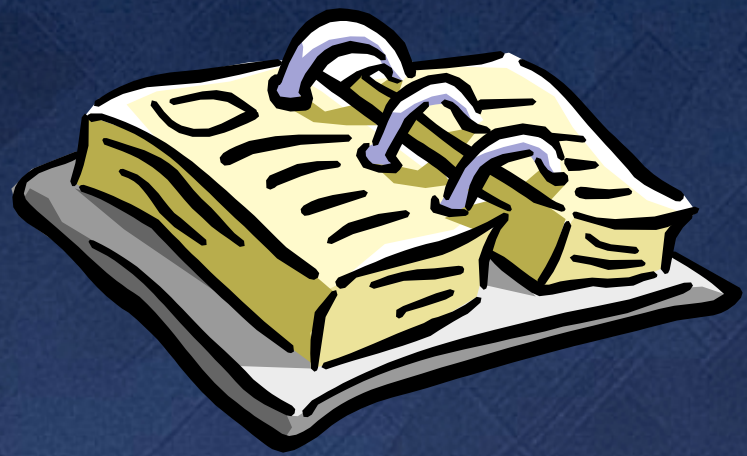
La sécurité avec Windows 2000

Patrick CHAMBET
IBM Global Services
pchambet@fr.ibm.com
pchambet@club-internet.fr

Planning

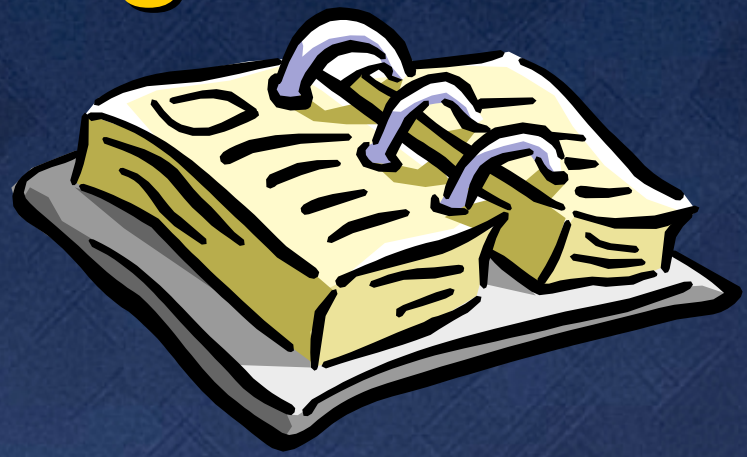
- Objectifs
- Rappels
- Points forts
- Risques
- Outils
- Conseils de configuration
- Conclusion



Objectifs

- Ce n’est pas de présenter les nouveautés de Windows 2000
  (cf présentation précédente)
- Mais de découvrir les implications des nouveautés de Windows 2000
- Découvrir les possibilités de configuration de sécurité de cet OS
- Utiliser les nouveaux outils de sécurité de Windows 2000

Planning



- Objectifs
- **Rappels**
- Points forts
- Risques
- Outils
- Conseils de configuration
- Conclusion

Rappels

- Windows 2000 est un « nouvel » OS
  - Code remanié
  - Intégration de toutes les corrections de NT 4.0
  - Sécurité prise en compte très en amont
- D'où un challenge à relever
  - Windows 2000 ne devrait plus avoir de réputation d'OS faiblement sécurisé

