SÉCURITÉ INFORMATIQUE

numéro 25 juin 1999

SÉCURITÉ DES SYSTÈMES D'INFORMATION

100 millions d'amis sur le NET ?

éditorial

Faire avancer la science, produire des savoirs, enrichir la connaissance, ouvrir de nouvelles perspectives de progrès, telles sont les finalités des recherches qui s'accomplissent quotidiennement dans nos laboratoires en se nourrissant des échanges qu'entretiennent nos chercheurs avec la communauté scientifique internationale. Peut-on pour autant distribuer, à quiconque les demande, les résultats de l'innovation scientifique ou le détail des techniques ayant permis de les obtenir ? Assurément non, lorsque l'innovation en question est susceptible de devenir, entre des mains étrangères, un atout de compétitivité qui va se retourner contre nos intérêts, ou, bien pis, entre des mains malveillantes, une menace pour la sécurité ou la liberté d'êtres humains.

C'est pourquoi, dans chaque établissement public de recherche scientifique, un «Fonctionnaire de sécurité de défense» est particulièrement chargé de la protection du patrimoine scientifique et technologique dans les échanges internationaux. Jusqu'ici, sa mission a surtout consisté à veiller, dans certains domaines scientifiques sensibles, à ce que les coopérations internationales et les séjours de chercheurs étrangers dans nos laboratoires ne créent pas les conditions de transferts inopportuns de savoir ou de savoir-faire.

Mais, compte tenu du développement rapide des réseaux et systèmes informatiques, et avec la banalisation des outils et procédures d'attaque de ces derniers, ceux qui convoitent nos découvertes disposent désormais de moyens bien plus sournois pour se les approprier. Nous sommes ainsi confrontés à des formes nouvelles d'investigation, de recueil, voire d'altération ou de destruction de données scientifiques à l'endroit même où elles sont établies et conservées. Ces attaques font de plus en plus partie de véritables plans stratégiques de mainmise sur la production et la circulation de la connaissance.

Il appartient à chacun d'entre nous de déjouer ces manœuvres en commençant par déterminer, parmi les données qu'il entrepose dans des mémoires électroniques, celles qui méritent d'être protégées et à quel degré ; en leur appliquant ensuite les mesures de protection idoines ; en respectant enfin, dans l'esprit comme dans la lettre, les consignes et chartes de sécurité en vigueur dans son unité de recherche. Dans cette longue chaîne qui relie les acteurs de la recherche, ne soyez pas le maillon faible dont la rupture compromettrait les fruits du travail de tous.

Jean-Jacques Sussel

Haut fonctionnaire de défense
auprès du ministre de l'Éducation nationale,
de la Recherche et de la Technologie

La protection du patrimoine scientifique

pourquoi et comment?

La notion de protection du patrimoine scientifique et technologique est apparue il y a 700 000 ans lorsqu'un «homo erectus», ayant découvert l'usage du feu pour se chauffer, se nourrir et durcir la pointe de son épieu, se demanda s'il fallait en faire profiter les cavernes voisines au risque de voir des imprudents provoquer un incendie dévastateur de la savane nourricière.

Cette interrogation étant toujours d'actualité, quelles raisons peut-on avancer pour ne pas mettre les découvertes de la recherche scientifique entre toutes les mains ?

Pourquoi protéger la production scientifique et technologique ?

- Éviter l'apparition de menaces nouvelles contre la liberté et la sécurité de nos concitoyens, lorsque l'appropriation de la découverte peut aider un Etat, qui ne nous veut pas que du bien, à développer et perfectionner sa panoplie guerrière. Les thèmes scientifiques sensibles sont ceux qui peuvent conduire à la technologie des armements nucléaires, biologiques, chimiques ou conventionnels ainsi que leurs vecteurs et leur environnement opérationnel.
- Contribuer à la prospérité de notre économie, lorsque l'appropriation de la découverte est susceptible de compromettre la compétitivité de nos entreprises et d'y détruire des emplois. L'espionnage scientifique et technologique fait partie de ce qu'on appelle «l'intelligence économique», activité qui occupe de plus en plus les services de renseignement traditionnels et des officines privées. Les thèmes sensibles sont ceux qui peuvent conduire à des applications industrielles, et notamment ceux qui sont financés par des contrats de recherche passés avec des entreprises. Peuvent également être considérées comme sensibles les études à caractère politique, économique ou sociologique dont la divulgation prématurée serait contraire aux intérêts nationaux.
- Veiller au respect de l'éthique scientifique, lorsque l'appropriation de la découverte pourrait créer de nouveaux risques pour l'humanité et son environnement. Les thèmes sensibles sont ceux qui ont fait ou pourraient faire l'objet de prises de position restrictives par les instances nationales d'éthique.
- Assurer la protection de la vie privée, lorsque des fichiers scientifiques contiennent des informations nominatives que leurs propriétaires ne tiennent pas à voir révélées. Tout fichier nominatif doit *a priori* être

suite page 3

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Vers un monde sans lois ?

