SÉCURITÉ INFORMATIQUE

numéro 21 octobre 1998

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Intégrité et fiabilité…

Le maniement d'un instrument de laboratoire n'est jamais exempt de risques et ceux qui s'en servent, chercheurs, ingénieurs ou techniciens, admettent volontiers que des précautions d'utilisation soient prises et des procédures clairement énoncées.

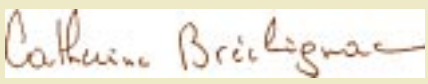
éditorial

Il faut qu'il en soit de même pour l'informatique. En dépit d'une facilité accrue d'utilisation – on nous dit que les matériels se définissent maintenant par la formule «branche et joue» (*) –, les systèmes informatiques sont vulnérables. Si les autoroutes de l'information permettent à tout un chacun de communiquer avec le monde entier, elles offrent également un champ pratiquement illimité à de nouvelles formes d'agression. Il appartient donc à chacun de se soucier de l'intégrité et de la fiabilité de cet outil de travail désormais irremplaçable.

La sécurité des systèmes d'information repose avant tout sur une démarche à la fois individuelle et collective : une vigilance constante, une organisation adaptée, des modes de travail, et des procédures qu'il faut évaluer de temps à autre pour vérifier qu'elles fonctionnent convenablement.

C'est cette démarche que les articles qui suivent vous invitent à découvrir. Les opérations-pilotes que le CNRS a menées à Nice, Grenoble, Toulouse et Marseille ont montré qu'il y avait encore beaucoup à faire dans nos laboratoires, mais qu'on y trouvait aussi les volontés et les compétences pour aller de l'avant.

Prenez le temps de lire ces quelques pages et d'en discuter avec vos collègues et vos collaborateurs. C'est notre intérêt à tous.



Catherine Bréchignac
Directeur Général du CNRS

(*) «Plug and play» dans le jargon de l'Internet.

Gérer la sécurité informatique :

pourquoi, comment ?

La sécurité informatique est devenue une préoccupation importante dans notre environnement, mais de nombreux responsables de laboratoire restent perplexes sur l'intérêt d'une politique de sécurité, qui inévitablement établira des contraintes, et sur la méthode à suivre pour la définir.

L'analyse des risques

Parlant de sécurité informatique, on pense immédiatement à la protection du système contre le vol des données, de logiciels ou plus globalement du savoir-faire : c'est la protection de la production et du patrimoine scientifiques.

Le vol (piratage) fait partie de ce risque ; la corruption des fichiers en constitue un autre aspect d'autant plus pernicieux que celle-ci peut ne pas être identifiée immédiatement.

Nous pensons moins souvent aux problèmes de responsabilité liés au stockage de logiciels ou de données sur nos systèmes informatiques : pour autant que nous utilisions des logiciels sous licence ou que nous soyons dépositaire de données qui nous sont confiées pour un traitement, la responsabilité du laboratoire peut être engagée si un défaut de protection a permis à des indélicats d'emprunter ces informations.

L'intrusion dans les systèmes informatiques n'est pas seulement destinée au vol ou motivée par l'intention de perturber le travail d'une équipe. On constate malheureusement que c'est pour certains une sorte de sport auquel ils se livrent pour le simple plaisir de démontrer leur habileté à pénétrer des environnements informatiques. Des bandes organisées sévissent en utilisant toutes les facilités offertes par le réseau.

Le risque pour les laboratoires n'est pas seulement la destruction totale ou partielle de leur propre système informatique, mais aussi celui d'être utilisés – involontairement – comme relais pour accéder à d'autres systèmes. Là aussi, notre responsabilité peut être engagée comme intermédiaire même involontaire.

À cette famille de risque est rattachée l'installation de «chevaux de Troie» qui permettent à un pirate de se connecter sur des systèmes intermédiaires pour attaquer d'autres systèmes sans se faire repérer.

De même nature, l'utilisation de serveurs de messagerie distants pour inonder de messages une population donnée (attaques de type «SPAM») est une atteinte à la sécurité informatique dont les conséquences pour tous sont bien connues.

Lorsqu'un système informatique est indélicatement utilisé comme relais pour des actes perturbateurs, la réaction de certains des administrateurs de systèmes ainsi perturbés est d'isoler ou de faire isoler le système (relais) d'où vient la perturbation. On a ainsi vu des sites entiers temporairement exclus des tables de routage internationales de l'Internet par mesure de protection ou simplement de protestation.

