Arnaque Informatique

THIERRY MORIN

La fraude informatique a déjà sa légende. Au début de l'été dernier, une bande de gamins astucieux fait trembler le monde informatique américain. Ils se nomment eux-mêmes le groupe 414, chiffres qui sont ceux de l'indicatif téléphonique de leur ville. Armés d'un simple micro-ordinateur et d'un modem, ils se sont mis en tête de pénétrer à distance, grâce à la connexion ordinateur-téléphone, dans toutes les banques de données dont ils pourront forcer la porte. La tâche s'avère beaucoup plus aisée que prévu. En quelques semaines, les 414 percent les défenses d'une soixantaine de banques de données privées ou publiques. Quand ils sont arrêtés par le FBI au terme d'une enquête difficile, un vent de panique souffle sur les responsables informatiques de tout le pays. Si des gamins peuvent se jouer des systèmes de sécurité, des pirates mal intentionnés sont capables de faire des ravages.

A tel point que le FBI a décidé de réagir. A la mi-octobre, les policiers fédéraux ont lancé toute une série de perquisitions dans plusieurs villes des Etats-Unis et procédé à de nombreuses saisies après avoir démasqué plusieurs groupes de visiteurs d'ordinateurs. A Irving (Californie), les domiciles de quatre adolescents ont ainsi été fouillés et les agents fédéraux y ont saisi pour plusieurs milliers de dollars de matériel électronique. Des descentes semblables ont eu lieu à New York, Tucson (Arizona), à Oklahoma City et à Détroit (Michigan). Dans cette dernière ville, le chef d'un petit groupe composé de jeunes gens de 14 à 17 ans

WAR GAMES :

« c'est techniquement possible » nous déclare le général Quentin,

chef de la Division Informatique et Recherche Opérationnelle de l'Armée de Terre.

CIC

avait pris le nom de guerre de « sorcier de l'Arpanet », du nom d'un réseau de communication informatique utilisé par le Pentagone. Selon la mère d'un des jeunes gens, le FBI reproche aux jeunes pirates d'avoir pénétré par effraction des banques de données en principe inaccessibles comme celles du Massachussetts Institute of Technology, du Centre de recherche nucléaire de Los Alamos et de la base aérienne de Mc Clellan en Californie.

Quelques années plus tôt, un employé astucieux d'une grande banque américaine fait verser par ordinateur sur son compte tous les dixièmes de centimes qui sont produits par toutes les opérations de la banque dont le résultat ne tombe pas juste (calculs d'intérêts, agios, etc.) et qui n'apparaissent pas sur les bordereaux. Comme le nombre des opérations effectuées est immense, ces infimes ruisseaux financiers forment une grande rivière d'argent détourné.
Une des actions les plus spectaculaires de détournement de fonds a eu lieu récemment à Londres. Des pirates ont pu se brancher sur la ligne téléphonique d'un banquier et connaître ainsi le code de procédure de virements. L'équivalent de 780 000 £ en pièces d'or sud-africaines a été ainsi viré sur un compte factice.
Ces anecdotes parfaitement réelles sont aussi constitutives de la mythologie de la piraterie informatique. Le cinéma s'en est emparé. Dans « War games », film qui sort ces jours-ci en France, une bande de gamins pénètre dans un ordinateur de la défense nationale américaine aux risques de provoquer une guerre mondiale. Dans « Superman III », Richard Pryor campe un surdoué de l'informatique qui entre dans la carrière criminelle en appliquant la tactique des dixièmes de centimes. Ces représentations de fiction ont instillé dans l'opinion, et même parmi certains professionnels, l'idée que les systèmes informatiques sont aussi vulnérables au piratage que puissants dans l'exercice de leur fonction de traitement.
Il est un fait que la criminalité informatique progresse à grands pas, sans doute au rythme même de développement de l'équipement en ordinateurs des sociétés et des particuliers. Les spécialistes sont bien incapables de donner du phénomène une mesure précise : par définition, la fraude bien faite n'est pas détectée ; très souvent, les victimes qui réalisent leur infortune préfèrent garder le silence de peur d'altérer leur crédit auprès du public : la vulnérabilité de l'ordinateur tient d'abord à la négligence de ceux qui les possèdent. les fraudeurs peuvent beaucoup. Mais les parades techniques existent, et dissuadent la plupart des attaques quand elles sont correctement mises en œuvre.

