Université Pierre et Marie Curie (Paris VI) **Université René Descartes (Paris VII)**

Commission Réseau du Campus Jussieu
Groupe Sécurité
[groupe-securite@ccr.jussieu.fr]

Les réseaux du campus Jussieu et la sécurité informatique

1 - Sensibilisation

Si vous êtes utilisateur(trice) d'un ordinateur connecté au réseau informatique du campus, vous êtes concerné(e) : lisez attentivement ce papier.

Les réseaux informatiques du campus Jussieu font partie de l'*Internet*, un vaste réseau informatique qui couvre une grande partie de la planète. Le chercheur qui s'y connecte accède facilement à de nombreux services. Mais il s'expose du même coup à des risques, car la connexion de plus en plus performante à cet espace informatique ouvre de fantastiques perspectives à la communauté scientifique et... aux pirates. Le problème est que si l'on accède, à partir de son réseau local à tout l'*Internet*, l'inverse est également vrai.

Ce premier document est une mise en garde contre les risques liés à la connexion à l'*Internet*. Il ne les recense pas de façon exhaustive et ne dit pas comment s'en prémunir. Ce sera le rôle des documents suivants.

1 La nature des risques

En plus des risques physiques (vol de micro-ordinateur, coupure de réseau...) les risques logiques sont de plusieurs ordres:

1. **confidentialité**: le vol de données est peut-être le risque le moins grave en milieu universitaire naturellement ouvert. Néanmoins, certains projets, par exemple en liaison avec des contrats de recherche, peuvent nécessiter une certaine confidentialité...
2. **intégrité**: les atteintes à l'intégrité du système et/ou des données peuvent être, par exemple, l'effacement de toute la hiérarchie des fichiers, ou des manipulations plus subtiles parfois longues à déceler (corruption de données, remplacement de fichiers sensibles) qui obligent à une restauration (toujours laborieuse et pas toujours complète) du système et des données.

3. **usurpation d'identité**: l'utilisation frauduleuse d'un compte par vol du mot de passe est sans doute le risque le plus pernicieux. L'*Internet* est construit sur la notion de responsabilité des entités et individus qui l'utilisent. Si quelqu'un emprunte votre identité sur le réseau, ou profite du système ou du réseau local dont vous avez la charge, vous pouvez être tenu pour responsable en cas de négligence quant à la sécurité, et subir des conséquences qui vont de l'exclusion d'accès à certains services à la déconnexion pure et simple, sans parler des conséquences administratives et... des dommages subis par votre réputation et par celle de l'université.
4. **indisponibilité**: l'accès au service informatique peut être perturbée, par exemple, par des blocages de modems, des virus rendant inutilisable votre imprimante, des manipulations d'éléments du réseau, des abus d'utilisation (saturation de serveur et/ou de réseau), des tentatives de *login* jusqu'à blocage du compte, etc. Cela n'est pas forcément de la malveillance à proprement parler, mais cela entre dans le cadre de la mauvaise utilisation des ressources informatiques mises à votre disposition.

À ces quatre risques on pourrait en ajouter un cinquième: celui de succomber soi-même (ou de voir succomber un proche) à la tentation de se lancer dans le piratage. La tentation peut être forte (par exemple par esprit ludique) et les risques peuvent paraître faibles. Néanmoins les sanctions administratives et judiciaires sont désormais considérables.

2 Quelques exemples

- Propagation d'un virus par le réseau (ou par disquette) qui bloque pendant un bon moment le fonctionnement du réseau d'un laboratoire. Cela empêche tout le monde de travailler.
- Espionnage d'un réseau de laboratoire à l'aide d'un *sniffer* (pour y extraire des trames contenant des mots de passe). Cela permet de s'introduire sur des machines non autorisée par usurpation d'identité.
- Prêt de son mot de passe à son fils, qui le prête à ses copains, qui se font prendre en train d'essayer de *pirater* des machines de par le monde. La responsabilité du propriétaire du compte est engagée.
- Exécution d'un programme spécialisé (et très facile à se procurer) qui donne en quelques minutes les mots de passe les plus simplistes. Tous les comptes ainsi *crackés* sont visités.
- Infiltration d'intrus sur une machine de laboratoire qui se livrent à quelques subtiles modifications du système (difficilement décelable par l'administrateur) afin de l'utiliser comme base pour d'autres attaques. Il y a alors la menace de déconnexion de l'*Internet* si le problème n'est pas rapidement résolu. La responsabilité du laboratoire et/ou du campus est engagée.

3 La situation à Jussieu

Nous avons eu beaucoup de chance jusqu'ici: il n'y a eu que peu d'incidents sérieux à Jussieu. Mais si rien ne se fait, les problèmes vont rapidement se multiplier à l'instar d'autres entités...

Il y a sur Jussieu beaucoup de systèmes vulnérables: mal configurés, sans suivi, voire pas gérés du tout. Cela va de la station de travail sans mot de passe ou avec des mots de passe triviaux, jusqu'aux ordinateurs bien gérés mais avec des versions de système obsolète et/ou des logiciels constructeurs présentant des failles de sécurité, en passant par le prêt de compte...

Il faut quand même savoir que ce sont des cibles faciles, bien visibles à travers l'*Internet*. Il peut sembler qu'une cible paraisse sans intérêt : ça n'est jamais le cas puisque, une fois cette machine *piégée*, elle peut fournir aux pirates des informations permettant la connexion vers une autre machine. Ainsi, de proche en proche, les pirates peuvent accéder à des machines qui étaient leurs véritables cibles en vous transformant en complice qui devra alors se battre pour prouver son innocence ! Votre machine peut donc être un *nid de coucou*.

