». L'auteur de ces lignes a occupé cette fonction pendant sept années, au long desquelles il a vérifié qu'il était fui par ceux qui craignaient d'avoir à tenir compte de ses avis.

Dans ce contexte, WikiLeaks, de toute évidence, a fourni une contribution majeure à l'amélioration de la situation ! Le spectacle des dépêches confidentielles du corps diplomatique américain étalées sur le Web (même s'il ne s'agissait pas, après tout, d'informations ultra-secrètes) a suscité une prise de conscience qu'aucun travail pédagogique n'aurait accompli. Certes, la plupart des informations publiées par WikiLeaks ne sont pas obtenues par des procédés informatiques : ce sont le plus souvent des détenteurs légitimes qui en ont organisé l'évasion. Les moyens qui permettent l'acheminement de ces données de telle sorte que l'origine en soit brouillée reposent bien sur des infrastructures informatiques établies à cet effet, mais qui existent depuis des années au vu et au su de chacun, comme le service d'anonymisation Tor [4].

Le souci primordial des administrateurs de WikiLeaks, on le comprend aisément, est de protéger leurs sources ; ils ont cette préoccupation en commun avec les journalistes d'investigation. Bien que par définition les mesures prises pour assurer cette protection ne soient pas publiques, elles reposent sur la multiplication de serveurs dispersés géographiquement et non administrés par une seule entité, le chiffrement, l'acheminement des données par des itinéraires non publiés selon les normes habituelles. Pour citer la page d'accueil du projet Tor : « Tor vous protège en faisant transiter vos communications au

sein d'un réseau distribué de relais hébergés par des volontaires partout dans le monde : il empêche quiconque observant votre connexion Internet de savoir quels sites vous visitez, et il empêche le site que vous visitez de savoir où vous vous trouvez. Tor fonctionne avec bon nombre d'applications existantes, y compris les navigateurs web, les clients de messagerie instantanée, les connexions à distance, et autres applications basées sur le protocole TCP. » [5].

Daniel Berg-Domscheit [6] indique un procédé astucieux et très facile pour communiquer discrètement : le partage d'un compte Webmail chez un opérateur quelconque, dont tous les participants à la conspiration possèdent le mot de passe. Les messages sont écrits, placés dans le dossier « Brouillon », et jamais envoyés, la boîte aux lettres du compte n'est jamais relevée, ainsi il n'y a aucun trafic, aucune circulation de données, juste des connexions à un compte Yahoo ! ou Gmail quelconque.

Les rebondissements judiciaires consécutifs aux publications de WikiLeaks et aux actions en justice contre son fondateur ont révélé que les institutions les plus sérieuses en apparence pouvaient être vulnérables du point de vue de la sécurité de leur système d'information. Le groupe d'activistes Anonymous [7] a soutenu et défendu WikiLeaks : lorsque PayPal et Mastercard ont bloqué les comptes de WikiLeaks, les membres d'Anonymous ont paralysé leurs sites par des attaques en déni de service distribué. Ils ont de même attaqué les sites des gouvernements tunisiens et égyptiens lorsque les dirigeants de ces pays, dans le cadre de leurs actions pour couper court au soulèvement de leurs peuples, ont voulu réduire WikiLeaks au silence sur leurs territoires.

Finalement, le travail de WikiLeaks est un peu le même que celui du *Canard enchaîné* ; l'apport de la dimension informatique, c'est la possibilité de divulguer instantanément un énorme volume de données à la planète entière.