A Irvine, Californie, le 14 octobre dernier, quatre adolescents tenaient une conférence de presse dans leur école de Woodbridge pour expliquer comment avec leur micro-ordinateur ils sont parvenus à pénétrer un réseau informatique payant. Wayne CORRCIA, 17 ans, Gary KNUTSON, 15 ans, Greg KNUTSON, 14 ans et David HILL, 17 ans, ont ainsi expliqué à la presse comment et pourquoi le FBI est venu confisquer leurs micro-ordinateurs et du matériel électronique à la suite d'une plainte posée par une société californienne. Cette dernière avait été facturée de plusieurs milliers de dollars par la société exploitant le réseau. Les enfants n'ont d'ailleurs pas été arrêtés.
Pour les seuls États-Unis, le montant des escroqueries à l'ordinateur a été évalué à 300 millions de dollars...
AFP

« C'est techniquement possible, mais on ne le fera jamais, commente le général à la sortie de la salle de projection de « WAR GAMES ». La philosophie du film est véridique. Le réalisateur et les auteurs du scénario ont certainement travaillé avec des militaires, car de nombreuses scènes du film sont proches de la réalité. Mais, contrairement à ce qui se passe dans le film, il est exclu que les militaires laissent la chaîne complète du commandement à un ordinateur : entre la prise de renseignement, l'exploitation, la décision et l'action, nous glissons des verrous de sécurité. De la même façon, un intrus ne pourra pas avec son micro-ordinateur « entrer » sur les réseaux militaires car nous n'avons pas de connection automatique, avec le réseau public, dans des domaines aussi sensibles.

WAR GAMES (sortie en France le 14 décembre) est l'histoire d'un adolescent féru d'informatique qui modifie le programme de l'ordinateur de la Défense nationale américaine en s'amusant à ce qu'il croyait être un jeu vidéo. Et c'est le chaos ! On se dirige tout droit vers une guerre nucléaire. Conscients du drame, David, 17 ans, et son amie Jennifer vont réussir à éviter (à la dernière minute...) la catastrophe.

Alors ? WAR GAMES serait-il possible ? « Non ! c'est tout à fait impossible », se sont exclamées les autorités du NORAD (North American Air Defence Command) lors de la sortie du film aux U.S.A. Nous ne croyons pas à la possibilité d'intervention d'un micro-ordinateur sur les systèmes informatiques de la Défense nationale ».

Et pourtant, quelques semaines plus tard, la très sérieuse revue de l'« U.S. Navy » publie l'article de deux lieutenants de la Navy qui expliquent comment ils ont accédé à différents systèmes informatiques de la Défense américaine, parvenant même à en contrôler entièrement l'ordinateur à l'aide d'un micro-ordinateur personnel : « Il est possible d'accéder à tous les systèmes informatiques, même les plus secrets », affirment les deux informaticiens de l'U.S. Navy.

Le général Quentin, chargé d'organiser l'ensemble du système informatique de l'Armée de Terre, est beaucoup plus nuancé. « Si WAR GAMES est techniquement possible, il ne s'agit que de l'extrême limite de ce qui pourrait être envisagé, raconte-t-il. Les jeux de simulation que nos militaires suivent à l'Ecole de Guerre ne sont pas très éloignés dans leur principe de ceux de WAR GAMES. Quant au problème de la conception des logiciels de grande dimension, il n'est toujours pas résolu. A partir du moment où celui qui a conçu le programme a disparu, il est pratiquement impossible de prendre sa place. C'est ce que l'on voit dans le film avec le rôle du professeur Falken.

