Extrait du Spyworld Actu

http://www.spyworld-actu.com/spip.php?article13145

Les défis de la cyber-sécurité et le contre-espionnage après la Guerre Froide et le onze septembre

- Renseignement - International -

Date de mise en ligne : vendredi 30 avril 2010

Spyworld Actu

Etant reconnue par Président Obama comme "un des défis les plus sérieux pour l'économie et la sécurité nationale auquel la nation fait face," [1] la cyber-sécurité, mise en corrélation avec le contre-espionnage, a fait l'objet d'un symposium le 21 avril à l'Université de Pennsylvanie, à Philadelphie. Ce symposium a réuni des acteurs du gouvernement américain, du secteur privé et des universités pour discuter les défis de la sécurisation des systèmes, de l'encadrement des utilisateurs, et de l'application des lois.

Les nouvelles formes et sources de l'espionnage

Bien évidement l'espionnage n'est pas quelque chose de nouveau. L'intervenant principal, Mme. Michelle van Cleave, chercheur "senior" du College of International Affairs a l'Université nationale de la Défense (NDU), a évoqué l'histoire des espions et le KGB pendant la Guerre Froide.

Même si l'espionnage continue aux Etats-Unis, explique le Dr. Joseph Kielman du Department of Homeland Security, il n'est plus le fait de l'URSS ou de la Mafia (et selon Randall Fort du Raytheon Corporation, ce n'est même pas la Chine) ; il s'agit plutôt des états-nations ou des groupes "voyous (rogue)". Un représentant de Deloitte Consulting, Michael Dorsey, a donné l'exemple de "Solar Sunrise" en 1998, une attaque sur les ordinateurs du DoD (Department of Defense) qui a été coordonnée non pas par des Russes ou des Iraquiens mais par deux adolescents en Californie et un en Israël. Son autre exemple a été "Moonlight Maze", des attaques qui ont duré plus de trois ans et qui ont été liées à un ordinateur à Moscou, mais dont l'origine n'est toujours pas connue, problème classique des "cyber attacks".

Selonle Dr. Kielman, la solution aux problèmes d'attaques est d'essayer de créer des systèmes non pas parfaits, mais "résilients", qui peuvent rebondir.

La relation gouvernement-secteur privé et la question de l'application des lois

L'un des thèmes les plus souvent mentionnés au cours du symposium est la relation entre le gouvernement et le secteur privé. Randall Fort, Directeur des programmes de sécurité au Raytheon Corporation, a expliqué que "85 à 95 pourcent de la collection d'informations est dans les mains du secteur privé." Avec ce changement, le gouvernement devient dépendant d'eux.

Les compagnies privées ont de la flexibilité et de la capacité d'intervention rapide (agility), pendant que le gouvernement connait des obstacles bureaucratiques. Néanmoins, seul le gouvernement peut gérer les opérations offensives, comme fermer des ordinateurs ou des noeuds compromis (botnets) et ce sont les organisations comme le FBI qui gèrent les enquêtes ; le secteur privé doit suivre. L'interaction du gouvernement et des compagnies est très compliqué et sans résultats assurés. Mais que peut attendre du gouvernement une organisation comme Google, objet d'une attaque venant de deux ordinateurs en Chine ? Selon un représentant du Control Risks Group, ils ont besoin d'une "politique étrangère" dans le domaine de la cyber-sécurité. Quant à Novartis Pharmaceuticals, ils préfèrent assurer eux-mêmes leurs biens et leur parties de la "supply chain" en utilisant le GPS qui protège leurs camions.

Presque 10 ans après le 11 septembre, ce ne sont plus seulement des problèmes techniques mais aussi une question d'utilisateurs

Jonathan Smith, professeur d'informatique à l'Université de Pennsylvanie, a évoqué l'importance de l'encadrement des utilisateurs d'ordinateurs, en tout ce qui concerne la sécurité de leurs machines et de leur informations

personnelles. Un manque de fiabilité et de "discipline" des utilisateurs menace les systèmes techniques qui ne sont pas parfaits mais qui sont très avancés et fort complexes.

