Novell met les entreprises en garde contre les failles des systèmes d'information

Novell publie aujourd'hui les résultats de son étude *« Threat Assesment »*, qui vise à évaluer les menaces qui pèsent sur les systèmes informatiques. Ces données sont tirées de l'outil de test Threat Assessment Tool, qui permet de mesurer le risque pesant sur le système d'information de l'entreprise. Les résultats sont plus qu'alarmants.

« Les menaces progressent à vue d'œil et tous les jours des données vitales sont perdues. L'enquête 'Threat Assessment' *permet aux entreprises de prendre davantage conscience de leur vulnérabilité. Elle a pour but de les aider à mettre en place les bonnes pratiques pour mieux sécuriser leurs périphériques et protéger leurs données sensibles »*, explique **Grant Ho**, directeur des solutions Endpoint Management chez Novell.

71 % des sociétés interrogées ne chiffrent pas les données de leurs ordinateurs portables, une précaution pourtant nécessaire en cas de vol. **73 %** des sondés ne chiffrent pas non plus les fichiers stockés sur des disques externes. Ce problème devient critique avec les clés USB, qui peuvent être facilement perdues.

Dans **72 %** des cas, les données copiées sur des périphériques externes ne sont pas contrôlées. Ceci mène à des situations inextricables, puisque **73 %** des entreprises n'ont pu empêcher un périphérique non conforme de propager des infections… ou de se voir infecté.

Enfin, la nature des fichiers enregistrés n'est pas précisée dans **78 %** des cas. Des problèmes de diffusion ou de conformité peuvent alors apparaitre. Globalement, **76 %** des entreprises avouent qu'elles sont incapables d'assurer le contrôle des périphériques sortant de l'entreprise.

Des réseaux ouverts à tous les vents

Le constat est encore pire dans le domaine du réseau. **90 %** des sociétés admettent qu'elles ne peuvent empêcher leurs salariés de se connecter à des réseaux externes non sécurisés (bornes Wifi publiques, *etc.*). Ceci réduit à néant toute tentative de contrôle du réseau interne.

Dans l'autre sens, **65 %** des professionnels signalent que des personnes non accréditées sont en mesure d'accéder au réseau de l'entreprise (par exemple en connectant leur machine à une prise réseau).

Dernier élément, encore plus crucial, plus de la moitié des sociétés (**53 %**) ne sont pas en mesure d'interdire l'accès aux réseaux *peer to peer* depuis les postes de travail de l'entreprise. Un risque en terme de sécurité, qui peut se transformer en problème légal en cas de téléchargement illicite, la responsabilité de la société pouvant alors être engagée.

Le Threat Assessment Tool sera un bon point de départ pour permettre aux responsables IT de repérer les faiblesses de leur infrastructure. Novell conseille par ailleurs de disposer de solutions de contrôle des périphériques et du réseau, administrées depuis une console unique.