Sécurité informatique et réseau au CNRS : bilan des actions menées et en cours

Jean-Luc Archimbaud

SECURITE INFORMATIQUE ET RESEAU AU CNRS

BILAN DES ACTIONS MENEES ET EN COURS

Jean-Luc Archimbaud
Directeur Technique de l'UREC
Chargé de mission sécurité réseau auprès du Fonctionnaire de défense
30 avril 2001

Ce document établit un bilan des actions menées et en cours en sécurité informatique et réseau au CNRS au printemps 2001. Ces actions sont une mise en œuvre pragmatique et concrète des éléments obligatoires d'une politique de sécurité.

Ce document présente rapidement les besoins en terme de sécurité au CNRS, les spécificités de l'organisme et de ses systèmes d'information ainsi que les personnes impliquées dans la sécurité. Il approfondit ensuite les différentes actions :

- La méthodologie employée pour, dans les unités, sensibiliser, faire un état des lieux, initier le travail de sécurité et lancer une dynamique sécurité régionale : **les opérations sécurité,**
- L'organisation humaine mise en place : **les coordinateurs régionaux** sécurité et **les correspondants sécurité dans les laboratoires,**
- La formation de ces personnes : **la formation SIARS,**
- **La diffusion et la circulation d'informations,**
- **Le traitement des incidents,**
- **Les recommandations,**
- **L'architecture réseau** recommandée et fortement insufflée,
- **Les outils** techniques recommandés et fournis,
- La mise en place d'une **autorité de certification**, fondation sur laquelle pourront s'appuyer toutes les applications pour assurer l'authentification, l'intégrité, la confidentialité et le contrôle d'accès.

Toutes ces actions ne couvrent pas encore l'ensemble des unités, ni tout « ce qu'il faudrait faire ». Mais le travail réalisé depuis quelques années est important et l'utilité n'est plus à démontrer.

1. Deux besoins de sécurité et une obligation

L'informatique et les réseaux sont présents partout. Parallèlement, le nombre de problèmes de sécurité, en particulier les intrusions par l'Internet, a augmenté de manière très important ces dernières années, et cette courbe ascendante ne devrait malheureusement pas s'infléchir. Il ne faut pas oublier les risques classiques, vols, disfonctionnements dus à des négligences ou à des actes malveillants internes, ... toujours présents. Il faut donc se protéger. Mais que protéger ?

Au CNRS, on peut considérer que l'on a deux besoins principaux en terme de sécurité.

Le premier est **la protection d'un outil de travail,** les postes informatiques, les réseaux, les applications et les données, l'ensemble constituant le système d'information. En effet, cet ensemble est maintenant indispensable à la fois pour les activités nécessaires à la recherche (calcul, pilotage d'expériences, modélisation, traitement de l'information, communication, bureautique, …), mais aussi pour la gestion des laboratoires. Etant devenu indispensable, ces outils sont à protéger. Une attaque peut par exemple provoquer l'indisponibilité du serveur de messagerie ou de calcul pendant plusieurs jours, celle-ci sera très difficile à supporter par l'ensemble du personnel.

Le second est **la protection du patrimoine** en particulier scientifique des laboratoires, c'est à dire des articles en préparation, des résultats de recherche, des développements, des contrats industriels, … La recherche étant de plus en plus financée par des contrats privés, les travaux des laboratoires seront de plus en plus à considérer comme confidentiels et donc à protéger.

Ces deux classes de besoins en sécurité, qui constituent en fait deux objectifs différents, peuvent être satisfaites avec les mêmes méthodes et les mêmes outils. En effet si l'on protége une station informatique, on protége aussi les informations confidentielles qui y sont stockées.

Il ne faut pas oublier une obligation. **L'ensemble du personnel des laboratoires doit respecter la législation française**, sur la criminalité informatique, sur l'édition qui s'applique aux serveurs Web, sur la protection de la vie privée (fichiers nominatifs, courrier personnel confidentiel, …), … C'est un domaine difficile, car nouveau (il y a encore très peu de jurisprudence sur les utilisations de l'Internet) et qui demande des réponses non pas techniques mais plutôt en terme de sensibilisation et de recommandation éventuellement de réglementation auprès des personnels.

2. Handicaps et avantages (sécurité) du CNRS

Le CNRS n'est pas un milieu facile et les mesures de sécurité ne sont ni évidentes à définir, ni faciles à faire accepter. De part sa structure, son mode de fonctionnement et ses missions, le CNRS est un organisme qui part avec beaucoup de handicaps sur le chemin amenant à une bonne sécurité. On peut en citer quelques uns.

- C'est une structure éclatée, avec plus de 1300 laboratoires sur plusieurs centaines de sites souvent dans des environnements ouverts comme les campus. Il est donc très difficile de délimiter des zones (en terme de locaux ou de réseau informatique) à protéger.
- Parmi ces laboratoires, peu sont des unités propres, la grande majorité est associée à d'autres organismes. Il faut ainsi que les laboratoires respectent les règles du CNRS mais aussi des autres organismes de tutelle. On ne peut donc pas décider une politique CNRS sans concertation avec les autres organismes.
- Les laboratoires manquent souvent de moyens financiers et en personnel. On ne peut donc pas recommander d'installer systématiquement certaines protections (un garde-barrière à la porte de chaque laboratoire par exemple) car la plupart des laboratoires n'auront ni l'argent nécessaire pour le financer, ni le personnel pour l'administrer.
- Dans chaque laboratoire, il y a du personnel temporaire, étudiants, thésards, contractuels, visiteurs, …. Moins sensibles à la bonne marche du laboratoire que le personnel permanent, ils constituent naturellement un groupe à risque qui demande une surveillance particulière.
- Dans un autre domaine, de part son activité, la recherche fondamentale demande énormément de coopérations extérieures souvent internationales ; la communication et l'ouverture sont alors obligatoires. Il est donc très difficile de limiter celles-ci, alors que ce sont des mesures évidentes pour une meilleure sécurité réseau par exemple.
- L'activité du CNRS couvre tous les domaines scientifiques qui ont chacun un mode de fonctionnement et même parfois de pensée spécifique. Dans ces conditions, il est difficile d'établir des recommandations adaptées et acceptées par toutes ces populations différentes.

Mais le CNRS possède aussi des avantages. Le personnel en particulier en informatique est généralement compétent, avec un esprit d'initiative et de création qui permet à cet organisme d'être souvent précurseur dans le domaine de l'informatique et des réseaux malgré des moyens limités. On n'a pas peur de la nouveauté et on sait faire au mieux avec les moyens dont on dispose. Il existe aussi une habitude d'ouverture, d'échanges et d'entraide entre les ingénieurs qui est un avantage très important par rapport à des structures plus cloisonnées et où l'esprit de compétition bloque tout travail de groupe. L'organisation de sécurité mise en place au CNRS ne pourrait d'ailleurs pas fonctionner sans cet esprit d'équipe.

Ainsi le CNRS a des spécificités très particulières, difficiles. Mais même si le milieu n'est pas favorable à l'esprit de sécurité il faut, sans les cacher ni les ignorer, tenir compte de ces particularismes pour définir une bonne politique de sécurité. **Il est préférable de se fixer des objectifs limités mais réalistes plutôt que de viser un modèle « standard», cadre rigide**

inacceptable par notre communauté, modèle que l'on n'atteindra jamais vues nos spécificités.