Les attaques de l'intérieur

Selon des statistiques américaines, plus de 80 % des fraudes recensées sont le fait de personnes travaillant dans l'entreprise.
Il peut d'abord s'agir d'un simple détournement de temps machine. Un salarié utilise l'ordinateur de l'entreprise pour ses besoins personnels. Plusieurs ingénieurs informaticiens ont ainsi monté leur propre cabinet de conseil ou de traitement de données en détournant à leur profit des heures machine.
La deuxième catégorie d'infraction ressort du vol banal. Un employé s'empare d'informations contenues sur les bandes informatiques de l'entreprise, soit en partant le soir avec une ou deux bandes sous le bras soit en les copiant discrètement. Il faut toutefois disposer d'un

accès facile aux ordinateurs. Un très grand nombre d'entreprises voient ainsi des informations confidentielles tombées entre les mains de leurs concurrents. La pratique est particulièrement répandue dans le secteur de la vente par correspondance. L'Etat français lui-même ne dédaigne apparemment pas d'y recourir. Rappelez-vous l'histoire des comptes en Suisse !
Si l'on en croit d'ailleurs la Tribune de Lausanne, ces listes viennent d'un piratage électronique dont aurait été victime l'Union de Banques Suisses.
Les compagnies d'assurance sont tout aussi friandes de fichiers. A Denver aux Etats-Unis, plusieurs compagnies ont été récemment inculpées d'obtention illégale de renseignements. Elles utilisaient les services d'un réseau de vol informatique qui pillait systématiquement les fichiers des hôpitaux de la ville.

Les nouveaux Arsène Lupin

Le vol d'informations prend même un tour dramatique si un salarié parvient à s'emparer d'informations vitales pour la survie de l'entreprise, et à en détruire toutes les copies. Il est alors en mesure d'exercer un chantage destructeur sur sa compagnie en menaçant de détruire ou de divulguer le dernier exemplaire. On imagine facilement qu'une entreprise voyant disparaître son fichier clients, sa comptabilité et son plan de développement à moyen terme soit prête à mettre le prix pour les récupérer.
Certains fraudeurs se contentent d'emprunter des sommes immatérielles pendant quelques heures à leur employeur pour les jouer sur tel ou tel marché spéculatif. La pratique n'est pas rare dans les charges d'agents de change et les équipes de cambistes. L'établissement de dossiers fictifs dans le fichier de tel ou tel organisme est une méthode elle aussi très populaire. Un employé de l'ANPE s'était ainsi constitué plusieurs dossiers de chômeur indemnisé, et touchait un nombre porportionnel d'allocations mensuelles. Il est aussi possible aux informaticiens de gonfler leur feuille de paie, ou celle d'un salarié complice.
Dans tous ces cas, les techniques utilisées par les fraudeurs n'ont rien de particulièrement spectaculaire. Les gens de l'intérieur sont par définition habilités à utiliser le système informatique de leur société. Il existe certes des systèmes de mots de passe qui interdisent l'accès de telle catégorie d'employés à telle fonction de la machine. Mais le fraudeur bénéficie souvent du manque de discrétion qui préside à l'utilisation des mots de passe. Il dispose aussi de tout le temps nécessaire pour chercher à deviner les mots de passe de ses collègues ou supérieurs hiérarchiques. C'est la raison pour laquelle les spécialistes de sécurité informatique préconisent l'utilisation de techniques plus sophistiquées. « *La défense la plus efficace* », explique M. Brignogne, responsable de la société de conseils Protexarms, « *c'est la journalisation des transactions.* » On ajoute dans la machine un programme qui garde la trace de toutes les transactions effectuées dans une journée. Le voleur peut toujours agir, mais il prend le risque de laisser dans l'ordinateur une trace qui permettra de l'identifier très vite. Le système peut être complété avec des indicateurs de vraisemblance. On détermine pour chaque type d'opération (versement de salaire, paiement d'indemnités, opérations de change, etc.), un montant vraisemblable de la transaction.
Si une transaction anormale est effectuée dans le programme une alarme se déclenche. Le service responsable de la sécurité peut alors réagir et détecter une fraude éventuelle, défense qui reste toutefois insuffisante. Elle doit généralement être doublée par une restriction des droits d'accès à l'ordinateur. On réserve alors la possibilité technique d'effectuer certaines opérations aux seules personnes directement concernées. Joël Lebidois, un des meilleurs spécialistes français, qui préside la société de conseil « Infoscript », explique qu'il deviendra vite nécessaire d'affecter à chaque opérateur des mots de passe variables constamment remis à jour par la machine en fonction du type de transaction et du moment où elle est effectuée.