Rappels

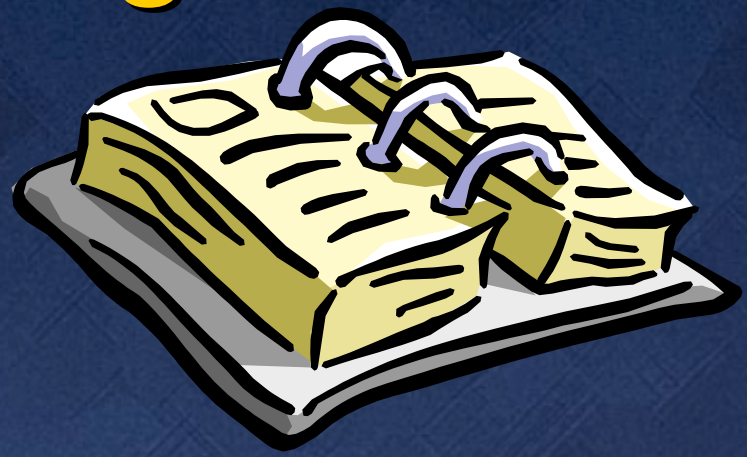
- La sécurité de Windows 2000 Professional
  - Authentification par Kerberos v.5
  - Permissions d'accès aux fichiers plus fines
  - Paramètres de la Registry plus sécurisés
  - Security Configuration Tool Set et Secedit
  - Encrypting File System (EFS)
  - IP Security (IPSec)
  - Protection des fichiers système
  - Support des PKI intégré
  - Support de Smart Cards intégré

Rappels

- La sécurité de Windows 2000 Server

  En plus:
  - Sécurité Active Directory
  - Stratégies de Groupes
  - Modèles de sécurité
  - Autres possibilités (suppression de NetBIOS, ...)

Planning



- Objectifs
- Rappels
- Points forts
- Risques
- Outils
- Conseils de configuration
- Conclusion

Points forts

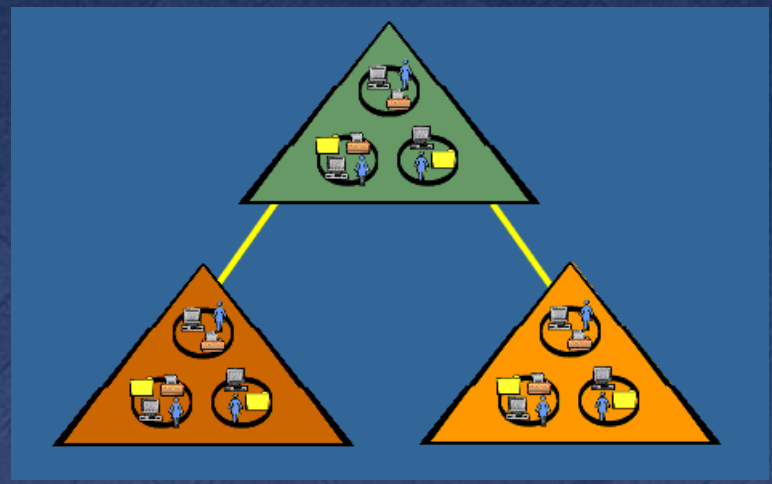
- Lors d'une migration, Windows 2000 conserve vos paramètres de sécurité:
  - comptes
  - stratégies d'audit
  - paramétrages fins de la Registry
  - permissions d'accès, etc.
- Insensible aux attaques courantes sur NT 4.0 (DoS divers, RedButton, etc.)
  - à finir de tester…

Mots de passe

- Insensible à L0phtCrack 2.5
  - Chiffrement 128 bits des mots de passe dans la SAM
  - Comptes locaux listés uniquement, pas d'accès à Active Directory et donc aux comptes de domaines
- Insensible à pwdump2

