# Opérations sécurité sur les sites

Jean-Luc Archimbaud et Nicole Dausque CNRS/UREC V2 3/9/98

# 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 régionales 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 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 efficace, sans monopoliser pendant trop de temps les ingénieurs des laboratoires déjà très sollicités.

**Nous avons donc conçu notre propre méthode**.

A l''automne 97, 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 2 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 20 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 3 opérations pilotes sur des sites choisis pour leurs spécificités : la première à Sophia-Antipolis en décembre 97 sur un campus CNRS " récent " avec principalement des petites ou moyennes unités, la seconde à Toulouse en mars 98 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 3 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'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 6 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

Pour avoir une idée plus précise, voici deux exemples de questions que l''on trouve dans cette liste :

Chapitre organisation :

*. Question : existence d'une charte ?*
*. Recommandation : une charte doit être proposée à chaque utilisateur au moment de l''ouverture de son compte. Elle doit être signée et approuvée par lui. Le compte ne peut lui être ouvert qu''à cette condition. Il existe un modèle du CNRS, vous pouvez y ajouter des consignes strictes et si besoin des clauses propres au site (modèle disponible sur le site : http://www.auteuil.cnrs-dir.fr/Infosecu/document.html).*

Chapitre réseaux :

*. Question : tournez-vous un sendmail de version égale à 8.8.8 ?*
*. Recommandation : les sendmail constructeurs ou de version inférieure à 8.8.x doivent être remplacés pour utiliser un sendmail V8.8.8 (binaire disponible sur ftp://ftp.lip6.fr/jussieu/sendmail/bin) ayant la fonction " RELAY " invalidée. Conseil : envisager une politique d''établissement avec une seule machine autorisée à recevoir du mail de l''Internet avec une redistribution interne. La documentation est disponible sur : ftp://ftp.lip6.fr/jussieu/sendmail/kit. Si vous avez des clients " Eudora ", vérifier que leur " shell " est /bin/false.*

Vues 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.

# 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 moyen, à au contraire 2 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.
. Etablir 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, la coordination locale sont deux éléments jugés fondamentaux par les participants.

Les 3 opérations ont conduit aussi, pour un laboratoire à revoir complètement son architecture réseau, pour 3 autres à affecter un poste d'ITA pour administrer l'informatique et pour de nombreux laboratoires à réorganiser les services réseaux, à acheter un équipement filtrant et à imposer 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 3 délégations régionales une liste de diffusion électronique a été lancée et fonctionne bien et des réunions thématiques locales sur ce sujet ont été prévues. Ceci 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 laboratoires 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 essaieront 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 …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 3 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 de 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 choses 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 voir plus importantes sur ces matériels que sur les serveurs, ceci 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 d'étection automatique de vulnérabilités que 2 laboratoires sont en train de tester pour nous. Nous attendons les résultats. Si d''autres logiciels de sécurité nous paraissent intéressant pour les laboratoires, nous incluerons 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 3 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