

Information bien gardée, entreprise avisée

La sécurité des systèmes d'information est une nécessité de bon sens pour les entreprises, exposées au vol de données et à la malveillance. Et un avantage concurrentiel pour les premières qui s'en préoccupent.

Par Rémy Février, commandant de gendarmerie spécialiste en intelligence économique, et Joël Ferry, colonel de gendarmerie, commandant la section recherches de Versailles.

Avec une compétition économique mondiale opposant un nombre croissant de pays, l'impact des technologies de l'information, dans une économie de la connaissance où l'information a une valeur intrinsèque majeure, mène à la guerre économique. Celle-ci rend plus cruciale la recherche d'avantages concurrentiels pérennes. Longtemps considérée comme un simple support de la chaîne de valeur de l'entreprise, les systèmes d'information (SI) sont à présent au cœur de l'activité. La mise en place, la gestion et la pérennité d'un SI obéissent à des impératifs de plus en plus complexes. Les réseaux sont soumis à des forces diverses et souvent contradictoires induisant des mouvements dont la méconnaissance peut être très préjudiciable.

Les risques liés à une insuffisante sécurité du SI d'une entreprise sont de deux types : la perte directe d'informations stratégiques et l'atteinte à l'image.

Perte d'informations stratégiques

Alors qu'une gestion optimale du SI devient essentielle,

rare sont les dirigeants de PME qui mettent l'accent sur sa sécurité. Pourtant, les modes de captation des informations depuis les serveurs et postes de travail sont multiples, et quelques précautions de bon sens réduiraient beaucoup les risques liés à l'utilisation d'un SI peuvent être envisagés selon une nomenclature récurrente.

Les postes de travail

Un des points fondamentaux mis en évidence par la grande majorité des études relatives aux SI réside dans la méconnaissance, de la part des collaborateurs, des dangers inhérents à leur utilisation. Seuls les périls connus du grand public et faisant l'objet d'une diffusion médiatique récurrente paraissent plus ou moins identifiés. Bien peu de collaborateurs font le lien entre virus et portail ou messagerie électronique : de nombreux utilisateurs naviguent paisiblement sur la Toile sans imaginer que cette connexion est toujours à double sens, du fait d'un échange permanent de fichiers potentiellement infectés («cookies»). De même, l'utilisation désinvolte d'une messagerie électronique peut s'avérer dramatique pour l'ensemble d'un réseau interne, notamment par le téléchargement d'un code infecté présent dans un pièce jointe ou plus rarement dans le corps du message. Ce code est susceptible de provoquer de graves dysfonctionnements dans l'ordinateur cible, de se propager à l'ensemble du réseau, voire d'ouvrir une porte dérobée par laquelle son auteur pourra prendre à distance le contrôle du poste de travail. La conjonction de ces deux utilisations peut devenir

dramatique lorsque le salarié communique, sur un site commercial par exemple, l'adresse de messagerie qui lui a été affectée par son employeur, alors qu'elle peut être détournée au détriment de l'entreprise.

Les « nomades »

Le large succès de l'ordinateur portable en fait une cible de choix. Les portables contiennent souvent des données de première importance, mais la menace n'est pas toujours évaluée correctement. Les efforts de protection des SI sont insuffisants : la plupart portent prioritairement sur le réseau physique interne. Les formalités de mise à disposition d'un ordinateur portable auprès d'un collaborateur se limitent souvent à la signature d'une décharge qui exonère le service informatique de toute responsabilité ultérieure et au choix d'un mot de passe personnel.

Le récipiendaire devrait, au minimum, se voir spécifier l'ensemble des dangers relatifs au vol de son matériel informatique (il faut toujours le conserver à portée de vue en cas de déplacement) ou à l'interception de ses données, ainsi que la nécessité de définir un mot de passe suffisamment long et complexe pour éviter une intrusion rapide dans le système.

Les réseaux sans fil

Le WiFi (*Wireless Fidelity*) constitue une ressource de plus en plus employée dans les entreprises : sa facilité d'utilisation et la mobilité qu'il autorise en font un moyen plébiscité par les utilisateurs. Néanmoins, de par leur nature (ondes radioélectriques), dans le cas d'entreprises de taille modeste, la pénétration des réseaux WiFi alimentés par des connexions particulières est assez simple.