Christian Harbulot dirige actuellement l'École de guerre économique[1] fondée en 1997 par Jean Pichot-Duclos, Benoît de Saint-Sernin et lui-même. Cette École, unique en Europe, propose un enseignement sur les méthodes d'attaque et de défense auxquelles sont confrontées les entreprises dans la compétition économique mondiale. Christian Harbulo vient de publier avec Jean Pichot-Duclos un ouvrage[2] capital sur les techniques de conquêtes commerciales utilisées par certains «compétiteurs» internationaux : «encerclement des marchés», contrôle de l'information et de «l'industrie de la connaissance», etc., techniques qui s'écartent quelque peu du «laisser faire, laisser aller» qu'ils professent par ailleurs. Il a accepté de répondre à quelques questions.

Sécurité informatique : *Vous critiquez dans votre livre la vision purement défensive que nous avons en France de la protection du patrimoine. Quelle pourrait être une vision plus offensive pour le monde de la recherche ?*

Christian Harbulot : Avant de répondre à cette question, il me semble nécessaire de cadrer le débat. De 1917 à la fin de la guerre froide, les rapports de force géoéconomiques ont été passés volontairement sous silence par les pays occidentaux. Cette *omerta* visait à ne pas affaiblir ou décrédibiliser le bloc de l'Ouest en révélant au grand jour ses divisions internes. Une des dernières manifestations de ce type d'impasses nous est fournie par la récente publication de l'ouvrage de M. Couteau-Bégarie[3]. Dans ce traité sur la stratégie ne figure aucune analyse sur le poids de l'économie dans les rapports de force entre puissances. La notion défensive de la préservation du patrimoine d'un pays résulte de cette approche purement militaire et géopolitique du conflit.

Avec une telle grille de lecture, il est difficile, voire impossible, de décoder des stratégies offensives dont la finalité est à dominance géoéconomique. Le cas du Japon est sur ce point exemplaire. Confronté au XIXe siècle à une menace de colonisation américaine, l'empire du Soleil Levant a cherché à sauvegarder son indépendance en relevant notamment le défi du développement industriel. Cette stratégie de préservation de l'intérêt de puissance n'est pas le fruit de la main invisible du marché. Sous la conduite de l'empereur, les élites nipponnes ont inventé ce que l'Américain Edward Luttwak définit aujourd'hui comme une économie de combat. Cette démarche a permis au Japon de combler son retard et de se hisser au deuxième rang mondial en dépassant la Grande-Bretagne et la France qui étaient au début du siècle à la pointe de l'économie mondiale.

S.i. : *Le Japon a donc eu une doctrine offensive en matière de politique de recherche ?*

C.H. : Tout pays dont le développement est dépendant d'une politique de conquête commerciale se doit de tirer le maximum d'avantages dans sa collecte globale de renseignements, d'informations et de connaissances. La recherche scientifique n'échappe pas à la règle. Les États-Unis déploient depuis 1945 des stratégies, élaborées en amont, de maîtrise et de contrôle des flux de connaissances. La première bataille qui a été perdue par l'Europe dans ce domaine a été celui de la communication scientifique. Le chercheur qui veut valoriser ses travaux doit publier en anglais. Le monde de l'édition anglo-saxon est devenu le point de passage obligé pour acquérir une notoriété internationale. Ce processus n'est pas *gratuit*. La masse de connaissances d'origine européenne qui transite ainsi par les Etats-Unis donne à ce pays un avantage non négligeable en amont de la compétition économique mondiale.

