Sécurité

Les problèmes à résoudre

• Pas d'utilisation non autorisée des services:
  – identification de l'usager et contrôle de l'identification
  – contrôle de l'accès sélectif aux ressources
  – enregistrement de l'usage des ressources

• Confidentialité des données et des messages

• Intégrité – Protection contre la perte ou la modification

• Disponibilité – Absence de refus de service

Remarque : C'est un problème aussi matériel

Comment les résoudre

Les solutions les plus simples :
• supprimer le partage des ressources, isoler les machines (ou les éteindre)
• construire une salle blindée et cage de Faraday avec gardes (et leur faire confiance)
• sauvegarde, copies hors site

—> La sécurité est un compromis entre services offerts et contrôles
Il n'y a pas de sécurité à 100%
C'est avant tout un état d'esprit, et un choix après évaluation des risques

Exemple de risques

Problèmes non spécifiques aux réseaux

- Comptes mal gérés : abandonnés, plusieurs utilisateurs
- Mots de passe trop simples, ou ne changeant jamais
- Terminaux laissés connectés sans surveillance
- "Chevaux de Troie" — "path" incorrect, bugs systèmes (sendmail, fingerd, …), déposés par des pirates
- Fichiers mal protégés (passwd, /dev/mem, catalogue de programmes, /etc …)
- Commandes "setuid" et "sushi" (scripts setuid)

Problèmes particuliers aux réseaux

- Existence de machines non administrées
  –> ne plus faire confiance aux noms et numéros de compte
- Réseau à diffusion
  –> écoutes possibles, fausses identités, routes fausses
- Accès à travers un réseau mondial
  –> propagation des virus, vers, pirates

Il existe des “packages” clés en main de piratages distribués par ftp

Remarques

Difficile de séparer réseau et machine

–> Il faut voir sécurité du système d'information

Le niveau de sécurité est souvent celui du maillon le plus faible

Critères de choix

- Coût / Efficacité
  - Ex : confidentialité ou intégrité sélective selon l'importance des données
  - temps pour reconstruire le site/coût redondance
- Facilité d'utilisation et d'apprentissage
  - Risque de rejet ou de contournement si trop contraignant
  - Ex: mots de passe compliqués et changeant trop souvent
  - méthodes d'accès aux fichiers
- Souplesse d'adaptation & portabilité
  - Tenir compte de l'évolution, du matériel hétérogène
  - ---> normes, standards
  - Ex: niveaux de sécurité de l'Orange Book
  - Kerberos, DES, …
- Méthode d'audit
  - Après ou pendant le problème
  - Nécessaire pour comprendre et éviter la réédition
  - Mais : Problème du dépouillement
  - Problème du volume de données
- Alarmes quand événements anormaux
  - Ex : charge du réseau
  - appels infructueux

Propriétés liées à la sécurité

Disponibilité – fiabilité

Le réseau doit être opérationnel (en particulier routage fiable).

Les matériels doivent fonctionner.

Les logiciels doivent pouvoir fonctionner (saturation réseau, mémoire - cas des vers et virus).

=>
- Maillage
- Duplication des équipements
- Protection contre l’agression physique (feu, vol, …)

Absence de refus de service

Un intrus ne doit pas pouvoir faire perdre un droit à un tiers.

Point lié à la disponibilité, à l'authentification

Ex. de problème:
un système invalidant un compte si trop d'erreurs de login,
ou interdisant deux login sur un même compte

Confidentialité

Un message doit être compris uniquement par le destinataire.

Remarque : L'indication de trafic est déjà une information.

Exemple de violation : écoute d’un câble ethernet

Solutions :

- chiffrement — problèmes : coût, disponibilité (législation)
- dispersion de l'information

Non répudiation

L'émetteur ne peut nier l'émission, ni le destinataire la réception.

Exemple: transfert de fonds

Solutions :

- trace des transactions sur des machines "sûres"
- numéros de séquences inviolables
- utilisation d'un tiers (notaire)

Intégrité

Un message reçu est identique à celui émis.
Une intrusion est détectée.

Exemple d’intrusion : écoute puis “reexécution” d’un message

Solution : signature, e.g. somme de contrôle codée, avec partie propre à chaque message

Contrôle d'accès aux ressources

Vérifier que l'émetteur à le droit de faire l'opération.