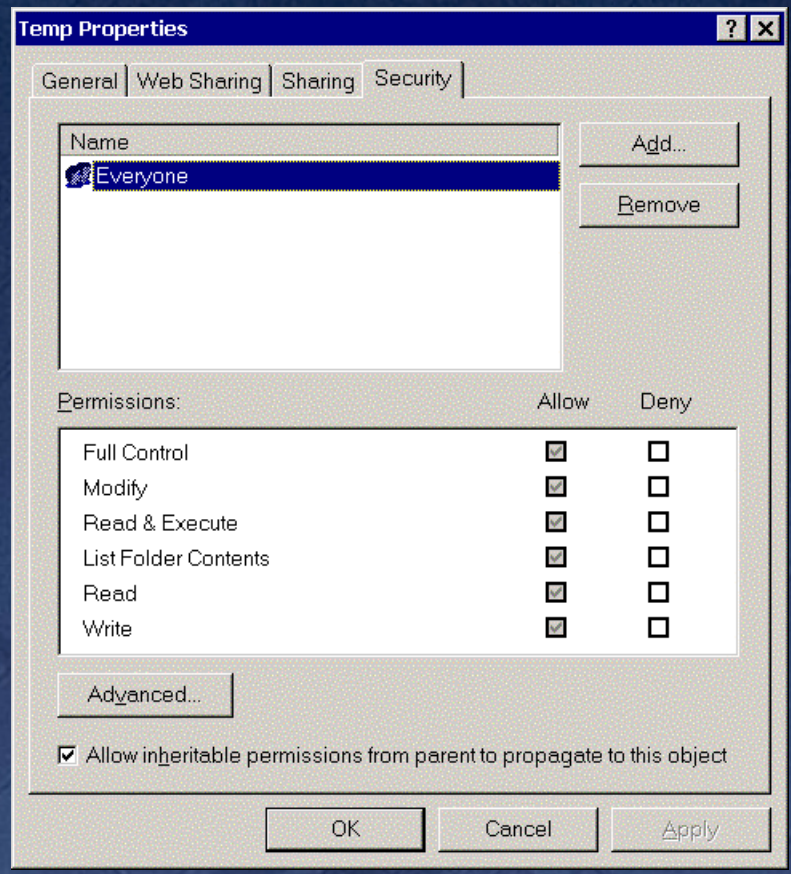
Active Directory

- Affectation extrêmement fine des permissions d'accès aux objets (ressources)
- Héritage
- Centralisation de l'administration
- Délégation de l'administration
- ADSI



Héritage des permissions

- Ensemble des permissions héritées et des permissions affectées localement
- L'héritage peut être bloqué



Stratégies de Groupes

- Sous NT 4.0:
  - Etablies avec Poledit
  - S'appliquent aux domaines
  - Peuvent être contrôlées ensuite par les groupes auxquels appartient l'utilisateur
  - Sont persistantes dans la Registry (jusqu'à ce que la stratégie soit supprimée ou la Registry éditée: `HKLM\Software\Policies` et `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies`)
  - Sont limitées à la sécurisation du bureau

Stratégies de Groupes

- **Sous Windows 2000:**
  - Etablies dans AD (ou en local)
  - Méthode privilégiée pour gérer les configurations de manière centralisée
  - Peuvent être affectées à des conteneurs Active Directory (sites, domaines et OU)
  - Affectent tous les utilisateurs et les ordinateurs de ce conteneur
  - Peuvent être contrôlées ensuite par les groupes auxquels appartiennent l'utilisateur et l'ordinateur
  - Sont plus sûres
  - Ne sont pas persistantes dans la Registry
  - Permettent de sécuriser le bureau ET l'environnement de l'utilisateur

Stratégies de Groupes

- **Ordre d'application:**
  - Stratégies style NT 4.0 (NTConfig.pol)
  - Stratégie de Groupe locale
  - Stratégies de site, dans l'ordre administratif
  - Stratégies de domaine, dans l'ordre administratif
  - Stratégies d'OU, du haut vers le bas et dans l'ordre administratif
- **Par défaut, les dernières stratégies « écrasent » les premières**

Les profils

- Stockés non plus dans `C:\WINNT\Profiles\UserName` mais dans `C:\Documents and Settings\UserName`
- Les clefs CryptoAPI et les certificats ne sont plus dans la Registry (`HKLM\Software\Microsoft\Cryptography\MachineKeys` et `HKCU\Software\Microsoft\SystemCertificates`) mais dans `\Documents and Settings\UserName\Application Data\Microsoft\Crypto` et `\SystemCertificates`

