IBM et la cybercriminalité : le danger vient de l'intérieur

2.700 experts, plus de 100 clients en infogérance, plus de 8 millions de censeurs, et plus de 100 millions d'attaques réelles ou suspectées par mois, IBM dispose d'une vision des menaces qui pèsent sur les IT et de l'évolution de la cybercriminalité.

Le système de classification des menaces d'IBM est sur quatre niveaux. En 2005, les attaques ont affiché quelques pics mais n'ont jamais atteint les niveaux '*haut*' et '*critique*'. En 2005, le spam affiche une légère réduction, en passant de 72 % des e-mails reçus en 2004 à 68 %. Le repli est plus sensible sur les virus. De 6 % d'e-mails vérolés en 2004, ils seraient passés à 2,8 %. En revanche, le phishing enregistre une croissance importante. Après avoir connu un pic en mai, il a repris de plus belle depuis le mois d'août. Il concernait 1 mail sur 304 en 2004, un chiffre qui est passé à 1 mail sur 143 en 2005. Ce qui caractérise l'évolution des attaques en ligne, c'est d'abord qu'elles sont de plus en plus ciblées. Et les victimes sont essentiellement des individus, comme les employés des banques. IBM extrapole pour 2006. « *Le cybercrime profite, il recherche les gains financiers, de l'info à revendre. Il va enregistrer une forte croissance en réduisant les volumes d'attaques pour augmenter la précision des attaques afin de récolter des informations bancaires et des informations stratégiques. Quant aux cybercriminels, ils vont migrer vers les pays où la loi est plus souple, plus conciliante*. Les attaques se dirigent vers le maillon le plus faible. Ce n'est plus le serveur mais l'individu. Qu'il s'agisse du phishing avec l'ingénierie sociale qui laisse croire en des gains et avantages substantiels contre le dépôt de renseignements privés, ou d'attaques de l'intérieur de l'entreprise par malveillance ou par espionnage, **l'individu est le maillon faible**. Quant aux applications, elles créent des risques nouveaux, comme les blogs avec la mise en ligne d'informations confidentielles, les mobiles – « *c'est de l'informatique, ils ont un disque dur dedans* » -, les messageries instantanées ou la VoIP. « *Le risque d'ouverture des applications sur les réseaux est parfois inconsidéré*« . La plupart des problèmes de sécurité sont internes ? employés, stagiaires, intérimaires. « *Les fuites sont causées volontairement par les employés des sociétés* » « *Paradoxalement, si l'accroissement du marché pousse à la consolidation des entreprises de sécurité, nous constatons un foisonnement de créations de petites activités*« . Et du côté des pirates ? Plus de la moitié des personnes qui écrivent des virus sont des salariés, affirment les experts d'IBM. L'approche de la sécurité a évolué, constate IBM. « *La sécurité n'est plus une réponse à une situation anxiogène. C'est une réponse technologique, une anticipation. Nous dépassons la sécurité périphérique. La complexité croissante des équipements informatiques ne peut se satisfaire des solutions de sécurité acquises a posteriori, qui sont source de ralentissements et présentent des problèmes d'intégration*« . « *La sécurité doit être pensée à tout niveau de l'entreprise, c'est la résilience de l'entreprise (?) Elle doit s'impliquer dans les processus, et non plus seulement par les technologies*« . Avec la protection périphérique, il est plus difficile d'attaquer l'entreprise de l'extérieur, et donc les pirates plus ciblent les individus. Mais quel est le coût de la protection, et surtout des attaques ? « *C'est très difficile à évaluer. Beaucoup d'entreprises ne savent pas qu'elles sont attaquées, ou ne veulent pas en parler. Les gens ne se vantent pas ! Le coût de la prévoyance est connu, il est d'un milliard d'euros en France. Quant au coût des attaques, l'objectif d'IBM est d'atteindre un coût nul !*«