

Extrait du Spyworld Actu

<http://www.spyworld-actu.com/spip.php?article10731>

Open source : la transparence, facteur de confiance

- Informatique - Software -



Date de mise en ligne : lundi 18 mai 2009

Spyworld Actu

Dans [mon dernier billet](#), après avoir demandé à mes collègues pourquoi ils avaient choisi Linux plutôt que Windows ou Mac, j'en étais arrivé à une double conclusion : les gains de productivité d'une part, et le plaisir d'autre part. On avait bien évoqué la notion d'ouverture du code, mais sans pour autant mettre en avant un exemple concret. Coup sur coup, je viens de trouver deux exemples flagrants où l'ouverture du code est essentielle.

La première, c'est l'Etat de Géorgie [qui se méfie de l'antivirus Kaspersky](#), parce que la société est russe et que cela pose des problèmes d'espionnage, compte tenu de la situation tendue entre les deux pays.

Il est vrai qu'un antivirus propriétaire, parce qu'il est connecté à Internet, peut facilement chercher des données confidentielles pour les transmettre à l'extérieur. On notera que ça n'est pas la première fois qu'un logiciel propriétaire est soupçonné d'espionner ses utilisateurs, on se souviendra des soupçons non confirmés envers une [clé bizarrement nommée](#) dans Windows (qu'on attribuait probablement à tort à la sulfureuse agence américaine [NSA](#)) et à la méfiance engendrée par [Skype dans les universités françaises](#).

Le second exemple où la transparence est importante nous est rapporté par Bruce Schneier, un expert en sécurité très en vue aux Etats-Unis. Il concerne un [alcootest électronique](#), dont le code embarqué - propriétaire - s'est révélé de très mauvaise qualité. Le souci, c'est que le détecteur est utilisé par les forces de police dans leur mission. Un défaut dans le logiciel peut mener à des injustices.

Bruce Schneier explique que la transparence offerte par le fait que le code source soit public est essentielle dans cet environnement. On peut citer d'autres exemples, comme les fameuses machines à voter, boîtes noires de la démocratie ([l'Irlande vient de mettre les siennes au rebut](#), faute de fiabilité), ou encore [les mouchards annoncés dans le cadre de la loi Hadopi](#), qui peuvent mener à la coupure d'accès à Internet. Comme l'explique Bruce Schneier, à partir du moment où l'enjeu est important (élections, décisions de justice), il faut être sûr que le logiciel qui aide à la prise de décision soit transparent, et qu'on puisse le compiler soi-même pour être sûr que le code source qu'on analyse est bien celui qu'on exécute. Cela implique en substance que le logiciel en question soit libre.

Bien sûr, tous les fournisseurs ne sont pas prêts à payer le prix de la transparence, ne serait-ce que parce qu'il est parfois inconfortable d'être scruté par les clients, mais nombreuses sont les entreprises qui font le pari de l'open source, parce qu'il permet de toucher plus de clients. Espérons qu'il en soit de même pour tout ce qui touche à la justice et aux élections ! La liberté et la confiance des citoyens sont à ce prix. Tristan Nitot

Tristan Nitot est une personnalité emblématique du monde de l'open source. Il est le fondateur et l'actuel président de [Mozilla Europe](#), connu pour son navigateur Web Firefox. Il est également l'un des initiateurs du projet de documentation libre Openweb.eu.org, qui vise à promouvoir les standards du Web et son accessibilité afin de le rendre utilisable par tous. Tristan Nitot, qui a mené une partie de sa carrière chez Netscape, tient également un blog depuis 2002 sur [Standblog.org](#).

Post-scriptum :

<http://pro.01net.com/editorial/5024...>