Granularité du contrôle d'accès :

- machines
- services : calcul, impression
- informations - données (lecture, écriture, opérateurs, ...) (problème de taille : nécessité d'une information de contrôle associée à chaque objet)

Différentes méthodes de contrôle :

- mode Unix (utilisateur, groupe, autre)
- listes d'accès
- niveau de sécurité (confidentiel, secret, …)

Problème de délégation : un serveur doit pouvoir hériter des droits de son client.

Identification et authentification

Identification: savoir qui est qui
Authentification: vérifier que X est bien qui il affirme être

Nécessaire dans les 2 sens :

- Appelant (individu) -> Appelé (application)
- Appelé (application) -> Appelant (individu)

• cas d'une machine
En général par l'adresse IP – utilisation du name server pour avoir le nom.

Possibilité d'appel en retour pour identification, e.g. modems, ou sur TCP protocole *authentification server* (RFC 1413)

• cas de l'utilisateur
– Soit on fait confiance à la machine source
Ex: rlogin, rsh : utilisation des .rhosts ou de /etc/hosts.equiv
authentification serveur de TCP

– Soit on ne lui fait pas confiance —>
– mot de passe — problèmes:
Où est il stocké ?
Confidentialité lors du transport dans le réseau
– protocoles par défi/réponse
– certificat d'identité — e.g. Kerberos
– objet que détient l'utilisateur — e.g. carte à puce, calculette SecurId
Problèmes : coût, normalisation

Principes généraux

- **Besoin d'une politique globale, après réflexion globale**

– Une solution clé en main peut ne pas traiter tous les problèmes (chiffrement vs crackers de mots de passe, firewall v.s. action interne, …)

– Besoin d'analyse globale : sauvegardes, contrôles d'accès, protection physique matériel/données, participation des utilisateurs

- **Organisation**

– Nomination d'un responsable sécurité
rattaché à la direction
coordination technique, négociation

– Relais par correspondants, groupes de travail

– Contact avec un CERT

– Vérifier le respect des lois (CNIL, copies, chiffrement, sur la presse/éditeurs "minitels"…) problèmes (chiffrement vs crackers de mots de passe, firewall v.s. action interne, …

- **Définir une charte de bons usages ou un règlement intérieur**

Charte : signée par les utilisateurs, règlement : voté par conseil

– But : Responsabiliser, sensibiliser

– Bon usages des outils : usage professionnel et personnel, pas d'intrusion, pas d'attaque, ne pas rendre vulnérable

– Pas de page WWW personnelle sans autorisation

– Rappel des lois, définir les sanctions internes

– Appliquer les directives des administrateurs du système

Fonctionnement

• **Première sensibilisation**
– direction : responsabiliser
– utilisateurs : motiver - rappels, informations, exemples
– administrateurs : recommandations, diffusions avis CERT

• **Campagnes pour la sécurité**
– comptes dormants
– mots de passe solides, personnels
– sauvegardes
– anti-virus
– protection des serveurs

Références

– Universités http://www.cru.fr/securite
– CNRS http://www.urec.cnrs.fr/securite
  cours
  articles
  exemples de chartes
  adresses utiles

– 3615 CNIL

Schémas techniques - Filtrage

Isolement et filtrages

– complet d'une machine(cage de Faraday)
– d'un service (pas de connexion à l'extérieur, pas de partage)
– par adresses et/ou ports (routeurs filtrants)

Routeurs filtrants

• Filtrage sur adresses (source, dest), type de message (TCP, UDP, source route,…), ports (source/dest)
• Deux politiques
– Refus explicite : on rejette ce qu'on ne veut pas (NIS, tftp,…)
Facile à mettre en place - mais on est sans cesse à surveiller les nouveaux risques.
– Autorisation explicite : on accepte une liste limitée (DNS, mail vers serveur, ftp sortant vers xxx,…), et on ouvre progressivement
Facile à sécuriser - mais risque de mécontentements et lourd à gérer.

Configuration difficile - des outils apparaissent.
Attention : un traffic a deux directions -> plusieurs directives
Peu de traces si problème.

