

le salon de
la sécurité **informatique**



FRANCE
21-22 NOVEMBRE 2000
CNIT-PARIS La Défense



© EdelWeb 2000

SÉCURISATION D'UN RÉSEAU EXPLOITÉ SOUS WINDOWS 2000



Patrick CHAMBET

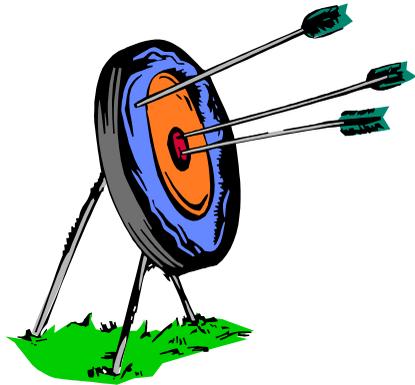
Jean OLIVE

EdelWeb

patrick.chambet@edelweb.fr

jean.olive@edelweb.fr

<http://www.edelweb.fr>

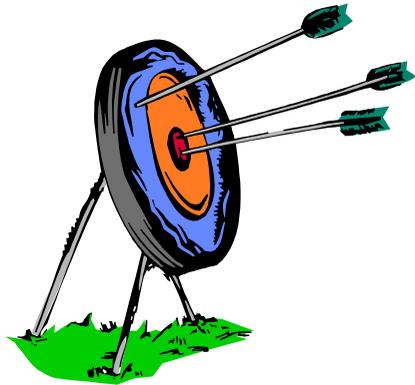


- Identifier les principaux écueils de la sécurisation d'un réseau sous Windows 2000
- Parcourir la boîte à outils de sécurité de Windows 2000
- Présenter une démarche globale
 - ✓ Pourquoi ?
 - ✓ Les grandes lignes
 - ✓ Les résultats
- Proposer / montrer quelques mesures de sécurisation



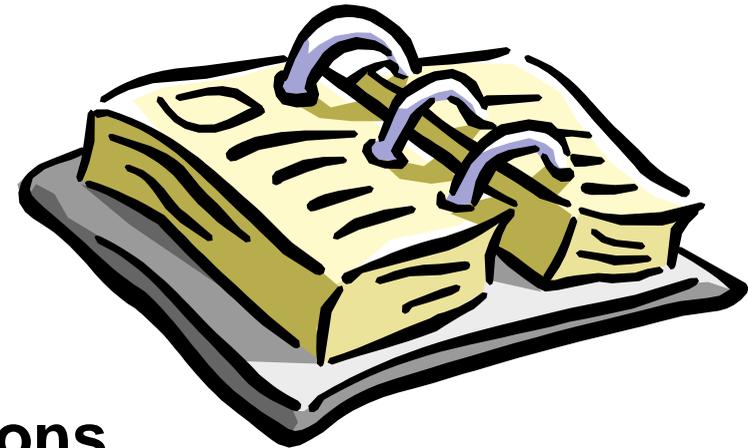
- **Le pôle sécurité Windows 2000**
- **Les apports de Windows 2000 sur le plan de sécurité**
- **Les écueils**
- **Une démarche de sécurisation**
- **Les principales recommandations**





- **La sécurité Windows 2000, pourquoi ?**
- **Constitution d'un pôle spécifique**
 - ✓ Une équipe de 4 experts depuis 6 mois
 - ✓ Développement / études / ...
- **Résultats**
 - ✓ Des formations sécurité Windows 2000
 - ✓ Des « EdelFiles »
 - ✓ Une méthode
 - ✓ Des revues / qualifications de vulnérabilités et des tests de parades

- **Le pôle sécurité Windows 2000**
- ✓ ➤ **Les apports de Windows 2000 sur le plan de sécurité**
- **Les écueils**
- **Une démarche de sécurisation**
- **Les principales recommandations**



Principales lacunes de NT 4.0	Solutions de Windows 2000
Aucune protection contre le vol d'information	EFS
Options de sécurité répartis sur plusieurs outils et difficile à déployer	Stratégies de sécurité
Manque de granularité des privilèges d'administration	ACL sur les objets et leurs propriétés Unité Organisationnelle
Écrasement des DLL système par des programmes d'installation	Windows File Protection (WFP)
Lacunes	Solutions partielles
Bogues et vulnérabilités	Communes / Nouvelles / Peu de retour du terrain
Majorité des services ne fonctionnant qu'avec des privilèges étendus	Aucune solution

