Note de Veille Cyber n°3

Du 12 mars au 8 avril 2011 par Alix Desforges

Note préalable à la lecture : du fait de la nature du sujet et de l'intérêt d'une note conçue à l'appui de l'ensemble des sources d'information disponibles sur le web (blog, journaux, etc.), la totale fiabilité des informations proposées ne peut être pleinement garantie. Cette note propose d'ouvrir des perspectives. A chacun de poursuivre le travail.

Piratage

La vengeance de Stuxnet. Source

Un jeune pirate informatique iranien a revendiqué le piratage de deux associés italiens de l'éditeur de solutions de sécurité Comodo. Il a ainsi réussi à créer neuf certificats frauduleux de sécurité. Ce type de certificat est notamment utilisé par les services Gmail, Yahoo ! Mail, Hotmail ou encore Skype. Il a aussi mis à disposition sur un site de téléchargement le faux certificat de la plate-forme de téléchargement des extensions Mozilla. Dans une lettre ouverte, le pirate déclarait que le piratage visait à venger l'Iran du ver Stuxnet. Il précisait également avoir agi seul, sans lien avec le gouvernement iranien. La société Comodo évoquait cependant la piste gouvernementale. Le FBI et la police italienne ont été chargés de l'enquête.

La Commission Européenne victime d'une cyberattaque. Source

Le jeudi 24 mars 2011, à la veille de la réunion du Conseil de l'Europe, la Commission Européenne a révélé avoir été la cible d'une cyberattaque. L'accès externe aux emails et l'intranet ont été suspendu afin de rétablir le réseau. Il a aussi été demandé aux employés de changer leurs mots de passe. Antony Gravili, porte parole administratif de la Commission a précisé que plusieurs hauts officiels de la Commission ont été spécifiquement visés. Les services diplomatiques de la Commission et le Service Européen pour l'Action Extérieur ont été particulièrement touchés.

Des services spatiaux de la NASA vulnérables aux attaques informatiques. Source

Un rapport du Bureau de l'Inspection Générale révèle que six serveurs de la NASA auraient des vulnérabilités critiques. Ces vulnérabilités auraient pu compromettre plusieurs programmes dont le télescope Hubble, l'ISS ou encore le programme des navettes spatiales. Les vulnérabilités ont été corrigées mais estiment que « des pratiques de sécurité inadéquates exposent les réseaux critiques de la NASA aux cyberattaques ».

Organisation et doctrine des armées

Un Memorandum of Understanding pour une cyberdéfense européenne. Source

Les ministres de la Défense de l'Union Européenne se sont réunis les 10 et 11 mars pour évoquer une future stratégie commune de cyberdéfense. Un Memorandum Of Understanding a été signé entre les ministres européens de la Défense et l'OTAN. Il a jeté les bases de cette coopération. Le partage de l'information et la promotion des bonnes pratiques devraient en être les pierres angulaires. La riche actualité du domaine pour l'année 2010 a fait l'objet de nombreuses discussions et interrogations entre les ministres : Opération Aurora, Stuxnet…

L'Allemagne peaufine sa stratégie de cyberdéfense. Source

Après l'annonce de la création du Centre National de Cyberdéfense (Nationales Cyber-Abwehrzentrum, NCAZ), la stratégie allemande en matière de cyberdéfense est précisé dans un document. Il annonce la création d'une deuxième agence : le Conseil National pour la cybersécurité (Nationaler Cyber-Sicherheitsrat). Le Conseil, pleinement intégré à la chancellerie, devait entamer son travail au 1er avril. Des représentants des ministères clés (Intérieur, Défense, Justice, Economies, Finances…) y siègeront sous la présidence de Cornelia Rogall-Grothe. De source anonyme, les deux entités seraient déjà critiquées en interne.

