

Séminaire CNRS 03/10/07

- Ecole des Mines de Nantes
- SIC – Missions
- Sécurité – les besoins
- Sécurité – l'accès aux données
- Sécurité – les droits
- Sécurité – les réseaux



Ecole des Mines de Nantes

- 600 élèves (sup -spé)
- 5 labos de recherche
 - Subatech
 - Informatique (UMR Lina – INRIA obasco)
 - Auto-Prod (UMR Ircyn)
 - DSEE (UMR GPEA)
 - SSG
- Adminisatation
 - Secrétariat général
 - Direction des études
 - Direction de la recherche
 - Services support COM et SIC



S.I.C. - Missions

- Réseau – Systèmes / 1 Ing, 2 tech
 - ◆ Réseau : TCP/IP
 - ◆ Systèmes : Windows-Unix - MacOS
- Techno Web / 1 Ing
 - ◆ intra-extra-Internet
- Développement / 1 Ing, 1 tech
 - ◆ Bases de données
 - ◆ AMO
- Divers / 1 tech
 - ◆ Téléphonie
 - ◆ Cartes à puce

02/10/07

Ecole des Mines de Nantes

Passer à la
première page



Les besoins des usagers

- Accès aux données
 - Comment?
 - Quels outils
- Protection des données
 - Droits et permissions
 - Sauvegardes
 - Audit
- Protection des communautés
 - Interne
 - Externe



Accès aux données

- Comment

- Charte de bon usage

- ☞Droit et devoir de l 'usager du réseau

- Idem pour le Maison des élèves (MDE)

- Sanctions

- ☞Coupure du compte

- ☞Coupure MDE

Accès aux données

- 2 mots de passe - même login
 - ◆ faible (weak)
 - ☞ Extranet, wifi
 - ◆ fort (strong)
 - ☞ Mail, login (Unix, Windows)
- Modification
 - ◆ <http://x-sic.emn.fr/dir-admin/authlogin.php>

Accès Données

- Outils :
 - Besoins de base
 - OS, Bureautique, mail, navigateur..
 - > Anti-virus, anti-spam, filtres
 - > mail (sendmail, anti virus clamav, listes grises et noires via milter)
 - > site Web (Apache / php) contrôle des accès
 - Besoins métiers
 - Application associées
 - > risques évalués au cas / cas



Protection des données

- Droits et permission
 - Elèves -> cours d'initiation (linux/windows)
- Sauvegarde
 - “Pas plus d'une journée de perte de travail”
 - > sauvegardes journalières (serveurs de données)
 - > sauvegarde à la connexion des portables (backupPC)
 - > restauration à la demande ou individuellement (portable)
- Audit
 - Accounting postes fixes
 - Log des transactions Internet



Protection des communautés

- Interne

- Discrimination de la population

- Chercheur, élève, administratif, invité

- > création de vlan

- Pour le wifi (802.1X (WEP, radius, ldap))

- > filtrage niveau 3 et 4 inter vlan

- > règles spécifiques ou passelle protégée pour les cas particuliers (recherche -> eleve)



Protection des communautés

- Externe

- Protection vis à vis du Net

- Adressage IP privé

- Recherche - > NAT

- Eleve, admin -> proxies par service

- Accessibilité

- Création d'accès spécifiques par Vlan

- > VPN (OpenVPN), SSH



Protection des communautés

- Externe (suite)
 - Accès externe aux services internes
 - Accès Intranet (proxies apache via ssl)
 - Accès mail (smtpssl, relayage de pops et imaps)
 - Définition d'une DMZ
 - Règles de base:
 - Protocole SSL pour tout ce qui fait transiter un login/password
 - Pas de compte sur les serveur à l'exception du root
 - Suppression de tous les services non utiles



Protection des communautés

- Externe (suite)

- DMZ

- Zone protégée par deux routeurs
 - Linux deux interfaces ethernet
 - Sécurité d'accès gérée par Iptables
 - Routeur Cisco en charge des Vlan
 - Sécurité gérée par access list

Merci

- Questions?

02/10/07

Ecole des Mines de Nantes

Passer à la
première page