3. Trois ensembles de systèmes d'information

De fait, trois ensembles de systèmes d'information coexistent au CNRS :

- **Le système d'information de gestion** géré par la DSI, réparti entre les centres serveurs de la DSI et les délégations. Le réseau qui interconnecte ces sites est un réseau privé, ensemble de liaisons point à point (VPs ATM sur Renater). L'administration de cette informatique et de ce réseau est effectuée par une équipe technique centrale qui inclut une fonction de sécurité. La politique de sécurité classique d'une entreprise multi-sites avec un réseau privé et une administration informatique centralisée est appliquée : contrôle d'accès en entrée du réseau privé, limitation des communications aux applications de gestion, …
- **Quelques gros centres de service** (calcul comme l'IDRIS, de diffusion d'informations scientifiques comme l'INIST, …). Chaque centre, situé sur un seul site, a une activité bien définie, des utilisateurs clairement identifiés, une équipe informatique solide qui administre l'ensemble et un responsable de la sécurité informatique. La politique de sécurité mise en œuvre suit le modèle « centre de calcul avec utilisateurs distants » : contrôle d'accès en entrée, identification des utilisateurs, …
- **Plus de 1300 laboratoires** qui ont chacun leur système d'information : réseau local, stations diverses (Unix, Win-9X, Win-NT, …), logiciels variés pour les activités bureautiques, Internet, calcul, modélisation, pilotage d'expérience, … Les équipements et l'architecture sont choisis « librement » par la direction du laboratoire, nous ne pouvons les orienter que par des recommandations ou lors d'opérations d'envergure financées au niveau central, par le COMI par exemple. Dans chaque unité, cet ensemble est administré localement par un ou plusieurs administrateurs informatiques, personnel du laboratoire.

Tous ces systèmes d'information sont interconnectés par le même réseau, Renater, lui-même connecté à l'Internet. Sous l'aspect sécurité, Renater est un réseau sans contrôle particulier de sécurité et une connexion à Renater est « aussi risquée » qu'une connexion directe à l'Internet. Il n'y a donc pas un réseau CNRS et nous n'avons pas d'Intranet. A noter qu'il serait difficile de faire autrement, la plupart des unités étant mixtes par exemple, un réseau purement CNRS pourrait difficilement être mis en place. Mais cette architecture de réseau nous rend très vulnérable aux attaques venant de l'Internet.

Le système d'information de gestion et les centres de service ont du personnel en charge de la sécurité informatique et les politiques de sécurité à appliquer sont «standards ». Ils ont donc un niveau de protection correct. Par contre, pour les laboratoires, nous n'avions pas de modèle de politique de sécurité à appliquer. Il a donc fallu un peu innover dans les actions à entreprendre et la définition des priorités.

4. Les personnes impliquées au niveau national dans la sécurité informatique et réseau

Plusieurs entités pilotent ou sont responsables de la sécurité des systèmes d'information au CNRS. Au niveau de l'ensemble de l'organisme, il existe deux unités nationales :

- Le **service du fonctionnaire de défense** avec 2 ingénieurs chargés de mission pour la sécurité informatique : Robert Longeon et Jean-Luc Archimbaud.
- L'**UREC**, Unité REseaux du CNRS, avec Jean-Luc Archimbaud ingénieur aussi directeur technique de l'UREC et deux ingénieurs Nicole Dausque et Marie-Claude Quidoz. Plus récemment deux autres ingénieurs Claude Gross et Philippe Leca travaillent au développement et à la mise en place de l'autorité de certification CNRS.

D'autres personnes ont des fonctions sécurité à d'autres niveaux dans l'organisme. On peut citer :

- Bernard Perrot, ingénieur, responsable sécurité à l'**IN2P3**
- Lionel Maurice, ingénieur, responsable sécurité à l'**IDRIS**
- Olivier Porte, ingénieur, chargé de la sécurité à la **DSI**

L'ensemble de ces personnes recouvre les 3 systèmes d'information du CNRS. Toutes ces personnes collaborent entre elles et se retrouvent dans des groupes communs. Ainsi elles font toutes partie du **groupe des coordinateurs sécurité** (voir chapitre 6, l'organisation humaine).

A ces personnes il faut rajouter les autres coordinateurs sécurité, administrateurs systèmes et réseaux dans des laboratoires ou des campus qui consacrent une partie de leur temps à la sécurité pour l'ensemble de la communauté et pas uniquement pour leur laboratoire.

Nous travaillons aussi en collaboration avec les personnes en charge de la sécurité informatique dans les autres organismes ou ministères, ainsi qu'avec le CERT Renater (CERT : Computer Emergency Response Team)

5. Les opérations sécurité

Fin 1997, l'UREC et le service du fonctionnaire de Défense, ont décidé de lancer des opérations de sécurité informatique et réseau sur des groupes de laboratoires CNRS dans les régions (http://www.urec.cnrs.fr/securite/articles/ope.secu.html). **Nous avons inventé une méthode adaptée au mode de fonctionnement de l'organisme et des laboratoires**.

Le but de ces opérations est d'aider les unités à améliorer leur sécurité en :

- **Les sensibilisant à la sécurité (en particulier les directeurs),**
- **Les aidant à faire un bilan de leurs vulnérabilités,**

- **Proposant des actions correctrices et des outils de sécurisation,**
- **Proposant des améliorations de l'organisation technique et humaine,**
- **Vérifiant l'application des recommandations CNRS,**
- **Créant un réseau humain.**

Nous avons d'abord rédigé **une liste de contrôles** qui fait actuellement 37 pages et qui comprend 7 chapitres : présentation du laboratoire, organisation de la sécurité, 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. C'est un questionnaire qui regroupe toutes les vulnérabilités les plus répandues à notre connaissance dans les laboratoires et qui **propose pour chaque point une recommandation et éventuellement une correction appropriée**. Ainsi ce n'est pas un outil d'audit mais d'aide aux laboratoires. Cette liste a été rédigée par 11 experts (cf annexe 14.1), responsables sécurité de centres de service, ingénieurs UREC et chargé de mission sécurité mais aussi administrateurs informatiques de laboratoire. Cette liste est **régulièrement mise à jour** par les ingénieurs de l'UREC, après chaque opération sécurité en tenant compte des remarques des participants et des nouveaux types d'intrusions qui nous sont signalées par les laboratoires ou par le CERT-Renater. La valeur de cette liste est surtout due à sa taille « raisonnable ». Il est très facile de rédiger une liste générale de contrôles à effectuer, il en existe d'ailleurs plusieurs sur l'Internet, il suffirait de les compiler. Le problème est quelle serait trop volumineuse pour être appliquée dans les laboratoires. Par opposition, dans cette liste, nous nous limitons à ce qui est le plus important à vérifier en se basant sur notre expérience et sur les nouvelles attaques dont nous avons connaissance dans notre communauté.