➤ Mais également :

- ✓ Gestion centralisée des ressources et des services
- ✓ Structure logique décorrélée de la structure physique
 - ⇒ Active Directory
- ✓ Nouveaux objets
- ✓ Nouveaux outils
- ✓ Nouveaux protocoles
 - Kerberos v5
 - IPSEC, PPTP, ...
- ✓ PKI
- ✓ Support des SmartCards

- **Le pôle sécurité Windows 2000**
- **Les apports de Windows 2000 sur le plan de sécurité**
- ✓ ➤ **Les écueils**
- **Une démarche de sécurisation**
- **Les principales recommandations**



- **Choisir face à la richesse fonctionnelle**
 - ✓ NTLM / Kerberos / PKI
 - ✓ NTFS / EFS
 - ✓ Active Directory
 - ✓ ...
- **Migration**
 - ✓ Architecture du système d'information
 - ✓ Applications
- **Eviter les vulnérabilités**
 - ✓ Système encore neuf
 - ✓ Exemples ...

- **Le pôle sécurité Windows 2000**
- **Les apports de Windows 2000 sur le plan de sécurité**
- **Les écueils**
- ✓ ➤ **Une démarche de sécurisation**
- **Les principales recommandations**



LA DEMARCHE : POURQUOI ?

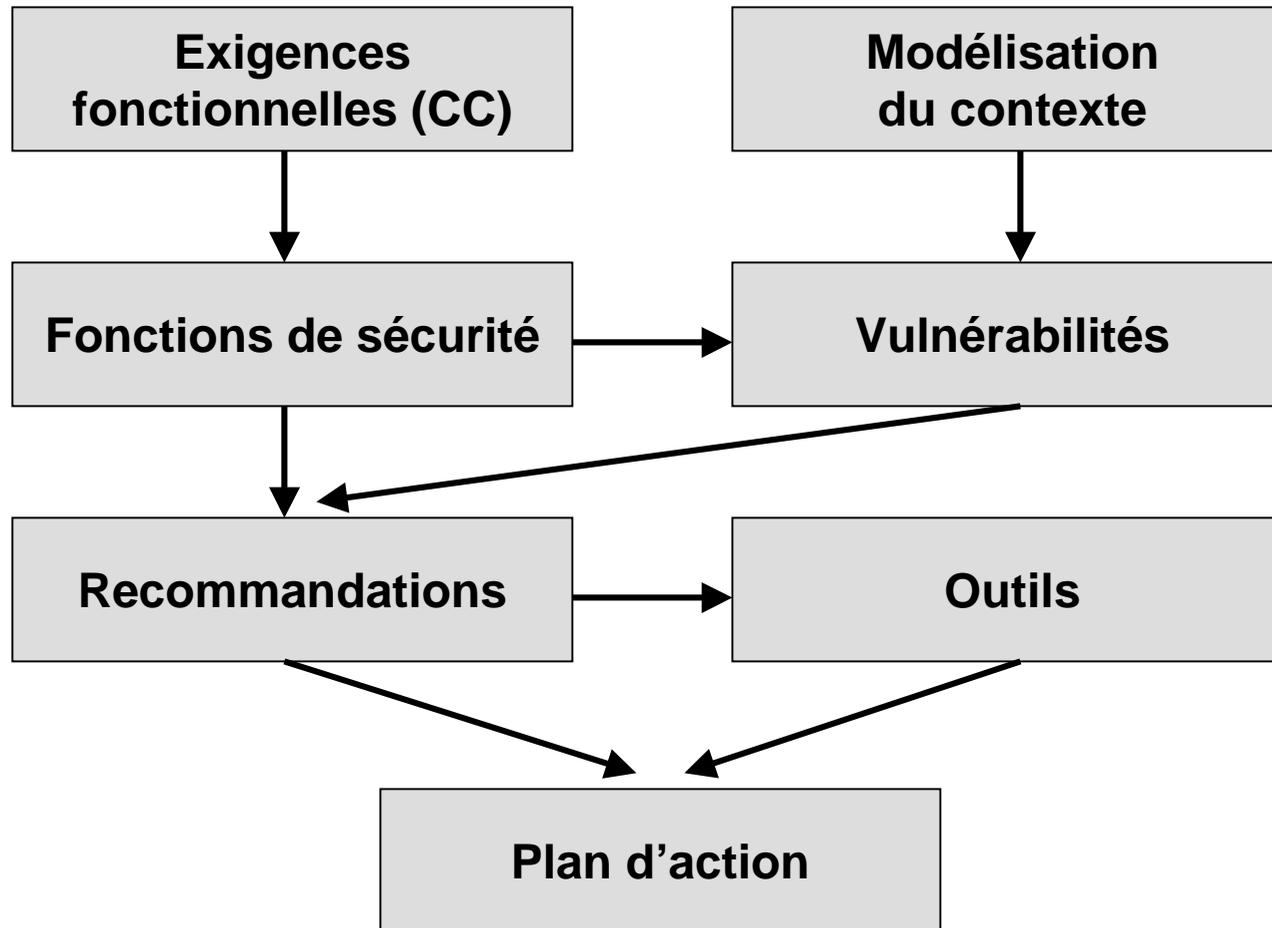
- **L'installation de Windows 2000 nécessite des choix d'architecture irréversibles**
 - ✓ Identifier les éléments structurants
 - ✓ Proposer les grandes orientations et identifier les impacts
- **Windows 2000 présente des vulnérabilités, des lacunes, des dangers**
 - ✓ Identifier et qualifier les vulnérabilités connues
 - ✓ Couvrir l'ensemble des vulnérabilités pertinentes pour l'entreprise
 - ✓ Assurer un suivi et une veille technologique permanente
- **Windows 2000 supporte des systèmes d'information**
 - ✓ Mettre en place une politique de sécurité globale du réseau de l'entreprise sous Windows 2000
 - ✓ Définir un niveau minimum de sécurité non dérogeable
 - ✓ Proposer des compléments pour répondre à des besoins renforcés

