La sécurité des postes clients

Marie-Claude QUIDOZ - CNRS/UREC

11/05/2004

Introduction (1)

- **De nombreuses façons de traiter le sujet**
- **Par point de vue :**
  - **d'un utilisateur : besoins / refus / soucis**
  - **d'un administrateur : administration / sécurité**
  - **…**
- **Par catégorie :**
  - **Par opposition (tous sauf un serveur)**
  - **Par type de machines (fixe ou portable)**
  - **Par système d'exploitation (Windows, Macintosh, Unix, …)**
  - **Par technologie (Wifi, Bluetooth, Firewall, …)**
  - **…**

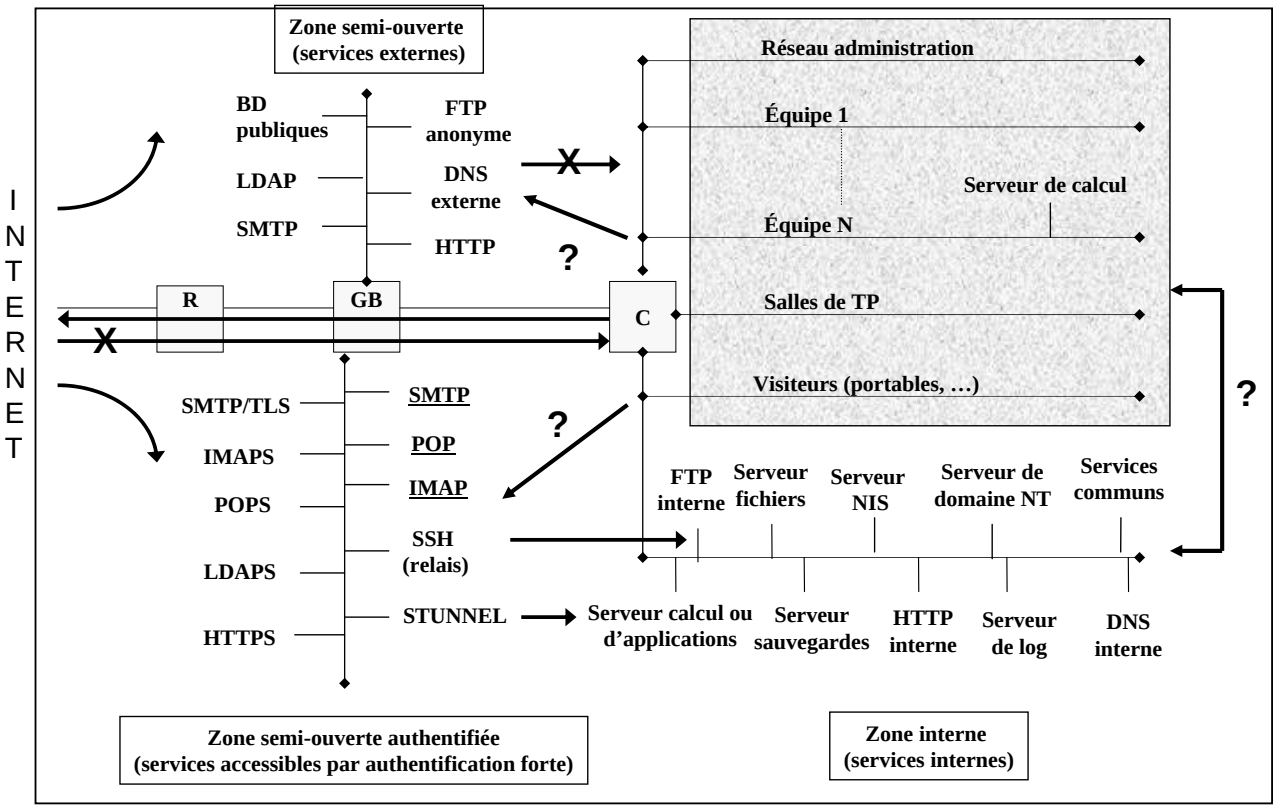
Introduction (2)

- **Trame suivie : plutôt point de vue de l'utilisateur**
- **Le but de cette présentation n'est pas d'apporter des réponses toutes faites**
- **Mais de poser des questions et d'essayer d'apporter des éléments de réponses qu'il vous faudra adapter à votre environnement**
- **Cf. chapitre 8 de SIARS https://www.urec.cnrs.fr/securite/corres-secu/support-siars-mars2003.pdf**

Définition / postes « individuels »

- **Où sont-ils situés / architecture sécurisée ?**
- **A quoi servent-ils ?**
- **Par qui sont-ils utilisés ?**
- **Par qui sont-ils gérés ?**
- **Où sont-ils utilisés ?**
- **A qui appartiennent-ils ?**
- **Quels sont les risques ?**
- **…**

Où sont-ils situés / architecture sécurisée ?



A quoi servent-ils ?

- **Bureautique :**
  - **Traitement de texte, présentation, ...**
  - **Messagerie, consultation de site web**
- **Calcul scientifique :**
  - **Programmation, calcul, …**
- **Machine d'expérimentation :**
  - **Robot, sonde, expérience scientifique, …**
- **Poste individuel ou poste collectif ?**
  - **Bureautique = poste individuel**
  - **Calcul scientifique = poste individuel et/ou poste collectif**
  - **Machine d'expérimentation = poste collectif**

Par qui sont-ils utilisés ?

- **Utilisateurs permanents :**
  - **Informaticiens**
  - **Non informaticiens**

- **Utilisateurs non permanents :**
  - **Stagiaires**
  - **Étudiants**
  - **Visiteurs**

- **Deux populations très différentes ?**
  - **Connaissances / règlements**
    - **Charte Renater, charte du laboratoire, lois / copyright, …**
  - **Habitudes de travail**
  - **…**

Par qui sont-ils gérés ?

- **Service informatique (voire des correspondants informatiques) :**
  - **Installation, mise à jour, ...**
  - **En totalité ou en partie seulement ?**

- **Utilisateur directement :**
  - **En totalité ou en partie seulement ?**
  - **Par choix ? par nécessité ?**

- **Dans le second cas, il faudra en plus des recommandations d'utilisation :**
  - **Diffuser de l'information en interne sur les risques, failles,…**
  - **Former et/ou sensibiliser les utilisateurs à l'administration**

- **Faut-il forcément appliquer la même règle à tous les membres d'une équipe ?**

Où sont-ils utilisés ?

- **Poste fixe :**
  - **En un seul lieu (généralement le laboratoire)**
  - **Dans un environnement peu, voire pas hostile**

- **Portable :**
  - **Indifféremment dans plusieurs lieux**
  - **Dans un environnement peu, voire pas hostile (laboratoire)**
  - **Dans un environnement hostile (congrès, maison, …)**

- **Changement d'environnement**
  - **➔ Risques importants de contagions**

A qui appartiennent les postes ?

- **Au laboratoire :**
  - **Acquis sur les crédits du laboratoire**
  - **Choisis par le service informatique**

- **A l'utilisateur :**
  - **Acquis / contrats de recherches « individuels »**
    - **Rarement choisis par le service informatique**
  - **Acquis sur les propres deniers de l'utilisateur**
    - **Étudiants dans les laboratoires « pauvres »**
    - **Jamais choisis par le service informatique**

- **Dans le second cas, il peut être difficile de :**
  - **Maintenir une cohérence / équipement informatique existant**
  - **Imposer des choses**
  - **…**

Quels sont les risques ?