Les PC et MAC sont relativement moins vulnérables aux attaques par réseau mais, par contre, constituent d'excellentes bases de départ d'attaques. Les libre-services en sont souvent équipés... De plus, ils sont bien plus vulnérables aux virus.

4 Des éléments de réponse

Un certain nombre de précautions élémentaires devraient permettre une protection suffisante

- des réseaux de Jussieu contre les attaques venant de l'extérieur
- des réseaux Internet (Jussieu compris) contre des attaques venant de... Jussieu (machines en libre service, accès téléphoniques et Transpac, etc).

Cela n'empêche pas la mise en place d'outils plus complexes mais plus contraignants qui ne seraient activés qu'en cas de problèmes sérieux. Il y a un compromis à trouver entre la facilité d'accès aux services Internet et le niveau de sécurité désiré.

Un certain nombre d'acteurs se sont mis en place (ou vont s'y mettre) pour combler le *déficit sécurité* créé lors de l'extension rapide des réseaux :

1. Nos autorités de tutelle (Ministère de l'Enseignement Supérieur et de la Recherche, CNRS) ont mis en place des structures de sécurité des systèmes informatiques: hauts fonctionnaires de défense, organismes de coordination (CRU pour MESR, UREC pour CNRS), nomination de correspondants sécurité (un par université ou grande école) et organisation de leur formation, etc.
2. Le Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche (RENATER) a mis en place un certain nombre de services sécurité de base (authentification d'adresse d'appelant et contrôle d'accès au niveau réseau, confidentialité des données pendant leur transit sur RENATER) et complémentaires (contrôle d'accès étendu, chiffrement) assurés par l'opérateur (France Télécom). Une charte de bon usage et de sécurité doit être signée par les responsables des sites contractant au niveau des ministères. Un CERT (Computer Emergency Response Team) a été créé pour la prévention et la coordination des actions à mener en cas d'attaque (virus, intrusion...)
3. Au niveau des universités, des laboratoires, des divers centres de calculs de Jussieu, il devra y avoir adoption d'une attitude claire vis à vis de ces problèmes (matérialisée, par exemple, par la mise en place pour tout le campus d'une **Charte de bonne utilisation des ressources informatiques** comme c'est déjà le cas pour le CCR et le CICRP) qui évite la dilution des responsabilités et serve de base à la mise en place d'une politique globale de sécurité informatique cohérente.

4. La Commission Réseau du campus a mis en place un **groupe sécurité** avec pour rôle la sensibilisation (ce papier en est la première émanation), la collecte et la diffusion des informations à ce sujet, l'élaboration de recommandations pour la mise en place d'un *minimum de sécurité* sur toute machine du Campus, la mise à disposition de logiciels apportant un plus par rapport aux systèmes standards. Il peut également être mis en place au niveau de la *dorsale* du réseau Jussieu des mécanismes d'audit et de contrôle des accès.

5. La prise de conscience de ces problèmes doit mener chaque laboratoire à s'impliquer dans l'administration de ses systèmes : il y a nécessité d'avoir un (ou plusieurs) administrateur(s) système et réseau dans chaque laboratoire connecté. Le réseau peut alors se révéler très utile pour developper les compétences de ces administrateurs par échange d'informations (liste de diffusion, e-mail, news, ftp, etc). La mise à niveau des systèmes, installation des *patches* (corrections fournies par le concepteur ou diffuseur du logiciel), correction des erreurs de configuration, installation de mécanismes d'audit et/ou de filtrage fera partie de leurs attributions.

6. Mais la sécurité de l'ensemble du réseau du campus dépend **avant tout** de la prise de conscience des risques par chacun des utilisateurs (même occasionnels) et responsables des laboratoires et unités.

5 Pour résumer...

On le voit, la sécurité informatique ne doit plus être prise à la légère. Il faut donc mettre en place des garde-fous pour éviter au maximum les risques de malveillance venant de l'extérieur et partant de Jussieu tout en restant un monde ouvert.

Il n'y a pas de *cent-pour-cent sécurité* à partir du moment où on est connecté. Aucun remède miracle n'existe, mais pour éviter le *zéro-pour-cent sécurité*, il n'y a souvent besoin que d'un certain **bon sens** et un peu de temps. Les outils sophistiqués de protection ne sont en général pas nécessaires sauf pour des laboratoires ou machines potentiellement *intéressants* (en entrée) ou d'accès *moins contrôlés* (en sortie).

C'est d'abord une question humaine : prise de conscience individuelle, disponibilité et formation des utilisateurs et administrateurs. La sécurité informatique de tout le campus n'est que l'addition des mesures prises au niveau de chaque ordinateur : il ne sert à rien de *blinder* une machine si ses voisines présentent d'énormes failles de sécurité.

Enfin, bien que ce soit souvent en conflit avec d'autres priorités, les responsables des laboratoires et services doivent prendre conscience de la nécessité de consacrer des ressources à la sécurité des systèmes informatiques (temps, équipements, crédits, etc).

Le campus Jussieu peut et doit se prémunir afin que les activités de recherche et d'enseignement puissent s'exercer dans les meilleures conditions possibles avec des outils informatiques sûrs et performants.