Cyberguerre : sortons du domaine du fantasme !

Le 26 novembre 2012 (14:12) - par Valéry Marchive

Rubriques : Technologie, Sécurité Tags : cyberguerre, Elysées, france, piratage

En sait-on vraiment plus sur le piratage de l'Elysée et sur la posture de la France en matière de sécurité informatique et de cyberdéfense après le dossier spécial de l'Express daté du 21 novembre ? Pas sûr. En tout cas, à de nombreux égards, il continue d'alimenter le fantasme plutôt que d'encourager à une approche pragmatique du sujet.

Le dossier de l'Express sur le piratage de l'Elysée a largement fait parler de lui. Pour au moins une bonne raison : tous les ingrédients du buzz sont réunis. On parle là du sommet de l'Etat, de cette chose dont les arcanes restent obscures pour beaucoup – l'informatique -, de cette autre chose tout aussi obscure et largement fantasmatique que sont les barbouzeries... Le cocktail est détonant et rempli parfaitement son office. Pour autant, force est de constater que, pour l'essentiel, les informations révélées par nos confrères l'avaient déjà été par ceux du Télégramme de Brest. En outre, il faut être objectivement bien naïf pour s'étonner de l'existence d'efforts de renseignement entre alliés, mais néanmoins concurrents dans de nombreux domaines. Et s'il est légitime que les Etats-Unis plaident non coupable des accusations que fait peser sur eux l'Express, ces déclarations méritent assurément la plus grande réserve.

Où un peu de transparence permettrait de sortir du fantasme

Certes, Charles Haquet et Emmanuel Paquette, auteurs du dossier de l'Express, ont consciencieusement enquêté et étayent leurs propos de nombreuses citations. L'anonymat requis ici par les sources de nos confrères ne surprend guère : c'est souvent la règle du jeu pour ce genre d'informations et l'on fait volontiers confiance aux deux journalistes pour avoir su juger du sérieux de leurs interlocuteurs. Mais cela ne suffit pas à exclure une tentative de manipulation. Par les sources elles-mêmes ou par des tiers. Et là, il est évident que quelqu'un a un intérêt à ce que ces informations sortent, dans ce que l'on appelle la grande presse, un peu comme il en avait été du piratage de Bercy, afin de donner un retentissement maximum à l'affaire. La question n'est pas ici de savoir si quelqu'un tire les ficelles, ni qui. Mais l'évocation de Flame, ce super-malware découvert au printemps dernier, peut faire tiquer. Est-ce bien vrai ? N'est-il pas seulement convoqué pour couper court à tout questionnement quant à la véritable sophistication de l'attaque ? Le problème ici est encore une fois, comme pour Bercy, l'absence totale de transparence sur l'incident. Une absence qui fait le terreau de tous les fantasmes et empêche d'aborder le sujet de la sécurité informatique de manière objective, sereine et efficace.

Cyberguerre : sortons du domaine du fantasme !

La sensibilisation, cette grande oubliée

Et le problème est bien là. A cultiver l'opacité en insistant sur la prétendue sophistication des attaques, on en laisse de côté le point clé de l'humain. Certes, beaucoup rêvent d'une sécurité transparente pour l'utilisateur final, et totalement infaillible. Peut-être y parviendra-t-on un jour. Mais à ce jour, on en est loin. Et comme le soulignent nos confrères de l'Express, la porte d'entrée sur le Château fut ouverte par ingénierie sociale. En clair : la victime 0 s'est laissée bernée par un attaquant rusé qui avait bien affuté son discours et préparé son approche. Un autre cas de phishing ciblé. Parce que c'est loin d'être le premier : le phishing ciblé est même le point de départ de nombreuses attaques. RSA, spécialiste de la réponse technologique aux problèmes de sécurité, en sait quelque chose... Et si, à la suite de l'attaque dont il a été victime, il a mis en place des nouvelles solutions technologiques, il a aussi travaillé la sensibilisation de ses équipes et ces procédures internes. Accessoirement, si le phishing et autres arnaques en ligne continuent de faire de nombreuses victimes, c'est bien que les individus sont faillibles. Et l'on peut imaginer que même les plus hauts fonctionnaires de l'Etat le sont; cela n'a rien de dégradant.