S.i. : *Vous dites que «le contrôle de l'information», aussi bien par le contrôle des «tuyaux» que par celui des contenus est un objectif stratégique des États-Unis. Face à la domination technique des États-Unis, la France a-t-elle des cartes à jouer ?*

C.H. : Absolument. Les Français ont géré le Minitel comme une technologie innovante. En revanche, les Américains développent Internet en pensant à la pérennité de leur prédominance économique. Les standards informatiques anglo-saxons développés sur le moyen et long terme et la conception du réseau Internet constituent un autre verrou sur lequel les Européens n'ont pas guère de prise. À quoi sert la réflexion européenne sur la propriété intellectuelle si les Américains appliquent une autre réglementation sur les licences d'exploitation des logiciels informatiques ? C'est la question cruciale que soulève Philippe Baumard dans sa réflexion menée sur le code 2B[4]. L'innovation liée au commerce électronique n'est pas dissociable des enjeux concurrentiels sous-tendus par son développement. Dans cette compétition où le rôle des États est loin d'être secondaire, les milieux français de la recherche ne sont pas dispensés d'avoir une vision stratégique sur l'avenir de l'industrie de la connaissance. C'est d'autant plus important que les entreprises françaises abordent pour l'instant cette question en se préoccupant surtout des tuyaux et très peu de leur contenu.

S.i. : *Vous analysez dans votre livre les stratégies «d'encerclement» et de «contournement» des marchés. En quoi consistent au juste ces stratégies ?*

C. H. : Les élèves de l'École de guerre économique ont été sensibilisés cette année sur le cas de l'Ukraine. Un représentant de l'Agence de Développement de l'Alsace est venu leur expliquer comment les Américains opèrent dans cette région du monde. C'est l'organisation non-gouvernementale *US Aid* qui fournit les statistiques fiables sur le pays. Au bout du troisième rendez-vous, les chefs d'entreprise alsaciens ont devant eux un interlocuteur lié directement ou indirectement à des intérêts américains. Plus de deux mille personnes sous passeport diplomatique d'outre-Atlantique sillonnent la zone alors que les forums de discussion anglo-saxons sur Internet déconseillent de faire du business en Ukraine. L'élaboration des nouvelles sources d'information, la sensibilisation des élites locales aux standards éducatifs occidentaux, le pilotage de l'agence de privatisation sont des démarches qui peuvent déboucher sur ce qu'on définit dans notre jargon comme une stratégie d'encerclement de marché.

Contrairement aux apparences, ce concept d'encerclement de marché n'est pas si abstrait. Il suffit de lire la presse. Le procès engagé contre Microsoft a donné une tribune à ses concurrents pour dénoncer les pratiques offensives du numéro 1 mondial des logiciels informatiques. Les avocats de Bill Gates ont d'ailleurs expliqué qu'il était difficile de se maintenir à la tête du marché mondial sans se battre par tous les moyens. Dans cette compétition qui sort des affrontements classiques produits/marchés, la recherche est devenue une cible de choix. Sur un marché aussi évolutif que l'électronique et le multimedia, une innovation développée par un chercheur ou une start-up peut renverser très rapidement le cours des choses. L'industrie américaine s'est donné les moyens d'identifier en moins d'un an toutes les innovations émergentes afin de pouvoir en bénéficier (apport de capital risque, rachat, débauchage d'ingénieurs...) ou éventuellement de la contrer.

S.i. : *Votre livre est très sévère vis-à-vis de la politique américaine. En France, tout est idéologie, dès qu'il s'agit des États-Unis, on est immédiatement classé en «anti» ou en «pro». N'est-il pas possible d'étudier la géopolitique mondiale et*

1. École de guerre économique : 1, rue Bougainville - 75007 Paris. Pour plus de renseignements, consulter http://www.ege.eslsca.fr/default.htm
2. *La France doit dire NON*, Christian Harbulot et Jean Pichot-Duclot, Plon, 1999.
3. Editions Economica, 1999.
4. Philippe Baumard, «L'article 2B du nouveau code de commerce uniforme : une prédation sur la plus grande industrie du XXIe siècle». *Revue française de géoéconomie*, volume 2, n° 8, janvier 1999.

d'essayer d'y placer les intérêts à moyen et long terme de notre pays, sereinement, sans obligatoirement avoir à se situer dans un camp ou dans l'autre ?

