

# Sécurité: IBM et Cisco s'associent. Phase 2

IBM et Cisco étendent leur alliance sur la sécurité: il s'agit notamment d'intégrer une partie du logiciel de conformité de politique de sécurité IBM Tivoli avec les diverses technologies de commande d'admission de réseau de Cisco Network Admission Control. L'objectif est de »

*garantir la mise en conformité des équipements informatiques (ordinateurs portables, postes de bureau, périphériques sans fil), ainsi que la mise en quarantaine et le dépannage des équipements à risque. C'est le principe des solutions préventives d'autoprotection»* . Il s'agit, pour l'essentiel de solutions préventives d'autoprotection, qui permettent de contrôler automatiquement qui a accès à quoi sur le réseau, sur la base des règles de sécurité de l'entreprise. « *L'environnement informatique actuel est fortement marqué par la mobilité. Il est donc très facile de connecter à l'entreprise des systèmes et périphériques équipés de systèmes d'exploitation obsolètes, dépourvus de pare-feu, présentant des failles de sécurité ou des mots de passe peu sécurisés.* » Cette offre constitue la phase 2 d'un programme de coopération présenté en février dernier. **Mise en conformité, mise en quarantaine...**

L'offre de sécurisation IBM – Cisco, phase 2, est ainsi présentée: -garantie de conformité: IBM Tivoli Security Compliance Manager, travaillant en même temps que l'infrastructure réseau de Cisco, permet aux entreprises d'appliquer et respecter leurs politiques de sécurité. Les outils sondent automatiquement les périphériques qui se connectent au réseau pour identifier les systèmes non conformes. Le logiciel d'IBM détermine si le périphérique est conforme aux politiques de sécurité en vigueur: présence des derniers correctifs du système d'exploitation, mise à jour de

l'antivirus, paramétrage des mots de passe et autres règles personnalisées. -Mise en quarantaine: Cisco Secure Access Control Server (ACS), sous-ensemble de l'architecture Network Admission Control de Cisco, prend la décision d'autoriser ou de bloquer l'accès au réseau. Si le périphérique est déclaré conforme, son utilisateur peut accéder sans problème au réseau. Si le périphérique est déclaré non conforme, Cisco ACS le place dans une zone de sécurité spécifique, comme un réseau local virtuel, pour l'isoler des autres parties du réseau. - Rétablissement de la conformité: une fois que le périphérique est isolé, IBM Tivoli Provisioning Manager peut automatiser de simples tâches, comme inviter les utilisateurs à configurer des mots de passe plus sécurisés, ou des tâches plus complexes, comme l'installation de correctifs pour le système d'exploitation ou d'une mise à jour de l'antivirus. Les clients bénéficient également de l'accès à la bibliothèque OPAL (Orchestration and Provisioning Automation Library) d'IBM, ressource en ligne permettant aux partenaires commerciaux et clients d'IBM de partager des workflows automatisés, comme les processus de mise en conformité de la sécurité. De surcroît, les utilisateurs des ordinateurs portables IBM ThinkPad et IBM ThinkCentre peuvent exploiter IBM Rescue and Recovery Antidote Delivery Manager, une technologie ThinkVantage, pour rechercher des mises à jour dans un référentiel et procéder automatiquement à l'actualisation des périphériques des environnements Windows.

Enfin, IBM Global Services propose des services d'audit pour évaluer le degré de sécurité des infrastructures informatiques et recommander des mesures à prendre.