Avec cette liste comme outil de base, le déroulement d'une opération de sécurité est le suivant. Nous choisissons une délégation (ou une communauté spécifique, nous avons par exemple fait une opération pour les laboratoires SHS de Paris). Au départ nous sollicitions certaines délégations, maintenant on nous demande d'intervenir. Dans cette région nous contactons 2 (maintenant parfois 3) ingénieurs en informatique de la région qui connaissent les laboratoires de leur région, les problèmes de sécurité, qui ont un sens du travail en groupe et de coordination et qui sont volontaires pour consacrer du temps pour la « collectivité CNRS ». Ce peut être l'administrateur du réseau du campus CNRS quand il y en a un dans la région, le responsable des systèmes d'information (RSI) de la délégation, un ingénieur en informatique d'un laboratoire, … Nous contactons ensuite le délégué pour lui exposer l'objet de ces opérations et lui proposer ces personnes pour piloter l'opération dans sa région. Avec son accord, ces personnes sont désignées **coordinateurs sécurité**. Avec ces coordinateurs et le délégué nous établissons la liste des laboratoires qui vont participer à l'opération (en moyenne 15, plutôt « proches » du CNRS), la liste des directeurs et des administrateurs informatiques, le planning, l'organisation, …

Ensuite :

- Nous intervenons **2 jours dans la région** :

  Une demi-journée de sensibilisation des directeurs des unités qui participent à l'opération, avec une intervention du délégué, de l'UREC, du fonctionnaire de défense, de la DST. Nous présentons aussi l'opération.

  Un jour et demi de travail avec les administrateurs où nous présentons la liste de contrôles, effectuons un tour de table où les administrateurs présentent leur environnement, leurs problèmes, … (cela permet de commencer à créer un groupe) et des présentations techniques adaptées aux laboratoires participants. Deux ingénieurs de l'UREC pilotent ce travail.

- **Nous laissons travailler les administrateurs 20 jours** environ dans leur laboratoire pour qu'ils appliquent la liste de contrôles sur leurs serveurs et sur un échantillon représentatif de leur matériel et commencent à installer quelques outils de sécurité. Les coordinateurs créent une liste électronique pour permettre l'échange d'informations entre ces administrateurs et ils peuvent aider certains laboratoires qui manquent de personnel à utiliser cette liste de contrôles.
- Les coordinateurs recueillent les listes de contrôles remplies et en font une compilation
- Deux ingénieurs de l'UREC interviennent ensuite **1 jour pour faire un bilan** :
  Présentation de la compilation des réponses par les coordinateurs
  Tour de table pour recueillir les remarques des administrateurs et les vulnérabilités importantes découvertes dans leur laboratoire
  Bilan provisoire de notre part
  Une présentation technique
- Nous rédigeons un **rapport** qui résume les points les plus vulnérables que nous avons découverts et qui fait certaines propositions (besoin de demande de poste, de mise en place d'organisation, d'achat d'équipement particulier, …). Celui-ci est envoyé aux directeurs et aux administrateurs informatiques.

Les coordinateurs de l'opération suivante assistent à l'opération en cours. Sont aussi invités les responsables des structures non CNRS qui peuvent être impliqués dans la sécurité : administrateurs du réseau métropolitain, régional, responsables de CRI universitaire, RSSI université, … Ces personnes font souvent des présentations lors des opérations. A Lyon, l'opération a ainsi été faite en collaboration avec les universités. Cette participation « externe » tient compte de la réalité des laboratoires du CNRS où les interactions avec les universités en particulier sont très fortes. Chaque opération est aussi différente pour cadrer avec la région.

A ce jour **nous avons mené 13 opérations**. Nous avons débuté par 3 opérations pilotes, Sophia (12/97), Toulouse (3/98), Grenoble (6/98). Devant le succès de ces opérations nous avons continué par Marseille (9/98), Nancy (10/98), Gif (04/99), Orléans (11/99), SHS Paris (3/00), Strasbourg (5/00), Besançon (9/00), Orsay (10/00), Lyon (12/00), Montpellier (3/01). La prochaine sera Meudon en mai-juin 2001. **Notre rythme est ainsi de 4 opérations par an.**

Ces opérations ont été complétées par la diffusion d'un logiciel de détection de vulnérabilités Internet Scanner, présenté au chapitre 12 (Les outils techniques recommandés et fournis).

6. L'organisation humaine mise en place

6.1 Les coordinateurs sécurité

Ces opérations sécurité ont permis progressivement de mettre en place une organisation humaine gérée par l'UREC. Nous avons ainsi regroupé **les coordinateurs** des opérations sécurité, les responsables sécurité (DSI, IDRIS, IN2P3, …) et quelques experts dans un groupe national actuellement composé de **44 personnes**, listées en annexe 14.2.

Une liste de diffusion électronique regroupe ces coordinateurs sécurité et nous les réunissons maintenant régulièrement, environ 3 ou 4 fois par an. Ils sont notre interface vers les laboratoires pour diffuser les recommandations, intervenir en cas d'incident de sécurité, faire remonter les demandes, … Ils participent aussi à des groupes de travail que nous pilotons pour tester et choisir certains logiciels, rédiger des recommandations, monter des formations (cf formation SIARS). **Ils constituent le « noyau dur » sur lequel nous pouvons nous appuyer.**

6.2 Les correspondants sécurité

Dans les laboratoires nous avons **les correspondants sécurité**, administrateurs informatiques et réseaux qui ont participé aux opérations sécurité, **actuellement 300**. En région, chaque équipe de coordinateurs réunit aussi régulièrement, souvent chaque mois, les correspondants sécurité des laboratoires pour effectuer le même travail qu'au niveau national. Ces réunions régionales permettent de créer ainsi des groupes d'administrateurs informatiques qui partagent leurs problèmes et leurs expériences et ainsi coopèrent, sans perdre du temps à redécouvrir ce qu'un autre administrateur a déjà résolu. Ceci rompt l'isolement des ingénieurs informatiques, un des points faibles de l'organisation des laboratoires.

Nous avons ainsi un réseau à 2 niveaux. Ce réseau et tous les échanges qui s'y font permettent d'aider les laboratoires tout en tirant partie d'un avantage du CNRS déjà cité, les différentes compétences réparties dans les unités. Il permet ainsi maintenant de facilement mettre en place les actions décrites ensuite : formation, diffusion d'information, gestion des incidents, …

6.3 Problème de cette organisation

Le talon d'Achile, qui posera certainement des problèmes à moyen terme, est que ce dispositif repose sur des personnes rattachées à des laboratoires qui assurent ces tâches, avec l'accord de leur directeur, en plus de leur travail quotidien dans leur unité. Dynamiques, ces personnes sont facilement volontaires pour participer ou mener des actions dans le domaine nouveau et techniquement intéressant de la sécurité où beaucoup de choses restent «à découvrir ». Mais cette nouveauté risque de ne pas durer. Il faudrait revoir ce principe du volontariat systématique. Mais ce n'est pas le but de ce document qui se veut uniquement être un bilan.