C.H. : Je préfère le qualificatif de lucide plutôt que celui de sévère. Dans la longue histoire de la mondialisation des échanges, une puissance n'a jamais eu pour principe de faire de cadeaux à ses rivaux potentiels. Il en va de même aujourd'hui. Les États-Unis n'ont aucun intérêt à voir l'Europe ou l'Asie les dépasser économiquement. Une compétition loyale ancrée à l'idéal démocratique relève encore du mythe. Autrement dit, la classification en «anti» ou «pro» américain est un faux problème qui souligne simplement le niveau du débat en France. La complexité du monde post-guerre froide renforce la nécessité d'une maîtrise totale des enjeux stratégiques. Chaque épisode en est l'illustre démonstration. Nous étions alliés des Américains durant la guerre du Golfe. Ils ont été ensuite nos plus farouches adversaires dans les répartitions de contrats militaires et civils conclus à l'issue de ce conflit avec l'Arabie Saoudite ou le Koweit. Je me souviendrai toujours de cette interview donnée à deux journalistes du magazine *L'Expansion* par Yves Sillard, alors PDG du groupe Défense Conseil International. Il rappelait la visite de courtoisie que la plupart des intermédiaires de l'industrie d'armement française avait reçue aux lendemains de la défaite de Saddam Hussein. Des personnes proches d'une agence fédérale américaine leur ont proposé le marché suivant : désormais soit vous travaillez pour nous, soit vous allez connaître de grosses difficultés...

S.i. : *Vous situez «les enjeux» économiques dans le cadre des Nations. La bataille aujourd'hui n'est-elle pas plutôt à l'échelle des «grands ensembles régionaux» ?*

C.H. : L'émergence des blocs économiques comme l'Union européenne n'a pas fait disparaître l'échiquier des intérêts nationaux. L'agriculture, l'énergie nucléaire, l'aéronautique, le spatial, les télécommunications, la banque sont encore vécus par les instances de décision nationales comme des *territoires* à défendre contre des démarches prédatrices d'origine étrangère. Certains pays ont donné d'autres dimensions à la défense des intérêts économiques nationaux. M. Reich, conseiller du président Clinton lors de son premier mandat, plaidait pour le maintien sur le sol nord-américain de certaines élites indispensables au développement des nouvelles technologies ou du secteur défense, mais aussi de nombreuses entreprises de la Sillicon Valley. La délocalisation de ces activités au Mexique, pays partenaire de l'ALENA, n'était pas à l'ordre du jour et ne l'est toujours pas... Les récentes dispositions prises par M. Allègre pour aider les chercheurs à créer leur propre entreprise tiennent compte de ces impératifs.

S.i. : *Vous parlez finalement très peu d'Internet. Pourtant les États-Unis, qui y contrôlent à la fois les «tuyaux» et les «contenus», ne se sont-ils pas donné là un atout fantastique pour maîtriser l'information à l'échelle de la planète ?*

C.H. : Vous avez raison. C'est une des lacunes du livre. Mais ce sujet mérite un livre à part entière car il couvre un champ stratégique à têtes multiples. Le contrôle en amont de la circulation des connaissances est un enjeu que nous résumons en France par des formules comme *Big Brother* ou *1984*. Une fois de plus, notre attention se focalise avant tout sur la défense des libertés individuelles. Mais il est impossible de réfléchir sur un tel thème sans croiser celui-ci avec d'autres sujets de réflexion comme la préservation des intérêts de puissance. La surveillance des voies de circulation de l'information sous toutes ses formes est une des préoccupations majeures des États-Unis d'Amérique. Un tel système de surveillance ne se limite pas à la lutte contre les ennemis de la démocratie. Il intègre les autres niveaux de rapports de force, en particulier dans le domaine économique.

Si la bataille des tuyaux semble bien mal engagée, celle du contenu peut être encore gagnée. La création de connaissances sur Internet est un défi à la portée de la nation qui a été à l'origine du siècle des Lumières. Dans cette vaste compétition générée par la société de l'information, le CNRS et les professionnels de l'éducation sont en première ligne. Mais rares sont celles ou ceux qui étaient habitués, jusqu'à présent, à analyser la production de connaissances sous l'angle de la confrontation géoéconomique. Cet aspect du problème ne doit pas être délaissé, sous peine de faire courir le risque à l'industrie française de la connaissance d'être confinée dès sa naissance au statut peu enviable de l'exception culturelle.