- **Incidents / infection du système :**
  - **Virus**
  - **SPAM**
  - **…**
- **Installation de porte dérobée :**
  - **Prise en main à distance du système**
  - **Attaque d'un autre site**
  - **…**
- **Utilisation du poste pour des activités illicites :**
  - **Diffusion d'information (Peer to Peer, site warez, …)**
  - **…**
- **Perte de données :**
  - **Vol de données**
  - **Vol de matériel**
  - **…**

Ce que veulent (ou pas) les utilisateurs

Ce qu'ils veulent …	Ce qu'ils ne veulent pas …
▪ Administrer leur machine ▪ Échanger des données avec l'extérieur ▪ Utiliser leur carte sans fil ▪ Utiliser leur portable ▪ Travailler depuis leur domicile ▪ Suivre des conférences à distance ▪ Faire de la visioconférence ▪ Avoir leur données sauvegardées ▪ …	▪ Avoir des problèmes de sécurité (SPAM, virus, « site warez », …) ▪ Perdre leur données ▪ Gérer leur machine ▪ Avoir des procédures complexes ▪ Se voir imposer des choses ▪ …

Ces demandes devront être affinées lors de réunions entre le service informatique et les utilisateurs

Ce qu'ils ne veulent pas …

Avoir des problèmes de sécurité

Incidents : Quelques éléments

- **Incident = tout ce qui n'est pas normal**
- **SPAM, virus, mouchard, …**
- **Utilisation non autorisée des ressources d'une machine :**
  - **Disque dur, CPU, …**
  - **FTP Warez**
- **Vol de données**
  - **Suite à intrusion informatique**
  - **Suite à un vol physique**

SPAM

SPAM : Quelques éléments

- **Pourriel, pollupostage**
- **Messages électroniques non sollicités**
- **Utilisation de relais de messagerie ouverts ou machines mal sécurisées**
- **Nuisance de plus en plus importante :**
  - **Nombre de messages reçus**
  - **Contenu des messages**

  ➔ S'apparente au déni de service en sécurité
- **Activité plus ou moins légale mais lucrative**

SPAM : Prévention

- **Ne pas rendre visibles les adresses électroniques de vos correspondants lorsque vous créez un groupe ou une liste de diffusion**

- **Coder les adresses électroniques dans les pages web pour les rendre indétectables par les logiciels d'extraction des spammers**

- **Sensibiliser les utilisateurs**
  - **À ne pas divulguer les adresses électroniques**
  - **…**

SPAM : Protection / niveau 1

- **Mettre en place un mécanisme de filtrage de contenus**

- **Au niveau du serveur de messagerie :**
  - **Méthode la plus souvent retenue : par mots clefs / patterns**
    - **Exemple : SpamAssassin**

- **Principes :**
  - **Analyse le contenu du message (et non seulement l'en-tête)**
  - **Marque les messages ({Spam?} Better off to try)**

- **Former les utilisateurs à la mise en place de filtres sur leur messagerie individuelle**
  - **Pour filtrer automatiquement les messages « marqués »**

- **Leur expliquer le fonctionnement pour qu'ils :**
  - **Consultent de temps à autre leur « poubelle »**
  - **Donnent des indications à leurs « vrais » correspondants**

SPAM : Protection / niveau 2

- **Mettre en place un mécanisme de filtrage de contenus**
- **Au niveau des postes individuels :**
  - **Méthode la plus souvent retenue : par analyse statistique**
    - **Classification Bayesienne**
      - Intégré au produit : Netscape 7.1, Mozilla 1.3, Eudora 6 Pro, Mail (MacosX), …
      - En utilisant un proxy : spamihilator, …
    - **Documentation : http://www.mozilla.org/mailnews/spam.html**
- **Principes :**
  - **Analyse le contenu du message (et non seulement l'en-tête)**
  - **Change le statut du message (ham vs junk)**
- **Former et sensibiliser les utilisateurs à l'utilisation des mécanismes de filtrage / postes individuels**
- **Leur expliquer le fonctionnement**
  - **Analyse du contenu du message ➔ Problème de lenteur ➔ deux profils ?**

SPAM : Exemple de message à envoyer …

- **Le SPAM est devenu un véritable fléau. Au niveau du serveur de messagerie, nous avons mis en place un filtrage de contenu qui marque vos messages. A vous maintenant de les rediriger dans la bonne boîte aux lettres.**
- **Nous vous conseillons aussi d'utiliser les fonctionnalités propres à votre outil de messagerie pour réaliser un deuxième filtre.**
- **Le SPAM s'appuyant sur un modèle commercial, vous pouvez à votre niveau participer à son éradication :**
  - **En faisant toujours preuve de vigilance quand vous communiquez votre adresse électronique.**
  - **En ne répondant jamais à un SPAM ; en ne cliquant pas sur les liens hypertexte insérés dans le corps du SPAM ; en n'ouvrant jamais un fichier joint figurant dans un SPAM.**

SPAM : Pour en savoir plus

- **Site des correspondants sécurité UREC**
  - **https://www.urec.cnrs.fr/securite/corres-secu/index.html**
  - **Matthieu Herrb (LAAS)**
    - **SPAM : état des lieux - mars 2004**
    - **Filtres Anti-virus / Anti-SPAM pour Sendmail - mars 2003**
    - **Filtres Anti-SPAM - février 2003**
  - **Joël Marchand (Institut de Mathématiques de Jussieu)**
    - **Messagerie : conseils pour lutter contre les spam et les virus - mai 2003**
  - **Michel Gallou (Délégation Bretagne & Pays de Loire)**
    - **Bilan de l'opération de lutte anti-SPAM (DR17) - février 2003**
- **Produit Spamihilator : http://www.spamihilator.com/**

Virus

Virus : Quelques éléments

- **Virus, ver ?**
  - **Catégorie des programmes autoreproducteurs**
- **Méthodes d'infection :**
  - **Messagerie électronique, …**
  - **Disquettes, CD, …**
  - **Partage réseau**
  - **Vulnérabilité des systèmes**
  - **…**
- **Plates-formes vulnérables :**
  - **Actuellement Windows**
  - **Mais les autres systèmes n'en seront peut-être pas exempt éternellement**
    - **Unix, Macintosh, …**

Virus : Conséquences

- **Envoi de messages « publicitaires » (SPAM)**
- **Envoi de fichiers personnels**
- **Ajout, destruction ou modification de fichiers**
- **Désactivation de logiciel de sécurité**
  - **Antivirus, garde-barrière**
- **Installation de porte dérobée**
- **Attaque ciblée de sites web**
  - **Déni de service**
- **Écoute du trafic**
  - **Vol de mot de passe**
- …

Virus : Netsky.Q (http://www.secuser.com)

- **Netsky.Q est un virus qui se propage par email.**
- **Il se présente sous la forme d'un message avec importance haute dont le titre et le corps sont aléatoires, accompagné d'un fichier joint dont l'extension est .SCR, .EXE, .PIF ou .ZIP (28 Ko), en se faisant passer pour un message d'erreur en réponse à un courriel mal adressé ou endommagé.**
- **Si l'ordinateur n'est pas à jour dans ses correctifs, la simple ouverture ou prévisualisation du message HTML provoque l'exécution du fichier joint. Si ce dernier est exécuté, le virus s'envoie aux adresses présentes dans le carnet d'adresses Windows et divers autres fichiers, puis lance une attaque contre plusieurs sites web.**
- **PREVENTION :**
  Les utilisateurs concernés doivent mettre à jour leur antivirus. En cas de doute, les utilisateurs d'Internet Explorer doivent aussi mettre à jour leur navigateur via le site de Microsoft ou le service WindowsUpdate afin de corriger la faille exploitée par le virus pour s'exécuter automatiquement.
- **DESINFECTION :**
  Avant de commencer la désinfection, il est impératif de s'assurer avoir appliqué les mesures préventives ci-dessus afin d'empêcher toute réinfection de l'ordinateur par le virus. Les utilisateurs ne disposant pas d'un antivirus peuvent utiliser gratuitement l'utilitaire de désinfection FxNetsky pour rechercher et éliminer le virus.

Virus : Bagle.U (http://www.secuser.com)

- **Bagle.U est un virus qui se propage par email.**
- **Il se présente sous la forme d'un message dont le titre et le corps sont vides, accompagné d'un fichier joint avec une extension en .EXE (8 Ko).**
- **Si ce fichier est exécuté, le virus s'envoie aux adresses présentes dans le carnet d'adresses Windows ainsi que divers autres fichiers, puis installe une porte dérobée autorisant la prise de contrôle à distance par un individu malveillant de l'ordinateur infecté.**
- **PREVENTION :**
  Les utilisateurs concernés doivent mettre à jour leur antivirus. D'une manière générale, même si son nom est attrayant il ne faut pas exécuter un fichier joint douteux sans avoir fait confirmer son envoi par l'expéditeur du message.
- **DESINFECTION :**
  Avant de commencer la désinfection, il est impératif de s'assurer avoir appliqué les mesures préventives ci-dessus afin d'empêcher toute réinfection de l'ordinateur par le virus. Les utilisateurs ne disposant pas d'un antivirus peuvent utiliser gratuitement l'utilitaire de désinfection FxBeagle pour rechercher et éliminer le virus.

