Alcatel et Right Vision feront ensemble du tout-IP pour PME

Huit attaques sur dix contre les ordinateurs de l'entreprise pourraient être bloquées si celle-ci validait l'identité non seulement des utilisateurs, mais aussi des machines qui se connectent au réseau.

C'est la conclusion d'une étude réalisée à la demande de Phoenix Technologies, concepteur de Bios (*Basic Input Output System*), qui a fait analyser les affaires d'attaques de systèmes informatiques suivies par les autorités fédérales américaines de 1999 à 2006. Selon l'étude, les attaques basées sur les log-in dérobés ou détournés par incrémentation (test de codes où un robot incrémente automatiquement sur le numéro ou la lettre suivante) feraient autrement plus de dégâts que les 'classiques' attaques par ver ou virus interposés. Lorsqu'un compte serait pénétré par une personne non autorisée, les dégâts s'élèveraient en moyenne à 1,5 million de dollars, contre 2.400 si c'est un virus qui perce la carapace ! **Le pirate pénètre le système, et après ?** « *Les cyber criminels qui accèdent aux comptes d'un réseau obtiennent les identifiants et mots de passe de diverse manières. En 'sniffant' le réseau, en utilisant des programmes pour 'cracker' les mots de passe, ou encore plus simplement en s'entendant avec un employé*« , a indiqué Dirck Schou, directeur de la sécurité des solutions Phoenix. Il est d'ailleurs commun de voir des collègues de travail partager leurs identifiants et mots de passe, ce qui facilite le travail des personnes malveillantes. On comprend aussi pourquoi la majorité des campagnes de vers et virus visent à obtenir les codes des utilisateurs. Ce qui permet d'affirmer que « *Les virus équivalent à du vandalisme, les introductions non autorisées à du vol*. » En revanche, si six attaquants sur dix n'ont pas de relation avec leurs victimes, ils sont un peu plus du tiers (36 %) à être ou avoir été employés par l'entreprise. L'étude vient ici réfuter l'argument très répandu que la majorité des attaques de systèmes viendraient de l'intérieur ! Enfin, 84 % des attaques proviendraient d'ordinateurs dont la présence sur le réseau n'a pas été validée, et en particulier 78 % d'ordinateurs personnels au domicile. En conclusion, selon Phoenix, 84 % des attaques vérifiées auraient pu être évitées si les victimes avaient été protégées par une procédure d'authentification des machines. Cette démarche consiste simplement à valider si un matériel est autorisé à être présent sur le réseau. Attention, cependant, Phoenix avertit que beaucoup d'entreprises, ou même de responsables informatiques, cachent les attaques dont ils ont été victimes ou minimisent les dégâts réels. Certains chiffres révélés par l'étude pourraient donc être sous évalués?