Christian Harbulot
Directeur de l'École de guerre économique
1, rue Bougainville, 75007 Paris
tél. : 01 45 56 91 12 - fax : 01 45 54 00 02
christian.harbulot@ege.eslsca.fr

La bibliographie des œuvres publiées par C. Harbulot est consultable à http://www.ege.eslsca.fr/biblio_ch.html

suite de la page 1

déclaré et protégé et, à plus forte raison, lorsqu'il traite de populations présentant certaines particularités (médicales, sociologiques, historiques...).

Que protéger ?

Il n'est pas possible, au niveau d'un organisme comme le CNRS, de publier un répertoire détaillé des thèmes scientifiques à protéger. Le temps nécessaire pour recueillir, trier, présenter et diffuser cette somme d'informations rendrait ce document largement obsolète au moment même où il arriverait sur les paillasses des laboratoires. Il n'est pas plus envisageable de le mettre sur WEB, qui offre pourtant d'intéressantes possibilités d'actualisation en temps réel, car l'accès direct à un tel catalogue faciliterait par trop les investigations des prédateurs potentiels.

C'est donc à chacun d'entre vous, chercheur, ingénieur, technicien, de réfléchir sur l'information que vous confiez au disque dur de votre ordinateur. Chaque fois que vous introduisez de nouveaux fichiers dans votre machine, vous devez vous poser trois questions :

– L'information contenue dans ce fichier mérite-t-elle d'être protégée au vu d'une des quatre raisons détaillées plus haut ?
– Pendant combien de temps faut-il la protéger ?
– À quel niveau de sécurité faut-il la protéger ?

Prenons l'exemple de la publication scientifique qui est la raison d'être du chercheur. Pendant toute son élaboration, et jusqu'au moment où vous la soumettez à un éditeur, ne serait-il pas regrettable qu'un petit malin vienne vous chiper ce qui en fait l'originalité afin de vous prendre de vitesse ? S'il s'agit de la découverte du chaînon manquant entre l'*homo habilis* et l'*homo erectus*, seule votre renommée en pâtira ; s'il s'agit de la molécule-miracle pour maigrir avant l'été, dommage pour les royalties que le CNRS et vous-même pourriez en retirer ! Gardez donc en lieu sûr votre prochaine communication. Après sa parution, vous pourrez la laisser traîner où vous voudrez (avant de la mettre sur une page WEB, assurez-vous cependant que l'éditeur ne s'y oppose pas).

Comment protéger ?

Vous venez de déterminer que telle ou telle part de votre production scientifique comportait des «informations sensibles» et méritait un traitement particulier pour en préserver intégrité et la confidentialité. Plusieurs procédés sont utilisables, et c'est en les additionnant que vous aurez les meilleures chances de ne pas être pillé.

suite page 4

suite de la page 3

Les sauvegardes

L'information scientifique stockée sur le disque dur de votre machine n'est pas exposée qu'aux seules attaques de pirates, qu'elles viennent des antipodes ou du bureau voisin ; elle peut aussi être altérée ou détruite accidentellement, par la maladresse d'un utilisateur, par un incendie, une explosion ou une inondation. Il faut donc la sauvegarder dans un endroit sûr et à bonne distance de votre lieu de travail. La fréquence à adopter représente le temps que vous acceptez, *a priori*, de consacrer à la reconstitution de l'information détruite. Comme support, il existe des disques de 1 à 2 Go, qui tiennent dans la poche d'un veston, et dont l'acquisition avec le lecteur *ad hoc* ne représente qu'un ou deux jours de «coût budgétaire moyen d'un chercheur».

La protection de votre machine

Si vous ne voulez pas que n'importe qui vienne fureter dans vos fichiers, quelques précautions élémentaires et complémentaires sont à prendre :

- Interdire l'utilisation de votre machine, lorsque vous vous absentez momentanément, par un mot de passe (bien choisi et caché) pour clavier, économiseur d'écran, mémoire flash, mémoire prom...
- Couper l'alimentation électrique de votre machine lorsque vous vous éloignez plus longtemps, et notamment pendant la nuit, les week-ends et les jours fériés, périodes où les pirates se montrent particulièrement entreprenants.
- Enregistrer vos fichiers sensibles sur des disques extractibles ou sur des lecteurs externes que vous mettrez sous clé dès la fin du travail.
- Fermer et verrouiller les portes et les fenêtres en quittant votre laboratoire ou votre bureau.

La protection du réseau interne du laboratoire

Pour déjouer les attaques venant de l'extérieur et même de l'intérieur, il faut une architecture structurée et cohérente, combinant prévention et sécurité active pour réaliser trois fonctions :
– Le filtrage des accès et des services.
– La journalisation de l'activité.
– L'authentification forte par carte à puce.