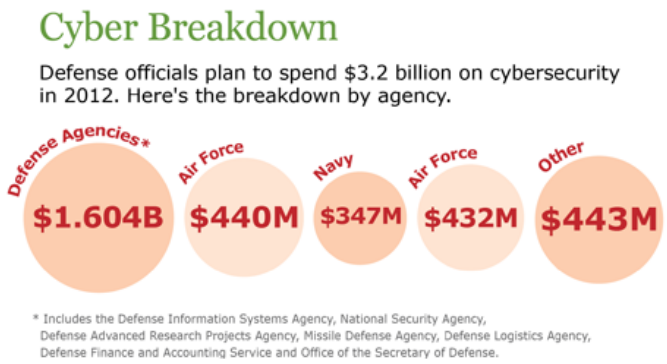
L'informatique dans les nuages débarque à l'US CYBERCOM. Source

L'US Cyber Command, qui devrait être totalement opérationnel d'ici Octobre 2011, va utiliser les capacités offertes par l'informatique dans les nuages ou « cloud computing ». Pour le chef du centre de commandement, Keith Alexander, « l'architecture « cloud » peut paraitre particulièrement vulnérable mais nous sommes convaincu que les contrôles et les

outils qui seront élaborés dans le « cloud » garantiront un accès sécurisé ».

Le Pentagone cafouille son budget pour la cybersécurité. Source

Après avoir évoqué dans un premier temps un budget de 2,3 milliards de dollars il y a un mois, le DoD réclame désormais 3,2 milliards pour la cybersécurité de l'ensemble du Département. Dans le même temps, l'US Air Force réclamait à elle-seule une enveloppe de 4,6 milliards de dollars. Des questions de lignes de budget expliqueraient ce manque de précision. Selon la porte parole du DoD « Le précédent montant de 2,3 milliards de dollars ne reflète qu'une partie du budget demandé par le DoD pour l' « Information Assurance ». Le Département reconnaît que des activités qui ne dépendent pas traditionnellement du budget relatif à l'« Information Assurance » font partie intégrante des activités en matière de cybersécurité ». Ces imprécisions semblent surtout témoigner des difficultés des différentes composantes du DoD à s'accorder sur la terminologie.



D'un point de vue de la stratégie, un officiel du DoD a annoncé que le Département serait en train de finaliser sa stratégie en matière de cyberguerre. Le document devrait être rendu public dans quelques semaines. Le papier consacrerait une grande part à la coopération internationale, volet qui sera suivi par le Département d'Etat épaulé des militaires.

Le Général Keith Alexander a également précisé les cinq priorités de l'US Cyber Command :

- *Traiter le cyberespace comme un domaine au sein du DoD,*
- *Employer des approches de cyberdéfense actives combinées à des nouvelles approches de défense,*
- *S'associer aux autres agences fédérales et au secteur privé pour établir une cybersécurité nationale,*
- *Resserrer les liens avec les partenaires internationaux*
- *Recruter une main-d'œuvre spécialisée en cybersécurité.*

Martin Libicki, chercheur à la RAND Corporation, affirme cependant que considérer le cyberespace comme un champ de bataille, au même titre que les autres, constitue une mauvaise approche pour les militaires. « Les activités dans le cyberespace sont uniques et ne relèvent pas d'autres formes de guerre » a-t-il précisé. Selon lui, le concept de cyber-dissuasion n'est pas pertinent et ne permet pas d'éviter les cyberattaques.

En Iran, un groupe paramilitaire pour la cyberguerre. Source

Le groupe des « bassijis » a créé sa propre division pour la cyberguerre. Chargée « d'attaquer les sites ennemis » en réponse à leurs « attaques », l'unité serait dirigée par le Général Ali Fazli.

Un groupe d'experts israéliens pour développer la stratégie de cyberdéfense. Source

Le Premier Ministre israélien a formé un groupe d'experts, présidé par le Major Général Isaac Ben-Israël, pour définir une stratégie de défense contre les cyberattaques visant les réseaux militaires et gouvernementaux. Le bureau de lutte contre le terrorisme et aurait conseillé Benyamin Netanyaou. Le Shin Bet aurait une branche entière consacrée aux technologies de pointe qui prend également en charge la défense des réseaux informatiques. Le Mossad aurait une entité similaire. Selon l'article, les services de renseignements de l'armée israélienne auraient créé une nouvelle entité pour traiter des aspects offensifs et défensifs de la cyberguerre.