Exemples de filtres :
- Tout traffic entre machine hors réseau local et la machine X
- Le traffic venant de l'extérieur et ayant une adresse source locale (tentative d'intrusion - ou test complexe !)
- Le traffic avec "source routing"

Filtrage - suite

- SMTP (mail) : seulement pour serveurs officiels

type=TCP src@=any dst@=serv-off-X dstport=25 permit ! 1/serveur

type=TCP src@=serv-off-X dst@=any srcport=25 permit ! 1/serveur

type=TCP src@=any dst@=serv-off-X srcport=25 permit ! 1/serveur

type=TCP src@=serv-off-X dst@=any dstport=25 permit ! 1/serveur

type=TCP src@=any dst@=any dstport=25 deny

type=TCP src@=any dst@=any srcport=25 deny

Pour plus de détails, cf. cours Archimbaud (http://www.urec.fr)

Exemple de filtres sur Cisco (à contrôler, non testés)

! supprimer source routing

no ip source-route

! declarer un filtre

interface ethernet 1

ip access-group 101 out

! interdire toute IP veant du resau local (spoofing)

access-list 101 deny ip 192.56.62.0 0.0.0.255 0.0.0.0 255.255.255.255

access-list 101 deny ip 127.0.0.0 0.255.255.255 0.0.0.0 255.255.255.255

! interdire toute connexion IP venant d'une machine

access-list 101 deny ip 129.88.1.1 0.0.0.0 0.0.0.0 255.255.255.255

! interdire toute connexion IP venant d'une machine

access-list 101 deny ip 129.88.1.1 0.0.0.0 0.0.0.0 255.255.255.255

! interdire portmap

access-list 101 deny udp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 111

access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 111

! limiter http a une machine

access-list 101 permit tcp 0.0.0.0 255.255.255.255 192.56.62.20 0.0.0.0 eq 80

access-list 101 deny tcp 0.0.0.0 255.255.255.255 192.56.62.0 0.0.0.255 eq 80

……

! permettre tout le reste (politique liberale !!)

access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255

Schémas techniques - Outils

cf. ftp://ftp.urec.cnrs.fr/pub/securite

Seulement pour audit interne !!

– tcpwrapper : filtrage des connexions aux démons

Filtrages d'accès aux démons selon adresse source, par règles (dans /etc/inetd.conf)

– ISS : Security scanner : audit réseau

Teste des trous de sécurités connus : comptes de service (sync, lp, guest), port 25 (sendmail), aliases mail, ftp anonyme, NIS, NFS, …

– SATAN : audit réseau

mêmes usages que ISS

– COPS : vérifications des trous sur une machine

permissions fichiers, mots de passes, crontabs, suid, ftp anonyme, modification fichiers (calcul signature)

– CRACK : test passwords faibles (dictionnaire)

– Anti virus …

– ssf : accès à distance chiffré (version de ssh adapté à la France) ; ssh (si et quand autorisé)

– pgp/pem : mail sécurisé (si et quand autorisé)

Garde-barrière

Dispositif physique pouvant assurer certaines fonctions de sécurité et placé en un point du réseau

Postulat : Frontière entre le monde extérieur (dangereux) et le monde intérieur (sans danger)

Point de passage obligé où peuvent être assurés :

- L'authentification (fichier de mots de passe)
- Le contrôle d'accès (fichier des droits)
- L'audit, la facturation
- Une certaine convivialité : menu d'accueil
- La conversion de protocoles

Avantages

Permet de ne pas modifier/surveiller tous les systèmes

Inconvénients

Problèmes de performance, charge, fiabilité
Manque de convivialité (indirection)
Point d'attaque privilégié
Attention au contournements (modems, …)

Exemple

Une machine à cheval sur le réseau interne et le réseau externe (X25, ou internet sans routage interne-externe)

- Soit les utilisateurs se connectent sur cette machine pour accéder du monde intérieur à l'extérieur (ou de l'extérieur à l'intérieur)
- Soit des démons relais et filtres (telnet, ftp) sont installés sur cette passerelle

Autres techniques

- **Utilisations de systèmes fiabilisés**
  - Noyau système de niveau au moins C2
  - Authentification par clés: Kerberos, secure NFS
  - chiffrement des données, des messages, …
  - système sécurisé spécifique
- **Fichiers et commandes à surveiller/nettoyer**
  - inetd.conf : tftpd, rexd, fingerd
  - ftp anonyme
  - passwd : éliminer les vieux comptes
  - hosts.equiv
  - uucp, rwhod
  - programmes setuid : PAS de scripts setuid
  - scripts root : PATH= IFS=, fichiers en chemins absolus
  - tables de routage
  - exports NFS, mount avec option setuid
  - sendmail : toujours le dernier patch
  - X11 : pas de xhost +, utiliser xauth
  - logs : commandes, logins, …

Architectures

Pour plus de détails, cf. cours Archimbaud (http://www.urec.fr)

Exemple de liste de contrôle

(Extrait du document “Improving the security of your Unix system”, D.A. Curry, SRI International)

APPENDIX A — SECURITY CHECKLIST

This checklist summarizes the information presented in this paper, and can be used to verify that you have implemented everything described.