Les profils

- Dossiers Temp et Recent stockés dans:

  `C:\Documents and Settings\`*`UserName`*`\Temp` et
  `C:\Documents and Settings\UserName\Recent`

- Penser à les contrôler ou utiliser le nouvel outil DiskCleanup (Accessories\System Tools)

Fichiers système

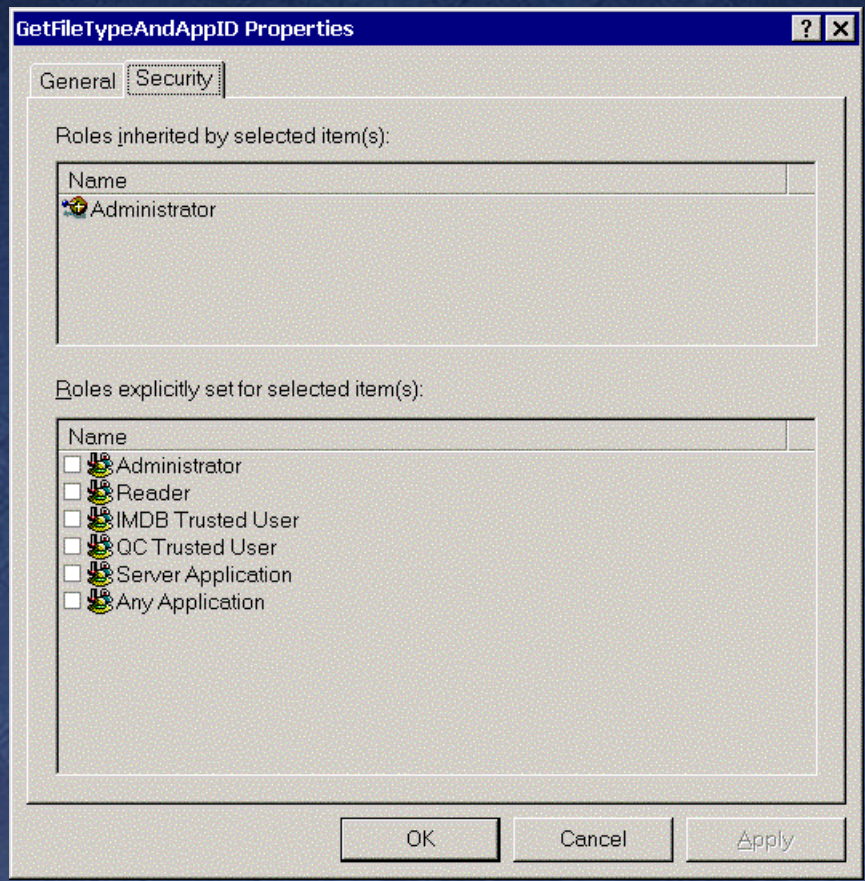
- **Windows File Protection (WFP)**
  - **Les fichiers système** .SYS, .DLL, .EXE, .OCX, .DRV et certaines polices sont protégés
  - En cas d'écrasement, ils sont restaurés à partir du répertoire compressé **`\WINNT\system32\dllcache`**