Menaces

« L'effet Stuxnet » met la protection des infrastructures critiques au cœur des préoccupations. Source

Une nouvelle étude menée par l'Institut Ponemon révèle que 67% des entreprises gérant les infrastructures relatives à l'énergie n'ont pas déployé de solutions de sécurité informatique appropriées. Dans les majorités de ces entreprises, les dirigeants ne comprendraient pas les enjeux relatifs à la cybersécurité. Comme pour en appeler au gouvernement, un consultant en cybersécurité estime que « la régulation est désagréable mais dans certains cas, l'alternative est pire. La cybersécurité est l'un de ces cas ».

Dans ce contexte, un chercheur a publié 34 exploits utilisant sept vulnérabilités des systèmes SCADA de Siemens, Iconics,7-Techologies et DATAC. Selon les experts, ces vulnérabilités ne permettraient pas une prise de contrôle totale du système par l'attaquant. Mais dans le même temps, un test de sécurité sur le réseau de distribution des eaux de Los Angeles a révélé

qu'il était possible de rendre l'eau du réseau non potable grâce à l'ajout de composant chimique.

Les voitures aussi pourraient être victime de cyberattaques. Source
Des chercheurs de l'Université de San Diego et de Washington ont mené des tests de pénétration pendant deux ans sur les systèmes électroniques des voitures. Ces tests ont révélé de nombreuses failles qui permettraient à un attaquant de prendre le contrôle du véhicule. L'insertion d'un code malicieux dans un fichier de musique numérique constitue l'une de ces failles.

L'Arménie déconnectée accidentellement. Source
C'est effectuant des forages dans son jardin, qu'une géorgienne de 75 ans a accidentellement coupé un câble de fibre optique qui permet la connexion à Internet de près de 90% de la population arménienne. La compagnie géorgienne Railway Telecom a pu rétablir la connexion après une coupure de 12h.

Initiatives

L'Australie protège ses informations sensibles. Source
Selon une source anonyme, le CERT australien, en coopération avec les agences de renseignements, serait sur le point de créer une unité de cyber-espions pour protéger les informations sensibles du gouvernement australien et des industries importantes. Il s'agit de limiter l'espionnage par les réseaux Internet venant d'Etats étrangers ou d'individus malveillants. L'Australie a révélé en mars avoir été la cible d'une cyberattaque dont le but était l'espionnage. Les ordinateurs du Premier Ministre et des Ministres des Affaires Etrangères et de la Défense ont notamment été touchés.

Publications récentes

Rapports

- Internet Security Alliance, Improving our Nation's Cybersecurity through the Public-Private Partnership, White Paper, Mars 2011
- Charles Ebinger, Kevin Massy, Software and hard targets : enhancing smart grid cyber security in the age of information, février 2011
- Office of Audits, Inadequate Security Practices Expose Key NASA Network to Cyber Attack, 28 mars 2011
- Symantec, Internet Security Threat Report, avril 2011

Publications universitaires et comptes-rendus de conférence

- Anthimos Alexander Tsirigotis, Cyber Warfare : Virtual war Among Virtual Societies, Proceedings of the 9th European Conference on Information Warfare and Security, July 2010
- Roland Heickero (Swedish Defence Resaerch Agency), Cyber Antogonism Between Hacker Group Develops new Challenges, Proceedings of the 9th European Conference on Information Warfare and Security, July 2010
- Aki-Mauri Huhtinon (National Defence University, Helsinki), The Way of Warfare in Three Possible Worlds – from art of war to Information Warfare, Proceedings of the 9th European Conference on Information Warfare and Security, July 2010

Stratégie nationale

- Federal Ministry of the Interior, Cyber Security Strategy for Germany, février 2011