La signature, parade infaillible

Le contrôle d'idendité réalisé par la machine peut même aller beaucoup plus loin. Les ordinateurs reconnaissent sans difficulté les empreintes digitales de l'utilisateur. Mais les responsables informatiques hésitent à recourir à cette arme absolue en raison de sa connotation trop policière. Ils préfèrent se tourner vers la méthode dite de la « signature dynamique ». Un ordinateur peut difficilement reconnaître le graphisme d'une signature. Il peut en revanche, identifier avec une marge d'erreur insignifiante une signature au moment où elle est effectuée. La vitesse du stylo sur le support, la pression de la pointe aux différents endroits du paraphe fournissent une structure stable et unique que la machine peut reconnaître entre mille. De plus en plus, les opérateurs en informatique devront signer leurs transactions et donc leurs méfaits éventuels. L'arme est très dissuasive.
Toute cuirasse a son défaut. Le rétablissement d'un niveau de sécurité acceptable face aux attaques internes ne pose pas de problème technique ou financier insurmontable. La journalisation des opérations connue aux alentours de 250 000 F pour un système moyen. La dépense est supportable si on la compare aux dommages immenses qu'une piraterie bien menée peut causer à une entreprise. En revanche, les défenses deviennent soudain très perméables face au danger potentiel que représente un service de maintenance pénétré par des individus mal intentionnés.
Organisé généralement par le constructeur pour ses clients, le service de maintenance intervient sur une machine dès quelle est victime d'une défaillance technique. Rien n'est plus facile pour lui que de truquer un programme ou d'ouvrir une brèche dans les défenses de l'ordinateur, dans laquelle des complices de l'entreprise utilisatrice pourront s'engouffrer. A cela une seule parade : sélectionner de la manière la plus stricte qui soit le personnel de maintenance. Si l'on en croit les spécialistes, peu de constructeurs ont franchi le pas.