7. La formation SIARS : Sécurité Informatique pour les Administrateurs Réseaux et Systèmes

Des journées de formation (sensibilisation, protection du patrimoine, …) sont organisées par différentes structures (DCSSI, ministère, ...) où des places sont réservées au personnel CNRS. Mais elles ne couvrent pas les besoins «de base » des administrateurs systèmes et réseaux des laboratoires. A chaque opération sécurité, nous assurons des présentations ponctuelles d'outils et de mécanismes de sécurité. Mais nous ne pouvons répondre à toutes les attentes d'information. Nous avons aussi fait le constat que **les ingénieurs dans les laboratoires n'ont pas été formés pour définir une politique de sécurité informatique dans leur laboratoire et se trouvent dépourvus au moment de choisir et d'installer les bons outils**. En parallèle, les produits de

protection sont maintenant nombreux et un ensemble de méthodes, de techniques et d'outils, souvent du domaine public, «acceptables » par un laboratoire sont disponibles. Ce sont les raisons pour lesquelles les coordinateurs et les correspondants sécurité nous ont demandé une formation de base dans ce domaine mais concrète et adaptée aux laboratoires.

Nous avons fait un tour d'horizon des différentes formations proposées par les entreprises ou organismes spécialisés. Notre conclusion est qu'elles sont coûteuses (environ 3000 F par jour par personne), trop détaillées (une semaine pour chaque type de système informatique par exemple) ou trop générales (sans présentation d'outils concrets). En résumé, elles ne sont pas adaptées à des ingénieurs qui administrent des équipements réseau et des systèmes informatiques très variés et qui doivent aussi veiller à leur sécurité.

L'UREC a donc décidé de mettre en place une formation dans ce domaine en coopération avec la formation permanente du CNRS (http://www.urec.cnrs.fr/securite/formation.6.pdf) . Nicole Dausque (UREC) en assure la coordination. Le bureau national de la formation permanente nous appuie totalement dans ce projet.

Un **comité de pilotage** a été constitué et s'est réuni en octobre 2000. Constitué de A. Marchal, Délégué de Bretagne (président), Y. Ellien bureau national de la formation permanente, N. Lucciani-Chapuis responsable formation permanente Marseille, P. Richy expert extérieur (France Télécom, enseignant ENST), Y. Deswartes expert CNRS (Directeur de recherche au LAAS), A. Schwenck Fonctionnaire de défense, S. Manoussis chargé de mission informatique du département SDU, M-A Caron DRH, J. Marchand administrateur informatique laboratoire de Maths, J-L Archimbaud et N. Dausque UREC, ce comité nous a vivement encouragé dans cette démarche et s'est montré très intéressé par suivre le déroulement.

Le principe le plus efficace et le moins coûteux que nous avons retenu est de **former les coordinateurs pour qu'ils forment à leur tour les correspondants**. Les coordinateurs seront donc des formateurs.

Nous avons défini et suivons 3 étapes :

1. **Préparation du programme et du support de cours** avec un sous-ensemble des coordinateurs, chaque participant amenant une compétence dans un domaine. Ce sont **les 15 rédacteurs** listés en annexe 14.3. Ce travail s'est déroulé fin 2000. On dispose ainsi d'un support de cours, ouvrage collectif, de plus de 400 pages. Les chapitres, tous ayant trait à la sécurité, sont :

- Organisation, méthodologie et législation
- Eléments de base (TCP/IP, cryptographie, IGC, …)
- Unix
- Windows-NT et Windows-2000
- Services réseaux locaux
- Services Internet
- Postes individuels
- Applications

- Architectures réseaux
- Outils de sécurité et applications sécurisées
- Recommandations, mise en œuvre

2. Avec le bureau national de la formation permanente, **formation de tous les coordinateurs sécurité** pendant 2 semaines en janvier 2001, avec la partie technique assurée par les rédacteurs du cours et un jour de pédagogie donnée par une société externe. Le but était de former ces coordinateurs pour qu'ils acquièrent les bases techniques nécessaires pour leur travail de coordination régionale et pour qu'ils puissent redonner cette formation à d'autres ingénieurs : les correspondants sécurité. Cette formation s'est très bien passée et tous les coordinateurs ont été volontaires pour organiser cette formation dans leur région respective.

3. **Formation des correspondants sécurité des laboratoires** d'une durée de 6 jours, organisée par les coordinateurs avec le responsable de la formation permanente de chaque délégation. Les cours seront assurés par les coordinateurs locaux ou d'autres régions si besoin. L'objectif est de former les administrateurs informatiques de laboratoire pour qu'ils puissent définir une politique de sécurité adaptée à leur laboratoire. C'est à dire conseiller et aider ces administrateurs pour qu'ils acquièrent une méthodologie et une démarche sécurité, une vue des techniques et des outils de protection actuels, et soient aptes à installer un ensemble minimum d'outils de sécurité dans leur laboratoire, ceci avec des critères compatibles avec la vie des laboratoires de recherche. Ces formations seront étalées sur l'année 2001, certaines sont déjà planifiées pour mai-juin 2001. On pense ainsi que les 300 correspondants sécurité auront reçu la formation durant l'année 2001. Une seconde session de formation pourra être redonnée l'année suivante dans certaines régions car on peut penser qu'il y aura d'autres demandes.

La remise à jour du support de cours, indispensable dans ce domaine très évolutif de la sécurité informatique, sera réalisée par les rédacteurs. Si le support de cours, après les nouvelles corrections qui vont arriver, est d'une bonne qualité, nous envisageons de le diffuser sur le Web et peut-être sous forme d'une édition papier. Les universités et d'autres organismes de recherche sont déjà intéressés par ce cours. Les mêmes besoins existent qu'au CNRS et ce support de cours pourrait être ainsi mis à leur disposition.

8. La diffusion et la circulation d'informations

Actuellement, **2 serveurs Web, 3 listes de diffusion et un bulletin d'information** sont nos principaux outils pour diffuser des informations.

L'UREC administre un serveur Web de référence pour les laboratoires sur la sécurité informatique et réseaux http://www.urec.cnrs.fr/securite. Régulièrement mis à jour, il comprend les pages suivantes :

- Des **brèves de clavier** qui annoncent les nouveautés : lois, outils, …
- Les **informations CNRS** qui décrivent l'organisation en place, les contacts, que faire en cas d'incident, les chartes, les recommandations CNRS (serveurs Web, architecture, …), la

description de la formation SIARS, des pages réservées aux coordinateurs sécurité (accès avec certificat)

- Des **informations sur les autorités de certifications** : documents, serveur de certificats CNRS-Test, …
- Des **documentations sur la sécurité produites par l'UREC** : articles, cours et présentations
- Des **outils de sécurité (audit ou prévention) testés et recommandés** par l'UREC pour Unix et Windows NT (cf chapitre 12)
- Des pointeurs sur les anti-virus, les **virus** et les canulars
- Des pointeurs sur les **CERTs** et les avis du CERT-Renater
- Des pointeurs vers d'**autres serveurs** : service juridique du CNRS, CNIL, DCSSI, CRU, …

Ce serveur n'est pas un serveur généraliste sur la sécurité, il est ciblé sur ce qui peut être utile dans ce domaine aux laboratoires du CNRS.

