01netPro.

07/12/2012 00:20

Pierre Fontaine, avec AFP

Les entreprises françaises doivent se préparer à des cyberguerres

Les entreprises françaises doivent se préparer à des cyberguerres

Les sociétés françaises son conscientes des dangers du cyberespaces. Le président du Club des directeurs de sécurité des entreprises déclaraient qu'il leur faut se préparer à des guerres cyber informatiques.

Le président du Club des directeurs de sécurité des entreprises (CDSE), Alain Juillet, a jugé jeudi qu'il fallait « se préparer à des guerres cyberinformatiques », plaidant pour un Observatoire commun entre Etat et entreprises pour une *« veille »* commune. *« La France n'est plus en guerre depuis cinquante ans, mais la conquête du cyberespace va mener les peuples à découvrir de nouvelles formes de conflits, il va falloir se préparer à des guerres cyberinformatiques »*, a-t-il déclaré lors du colloque annuel du CDSE, organisé en partenariat avec l'office européen de police Europol.

Un village global à sécuriser

Face à une menace « qui s'annonce systémique, il est nécessaire pour les gouvernants de ne pas se limiter à des effets d'annonces et du saupoudrage de moyens », a-t-il prévenu. Aujourd'hui, selon lui, un *« accident local »* au niveau de la sécurité informatique *« peut générer une chaîne de réactions et un accident intégral »*,c'est-à-dire de portée mondiale. *« Notre devoir est d'anticiper ce genre de crise systémique, d'imaginer une réponse à une crise encore inconnue »*, a-t-il souligné, évoquant la possibilité d'un virus informatique *« beaucoup plus robuste et paralysant »* que Stuxnet, qui avait massivement affecté à l'automne 2010 le programme nucléaire iranien en s'en prenant aux centrifugeuses.

Solidarité = sécurité

Un outil de cyberattaque que certains experts en sécurité, notamment ceux du laboratoire Kasperky, et des journalistes du New York Times ont attribué aux Etats-Unis et à Israël.

M. Juillet a jugé *« indispensable que l'Etat, les entreprises et les organismes mettent en place un Observatoire conjoint de veille et d'analyse »* de la cybercriminalité.

Ce n'est qu'ensemble que nous garantirons une sécurité. Etat comme entreprises, nous sommes tous confrontés aux mêmes risques, selon lui. Il a souligné l'importance *« d'outils de réflexion communs entre Etat et entreprises, une co-production indispensable pour répondre au mieux aux incertitudes futures. Les défis et les enjeux sont énormes, et les réponses encore à découvrir »*,a-t-il résumé.

Les entreprises françaises doivent se préparer à des cyberguerres

Positions franco-françaises

Une position qui n'est pas totalement étrangère au rapport du sénateur Bockel. Lui encourageait une collaboration entre Etat et entreprises, mais sur deux axes principalement. Le premier étant un effort pédagogique, pour former les TPE et PME aux risques du cyberespace. Le second était celui de la collaboration avec les grandes entreprises de recherches et de pointes, tel qu'EADS.

Pour autant, le Sénateur Bockel insistait beaucoup, en politique qu'il est, sur le rôle moteur que devait avoir le pouvoir exécutif dans un tel contexte. En revanche, il ne voyait pas forcément d'un bon œil la mise en place de structures à l'échelle européenne, au-delà de regroupement ponctuel et bipartite. L'enjeu de la cyberdéfense est un enjeu mondial et une priorité nationale, comme l'indiquait le titre du rapport de Jean-Marie Bockel. Une position qui fait sourciller certains acteurs de la sécurité, tel que Check Point, dont le directeur technique européen Thierry Karsenti, nous indiquait récemment lors d'un interview que l'enjeu de la sécurité ne peut être uniquement abordé à l'échelle nationale. L'enjeu étant mondial, le combat est à porter au niveau européen, a minima.