Le livre de Daniel Berg-Domscheit, un collaborateur congédié et déçu par Julian Assange, le fondateur de WikiLeaks, donne (p. 327) une récapitulation chronologique des activités du site : premières publications fin 2006, mise en ligne du manuel de la prison de Guantánamo fin 2007, en 2008, publication de documents secrets de l'Église de Scientologie, d'une liste de membres du *British National Party* (nationaliste, xénophobe, raciste), du rapport de l'ONG Oscar sur les escadrons de la mort de la police du Kenya. En 2009, publication de 6 700 rapports de recherche commandés par le Congrès américain, du rapport d'un soldat sur une bavure de l'armée américaine dans la province afghane de Kunduz, en 2010, nouvelles publications sur des opérations et des bavures en Afghanistan et en Irak, arrestation du soldat Bradley Manning, accusé d'être à l'origine de certaines fuites. Depuis Bradley Manning est incarcéré sans jugement dans des conditions qui ne respectent pas les droits de l'homme. La bande vidéo sur l'Irak, mise en ligne sous le titre *Collateral Murder*, « montrait, vus depuis le viseur du canon d'un hélicoptère militaire, des soldats américains en train de tirer sur des civils irakiens. Deux journalistes de l'agence Reuters avaient aussi été tués ce jour-là… Des soldats qui tiraient sur les civils sortis d'un minibus qui passait par là pour porter secours aux deux journalistes et aux autres victimes. Leurs commentaires cyniques ont provoqué l'indignation du monde entier. » (pp. 193-194). Cette publication a marqué une date pour la notoriété de WikiLeaks, et c'est parce qu'il est soupçonné d'être à l'origine de la fuite qui l'a permise que Bradley Manning est emprisonné.

Les spécialistes des relations internationales ne manquent pas de souligner que la généralisation de publications de documents confidentiels tels que ceux mis en ligne par WikiLeaks serait de nature à modifier considérablement les conditions d'exercice de la diplomatie et, plus généralement, de la négociation politique. De par la nature d'une négociation, chaque négociateur est amené à proposer à la partie adverse des concessions et des compromis, à certains desquels aucune suite ne sera donnée, mais dont la divulgation prématurée serait de nature à faire échouer toute la transaction, et dont même la publication ultérieure pourrait être très embarrassante pour les parties concernées. On peut citer ainsi les négociations qui ont eu lieu durant les années 1980 entre les juntes militaires au pouvoir dans certains pays d'Amérique du Sud (Brésil, Uruguay, Chili, Argentine) et les partis politiques qui leur ont succédé, ou celles qui ont permis la transition démocratique dans les pays du Pacte de Varsovie après la chute du mur de Berlin : elles ont abouti parce qu'elles ont pu rester secrètes.

Dès lors qu'un diplomate se saurait exposé, à tout moment, à l'étalage sur le Web de tout ce qu'il aurait pu dire lors d'une négociation de cette nature, il est hors de doute que son comportement sera différent, plus prudent à tout le moins.

En tout cas, la violence des réactions et de la répression déclenchées par WikiLeaks démontre que le phénomène n'a rien d'anodin. Cela dit, l'expérience tend à prouver que la divulgation des turpitudes des pouvoirs au nom de la transparence peut servir la démocratie, mais tout aussi bien les pires totalitarismes : tout dépend en fait de l'usage que veulent en faire les citoyens et les sociétés.

Stuxnet

Le ver Stuxnet, qui s'attaque aux systèmes Windows, a été identifié en juin 2010 par la société biélorusse VirusBlokAda. Il est plus particulièrement destiné à modifier le comportement des systèmes de commande des installations industrielles, et notamment des automates programmables de la marque Siemens.

La lecture du bulletin signalétique détaillé émis par l'éditeur d'anti-virus Symantec [8] nous apprend que Stuxnet a contaminé des dizaines de milliers de systèmes, surtout situés en Iran, mais aussi en Allemagne, en Inde et en Indonésie. Son mode de propagation favori est par clé USB.

Le même document révèle que le virus Stuxnet obéit à une conception révolutionnaire, d'une complexité jamais vue : il utilise quatre failles zero-day d'un coup, ce qui est un luxe particulièrement dispendieux. Il utilise deux certificats légitimes émis au nom de sociétés bien connues (JMicron et Realtek) pour échapper aux anti-virus, et se camoufle dans le système infecté au moyen d'un *rootkit*. Les spécialistes estiment que ce ver a demandé un travail de six mois à un an à une équipe de 6 à 10 ingénieurs.

Une fois installé sur un système de contrôle de processus industriel, Stuxnet est capable de modifier le comportement des machines que ce système pilote, et c'est bien par ce procédé qu'il a atteint une célébrité planétaire.