Les autres composants

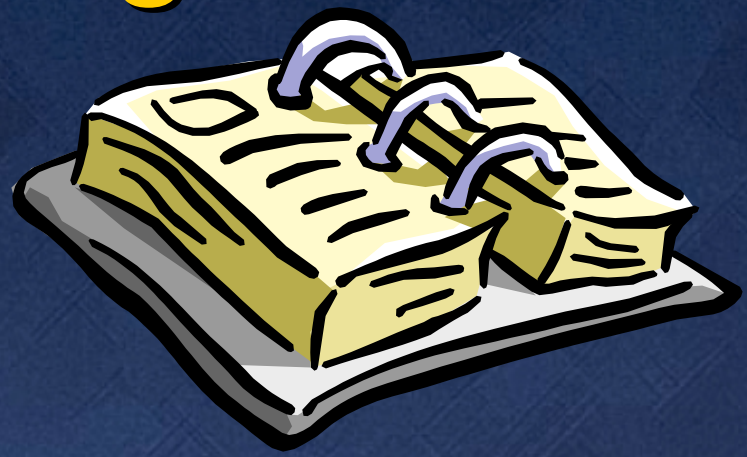
- IIS 5.0
  - Méthode d'authentification supplémentaire:
    - Anonymous Authentication
    - Basic Authentication
    - Digest Authentication
    - Integrated Windows Authentication (ex-NTLM)
    - Certificate Authentication
  - Envoie un hash du mot de passe
  - Fonctionne à travers les proxies et firewalls, mais nécessite les mots de passe en clair sur le DC...
  - Vulnérabilité de la Metabase non corrigée (http://pulhas.org/xploitsdb/NT/iis34.html)

Les autres composants

- **Component Services (ex-MTS)**
  - **Permissions d'accès au niveau méthode et non plus composant**



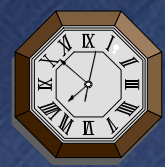
Planning



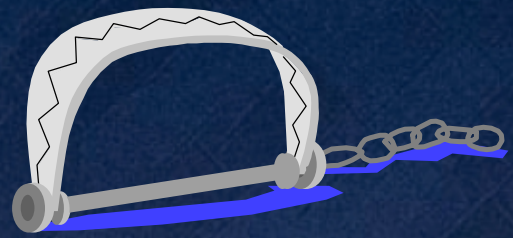
- Objectifs
- Rappels
- Points forts
- **Risques**
- Outils
- Conseils de configuration
- Conclusion

Risques

- Vulnérabilité pendant l'installation (partages administratifs)
- Kerberos
  - Les horloges des serveurs doivent être synchronisées à 5 min près (par défaut), sinon échec de l'authentification.



Risques

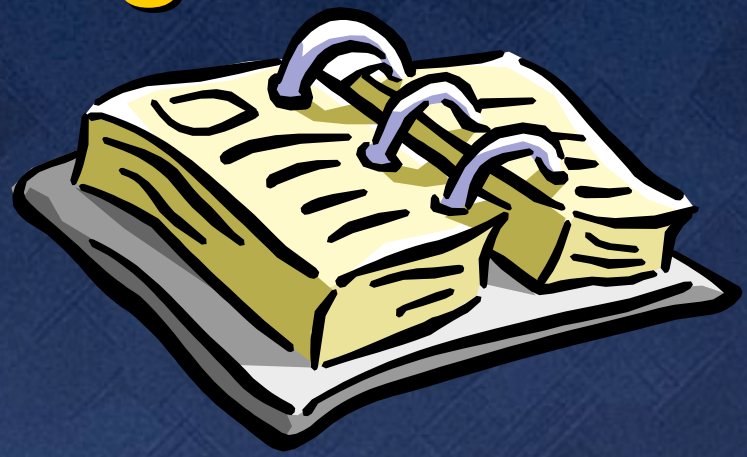


- **Encrypting File System (EFS):**
  - **Les DDF (Data Decryption Field) et les DRF (Data Recovery Field) sont stockés dans des Alternate Data Fields -> danger ? (étude en cours: cf démo)**
  - **Ne protège pas contre la destruction (EFS ne remplace pas les permissions d'accès !)**
  - **Une copie applicative n'est pas cryptée**

L'ERD

- RDISK n'existe plus (plus de AT…)
- Pour créer un Emergency Repair Disk, on utilise l'utilitaire Backup (ntbackup.exe) et toujours le répertoire \WINNT\repair...
- Pour réparer un système, on utilise le Setup ou la Recovery Console:
  - `\i386\winnt32.exe /cmdcons`
- Un boot avec la Recovery Console peut être une porte d'entrée...