Virus : Mydoom.F (http://www.secuser.com)

- **Mydoom.F est un virus qui se propage par email et via les dossiers partagés.**
- **Il se présente sous la forme d'un message dont le titre est aléatoire, avec un fichier joint (34 Ko) dont l'extension est .BAT, .CMD, .COM, .EXE, .PIF, .SCR ou .ZIP.**
- **Si ce fichier est exécuté, le virus s'envoie aux adresses figurant dans le carnet d'adresses Windows et divers autres fichiers, installe une porte dérobée autorisant le téléchargement et l'exécution de fichiers à l'insu de l'utilisateur, tente de désactiver certains antivirus et de supprimer certains fichiers en .AVI, .BMP, .DOC, .JPG, .MDB, .SAV et .XLS., puis selon la date lance une attaque contre les sites Microsoft.com et Riaa.com.**
- **PREVENTION :**
  Les utilisateurs concernés doivent mettre à jour leur antivirus. D'une manière générale, même si son nom est attrayant il ne faut pas exécuter un fichier joint sans au moins l'avoir au préalable analysé avec un antivirus à jour.
- **DESINFECTION :**
  Avant de commencer la désinfection, il est impératif de s'assurer avoir appliqué les mesures préventives ci-dessus afin d'empêcher toute réinfection de l'ordinateur par le virus. Les utilisateurs ne disposant pas d'un antivirus peuvent utiliser gratuitement l'utilitaire de désinfection Stinger pour rechercher et éliminer le virus.

Virus : Gaobot (http://www.secuser.com)

- **Gaobot est une famille de virus ciblant les ordinateurs vulnérables notamment à la faille RPC de Microsoft.**
- **Si une machine connectée à Internet n'est pas à jour dans ses correctifs, Gaobot l'infecte via le port 135, 445 ou 80 puis scanne le réseau à la recherche de nouvelles machines vulnérables. Il installe par ailleurs une backdoor qui permet la prise de contrôle à distance de l'ordinateur contaminé. L'application des correctifs est impérative avant la désinfection de l'ordinateur pour empêcher de virus de réinfecter l'ordinateur.**
- **PREVENTION :**
  Les utilisateurs concernés doivent mettre à jour leur antivirus. En cas de doute, les utilisateurs de Windows NT, 2000, XP et 2003 doivent également mettre à jour leur système via le service WindowsUpdate (en français) afin de corriger les failles de sécurité exploitées par le virus pour s'exécuter automatiquement.
- **DESINFECTION :**
  Avant de commencer la désinfection, il est impératif de s'assurer avoir appliqué les mesures préventives ci-dessus afin d'empêcher toute réinfection de l'ordinateur par le virus. Les utilisateurs ne disposant pas d'un antivirus peuvent utiliser gratuitement l'utilitaire de désinfection FxGaobot pour rechercher et éliminer le virus.

Virus : Précautions / niveau 1

- **Au niveau du serveur de messagerie, installer un antivirus**
  - **Dispositif indispensable voire OBLIGATOIRE**
  - **Deux grandes familles :**
    - **Antivirus « classique » + MTA + scanner de mail**
      - Sophos, clamAV, attention pour F-Secure la licence n'est pas acquise
    - **Antivirus de flux SMTP, FTP, HTTP, POP, …**

- **Au niveau du réseau, autoriser un seul serveur de messagerie**

- **Prendre quelques précautions :**
  - **Prévoir une machine supportant la charge**
  - **Respecter la loi (information de l'utilisateur)**
  - **Avoir l'aval de la direction (conseil de laboratoire)**

Virus : Précautions / niveau 2

- **Sur chaque poste individuel :**
  - **Machine professionnelle et/ou personnelle**
  - **Windows, …**

- **Installer un antivirus et avoir une base de signatures à jour !**

- **Installer un garde-barrière personnel**
  - **But : éviter les attaques vers d'autres sites, …**

- **Mettre à jour le système d'exploitation et les logiciels**
  - **Surtout les navigateurs et les outils de messagerie**

- **Former les utilisateurs :**
  - **Ne pas cliquer sans savoir !**
  - **Être attentifs aux fichiers attachés**
  - **Connaître les adresses des sites «canulars »**
  - **…**

Virus : Accords nationaux / groupe logiciel

- **Cinquième opération nationale (Janvier 2004 - 3 ans)**
- **Trois produits :**
  - **Norton Antivirus (Windows, Macintosh)**
  - **F-Secure (Windows, Linux)**
  - **McAfee / VirusScan Security (Windows, Macintosh, Unix, ..)**
- **Mais un principe :**
  - **Toute installation nouvelle se fait obligatoirement avec « NAI Active ViruScan Security Suite »**
  - **Lors d'un remplacement de matériel, l'anti-virus du matériel précédent doit être réinstallé dans sa version actuelle**
- **Anti-virus F-secure et de NAI incluent des gardes-barrière personnels**

Virus : NAI Active ViruScan Security Suite (1)

- **VirusScan Enterprise v7.1.0 [Antivirus pour Windows NT, 2000, XP, 2003]**
- **VirusScan Multiplatform v4.5.1 [Antivirus pour Windows 9x]**
- **Virex pour Macintosh – 6.1 pour MacOS 7.5 à 9 ; 7 pou MacOS X**
- **VirusScan Command Line Scanners [Antivirus pour AIX, Free BSD x86, HP-UX, Linux x86, SCO x86, Solaris Sparc - Une version par système]**
- **VirusScan Wireless [Antivirus pour PDA Palm et Pocket PC - S'installe sur Windows 9x, NT, 2000, XP et effectue le scan à la synchronisation entre le PDA et le PC]**
- **NetShield for Netware v4.61 [Antivirus pour Netware 4, 5, 6]**
- **VirusScan Thin Client [Antivirus sans interface de configuration sur le poste pour Windows 9x, NT, 2000, XP - Nécessite le serveur EPO]**

Virus : NAI Active ViruScan Security Suite (2)

- **McAfee Desktop Firewall v8.0 [Firewall pour Windows 9x, NT, 2000, XP]**
- **Alert Manager v4.7.0 [Serveur de centralisation des alertes]**
- **AutoUpdate Architect v1.1.1 [Serveur de mises à jour]**
- **ePolicy Orchestrator v3.0.1 (ePolicy Orchestrator 3.0.0 SP1) [Serveur de déploiement et d'administration]**
- **Installation Designer v7.1.0 [Création de package d'installation personnalisée de VirusScan Enterprise v7.1.0 et McAfee Desktop Firewall v8.0]**
- **Installation Designer v1.1.0 [Création de package d'installation personnalisée de VirusScan Multiplatform v4.5.1]**
- **McAfee Threatscan [Scanner de failles pour Windows NT, 2000]**

Virus : Accords logiciels / groupe logiciel

- **Sophos (signé) :**
  - **SAV (Windows, Unix, Macintosh)**
  - **Mail Monitor for SMTP (Linux, Windows, Solaris)**
- **Trend Micro (signé) :**
  - **Office Scan (Windows 9x, NT, 2000, XP)**
  - **Interscan VirusWall (Solaris, Linux, Windows NT/2000)**
  - **Scanmail (MS Exchange & Lotus Note)**
- **Networks Associates (?) :**
  - **Webshield (unix, Windows NT)**
  - **GroupShield (Ms Exchange & Lotus Note)**
- **Symantec (?) :**
  - **Norton Antivirus for Gateway (Solaris, Windows NT & 2000)**
  - **Norton Antivirus for MS Exchange & Lotus Note**

Virus : Quelques réflexions

- **Solution actuelle :**
  - **Multiplier les antivirus**
    - **Flux internet, serveur de fichier, poste de travail**
  - **Diffuser des mesures de prévention et de vigilance**
  - **Filtrer des ports (au niveau du réseau et/ou poste individuel)**
  - **…**

➔ **Tous ces points de contrôle seront-ils encore valables quand tout sera chiffré ?**

- **Ne faudrait-il pas redonner à la messagerie son rôle initial, c'est-à-dire diffuser des messages (et non des fichiers) ?**

- **Ne faudrait-il pas diversifier son environnement de travail (système d'exploitation, outils de messagerie, …) ?**

- **Remarque : à ce jour, les virus sont « gentils » mais ils pourraient aussi faire exécuter automatiquement une commande style « delete » !**

Virus : Pour en savoir plus

- **Informations / produits disponibles**
  - **CRI d'établissement**
  - **https://www.services.cnrs.fr/corres-secu/ (accès avec certificat CNRS)**
  - **https://www.services.cnrs.fr/ars/ (accès avec certificat CNRS)**

- **Références / virus :**
  - **Sur le site de l' UREC (http://www.urec.cnrs.fr/securite)**
    - **Virus, filtrage / serveur de messagerie, antivirus / poste de travail**
  - **Secuser Alert (http://www.secuser.com)**
    - **Liste de diffusion répercutant les principales alertes virus, hoax et vulnérabilités en temps réel**
  - **Revue Misc – numéro 5 « Virus : mythes et réalités » Janvier 2003**
  - **Sécurité Informatique n° 38 (http://www.cnrs.fr/Infosecu/num38.pdf)**