- **OBJ 1 : Couvrir les risques de sécurité du réseau cible en utilisant des éléments méthodologiques reconnus et réutilisables (CC)**
- **OBJ 2 : Adapter les mesures aux besoins**
- **OBJ 3 : Définir une organisation de la sécurité Windows 2000 cohérente et globale**
- **OBJ 4 : Disposer d'un cadre de référence pour mettre en place l'ensemble des services de sécurité**
- **OBJ 5 : Avoir un référentiel de suivi de la sécurité**



- **Les référentiels actualisés quotidiennement**
 - ✓ **La modélisation du contexte**
 - ✓ **Les exigences fonctionnelles des Critères Communs**
 - ✓ **Les fonctionnalités de sécurité de Windows 2000 et leurs consignes de mise en œuvre**
 - ✓ **Les vulnérabilités et limites des fonctions de sécurité**
 - ✓ **Les recommandations et parades**
 - ✓ **Les outils**

➤ La méthode:





LA DEMARCHE : LES RESULTATS



Démo

Base de vulnérabilités Windows 2000 - interface - [PPListe : Formulaire]

Echier Edition Affichage Insertion Format Enregistrements Outils Fenêtre ?

Exigences et fonctions de sécurité

Exigences de sécurité type Critères Communs

- FAU Audit de la sécurité
 - FAU_SAA Analyse de l'audit de sécurité
 - FAU_SAR Revue de l'audit de sécurité
 - FAU_SEL Sélection des événements de l'audit de sécurité
 - FAU_STG Enregistrement d'événements de l'audit de sécurité
 - FAU_APP Réponse automatique de l'audit de sécurité
 - FAU_GEN Génération des données de l'audit de sécurité
- FDP Protection des données de l'utilisateur
- FIA Identification et authentification
 - FIA_UID Identification d'un utilisateur
 - FIA_USB Liens utilisateur-sujet
 - FIA_AFL Défaillances de l'authentification
 - FIA_AFL.1 Gestion d'une défaillance de l'authentification
 - FIA_AFL.1.1 La TSF doit détecter X tentatives d'authentification infructueuses
 - FIA_AFL.1.2 Action en cas de tentatives d'authentification infructueuses
 - FIA_ATD Définition des attributs d'un utilisateur
 - FIA_ATD.1 Définition des attributs d'un utilisateur
 - FIA_ATD.1.1 Liste d'attributs de sécurité obligatoires
 - FIA_SDS Spécification de secrets
 - FIA_UAU Authentification d'un utilisateur

Description:

La TSF doit maintenir la liste suivante d'attributs de sécurité appartenant à des utilisateurs individuels : [spécification : liste d'attributs de sécurité].

