

Sécurité : les tablettes catalysent les craintes du consommateur

L'année 2012 est marquée par une recrudescence des menaces virales (BitDefender évoque notamment une forte croissance des *malwares* sur Android, de l'ordre de 6000 %) et des attaques ciblées. Dans ce contexte, moins de la moitié des Français détenteurs de tablettes tactiles estiment leur appareil sécurisé (seuls 41 % pensent qu'il l'est). La tendance est analogue à l'échelle des six pays européens qu'ont parcourus à cette occasion les équipes de Kaspersky.

À l'appui des témoignages de quelque 2478 personnes, dont 415 résidents de l'Hexagone, l'étude de l'éditeur accouche de conclusions évocatrices. Au premier rang des victimes potentielles, les terminaux mobiles, en proie à la consomérisation, revêtent un double enjeu. Et pour cause : quand bien même les DSI n'ont aucun contrôle sur cette flotte de pièces rapportées, il y transite un volume considérable de données d'entreprise.

D'où la nécessité d'une sensibilisation aux [dangers du BYOD](#) (*Bring Your Own Device*), alors que l'année 2011 s'est imposée comme le théâtre d'un florilège d'actes de piratage (Anonymous, LulzSec), de failles 0-day, de réseaux de botnets... mais aussi d'attaques préméditées de longue date, visant des contenus particuliers.

Mettre en place des mesures de protection

Il incombera à l'écosystème des équipementiers et développeurs d'adopter en parallèle des mesures proactives vouées à prévenir les intrusions qui résulteraient de vulnérabilités détectées dans des composantes telles que les logiciels, les nouveaux langages de programmation et les protocoles de communication, l'IPv6 en tête.

À cet égard, intégrer la dimension du *cloud* au sein des solutions de protection semble faire consensus. Dans sa mouture 7.0, [l'antivirus avast!](#) use de ce recours pour systématiser la diffusion des signatures de virus et augmenter la fréquence des mises à jour. En novembre dernier, [Trend Micro mettait en place](#) un service similaire destiné à unifier la protection des parcs informatiques.