En effet, Stuxnet est soupçonné d'avoir été utilisé pour perturber le fonctionnement des centrifugeuses des installations nucléaires iraniennes de Natanz ; les déclarations des autorités iraniennes à propos d'un arrêt de certaines activités de centrifugation et d'enrichissement d'uranium de mars à septembre 2010 à cause d'un sabotage informatique sembleraient corroborer ces soupçons, mais elles doivent être prises avec précaution parce que plusieurs versions contradictoires en ont été données. Les services secrets israéliens et américains figurent au rang des suspects d'un éventuel sabotage. Le général israélien Gabi Ashkenazi aurait reconnu être le père du ver Stuxnet.

On pourra lire avec intérêt l'analyse de Daniel Ventre pour la revue MISC [9]. Le même auteur a également consacré une étude aux capacités des deux Corées en termes de cyberguerre [10]. On consultera aussi l'article de James P. Farwell et Rafal Rohozinski [11] *Stuxnet and the Future of Cyber War*.

Tunisie, Égypte : Internet pour la liberté

Lors des soulèvements révolutionnaires du « Printemps arabe [12] » de 2010-2011 qui ont abouti au renversement des dictatures en Tunisie et en Égypte, les réseaux sociaux en ligne tels que Facebook et Twitter ont joué un rôle que les premiers commentaires ont sans doute surestimé, mais qui ne saurait néanmoins être négligé. Les Tunisiens et les Égyptiens n'avaient sans doute guère besoin de l'Internet pour savoir à quoi s'en tenir sur les dirigeants de leurs pays, mais ces réseaux ont permis, comme en Iran lors des manifestations consécutives aux élections truquées de 2009, des échanges d'informations instantanés et discrets entre les manifestants, pour déclencher des rassemblements, etc. Surtout, ils ont créé un sentiment d'appartenance à une collectivité dotée de valeurs, de soucis et de buts communs, ou en d'autres termes ce que logiciens et économistes ont nommé, dans la théorie des jeux, du savoir

commun (Mutual Knowledge). Là encore, l'Internet fut un facteur d'ouverture au monde et de libération des esprits.

Peut-on éteindre l'Internet ?

Ces événements donnèrent lieu à une expérience inédite : l'extinction de l'Internet, tentée d'abord à une échelle partielle par les services de sécurité tunisiens [13], puis de façon plus radicale en Égypte [14].

Pour toutes les raisons évoquées ci-dessus (et quelques autres), l'Internet énerve parfois les détenteurs du pouvoir (ou d'un pouvoir), qui sont alors tentés de s'en débarrasser. Le gouvernement des États-Unis rêve ainsi de l'*Internet kill switch* [15], un gros bouton rouge qui permettrait au président, « en cas de crise internationale grave ou de cyber-attaque », de couper l'Internet. De façon plus insidieuse, des acteurs moins puissants, comme l'industrie du divertissement, ou le gouvernement français lorsqu'il se laisse influencer par elle, tentent toutes sortes de mesures pour censurer ou filtrer l'Internet, comme la loi Hadopi et la loi Loppsi.

Comme nous allons le montrer, et pour citer Pierre Col [16], « l'Internet est à la fois globalement robuste et localement vulnérable ».

Par attaque de la racine du DNS ?

La première idée qui pourrait venir à l'esprit d'un candidat à l'extinction de l'Internet serait sans doute de s'en prendre à la racine du DNS : les explications des chapitres précédents montrent que la difficulté d'une telle entreprise, si l'on voulait une interruption planétaire d'une durée supérieure à quelques dizaines de minutes, serait pratiquement insurmontable, parce qu'il faudrait neutraliser (ou gruger) des centaines de serveurs dispersés à la surface de la terre, qui s'appuient sur des technologies diverses et variées. Et au fur et à mesure que DNSSEC, protocole destiné à sécuriser les données envoyées par le DNS, sera déployé, les possibilités de corrompre les serveurs DNS, en leur insinuant des informations fallacieuses, se réduiront considérablement. Une telle attaque ne serait d'ailleurs qu'imparfaitement efficace car l'accès par les numéros IP resterait possible et parce que la mise en place d'un autre DNS est relativement facile.

