



Article de Jacques Bourdeau
Ingénieur en sécurité
ESI Technologies

Les codes sources libres sont-ils sécuritaires ?

De plus en plus d'entreprises envisagent d'avoir recours à des logiciels à code source libre. Du point de vue de la sécurité, de tels programmes confèrent des avantages indéniables.

Mis au point par une communauté de fervents développeurs, ils respectent à la lettre les règles de base de la programmation. Ainsi l'écriture sera bien commentée, la structure simple, et les fonctions éprouvées. Il serait difficile d'en être autrement, puisque des centaines, voire des milliers de personnes sont appelées à manipuler un code donné. Il est donc primordial que les conditions de programmation soient optimisées. Quand ce n'est pas le cas, le problème est vite corrigé par les membres de la communauté.

Au sein de celle-ci, il existe une saine concurrence, qui pousse les développeurs à faire montre de savoir-faire et à placer bien haut la barre mesurant la qualité. Le code étant ouvert, leur travail est exposé à la critique. La contribution de nombreux spécialistes donne lieu à une importante activité de filtrage et de comparaison, de sorte qu'on ne conserve que le meilleur de ce qui est proposé.

Or, qui dit qualité dit aussi très souvent sécurité. Les développeurs de code source libre portent une attention particulière à cette question. Depuis qu'existe le concept, ils se préoccupent de protéger leurs produits non seulement contre les intrusions, mais aussi contre les pannes. De plus, les développeurs de logiciels libres n'accordent normalement qu'une faible marge de manoeuvre à leur logiciel; en général, les droits d'utilisation sont limités au strict minimum, ce qui a pour effet de rehausser le niveau de sécurité. Les logiciels propriétaires, au contraire, ont tendance à octroyer des droits plus élevés afin de limiter les contraintes de programmation.

Des études publiées sur Internet plus tôt cette année, comme celle de Reasoning⁽¹⁾, important fournisseur d'outils de contrôle de la qualité des logiciels, révèlent que les applications à code source libre contiennent en moyenne cinq fois moins de trous de sécurité que les logiciels propriétaires. Cette statistique se base sur le nombre d'erreurs par ligne de code. La robustesse des codes source libres est d'autant plus incontestable que, dans leur grande majorité, les logiciels libres comportent en plus un code substantiellement plus court.

De même, la correction des erreurs trouvées sera beaucoup plus facile et rapide, puisqu'il s'agit de code ouvert. Il est question ici de minutes par rapport à des mois dans le cas de logiciels exclusifs.

Nombre d'organisations hésitent encore à adopter des logiciels à code source libre. Pourtant, il s'agit d'une solution parfaitement viable. En témoigne l'immense succès remporté par le serveur Web Apache, utilisé par plus de 60 % des sites Internet à la grandeur de la planète. Même l'assistance technique - élément comptant pour beaucoup dans les craintes nourries par les entreprises à l'égard du logiciel libre - est offerte à grande échelle par diverses firmes spécialisées en informatique.

Bien entendu, pour tirer parti des avantages que recèle le code libre, il importe de faire une intégration adéquate, de calibre professionnel. Il ne s'agit pas d'une solution miracle pouvant remplacer n'importe quel élément d'un système. Alternative intéressante aux logiciels propriétaires, le code source libre offre de grandes possibilités et une sécurité particulièrement élevée.

(1) Étude métrique sur le nombre de vulnérabilité entre les codes sources ouverts et les logiciels propriétaires :

http://www.reasoning.com/newsevents/pr/02_11_03.html