

Microsoft s'offre une légitimité en matière de sécurité

L'éditeur de logiciels se penche de plus en plus sur les problématiques de sécurité. Bien qu'il existe des sociétés spécialisées dans ce secteur, le géant américain estime malgré tout avoir son mot à dire.

Au final, cette initiative pourrait être positive pour l'image de l'éditeur, car Microsoft s'est souvent fait épingleur sur des problèmes de sécurité. Ces chiffres sont néanmoins à prendre avec des pincettes.

Microsoft justifie cette expertise par une présence mondiale hégémonique et un retour d'expérience des utilisateurs très important. Interrogé, le groupe précise procéder à l'analyse de près **450 millions de machines par an**.

Les données présentées par Microsoft viennent de deux grandes sources, à savoir l'exécution sur le poste client de deux outils, le Malicious Software Removal Tools (MSRT) et Windows Defender qui protège l'OS de près d'**1,8 million de codes malveillants**.

Premier bilan dressé par l'éditeur, le second semestre 2007 a vu une baisse de 15 % des divulgations de nouvelles vulnérabilités, atteignant ainsi le chiffre le plus bas depuis la seconde moitié de l'année 2005.

Les vulnérabilités demandant un bas niveau de complexité pour être exploitées ont continué de décroître pendant le second semestre 2007. Cela signifie que les failles d'indice « Élevé » divulguées sont plus difficiles à exploiter et nécessitent un certain niveau de spécialisation.

pendant cette année 2007, 32,2 % des vulnérabilités de sécurité (CVE) connues étaient associées à un code malveillant facilement accessible. Ce pourcentage était de 32,7 % en 2006.

En 2007, Microsoft a diffusé **69 Bulletins de sécurité traitant plus de 100 vulnérabilités contre 78 en 2006**. Microsoft note une baisse de 11,5 % du nombre de bulletins de sécurité et de 29,6 % du nombre de vulnérabilités spécifiques en 2007.

Les produits Microsoft sont moins vulnérables

Dixit la firme de Remond, ce constat est particulièrement vrai pour Microsoft Office. Au cours de l'année 2007, le pourcentage de codes malveillants identifiés pour Office 2000 a été de **52,4 %** alors que pour Office XP et Office 2003, ce pourcentage a chuté de **6,6 %**.

Enfin, pour le système Microsoft Office 2007, ce chiffre a été de 11,1 % seulement, ce qui représente une baisse de 41,3 % par rapport à Office 2000.

Entre 2000 et 2007, les codes et logiciels malveillants ainsi que le piratage n'ont constitué que 23 % des notifications de violation de la sécurité enregistrées et n'ont représenté que 13 % des notifications de violation de la sécurité pour la seconde moitié de l'année 2007. Pour le second semestre 2007, la perte ou le vol d'équipement représentait 57 % des violations divulguées.

Les racines du mal

Le phishing est essentiellement un phénomène touchant les pays anglophones. Entre 75 et 80 % des pages de phishing enregistrées par le filtre anti-hameçonnage de Microsoft à un instant de la seconde moitié de 2007 étaient rédigées en anglais, le reste des pages l'étant en majeure partie dans des langues européennes comme l'italien, l'espagnol, l'allemand, le français et le turc.

129,5 millions de logiciels potentiellement indésirables ont été détectés entre le 1er juillet et le 31 décembre 2007 et 71,7 millions ont été supprimés. Ces chiffres représentent une hausse de 66,7 % du nombre total des détections et de 55,4 % des suppressions pour le premier semestre 2007.

Les logiciels de publicité restent la catégorie la plus importante de logiciels potentiellement indésirables pour la seconde moitié de 2007. Leur augmentation a été de 66 %, passant ainsi de 20,6 millions de détections à 34,3 millions.

Le courrier indésirable représente aujourd'hui plus de 90 % des messages électroniques envoyés par Internet. Outre la gêne occasionnée pour le destinataire et la diminution des ressources des messageries électroniques qu'il entraîne, le déferlement de courriers indésirables crée un vecteur potentiel d'attaques de programmes malveillants et de tentatives de phishing.

`/images/d/detecverregion/large.jpg » />`