Fonctions de sécurité correspondantes sous Windows 2000

Analyse des traces : détection d'activité anormale
Analyse des traces : événements suspects
Analyse des traces : identification des attaques
Attributs d'un utilisateur
Journal des événements : actions en cas de défaillance
Journal des événements : actions en cas de défaillance
Journal des événements : événements auditable
Journal des événements : protection du journal contre la suppression
Journal des événements : protection du journal contre l'altération
Stratégie de verrouillage de compte : actions
Description de la vulnérabilité de sécurité : conditions

Description (paramètres, consignes de mise en oeuvre):

Windows 2000 gère pour chaque compte utilisateur local la liste des attributs de sécurité suivants :

- L'identifiant du compte,
- Le mot de passe,
- L'interdiction de changer le mot de passe,
- L'invariabilité du mot de passe,
- Les groupes utilisateurs auxquels le compte appartient (définissant les droits des utilisateurs sur les serveurs et postes de travail accessibles),
- Les créneaux horaires de connexion,
- Sur Windows 2000 Server, le nom des stations de travail auxquels peut se connecter le compte,

Vulnérabilités associées:

Non remise à jour des attributs de sécurité

Ajouter une fonction de sécurité Sortir

Enr : 14 sur 1

Mode Formulaire

LE GUIDE DE SECURISATION DE WINDOWS 2000

Base de vulnérabilités Windows 2000 - interface - [Vulnérabilités]

Echier Edition Affichage Insertion Format Enregistrements Outils Fenêtre ?

Vulnérabilités

Nom: **Non remise à jour des attributs de sécurité**

ID Vulnérabilité: 13 Date de publication: A été vérifiée: Type: Vulnérabilité Lacune Danger
 Date de saisie: 11/15/2000 Commune avec NT:

Description:
 Les attributs de sécurité sont attribués à la connexion de l'utilisateur.
 Si un utilisateur ne s'est pas déconnecté ou a été authentifié par une autorité sur laquelle la mise à jour des attributs n'a pas été réalisée, cet utilisateur conserve ses attributs précédents la mise à jour.

Sources d'information:

URL 1:
 URL 2:
 URL 3:

Correctifs:
 Aucun

URLs des correctifs:

Composants affectés:
 Windows 2000 Server Gold
 Windows 2000 Server SP1
 Windows 2000 Pro Gold
 Windows 2000 Pro SP1

Composants recensés:
 Windows 2000 Server Gold
 Windows 2000 Server SP1
 Windows 2000 Pro Gold
 Windows 2000 Pro SP1
 Windows 2000 DNS
 Office 2000
 Index Server 2.0
 IS 4.0

Recommandations à appliquer:
Forcer la déconnexion des utilisateurs

Recommandations recensées:
 Désactiver les services inutiles
 Filtrer les ports NetBIOS
 Désactiver NetBIOS
 Mettre des ACLs sur les fichiers
 Mettre des ACLs sur les clés de registre
 Mettre les fichiers du serveur Web
 Mettre des ACLs sur les fichiers
 Limiter les droits et permissions
 Spécifier une durée de vie minimale
 Empêcher le démarrage sous un compte invité
 Protéger physiquement les stations