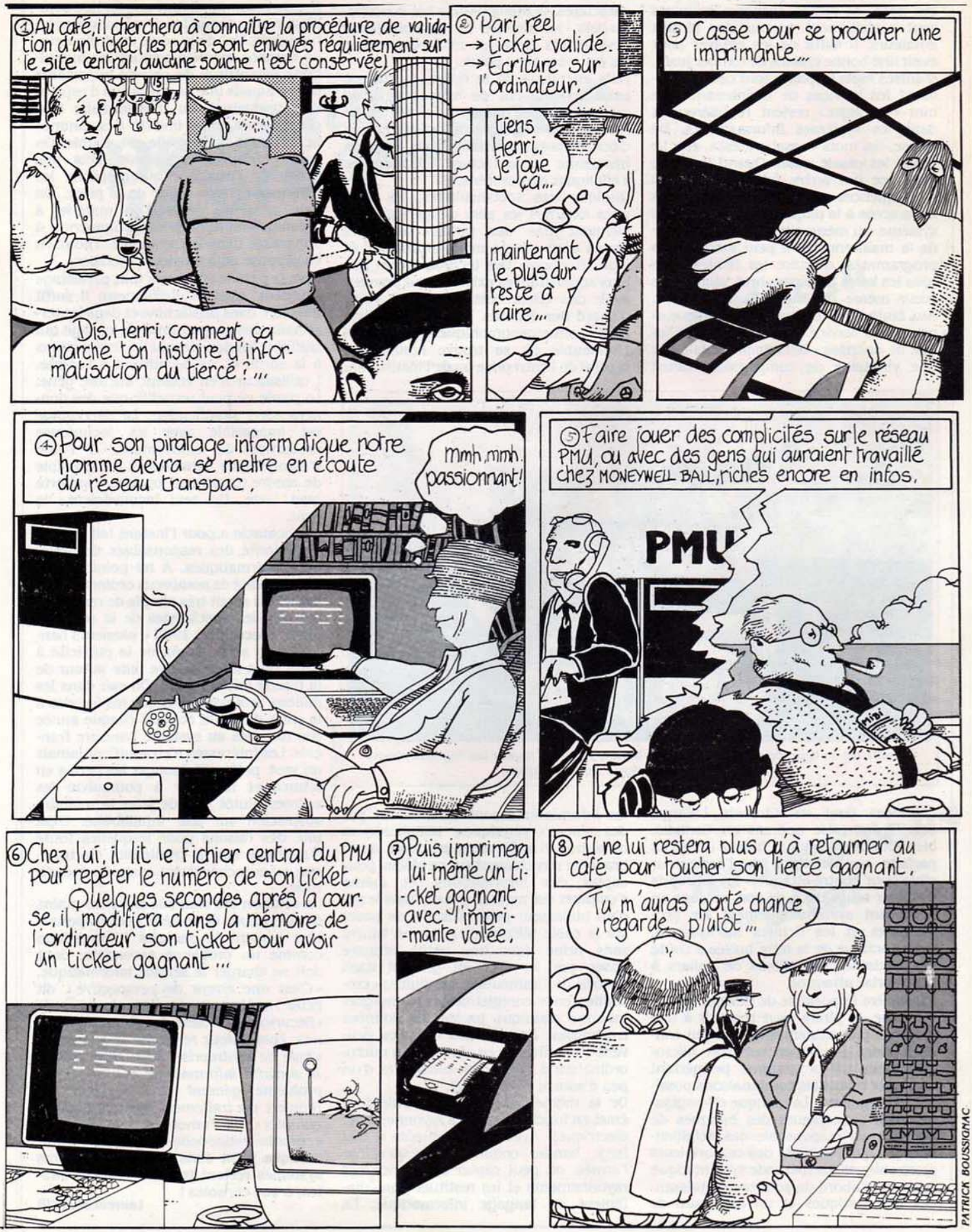
La pression et la vitesse de la signature sont enregistrées sur cette table de contrôle.

Les attaques extérieures

Il y a quelques années, un groupe d'adolescents habitués du centre informatique du Palais de la Découverte ont provoqué une belle panique en pénétrant par effraction dans les fichiers ultra-protégés de l'ordinateur IBM. La technique utilisée par ces monte-en-l'air d'un nouveau genre se ramène toujours aux mêmes constantes. Ils disposent d'un micro-ordinateur relié par un modem au réseau téléphonique. Ils peuvent donc appeler sans difficulté le numéro de telle ou telle banque de données, comme le fait un utilisateur habilité. Une fois en contact avec le système, ils doivent préciser leur identité en donnant un mot de passe en principe connu des seuls utilisateurs. La méthode la plus simple consiste bien sûr à se faire communiquer le sésame par quelqu'un de l'intérieur. La discrétion n'est pas encore entrée tout à fait dans les mœurs des utilisateurs : un mot de passe divulgué se répand comme une traînée de poudre. Il existe aux Etats-Unis des groupes d'amateurs qui font circuler les mots de passe, généralement par le biais de réseaux télématiques reliant entre eux les micro-

TICKET GAGNANT

L'arnaque informatique, c'est bon pour faire trembler les mâcheurs de chewing-gum, pensez-vous. Pas de ça au pays du béret, de la baguette et du tiercé. Du tiercé ? Tiens, tiens ! Oyez plutôt l'histoire de Marcel-la-débrouille, qui n'a pas son modem dans sa poche...