Par attaque sur le routage ?

Une attaque sur le routage serait plus prometteuse : les expériences réussies de *Pakistan Telecom* [17] montrent que des choses sont possibles, notamment parce que le protocole BGP (qui sert à transmettre les informations de routage entre *Autonomous Systems*) est traditionnellement dépourvu de toute sécurité. Mais dans tous les exemples documentés de telles attaques, le dysfonctionnement n'a été que partiel et le caractère décentralisé de l'Internet a permis un rétablissement rapide du fonctionnement de la plupart des réseaux, ce qui confirme la véracité de l'aphorisme de Pierre Col cité ci-dessus.

Comment les dictateurs tunisien et égyptien ont-ils procédé ? Dans les deux cas il s'agissait, d'une part, de régimes politiques dotés d'une police toute-puissante et, d'autre part, de pays avec un nombre restreint de FAI. Le cas de l'Égypte, par exemple, a été particulièrement simple : un ministre ou un fonctionnaire de grade suffisamment élevé a décroché son téléphone et a ordonné aux quatre FAI du pays de couper les communications, ce qu'ils ont fait en interrompant le routage par la suppression des annonces de routes BGP. L'idée qu'ils puissent ne pas obtempérer n'était même pas envisageable. La censure tunisienne a été dans un premier temps brutale : six mois de coupure franche de l'Internet, suivis d'une période d'accès sélectif contrôlé par le système de filtrage surnommé Ammar404 par les opposants, qui n'a pris fin qu'avec le renversement du régime.

Il est clair que si le président des États-Unis voulait s'attaquer à l'Internet, comme certains parlementaires lui conseillent de s'en donner les moyens, il pourrait faire plus de dégâts : ainsi, beaucoup de communications entre pays tiers, ou même entre deux FAI d'un même pays tiers, transitent par les États-Unis, soit parce que l'infrastructure est ainsi faite pour des raisons techniques ou géographiques,

soit pour des raisons tarifaires. Dès lors, en appuyant sur le gros bouton rouge d'extinction de l'Internet, il ne parviendrait peut-être pas à couper toutes les communications internes aux États-Unis, mais il en couperait beaucoup à l'extérieur.

La cybersécurité en 2011

En janvier 2011 le *Center for Strategic & International Studies* à Washington, un think-tank dévolu principalement aux questions de défense et de politique étrangère, a publié un rapport intitulé *Cybersecurity Two Years Later* [18], qui émet des recommandations adressées au gouvernement américain, qui pourraient tout aussi bien s'adresser au gouvernement français. Ces recommandations sont centrées autour de « dix domaines clés où des progrès doivent être accomplis » :

. Une organisation et un leadership cohérents pour des efforts dans le domaine de la cybersécurité, et la reconnaissance de la cybersécurité comme priorité nationale.

. Une autorité clairement identifiée à même d'imposer une amélioration de la cybersécurité des infrastructures critiques et de développer des collaborations innovantes avec le secteur privé.

. Une politique étrangère qui utilise tous les leviers de la puissance américaine pour créer des normes, de nouvelles approches pour la gouvernance et des suites aux actions malveillantes dans le cyberespace. Cette nouvelle politique devra comporter une vision pour l'avenir de l'Internet mondial.

. Une aptitude accrue à utiliser les services de renseignements et les capacités militaires aux fins de défense contre les menaces étrangères de pointe.

. Une attention renforcée pour la protection de la vie privée et des libertés civiles, avec des règles claires et des procédures adaptées aux technologies numériques.

. Améliorer l'authentification des identités pour l'accès aux infrastructures critiques.

. Accroître les effectifs d'experts en cybersécurité tant en quantité qu'en niveau de compétence [19].

. Modifier la politique d'achats publics afin d'inciter le marché à fournir des produits et des services plus sûrs.

. Réviser la politique et le cadre légal de façon à guider les actions du gouvernement en matière de cybersécurité.

. Développer la recherche et le développement sur les problèmes difficiles liés à la cybersécurité, un processus d'identification de ces problèmes, et leur allouer des crédits de façon coordonnée.