Robert Longeon administre un serveur Web complémentaire dans ce domaine (http://www.cnrs.fr/Infosecu/accueil.html) avec 4 parties :

- Des **informations rapides** : annonces de stages, formations, …
- La **protection du patrimoine**
- La **revue « Sécurité informatique »** (cf ci-après)
- Les **virus** : documentation, pointeurs, anti-virus, …

Trois principales listes de diffusions sont utilisées par les laboratoires :

- **sos-virus**, liste très active avec 5 à 10 messages par jour sur les virus, elle comprend près de 500 abonnés et est ouverte à des personnes d'autres organismes que le CNRS (http://www.services.cnrs.fr/wws/info/sos-virus).
- **csec** qui regroupe les coordinateurs sécurité (44 abonnés). Très modérée et contrôlée, elle permet à ce groupe de travailler ensemble. La diffusion dans cette liste est contrôlée par certificat CNRS-Test.
- **corres-secu** qui regroupe près de 300 correspondants sécurité des laboratoires CNRS. **Les avis du CERT-Renater** sur les vulnérabilités découvertes sont diffusés dans cette liste. Le CERT-Renater a ainsi annoncé environ **400 annonces de vulnérabilités durant l'année 2000** rediffusées dans cette liste. C'est aussi notre moyen de diffusion pour annoncer les recommandations CNRS, formations, et d'insister sur certains avis de sécurité du CERT-Renater que nous jugeons importants. L'accès à cette liste est restreint aux correspondants sécurité du CNRS.

Le bulletin « Securité informatique » (http://www.cnrs.fr/Infosecu/Revue.html) dont le responsable de la publication est Robert Longeon, avec une parution de 5 numéros par an, propose des articles de fond sur la sécurité. A titre d'exemple, les derniers numéros ont traité de :

- La politique de sécurité informatique
- La correspondance privée et le courrier électronique
- Les virus

– Les produits de simulations d'intrusion

Tiré à plusieurs milliers d'exemplaires à la fois sous forme papier et avec une diffusion électronique il est très connu et très lu dans les laboratoires et maintenant reconnu à l'extérieur de l'organisme comme un bulletin de référence.

Un **Guide la sécurité des systèmes d'information à l'usage des directeurs** (http://www.cnrs.fr/Infosecu/guide/guide.pdf) de 90 pages a été rédigé par R. Longeon et Jean-Luc Archimbaud. Tiré à plusieurs milliers d'exemplaires, il a été envoyé à tous les directeurs d'unité CNRS fin 1999. Destiné à sensibiliser les directions aux problèmes de sécurité et à présenter les principales vulnérabilités et les premières protections à mettre en place, il a aussi été diffusé dans d'autres organismes de recherche qui étaient intéressés par cet ouvrage.

Autre élément de sensibilisation, lors du **stage destiné aux nouveaux directeurs**, un créneau est réservé à la protection du patrimoine et à la sécurité des systèmes d'information. Assurée par le fonctionnaire de défense, elle permet un dialogue direct avec les nouveaux directeurs.

9. Le traitement des incidents

Une procédure connue des correspondants sécurité de laboratoire et disponible en ligne (http://www.urec.cnrs.fr/securite/chartes/quefaire.html) décrit les mesures à prendre en cas de détection d'un incident de sécurité (intrusion par exemple). Elles consistent à :

- Avertir le responsable sécurité et le directeur du laboratoire,
- Supprimer l'accès au système depuis l'extérieur et faire une sauvegarde pour garder des traces,
- Remplir la fiche "suivi d'incident" et l'envoyer au CERT Renater avec copie aux coordinateurs sécurité nationaux (nous même) et aux coordinateurs sécurité de votre région. (http://www.urec.cnrs.fr/securite/chartes/fiche_suivi_incident.txt),
- En accord avec le Directeur du laboratoire, contacter le fonctionnaire de défense si un dépôt de plainte est envisagé,
- Regarder les dégâts et déterminer la cause de l'incident (http://www.CRU.fr/securite/Documents-generaux/Recommandations.html),
- Réinstaller le système et les comptes utilisateurs,
- Corriger les failles utilisées avant de reconnecter le système à l'Internet.

Nous rappelons ces conseils lors de chaque opération sécurité pour sensibiliser mais aussi rassurer les administrateurs qui sont souvent très « perturbés » par une intrusion.

Lors des intrusions venant de l'Internet, ces dernières années c'est le CERT Renater avec ses 4 permanents qui a assuré l'assistance techniquement aux sites de manière très efficace (http://www.renater.fr/Securite/CERT_Renater.htm). Nous intervenons pour mettre en contact le CERT Renater avec le correspondant sécurité du laboratoire (ou inversement), en cas de besoin spécifique CNRS, pour s'assurer que les recommandations CNRS sont suivies, que les différents

acteurs (direction, … éventuellement d'autres laboratoires) sont au courant et pour d'éventuels conseils de fond (revoir l'architecture du réseau par exemple).

Durant l'année 2000, 61 incidents sécurité nous ont été signalés, en grande majorité des intrusions Internet. Ces chiffres n'incluent pas les tests classiques de vulnérabilité sur Internet (scans) qui ne donnent pas lieu réellement à des intrusions.

10. Les recommandations

Plusieurs recommandations ont été émises dans le domaine de la sécurité informatique et sont toujours d'actualité.

La plus importante est la « **Charte utilisateur pour l'usage des ressources informatiques et de services Internet** » (http://www.cnrs.fr/Infosecu/Charte.pdf). Celle-ci a été publiée au bulletin officiel du CNRS en février 1999. De fait, elle est donc incluse dans le règlement intérieur de chaque unité. Il est recommandé de la faire largement connaître dans les laboratoires (affichage, …) et de la faire signer aux personnes non permanentes dans les laboratoires avant qu'elles accèdent aux ressources informatiques et réseaux du laboratoire. Elle permet entre autres de rappeler la législation française en vigueur (toute tentative de piratage est punie par la loi …), que la sécurité est l'affaire de tous, que les utilisateurs ont des devoirs et que l'utilisation de ces ressources n'est autorisée que dans le cadre de l'activité professionnelle. Cette charte est maintenant largement connue et appliquée dans la grande majorité des unités.

D'autres recommandations ont aussi été diffusées, pour en particulier mieux administrer les services de diffusion d'information Internet. Les laboratoires ont été des pionniers dans l'installation de ces services et ceux-ci avaient été créés dans un esprit de liberté avec un Internet académique convivial, par des « bonnes volontés ». Ces recommandations, rédigées par le **comité de coordination Web** sont destinées à mieux cadrer ces diffusions pour respecter la législation et être en accord avec les missions du CNRS. Actuellement elles sont appliquées sauf exception. Elles sont regroupées dans la page http://www.urec.cnrs.fr/securite/recommandations_cnrs.html :

- **Installation et gestion d'un serveur WWW**
- **Création, administration et gestion des FTP anonymes**
- **Création, administration et gestion des listes de diffusion**

A la demande de la DCAJ et du COMI, nous avons récemment créé un groupe de travail pour essayer d'établir des **Recommandations dans la pratique du métier d'administrateur systèmes et réseaux dans un laboratoire CNRS**. Le but est d'informer les administrateurs sur leurs droits mais aussi leurs devoirs (respect de la législation : confidentialité des correspondances privées, …). L'objectif est de prévenir les excès dans un sens, comportement trop laxiste où on ne surveille plus rien car tout est considéré comme confidentiel, ou dans un autre, comportement trop « policier », des administrateurs.