Mouchard

Mouchard : Quelques éléments

- **Spyware, espiologiciel, …**
- **Programme indésirable installé sur un poste de travail permettant de récupérer des informations sur une personne ou une société sans qu'il en soit informé**
- **Adware : collecte d'information pour des régies publicitaires**
  - **L'utilisateur a donné son accord mais de façon involontaire (licence)**
- **Des buts différents :**
  - **Constitution de profil d'internautes pour des régies publicitaires**
  - **Espionnage industriel**
  - **Introduction de chevaux de Troie par des pirates**

Mouchard : Formes de programmation

- **Deux formes de programmation**
- **Programme externe : code distinct dans un programme autonome ayant son activité propre ou étant activé par l'hôte**
- **Programme interne ou intégré : code intimement mêlé au code du programme hôte. Installation simultanément du programme et du mouchard sur l'ordinateur de l'utilisateur**
  - **Souvent le cas pour des logiciels « gratuits »**
  - **Problème : impossibilité de retirer le mouchard**

Mouchard : Risques

- **Manque de recul actuellement**
- **Risque assez faible :**
  - **Ouverture impromptue de pages web sur des sites non professionnels ou apparition de pop-up**
  - **Moyen de collecter des adresses électroniques / SPAM**
  - **Profilage des internautes / respect de la vie privée**
  - **Utilisation de la bande passante**
  - **…**
- **Risque fort si détourné de son utilisation première :**
  - **Récupération de données sensibles, personnelles, ...**
  - **Installation de porte dérobée**
  - **...**

Mouchard : Précautions

- **Faire attention à ce que l'on télécharge sur Internet :**
  - **Particulièrement aux logiciels gratuits et aux logiciels Peer to Peer**
  - **Lire les licences !**

- **Utiliser de temps à autre un outil anti-spyware**
  - **3 outils spécifiques :**
    - **Détection et nettoyage : Spybot (gratuit) et Adware (gratuit)**
    - **Détection uniquement en version d'évaluation : PestPatrol**
  - **Certains antivirus intègrent aussi cette fonctionnalité**
    - **Mais les mouchards détectés ne sont pas les mêmes**
    - **Mouchard légitime ? Non légitime ?**

- **Utiliser un garde-barrière personnel pour filtrer les paquets sortants**
  - **Si le mouchard est interne à un programme utilisé, pas de détection possible**

Mouchard : Pour en savoir plus

- **Quelques définitions**
  - **http://www.pestpatrol.com/PestInfo/G/Glossary.asp**

- **Mémoire du DESS Audit et Expertise en Informatique « Mouchards Informatiques : de l'atteinte à la vie privée à l'espionnage des états – Principes, Technique et Législation », Laure Brignone, Université Paris II Panthéon-Assas, Septembre 2003**

- **Spybot http://www.safer-networking.org/**
- **PestPatrol http://www.pestpatrol.com/**
- **Adware http://www.lavasoft.de/**

Autres incidents

Autres incidents : Quelques éléments

- **Tout ce qui n'est pas :**
  - **SPAM, virus, mouchard, …**
- **Utilisation non autorisée des ressources d'une machine :**
  - **Disque dur, CPU, …**
  - **FTP WAREZ**
- **Vol de données :**
  - **Suite à intrusion informatique**
  - **Suite à un vol physique**

Autres incidents : Quelques raisons

- **Utilisation d'une faille de sécurité :**
  - **Du système d'exploitation**
  - **D'un logiciel client : Internet Explorer, Acrobat,…**
  - **Éventuellement d'un logiciel serveur : IIS, MSSQL, …**
- **Utilisation d'une faiblesse :**
  - **Mot de passe faible (ou pas de mot de passe)**
  - **Partage de disque**
- **Utilisation d'un binaire infecté :**
  - **Distribué par mail ou par des réseaux Peer to Peer ou IRC**
  - **…**

Précautions à prendre pour

Avoir moins de problèmes de sécurité

Incidents : Précautions / niveau 1

- Au niveau du service informatique
- Mettre en place une architecture sécurisée
  - Avec des zones de taille « raisonnable »
- Mettre un antivirus sur le flux SMTP (au minimum)
  - Flux FTP, HTTP ?
- Mettre à la disposition des utilisateurs
  - Logiciels anti-virus, anti-spyware, …
- Informer et sensibiliser les utilisateurs
  - Avis de sécurité, virus, …
  - Vulnérabilités, …

Incidents : Précautions / niveau 2

- Au niveau de chaque poste de travail
- Mettre à jour régulièrement :
  - Système d'exploitation
  - Logiciel
- Choisir de bons mots de passe
- Désactiver au maximum :
  - Tout ce qui est réputé dangereux (compte invité, …)
  - Tout ce qui est inutile sur un poste client
- Installer un anti-virus et éventuellement un garde-barrière

Ce qu'ils ne veulent pas …

Perdre leur données

Sauvegarder les données

- **Sauvegarde :**
  - **Pannes matérielles, vols, incendies, virus**
  - **Serveur et aussi les postes clients**
  - **Tout est « important » (fichier, messagerie, bookmark, etc.)**

  ➔ Mettre les sauvegardes dans un lieu sûr !

- **Fournir des moyens de sauvegarde aux postes clients :**
  - **Disque partagé sur le serveur**
  - **Clients de sauvegarde (par exemple Legato, etc.)**
  - **« Zip » , graveur de CD, etc.**

- **Sensibiliser et former les utilisateurs :**
  - **Informations à sauvegarder**
  - **Fréquence de sauvegarde**
  - **Restauration**

Ce qu'ils ne veulent pas …

Gérer leur machine

La situation idéale ? (1)

- **A première vue, oui**
- **Mais la situation actuelle n'est pas idéale**
- **Quelques exemples :**
  - **Nombre de machines est en forte augmentation**
  - **Nombre d'administrateurs est stable, voire …**
  - **De moins en moins de terminaux X et de plus en plus d'ordinateurs individuels**
    - **Passage d'une informatique « centralisée » à une informatique « décentralisée »**
  - **De nombreux systèmes d'exploitation, voire de nombreux niveaux**
    - **Windows, Macintosh, Linux, ...**

La situation idéale ? (2)

- **La situation est meilleure si le parc est homogène :**
  - **Possibilité de cloner les machines**

- **Mettre en place au maximum des gestions centralisées**
  - **Mise à jour automatique des systèmes d'exploitation**
    - **https://www.urec.cnrs.fr/securite/corres-secu/index.html**
      - Installation d'un serveur SUS
      - Mise à jour des clients par GPO
  - **Déploiement de solution antivirus + garde-barrière**
    - **Par exemple, ePolicy Orchestrator (McAfee)**

Conseil : Fournir des recommandations

- **Pour sensibiliser l'utilisateur à son rôle dans la sécurité du laboratoire**

- **Quelques idées :**
  - **Choisir un bon mot de passe**
  - **Ne pas coller son mot de passe sous le clavier**
  - **Ne pas installer de logiciels piratés**
  - **Ne pas modifier les configurations définies**
    - **Au niveau du système, de l'antivirus, du garde-barrière, ..**
  - **Activer le verrouillage automatique de l'écran**
  - **Manipuler avec précaution les partages de fichier**
  - **…**

Ce qu'ils veulent …

Administrer leur machine

Poste « autogéré »

- **Ne pas faire la confusion :**
  - **Avoir le mot de passe de l'administrateur ne signifie pas forcément administrer sa machine !**
  - **Un poste autogéré ne signifie pas forcément un poste mal géré !**
- **Dialoguer avec l'utilisateur :**
  - **Essayer d'en connaître les raisons**
  - **Définir le niveau de partage des tâches**
- **Le tenir informé :**
  - **Diffuser les avis de sécurité**
- **Le conseiller et éventuellement le former :**
  - **Par exemple à faire deux partitions**
    - **Système + logiciels (à cloner) ; données (à sauvegarder)**

Exemple de recommandation à fournir … (1)

- **Faire une installation sécurisée :**
  - **Ne pas faire une installation en « pointillé »**
  - **Installer les patchs de configuration :**
    - **Avant de mettre une machine sur le réseau**
    - **Dès la sortie des nouveaux patchs**
    - **➔ Se tenir informé !**
  - **Ne laisser que les services utiles**
    - **Proscrire les services web, ftp, smtp**
  - **Informer le service informatique de l'installation faite**

Exemple de recommandation à fournir … (2)

