

Windows NT (II)

Sicherheit von Windows NT in Netzwerken

Der Einsatz von Microsoft Windows NT auf PCs als Arbeitsplatzrechner und für Serveranwendungen nimmt auch an der TU Clausthal einen wachsenden Stellenwert ein. Beinahe in jedem Fall damit verbunden ist eine Anbindung des Computers an das Hochschulnetzwerk und damit an das Internet. Dies stellt, je nach Einsatzbereich, verschiedene Anforderungen an die Absicherung des Systems gegen unberechtigten Zugriff von außen, also aus dem Netzwerk und lokal, also durch einen Benutzer an der Konsole. Dieses DV-Info soll NT-Administratoren einen Überblick über die verschiedenen Möglichkeiten der Absicherung von Windows NT gegen diesen unberechtigten Zugriff bieten. Es kann nicht die Sicherungsmöglichkeiten im einzelnen erschöpfend behandeln, im Anhang wird aber auf weitergehende Literatur und Bezugsquellen für Dokumentation und Software verwiesen.

Netzwerksicherheit

Mit Windows NT sind zahlreiche Möglichkeiten gegeben, Informationen über Netzwerke zugänglich zu machen und auf solche zuzugreifen, vom Freigeben von Dateien und Verzeichnissen bis hin zum WWW- oder FTP-Server. Hier bieten sich für einen Angreifer Möglichkeiten, unauthorisierten Zugriff auf das System zu erlangen oder schwerwiegende Funktionsstörungen hervorzurufen.

Dateifreigaben

Wichtiger Bestandteil von Windows-Netzwerken sind freigegebene Laufwerke und Verzeichnisse. Wichtig bei der Vergabe von Zugriffsrechten für diese ist die Unterscheidung von Freigabe- und Dateiberechtigungen: Freigaberechte gelten jeweils für den gesamten freigegebenen Datenbereich, NTFS-Berechtigungen können auf Dateiebene, also wesentlich feiner gesetzt werden. Bei der Ermittlung der Zugriffsrechte eines Benutzers auf eine Datei wird die jeweils restriktivste Einstellung verwendet.

Aus diesem Grund ist eine sinnvolle Vorgehensweise, die Freigabeberechtigungen nicht zu restriktiv zu setzen (z.B. „Ändern“-Zugriff für alle Domänen-Benutzer) und die genaueren Einstellungen auf NTFS-Ebene zu setzen. Bei der Vergabe von Rechten ist daran zu denken, daß „Jeder“ (oder in der englischen Version „everyone“) tatsächlich auch nicht an der Domäne angemeldete Clients

meint, also wirklich **jedem** der Zugriff auf diese Ressourcen ermöglicht wird.

IIS

Der Internet Information Server (IIS) ermöglicht es unter anderem, eigentlich klassische Unix-Serverdienste wie WWW und FTP auf einem NT-Server anzubieten. Aus Sicherheits- und Stabilitätsgründen ist von diesem Einsatz jedoch abzuraten.

TCP/IP-Implementation

Das TCP/IP-Protokoll unter Windows NT beinhaltet einige Programmierfehler, die es ermöglichen, von außen das System zu unvorhergesehenem Verhalten oder einem Systemcrash zu bringen. Um hiervor einigermaßen geschützt zu sein, sollten das jeweils aktuelle NT-Servicepack und zumindest die für dieses Protokoll veröffentlichten Hotfixes von Microsoft installiert werden. Ein Mirror dieser Dateien findet sich auf [ftp.tu-clausthal.de](http://ftp.tu-clausthal.de/pub/winnt-fixes) im Verzeichnis `/pub/winnt-fixes`.

Sicherung der Konsole

Systemrichtlinien

In einer NT-Domäne (also einem Netzwerk mit mindestens einem NT-Server, der als PDC fungiert und mehreren NT-Workstations) ist eine wirkungsvolle Kontrolle der Benutzer an den Workstations über Systemrichtlinien (Policies) möglich. Hierbei handelt es sich um eine Sammlung von Registrierungseinträgen, die vom NT-Server bereitgestellt und beim Anmelden eines Benutzers an einer Workstation von dieser in die lokale Registry importiert werden. Diese Richtlinien können dabei entweder benutzer- oder rechnerabhängig definiert werden, je nachdem, in welchem Teil der Registry sie gespeichert werden. Der NT-Server verfügt zum Editieren dieser Einstellungen über den Policy-Editor (`poledit.exe`), mit welchem solche Richtliniendateien erstellt werden können.