Toutes ces recommandations ont pour but d'éviter les dérives et si possible d'anticiper les problèmes qui pourraient arriver aux laboratoires dans le monde très évolutif des systèmes

d'information, des réseaux et plus globalement de l'Internet où il n'y a encore ni réglementations, ni lois, ni jurisprudences précises.

11. L'architecture réseau

La plupart des réseaux dans les laboratoires et les campus datent du milieu des années 90 et les laboratoires sont connectés à l'Internet (Renater pour nous) depuis l'origine de ce réseau. Lors du choix de l'architecture interne de ces réseaux et de leur connexion à Renater, le but principal était alors que toutes les machines des sites, sans exception, puissent accéder et être accédées de l'Internet (ouverture totale). L'Internet n'était qu'un ensemble de réseaux de recherche convivial. On n'avait pas d'attaque de spam, scan, smurf, flood, spoofing, sniffer, … Maintenant c'est devenu un outil de communication mondial, utilisé par des bons mais aussi des mauvais citoyens et toutes les déviances courantes y sont présentes. Il a donc fallu revoir l'architecture de nos réseaux pour éviter la prolifération des intrusions.

Nous avons établi en janvier 2000 un modèle de référence d'architecture (cf annexe 14.4) basé sur une segmentation du réseau interne avec :

- Une zone pour les serveurs « publics » (machines accédées depuis l'Internet : serveur Web, messagerie, bases de données publiques, …). Nous recommandons que ces services soient sur des machines dédiées.
- Plusieurs zones internes : une par laboratoire ou équipe de recherche, une pour les salles de TP, une autre pour les serveurs internes, …
- Des filtrages entre ces zones autorisant ou non certains trafics.
- Un filtrage en entrée de site pour ne laisser passer que ce qui est vraiment utile et protéger les machines internes des attaques.

Cette architecture ne réduit pas les services de l'Internet pour le personnel de laboratoire, elle devrait être transparente. Elle permet simplement de faire un tri, ce qui facilite l'administration et la surveillance, et de bien protéger ce qui doit l'être.

Nous présentons cette architecture (http://www.urec.cnrs.fr/securite/articles/archi.reseau.pdf) dans toutes les opérations sécurité et à cette occasion vérifions que les laboratoires évoluent dans ce sens. Tout à fait comprise et admise, l'évolution vers ce modèle est partout en bonne voie. C'est certainement cela qui nous a mis à l'abri d'une avalanche d'attaques qui seraient arrivées ni nous n'avions pas corrigé à temps nos architectures. Cette recommandation est largement connue et est reprise par la plupart des organismes de recherche et des universités.

Il reste actuellement un besoin essentiel à prendre en compte : comment permettre aux utilisateurs à l'extérieur de leur laboratoire, depuis leur domicile, en congrès, … d'accéder à leur boite aux lettres, éventuellement à leur machine et à leurs données, … donc à certains services de leur laboratoire ceci de manière sécurisée (sans que leur mot de passe soit écouté durant leur connexion par exemple). Des solutions techniques existent (SSH, Webmail, IMAPS, IPSec, …) et commencent à être mises en place dans des unités. Mais ce domaine touffu et complexe demande un travail de fond. Nous avons récemment créé un groupe de travail pour évaluer toutes ces méthodes et faire des

recommandations pratiques pour les laboratoires : quels produits utiliser pour quels services ? Marie-Claude Quidoz (UREC) anime ce **groupe de travail « accès distants sécurisés ».**

12. Les outils recommandés et fournis

Il n'existe malheureusement pas « une boite » ou « un logiciel » qui résoudrait tous les problèmes de sécurité des laboratoires. Par contre il existe de nombreux outils, souvent du domaine public, qui peuvent améliorer la sécurité et certains sont adaptés à notre environnement. Il faut donc faire un choix. Avec l'aide des coordinateurs et des correspondants, **nous tenons à jour une liste d'outils que nous avons testés et que nous recommandons**. Régulièrement de nouveaux tests sont effectués sur de nouveaux logiciels qui apparaissent. Dans les derniers mois la liste des outils pour Windows-NT et Windows-2000 s'est par exemple beaucoup étoffée suite à de nombreux tests réalisés.

Ces outils logiciels (vérification de la solidité des mots de passe, contrôles d'accès réseau, vérification de l'état des systèmes, …) sont disponibles sur le serveur de l'UREC dans les pages : http://www.urec.cnrs.fr/securite/outils/nt/ et http://www.urec.cnrs.fr/securite/outils/. Les principaux sont présentés dans la liste de contrôles utilisée pour les opérations sécurité et ils sont aussi longuement décrits dans le cours de formation SIARS. Il y a donc une même recommandation entre ces différents moyens de diffusion.

Parallèlement, les laboratoires peuvent obtenir gratuitement certains antivirus (Norton, Fsecure-AVP, Virus scan) auprès des CRI principalement des universités.

Pour compléter les opérations sécurité en 1999 nous avons acheté 2000 licences d'un logiciel de détection de vulnérabilité sur le réseau appelé IS (**Internet Scanner**) avec 2 ans de mise à jour. Ce logiciel est en fait une liste de 700 contrôles qui s'exécutent automatiquement depuis un poste vers des stations via le réseau. Il a été diffusé par l'UREC aux laboratoires qui ont suivi les opérations sécurité. Pouvant être dangereux dans une utilisation non contrôlée, cette diffusion a été accompagnée d'une méthodologie de mise en œuvre : rédaction de recommandations d'utilisation, formation des administrateurs à l'utilisation, utilisation par ces administrateurs dans leur unité et bilan.

13. L'autorité de certification

Les actions décrites dans les chapitres précédents sont des mesures défensives, pour se protéger contre des attaques. De plus, elles ne permettent pas d'apporter des services de sécurité (authentification, intégrité, confidentialité, contrôle d'accès) aux applications utilisées au CNRS : messagerie, accès aux serveurs Web, applications de gestion, ...

La mise en place d'une **autorité de certification, la création et l'utilisation de certificats électroniques**, **vont dans le sens d'une sécurité active**. Et ces éléments constituent la fondation sur laquelle pourront s'appuyer toutes les applications au CNRS (http://www.urec.cnrs.fr/securite/articles/certificats.kezako.pdf). De plus, ces mécanismes pourront

permettre des économies importantes en utilisant mieux le réseau. Ainsi lorsque chaque personne travaillant dans un laboratoire aura un certificat, ceci permettra :

- De diffuser toutes les notes officielles (ou équivalentes) par voie électronique. Actuellement cette option techniquement possible est trop dangereuse, car l'origine des messages n'est pas garantie. Quand chaque directeur et responsable aura un certificat, il pourra signer tous ses envois électroniques et ainsi garantir l'origine et l'intégrité des messages émis.
- Les certificats pouvant être utilisés pour assurer en plus la confidentialité et l'intégrité des messages, ceci permettra d'utiliser la messagerie électronique pour les élections, les notations, la gestion du personnel, …
- Toutes les applications de gestion pourront s'appuyer sur un seul type de contrôle d'accès : les certificats, mécanisme qui permettra d'homogénéiser les différentes méthodes actuelles.
- On pourra créer des Intranet de personnes pour mettre en ligne des documents uniquement accessibles aux agents CNRS, à un département scientifique, à un laboratoire, à des communautés particulières, … Actuellement ceci très difficilement réalisable.
- Les certificats devraient faciliter la mise en place d'outils pour accéder à distance à sa boite aux lettres, à des machines du laboratoire, … sans circulation du mot de passe en clair sur le réseau.
- Les certificats permettent d'authentifier les machines. Ainsi il sera possible de déployer de manière sécurisée des applications avec un serveur et plusieurs agents distants par exemple.
- Les certificats sont obligatoires dans toute mise en commun de ressources distribuées comme les grilles de calcul où les utilisateurs mais aussi les machines et leurs équipements doivent être authentifiées.