- **Fournir des conseils par type de machine**
- **Exemple : système Linux**
  - **Ne pas laisser de compte accessible sans mot de passe**
  - **Ne pas mettre de répertoire en écriture pour ftp anonyme**
  - **Supprimer les services inutiles**
  - **Restreindre les partages de fichiers (nfs, samba, etc.)**
  - **Suivre les patchs de sécurité**
  - **Ne pas divulguer le mot de passe de root**
  - **Surveiller les logs**
  - **Sauvegarder régulièrement**
  - **Ne pas mettre de route par défaut si inutile**

Exemple de recommandation à fournir … (3)

- **Exemple : système Windows NT WKS**
  - **Installer les derniers patchs de sécurité**
  - **Utiliser un domaine / groupe de travail**
  - **Utiliser Poledit au lieu de regedt32.exe si nécessaire**
  - **Mettre les disques en NTFS**
  - **Ne pas mettre en place de partage de fichier**
  - **Supprimer les services inutiles**
  - **Désactiver le compte « invité »**
  - **Surveiller les comptes qui sont dans le groupe Administrateur**
  - **Ne pas divulguer le mot de passe de l'administrateur**
  - **Surveiller les logs**
  - **Sauvegarder régulièrement**
  - **Ne pas mettre de route par défaut si inutile**

Exemple de recommandation à fournir … (4)

- **Exemple : système Windows 9.x**
  - **Supprimer les services « serveurs »**
  - **Utiliser les logon de domaines avec sécurisation via Poledit**
  - **Faire une image de la machine après installation**
  - **Sauvegarder régulièrement les données**
  - **Ne pas installer de cartes modem**
  - **Ne pas mettre en place de partage de fichier**

- **Exemple : système Macintosh**
  - **Bloquer le gestionnaire de configuration**
  - **Supprimer les services « serveurs »**
  - **Ne pas mettre en place de partage de fichier**
  - **Sauvegarder régulièrement les données**

De toute façon quelle que soit la situation

- **Avoir un inventaire du parc informatique :**
  - **Liste des machines avec leur système d'exploitation**
  - **Liste des services offerts**
  - **Liste des logiciels installés**

  ➔ Recenser les machines sur lesquelles les patchs doivent être installés

- **Avoir un correspondant par machine :**
  - **Quelqu'un qui connaît la machine**
  - **Administrateurs ou utilisateurs**

  ➔ Si nécessaire, mettre en place une liste de diffusion interne au laboratoire pour assurer la diffusion des avis de sécurité

Ce qu'ils veulent …

Échanger des données avec l'extérieur

Échanger des données avec l'extérieur

- **De nombreuses méthodes :**
  - **Disquette, CD, clef mémoire USB, …**
  - **FTP**
  - **Pièce jointe / messagerie**
  - **HTTP**
  - **Peer to Peer**
  - **…**
- **Certaines sont parfois interdites :**
  - **En fonction du « contenu supposée illicite » (Peer to Peer)**
  - **En fonction de la « dangerosité supposée » (FTP)**
  - **…**
- **Certaines sont parfois involontaires :**
  - **« Site warez » ouvert par les pirates**
  - **…**

P2P : Quelques éléments

- **Échange direct des ressources et services entre ordinateurs ; chaque élément étant à la fois client et serveur**
- **Mise en réseau de postes individuels (ou non)**
- **But : récupérer et/ou diffuser des informations**
  - **Professionnel (travaux de recherche, RedHat 9/Ratiatum, Mozilla 1.7)**
  - **Personnel (données vidéo, audio, …)**
- **Avantages :**
  - **Augmentation de la vitesse et de la fiabilité de téléchargement**
  - **Contournement des règles de filtrage**
    - **FTP, garde-barrière / politique de sécurité, anti-virus / flux, etc.**
- **Des exemples de logiciel : eMule / eDonkey / Kazaa**

P2P : Risques

- **Légalité / produits téléchargés (code de la propriété intellectuelle)**
- **Légalité / charte Renater :**
  - **Utilisation à des fins strictement professionnelles**
  - **Utilisation rationnelle des ressources du réseau**
- **Infection de la machine (virus, backdoor, spyware, …)**
  - **Introduits presque systématiquement lors du téléchargement du logiciel**
- **Fuite d'information (partage de données privées sans le savoir)**
  - **➔ Conséquence d'un virus ou d'une mauvaise programmation**
- **Introduction d'une porte d'entrée sur le réseau sécurisé**

P2P : Détection

- **Différentes possibilités :**
  - **Faire des mesures (analyse de flux)**
  - **Utiliser un système de détection d'intrusion (IDS)**
  - **Examiner les traces à la recherche d'adresses d'origine « non courantes » dans notre environnement, …**
    - **Un moyen si on n'a pas d'outil à sa disposition**
- **Comment caractériser les flux P2P ?**
  - **Port par défaut des applications**
    - **EDonkey : 4662 à 4665 ; BitTorrent : 6881 à 6889**
  - **Adresses IP des « meta » serveurs**
  - **Taille des flux**
    - **Correspond au débit d'une ligne ADSL 512kbits/s sur 5 minutes**
  - **…**
- **Attention, évolution constante dans ce domaine**

P2P : Protection

- **Définir une politique « tout est interdit sauf »**
  - **Être uniquement client et NON serveur = une solution envisageable**
- **Utiliser les possibilités de son garde-barrière**
  - **« Module » spécifique P2P (http://mega.ist.utl.pt/~filipe/iptables-p2p/)**
  - **Analyse de contenu des trames (niveau 7) (http://l7-filter.sourceforge.net/)**
- **Limiter le trafic**
  - **Bloquer les ports « classiques », protéger les machines légitimes, ralentir le reste**
- **Utiliser un système de prévention d'intrusion (IPS)**
  - **Détruire les sessions au vol quand on reconnaît du P2P**
- **Attention, évolution constante dans ce domaine**

P2P : Exemple de message à envoyer …

La technique du Peer to Peer consistant à mettre en réseau des postes individuels pour échanger des données avec n'importe quel internaute de la planète (données vidéo et audio à caractère privé) est strictement interdite sur notre réseau. La charte Renater (notre prestataire réseau) et le règlement intérieur du laboratoire ne le permettent pas.

Les raisons:

1 - Les logiciels qui utilisent ces techniques peuvent posséder des failles, il en découle que le matériel ainsi configuré peut se retrouver donné en pâture aux internautes du monde entier !

2 - Il y a un aspect légal dépendant du contenu des données ainsi distribuées.

3 - Les infrastructures de notre réseau ne sont pas mises en oeuvre à des fins privées. La bande passante du réseau n'a pas à pâtir de trafic important à caractère privé.

Tout trafic anormal sur notre réseau nous signalant la présence de serveurs Peer to Peer entraînera l'isolement du poste détecté (plus de communication avec l'extérieur possible).