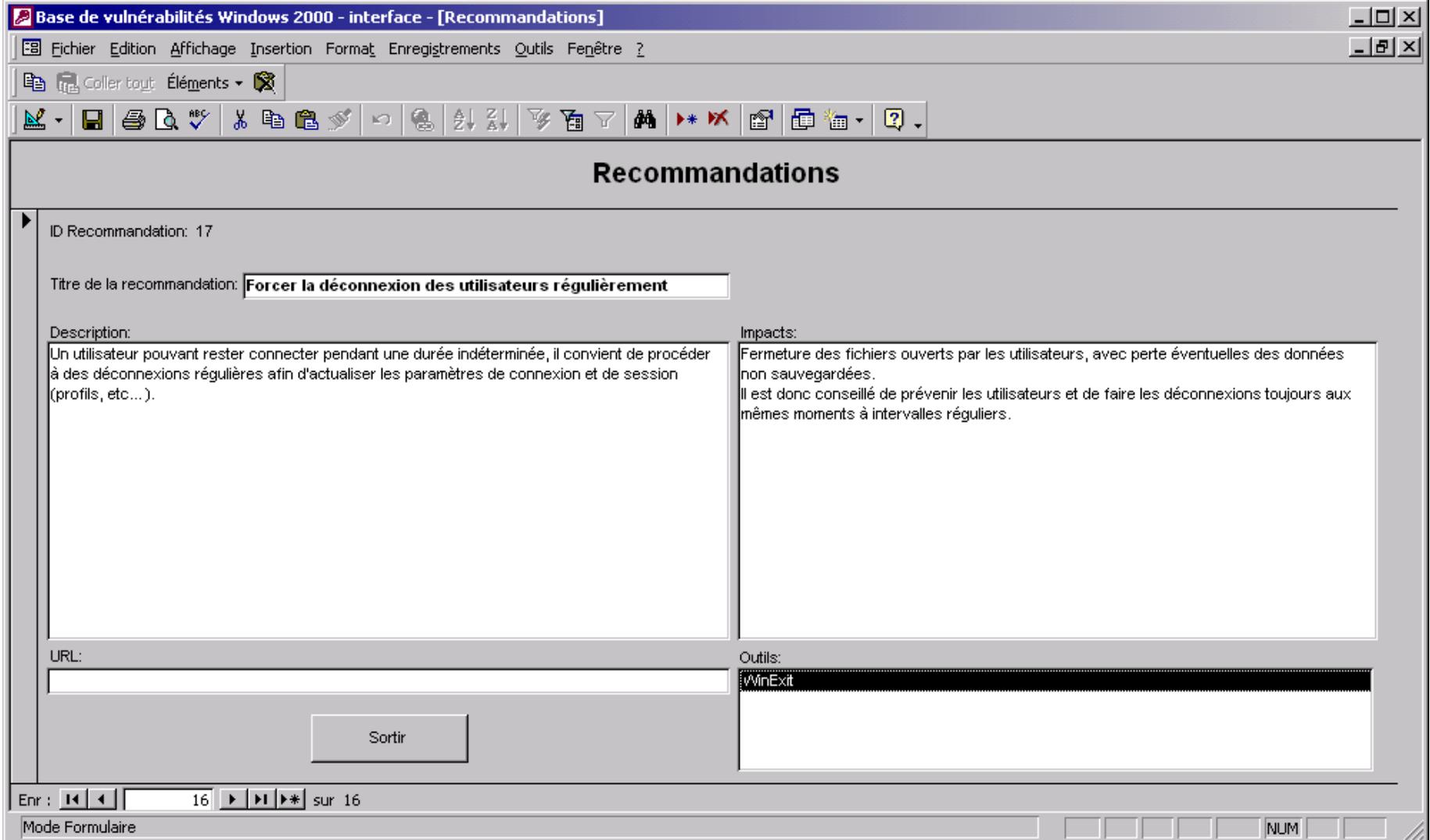
Exploitation:
 Internet
 Intranet
 Accès physique
 Utilisateur connecté

Conséquences:
 Accès non autorisé
 Gain d'information
 Déni de service
 Gain de privilèges

Sortir

Enr : 14 sur 20

Liste des recommandations



Base de vulnérabilités Windows 2000 - interface - [Recommandations]

Fichier Edition Affichage Insertion Format Enregistrements Outils Fenêtre ?

Coller tout Éléments

Recommandations

ID Recommendation: 17

Titre de la recommandation: **Forcer la déconnexion des utilisateurs régulièrement**

Description:
Un utilisateur pouvant rester connecté pendant une durée indéterminée, il convient de procéder à des déconnexions régulières afin d'actualiser les paramètres de connexion et de session (profils, etc...).

Impacts:
Fermeture des fichiers ouverts par les utilisateurs, avec perte éventuelles des données non sauvegardées.
Il est donc conseillé de prévenir les utilisateurs et de faire les déconnexions toujours aux mêmes moments à intervalles réguliers.

