Hervé Lemaitre, Red Hat : « Avec l'Open Source, les entreprises doivent changer de modèle opérationnel »

« Le problème n'est pas l'Open Source mais la façon dont les entreprises l'appréhendent. » C'est, en substance, le message qu'a souhaité faire passer Hervé Lemaitre (photo), fin connaisseur de l'environnement du Libre en tant que Senior Business Strategist chez Red Hat France. Le responsable a profité de notre article sur les risques que font peser les failles de sécurité des composants Open Source sur les entreprises pour faire le point sur le modèle ouvert. Nous y rapportions le constat dressé par Black Duck Software, fournisseur de solutions d'audit logiciels et de gestion des risques, qui pointait que des problèmes de vulnérabilité touchaient plus des deux-tiers des composants Open Source présents au sein des organisations. Sujet qui a titillé la sensibilité de la communauté Open Source.

En premier lieu, Hervé Lemaitre *« ne conteste pas »* les résultats d'audit publiés par Black Duck via sa structure Cosri (Center for Open Source Research & Innovation). *« On les connaît bien en tant que partenaire, avec qui on travaille sur les questions de sécurité pour du scanning de vulnérabilités dans les conteneurs »*, assure le porte-parole de Red Hat. Qui ajoute que ce constat montre que *« l'Open Source est de plus en plus utilisé et illustre le fait que pas beaucoup d'entreprises sont capables de mettre à jour leurs processus et méthodes pour travailler avec l'Open Source »*. Car, le Libre s'inscrit dans un modèle «□pull□» où c'est la responsabilité de l'utilisateur de s'assurer des mises à jour des composants et de l'application des correctifs de sécurité.

Absence d'historisation du code

Or, si l'Open Source est incontournable aujourd'hui, Hervé Lemaitre regrette que *« beaucoup d'organisations utilisent de l'Open Source communautaire où aucune historisation de l'ancienneté du code n'est assurée »*. Autrement dit, les codes vieux de plusieurs années ne sont pas nécessairement suivis dans le temps par le fournisseur qui l'utilise dans ses solutions. Les exemples de caméras de surveillance et autres enregistreurs numériques connectés attaqués par le botnet Mirai (ou Hajime plus récemment) qui a profité de composants vieillissants et non mis à jour, illustrent parfaitement cette problématique.

D'autant qu'Hervé Lemaitre souligne que les correctifs élaborés par la communauté le sont généralement pour les dernières versions des logiciels. Pas pour les versions plus anciennes. Seules des sociétés de services, comme Red Hat, sont en mesure d'assurer ce suivi historique. *« Quand est apparue la faille OpenSSL (dite Heartbleed en 2014, NDLR), nous avons corrigé la dernière version de notre OS RHEL 7 mais nous sommes aussi remontés jusqu'à la version de 2004 sur RHEL 4*, souligne le responsable. Qui reconnaît que *ce n'est pas facile pour une entreprise de suivre dans le temps la complexité des projets Open Source et des mises à jour. »* D'où la raison d'être de Red Hat qui, armé de 5000 développeurs et de processus industriels de production et diffusion, est capable de mitiger les risques de sécurité en des temps très courts après l'apparition de la faille. *« 92% des 158 failles*

critiques relevés sur RHEL 7 ces trois dernières années ont été corrigées le jour même, illustre notre interlocuteur. *Une seule a nécessité 20 jours, un composant fourni de manière non supporté autour de Java, ce qui fait baisser la moyenne. »*

Tout code à ses failles

Car il reconnaît que *« tout code a ses failles »*. Mais contrairement aux environnements propriétaires, *« elles sont corrigées plus rapidement car détectées très vite. Et le nombre d'attaques zero day est très faible »*. Du moins au sein des entreprises qui assurent un suivi régulier des évolutions logicielles ou qui s'adressent à des fournisseurs de services Open Source. *« Chez Red Hat, on pousse les correctifs*, insiste Hervé Lemaitre. *C'est notre métier d'assurer le cycle de vie des produits. »*

Il n'en reste pas moins vrai que la présence de composants Open Source non patchés font peser des risques sur la sécurité des entreprises. Au même titre, d'ailleurs, que les solutions propriétaires, mais à la différence que les vulnérabilités du Libre sont publiques. Ce qui pose un problème tant que les entreprises ne s'adaptent pas au mode de fonctionnement de l'Open Source en s'impliquant plus dans son développement. *« Il y a toute une éducation à faire*, note Hervé Lemaitre. *Nous poussons les organisations à passer d'un modèle de consommation à un modèle de contribution. »* Chantier énorme que l'évolution de la législation qui, à travers la Loi de programmation militaire (LPM) ou le futur GDPR qui durcissent les exigences de la chaîne de sécurisation, aidera peut-être à mettre en œuvre plus efficacement que jusqu'à présent. Peut-être.

Lire également
L'Open Source fait peser des risques sur la sécurité de l'entreprise
Une faille zero day sur les serveurs Apache massivement exploitée
Black Duck Software fait le point sur les licences 'open source'