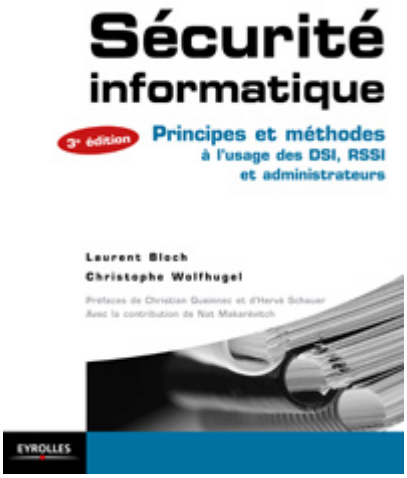
Plus

Laurent Bloch et Christophe Wolfhugel,
Sécurité informatique. Principes et méthode à l'usage des DSI, RSSI et administrateurs, Paris, éd. Eyrolles, 3e édition en librairie le 23 juin 2011

Présentation de la 3e édition

Que recouvre le terme de sécurité informatique pour l'entreprise ? Existe-t-il des normes et bonnes

pratiques universelles ? Comment mettre en œuvre une politique de sécurité et mettre au point des chartes de conduite pour minimiser le risque humain ?
Une bible pratique et systématique pour le responsable informatique
Écrit par un responsable de la sécurité des systèmes d'information devenu DSI, et par un expert des réseaux et des systèmes, ce livre limpide expose les risques inhérents à tout système informatique – et les moyens de s'en protéger. S'adressant aux administrateurs et responsables informatiques comme à leurs interlocuteurs, il offre au professionnel consciencieux un exposé clair des modes opératoires des programmes nocifs et des outils censés les contrer, ainsi qu'une méthode rigoureuse pour concevoir une véritable politique de sécurité.
Outre un modèle de politique de sécurité et de charte d'utilisation que le lecteur pourra adapter à son environnement, cette troisième édition, mise à jour avec les dernières évolutions en matière de menaces et de sécurité, propose notamment un éclairage sur la dimension géostratégique de la sécurité liée à l'Internet (WikiLeaks, attaques contre la Géorgie et l'Estonie, coupure de l'Internet en Égypte ou en Tunisie, etc.).



À qui s'adresse cet ouvrage ?

. Aux administrateurs de systèmes et de réseaux, mais aussi aux DSI et aux responsables de projets ;

. À tous ceux qui doivent concevoir ou simplement comprendre une politique de sécurité informatique.

Références

[1]
Projet Tor. Avril 2011. http://www.torproject.org.

[2]
« The web's trust issues ». The Economist, avril 2011.
http://www.economist.com/blogs/babbage/2011/04/internet_security&fsrc=nwl.

[3]
Jean-François Abramatic. « Croissance et évolution de l'Internet ». Université de tous les savoirs – Les Technologies, 7, Paris, 2002. Odile Jacob.

[4]
Daniel Berg-Domscheit. *Inside WikiLeaks*. Grasset, Paris, 2011. 319 p – ISBN 9782246785422.

[5]

Laurent Bloch. Les systèmes d'exploitation des ordinateurs – Histoire, fonctionnement, enjeux. Vuibert, Paris, 2003. Texte intégral disponible ici : http://www.laurentbloch.org/spip.php?article13.

[6]
Laurent Bloch. Systèmes d'information, obstacles et succès – La pensée aux prises avec l'informatique. Vuibert, Paris, 2005. Texte intégral disponible en ligne ici : http://www.laurentbloch.org/spip.php?rubrique5.

[7]
Laurent Bloch. « La régulation universelle de l'internet, enjeu économique et culturel ». Questions internationales, (39), septembre-octobre 2009. http://www.ladocumentationfrancaise.fr/revues-collections/questions-internationales/39/sommaire39.shtml.

[8]
Laurent Bloch. « La maîtrise d'Internet : des enjeux politiques, économiques et culturels ». Questions internationales, (47), janvier-février 2011. Numéro spécial Internet http://www.ladocumentationfrancaise.fr/revues-collections/questions-internationales/47/sommaire47.shtml.