Il est spécialement important de contrôler rigoureusement – et même de limiter – les droits d'accès attribués aux utilisateurs du laboratoire, surtout quand il s'agit de visiteurs temporaires, invités, étudiants ou stagiaires.
Lorsque vous vous connectez sur le réseau de votre laboratoire depuis une installation extérieure, sachez que votre login et votre mot de passe transitent en clair. Si vous le faites depuis un pays étranger, ils peuvent être interceptés et réutilisés pour des connexions illicites. Si vous ne pouvez éviter d'y recourir, la meilleure précaution est d'utiliser des mots de passe à usage unique. Il existe pour ce faire des dispositifs astucieux et peu coûteux à installer avec le concours de votre administrateur système.

Le chiffrement des données

La récente libéralisation de l'usage de la cryptologie offre désormais un accès aisé à la sécurisation du stockage et de la transmission de l'information. Parmi les services que vous pouvez dès maintenant acquérir pour quelques centaines de francs seulement par poste de travail, se trouvent :
– pour la création et l'archivage de fichiers, des procédés automatiques de déchiffrement à l'ouverture, de chiffrement à la fermeture et d'effacement sécurisé ;
– pour le courrier électronique, des procédés de chiffrement autodécryptables des pièces attachées qui n'imposent au destinataire que l'usage d'un mot de passe que vous lui avez transmis par une autre voie. Dans ce procédé, à la protection de la confidentialité s'ajoute la garantie de l'authenticité et de l'intégrité du document. Ces procédés, faciles à installer, ne conviennent qu'à un nombre très limité de liaisons.

La création d'un système plus vaste de messagerie chiffrée en ligne exige la mise en place d'une organisation et de procédures qu'il n'est pas possible de détailler ici, mais vous pouvez utilement consulter à ce sujet le précédent numéro de *Sécurité Informatique* (n° 24 – disponible sur http://www.cnrs.fr/Infosecu/Revue.html).
Le choix d'un fournisseur de procédés de chiffrement n'est pas innocent. Lorsque le produit est importé d'un pays étranger, vous risquez en effet d'acquérir un produit affaibli, et ce que vous pensiez dissimuler aux grandes oreilles des officines d'intelligence économique pourrait bien se retrouver entre les mains de celui qui convoite vos découvertes. Pour vos communications hexagonales, utilisez de préférence un produit conçu par une entreprise nationale.

Pour conclure

Se protéger des menaces qu'Internet fait peser sur le patrimoine scientifique des établissements de recherche publique nécessite de la volonté, de la rigueur dans le travail quotidien et quelques moyens qui ne devraient pas ruiner le budget de fonctionnement du laboratoire. Voyons, ... j'allais oublier... Ne reste-il pas un moyen infaillible pour déjouer toutes les tentatives d'attaque par le réseau ? Mais bien sûr... il suffit de ne pas y être connecté ! J'entends déjà ricaner au fond de la cour : et la messagerie... et le butinage sur le Net... et le téléchargement de données ! Si vous avez un PC portable, pourquoi ne pas l'utiliser pour ces tâches ancillaires et isoler du réseau votre machine principale ? À l'abri des pirates, des chevaux de Troie, des virus et des sniffers, elle ne sera qu'en meilleure forme pour se vouer à la partie la plus noble de votre travail.

Philippe Schreiber
Fonctionnaire de défense au CNRS

Guide sécurité des systèmes d'information à l'usage des directeurs

Le *Guide sécurité des systèmes d'information à l'usage des directeurs* est disponible.
Chaque directeur de laboratoire en recevra un exemplaire courant juin. Pour les gros laboratoires, des exemplaires supplémentaires pourront être réclamés à robert.longeon@cnrs-dir.fr.
La version électronique, téléchargeable par tous, sera disponible sur le web à http://www.cnrs.fr/Infosecu/ dès la mi-juillet. ■

Renouvellement de l'opération AVP

Le CNRS a renouvelé l'accord de licence avec le nouveau distributeur d'AVP, la société «I.D.». Les laboratoires CNRS ou universitaires qui désirent acquérir ce logiciel peuvent en faire la demande à robert.longeon@cnrs-dir.fr ■

SÉCURITÉ INFORMATIQUE
numéro 25 juin 1999
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61