Account Security

[ ] Password policy developed and distributed to all users
[ ] All passwords checked against obvious choices
[ ] Expiration dates on all accounts
[ ] No “idle” guest accounts
[ ] All accounts have passwords or “*” in the password field
[ ] No group accounts
[ ] “+” lines in *passwd* and *group* checked if running Yellow Pages

Network Security

[ ] *hosts.equiv* contains only local hosts, and no “+”
[ ] No *.rhosts* files in users' home directories
[ ] Only local hosts in “root” *.rhosts* file, if any
[ ] Only “console” labeled as “secure” in *ttytab* (servers only)
[ ] No terminals labeled as “secure” in *ttytab* (clients only)
[ ] No NFS file systems exported to the world
[ ] *ftpd* version later than December, 1988
[ ] No “decode” alias in the aliases file
[ ] No “wizard” password in *sendmail.cf*
[ ] No “debug” command in *sendmail*
[ ] *fingerd* version later than November 5, 1988
[ ] Modems and terminal servers handle hangups correctly

File System Security

[ ] No setuid or setgid shell scripts
[ ] Check all “nonstandard” setuid and setgid programs for security
[ ] Setuid bit removed from */usr/etc/restore*
[ ] Sticky bits set on world-writable directories
[ ] Proper umask value on “root” account
[ ] Proper modes on devices in */dev*

Backups

[ ] Level 0 dumps at least monthly
[ ] Incremental dumps at least bi-weekly

Discussion

Quelques affirmations à se rappeler:

- Le 0 défaut n'existe pas en sécurité
- L'apport de la sécurité n'est pas quantifiable mais son coût l'est
- La sécurité c'est 80 % de bon sens et 20 % de technique
- La sécurité est une affaire de Direction
- La sensibilisation des utilisateurs est primordiale
- La sécurité doit être traitée globalement
- 75 % des délits viennent de l'intérieur de l'entreprise
- La sécurité doit être prise en compte lors de la conception
- Mesures saines et simples : faire le tri
    - Ne pas connecter les machines avec des données très sensibles sur un réseau
    - Délimiter un périmètre de sécurité et verrouiller (ou contrôler strictement) l'accès à ce périmètre
    - Prévoir plusieurs réseaux étanches entre eux, chacun ayant un domaine d'application particulier ou un niveau de sécurité donné
- Il ne faut pas négliger les risques naturels (feu, eau,...) et la négligence (vol, pas de sauvegarde)

Législation

- Loi du 6 janvier 1978 (Informatique et Liberté)
  Contrôler la gestion d'informations nominatives
- Loi du 3 juillet 1985 (Protection des logiciels)
- Loi du 5 janvier 1988 (loi Godfrain), fraude informatique
  - Les accès illicites à l'information (lecture, modification, ...) ou les tentatives
  - L'entrave au fonctionnement (bombe logique ...)
  - Les associations ou ententes (club de hackers)
- Chiffrement (---> code secret : clé)
  - L'utilisation des produits de **chiffrement est réglementé**
  - Actuellement
    - authentification usage libre
    - chiffrement : usage contrôle selon longueur clé (40 bits libre, au delà autorisation et dépôt des clés)
    - Mais aussi : besoin de déclaration ou autorisation pour la fourniture de logiciel
    - libéralisation très large de l'usage promise.
  - Législations étrangères : varie beaucoup selon pays
    - divergences européennes (commerce vs sécurité)
    - américaine : Très stricte sur l'exportation de produits (impossible d'exporter des logiciels avec DES) Evolution vers libéralisation (?)
    - accords internationaux : via OTAN, Wassenaar

REGLEMENT D'UTILISATION DES MOYENS INFORMATIQUES DES COMPOSANTES, DEPARTEMENTS ET TOUS SERVICES DE L'ETABLISSEMENT

Adopté au Conseil d'Administration du 19 septembre 1997
Modifié au Conseil d'Administration du 20 janvier 1998

Article 1 - DOMAINE D'APPLICATION

Ces règles s'appliquent à toute personne utilisant les systèmes informatiques de l'UJF et les systèmes informatiques auxquels il est possible d'accéder à partir de l'établissement.