Planning



- Objectifs
- Rappels
- Points forts
- Risques
- ☑ Outils
- Conseils de configuration
- Conclusion

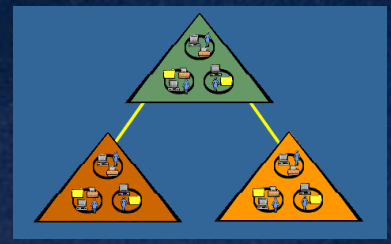
Le SCTS

- **Permet:**
  - de définir des modèles de sécurité
  - d'analyser le système par rapport à ces modèles
  - de signaler les mauvaises configurations
  - de réappliquer un modèle de configuration à tout le système

Démonstration

SCTS

ADSI



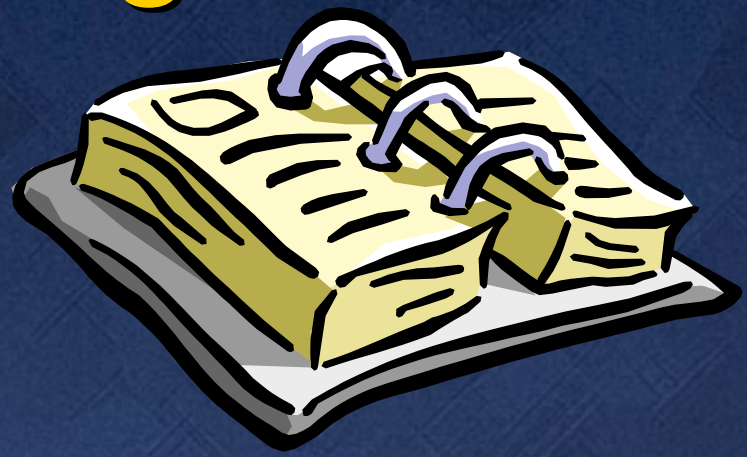
- Active Directory Services Interface
- Interface vers le modèle objet d'AD
- Permet de manipuler AD à partir de tout langage grâce à des objets COM
- Utilitaire adsiedit.exe du ResKit (Windows 2000 Support Tools)

- cf: http://www.internet-professionnel.net/ip/article/IP025/miseenoeuvre/administration/2510001.htm

Démonstration

ADSI depuis un browser

Planning



- Objectifs
- Rappels
- Points forts
- Risques
- Outils
- **Conseils de configuration**
- Conclusion

Conseils de configuration

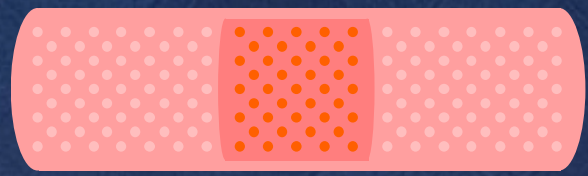
- Utiliser les Stratégies de Groupe pour établir les stratégies de sécurité
- Utiliser la stratégie d'audit pour contrôler les événements de sécurité
- Utiliser EFS pour vraiment maîtriser l'accès aux fichiers
- Utiliser le SCTS pour contrôler le tout, avec planification (AT)
  - `secedit /configure /DB myPol.inf /log scts.log`

Conseils de configuration

- Active Directory:
  - Accorder les autorisations d'accès aux groupes
  - Accorder des autorisations aux OU le plus possible
  - Utiliser l'héritage pour les stratégies de groupes
  - Surveiller les membres du groupe Enterprise Administrators
- Supprimer NTLM sur un réseau en mode natif (homogène Windows 2000)

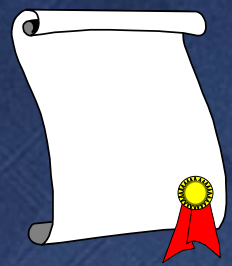
Aujourd'hui

- Quelques vulnérabilités (cf Security Bulletin MS00-006, SANS, NTBUGTRAQ, …)
- Des correctifs:
  - http://www.microsoft.com/windows2000/downloads
  - http://windowsupdate.microsoft.com
- Des articles dans la Knowledge Base:
  - Q253934, Q251170, Q252463, Q253342, Q252633, Q252891, Q251381, Q253341
  - http://support.microsoft.com/support/kb/articles/Q253/9/34.asp

