Microsoft met Longhorn hors de portée des hackers

- Informatique - Software -

Date de mise en ligne : jeudi 7 juillet 2005

Le prochain OS de Microsoft renforcera la protection des données personnelles et la gestion des droits d'accès.

Microsoft a révélé que Longhorn, son futur système d'exploitation, s'attachera à verrouiller les ordinateurs afin d'éviter les accès non autorisés aux logiciels et aux matériels. Selon Detlef Echert, principal conseiller en sécurité de Microsoft en Europe, différents éléments clés ont été conçus pour améliorer la sécurité dans ce système d'exploitation.

Le verrouillage du matériel grâce à une puce dédiée sera associé à un renforcement des modalités d'accès à la mémoire. La sécurité sera également améliorée via l'utilisation d'une technologie appelée User Account Protection (UAP), destinée à s'assurer que les utilisateurs ne disposent pas par défaut des droits d'administrateur.

Un coffre-fort pour les données personnelles

La sécurisation de Longhorn passera dans un premier temps par l'utilisation de Trusted Platform Module 1.2, une puce développée par l'organisme à but non lucratif Trusted Computing Group et déjà fabriquée par Inifeon, National Semiconductor et Broadcom. Elle servira ainsi de chambre forte pour stocker les identifiants et mots de passe de l'utilisateur.

Ainsi, en cas de vol de l'ordinateur, le voleur ne devra pas seulement le déverrouiller mais également s'introduire dans cette puce pour avoir accès aux informations personnelles. "Si quelqu'un veut essayer, je lui souhaite bonne chance", a déclaré Detlef Echert à VNUnet.com. "Ce n'est pas impossible à réaliser mais cela requiert des outils hautement spécialisés, beaucoup de temps et une certaine dose de chance. [Ce système] protègera les données dans 99 % des attaques."

Pas d'accès administrateur par défaut

La protection des ordinateurs passera également par ce que le représentant de Microsoft appelle le "renforcement du système", qui consiste à limiter les zones de la mémoire sur lesquelles il est possible d'écrire afin d'empêcher des programmes malveillants résidant en mémoire de causer des dysfonctionnements.

Enfin, l'UAP contribuera à la protection des ordinateurs contre les infections virales en verrouillant les droits de l'utilisateur, de sorte qu'un hacker ne puisse pas obtenir un contrôle total de la machine. Etlef Echert explique que tout le monde n'a pas besoin de disposer des droits d'administrateur mais que les développeurs, par facilité, les accordent souvent par défaut. Il sera toujours possible de donner des accès en administrateur sous Longhron mais seul l'accès local sera proposé par défaut.

(Article traduit de VNUnet.com)