

## ECONOMIE : Des remèdes pour contrer les pirates informatiques

**Date de parution:** Mardi 7 novembre 2006  
**Auteur:** Ghislaine Bloch

### **SECURITE. Iris Solution propose un système de surveillance, couplé à une assurance pour protéger ses clients.**

La plupart des entreprises sont équipées en pare-feu et autres antivirus mais le piratage externe ou interne reste problématique. Les pirates ont toujours une longueur d'avance et leurs attaques provoquent d'importants dégâts.

#### Surveillance en continu

Quelques jeunes sociétés en Suisse romande offrent à leurs clients différentes solutions innovantes pour lutter contre le piratage informatique. C'est le cas, par exemple, de la société genevoise Iris Solution, créée en juillet 2006. Ses clients - des PME essentiellement - sont connectés à un centre d'expertise via un boîtier placé entre le modem et le réseau. Ce boîtier analyse le flux Internet et transmet immédiatement ses observations au centre d'expertise. «Il permet par exemple de connaître l'origine du fichier», explique Thomas Noël, cofondateur de la société, aux côtés de Patrick Amon, un physicien qui travaille également à la Chaire de sécurité informatique de l'EPFL, et Thomas Maillart. Un moteur de calcul surveille toutes les incohérences et identifie les fichiers suspects. «Par exemple, si 10% de nos clients téléchargent au même moment le même fichier alors qu'ils ne sont pas localisés au même endroit ou qu'ils ne font pas du tout le même métier, le système d'intelligence artificielle nous alerte de l'anomalie et nous bloquons immédiatement la menace, souligne Thomas Noël. De plus, dès que nous avons identifié une nouvelle attaque et trouvé la solution adéquate, tous nos clients bénéficient immédiatement et automatiquement de ce savoir-faire à travers leurs boîtiers respectifs.»

#### Police d'assurance

Autre originalité du concept: la société propose une police d'assurance pour couvrir le risque résiduel. «Tout préjudice informatique éventuel est remboursé grâce à une police d'assurance, souscrite auprès de notre partenaire Unirisc, un courtier genevois en assurances», note Thomas Noël. Cette assurance permet de rembourser les frais d'intervention en cas d'attaque, les frais de reconstruction des données et les pertes d'exploitation sous-jacentes. Basée au Parc scientifique d'Ecublens, sur le site de l'EPFL, Nexthink édite pour sa part une solution destinée à la sécurité interne des entreprises. «Le risque d'intrusion depuis l'extérieur est limité car les entreprises ont très souvent des systèmes de sécurité satisfaisants. En revanche, le danger provient le plus souvent de l'intérieur de l'entreprise elle-même», souligne Vincent Bieri, CEO de Nexthink. On peut citer quelques exemples: un employé qui ouvre une pièce jointe, qui remplit sans hésiter des formulaires personnels, qui transmet un code confidentiel à un tiers ou qui installe tous les fichiers ou logiciels qu'il trouve. De plus en plus de sociétés proposent des solutions de gestion de la menace interne. Ce marché pourrait d'ailleurs atteindre 1,9 milliard de dollars en 2009, selon le spécialiste des technologies de l'information IDC.

«Nous installons en moins d'une heure un serveur dans le réseau de l'entreprise et équipons les postes de travail avec un logiciel très léger qui observe les différentes interactions entre les utilisateurs et leurs applications. Ces empreintes d'activité sont envoyées au serveur central de l'entreprise qui détecte en temps réel les comportements atypiques», explique Vincent Bieri. Des alarmes liées aux incidents sont envoyées à l'équipe de sécurité qui peut agir de façon adéquate. Un rapport d'audit est transmis au management qui peut mieux mesurer son risque opérationnel. Le procédé d'analyse, conçu par l'un des cofondateurs de l'entreprise, Pedro Bados, émane du Laboratoire en intelligence artificielle de l'EPFL.

Nexthink vend son produit par l'intermédiaire de sociétés de services spécialisées dans la sécurité, à l'exemple de Navixia, LAN Experts ou Sylog Consulting. Celles-ci revendent le produit à des banques, des assurances, des sociétés de luxe ou des hôpitaux. Nexthink compte actuellement seize clients.

#### Nouvelle levée de fonds

La société a réalisé une première levée de fonds en avril 2006, auprès de la société de capital-risque Venture Incubator (VI). Alain Nicod, managing director de VI, a rejoint le conseil d'administration de la start-up. Une deuxième levée de fonds devrait être clôturée d'ici à la fin de l'année pour attaquer de nouveaux pays.

Enfin, il faut encore citer plusieurs sociétés de services en Suisse romande qui effectuent des tests d'intrusion. C'est le cas, par exemple, d'Illion Security. L'entreprise améliore la sécurité informatique de ses clients en les mettant à l'épreuve des mêmes attaques que celles d'éventuels pirates. La société n'hésite pas à voler des mots de passe, télécharger des logiciels de type cheval de Troie ou se faire passer pour quelqu'un d'autre afin d'obtenir des données confidentielles. La société décèle ainsi les failles du système et propose des solutions adaptées aux besoins. «Il s'agit d'une analyse globale du risque. L'opération se fait ponctuellement et s'adresse à des grands groupes, explique Lorin Voutat, cofondateur d'Illion Security. Nous ne faisons pas de la surveillance 24 heures sur 24.»