Les activités spécifiques liées à l'administration des systèmes et des réseaux par les administrateurs désignés relèvent des règles détaillées en article 6.

On appelle "Utilisateur" toute personne, quelque soit son statut (étudiant, enseignant, chercheur, ingénieur, administratif, personnel temporaire, stagiaire, ...) appelée à utiliser les ressources informatiques et réseaux de l'établissement.

Article 2 - CONDITIONS D'ACCES AUX RESSOURCES INFORMATIQUES ET RESEAUX

L'utilisation des moyens informatiques et réseaux de l'UJF doit être limitée à des activités de recherche, d'enseignement, de gestion ou de vie universitaire. Sauf autorisation préalable, ils ne peuvent pas être utilisés pour des activités faisant l'objet d'un financement extérieur.

L'utilisateur ne peut pas connecter un équipement informatique aux ressources informatiques et réseaux de l'établissement sans autorisation préalable.

L'utilisateur doit respecter les modalités de raccordement des matériels aux réseaux de communication telles qu'elles lui sont précisées par le responsable des moyens informatiques. Ces raccordements ne pourront pas être modifiés sans autorisation préalable.

Le droit d'accès à un système informatique est personnel et incessible. L'utilisateur est responsable de l'utilisation des ressources informatiques (locales ou distantes) effectuée à partir de son droit d'accès.

Le droit d'accès est temporaire ; il est retiré dans les cas suivants :

- La fonction de l'utilisateur ne le justifie plus
- Non-respect du présent règlement

En conséquence

- Si un utilisateur étudiant interrompt sa scolarité en cours d'année,
- Si un utilisateur chercheur quitte de manière définitive un laboratoire de l'UJF,
- Si un utilisateur administratif ou technique quitte de manière définitive son service d'affectation,

Cet utilisateur doit prévenir son responsable des ressources informatiques (administrateur système) pour l'informer de son départ, afin que celui-ci lui retire son droit d'accès. (Additif du Conseil d'Administration du 20 janvier 1998)

Article 3 - RESPECT DU CARACTERE CONFIDENTIEL DES INFORMATIONS

Les utilisateurs ne doivent pas tenter de lire ou de copier les fichiers d'un autre utilisateur sans son autorisation.

Les informations contenues dans les fichiers d'un utilisateur sont privées même si les fichiers sont "physiquement" accessibles.

Les utilisateurs doivent s'abstenir de toute tentative d'interception de communications privées entre utilisateurs.

La création de tout fichier contenant des informations nominatives doit faire l'objet d'une demande préalable auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Les utilisateurs doivent s'abstenir de toute tentative de s'approprier ou de déchiffrer le mot de passe d'un utilisateur, de modifier, copier ou détruire des fichiers d'un autre utilisateur, et de limiter ou d'interdire l'accès aux systèmes informatiques d'un utilisateur autorisé.

Article 4 - RESPECT DES DROITS DE PROPRIETE

Les utilisateurs doivent s'abstenir de faire des copies de tout logiciel autre que ceux du domaine public. Les copies de sauvegardes sont la seule exception.

Article 5 - RESPECT DES PRINCIPES DE FONCTIONNEMENT DES SYSTEMES INFORMATIQUES

_Les utilisateurs acceptent les droits de l'administrateur, tels qu'il sont définis en article 6.

Article 5.1 - Sécurité informatique

Les utilisateurs sont tenus de participer à la sécurité du système (choix de bon mots de passe, protection de son espace de fichier, signaler tout problème de sécurité, ...)

Les utilisateurs ne doivent pas effectuer de manoeuvre qui aurait pour objet de méprendre les autres utilisateurs sur leur identité. L'utilisateur doit respecter les procédures d'authentification en vigueur de façon à ce que les actions qu'il mène au sein des systèmes soient identifiables.

Les utilisateurs ne doivent pas effectuer d'expérimentation sur la sécurité des systèmes informatiques et réseaux, ni sur les virus informatiques sans autorisation préalable. Le développement, l'installation, ou la simple détention d'un programme ayant les propriétés décrites ci-dessous sont également interdits :

- Programmes cherchant à contourner la sécurité d'un système
- Programmes contournant les protections des logiciels

Tout utilisateur d'un réseau informatique s'engage à ne pas effectuer d'opérations qui pourraient avoir pour conséquence :

- d'interrompre le fonctionnement du réseau ou d'un système connecté au réseau;
- d'accéder aux informations privées d'autres utilisateurs sur le réseau;
- de modifier ou de détruire des informations sur un des systèmes connectés au réseau;
- de nécessiter la mise en place de moyens humains ou techniques supplémentaires pour son contrôle.