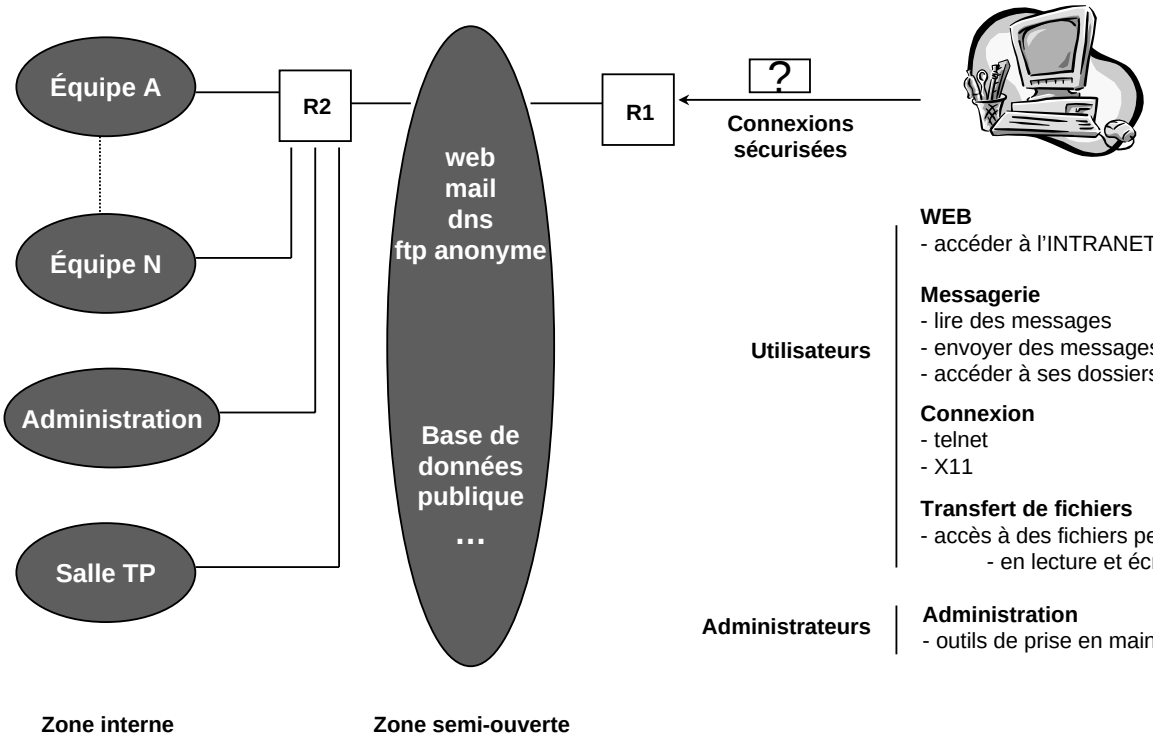
P2P : Pour en savoir plus

- **GERET Peer to Peer (Nancy - 25-28 mars 2004)**
  - **http://www.urec.cnrs.fr/geret/04.03.p2p/Programme.html**
- **« Les protocoles Peer-to-Peer, leur utilisation, leur détection », JRES2003, Gabrielle Feltin, Guillaume Doyen et Olivier Festor, Novembre 2003**
  - **http://2003.jres.org/actes/paper.70.pdf**
  - **http://2003.jres.org/diapo/paper.70.pdf**
  - **http://pc-media.univ-valenciennes.fr:8080/ramgen/jres2003/70.rm**
- **« Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security », whitepaper de Kevin Townsend, Avril 2003**
  - **http://www.pestpatrol.com/Whitepapers/CorporateSecurity0403.asp**
- **CERT A : Des recommandations sont en cours d'écriture**

Ce qu'ils veulent …

Travailler depuis leur domicile

Besoins d'accès distants (JRES2001)



Sécuriser les accès distants ?

- **Des réponses apportées à différents niveaux**
  - **Applicatif : SSH, S/MIME, …**
  - **Transport : SSL/TLS**
  - **Réseau : IPSec**
  - **➔ Réponses non concurrentes, mais complémentaires**

- **Synthèse des solutions présentées (cf. chapitre 10 / SIARS)**
  - **Pas UNE solution mais des solutions différentes en fonction :**
    - **Des besoins des utilisateurs**
    - **Des habitudes des utilisateurs**
    - **De l'environnement informatique du poste de travail (/filtrage)**
    - **Des moyens financiers et/ou humains**
    - **…**

SSH : points forts / points faibles (JRES2001)

- **Points forts**
  - **Solution opérationnelle :**
    - **Facile à utiliser en remplacement des "r-commandes" et telnet**
    - **Permet de sécuriser les applications TCP**
  - **Apports intéressants de la notion de "tunneling"**
    - **Diminuer le nombre de services offerts (filtrage)**

- **Points faibles**
  - **N'intègre pas la notion de certificat X.509 V3**
  - **Nécessite l'installation d'une application sur chaque poste client**
  - **Notion de "tunneling"**
    - **Difficile à appréhender pour les utilisateurs**
    - **Difficile à surveiller pour les administrateurs**
    - **Nécessite une adaptation de l'architecture sécurité mise en place**

SSL/TLS : points forts / points faibles (JRES2001)

- **Points forts**
  - **Intègre la notion de certificat (serveur et/ou client)**
  - **Offre les services de sécurité indispensables**
  - **Permet d'utiliser ses outils habituels (s'ils intègrent SSL !)**

- **Points faibles**
  - **Des adaptations nécessaires pour chaque application au niveau du serveur et/ou du client**
    - **Peu de clients (hors navigateur) intègrent le mode SSL**
    - **Problème de sécurisation pour les serveurs (protection des clefs)**
    - **Possibilité d'utiliser le logiciel « stunnel » pour la partie serveur**
  - **À ne pas conseiller dans toutes les situations (endroit hostile)**
    - **Protection du certificat utilisateur (utilisation symétrique)**
  - **À ce jour**
    - **https, pops, imaps sont véritablement opérationnels**
    - **De très bon espoir pour smtp/tls**

IPSec : points forts / points faibles (JRES2001)

- **Points forts**
  - **Sécuriser la connexion réseau et non les applications au cas par cas**
  - **Transparent pour les utilisateurs**
  - **Intégration du poste dans le réseau interne**
    - **Accès à tout son environnement**

- **Points faibles**
  - **Peu d'implémentation à ce jour dans notre environnement**
  - **Peut nécessiter l'installation d'une application sur chaque poste client**
  - **Extension du périmètre de sécurité**
  - **Fiabilité des postes individuels / sécurité ?**
  - **Utilise des protocoles et des ports souvent fermés / politique de sécurité**

- **De base, IPSec n'offre pas d'identification au niveau de l'utilisateur**

Travailler depuis … : Bilan

- **Bien définir les besoins avec les utilisateurs :**
  - **Messagerie, accès aux fichiers, ….**

- **Donner des solutions adaptées aux demandes :**
  - **Par exemple, VPN/IPSec n'est pas la réponse à la messagerie**
  - **Par exemple, « rendre disponible hors connexion » peut être la réponse pour accéder à ses fichiers windows (si on autorise les portables à se connecter sur le réseau interne)**

- **Mettre en place les solutions de base (par le service informatique)**
  - **Par exemple, SSH, passerelle de messagerie, pops, …**

- **Convaincre voire obliger, c'est-à-dire faire en sorte que les utilisateurs utilisent ces solutions**
  - **Formation indispensable à faire**

Travailler depuis … : Pour en savoir plus

- **Évolutions / produits :**
  - **F-secure SSH et les certificats X.509 V3**
  - **VPN/SSL ou les avantages de SSL et du VPN sans les inconvénients de IPSec (Néoteris, F5, Avantail, …)**

- **Évolutions / UREC :**
  - **Poursuite (voire mise à jour) des travaux faits par le groupe de travail dans les six mois à venir**

- **Documentations :**
  - **Fiches faites par le groupe de travail ADS**
  - **Différentes présentations : GERET, vCARS, JRES**
  - **…**
  - **Tout cela est disponible sur (accès avec certificat CNRS) https://www.urec.cnrs.fr/securite/corres-secu/index.html**

Ce qu'ils veulent …

Utiliser leur portable

Portables : Quelques éléments

- **« Je voudrais connecter mon ordinateur portable sur le réseau »**
- **Question posée le plus souvent au service informatique**
- **Posée par des populations différentes :**
  - **Par les utilisateurs permanents**
  - **Par les utilisateurs non permanents**
- **Qui possèdent un matériel appartenant :**
  - **Au laboratoire**
  - **À eux-mêmes**
- **Mais pourquoi (en quoi) est-ce problématique ?**

Portables : Problèmes

- **Machine qui a été contaminée et qui peut**
  - **Introduire des incidents sur le réseau (?)**
  - **Provoquer en chaîne l'infection de tout le réseau (virus)**
  - **Ouvrir un accès sur le réseau sécurisé (porte dérobée)**
  - **…**
- **Machine qui peut appartenir à un individu qui a des envies malveillantes / laboratoire**
  - **Vol d'information**
  - **…**
- **Machine qui peut appartenir à un individu « non respectueux » de l'organisation interne**
  - **Utilisation sauvage d'une prise, d'une imprimante, …**
  - **…**

Portables : Objectifs (1)

- **Objectif n° 1 : ne pas donner à n'importe qui tous les accès au réseau interne**

- **Donner des accès au réseau interne**
  - **À ceux qui sont permanents**
  - **À ceux qui ont déclaré leur adresse MAC**
  - **À ceux qui acceptent que le service informatique vérifie la bonne santé de leur poste**
  - **À ceux qui administrent « bien » leur machine**
  - **À ceux qui n'ont pas le mot de passe « administrateur »**
- **Donner des accès au réseau Internet uniquement aux autres**

- **Des solutions possibles :**
  - **DHCP fixe / adresse MAC**
  - **Mécanismes d'authentification (portail captif, 802.1X, …)**

Portables : Objectifs (2)

- **Objectif n° 2 : ne pas infecter tout le réseau interne**

- **Solutions techniques ?**

- **Définir une politique d'utilisation :**
  - **Installer un antivirus**
  - **Installer un garde-barrière**
  - **Interdire l'utilisation « familiale »**
  - **Sensibiliser et responsabiliser l'utilisateur**

- **Le rêve : avoir un moyen de s'assurer de la bonne santé du portable avant de le brancher !**
  - **Sas de décontamination**
  - **…**