La détermination de la clé de chiffrement « WEP » d'un émetteur WiFi prend, en moyenne, quelques minutes, même avec des clés de 128 bits. La maîtrise des outils nécessaires, accessibles depuis n'importe quel moteur de recherche, est à la portée de n'importe quel utilisateur un peu opiniâtre. Bien que surtout répandue comme support de téléphonie mobile, la technique Bluetooth peut ponctuellement faire l'objet d'interceptions, au travers de failles mises en évidence sur certains téléphones – souvent rapidement colmatées par les constructeurs lors de mises à jour des systèmes d'exploitation.

Les installations physiques

Pour autant, il serait erroné de considérer que seuls les matériels liés à l'utilisateur final sont vulnérables : les réseaux internes proprement dits peuvent constituer des cibles, au travers de failles logicielles ou matérielles : « pare-feu » sous-dimensionné, absence de véritable politique de gestion des mots de passe (changements réguliers et retraits des codes personnels des salariés ayant quitté l'entreprise sont indispensables), manque de sécurité du portail de l'entreprise...

L'usage du réseau

Le réseau est organisé de telle sorte qu'avec la convergence des systèmes les courriers électroniques échangés par les salariés au moyen d'un ordinateur de poche (*PDA*) peuvent donner lieu à captation d'informations permettant de connaître la stratégie ou les avancées techniques d'une entreprise.

Atteintes à l'image

Les autres risques liés à la sécurité défaillante d'un SI sont les atteintes à l'image ou à la réputation d'une entreprise. Le détournement d'un site constitue une arme redoutable dans une lutte opposant des groupes de pression ou ONG à des entreprises, pour les activités industrielles ou commerciales de celles-ci. Si ce type d'attaque est souvent limité à des enjeux médiatiques et sociétaux, il n'en demeure pas moins que n'importe quelle entreprise peut subir une campagne de dénigrement du fait d'une altération de l'intégrité de son SI.

La mondialisation de l'économie, conjuguée à la nécessité de préserver des parts de marché – a fortiori dans un contexte de ralentissement de l'activité – peut pousser des acteurs peu scrupuleux à franchir les limites de l'acceptable en termes de concurrence. L'atteinte à l'image d'une entreprise peut résulter d'une action malveillante visant l'un de ses responsables, qui aura bien du mal à prouver son innocence, tant il est vrai qu'il reste toujours un doute dans l'esprit du public. Que penser de l'envoi au directeur général d'une société de courriers électroniques contenant des images pédophiles ? L'image institutionnelle d'une entreprise et de ses marques commerciales, porteuses d'années d'efforts soutenus en communication, est très vulnérable en cas de menées concurrentielles agressives.

Responsabilité des dirigeants

Depuis plusieurs années, les tribunaux manifestent la volonté de responsabiliser les entreprises et leurs dirigeants, en ne s'intéressant non plus seulement à la faute, mais aussi aux personnes qui auraient pu l'empêcher. C'est la remise au goût du jour de la vieille notion, en droit civil, de « *bon père de famille* ». L'effet recherché est de pousser les dirigeants d'entreprise à prendre conscience du caractère indispensable que revêt la sécurité des SI et à utiliser toutes ressources à leur disposition afin de les protéger. Tel est le cas de la protection des traitements de données à caractère personnel.

La désignation d'un directeur de la sécurité des SI ne suffit pas à dédouaner les dirigeants de leurs responsabilités : le fait de déléguer une tâche ne fait pas disparaître l'obligation qu'a l'employeur de contrôler, au sens du Code civil, la légalité des actes commis par ses collaborateurs. De même, l'utilisation du matériel

informatique à disposition des salariés accordée à titre privé et sur le temps de travail ne l'exonère pas de sa responsabilité de surveillance au sens de l'article 1384 alinéa 5 du Code civil. (TGI de Marseille, 11 juin 2003). Il revient au dirigeant d'insuffler une véritable politique de sécurité des SI dans l'entreprise, et de faire en sorte qu'elle bénéficie d'un fort appui du haut encadrement, afin de susciter par capillarité l'adhésion de l'ensemble des collaborateurs.

La fréquente absence de précautions particulières, dans les entreprises, autour des systèmes d'information, corrélée au nombre et à la diversité des menaces potentielles, fait que l'entité économique soucieuse

de protéger son système dispose d'un avantage concurrentiel indirect. Cet avantage est susceptible non seulement de lui permettre de pérenniser son activité en cas de crise majeure, mais aussi d'éviter des mises en cause médiatiques très préjudiciables. Toutefois, l'acquiescer n'est envisageable qu'à partir de la définition et de la mise en place d'une politique de sensibilisation de l'ensemble des salariés de l'entreprise. A défaut, tout effort en matière de réduction des risques de perte d'informations stratégiques demeurera d'une efficacité illusoire.