PATRICK BOUSSIGNAC

ordinateurs domestiques. On peut ensuite chercher à deviner ces codes d'entrée. Il y a des mots de passe secrets connus comme le loup blanc. Toto, 007, big boss, et autres surnoms courants sont parfaitement connus des pirates amateurs. Il suffit de les essayer pour avoir une bonne chance de tomber juste. D'autres mots de passe sont ceux qu'utilisent les services de maintenance. Le mot « manager » revient régulièrement dans les systèmes informatiques. De même, les mots « essai », « test », etc. Le pirate les essaie aussi. Quand il tombe juste, ce qui arrive fréquemment, les conséquences sont désastreuses. Il a alors accès à la plupart des fonctions du système, au même titre que les hommes de la maintenance. Il peut modifier les programmes, détruire les fichiers, lire tous les mots de passe, bref, plonger au cœur même de l'institution attaquée. Aux Etats-Unis, un groupe de pirates surpris par le service de sécurité de la banque de données « Data Pack » (à laquelle une vingtaine de compagnies étaient abonnées dont les Ciments Lafarge, société française opérant au Canada), bien loin de prendre la fuite a utilisé sa parfaite connaissance de l'ordinateur cible pour contre-attaquer. Il a entrepris d'effacer toute trace de son passage en détruisant systématiquement les programmes et les fichiers du système. Cette tactique de la terre brûlée a coûté des centaines de milliers de dollars à l'entreprise attaquée.

S'il s'avère impossible de deviner le mot de passe, le pirate peut recourir à une méthode plus systématique. Le jeu consiste alors à réaliser sur son micro-ordinateur un programme permettant d'essayer toutes les combinaisons possibles (War games). Le manque d'imagination des concepteurs des banques de données est responsable des défaillances plus que l'habileté des cambrioleurs électroniques. La méthode systématique suppose d'abord de solides connaissances informatiques et un minimum de renseignements sur le système attaqué et notamment la longueur et la structure des mots de passe en vigueur. S'il s'agit de mots de passe à deux, trois ou quatre caractères, la manipulation est possible. Au-delà, le nombre de combinaisons devient très élevé. Un micro-ordinateur les énumère sans peine.

Mais en raison de la durée de chaque essai, et souvent de la nécessité de recomposer le numéro de téléphone (coupure automatique de la ligne en cas d'échec après un certain délai), le temps nécessaire et la facture téléphonique s'allongent démesurément.

Quoique très spectaculaires, les attaques externes les plus dangereuses ne viennent pas des pirates amateurs armés d'un simple micro-ordinateur et d'un téléphone. Des techniques un peu plus sophistiquées existent, qui peuvent avoir des effets destructeurs. Il s'agit d'abord des écoutes. Dès qu'un utilisateur se situe géographiquement hors de l'immeuble où se trouve l'ordinateur central de l'entreprise ou de l'institution, les informations sont acheminées par des réseaux physiques, téléphoniques ou autres. Il suffit alors au pirate de se brancher directement sur ce réseau pour capter des informations, et même s'emparer des mots de passe. Dans le cas d'un utilisateur privé, il suffit de poser sur le câble téléphonique (qu'on trouve sans peine dans une petite armoire posée par les PTT en général dans l'entrée de l'immeuble), des pinces « crocodile » pour enregistrer sur un magnétophone classique toutes les données transmises. Ensuite, ces données peuvent être affichées en clair sur un micro-ordinateur à l'aide d'un modem et d'un peu d'astuce (voir figure).

De la même manière, tout ordinateur émet en fonctionnant des rayonnements électriques. Avec des récepteurs à très large bande, comme ceux qu'utilise l'armée, on peut capter à distance ces rayonnements et les restituer immédiatement en langage informatique. La méthode est déjà beaucoup plus coûteuse : l'appareil en question est fort onéreux.

