USA : la note de la cyber-criminalité est salée

Pour mener à bien son analyse de la cyber-criminalité, le FBI s'est penché sur un échantillon de 2066 organisations du Texas, de l'Iowa, du Nebraska et de New York. L'ambition de cette étude est d'améliorer nos connaissances sur les dangers et les incidents ayant touché les ordinateurs du sol américain.

Basée sur un questionnaire de 23 questions, l'étude a été envoyée à un panel de sociétés évoluant dans différents secteurs d'activité. Ce questionnaire s'intéresse aussi bien aux problèmes de sécurité rencontrés par les différents groupes, qu'aux réponses et solutions apportées pour y remédier. Menée dans quatre États, l'enquête a été conduite par les agences du FBI. Enfin, toujours à propos de l'enquête, elle a été conduite de façon à ce que les personnes interrogées puissent y répondre de façon totalement anonyme. Approximativement 24.000 organisations ont reçu le questionnaire. Ces groupes étaient de 430 villes différentes avec des populations variantes, de 1.000 habitants à 8 millions pour New York. Les chiffres fournis correspondent à la période de juillet 2004 à juillet 2005. Toujours concernant la méthodologie de l'étude, plusieurs critères ont permis de choisir les organisations participantes. D'abord, elles devaient totaliser au minimum trois ans d'existence, avoirs 5 salariés ou plus, elles devaient être localisées dans un des quatre États, et enfin, elles devaient réaliser au minimum 1 million de dollars de revenus annuels. Attention tout de même a ne pas confondre cette dernière publication avec celle du CSI/FBI intitulée *« Computer Crime and Security Survey »*, qui a une méthode d'analyse radicalement différente. **Les points clés de l'étude** Tout d'abord, sur les 12 derniers mois, 64 % des sondés souffraient de pertes financières à cause d'incidents de sécurité informatique. Et cela peut s'expliquer par le fait que la plupart des sociétés ont augmenté le niveau de sécurité de leurs réseaux. Mais malgré ces efforts, pas moins de 5000 machines ont été confrontées a des problèmes de sécurité. En moyenne, les sociétés interrogées évaluent le montant du préjudice à 24.000 dollars par an. Si l'on fait le cumul des pertes des 2066 entreprises de l'étude, le montant total de la perte est de 32 millions. Ce chiffre astronomique de 67 milliards correspond en réalité à une extrapolation pour le marché américain dans son ensemble. La somme finale de 67 milliards pour tout le marché américain est donc obtenue par extrapolation, après avoir diminué l'estimation de 64 % d'entreprises touchées à un petit 20 %. Les incidents les plus fréquents sont les vers, virus, chevaux de Troie et autres malwares, avec 12 millions de dollars de pertes causées chez les sociétés étudiées. Et à propos des tentatives d'intrusion, le FBI indique qu'elles proviennent principalement des États-Unis, de Chine, du Nigeria, de Corée, d'Allemagne, et de Roumanie Ensuite l'on trouve le vol d'ordinateurs (3,2 millions), la fraude financière (2,8 millions) et les intrusions réseaux (2,7 millions). 98,2 % des entreprises étudiées ont répondu utiliser un antivirus, 90,7 % un pare-feu et environ 75 % un anti-malware. 84 % des entreprises interrogées ont souffert de virus, 80 % de spywares et 32,9 % de tentatives d'intrusion réseau.