URL:

Outils:
WinExit

Sortir

Enr : 16 sur 16

Mode Formulaire

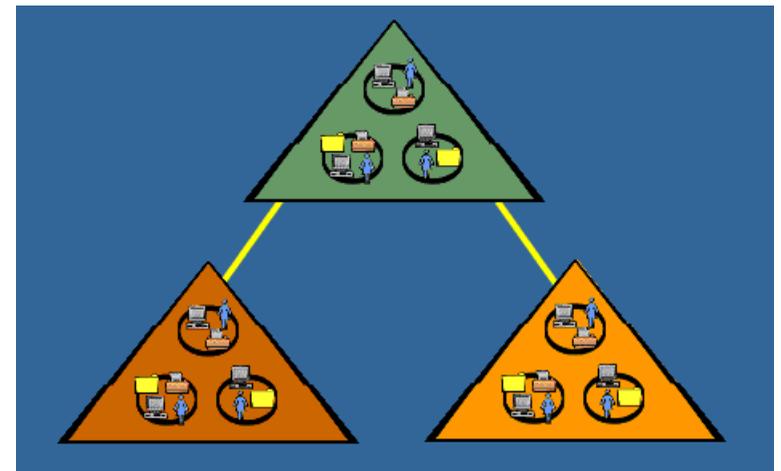
- **Le pôle sécurité Windows 2000**
- **Les apports de Windows 2000 sur le plan de sécurité**
- **Les écueils**
- **Une démarche de sécurisation**
- ✓ ➤ **Les principales recommandations**



- **Attention aux domaines multiples:**
 - ✓ Trafic de réplication
 - ✓ Opération de suppression de domaines fils complexe
- **Structurer grâce aux OU et aux Sites**
- **Passer en mode natif si possible**
- **Supprimer les clients pré-Windows 2000**



- **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**
- **Attention à la définition des droits sur les attributs**
- **Attention à la réplication**
 - ✓ **Volume**
 - ✓ **Sécurité des échanges**



- Utiliser les groupes et les OU (plutôt que les utilisateurs individuels)
- Utiliser les groupes de distribution autant que possible
- Définir des droits explicites (autoriser *ou* refuser)
- Limiter l'appartenance individuelle aux groupes universels
- Utiliser les stratégies de groupe
- Attention à l'héritage des permissions
- Attention à l'ordre d'application des permissions



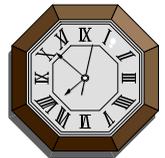
- **Sécuriser les permissions aux clefs sensibles (cf checklists)**
- **Les permissions par défaut sont plus sécurisées que sous NT 4.0**
- **RDISK /s n'existe plus (plus de AT possible)**
- **Pour créer une Emergency Repair Disk, on utilise l'utilitaire de Backup (NTBackup.exe) et toujours le répertoire `\WINNT\repair...`**

- **Ne pas utiliser le système FAT**
- **Utiliser NTFS 5**
- **Utiliser EFS**
 - ✓ **Supprimer l'agent de récupération local**
 - ✓ **Exporter le certificat de l'agent de récupération d'entreprise**
 - ✓ **EFS ne remplace pas les permissions d'accès**
 - ✓ **EFS ne protège pas contre la destruction**
 - ✓ **Une copie applicative n'est pas cryptée**
- **Attention à l'héritage des permissions**

Recommandations : Sécurisation des accès réseau (1)

➤ Authentification

- ✓ Désactiver le logon en clair (clients SAMBA)
- ✓ Désactiver LM
- ✓ Utiliser au minimum NTLM v2
- ✓ Désactiver les protocoles inutiles (NetBEUI, ...)
- ✓ Les horloges des serveurs doivent être synchronisées à 5 minutes près (authentification Kerberos)



➤ Services: désactiver les services inutilisés

- ✓ NetBIOS
- ✓ IIS
- ✓ RIS / TFTP
- ✓ Windows Media Player
- ✓ ...

Recommandations : Sécurisation des accès réseau (2)

- **Supprimer NTLM sur un réseau en mode natif (homogène Windows 2000)**
- **IPSEC**
 - ✓ Les versions export utilisent DES lorsque 3DES est demandé
 - ✓ Ceci peut entraîner des problèmes d'interopérabilité
 - ✓ **Correctif : High Encryption Pack:**
<http://www.microsoft.com/windows2000/downloads/.../recommended/encryption/default.asp>

- **Déléguer l'administration**
- **Activer les options de sécurité dans les stratégies**
- **Utiliser les stratégies d'audit**
- **Utiliser EFS pour vraiment maîtriser l'accès aux fichiers**



- **Nous obtenons un résultat concret: un niveau de sécurité élevé correspondant à vos besoins avec Windows 2000.**
- **Edelweb est prêt pour vous assister dans votre migration et dans tout projet évoluant autour de la plate-forme Windows 2000 au sein du système d'information de votre entreprise.**