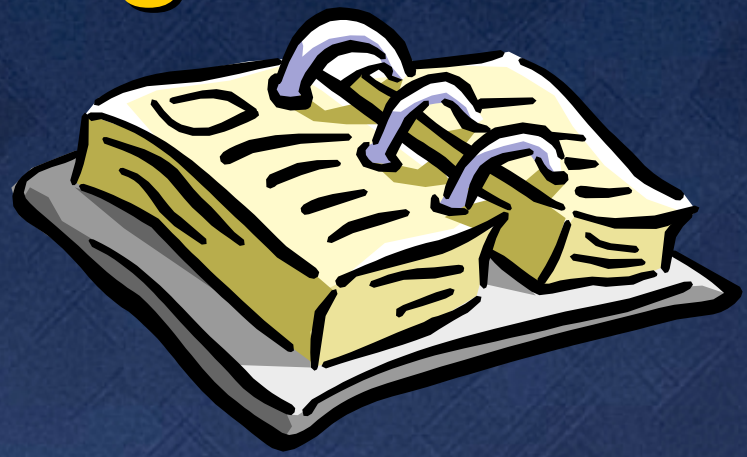


Demain

- **Windows 2000 devrait être certifié C2 vers 2002...**



Planning

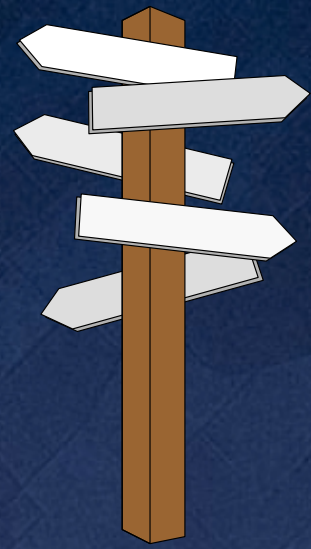


- Objectifs
- Rappels
- Points forts
- Risques
- Outils
- Conseils de configuration
- Conclusion

Conclusion

- Donc faut-il attendre le SP1 ou le SP2 de Windows 2000?
  - **OUI** pour des systèmes extrêmement critiques (mais il faudra courir vite ensuite)
  - **NON** en général: Microsoft semble avoir fait un effort relatif sur la qualité de son code

Pour en savoir plus



- Le site de Microsoft dédié à la sécurité:
  http://www.microsoft.com/security
- Les bulletins de sécurité de Microsoft:
  http://www.microsoft.com/france/technet/securite/default.htm#bulletin
- Les bases de la sécurité NT:
  http://www.microsoft.com/france/technet/securite/securnt.html
- Sécurité réseau:
  http://www.microsoft.com/france/technet/securite/secur_reseau.html
- Windows 2000:
  http://www.microsoft.com/windows2000
- Les stratégies de groupes de Windows 2000:
  http://technet.microsoft.com/cdonline/Content/Complete/windows/win2000/win2ksrv/prodfact/introgp.htm

Pour en savoir plus

- Kerberos:
  http://technet.microsoft.com/cdonline/Content/Complete/windows/win2000/win2ksrv/technote/msjkerb.htm
- Sécurité et technologies Internet:
  http://www.microsoft.com/france/technet/securite/info/msecuint1.html
- Le SCTS - Security Configuration Tool Set (article de P. Chambet):
  http://www.01net.com/contenus/ArtLong/Article/1,4210,92926+{}+1569,00.html
- CryptoAPI:
  http://www.microsoft.com/security/tech/cryptoapi/

QUESTIONS

(et même réponses)

A vous de jouer !

Jusqu'où sécuriserez-vous aujourd 'hui ?


STOP