Nos laboratoires sont raccordés sur un réseau ouvert, l'Internet, et les risques liés à la sécurité informatique sont permanents. Même si l'on

…… suite page 4 …

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Opérations sécurité sur les sites

Pourquoi ces opérations ? Le chercheur n'utilise plus son cahier d'expériences qu'il gardait précieusement dans un endroit protégé à clef : tout est maintenant sur son poste de travail informatique connecté à l'Internet. Or les problèmes d'intrusions et, plus largement, de sécurité informatique se sont multipliés ces derniers mois. Face à ce constat, nous n'avons pas une solution technique miracle, applicable partout. Le CNRS avec ses nombreuses unités dispersées sur des sites souvent ouverts, tous interconnectés par RENATER, réseau lui aussi ouvert, est un cas un peu atypique auquel on ne peut pas appliquer un modèle de protection classique recommandé par les experts du sujet. Par contre, les administrateurs réseaux et systèmes dans les laboratoires, malheureusement souvent trop peu nombreux, sont compétents, ouverts et toujours prêts à «faire quelque chose» dans ce domaine. Le problème est qu'ils sont isolés et ne savent pas «par où commencer» pour se protéger.
Il a été décidé de s'appuyer sur ces ingénieurs pour augmenter le niveau de sécurité de leur laboratoire, en leur apportant un ensemble de conseils et en les accompagnant dans ce travail. Nous avons choisi de procéder par petits groupes de laboratoires et de nous déplacer dans les délégations pour être au plus près des laboratoires afin d'avoir un contact direct toujours plus efficace, mieux perçu, et ainsi de nous adapter à chaque contexte.
Le but de ces opérations est de :
- *sensibiliser les unités aux problèmes de sécurité;*
- *les aider à faire un bilan de leurs vulnérabilités;*
- *les aider à améliorer et à organiser leur sécurité;*
- *proposer des actions correctrices et des outils de sécurisation ;*
- *veiller à l'application des recommandations du CNRS dans ce domaine.*

Méthodologie et opérations pilotes

Il existe différentes méthodes pour améliorer la sécurité, mais aucune n'est applicable facilement à notre environnement distribué, ouvert, avec du matériel hétérogène et une administration technique souvent décentralisée et minimale. Ces méthodes très lourdes et coûteuses sont destinées soit à évaluer le niveau de sécurité, soit à établir un schéma directeur de la sécurité qui revoit complètement le système d'information. Or notre but était double : avoir une partie vérification, mais surtout une partie amélioration de la sécurité, sans toutefois remettre totalement en question les organisations humaine et matérielle et sans conduire à l'achat d'équipements coûteux que les laboratoires ne peuvent se permettre. Nous désirions aussi être efficaces, sans monopoliser pendant trop de temps les ingénieurs des laboratoires déjà très sollicités.

Nous avons donc conçu notre propre méthode

À l'automne 1997, nous avons réuni un groupe d'experts de différents domaines (organisation, Unix, réseau, Windows-NT...) pour rédiger une liste de contrôles à effectuer dans chaque laboratoire. Ce document a été amélioré après chaque opération: la partie NT, par exemple, a été fortement complétée et remodelée. Nous avons ensuite défini une méthode d'intervention en plusieurs phases:

- Préparation de l'intervention avec le Délégué régional et un (parfois plusieurs) ingénieur de laboratoire local qui est alors le coordinateur de l'opération. Une liste de laboratoires est arrêtée –une douzaine en moyenne– et les modalités pratiques (planning, liste des ingénieurs de ces laboratoires, invitations...) sont définies.
- Intervention de deux jours sur le site pour :
  – sensibiliser les administrateurs et les directeurs de laboratoires concernés ;
  – faire un tour de table et connaître la configuration générale de chaque laboratoire ;
  – présenter la méthode et décrire la liste de contrôles ;
  – faire, si nécessaire, une partie cours et une présentation des outils que l'on recommande d'installer.
- Application pendant vingt jours environ de la liste de contrôles par les administrateurs dans leur laboratoire avec l'aide du coordinateur local.
- Intervention d'un jour sur le site pour récupérer les réponses à la liste de contrôles et faire le bilan de l'opération avec les administrateurs.

