

## INTERNATIONAL



[Prochains sommaires](#)

[Abonnements -](#)

[Publicité](#)

[Déposez votre CV](#)  
[Voir les offres d'emploi](#)

Google



Web



Global Security

Rechercher

Flux RSS



## Investigations

## La sécurité au cœur du Forum Mondial du Libre

décembre 2008 par [Marc Jacob](#)

**La sécurité a été un des thèmes abordés lors du Forum Mondial du Libre qui s'est déroulé les 1er et 2 décembre à la Maison de la chimie à Paris. A cette occasion, Matt Watchinski, Senior Director VRT de Sourcefire, avait fait le déplacement. A ses côtés, Jean-François Taltavull, responsable de l'offre produits de Wallix, Eric Leblond, directeur technique, d'INL et Vincent Ducrochet, Pre-Sales Engineer d'Ingres, et Olivier Bouzereau, journaliste, ont débattu sur la sécurité.**



Jean-Noël de Galzain

Jean-Noël de Galzain, organisateur du Forum Mondial du Libre et CEO de Wallix, après le message de bienvenue, a présenté rapidement les intervenants et les enjeux de la sécurité et a lancé le débat sur le thème du passage à l'Open Source.



Eric Leblond, INL, Vincent Ducrochet, Ingres, Matt Watchinski, Sourcefire et Jean-François Taltavull, Wallix

Olivier Bouzereau a dressé un panorama des enjeux de la sécurité surtout dans un contexte de crise économique. Eric Leblond, INL, estime que la crise devrait conduire à un renforcement des politiques de sécurité afin de prévenir, entre autres, les fuites d'information. Pour Jean-François Taltavull, Wallix, estime que les entreprises vont souhaiter obtenir une meilleure traçabilité sur leur SI. Ainsi, toutes les solutions comme l'IAM, les logiciels de collecte et d'analyse des logs... devraient être sans doute de plus en plus déployés dans les entreprises. Il a aussi rappelé que la mise en œuvre d'outils techniques doit s'accompagner de formation et d'information auprès des utilisateurs. En effet, ses derniers sont souvent le maillon faible de la sécurité.

Olivier Bouzereau a déploré que dans l'IT la sécurité ne représente que 4% des budgets alors que, par exemple, dans l'aéronautique le budget sécurité représente 20% des budgets. Il a conclu son intervention en présentant l'initiative réseau de Confiance qui permet à environ 120 professionnels RSSI, fournisseurs, consultants, intégrateurs d'échanger sur les thèmes de sécurité et plus généralement de l'informatique.

Un des auditeurs a rappelé que trop souvent dans les appels d'offres l'Open Source était oublié au profit des solutions commerciales. Eric Leblond considère que passer à des solutions Open Source permet de mieux connaître techniquement le cœur des produits.

Ainsi, il est possible de contrer plus facilement les tentatives d'intrusions malicieuses. Jean-François Taltavull a conclu cette première partie en précisant que le coût des licences du monde libre était beaucoup moins onéreux que celui des systèmes propriétaires.



Matt Watchinski a, pour sa part, présenté le travail de veille des équipes de Sourcefire qui permet d'assurer les évolutions de Snort et de ClamAV. Son équipe a pour objectif non seulement d'améliorer les produits mais aussi de contrer les menaces actuelles mais aussi de faire de la prévision sur les techniques d'attaques de demain. Pour effectuer cette veille, son équipe a de multiples sources d'informations : la communauté Open Source, la publication des vulnérabilités, l'utilisation de honey pots, de botfinders, de webcrawlers... Il a aussi évoqué quelques pistes pour améliorer la sécurité et répondre aux menaces : configuration des systèmes, la vérification et les tests...



Jean-François Taltavull, Wallix, a décrit l'offre technique de Wallix qui propose un UTM pour le réseau et une solution de sécurité de la messagerie. Son offre intégrée est constituée de solutions issues du monde du Libre comme ClamAV, Snort, SpamAssassin... Elle permet de répondre tant aux demandes des grands comptes grâce à une appliance à la PME avec des services d'infogérances. Au niveau technique, la solution repose sur Debian. Pour sa solution de sécurisation de la messagerie il utilise Clam AV, Spam Assassin, Postfix, Postgrey, Amarisd-new, Pyzer. Selon lui, cette solution peut-être déployée en une semaine pour une collectivité de taille moyenne pour un coût d'environ 10.000 euros (hors coût de maintenance). Bien entendu, comme dans toute solution de sécurisation de la messagerie, les réglages fins peuvent prendre environ 1 à 2 mois.



Eric Leblond d'INL a présenté le projet Netfilter. Aujourd'hui, cette solution permet d'obtenir un suivi d'état dans le filtrage. Il offre un historique et un état des connections. Le Projet Netfilter propose un outil IP Tables, un outil de journalisation ulogd, Comntrack. Netfilter est aujourd'hui utilisé dans la plupart des UTM du marché comme les produits Arkoon, Netasq, Fortinet, Wallix, Astaro... Il contient trois outils majeurs : du filtrage de paquets, un traducteur d'adresses et un suivi des connections.

Concernant la solution de filtrage, elle permet d'accepter, de refuser ou encore de mettre les paquets dans une file d'attente. L'outil TARPIT offre la possibilité de ralentir la réception des paquets afin de contrer les actions des spammeurs.

Le traducteur d'adresse est utilisé pour le routage d'adresse. Ulogd répond au besoin de traçabilité. Dans sa version 2 (ulogd2), il permet aussi de suivre le détail des connections en termes de volume et de connaître à partir d'une adresse IP publique de connaître l'utilisateur qui a généré la session.

[< précédent](#)   [suivant >](#)

**LANDesk® Security Suite**  
Détectez les Logiciels Espions  
Téléchargements, Infos, Devis  
[www.LANDeskSecuritySuite.fr](http://www.LANDeskSecuritySuite.fr)

**Protections Électriques**  
Jerlaure Audite, Conçoit & Installe Votre  
Salle Informatique Sécurisée  
[www.jerlaure.com](http://www.jerlaure.com)

**Trend Micro 2009**  
La protection intelligente pour PC  
Téléchargez la version gratuite ici  
[www.trendmicro.e-nettarget.com](http://www.trendmicro.e-nettarget.com)

Annonces Google