Dès lors, insister sur la sophistication des attaques et jouer l'opacité à tout prix a de quoi paraître contre-productif : en tant que société, regardons en face la question de la sécurité informatique et répandons la conscience de la menace. Tout le monde est concerné et un minimum de vigilance n'a rien de superflu. Et peut déjà commencer à faire la différence.

Une France vraiment en retard ?

Et cela paraît d'autant plus important que la cyberguerre n'est pas la guerre de demain : c'est déjà celle d'aujourd'hui (voire d'hier; pour certains, c'était déjà une réalité fin 2009). Et si le renseignement numérique fait encore surtout des dégâts économiques – comme le relève Christophe Barbier dans son éditorial en vidéo -, elle pourrait faire des dégâts matériels et humains dans un avenir proche. A ce propos, les inquiétudes de Patrick Pailloux, patron de l'Anssi, quant à la sécurité des systèmes informatisés de contrôle d'infrastructures industrielles (Scada), apparaissent parfaitement justifiées. Stuxnet, pour ciblé qu'il fut, n'en fait pas moins la démonstration. Alors, oui, la France doit se préparer. D'autant plus que beaucoup d'Etats le font à travers le monde : Israël qui a commencé le recrutement de cybersoldats, les Etats-Unis qui viennent de doter leur ministère de la Défense de la capacité légale de conduire des opérations informatiques offensives et qui seraient à l'origine de Stuxnet/Flame/etc, l'Allemagne qui se dote d'une unité de cyberdéfense offensive, la Chine – dont les capacités réelles font toutefois débat -, le Royaume-Uni, etc. Reste que, pour beaucoup, l'impréparation serait plutôt la norme, y compris au sein des Etats les plus avancés en la matière. Mais là où l'on peut penser que pèche la France, c'est peut-être moins sur l'absence de moyens que sur celle de communication. Encore une fois, l'omerta semble de mise sur le sujet de la doctrine de cyberdéfense nationale. Alors qu'il se disait déjà fin 2009 que le volet offensif de celle-ci venait de franchir une première étape, on en sait encore trop peu à son sujet. Un point que relève d'ailleurs le sénateur Jean-Marie Bockel : pour lui, il faut «s'interroger sur la pertinence de formuler une doctrine publique sur les capacités offensives ».

En complément, sur LeMagIT :

ERP open source

Un ouvrage en profondeur, de 120 pages, au format PDF, qui vous fera découvrir les concepts de l'ERP, une sélection des meilleures...

Toute l'actualité

Cyberguerre : sortons du domaine du fantasme !

Aujourd'hui Sur le même sujet Du même auteur

1. 1.OpenStack In Action : l'OpenStack Foundation vient séduire la communauté française
2. 2.Amazon détaille ses processus d'optimisation fiscale aux parlementaires britanniques
3. 3.Des médias chinois accusent Cisco d'aider à des opérations d'espionnage
4. 4.Débuts difficiles pour Surface ?
5. 5.Marché des serveurs : Gartner confirme la déprime au 3e trimestre
6. 6.Moody's dégrade la note de HP

Les plus populaires

Les plus lus Les mieux notés

1. 1.Cyberguerre : sortons du domaine du fantasme !
2. 2.Linux à Munich : la ville parle de 10 M€ d'économies
3. 3.François Tricot, CEVA, Santé Animales : « Avec notre approche connectée web, nous avons fortement abaissé le coût de possession du poste de travail »
4. 4.Rétropédalage : la ville de Fribourg abandonne OpenOffice pour Microsoft Office
5. 5.Le commutateur virtuel Cisco Nexus 1000v désormais proposé gratuitement