Sont présents aussi, à chaque opération, un ingénieur qui a participé à l'opération précédente, pour que l'expérience circule, ainsi que le coordinateur de l'opération suivante, pour le préparer.
Pour valider cette méthode, nous avons effectué trois opérations pilotes sur des sites choisis pour leurs spécificités: la première à Sophia-Antipolis en décembre 1997 sur un campus CNRS «récent» avec principalement des petites ou moyennes unités; la deuxième à Toulouse en mars 1998 avec de grosses entités bien équipées en informatique sur plusieurs sites; et la troisième à Grenoble en juin avec de gros laboratoires, principalement de physique, moyennement équipés et pauvres en ingénieurs, répartis sur plusieurs campus. Les trois contextes étaient ainsi très différents.

La liste de contrôles

Ce document permet à l'administrateur de mieux connaître son parc informatique, donc de mieux l'administrer, d'augmenter et d'améliorer la sécurité de l'ensemble, d'acquérir une méthode pour réagir rapidement en cas d'intrusion, et peut l'amener à revoir l'architecture du réseau et l'organisation des services offerts.
Sous forme de question-recommandation, la liste donne un certain nombre de vérifications à effectuer et, pour chacune, des conseils qui peuvent être : les actions correctrices à prendre, les versions des logiciels à mettre à jour, les outils de sécurité à installer en priorité... Plusieurs listes de ce type existent, mais elles se limitent à un système d'exploitation, sont trop longues et ne sont pas à jour. Le problème principal dans la constitution de cette liste est de faire des choix, d'être concis et précis. En effet, il faut aboutir à un document de taille restreinte pour être applicable en un temps assez court. Nous n'y avons pas indiqué toutes les vulnérabilités possibles, mais les plus dangereuses et les plus courantes dans notre environnement.
Il est donc adapté aux laboratoires.
Il se décompose en sept chapitres :

- Présentation du laboratoire.
- Organisation de la prévention, de la détection et de la protection.
- Sécurité sur les systèmes Unix.
- Sécurité des réseaux.
- Services et outils de sécurité Unix.
- Sécurité sur les systèmes NT.
- Sécurité des réseaux de micro-ordinateurs.

Vu les contraintes de temps que l'on impose aux administrateurs, on demande d'appliquer cette liste sur toutes les machines pour un petit site avec un parc informatique restreint, et, pour un grand site, sur tous les serveurs et machines «importantes» ainsi que sur un échantillon représentatif du matériel.

Pour avoir une idée plus précise exemples de questions que l'on t cette liste :

Chapitre «Organisation»
• Question : existence d'une c
• Recommandation : une char sée à chaque utilisateur au m ture de son compte. Elle approuvée par lui. Le com ouvert qu'à cette condition du CNRS, vous pouvez y strictes et, si besoin, des (modèle disponible sur l http://www.auteuil.cn ment.html).

Chapitre «Réseaux»
• Question : tournez-v sion égale à 8.8.8 ?
• Recommandation : ou de version infé remplacés pour u (binaire disponi sieu/sendmail/bin invalidée. Cons d'établissement sée à recevoir redistribution disponible su mail/kit. Si vo fier que leur

Bilan provisoire des opérations

Les trois opérations pilotes ont été pleinement satisfaisantes, la méthode a été globalement très bien perçue. Sur 45 laboratoires sollicités, un seul n'a pas pu participer à l'opération, tous les autres étaient présents aux réunions de préparation et au bilan final. Sur les deux semaines de travail potentiel, les administrateurs ont consacré en moyenne l'équivalent de 4 à 5 jours pour ce travail, avec des différences très marquées allant de quelques heures, faute de moyens, à au contraire deux semaines complètes. L'ensemble des ingénieurs a trouvé que la méthode était bonne et que cette opération avait été très bénéfique, car avant tout stimulante pour :

- sensibiliser le laboratoire aux problèmes de sécurité : une telle opération dans un temps borné est connue dans le laboratoire et permet de rappeler qu'il y a des risques et des règles de base de sécurité. Elle peut initialiser une réflexion sur une organisation de la sécurité ;
- corriger certains trous de sécurité ;
- installer localement un minimum d'outils de sécurisation, travail pouvant être poursuivi ensuite ;
- établir un lieu d'échanges techniques pour les problèmes et les outils de sécurité.