Zugriffsrechte

Windows NT bietet mit dem Dateisystem NTFS¹ erstmals in der Microsoft-Welt die Möglichkeit, mehreren

¹NEW TECHNOLOGY FILE SYSTEM

Benutzern verschiedene Zugriffsrechte auf Dateien zu geben. Leider sind nach der Installation insbesondere die Berechtigungen für die Systemverzeichnisse großzügiger vergeben als für den Betrieb erforderlich, Benutzer dürfen wesentliche Teile des Betriebssystems verändern. Eine genaue Anleitung zur Behebung würde den Rahmen dieses DV-Infos sprengen, die unten angegebene Literatur geht aber zumindest kurz auf dieses Thema ein.

Mail- und Makroviren

Es ist möglich, Mails mit angehängten Programmen zu versehen, die ohne Kontrolle des Benutzers ausgeführt werden und Schäden auf dem Rechner anrichten können. Das gleiche gilt für Makros, die in Dokumenten für zum Beispiel Winword, Access oder Excel enthalten sein können. Neben Aufklärung der Benutzer und aufmerksamer Programmkonfiguration können hier Virens Scanner Abhilfe schaffen, die auch Mails automatisch überprüfen können.

Überwachungsmöglichkeiten

Mit dem Betriebssystem wird ein Programm zur Überwachung von Systemereignissen installiert, die *Ereignisanzeige*². Hier werden nicht nur Ereignisse wie Fehler in Systemdiensten, An- und Abmeldungen von Benutzern und Meldungen von Anwendungsprogrammen gesammelt, auch *Auditingdaten* können gesammelt und überwacht werden. Im Sinne von Windows NT bedeutet *Auditing* das Überwachen von Zugriffen auf Dateien und Drucker. Es ist einstellbar, daß bei bestimmten Zugriffsarten (Lesen, Schreiben, Erfolg, Fehler, ...) von bestimmten Benutzern entsprechende Logmeldungen generiert werden. Auch hier muß auf die Fachliteratur verwiesen werden.

Service Packs und Hotfixes

In unregelmäßigen Abständen werden von Microsoft sicherheitsrelevante Fehler in Windows NT behoben. Mi-

²In der englischen Version *Event-Manager*

crosoft veröffentlicht dazu Patches, die *Hotfixes*, die auf betroffenen Systemen installiert werden können. Die aktuellen Hotfixes werden auf ftp.tu-clausthal.de bereitgehalten.

In größeren Zeitabständen faßt Microsoft mehrere Hotfixes und andere Patches, die nicht dringend genug für die Erstellung eines Hotfix waren, in Servicepacks zusammen, die zu installieren in jedem Fall empfehlenswert ist, auch wenn nicht unbedingt jeder Hotfix auf jedem System erforderlich ist. Manche Softwarepakete erfordern mindestens ein bestimmtes Servicepack; leider existiert auch Software, die ab einem gewissen Patchlevel nicht mehr läuft. Aktuell ist momentan SP 6 für Windows NT 4.0. Die Servicepacks sind ebenfalls auf ftp.tu-clausthal.de verfügbar.

Informationsquellen

RRZN-Broschüren, Online-Information (WWW, Mailinglisten)

- In der Materialausgabe des Rechenzentrums sind Dokumentationsschriften des Regionalen Rechenzentrums Niedersachsen (RRZN) zu Windows NT erhältlich. Insbesondere „Windows NT 4.0 für Systembetreuer“ und „Windows NT 4.0 Server-Netzadministration“ sind zu Sicherheitsfragen empfehlenswert.
- ASHLEY J. MEGGIT und TIMOTHY D. RITCHEY, „Windows NT User Administration“ O'Reilly & Associates, 1997, enthält unter anderem Informationen über scriptgesteuerte Benutzerverwaltung und Registryzugriffe mit der Scriptsprache Perl.
- WWW-Seiten des DFN-CERT:
<http://www.cert.dfn.de/>
- TUC-spezifisch:
<http://www.rz.tu-clausthal.de/PC-Pool/FAQ/>

T. Nordenholz <nz@thiemo.net>

DV-info

Datenverarbeitung an der TU Clausthal

Mitarbeiter der TU Clausthal können DV-info auch über die Hauspost beziehen. Wenden Sie sich bitte an das Geschäftszimmer des Rechenzentrums oder senden Sie eine EMail an:

DV-info-request@rz.tu-clausthal.de

Weitere Exemplare liegen z. B. im Rechenzentrum aus. Die PostScript Dateien werden über den FTP Server ftp.tu-clausthal.de veröffentlicht.



Herausgeber:

RECHENZENTRUM

Technische Universität Clausthal

Erzstraße 51

38678 Clausthal-Zellerfeld

Telefon: 05323/72-2352

Telefax: 05323/72-3536

WWW: <http://www.rz.tu-clausthal.de/>