



## > Table ronde / Assises de la Sécurité

Monaco, le 13 octobre 2006

### « Ce que l'Open Source a changé dans l'industrie du logiciel et pour la sécurité des systèmes d'information »

Animée par Jérôme Saiz, Journaliste Indépendant.

#### **Participants :**

Sylvère Léger, Responsable de la Sécurité du Système d'Information AGF  
Olivier Guilbert, P-DG d'Idealx  
Hervé Schauer, Consultant en Sécurité des Systèmes d'Information

\* \* \* \*

#### Compte-rendu

L'objectif de cette table ronde a été de tenter d'apporter quelques éléments de réponses autour d'une question centrale : le modèle open source est-il compatible avec les exigences de sécurité des RSSI et opérationnelles des DSI ?

Plus largement cette discussion entre experts a contribué à évoquer le marché de l'open source, la sécurité du SI et le code ouvert, les méthodes de développement, la certification ou encore les bénéfices de l'open source face aux solutions propriétaires.

#### **La maturité de l'offre**

Avant de devenir incontournable, la technologie open source s'est répandue dans le système d'information des entreprises et des administrations sans qu'elles s'en aperçoivent. Depuis, le temps à fait son œuvre et les solutions open source sont aujourd'hui considérées comme de réelles alternatives aux solutions propriétaires. Olivier Guilbert, prend les devants rappelant que le manque d'ergonomie et l'absence de documentation ont été les principaux reproches formulés à l'encontre des logiciels open source. Or ce n'est plus le cas chez Idealx et aujourd'hui les entreprises n'ont plus besoin d'experts car elles peuvent obtenir des solutions packagées. L'offre a grandement évolué et Olivier Guilbert souligne le nombre de projets effectués, y compris en environnements critiques, corroborant la maturité des projets, notamment dans les domaines de l'authentification forte ou de la gestion des identités. Du côté des utilisateurs, il indique que les pionniers furent issus la grande distribution, motivés par la réduction des coûts, vinrent ensuite les administrations qui permirent l'évolution des solutions, suivis par le secteur de l'industrie avec la confiance de grands groupes tels que Total, Areva, Michelin ou Nissan. Aujourd'hui l'éditeur constate une demande croissante du secteur des banques et assurances.

Sylvère Léger RSSI aux AGF a mis en œuvre une solution open source d'authentification renforcée voici bientôt quatre ans. Il précise que si l'open source peut être un choix politique, pour lui ce fut avant tout un choix technologique. Sa motivation pour adopter



une solution de sécurité reposait principalement sur les critères d'évolutivité et la possibilité d'un déploiement maîtrisé, ajoutant : « Aux AGF nous avons de fortes contraintes d'intégration dans un environnement hétérogène et outre l'interopérabilité, nous exigeons également un support sans faille ».

Sur ce point l'open source semble en effet permettre un support adapté à chaque contexte. Hervé Schauer, directeur du cabinet de sécurité HSC, -également membre de l'AFUL, du Cercle européen et de l'OSSIR - dénote l'attitude des éditeurs « propriétaires » qui n'intègrent pas souvent la politique de sécurité d'une entreprise, pour lui seul l'open source le permet. Il précise : « Lorsque vous entendez parler de DRM (Digital Right Management) ou MTP (Mesures Techniques de Protection) vous devez comprendre qu'il y a une politique de sécurité définie par d'autres qui est appliquée à votre insu ».

Tous les participants s'accordent à dire que l'open source est un standard de facto. De part ses qualités intrinsèques, il cohabite aisément sur tous les systèmes. De plus le modèle open source restaure le mode de développement originel des logiciels basé sur la mutualisation. Loin de la politique commerciale de certains éditeurs de logiciels à code source fermé qui visent à enfermer l'entreprise dans un carcan contraignant, l'entreprise bénéficiera au contraire d'une solution standard qui s'intégrera plus facilement à l'existant et dont elle pourra maîtriser le coût, la maintenance et l'évolution.

La mutualisation permet de partager les efforts de R&D entre utilisateurs grâce à un éditeur qui joue le rôle d'intermédiaire et assure la continuité des développements. Sylvère Léger mentionne : « lorsqu'on choisit une solution et qu'on est nombreux à le faire, c'est déjà un gage de pérennité ».

Pour l'éditeur Olivier Guilbert, il ne s'agit plus d'opposer open source et propriétaire mais au contraire de montrer comment l'open source a remis en cause certaines pratiques abusives des éditeurs « pourtant présentées depuis 20 ans comme les pratiques « normales » de l'industrie ».

Le modèle propriétaire se trouve ainsi profondément remis en cause par cette alternative. Ainsi les entreprises ont compris qu'il est possible et utile d'obtenir un accès au code source, que l'on peut imaginer un mode de tarification simple et non liée à la taxation par utilisateur, que leur participation à la définition de la « roadmap » des logiciels qu'ils utilisent est normale.

Il poursuit : « les éditeurs propriétaires ont adopté un modèle proche du système fiscal ! et les entreprises ne sont plus dupes. L'open source se développe rapidement pour être une alternative, voir un premier choix dans l'infrastructure et la sécurité : la pression du marché est très forte pour ouvrir les solutions dans ces 2 domaines ».

Selon l'éditeur la dynamique du marché est telle que plus aucun appel d'offre n'ignore l'alternative open source, ajoutant : « si certaines entreprises sont encore en tout propriétaire, alors c'est qu'elles n'ont pas optimisé leurs budgets et qu'elles dépensent trop inutilement. »

Effectivement on apprend que l'absence de coût de licence par utilisateur permet à Idealex de diviser par 5 le coût d'une PKI dans le cadre de grand projet. Olivier Guilbert regrette cependant que les processus d'achat des grandes entreprises ne soient pas encore adaptés en conséquence. En effet les processus d'évaluation restent très long et très coûteux et malheureusement trop souvent sans rapport avec les coûts et délais de réalisation effective du projet.

De son côté Hervé Schauer laisse supposer que l'idée de la confiance n'est pas possible avec le logiciel à code propriétaire. Pour cet expert le mode de développement des logiciels à code ouvert est idéal pour la sécurité du SI, soulignant : « cela permet un code mieux écrit et plus fiable, que n'importe qui peut auditer ».

En effet l'audit du code permet de valider la sécurité d'un programme et Olivier Guilbert confirme cette nécessité pour les entreprises, citant l'exemple du CEA, qui pour des raisons évidentes, a une exigence absolue en matière d'audit de code.

Sylvère Léger approuve : « Aux AGF le code est maintenu par des experts, d'excellents spécialistes internes. Ils connaissent leur code, c'est eux qui le mettent en œuvre et le font évoluer. »

Au sujet de la certification des pratiques de sécurité du SI ... comme par exemple les certifications des professionnels (CISSP, ProCSSI et ISO 27001 Lead Auditor par LSTI), Hervé Schauer insiste sur l'importance de la formation : « Former et donc certifier les exploitants, avant de penser à certifier la sécurité des logiciels libres ».