L'intervention sur place de l'UREC et des services du Fonctionnaire de défense et la coordination locale sont deux éléments jugés fondamentaux par les participants.

Les trois opérations ont conduit également les laboratoires à s'améliorer: l'un d'entre eux a revu complètement son architecture réseau; trois autres ont affecté un poste d'ITA pour administrer l'informatique; de nombreux autres, enfin, ont réorganisé leurs services réseaux, acheté un équipement filtrant et imposé l'ingénieur présent comme responsable de la sécurité informatique.

Cette méthodologie a permis en outre d'initier ou de promouvoir une dynamique locale sur le sujet avec le noyau des administrateurs qui ont travaillé ensemble. Dans les trois délégations en région, une liste de diffusion électronique a été lancée et fonctionne bien, et des réunions thématiques locales sur ce sujet ont été prévues. Cela permet de rompre l'isolement des administrateurs et de pouvoir nous appuyer sur ces groupes dans la diffusion des recommandations nationales et l'organisation de la sécurité au CNRS.

La seule ombre au tableau a été la très faible participation des directeurs de laboratoire qui n'ont pas pu être ainsi directement sensibilisés, ce qui peut mettre certains ingénieurs dans une situation délicate lorsqu'ils n'ont pas le soutien ferme de leur Direction dans l'installation de mesures de protection. Dans les prochaines opérations, nous essaierons de mieux toucher les directeurs en incluant la sensibilisation sécurité dans une autre réunion de Direction par exemple. Nous considérons que l'ensemble de la méthode est bonne et que l'accompagnement, les contacts, etc. sont primordiaux. Ainsi nous n'avons pas mis la liste de contrôles en accès public car elle ne constitue qu'un des éléments de l'ensemble et perd beaucoup de son intérêt si elle n'est pas incluse dans une opération.

Premières conclusions

Dans la liste de contrôles, nous mettons en avant trois priorités qui ne sont pas encore présentes dans tous les laboratoires :

- le filtrage des accès réseaux sur le routeur d'entrée (ACL) et sur les stations principales (tcp_wrapper) ;
- la gestion des mots de passe : création, vérification de la solidité... ;
- la sensibilisation des utilisateurs au moyen d'une charte.

On ne peut pas faire un état des lieux précis – ce n'est d'ailleurs pas le but de l'opération – mais quelques constats se dégagent de l'échantillon des laboratoires vus :

- La sécurisation est très inégale mais est en moyenne faible, en particulier dans les petites unités.
- Les administrateurs ont généralement une bonne connaissance technique et maîtrisent assez bien leur sujet : seul Windows-NT est un système où l'on manque beaucoup de pratique.
- On a pu faire très peu de chose dans les unités qui manquent de moyens en administrateur de systèmes. Ces unités n'ont, bien évidemment, pas pu traiter correctement la liste de contrôles et sont très vulnérables.
- Dans certaines unités, même moyennes, personne ne maîtrise ni ne possède la composition du parc informatique, en particulier les postes personnels. Or, les vulnérabilités étant tout aussi – voire plus – importantes sur ces matériels que sur les serveurs, cela est très dangereux. Il faut que la tâche d'administration du parc informatique soit reconnue, et affectée à un personnel clairement désigné, qui peut être interne ou externe au laboratoire.
- L'arrivée des Unix libres sur les PC personnels amène de très nombreuses vulnérabilités. Cela amplifie le besoin de maîtrise de l'ensemble du parc informatique par les administrateurs.
- En sécurité, la direction a trop rarement un rôle moteur, et elle a même parfois un rôle négatif. Il faut impérativement sensibiliser la Direction d'une majorité de laboratoires aux risques encourus.
- L'architecture du réseau de certains laboratoires est à revoir en incluant des contraintes de sécurité. Plus globalement, il faut penser à la sécurité dans tout nouvel achat ou réorganisation technique informatique.
- Il est obligatoire d'avoir un animateur local dynamique pour faire circuler l'information et aider les unités dépourvues d'administrateurs.

La suite

La méthode a été validée et a visiblement apporté beaucoup aux laboratoires avec un coût budgétaire très faible, uniquement de missions, et un temps ingénieur raisonnable. Deux opérations sont déjà sur les rails à Marseille en septembre et à Nancy en octobre ; d'autres suivront. Nous envisageons de compléter la méthode avec l'utilisation d'un logiciel commercial de détection automatique de vulnérabilités que deux laboratoires sont en train de tester pour nous. Nous attendons les résultats. Si d'autres logiciels de sécurité nous paraissent intéressants pour les laboratoires, nous inclurons leur diffusion dans les opérations.