Randall Fort, de Raytheon Corporation, l'appelle un problème de "social engineering." Dans son expérience professionnelle, ce phénomène marque un deplacement du débat de "comment est-ce que l'on crée les systèmes les plus fiables et les plus surs", juste après le 11 septembre 2001, vers "comment encadrer les personnes qui utilisent ces systèmes" aujourd'hui.

Par exemple, la brèche de sécurité de Google, selon la source de NYT[2], a commencé par un employé de Google en Chine qui a cliqué sur un lien dans un "instant message." Il s'est trouvé connecté à un site "infecté" qui a permis aux intrus d'avoir accès a son ordinateur personnel et, finalement, à un logiciel sensible utilisé par l'équipe de developpement de Google. Si un employé d'une grande compagnie technologique ne sait pas comment se protéger, comment s'assurer que "Joe the Plumber", par exemple, saura éviter les liens empoisonnés, le malware, et cetera ?

Les dangers du "cloud computing" et du réseautage personnel

Cette attaque sur Google a mis en question la securité du "cloud computing", où les informations personnelles de millions d'individus et de sociétés sont stockées dans une groupe d'ordinateurs centrals. Une seule infraction peut vouloir dire des pertes désastreuses. Dans le cas de Google, selon le NYT, une des pertes était celle de "Gaia", un système des mots de passe qui permet aux utilisateurs de se connecter avec leur mot de passe une fois ("single identifier") et puis d'accèder à tous les services.[3] La réponse de Google fut d'installer un nouveau niveau de codage pour Gmail, leur service d'email, et de "relever" la sécurité de ses centres de donnés.

La menace sur les informations personnelles et la "privacy" est bien évident dans le cas de Google, et aussi sur les sites du "social networking" comme Facebook. Peter Nolan du Control Risks Group a parlé de "l'utilisation aggressive des sites de réseautage personnel pour créer les relations qui peuvent produire des renseignements". Là encore on tombe sur la question de l'encadrement des utilisateurs, dans ce cas pour examiner, dans une mesure raisonnable, leurs contacts. Une solution technique est la bonne gestion de l'assertion des identités, parce qu'il faut savoir que l'on peut faire confiance à la plate-forme. Finalement c'est clair que nous risquons de perdre de la "privacy", mais la question evoquée par Mark Cohn le vice-président de la sécurité des entreprises au Unisys Corporation, est de savoir s'il reste encore de la vie privée à préserver.

Comment soutenir et encourager les acteurs futurs

Un problème relevé par Professeur Smith de l'Université de Pennsylvanie a été celui d'une hémorragie d'étudiants dans l'informatique après le diplome "bachelor." Parmi ses étudiants, il a noté que 40 pourcent ont choisi d'entrer dans le secteur financier, et que seuls 5 pourcent ont continué leurs études dans le domaine. En combinaison avec le fait que l'on ne peut toujours pas faire confiance aux connaissances des utilisateurs dits "normaux" des ordinateurs, cette perte d'hommes et femmes qui aurait pu faire progresser la sécurité des systèmes met en doute la capacite de repondre a ces problemes.

Dans la discussion qui a suivi, quelqu'un a noté que la principale motivation était l'argent. Comment les universités ou le gouvernement peuvent-ils concurrencer les compagnies qui paient ces diplomés avec des salaires beaucoup plus généreux ? Une solution potentielle suggérée etaient des programmes de "loan forgiveness," qui annulerait ou réduirait les dettes - souvent très importantes dans un système d'éducation supérieur qui peut couter plus de $40.000 par an. Une autre suggestion était la possibilité du financement d'études au niveau Master ou doctoral par les organisations comme le DARPA, l'Agence des projets recherché avancé sur la défense.

Post-scriptum :

http://www.bulletins-electroniques....