L'UREC a monté une plate-forme de test d'une **autorité de certification CNRS-Test en février 2000 pour évaluer les potentialités des certificats, les procédures et les logiciels à mettre en place, la faisabilité** (http://www.urec.cnrs.fr/securite/articles/CA.CNRS-Test.pdf). Des logiciels ont été développés à partir de briques du domaine public, des procédures écrites et mises en oeuvre et actuellement plus de 100 certificats ont été délivrés. On peut demander un certificat en suivant le mode d'emploi : http://www.services.cnrs.fr/ca/. Ces certificats ont été et sont toujours utilisés par les coordinateurs et correspondants sécurité pour :

- Signer les avis de sécurité du CERT-Renater, garantissant ainsi l'origine et l'intégrité de ces avis de sécurité,
- Chiffrer parfois des communications sensibles (rapports d'incidents de sécurité par exemple),
- Contrôler l'accès à des pages sur un serveur Web, pages réservées aux coordinateurs sécurité,
- Construire le cours SIARS avec une douzaine d'auteurs à distance : mise en ligne des différentes parties du cours, accès contrôlé par certificat en lecture et écriture pour y accéder, les modifier, ...

Ces certificats sont aussi utilisés pour mettre en œuvre les grilles de calcul dans le projet Datagrid (http://grid-france.in2p3.fr/) où un certificat est nécessaire pour chaque station et chaque utilisateur, ainsi que pour sécuriser les communications avec certains serveurs Web, passerelle d'accès à distance à la messagerie interne d'un laboratoire par exemple.

Ces tests ont été très encourageants, en montrant tous les avantages qu'un organisme éclaté comme le CNRS pourrait tirer de ces mécanismes mais en préconisant d'avancer pas à pas dans ce domaine nouveau.

Suite à ces tests, en juillet 2000 la direction du CNRS a décidé de créer une autorité de certification et d'en confier la mise en œuvre à l'UREC (http://www.urec.cnrs.fr/securite/certifications/decision_creation_AC_cnrs.pdf). Un comité de pilotage et un comité technique ont commencé à travailler à l'automne 2000. Une politique de certification et une description des procédures est en cours d'écriture, compatible avec les recommandations du DCSSI et de la commission interministérielle sur le sujet. Un ensemble de logiciels d'IGC (Infrastructure à Gestion de Clés) a été écrit par deux ingénieurs de l'UREC, Claude Gross et Philippe Leca, et est presque finalisé. Un groupe de sites pilotes a été choisi (LAAS, DR de Bordeaux, DR de Toulouse, DSI, IMAG, Datagrid-fr, sécurité). Ces sites vont utiliser les logiciels IGC développés et les procédures définies pour délivrer des certificats à partir de mai 2001 en suivant la politique de certification rédigée. Un bilan devrait avoir lieu fin juin. Le second semestre 2001 devrait être consacré à définir la méthode et les moyens à mettre en œuvre pour déployer la distribution des certificats dans l'ensemble de l'organisme.

En quelques mots, la politique de certification prévoit de délivrer des certificats pour toute personne travaillant dans une unité CNRS (pas uniquement aux agents CNRS) ou sur un projet CNRS, pour tout service réseau (serveur Web, routeur, …) d'une unité, éventuellement pour des codes développés dans les laboratoires (applets par exemple). Il y aura 3 sous-autorités :

- Une autorité CNRS-Standard qui délivrera des certificats pour des usages courants, l'autorité d'enregistrement (la personne qui décide de délivrer ou non un certificat) sera le directeur de l'unité ou son représentant,
- Une autorité CNRS-Plus qui délivrera des certificats pour des actes administratifs. L'autorité d'enregistrement pourrait être le délégué ou son représentant. Ces certificats pourraient être stockés sur une carte à puce, cette option est à l'étude.
- Une autorité CNRS-Projets pour des projets à durée de vie limitée, qui peuvent impliquer d'autres organismes … L'autorité d'enregistrement sera le responsable du projet.

Ceci est un vaste projet qui peut entraîner une révision complète de toutes les procédures administratives basées actuellement sur l'utilisation du papier, avec des gains très importants de productivité et d'efficacité si celles-ci basculaient en procédures électroniques dématérialisées.

14. Annexes

14.1. Rédacteurs de la première liste de contrôles

- Nicole Dausque UREC coordination et responsable de la mise à jour
- Jean-Luc Archimbaud UREC
- Eric Fageol EASI
- Philippe Leca UREC
- Robert Longeon Fct Déf
- Lionel Maurice IDRIS
- Marie-Laure Miniussi DR20
- François Morris LMCP
- Gilles Plançon IDRIS
- Eduardo Sepulveda IPGP
- Philippe Weill AERO

Depuis la première version rédigée début 1998, cette liste est mise à jour régulièrement par Nicole Dausque, Marie-Claude Quidoz et Philippe Leca (UREC)