Portables : En conclusion

- **Essayer d'évaluer les risques de façon objective, sans les sous-estimer mais sans non plus les surestimer**
- **Une architecture sécurisée avec des VLAN visiteurs est une bonne solution pour les non permanents**
- **Une architecture sécurisée avec des VLAN de taille « raisonnable » est peut-être un début de solution pour limiter la propagation d'un virus**
- **Ne pas oublier que le vol d'un portable (avec toutes ses données) peut être plus problématique pour un laboratoire qu'un virus**

Portables : Pour en savoir plus

- **Portail captif :**
  - **http://www.personaltelco.net/index.cgi/NoCatAuth**
  - **Authentification et nomadisme - Passerelle avec authentification pour des ordinateurs portables, Francois.Morris, http://www.lmcp.jussieu.fr/informatique/securite/Nomades.pdf**
- **Protocole 802.1X :**
  - **Le protocole IEEE 802.1X http://www.urec.cnrs.fr/securite/CNRS/vCARS2003/DOCUMENTS/saccavini.pdf**
  - **802.1X : Solution d'authentification sécurisée pour le futur réseau sans fil de l'Université Louis Pasteur http://2003.jres.org/actes/paper.143.pdf**
- **Documentation :**
  - **« Home Network Security » http://www.cert.org/tech_tips/home_networks.html**
- **Stage en cours « Études des solutions de connexion pour postes nomades dans un laboratoire de recherche »**

Ce qu'ils veulent …

Utiliser leur carte sans fil

Réseau sans fil : Besoins

- **Difficile de savoir pourquoi la demande sur le réseau sans fil est si forte (sentiment de liberté, d'indépendance, de mode, …)**
- **Expression par l'utilisateur d'un besoin simple :**
  - **Connecter son portable au réseau**
- **Ce besoin simple recouvre plusieurs situations :**
  - **Se connecter au réseau local :**
    - **quand il est au sein de son laboratoire**
    - **quand il est en dehors de son laboratoire**
  - **Se connecter au réseau Internet quand il est en dehors de son laboratoire**

  ➔ Notion de droits d'accès (notion proche de celle du nomadisme)

Réseau sans fil : Analyse des besoins

- **En réalité, la véritable expression du besoin est :**
  - **Connecter UN portable au réseau**

- **Pour pouvoir accéder au réseau dans un endroit où le réseau n'est pas présent physiquement (inaccessibilité d'une prise ethernet)**
  - **➔ Notion de lieu offrant du réseau / n'offrant pas …**

- **Pour pouvoir offrir à des utilisateurs non enregistrés sur notre réseau une connexion à Internet**
  - **➔ Notion d'utilisateurs authentifiés / non authentifiés (le cœur du problème sans doute)**

Réseau sans fil ≠ Réseau filaire ?

- **Sur le réseau filaire, les droits d'accès sont le plus souvent « gérés » par des VLAN par port ; aucune authentification de l'utilisateur n'est faite mais il existe une contrainte physique forte : il faut accéder à une prise murale (et il faut que la prise murale soit connectée à un élément de commutation !)**

- **Sur le réseau non filaire, en l'absence de contrainte physique forte, une seule solution : l'authentification de l'utilisateur. A noter qu'une fois que l'authentification sera faite, les droits d'accès seront les mêmes que ceux définis sur le réseau filaire ; les droits d'accès seront ceux définis dans la politique de sécurité de l'organisme.**

- **Sur le réseau non filaire, restera à gérer les utilisateurs non authentifiés et qui peuvent avoir droit d'accès à des ressources (par exemple, le public d'une bibliothèque universitaire).**

Réseau sans fil : Problèmes

- **Utilisable de partout et par tous**
  - **Extension du périmètre de sécurité (parking, …)**
  - **Accessible par tous (connexion illicite, …)**
- **Écoute du trafic**
- **Réseau sans fil = carte sans fil + borne sans fil**
  - **Sécurisation faible de nombreuses bornes**
    - **Administration possible par le réseau non filaire**
    - **Protocole faible (telnet, http),**
    - **Bouton « reset » facilement accessible,**
    - **…**

Réseau sans fil : Réponses

- **La situation n'est pas si dramatique :**
  - **Des mécanismes existent**
    - **WEP, WPA, SSID, filtrage par adresse MAC, …**
  - **Des bornes avec une meilleure sécurité existent**
  - **…**
- **En mettre un en place, peut faire progresser l'analyse des besoins :**
  - **Naissance de contrainte**
  - **Prise de conscience du faible débit**
  - **…**
- **Informer, sensibiliser, responsabiliser les utilisateurs :**
  - **Un réseau sans fil est une extension du réseau filaire**
  - **Le réseau est sous la responsabilité des administrateurs**
  - **…**

Réseau sans fil : Précautions

- **Sensibiliser les utilisateurs**
  - **Charte spécifique**
  - **Recommandation**
  - **…**
- **S'Informer et informer sur les développements en cours :**
  - **De nombreux projets au niveau des campus**
  - **…**
- **Détecter les bornes sans fil**
  - **Des logiciels existent (http://www.cru.fr/wl/)**
    - **Mais attention ils s'installent plutôt sur unix et utilisent plutôt des cartes « anciennes »**
  - **La meilleure solution est peut être d'utiliser simplement le logiciel accompagnant votre carte sans fil !**

Réseau sans fil : Pour en savoir plus

- **« Présentation WIFI » - Grenoble**
  - **Jeudi 29 avril, 14h-17h, Amphi D, ENSIMAG**
- **Liste de diffusion « sans-fil@cru.fr »**
- **À l'UREC, en préparation « Recommandations de sécurité destinées aux administrateurs systèmes et réseaux du CNRS sur l'installation de bornes sans fil (connexion d'ordinateurs portables dans une structure telle qu'un laboratoire de recherche) »**
- **Stage en cours « Études des solutions de connexion pour postes nomades dans un laboratoire de recherche »**

En conclusion

Quelques conseils

Ce qu'il faudrait peut-être activer …

Un garde-barrière sur chaque poste

Activer un garde-barrière … : Pourquoi ?

- **But : isoler au maximum un poste de travail de son environnement :**
  - **Pour le protéger des attaques externes menées contre lui (pirate)**
  - **Pour l'empêcher de réaliser des attaques vers l'extérieur (virus)**
  - **Pour bloquer l'envoi de données personnelles (spyware)**
  - **…**
- **Outil basé sur du contrôle de flux entrant et sortant**
- **Outil complémentaire à un antivirus**
  - **Mais aussi à une bonne administration, à une sensibilisation, …**

Activer un garde-barrière … : Produits

- **Sous Windows (XP, 2000) : garde-barrière (ICF)**
  - **Connexions (RTC, carte sans fil, réseau local, ...)**
  - **Non actif par défaut**
  - **Catégorie mémoire « d'état »**
  - **Configurable (Services, Flux ICMP, Journal de sécurité)**
  - **Limité (pas d'origine IP, pas de contrôle en sortie, …)**
- **Sous Unix : iptables, …**
- **Sous Macintosh : ipfw**
- **Rappel (accords nationaux / groupe logiciel) :**
  - **Les produits antivirus F-secure et NAI incluent des gardes-barrière personnels (uniquement pour Windows)**
  - **Toute installation nouvelle se fait obligatoirement avec « NAI Active ViruScan Security Suite »**

McAfee Desktop Firewall : Fonctionnalités

- **(Extrait de la documentation fournie avec le produit)**
- **Pare-feu : vérifier le trafic réseau entrant et sortant avant de bloquer ou de l'autoriser selon les règles que vous avez définies**
- **Système de contrôle des applications : surveiller les applications utilisées et empêcher celles que vous spécifiez de démarrer ou de s'interconnecter à d'autres programmes**
- **Système de détection des intrusions IDS : analyser le trafic destiné à votre ordinateur et identifier toute attaque potentiellement dirigée contre votre système**
- **Journal d'activité : enregistrer des informations relatives aux actions de Desktop Firewall ; à utiliser pour résoudre des problèmes ou examiner l'activité antérieure**
- **Pas obligatoire d'activer l'ensemble de ces fonctionnalités**

Activer un garde-barrière … : Bilan

- **L'intérêt est fonction du lieu d'utilisation des postes individuels :**
  - **Milieu hostile : indispensable**
  - **Milieu peu hostile : ?**
- **Pas de bilan sur le déploiement massif de garde-barrière sur les postes personnels dans un réseau local :**
  - **Facilité de déploiement, de configuration, d'utilisation, …**
  - **Intérêt de son utilisation sur un réseau « déjà » sécurisé**
  - **…**
- **Attention au terme « au maximum », il faut se protéger mais il serait dommage de perdre toutes les fonctionnalités de votre poste de travail**
  - **Partage de documents**
  - **Administration à distance**
  - **…**

