

Windows 2000

Windows 2000 wurde von Microsoft als Nachfolger von Windows NT für den Einsatz auf "Personal" Computern und für Unternehmensanwendungen entwickelt.

Wesentlicher Bestandteil von Windows 2000 ist der zentrale Verzeichnisdienst Active Directory, der die Integration unterschiedlichster Verzeichnisse ermöglicht in der alle relevanten Informationen über das Netzwerk, seine Benutzer bis hin zu Telefon- und E-Mail-Adressverzeichnissen hinterlegt sind, die bislang an verschiedenster Stelle mit redundantem Inhalt gepflegt werden mussten.

Unabhängig von der Datenschutzpolitik, die mit einem solchen zentralen Verzeichnisdienst verbunden ist, sind mit dem Einsatz eines Active Directory auch ganz konkrete sicherheitstechnische Probleme verbunden, da sich der Geltungsbereich der Domänen auf wesentlich größere Organisationsbereiche als bisher erstreckt. Während beispielsweise in der bremischen Verwaltung bislang ca. 200 Domänen eingerichtet sind, würde sich dort bei Einsatz eines Active Directory die Anzahl der Domänen auf einige wenige beschränken. Anstelle der ehemaligen NT-Domänen würden sogenannte Organisationseinheiten (OU) treten, zwischen denen - im Gegensatz zu einer NT-Lösung mit mehreren Domänen - permanent Vertrauensstellungen mit OE-übergreifendem Zugriff existieren. Die bisherigen NT-Barrieren auf Domänenebene müssen statt dessen durch eine strikte Vergabe der Zugriffsrechte auf OU-Ebene ersetzt werden. Dies kann in großen Unternehmen und Verwaltungen ein erhebliches administratives Risiko darstellen. Ein weiterer Nachteil von Active Directories besteht darin, dass Passworrichtlinien nur verzeichnisübergreifend gelten und nicht in einzelnen Organisationseinheiten (OU), in denen besonders sensible Daten verarbeitet werden, explizit verschärft werden können. Darüber hinaus richtet Windows 2000 standardmäßig zwischen allen Domänen transitive (gegenseitige) Vertrauensstellungen ein. Traut also Domäne A der Domäne B und Domäne B der Domäne C, dann traute auch Domäne A der Domäne C.

Für das Administrieren (Vergabe von Rechten, Einrichten von Benutzerkonten) der Domänen gibt es, wie unter Windows NT, die Gruppe der Administratoren. Durch die Vertrauensstellungen der Domänen untereinander ergibt es sich aber nicht automatisch, dass ein Administrator einer Domäne Rechte auf allen anderen Domänen hat. Eine Ausnahme bilden hier die Administratoren der Stamm-Domäne (Root-Ebene), sie sind in einer speziellen Gruppe, den Organisations-Admins. Die Organisations-Admins bekommen automatisch die Berechtigung, sich in allen Domänen der Gesamtstruktur mit unbeschränktem Zugriff anzumelden.

Da der Einsatz eines Active Directory aufgrund des internen Abstimmungsprozesses auch einen erheblichen personellen und technischen Aufwand bedeuten würde, wurde der Einsatz eines Active Directories in der bremischen Verwaltung zunächst zurückgestellt. Vorab sollen Erfahrungen mit Active Directories aus anderen Städten auf Wirtschaftlichkeits- und Datenschutzaspekte genauer geprüft werden. Trotz der Risiken, die mit Active Directories verbunden sind, ist der Einsatz von Windows 2000 als Server-Betriebssystem zu empfehlen, weil dieses Betriebssystem eine Reihe zusätzlicher Funktionen enthält, die zur Sicherheit von Netzen beitragen können:

- Das Dateisystem EFS (Encryption File System) erlaubt den Benutzern, Daten oder ganze Verzeichnisse auf lokalen Datenträgern online zu verschlüsseln. Dies ist beispielsweise bei Verlust von Wechselplatten oder bei Diebstahl des Gerätes ein entscheidender Vorteil gegenüber Windows NT. Realisiert wird der Schutz mit Hilfe einer auf öffentlichen Zertifikaten basierenden Verschlüsselung unter Nutzung der CryptoAPI-Architektur von Windows 2000. Die Dateien werden mit einem schnellen symmetrischen Verschlüsselungsalgorithmus verschlüsselt, der einen nach dem Zufallsprinzip erzeugten Schlüssel zur Datenverschlüsselung (Files Encryption Key - FEK) verwendet. Da EFS eng mit dem Dateisystem NTFS verknüpft ist, ist die Verschlüsselung der Daten transparent, d.h. der berechtigte Benutzer kann die Daten im Klartext lesen. Die Daten liegen nur dann in verschlüsselter Form vor, wenn die Daten in ein externes Dateisystem kopiert oder von einem unberechtigten Benutzer aufgerufen werden.
- Windows 2000 ermöglicht nicht nur die Authentifizierung der Benutzer gegenüber einem Domänen Controller, sondern unterstützt auch umgekehrt Identitätsnachweise bestimmter Netzwerkdienste gegenüber dem Benutzer. Für beide Arten der Authentifizierung verwendet Windows 2000 das Sicherheitsprotokoll Kerberos, Version 5. Kerberos v5 setzt zum Verschlüsseln von Kennwörtern kryptografische Mechanismen ein; somit werden Kennwörter nicht als Klartext sondern verschlüsselt über Netzwerkleitungen gesendet.
- Um die Integrität, Authentifizierung und Vertraulichkeit von Netzwerkdaten zu gewährleisten unterstützt Windows 2000 das Internet Protocol Security (IPSec). IPSec gestattet die Verschlüsselung (Ende-zu-Ende-Verschlüsselung) der Datenübertragung auf der Netzwerkschicht des OSI-Modells und eignet sich zur Absicherung von Client-Server-Anwendungen bzw. zum Sichern von Server-Verbindungen. Zum Verschlüsseln der Paketdaten wird der DES-Algorithmus (Data Encryption Standard) oder der 3DES-Algorithmus (Dreifach-Data Encryption Standard) verwendet. Es handelt sich hier um symmetrische Verschlüsselungsalgorithmen, die die Daten in Blöcken von 64 Bit (Bei 3DES wird jeder Block dreimal verarbeitet) verschlüsselt.
- Die Zertifikatsdienste von Windows 2000 ermöglichen den Aufbau einer Schlüssel-Infrastruktur (Public Key Infrastructure - PKI), die dazu genutzt werden kann, bei Bedarf einen großen Kreis von Benutzern zu authentifizieren und diesen Benutzern verschlüsselte und signierte Daten zuzuschicken. Zertifikatbasierte Prozesse unter Windows 2000 verwenden X.509v3 als standardmäßiges Zertifikatsformat.