Article 5.2 Gestion des ressources

Les utilisateurs doivent respecter les règles et procédures mises en place pour l'acquisition et la sortie des données sur les machines de l'établissement. Ils respecteront les procédures et restrictions d'acquisition/extraction des données à partir des supports électroniques. Ceci concerne principalement les accès téléinformatiques et les supports amovibles (disquettes, bandes, etc...).

Les utilisateurs ne doivent utiliser que les ressources pour lesquelles ils ont eu autorisation d'usage. Ceci est valable aussi bien pour les points d'accès, que pour des périphériques (imprimantes, traceurs, ...)

Les utilisateurs sont tenus de participer à l'exploitation des ressources en se conformant aux directives d'exploitation précisant les modalités d'accès et de partage de ces ressources. Le développement, l'installation, ou la simple détention d'un programme saturant les ressources (informatiques et/ou réseaux) sont également interdits.

Article 5.3 Respect d'un comportement correct

Un utilisateur ne doit pas utiliser les systèmes informatiques pour harceler d'autres utilisateurs par des communications non souhaitées par les tiers ou pour afficher/diffuser des informations illégales.

Il est rappelé que des lois plus générales s'appliquent pour des informations ou messages :

- à caractère injurieux,
- à caractère pornographique,
- à caractère diffamatoire,
- d'incitation au racisme,
- etc ....

Article 6 - DROITS ET DEVOIRS DE L'ADMINISTRATEUR D'UNE RESSOURCE INFORMATIQUE

Article 6.1 Les devoirs de l'administrateur

Les administrateurs sont responsables de la qualité de service des ressources qu'ils ont en charge.

Les administrateurs doivent appliquer la politique de sécurité informatique définie par l'établissement et donc appliquer les recommandations fournies par le responsable sécurité de l'établissement.

L'administrateur est tenu de prévenir le responsable sécurité de l'établissement lors de détections de problèmes de nature sécuritaire sur les équipements dont il est le responsable.

Lorsque l'administrateur détecte (ou est informé par un utilisateur) de problèmes liés à la sécurité informatique, il doit avertir le responsable sécurité de l'établissement. Ce dernier en fonction de la nature des problèmes et son degré de gravité déclenche un audit de sécurité avec l'administrateur.

L'administrateur doit respecter la confidentialité des fichiers utilisateurs, des courriers et des sorties imprimantes auxquels il peut être amené à accéder lors de ses tâches d'administration et/ou lors d'audit de sécurité. (Notion de secret professionnel)

Article 6.2 Les droits de l'administrateur

L'administrateur est responsable de la distribution et du retrait des droits d'accès.

Les administrateurs doivent faire respecter les droits et responsabilités des utilisateurs présents sur leurs ressources.

L'administrateur se réserve le droit de prendre toutes dispositions nécessaires pour assumer ses responsabilités et permettre le fonctionnement optimal des ressources informatiques qu'il a en charge. L'administrateur peut prendre des mesures "conservatoires" (arrêts de travaux, suppression de droits d'accès, verrouillage de fichiers, ...) en vue de :

- Arrêter un engorgement de ses ressources
- Figer un état lors de problèmes liés à la sécurité des systèmes informatiques

L'administrateur peut :

- accéder à des fichiers ou des courriers en vue de réaliser un diagnostic, une correction d'un problème et/ou s'assurer du bon fonctionnement des ressources qu'il a en charge.
- examiner des données utilisateurs en vue d'assurer la bonne marche du système qu'il a en charge et/ou de s'assurer du bon respect du règlement de la part des utilisateurs.
- contrôler la bonne utilisation des ressources et prendre des décisions pouvant affecter l'espace fichier ou les travaux lancés par un utilisateur.
- surveiller en détail les sessions de travail d'un utilisateur soupçonné de non-respect du présent règlement.

Tout utilisateur n'ayant pas respecté le règlement énoncé ci-dessus est passible de poursuites :

- **internes à l'établissement**
- **pénales pour les infractions relevant du Nouveau Code Pénal.**