Une démarche à moyen terme sera de faire vivre ces groupes qui se sont formés dans chaque région. Il pourrait être décidé de s'appuyer sur eux dans la politique sécurité de l'organisme.
Nous n'avons pas encore fait de traitement statistique des réponses pour déduire les vulnérabilités principales des laboratoires, mais cela pourrait être envisagé, quoique ceci ne soit pas le but de la méthode. Par contre, il semble intéressant de prévoir une visite systématique «un an après» sur les sites pour évaluer le changement et relancer la dynamique.

Jusqu'à présent, nous avons toujours gardé à l'esprit que ce type d'opération pouvait être inadapté à notre environnement, rejeté par les laboratoires. Ce n'est visiblement pas le cas. Mais nous avons commencé à travailler pas à pas, avec peu de moyen, en validant et corrigeant systématiquement après chaque itération, sans projet à long terme. C'est une méthode un peu empirique, mais qui est certainement efficace dans les trois domaines de la sécurité, de l'informatique et des réseaux où les évolutions rapides demandent une adaptation aussi rapide. Ainsi nous n'avons pas de plan précis pour l'avenir. L'évolution sera très liée à l'activité des groupes d'administrateurs et aux moyens dont nous disposerons pour faire vivre cette communauté.
Ces opérations ne sont pas terminées et elles se poursuivront, très certainement avec la même méthode de base.

Jean-Luc Archimbaud
et Nicole Dausque
CNRS/UREC
Jean-Luc.Archimbaud@urec.cnrs.fr
Nicole.Dausque@urec.cnrs.fr

, voici deux
ouve dans

arte?
te doit être propo-
oment de l'ouver-
doit être signée et
pte ne peut lui être
. Il existe un modèle
ajouter des consignes
clauses propres au site
e site:
s-dir.fr/Infosecu/docu

ous un sendmail de ver-

les sendmail constructeurs
rieure à 8.8.x doivent être
tiliser un sendmail V8.8.8
ble sur ftp://ftp.lip6.fr/jus
) ayant la fonction «RELAY»
eil: envisager une politique
avec une seule machine autori-
u mail de l'Internet avec une
interne. La documentation est
r: ftp://ftp.lip6.fr/jussieu/send
us avez des clients «Eudora», véri-
«shell» est /bin/false.

suite de la page 1

pense ne rien avoir dans ses fichiers qui puisse être volé, il n'est pas possible de se désintéresser de la sécurité de son système informatique.

Peut-on réellement se protéger ?

Il est nécessaire de traiter l'ensemble de l'outil informatique, réseau et systèmes informatiques, de façon globale, et la protection des seuls accès réseau n'est pas suffisante même si les tentatives d'intrusion arrivent par le réseau.
La politique de sécurité d'un site ou d'un laboratoire doit être définie à partir d'une analyse du parc, des utilisations et des modes de travail. Cette analyse permet de moduler les solutions à mettre en œuvre pour organiser une protection adaptée.
Dans cette démarche, il faut s'interroger sur les modes de travail du laboratoire autour de l'outil informatique. On s'aperçoit souvent que des facilités laissées aux utilisateurs pour accéder à une machine depuis un poste distant ou pour partager des fichiers constituent des brèches importantes dans le dispositif de sécurité, alors qu'une adaptation légère des modes de travail permettrait de remplir les mêmes besoins et de diminuer les risques.
On s'aperçoit aussi que certaines fonctions des systèmes d'exploitation qui peuvent constituer des risques de sécurité sont activées alors que personne ne les utilise, simplement parce que la machine a été livrée avec une configuration par défaut.
Plus généralement, la gestion de la sécurité est indissociable d'une administration des systèmes et il faut bien accepter d'y consacrer du temps et des ressources.
À l'opposé, il existe souvent dans les équipements installés dans les laboratoires, micros, stations ou routeurs, des dispositifs simples d'enregistrement ou de filtrage qui peuvent être activés et fournir des solutions suffisantes dans beaucoup d'environnements, sans qu'il soit nécessaire d'acquérir des outils supplémentaires.

