Sécurité réseau : gérer les risques, trouver les opportunités

AT&T et le cabinet d'analystes The Economist Intelligence ont mené une étude sur les risques d'intrusion, de piratage, de détournement de biens ou d'actifs via Internet, etc. Il en ressort que les budgets consacrés à la protection ou à la prévention s'inscrivent très nettement en hausse. La sécurité préoccupe. Elle consomme une part grandissante du budget informatique des entreprises, pour représenter aujourd'hui 13% en moyenne contre 9% en 2002. Autrement dit, le seuil critique des 10 %, à partir duquel une approche est considérée comme totalement intégrée dans la stratégie de l'entreprise, est largement dépassé. Explications? 2003 a été l'année la plus meurtrière » en termes d'attaques réseau via Internet. Les chiffres fournis par Computer Economics sont éloquents : les pertes mondiales engendrées ont frôlé les 13 milliards de dollars. Par ailleurs, le centre de coordination du CERT de l'université de Carnegie Mellon, souligne que le pourcentage d'augmentation de ces attaques entre 2003 et 2004 atteint les 68 % !! Outre leur fréquence, elle-même s'accélérant, ces attaques sont aussi caractérisées par leur violence, endommageant aujourd'hui dans un délai très bref de nombreux réseaux et utilisateurs. De viri Les attaques virales continuent de préoccuper prioritairement les directeurs informatiques. Mais, il est intéressant d'observer que d'ici deux ans, si cette préoccupation demeure la principale, d'autres soucis se font jour démontrant la dimension économique que prend la sinistralité informatique. Ce sont en effet les attaques des hackers, les dénis de service et l'espionnage par la concurrence qui connaissent les plus belles envolées à l'horizon 2006, suivies de près par le cyber-terrorisme. La lutte antispam semble, quant à elle, vouée à porter ses fruits d'ici deux ans, cette préoccupation reculant peu à peu. Comme le souligne M. Byrnes du Meta Group : » L'espionnage par la concurrence est probablement une menace plus importante que les virus et les vers. Les gens n'y pensent pas, jusqu'au moment où ils le vivent eux-mêmes. Et même dans cette situation, ils pensent être les seuls dans ce cas « . Or, il n'est pas rare pour un consultant sécurité de voir de nombreux lancements de produits paralysés du fait de la perte des plans d'ingénierie et de la commercialisation simultanée de produits similaires lancés par certains concurrents. L'ennemi dans l'entreprise, c'est l'homme ! 83 % des personnes interrogées considèrent que la plupart des sinistres viennent de l'intérieur de l'entreprise : sabotage interne, espionnage ou erreurs accidentelles. Par ailleurs, la merveilleuse candeur naturelle de l'humain fait que 78 % de ces individus admettent avoir ouvert au cours de l'année une pièce jointe à un e-mail provenant d'une personne inconnue. Ce qui fait dire à Rick Cudworth, responsable de la sécurité et de la continuité d'activité chez KPMG : » Les attaques externes recueillent toute l'attention, mais les brèches internes, tant criminelles qu'accidentelles, sont de loin les plus fréquentes « . La sécurité, un facteur de développement ? Investir en matière de sécurité semble toutefois être une approche permettant dans certains cas de consolider et de réduire les coûts. C'est notamment le cas en matière de : ? provisioning automatisé (l'économie s'effectuant au niveau de son administration et de la réduction induite des délais, source d'une meilleure productivité des équipes) ? Authentification unique (Single Sign On) : laquelle se répand avec la généralisation des annuaires LDAP, le tout facilitant l'utilisation des processus ? VPN (principalement MPLS, donc gérés par les opérateurs télécoms, lesquels apportent une garantie de service sécurisé). Ces réseaux privés virtuels, utilisant désormais des liaisons DSL, remplacent les lignes louées et sont bien moins

onéreux ? filtrage des contenus (aussi bien en matière de messagerie que de navigation Web). Ceci reduisant le temps perdu à se débarrasser du spam ou du surf « buissonnier ». Néanmoins, la situation réelle n'est pas aussi rose. La plupart du temps, les responsables sécurité doivent lutter avec les autres dirigeants en matière d'innovation. Fort heureusement, certaines initiatives tentent de s'assurer que toute proposition de projet identifie non seulement les solutions techniques mises en oeuvre, mais aussi prend en compte les risques directs associés à celles-ci. Les PC étaient fermés de l'extérieur Pour répondre à des besoins de plus en plus complexes en matière de sécurité, de nombreuses entreprises ont recours à l'expertise de prestataires de services. C'est le cas pour 32% des personnes interrogées qui utilisent déjà ou envisagent d'utiliser ces services gérés de sécurité au cours des deux prochaines années et un autre 14% sur le long terme. Toutefois, 70% de ces entreprises sont des PME. Les fournisseurs de services gérés de sécurité ne sont pas l'unique solution pour faire face à l'augmentation des attaques. Parallèlement, on note de nombreux changements en terme de politique de sécurité : * Dans certaines entreprises, les dirigeants des entreprises prennent eux-mêmes en charge les aspects liés à la sécurité du réseau. Dans d'autres, on assiste à la création d'un nouveau poste avec l'émergence de Responsables de Sécurité (CSO) » Chief Security Officer « . Responsable sécurité : un dirigeant comme les autres Cette montée en puissance de la sécurité informatique se ressent d'ailleurs également au niveau des attitudes adoptées vis-à-vis du responsable sécurité. Autrefois parent pauvre de l'informatique, écartelé entre les ressources humaines (dont il dépendait) et l'informatique (qu'il tentait de conseiller), le directeur sécurité est en passe de devenir aussi important que le directeur financier s'il faut en croire éditeur Amoroso, responsable sécurité informatique chez AT&T. Nous lui laisserons la paternité d'une telle allégation, laquelle ne trouve guère de chorus dans les entreprises françaises. Toutefois, il est vrai que la sécurité est désormais considérée comme la composante critique des réseaux d'entreprise. Entrez, c'est fermé ! Ceci induit un curieux paradoxe. La majorité des dirigeants souhaite ouvrir plus avant leurs réseaux à leurs partenaires, clients et collaborateurs. Mais une telle ouverture contribue à la création de vulnérabilités supplémentaires. On s'aperçoit d'ailleurs qu'il existe un lien étroit entre les objectifs technologiques des entreprises et les vulnérabilités de leurs systèmes d'information. Comme le fait remarquer Chris Bryne, vice-président et directeur des services du Meta Group : » Les entreprises développent des projets qui les rendent vulnérables « . Ainsi, plus de 80% des dirigeants interrogés pensent qu'en donnant accès au réseau de l'entreprise aux travailleurs nomades, et en mettant à disposition des données financières et opérationnelles aux employés, leurs entreprises deviennent plus vulnérables, voire extrêmement vulnérables en terme de sécurité. D'où la mise en place d'une batterie de procédures et autres pratiques de sécurité lesquelles, avouons-le, ne favorisent pas franchement l'ouverture. D'autant que si les faire adopter par les fournisseurs est relativement facile (dans la mesure où ils n'ont pas le choix s'ils veulent rester dans la supply chain de l'entreprise), faire de même avec les clients relève souvent du mariage de la carpe et du lapin.