Ce qu'il faudrait peut-être mettre en place …

De l'administration centralisée

Administration centralisée : virus

- **ePolicy Orchestrator : produit d'administration de logiciels**
- **Faciliter le déploiement des anti-virus et des gardes-barrière sur les postes de travail**
  - **Gestion centralisée (configuration, distribution, administration)**
- **Produit indispensable ?**
- **Quelques fonctionnalités :**
  - **Mise à jour de la liste des postes / domaine**
  - **Mise à jour des bases de signatures / site McAfee**
  - **Mise à jour automatique des postes**
  - **Élaboration de rapport (version de logiciel, virus détecté, …)**
  - **Surveillance à distance des règles d'application**
  - **…**

Administration centralisée : Windows

- **Permet de tenir à jour les postes sans que l'utilisateur ait à avoir le mot de passe « administrateur »**
- **Serveur Software Update Service (SUS) & Utilisation de stratégie de groupe (GPO)**
- **Cf. chapitre 5 / SIARS et groupe de travail SARI**
- **Installation d'un serveur SUS, Janvier 2004,**
  - **http://www.crhea.cnrs.fr/crhea/Software%20Update%20Services.pdf**
- **Mise à jour des clients par GPO, Janvier 2004,**
  - **http://www.crhea.cnrs.fr/crhea/Maj%20Windows%20par%20GPO.pdf**
- **Windows SUS, présentation OSSIR, Décembre 2003,**
  - **http://www.ossir.org/windows/supports/2003/2003-12-08/Windows%20SUS.pdf**
  - **https://www.urec.cnrs.fr/securite/corres-secu/Compte-rendu-sus-ossir.pdf**

Administration centralisée : Autres …

- **Unix :**
  - **Groupe de travail SARI : Gestion centralisée des PCs sous linux**
    - **http://sari.inpg.fr/rubriques/themes/zone_publique.groupe_linux/Publications.html**
  - **…**
- **Macintosh :**
  - **NetBoot / Netinstall – Gérard Lasseur – mars 2004**
    - **http://www.mathrice.org/mars.2004/NetBoot-NetInstall.pdf**
  - **…**

Administration centralisée : clients légers ?

- **UNE solution réaliste pour pallier aux nombreux problèmes des ordinateurs individuels**
  - **De nombreux avantages pour les administrateurs**
  - **Des inconvénients pour les utilisateurs**
    - **Nomadisme**
    - **…**

- **Des produits existent**
    - **Neoware (accord logiciel)**
    - **PC diskless**
    - **Terminal Server**
    - **…**

- **Des expériences existent dans notre environnement**
  - **Groupe Mathrice (http://www.math.cnrs.fr/documents/)**
    - **http://www.math.cnrs.fr/documents/clients_legers/clients_legers.pdf**

Ce qu'il vous faudra définir …

Les rôles de chacun

Définir les rôles d'un administrateur

- **Rôle technique :**
  - **Mise en place d'une architecture sécurisée**
  - **Mise en place des services indispensables au fonctionnement du laboratoire (exemple : domaine NT) ou utiles aux utilisateurs (exemple : pour suivre une conférence à distance)**
  - **…**
- **Rôle de sensibilisation :**
  - **Diffusion de la charte informatique**
  - **…**
- **Rôle d'information :**
  - **Sur l'utilisation des services offerts**
  - **A propos des journaux de traces**
  - **…**

Définir le rôle d'un utilisateur

- **Rôle important à jouer dans la sécurité du laboratoire**
  - **Respect de la charte informatique**
  - **Respect du travail de l'administrateur**
  - **...**
- **Pour mener à bien ce rôle, il a besoin d'être tenu informé, voir associé aux choix faits par le service informatique**

En conclusion

- **Il faut instaurer un dialogue au sein du laboratoire**

- **Dans les deux sens :**
  - **Soit initié par l'utilisateur**
    - **Avant d'acheter et d'installer une nouvelle machine, un nouveau logiciel**
    - **…**
  - **Soit initiée par l'administrateur**
    - **Avant d'installer de nouveaux services**
    - **…**

- **Mise en place de réunion périodique**
  - **Comité d'utilisateur, …**

➔Le but étant d'anticiper les besoins en réseau particulièrement.

Illustration : Faire de la visioconférence

- **De retour de mission, un de vos utilisateurs vous raconte, à la cafeteria, que tous ses collègues maintenant font de la visioconférence et que finalement en y réfléchissant bien, il trouve que cela serait super bien !**

- **Cette question vous amène les pensées suivantes**
  - **Encore un gadget**
  - **De quoi s'occupe-t-il ?**
  - **Est-ce qu'il croit que j'ai que ça à faire ?**
  - **…**

- **La réponse que vous lui ferez ne sera évidemment pas celle-ci. Vous lui proposerez d'en discuter dans un endroit mieux adapté !**

- **Et attendant la réunion, vous allez vous renseigner …**

Visioconférence : quelques éléments

- **La visioconférence consiste à échanger de la voix, de la vidéo, et des données qui proviennent de transfert ou de partage d'applications (éditeur de texte, graphique et autres).**

- **La visioconférence ne peut pas remplacer totalement des rencontres physiques mais apporte de nouveaux moyens de communication entre deux ou plusieurs collaborateurs.**

- **Pour en savoir plus sur la visioconférence IP :**
  - **Introduction, mise en oeuvre, informations, équipements, services, expérimentations, portail et groupe de travail.**
  - **http://www.univ-valenciennes.fr/CRU/Visio/**

Visioconférence : Deux types de solutions

- **Solution collective vs solution individuelle**
  - **Solution collective**
    - **Machine dédiée ou poste de travail dédié (sans utilisateur)**
  - **Solution personnelle**
    - **Poste de travail de l'utilisateur**

- **Poste de travail = système d'exploitation + logiciel + équipement matériel**
  - **Exemple :**
    - **Système d'exploitation : Windows**
    - **Logiciels : Netmeeting, MSN/Messenger, …**
    - **Équipements : carte son + micro + caméra**

- **Machine dédiée = système d'exploitation + équipement matériel**
  - **Exemple :**
    - **Système d'exploitation : pSOS (OS temps réel)**
    - **Équipements : Polycom ViewStation + micro + téléviseur**

- **Remarque : que la solution soit « individuelle » ou « collective », toute visioconférence H.323 à plus de 2 nécessite un pont**

Visioconférence : Avantages / inconvénients

- **Avantages :**
  - **Solution individuelle (poste de travail de l'utilisateur) :**
    - **Toujours disponible**
    - **Pas très coûteux**
  - **Solution collective :**
    - **Possibilité de mettre cette machine dans la zone semi-ouverte**
    - **Peu d'attaques (machine dédiée) ou sans grande conséquence (poste de travail dédié à cet usage)**

- **Inconvénients :**
  - **Solution individuelle (poste de travail de l'utilisateur) :**
    - **Ouverture supplémentaire d'une porte d'accès depuis Internet**
    - **Risque d'attaque important aux conséquences importantes**
  - **Solution collective :**
    - **Pas toujours disponible**
    - **Nécessite un déplacement de l'utilisateur ou de la machine**

Visioconférence : Problèmes

- **Incidents possibles :**
  - **Attaque de la machine (faille de sécurité)**
  - **Écoute des échanges**

- **Problèmes de la visioconférence :**
  - **Requiert l'ouverture de tous les ports UDP et TCP > 1024**

Visioconférence : Réponses

- **Proxy H.323 indispensable pour assurer le filtrage de ce service si la visioconférence repose sur une solution individuelle ; non indispensable dans le cas d'une solution collective (si votre réseau possède une zone semi-ouverte !)**

- **Attention pour discuter à plus de deux, il faut un pont, donc il faut le réserver, le louer, … (que la solution soit « individuelle » ou « collective »)**

Quelques compléments

Référence bibliographique

- **Rapport de la CNIL (Février 2002)**
  « La cybersurveillance sur les lieux de travail »
  - **http://www.cnil.fr/fileadmin/documents/approfondir/**
    - **Rapport : rapports/cybersurveillance2.pdf**
    - **Fiches de synthèse : dossier/travail/cyber_fiches.pdf**
    - **Principales conclusions : dossier/travail/cyber_conclusions.pdf**

- **Sécurisation des nomades - IGC et certificats pour sécuriser les accès d'utilisateurs nomades, François Morris, Jres2003, http://2003.jres.org/diapo/paper.41.pdf**