Enquête Promisec : 'Le risque interne reste une menace considérable'

L'enquête menées sur des milliers d'ordinateurs personnels fait apparaître la prolifération de logiciels non autorisés ou de versions obsolètes, des processus illicites, des failles de sécurité non corrigées… En clair, le bilan de Promisec est bien sombre!

Le document précise que 25.090 PC (13% du parc informatique testé) étaient connectés à des périphériques USB non autorisés, engendrant des risques potentiels de perte de données et d'intrusion de virus dans le réseau de l'entreprise.

Promisec, société israélienne, a mis au point des tests destinés aux grands parcs informatiques, des tests qui durent près d'une heure, après installation d'un logiciel d'analyse, « *Spectator Professional*« , sur un seul poste de travail de l'entreprise.

Une fois l'analyse terminée, le logiciel « mouchard » produit une vue d'ensemble et une étude détaillée des logiciels, des pilotes de périphériques, en discernant ceux qui dérogent aux régles de sécurité .

« Les entreprises sont aujourd'hui mieux armées pour identifier les menaces contre la sécurité de leurs réseaux externes. En revanche, les problèmes de sécurité interne demeurent considérables pour celles qui doivent prévenir la fuite de propriété intellectuelle ou l'infiltration de leurs réseaux ; des codes malveillants peuvent être introduits par inadvertance par des collaborateurs ou des partenaires », commente Amir Kotler, CEO de Promisec.

Les points clés de l'étude : – Sur 7720 (4%) de ces PC étaient installés des logiciels P2P.- 2895 (1,5%) des PC n'étaient pas dotés des plus récents Service Packs de Microsoft- 3281 (1,7%) présentaient des problèmes de maintien d'activité et de mise à jour de l'anti-virus- 2316 (1,2%) étaient dépourvus d'agents de sécurité tiers requis.- Enfin, 1582 (0.8%) comportaient des logiciels de prise de contrôle à distance non autorisés, et une proportion moindre de logiciels shareware non autorisés et non protégés.