SIARS

(Sécurité Informatique Administrateurs Réseau et Systèmes)

Séminaire 3 juin 2003
Jean-Yves Hangouët

SIARS

- Besoin de sécurité
- Contexte du CNRS
- Différents systèmes d'information
- Acteurs au plan national
- Opérations sécurité
- Organisation humaine
- Formation SIARS
- Extension aux collègues universitaires
- Bilan Région Alsace
- Perspectives

SIARS
Besoins de sécurité

- Alertes de plus en plus nombreuses sur Cert-Renater
  - 100 en 1996 à 400 en 2002
- Machines de plus en plus nombreuses
  - 150.000 en 1995 à 1.500.000 en 2002 sur .fr
- Courbe ascendante du nombre d'intrusion
- Risques classiques omniprésents (vols,négligence, malveillance)
- ➔ **Besoin de protection**

SIARS
Besoins de sécurité

1. **Protection de l'outil de travail**

- Postes informatiques, réseaux, applications et données constituent le système d'information

- Ensemble indispensable à la Recherche (Calcul, expériences, modélisations, bureautique, etc.) et à la gestion des laboratoires

SIARS
Besoins de sécurité

2. **Protection du patrimoine**

- Articles en préparation
- Résultats de recherches
- Développements
- Contrats industriels
- Confidentialité pour certaines disciplines

Mêmes méthodes et mêmes outils pour ces 2 classes de besoins.

SIARS
Contexte du CNRS: Handicaps

- Milieu difficile par sa structure, son mode de fonctionnement et ses missions
  - Structure éclatée : 1300 laboratoires sur plusieurs centaines de sites et campus ouverts
  - Majoritairement unités associées → Politique CNRS à harmoniser avec les autres organismes de tutelle
  - Manque de moyens financiers et personnels
  - Souvent personnels temporaires source de risques
  - Besoins de connectivité internationale
  - Domaines de recherches variés → recommandations adaptées

SIARS
Contexte CNRS: Avantages

- Personnel informatique compétent
  - Esprit d'initiative et de création → CNRS souvent précurseur en informatique et réseau malgré des moyens limités
- Ouverture, échanges et entraide entre ingénieurs ont permis la mise en place de l'organisation d'une politique sécurité efficace avec des objectifs limités mais réalistes

SIARS
3 systèmes d'information au CNRS

- Système d'information de gestion (DSI)
  - Réseau fédérant la DSI et les délégations régionales
- Gros centres de services : IDRIS, INIST,etc.
- Plus de 1300 laboratoires: Serveurs multi-plateformes, réseaux locaux, logiciels divers; choix des laboratoires

Interconnections sur RENATER → Pas d'intranet CNRS

Nécessité d'un niveau de protection minimum pour les laboratoires

SIARS
Acteurs au plan national

- Le service du fonctionnaire de défense
  - 2 ingénieurs chargés de mission
    - Pour les systèmes : Robert Longeon
    - Pour les réseaux : Jean-Luc Archimbault
- L'UREC (Unité REseau du CNRS)
  - 15 ingénieurs
- Responsables sécurité IN2P3, IDRIS, DSI
- Coordinateurs régionaux
- Collaboration avec le CERT-Renater(Computer Emergency Response Team)

SIARS
Opérations sécurité (1/2)

- Fin 1997 opérations sécurité informatique et réseaux menées dans les régions
- But:
  - Sensibiliser les directeurs
  - Etablir un bilan des vulnérabilités
  - Proposer des actions correctrices et des outils
  - Proposer des améliorations de l'organisation technique et humaine
  - Vérifier l'application des recommandations CNRS
  - Créer un réseau humain

SIARS
Opérations sécurité (2/2)

- Mode opératoire
  - 2 jours en régions
    - ½ journée sensibilisation directeurs (UREC, DST,fonctionnaire défense)
    - 1,5 jours administrateurs système – présentation liste de contrôle
  - Liste de contrôle (38 pages version avril 2003)
  - Compilation des listes de contrôle par les coordinateurs régionaux (2 par région) après 3 semaines
  - 1 jour de bilan puis rapport centralisé par l'UREC