La démarche que le CNRS vous propose

Conscient à la fois de la nécessité de gérer la sécurité informatique de nos laboratoires, mais aussi de la difficulté de beaucoup d'unités à y consacrer les ressources humaines et le temps suffisants, le CNRS a mis en place des moyens pour vous aider au quotidien en la matière ; nous vous les présentons dans les articles de ce numéro.

L'esprit général est de faire suivre aux laboratoires une démarche de sécurité : évaluer les points faibles de l'informatique du laboratoire et les risques associés ; activer les outils nécessaires pour gérer la sécurité et contrôler les accès ; s'associer au réseau d'expertise par lequel les compétences et les informations sont échangées ; s'obliger régulièrement à vérifier l'état des procédures de sécurité.
L'objectif est que la sécurité informatique reste un souci constant dans le développement de notre activité scientifique.

Christian Michau
Directeur de l'UREC
Christian.Michau@urec.cnrs.fr

CAP : un macro virus meurtrier

Le virus CAP est apparu en février 1997. Il contient 10 macros :
– CAP : macro contenant le code viral ;
– TOOLSMACRO : macro d'interception des commandes ;
– AUTOEXEC, AUTOPEN, FILEOPEN, FILESAVE, AUTOCLOSE, FILECLOSE, FILESAVEAS et FILETEMPLATE. Ces macros sont «vides».
Lors de l'infection, le virus parcourt les menus déroulants de WORD et en relève les noms. Ensuite il intercepte l'appel aux fonctions correspondantes et y insère un pointeur sur la macro CAP. Il détruit les macros systèmes contenues dans le NORMAL.DOT et y insère les siennes. Lors de l'utilisation de FILESAVEAS, le fichier document sauvegardé est vide mais infecté par le virus.
CAP infecte les documents quelle que soit la langue de WORD (français, anglais, allemand…).
L'éradication du virus doit se faire en deux étapes :
1. la première, une désinfection complète de tous les fichiers documents (DOC, DOT, WBK…) ;
2. la seconde, la destruction pure et simple du fichier NORMAL.DOT. ■

Marc Daniel
ctgn-stig@dial.oleane.com

Mythes et réalité

Tout le monde s'accordait à dire qu'on ne pouvait être victime d'une bombe informatique simplement en lisant un courrier électronique. Il fallait ouvrir ou exécuter le fichier envoyé en «pièce attachée» pour rendre possible une malveillance. Il n'en est plus rien. Les médias se sont fait l'écho, cet été, d'une vulnérabilité, découverte par l'université d'Oulu, sur certains clients de messagerie utilisant MIME. Des avis de sécurité ont été publiés à ce sujet par Microsoft, Netscape, AUSCERT, CIAC, NTBugTraq et d'autres. En résumé, elle permet à un agresseur d'introduire un Cheval de Troie ou une bombe logique *via* un fichier attaché. Le programme s'exécutera dès la réception courrier, quand le «client de messagerie» essaye d'afficher les noms des pièces jointes. La malveillance utilise la technique du débordement de buffer sur le nom du fichier. La réalité rejoint ainsi, d'une certaine manière, le vieux mythe du type «Good Time…» qui parcourt la communauté à intervalles réguliers.
Si vous êtes intéressé par les détails du mécanisme, vous pouvez consulter : http://www.cert.org/advisories/CA-98.08.qpopper_vul.html.
Rappelons que cette nouvelle vulnérabilité IMPOSE à tous les administrateurs système la mise à jour de leur «sendmail» pour qu'il effectue des contrôles avant que le courrier soit envoyé à un client vulnérable : http://www.sendmail.com/sendmail.8.9.1a.html. Il est également possible de mettre en place ce filtrage au niveau de procmail : http://www.wolfenet.com/jhardin/procmail-kit.html. ■

Liste provisoire des clients de messagerie présentant cette vulnérabilité

Systèmes	Clients messagerie
OpenLinux	mutt-0.93.1
HP-UX	CDE
Windows 95, Windows 98 Windows NT 4.0	Microsoft/Outlook98 Microsoft/Outlook-Express-4.0 Netscape/Communicator-4.x
Solaris	Microsoft/Outlook-Express 4.01 Dtmail mailtool
SCO	dtmail

SÉCURITÉ INFORMATIQUE
numéro 21 octobre1998
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité d'information. 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 - MIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61