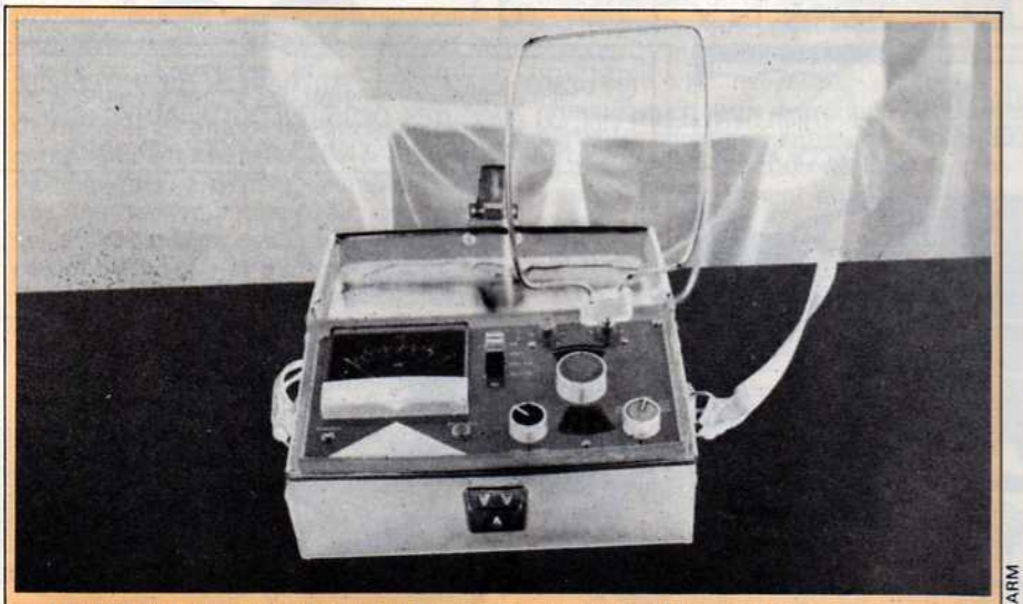
On sort dans cette hypothèse de la fraude courante. Il faut une équipe complète et une compétence technique pointue pour piller de la sorte un ordinateur. La menace inquiète surtout les institutions détentrices de secrets importants pour lesquels une organisation d'espionnage industriel, ou d'espionnage tout court, serait prêt à investir des sommes importantes. Le remède est double. On peut enfermer l'ordinateur dans une « cage de Faraday », qui empêche les rayonnements de sortir de la pièce. On peut aussi se doter d'un matériel à rayonnement limité, qui commence à apparaître dans le commerce. Thomson en propose déjà plusieurs modèles.

Mais la parade absolue à tout parasitage extérieur, c'est le chiffrement. Il suffit d'inclure dans la machine et dans les terminaux des programmes de codage qui chiffrent les données ou les transactions à la sortie et les déchiffrent à l'entrée. L'utilisateur n'en ressent aucune gêne. Le pirate ne peut recueillir que des données sans signification. Le décryptage est impossible avec les techniques modernes de chiffrement. A l'aide d'algorythmes variables, il est possible de rendre totalement opaque n'importe quel texte. Un seul inconvénient : le coût.

Cet obstacle a pour l'instant fait reculer la majorité des responsables de systèmes informatiques. A tel point que la vulnérabilité de nombreux ordinateurs, à laquelle il serait très simple de remédier, inquiète les spécialistes de la sécurité. Après « Securicom 1983 », plusieurs banquiers se sont plaints de la publicité à leurs yeux intempestive faite autour de la fraude informatique. On sait dans les milieux professionnels que les fraudes à la carte de crédit coûtent chaque année des fortunes au système bancaire français. Les intéressés n'en soufflent jamais un mot, préférant éponger les pertes en silence et renoncer à poursuivre les escrocs plutôt que de jeter la moindre suspiscion sur leur infaillibilité. C'est une des raisons pour lesquelles toute statistique sur la criminalité électronique est entachée d'une complète incertitude.

La solution est bien sûr entre les mains des directions de société. « Les responsables traitent la sécurité informatique comme un problème secondaire dont doit se charger le service informatique. *« C'est une erreur de perspective »*, dit Peter Hazelzet un des organisateurs de « Securicom », *« dans les firmes modernes, l'ordinateur renferme la substance vitale de l'entreprise. Pour cette raison, la sécurité informatique est en fait un problème général d'organisation qui requiert un traitement systématique et complet »*. La France est loin de cette approche rationnelle. La sécurité informatique y est dans l'enfance. Les gros systèmes restent très vulnérables. Pirates, à vos consoles !

Laurent JOFFRIN



PROTEXARM

A l'aide de ce type de récepteur à large bande, on peut capter les rayonnements émis par les équipements informatiques.