14.2. Coordinateurs en mars 2001 (44 personnes)

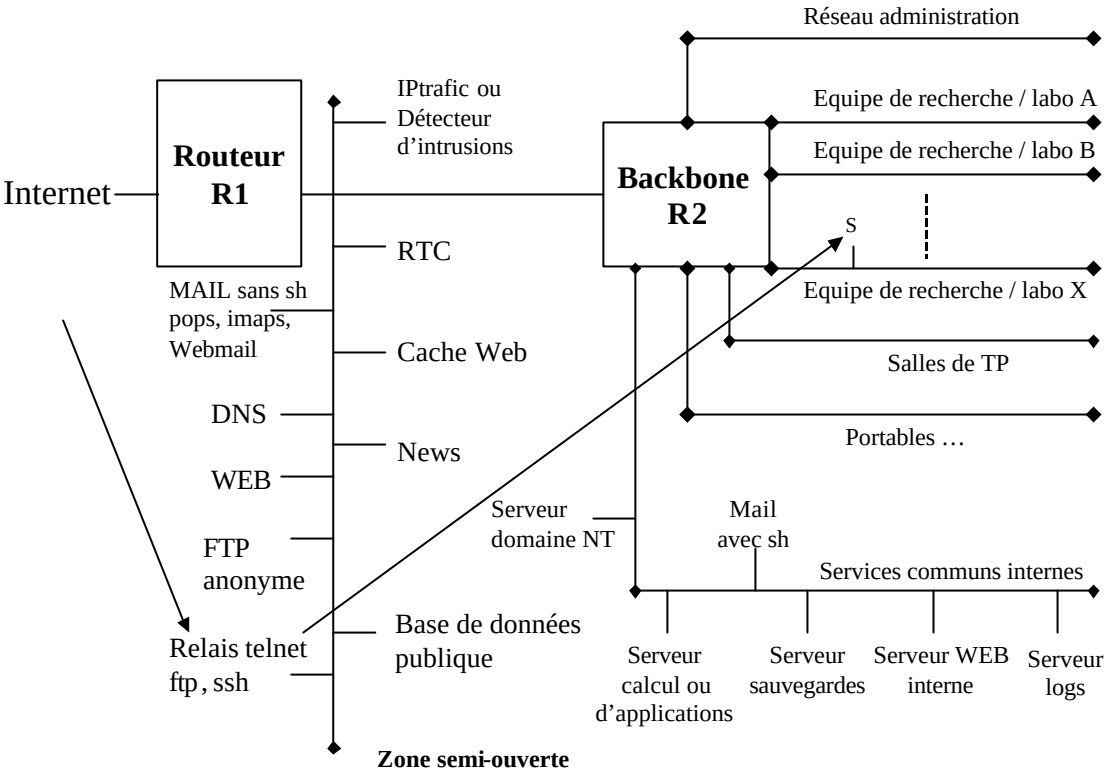
- UREC (pilotage) : Jean-Luc Archimbaud, Nicole Dausque, Marie-Claude Quidoz
- Auteuil : Daniel Nieto, Nicolas Lacheny
- Besancon : Francoise Gazelle
- DSI : Olivier Porte
- Experts : David Gras, Francois Morris, Philippe Weill
- Fct Défense : Robert Longeon, Alfred Schwenck
- Gif : Michel Debest, Jean-Pierre Scarpelli
- Grenoble : Francoise Berthoud, Patrick Juen
- IDRIS : Lionel Maurice, Gilles Plancon
- IN2P3 : Bernard Perrot
- Lyon : Laurence Besson, Ernest Chiarello
- Marseille : Sophie Nicoud, Maurice Libes
- Maths (laboratoires) : Joel Marchand

- Meudon : Jean-Jacques Rivy
- Montpellier : Denis Pugnere, Gilles Requile, Olivier Durant
- Nancy : Gabrielle Feltin, Olivier Servas
- Orléans : Cedric Hillembrand, Lyane Plancon
- Orsay : Jean-Claude Barbet, Jocelyne Sinzelle
- Paris SHS : Benedicte Sabatier, Yolande Kan
- Sophia : Laurent Minou, Eric Drezet
- Strasbourg : Jean-Yves Hangouet, Jean-Michel Trio
- Toulouse : Laurent Bardi, Roland Dartiguepeyron, Matthieu Herrb
- Vitry : Arnaud Dolin

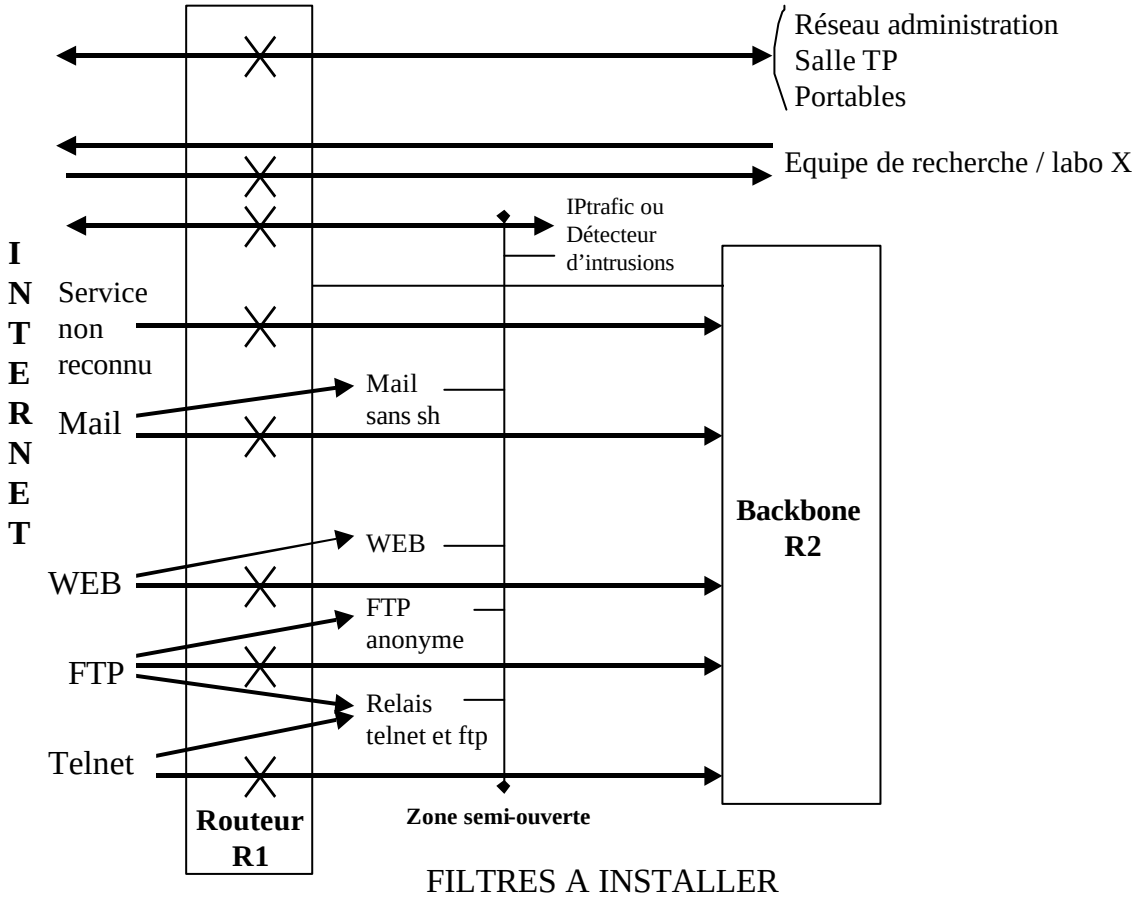
14.3. Rédacteurs du cours SIARS

- Nicole Dausque UREC Coordination
- Jean-Luc Archimbaud UREC
- Laurent Bardi IPBS Toulouse
- Gabrielle Feltin LORIA Nancy
- David Gras Délégation Strasbourg
- Matthieu Herrb LAAS Toulouse
- Philippe Leca UREC
- Maurice Libes Centre d'Océanologie Marseille
- Robert Longeon Fct Défense
- François Morris LMCP Jussieu
- Bernard Perrot IN2P3
- Olivier Porte DSI Meudon
- Marie-Claude Quidoz UREC
- Olivier Servas Délégation Nancy
- Philippe Weill Service d'Aéronomie Jussieu

14.4. Architecture sécurisée et filtres



ARCHITECTURE



FILTRES A INSTALLER