SIARS
Organisation humaine

- Coordinateurs sécurité (55 personnes):
  - Deux coordinateurs par région
  - Responsables sécurité IDRIS, IN2P3, DSI
  - Quelques experts
- Correspondants sécurité dans les laboratoires (476 personnes)
  - 1 par unité

SIARS
Coordinateur Sécurité: mission

- Désigné par le Délégué régional
- Liaison National <-> Laboratoires
- Coordination – animation du groupe des correspondants sécurité régionaux
- Expertise technique
- Participation au travail national
- Diffusion d'information
- Se tenir informé des incidents
- Mise à jour de la liste des correspondants
- Organisation de formation, réunions, séminaires, journée thématique, .. ☺

SIARS
Correspondant sécurité: mission

Dans son unité

- Faire appliquer les recommandations
  - Venant des instances nationales
- Prendre les bonnes mesures en cas d'incident:
  - Procédure Mayday
  - Avertir coordinateurs et instances nationales
- Sensibiliser les utilisateurs

En concertation avec le directeur de l'Unité

SIARS
Formation SIARS

- Mise en place d'un cours sécurité informatique de 7 journées
  - 2 jours + 3 jours + 2 jours à 15 jours d'intervalle

  À destination des correspondants sécurité
- Elaboration du cours en octobre 2000 sous l'égide de l'UREC
- Formation des coordinateurs régionaux en janvier 2001
- Formation des correspondants en régions par les coordinateurs

SIARS
Contenu du cours

- Cours de 500 pages couvrant:
  - Organisation, méthodologie et législation
  - TCP/IP, menaces, cryptologie et applications
  - Systèmes UNIX
  - Systèmes Windows
  - Services réseau locaux, services Internet
  - Problématique des postes individuels
  - Applications sécurisées
  - Architecture réseau
  - Outils de sécurité

SIARS
Bilan régional

- 2 stages organisés 12/2001 à 02/2002 pour les correspondants sécurité des labo CNRS: 32 administrateurs formés
- Bilan très positif
- Mise en place d'un groupe de travail régional sur la sécurité informatique

SIARS
en milieu universitaire

- Demande forte et légitime de nos collègues universitaires
- Constat d'une absence complète de formation des collègues universitaires concernés
- Mise en place de stages par le groupe X/STRA avec l'accord du CNRS et de l' UREC
- 1 stage 15 personnes Hiver 2002
- 1 stage 15 personnes Printemps 2003
- 1 stage 15 personnes prévu Automne 2003

SIARS
Perspectives régionales

- Travaux pratiques sur des sujets d'actualité
- Déploiement de solutions garde-barrière après études concertées
- Groupe d'entraide de 60 ingénieurs en charge de sécurité informatique dans les laboratoires et unités de services communs

SIARS
Perspectives au plan national

- Support du cours SIARS mis désormais à disposition
  - Universités – CRU : Jean-Paul Leguigner
  - INRIA : Luc Saccavini
  - INSERM : Laurent Bloch
  - CEA : Laurent Cabirol
  - RENATER : Dany Vandromme
  - Ministère de la Recherche : Françoise Brouaye
  - Ministère Education Nationale : Nadine Jude
  - CERT-A : Michel Dupuy
  - CNES : Yvon Klein
  - DSSSI/CFSSI : Philippe Wolf
  - IRD : Luc Veillon

SIARS
Conclusion

Grâce à cette opération

- Prise de conscience des directeurs et des responsables des enjeux
- Bilan et mise en place d'une politique sécurité
- Aide à la mise en place d'architecture réseau, de systèmes et d'applications sécurisées
- Reconnaissance d'un travail souvent ingrat
- Mise en place d'un réseau humain indispensable dans notre difficile métier