[9]
Laurent Bloch, Nat Makarévitch. « La signature électronique universelle ». Site Web de Laurent Bloch, mars 2007. http://www.laurentbloch.org/spip.php?article107.

[10]
James R. Langevin, Michael T. McCaul, Scott Charney, Lt. General Harry Raduege, James A. Lewis. « Cybersecurity Two Years Later ». janvier 2011. http://csis.org/publication/cybersecurity-two-years-later.

[11]
Ross Stapleton-Gray William Woodcock. *National Internet Defense – Small States on the Skirmish Line*. CACM, 54(3):50–55, Mars 2011.

[12]
Symantec. « W32:Stuxnet ». Symantec.com, juillet 2010. http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

[13]
Eneken Tikk, Kadri Kaska, Liis Vihul. International Cyber Incidents : Legal Considerations. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonie, 2011. http://www.ccdcoe.org/231.html.

[14]
Daniel Ventre. « Guerre de l'information et cyberguerre : les deux Corées face à face ». MISC, (55):62–71, mai-juin 2011.

[15]
Daniel Ventre. « Stuxnet : interprétations ». MISC, (53):53–63, janvier-février 2011.

[16]
Karen Evans Franklin Reeder. « A Human Capital Crisis in Cybersecurity : Technical Proficiency Matters ». novembre 2010. http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity.

P.-S.

Laurent Bloch est DSI de l'Université Paris-Dauphine. Christophe Wolfhugel est consultant et ingénieur chez Sendmail, Inc. pour l'Europe

Notes

[1] *Bot* est l'abréviation de robot.

[2] Ross Stapleton-Gray William Woodcock. *National Internet Defense – Small States on the Skirmish Line*. CACM, 54(3):50–55, Mars 2011.

[3] Eneken Tikk, Kadri Kaska, Liis Vihul. International Cyber Incidents : Legal Considerations. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonie, 2011. http://www.ccdcoe.org/231.html.

[4] Le projet Tor associe un logiciel libre et un réseau informatique de tunnels virtuels pour permettre à tout un chacun une communication confidentielle et anonyme : http://www.torproject.org

[5] *Projet Tor*. Avril 2011. http://www.torproject.org.

[6] Daniel Berg-Domscheit. *Inside WikiLeaks*. Grasset, Paris, 2011. 319 p – ISBN 9782246785422.

[7] Cf. http://fr.wikipedia.org/wiki/Anonymous_(communaut%C3%A9)

[8] Symantec. « W32:Stuxnet ». Symantec.com, juillet 2010. http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

[9] Daniel Ventre. « Stuxnet : interprétations ». MISC, (53):53–63, janvier-février 2011.

[10] Daniel Ventre. « Guerre de l'information et cyberguerre : les deux Corées face à face ». MISC, (55) pp. 62–71, mai-juin 2011.

[11] James P. Farwell and Rafal Rohozinski. « Stuxnet and the Future of Cyber War », *Survival*, vol. 53 n° 1, pp. 23-40, www.informaworld.com/smpp/title~content=t713659919.

[12] Le calendrier suggère plutôt « Hiver arabe », mais Printemps convient mieux au côté « renaissance » de l'événement, et rappelle le « Printemps des peuples » européen de 1848.

[13] Cf. http://www.bortzmeyer.org/eteindre-internet.html

[14] Cf. http://www.bortzmeyer.org/egypte-coupure.html

[15] http://news.techworld.com/security/3228198/obama-internet-kill-switch-plan-approved-by-us-senate-panel/

[16] http://www.zdnet.fr/blogs/infra-net/comment-l-egypte-a-pu-etre-deconnectee-d-internet-39757863.htm

[17] http://www.bortzmeyer.org/pakistan-pirate-youtube.html

[18] James R. Langevin, Michael T. McCaul, Scott Charney, Lt. General Harry Raduege, James A. Lewis. « Cybersecurity Two Years Later ». janvier 2011. http://csis.org/publication/cybersecurity-two-years-later

[19] Karen Evans Franklin Reeder. « A Human Capital Crisis in Cybersecurity : Technical Proficiency Matters ». novembre 2010. http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity.