Sicherheit in Windowssystemen

Referent: Roger Klose

IT-Sicherheitsprinzipien

Implementieren von Sicherheit

- Methoden der Implementierung
- Herausfinden von Sicherheitslücken
- Patchmanagement
- Authentifizierung
- Privilegien & Privilegienmanagement
- Hardening
  - An welchen Stellen kann das Betriebssystem gehärtet werden?
  - Installation
  - Absichern der Anmeldung
  - (Importierbare) Vorlagen
  - Benutzer & Gruppen
  - Dienste
  - Sicherheit durch Registrierungseinstellungen
  - Überwachung (Auditing)
  - Software einschränken
  - Browser & IE

Voraussetzungen für IT-Sicherheitsprinzipien

- System Ownership

  Für jedes IT-System und für jeden IT-Prozess sollte ein Verantwortlicher benannt werden. Zu den Aufgaben des Verantwortlichen zählen insbesondere die Festlegung der Sicherheits- und Qualitätsanforderungen an das System /an den IT-Prozess.

  Durch das Konzept des System Owner werden Verantwortlichkeiten zugewiesen.

  Die Definition /Zuweisung von Verantwortlichkeiten ist wesentlich für das Funktionieren von IT

- Dokumentation

  Für jedes IT-System und jeden IT-Prozess sollte es eine stets aktuelle Dokumentation geben.

  Eine stets aktuelle Dokumentation ist für das Funktionieren von IT im allgemeinen und für die Implementierung von IT-Security im Besonderen eine zwingende Voraussetzung.

IT-Sicherheitsprinzipien

1. Minimal Machine /Minimalsystem
2. Hoher Patchlevelstand
3. Least Privilege
4. Segregation of Duties
5. Nachvollziehbarkeit
6. Einsatz starker Authentifizierungsmechanismen
7. Defense in Depth
8. Secure the Weakest Link
9. Psychologische Akzeptanz
10. Legal Compliance

Minimal Machine /Minimalsystem

Gültig für Software und Hardware: Auf einem System sollen nur die Teilkomponenten installiert sein, die für die Anforderungen an dieses Systems notwendig sind. Alle weiteren Devices, Module, Dienste oder Applikationen machen das System anfälliger für Sicherheitslücken und sollen weder logisch noch physisch installiert werden.

Beispiele: Unnötige Systemdienste (z. B. Alerter); zus. Software; USB-Schnittstellen

Hoher Patchlevelstand

Der Patchlevel von Betriebssystem und eingesetzten Diensten und Applikationen sollte möglichst hoch sein.

Berichte aus der Praxis

Beispiel: WMF-Exploit von Windows-Systemen Dezember 2005

Least Privilege

Alle Benutzer, Dienste und Applikationen sollen nur mit dem für ihre Funktion minimal notwendigen Maß an Berechtigungen ausgestattet sein und das auch nur in der Zeitspanne, in der dies erforderlich ist.

Beispiele: Run as-Befehl; Local Service- & Network Service-Konten

Segregation of Duties

Zuständigkeiten und /oder Funktionalitäten sollen innerhalb eines Systems auf verschiedene Rollen und Personen, bei mehreren Systemen auf verschiedene Systeme und /oder Netzwerksegmente, für die ihrerseits unterschiedliche Rollen und Personen verantwortlich sind, verteilt sein.

Beispiele: VLANS; unterschiedliche Serverrollen; Kernel- und Usermode

Nachvollziehbarkeit

IT-Prozesse und sicherheitsrelevante Aktionen auf Systemen sollen nachvollziehbar sein. Nachvollziehbarkeit gewährleistet die eindeutige Zuordnung von IT-Prozessen und Aktionen auf/von Systemen zu den Rollen, die die Aktion /den IT-Prozess ausgelöst haben. Wenn Nachvollziehbarkeit gewährleistet ist, dann kann eindeutig geklärt werden, wer eine bestimmte Aktion durchgeführt hat.

Die Implementierung der 'Segregation of Duties' ist Voraussetzung für Nachvollziehbarkeit. Damit IT-Prozesse und sicherheitsrelevante Aktionen nachvollziehbar sind sollte insbesondere Folgendes gewährleistet sein:

- Einheitlichkeit: Installationen von ähnlichen Systemen und die Organisation von ähnlichen Prozessen sollten einheitlich sein.
- Logfiles und deren Auswertung: Für Systeme und Benutzer sollte nach definierten Regeln ein kontinuierliches Monitoring durchgeführt werden. Die daraus entstandenen Logfiles sollten in regelmäßigen Abständen analysiert und bewertet werden.
- Rollen- und Personentrennung
- Dokumentation

Einsatz starker Authentifizierungsmechanismen

Es sind möglichst starke Authentifizierungsmechanismen einzusetzen, und es ist ein formaler Prozess für das Management von Authentifizierungsmechanismen zu etablieren.

- Die Unterscheidung authorisierter Nutzer von (üblicherweise unauthorisierten) Angreifern findet anhand ihrer Authentifizierung statt.
- Der formale Prozess für das Managment von Authentifizierungsmechanismen garantiert die stetige Zuverlässigkeit dieser Mechanismen (z. B. Beantragunsverfahren).
- Den verwendeten Verfahren und ihrer Implementierung (etwa der Kennwort-Güte) kommt entscheidende Bedeutung bei der Sicherung von Netzen zu.
- Beispiele: Allgemeine Passwort-Policy; Multifaktorielle Authentifizierung

Defense in Depth

Viele Angriffe nutzen nicht eine, offensichtliche Sicherheitslücke, sondern vielmehr eine Aneinanderreihung mehrerer kleinerer Sicherheitsmängel.

IT-Sicherheit kann daher immer nur mehrstufig (d.h. auf allen beteiligten Komponenten) implementiert werden.

Beispiel:

- 1. Schritt: Verwendung eines Exploits (wg. unzureichendem Patchmanagement)
- 2. Schritt: Installation eines Rootkits (wg. fehlendem IDP /IDS)

Secure the Weakest Link

Es soll stets das schwächste Glied der Umgebung im Auge behalten werden. Hier existieren und entstehen vor allem Sicherheitslücken, nicht auf den besonders gut geschützten Systemen

Dem Prinzip liegt die Interdenpendenz und Komplexität heutiger Computersysteme zugrunde

Es ermöglicht eine realistische Einschätzung der Gefährdung des Gesamtsystems

Beispiele: Windows 98-PCs die Messstationen steuern (und in der Domäne oder Arbeitsgruppp sind); IIS 5.0-Default-Installationen

Psychologische Akzeptanz

Sicherheitsmethoden sollten den erlaubten Zugang zu Ressourcen nach Möglichkeit nicht erschweren.

Beispiele: Komplexitätsanforderungen an das Passwort unter Windows XP und Server 2003; hohe Passwort- /PIN-Anzahl in komplexen Umgebungen

Legal Compliance

Bei der Implementierung und Anwendung von Sicherheitsmethoden ist auf die Einhaltung aller landesspezifisch gültigen Gesetze, Verträge, organisationsinternen Vereinbarungen und sonstiger möglicher Regularien zu achten

Multinationale Firmen sollten bei landesübergreifende Vorgängen die Einhaltung der landesspezifischen Gesetze beachten

Beispiel: Schutz von P-Daten großer Unternehmen; unterschiedliche erlaubte Verschlüsselungsstärken in EU und USA.

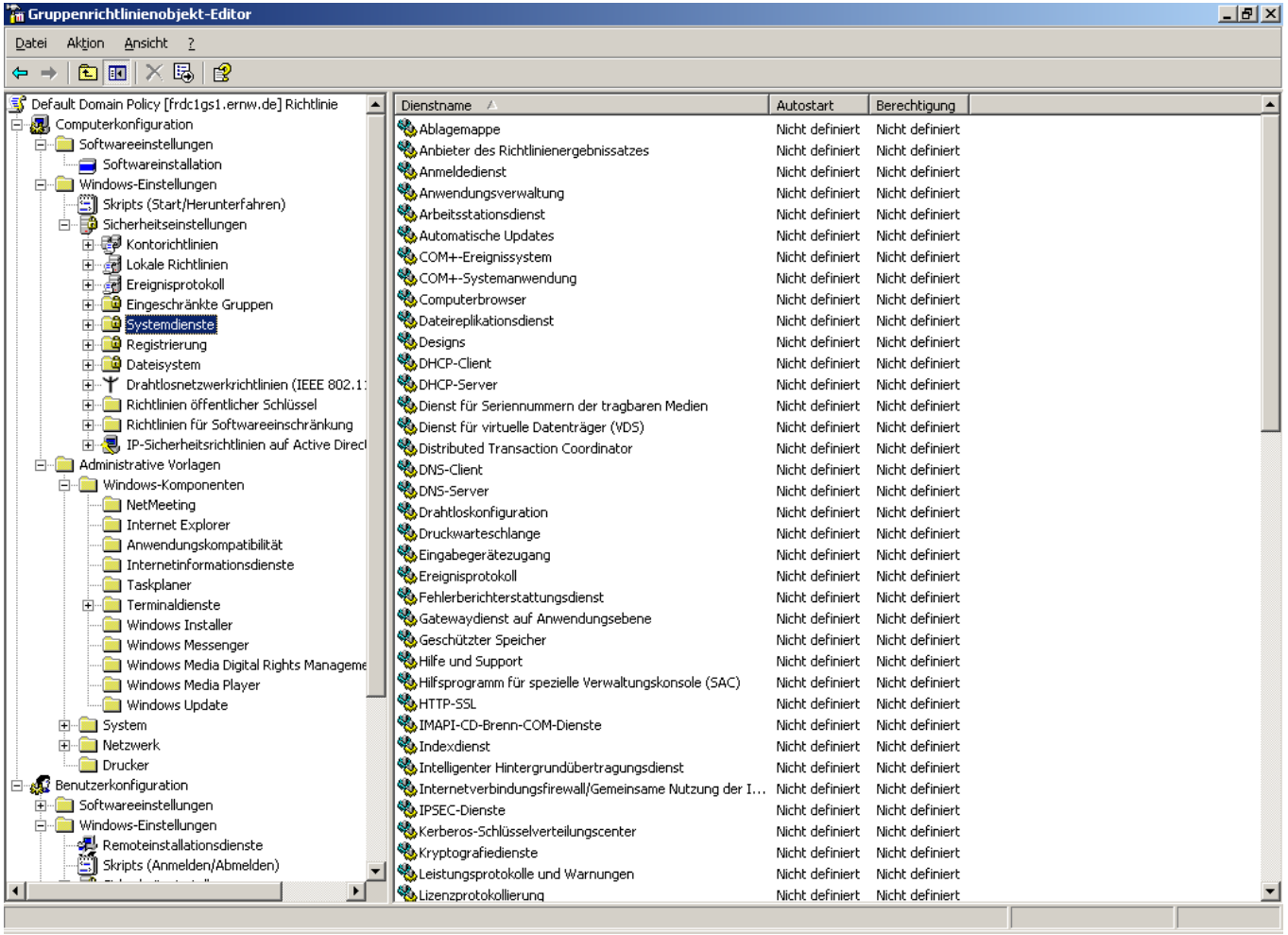
Verschiedene Methoden, Sicherheit in Windows XP zu implementieren:

- Verteilung per GPO (erfordert Active Directory-Umgebung)
- Verwendung von Vorlagen
- Konfiguration per Skript
- Manuelle Konfiguration
- Kombination aller Möglichkeiten

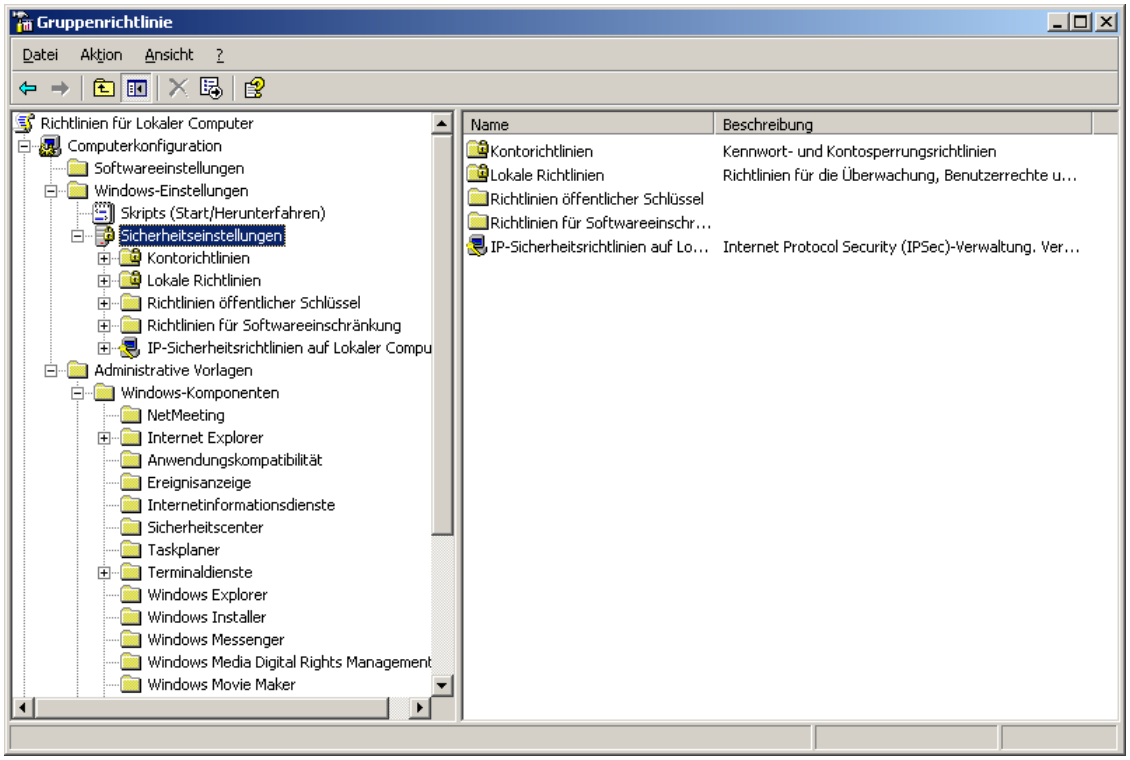
Grundsätzliches zur Verteilung per GPO (Vorteile gegenüber der Verwendung des lokalen GPO):

- Stellt wesentlich mehr Steuerungsmöglichkeiten gerade im Bereich der Sicherheit bereit (AD-GPOs bieten viel mehr Konfigurationsmöglichkeiten als das lokale GPO)
- Ermöglicht eine Konfiguration pro Benutzer + pro Computer (lokales GPO erlaubt keine Benutzerfilterung)
- Ermöglicht eine Strukturierung nach Computer-Rollen (z. B. Workstation, Entwicklungsdesktop, Außendienst-Laptop etc.)
- Einfachere Verteilung der Einstellungen auf viele Computer
- Nicht ein einziger Nachteil gegenüber lokalem GPO

- Sicherheitseinstellungen in einem Active Directory-GPO:



- Sicherheitseinstellungen im lokalen GPO:



Grundsätzliches zur Verwendung von Vorlagen:

- Liegen häufig in vorkonfigurierte Form vor und können daher einfach implementiert werden
- Es stehen viele Vorlagen von vertrauenswürdigen Organisationen im Internet frei verfügbar
- Müssen an die individuellen Bedürfnisse angepasst werden

Organisationen, die Sicherheitsvorlagen frei zur Verfügung stellen:

- Microsoft Corporation
  - Per Default mit jeder Installation ausgelieferte Vorlagen
  - Zusätzlich von Microsoft mit dem Sicherheitshandbuch für Windows XP zur Verfügung gestellte Vorlagen
- Center for Internet Security (CIS)
- National Institute of Standards and Technology (NIST)
- Defense Information Systems Agency (DISA)
- National Security Agency (NSA)

Konfiguration per Skript

- Die in vorgenannten Organisationen stellen auch sog. ‚Hardening-Skripte' bereit
- Skripte können alle ‚Bereiche' des Betriebsystems, an denen gedreht werden kann (siehe weiter unten) abdecken (z. B. Hardening der Registriy-Zugriffsrechte oder der Dienste-Konfiguration)
- Skripte müssen in der Regel für die eigenen Bedürfnisse individuell erstellt werden

Manuelle Konfiguration

- Weist den geringsten Grad an Automatisierung auf
- Ist (immer) am granularsten
- Kann alle ‚Bereiche' des Betriebsystems, an denen gedreht werden kann (siehe weiter unten) umfassen

Notwendige Begriffsdefinitionen

- Malware
- Exploit
- Rootkit
- Hook (-Methoden)

- (Malware-) Signatur
- Heuristische Methoden

- User Mode
- Kernel Mode
- Privilegien

Freeware Tools

- MBSA 2.0 (Microsoft) unterstützt folgende Microsoft-Software:
  - Windows 2000 SP3 oder neuere Version
  - Office XP oder neuere Version
  - Exchange 2000 Server oder neuere Version
  - SQL 2000 Server SP4

Herausfinden von Sicherheitslücken

- Für ältere Umgebungen und das Scannen anderer Microsoft-Produkte ist der MBSA 1.2.1 zu verwenden.
- MBSA prüft folgende Betriebssysteme und Anwendungen auf Fehlkonfigurationen:

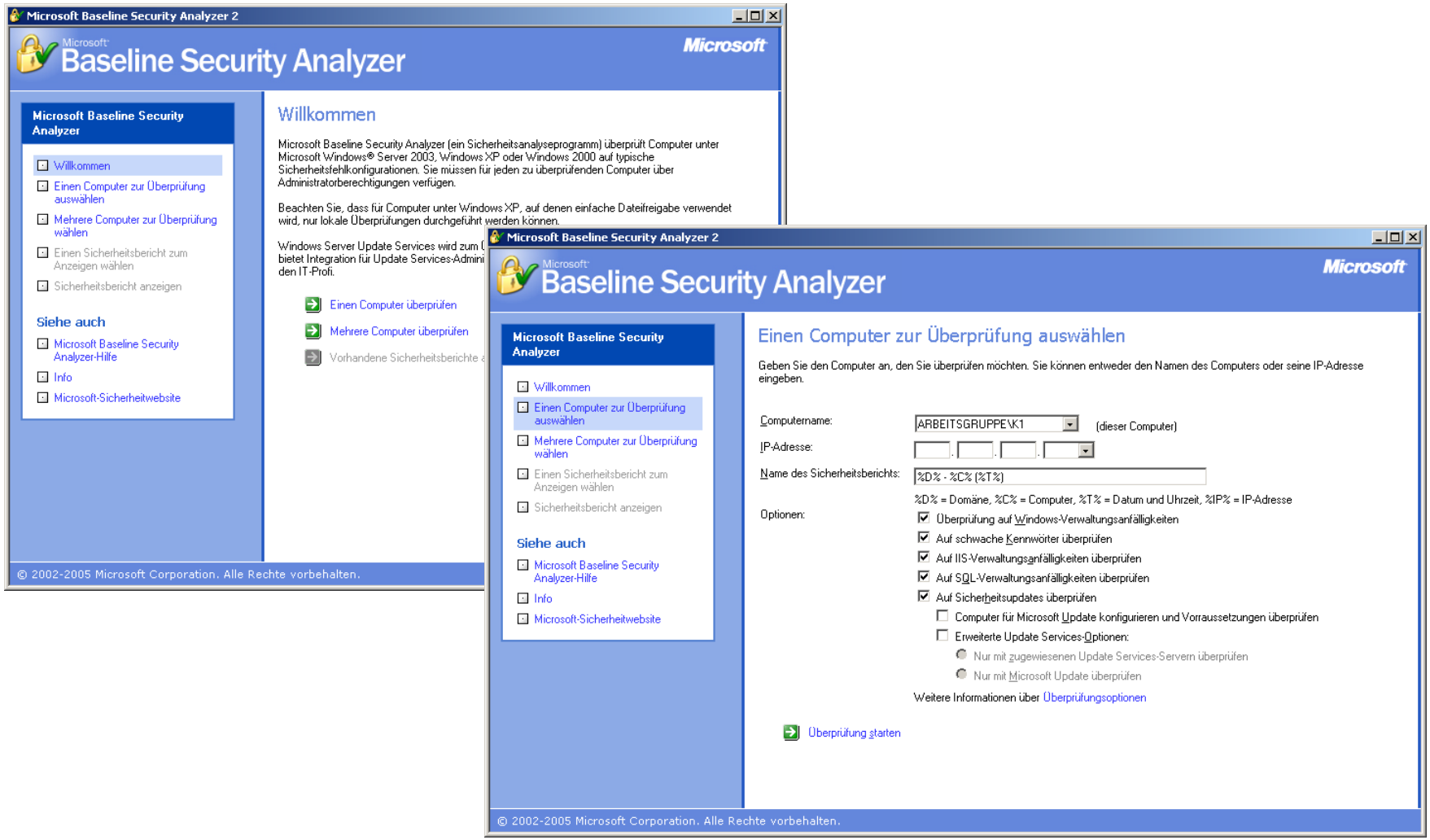
  Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003

  Internet Information Server (IIS), SQL Server, Internet Explorer, Office
- MBSA sucht nach fehlenden Sicherheitsupdates für folgende Produkte:

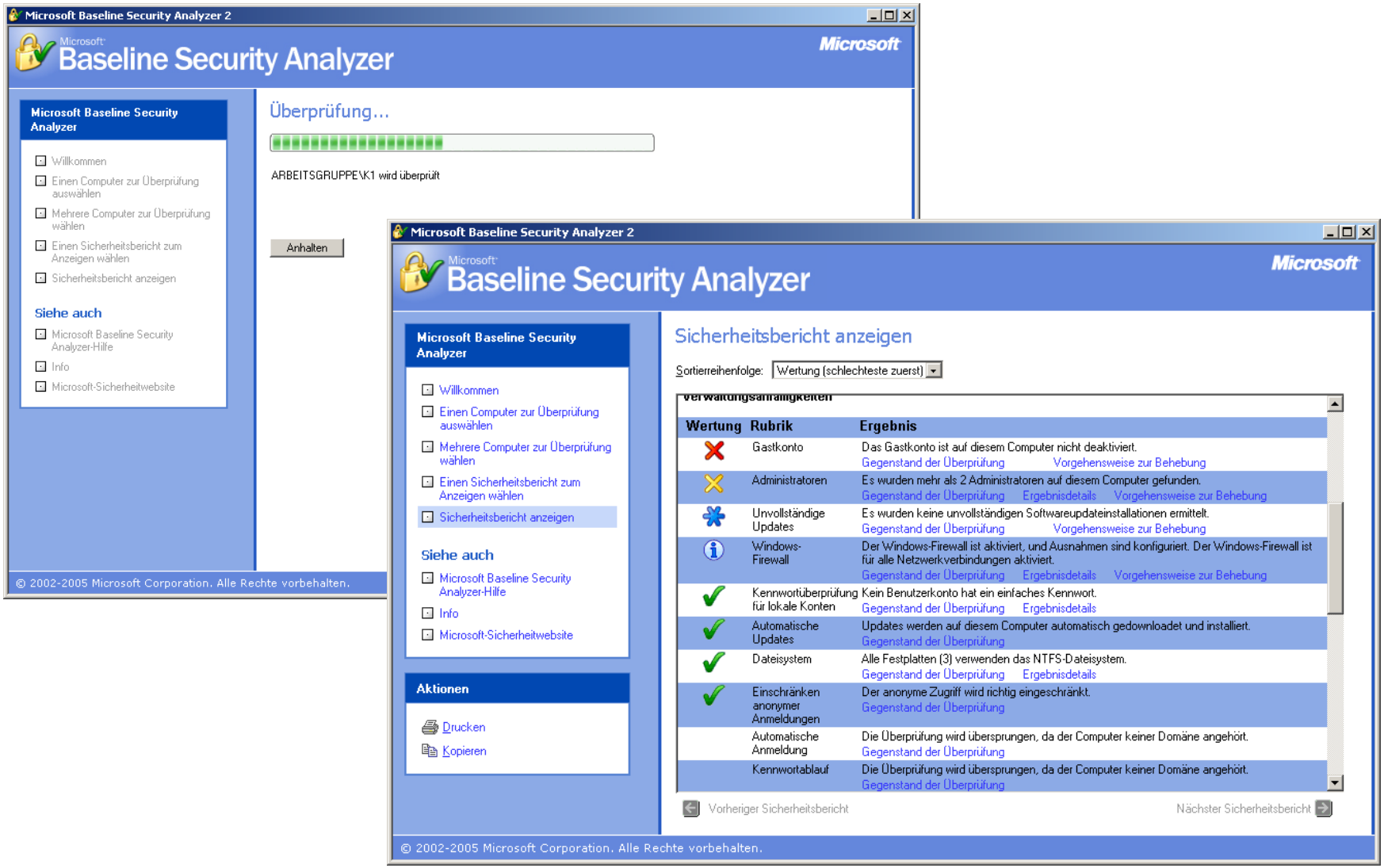
  Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003

  IIS, SQL Server, Internet Explorer, Office, Exchange Server, Windows Media Player, Microsoft Data Access Conponents (MDAC), MSXML, Microsoft Virtual Machine, Commerce Server, Content Management Server, BizTalk Server, Host Integration Server

- Das GUI von MBSA (2.0):

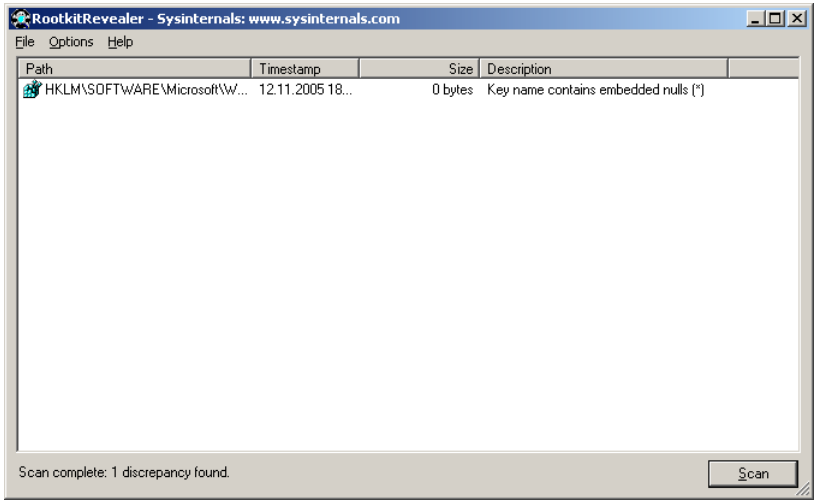


- Das GUI von MBSA (2.0):



Weitere Freeware Tools:

- Diverse Antiviren-Produkte (Signatur-basierte & heuristische Erkennung)
- Nessus (www.nessus.org) umfassender Vulnerability-Scanner
- VICE von Joanna Rutkowska (Aufspürung von Hooks)
- RootkitRevealer von Sysinternals (Suche nach persistenten Rootkits in Registry und im Dateisystem)



Kommerzielle Tools

- Nessus (professioneller umfassender Vulnerability-Scanner)
- Retina (von eEye - professioneller umfassender Vulnerability-Scanner)
- Blacklight (von F-Secure zur Aufspürung von Rootkits in Prozessen und Dateien)
- Strider Ghost Buster (von Microsoft zum Aufspüren von versteckten Dateien, Registry-Einträgen, Prozessen und geladenen Modulen)
- Tripwire (www.tripwire.com Integritäts-Checker für Festplatten)
- Copilot (an der Universität Maryland entwickelte Hardware-Lösung realisiert als PCI-Karte zum Aufspüren von Rootkits)

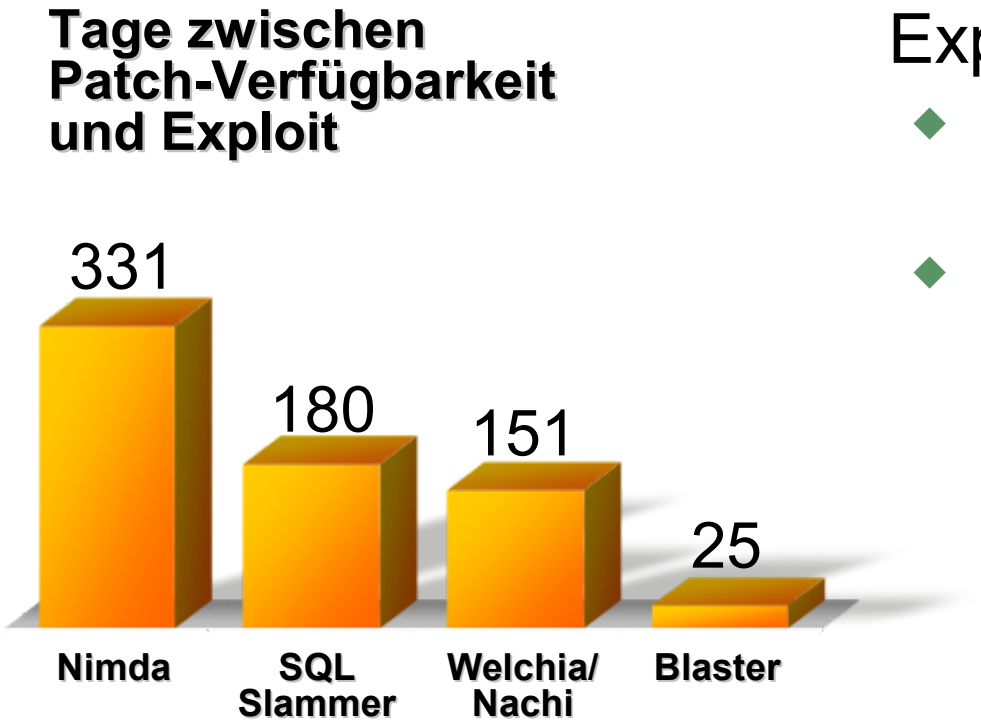
Praktischer Teil

- Download, Installation und Ausführung von MBSA 2.0
  - Scannen des lokalen Computers
  - Scannen eines remote Computers
  - Diskutieren der Ergebnisse
- Kurzdemonstration von Nessus
- Optional:
  - Download und Ausführung des RootkitRevealers
  - Download und Ausführung von VICE (erfordert .net-Framework)

Effektives (sprich: zeitnahes & korrektes) patchen wird immer wichtiger weil:

- „Time-to-Exploit“ wird immer geringer.
- Clients mittlerweile eines der Hauptangriffsziele darstellen.
- Die meisten erfolgreichen Angriffe über nicht-gepatchte Systeme führen.

Effektives Patch Management ist integraler Bestandteil einer erfolgreichen IT Security Strategie



“Tage” zwischen Patch und Exploit

- Patche werden in wenigen Tagen reverse-engineered
- Je kürzer die Zeit zwischen Patch und Exploit, umso zügiger muss geptacht werden -> hoher Automatisierungsgrad wünschenswert

Clients werden immer häufiger direktes Angriffsziel:

- Über den WebBrowser
- Per Malicious Code
- Mobile Clients befinden sich oft in nicht-kontrollierbaren Umgebungen (HotSpot am Flughafen, Hotel, etc)
- Cross-Plattform Viren/Würmer (Windows Mobile auf dem MDA/Smartphone als Angriffsplattform gegen den Standard PC)
- Neue Technologien ermöglichen neue Angriffsvektoren (z.B. Bluetooth, SSL-basierte VPNs)
- Viele tausende Clients von der „organisierten Kriminalität“ für Bot-Nets benötigt werden (je mehr, umso „besser“ das Botnet, umso mehr Geld lässt sich damit „verdienen“).

Nicht-gepatchte Systeme machen es Angreifern leicht…

- Für viele Vulnerabilities wird Exploit-Code veröffentlicht.
- Die Qualität des Exploit-Codes hat in den letzten Jahren kontinuierlich zugenommen.
- Mittlerweile gibt es „Angriffs-Frameworks“, die plug-in basiert neue Exploits einbinden: MetaSploit Framework
- Massen-Rooter (siehe z.B. „kaht2“ für die „alte“ RPC-DCOM Lücke, die auch von Blaster ausgenutzt wurde), die auch noch scriptbar sind (sprich: automatisch hacken, AV etc. deaktivieren, Hintertür einbauen, auf zum nächsten Opfer)

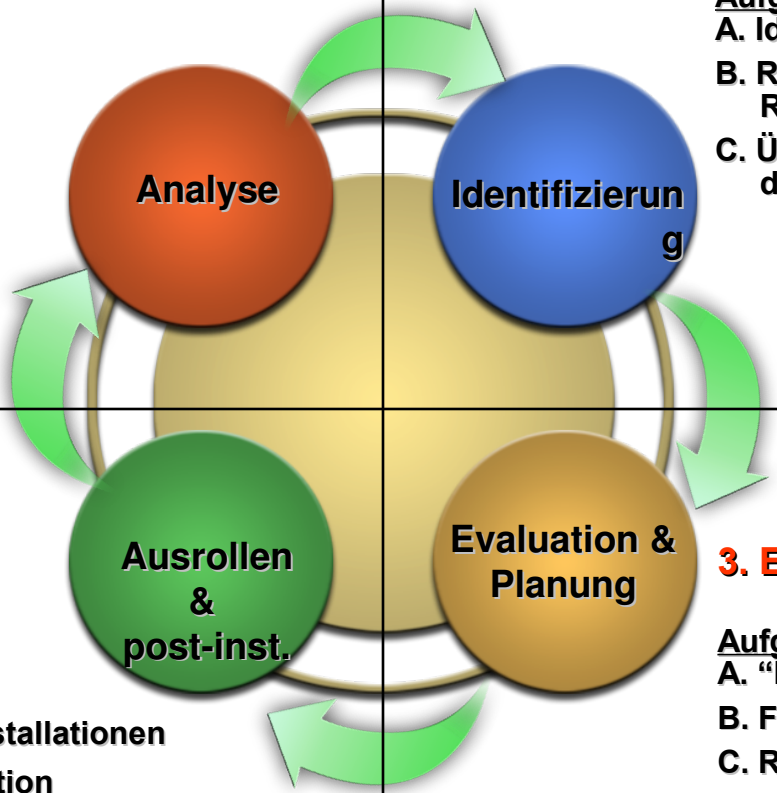
Ich erinner nur an Code Red, Nimda, SQL-Slammer, Blaster etc.
-> Patch war in jedem der Fälle zum Zeitpunkt des Ausbruchs verfügbar… aber eben nicht installiert. Wer von Ihnen war denn von einem der genannten Kandidaten betroffen? Keiner?

Patchmanagement als Prozess

1. Analyse der Umgebung

Periodische Aufgaben
A. Baseline der Systeme
B. Ist die Patch-Management Lösung noch adequat?
C. Review Infrastruktur/ Konfiguration

Fortlaufende Aufgaben
A. Discover Assets
B. Inventar der Clients



2. Identifizierung neuer Patche

Aufgaben
A. Identifizierung neuer Patche
B. Relevanz der Patche? Risiko-Analyse
C. Überprüfung Echtheit und Integrität des Patches (kein Virus, Hoax, etc)

3. Evaluation & Planung

Aufgaben
A. "Patch Acceptance"
B. Formales "ok" notwendig?
C. Risiko Analyse bzgl. der Install.
D. Planung der Patch Freigabe

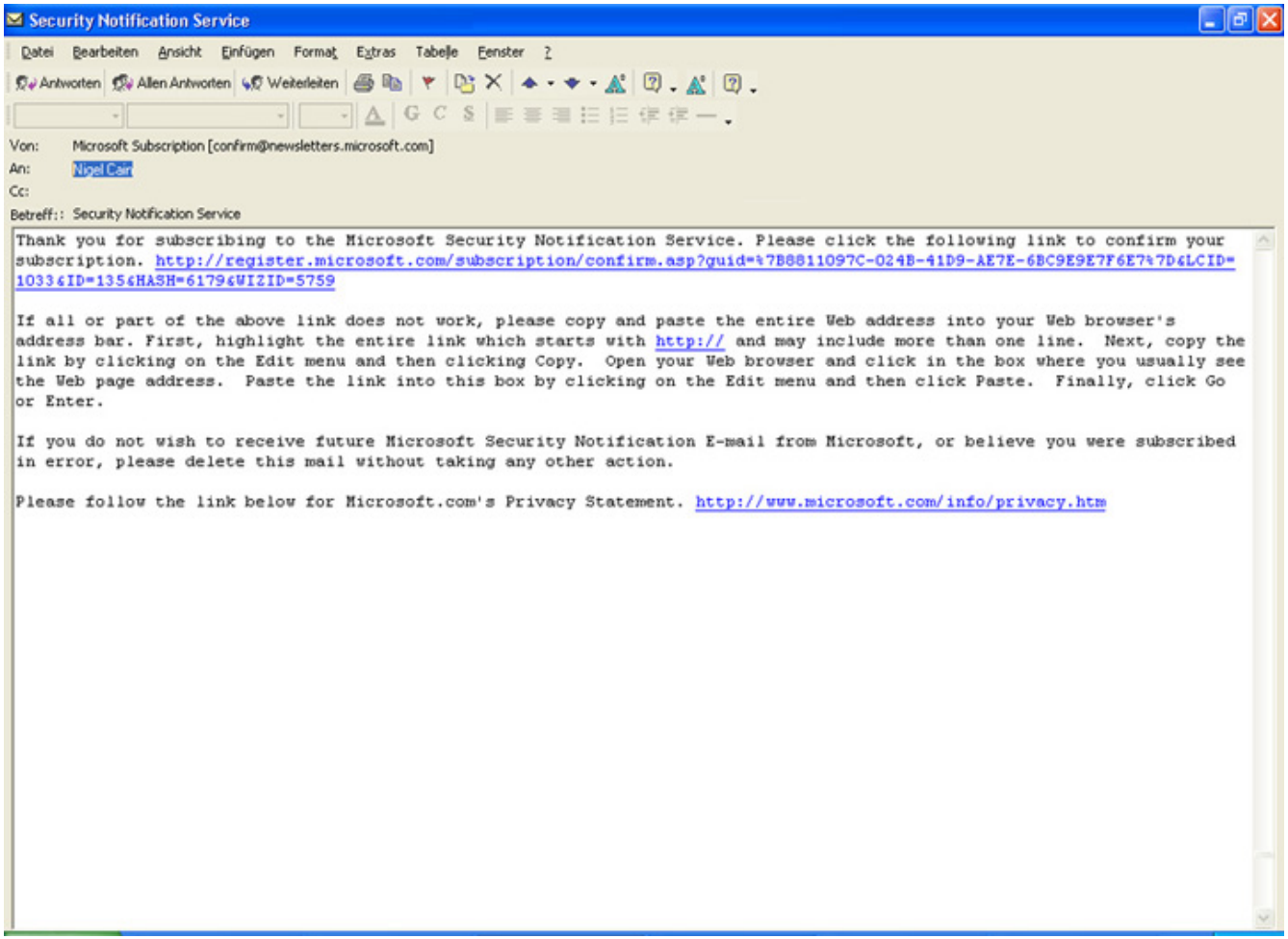
4. Ausrollen der Patche

Aufgaben
A. Verteilung & Installation
B. Bericht bzgl. Fortschritt
C. Auflösung von Konflikten und fehlgeschlagenen Installationen
D. Review der Patch-Installation
E. Post-Install, ggf. Aunahme ins Standard-Build

Benachrichtigung über neue Softwareupdates:

- kann dabei z. B. über das das Abonnieren des Microsoft Security Notification Service unter folgender Adresse: http://www.microsoft.com/technet/security/bulletin/notify.asp_ erfolgen.

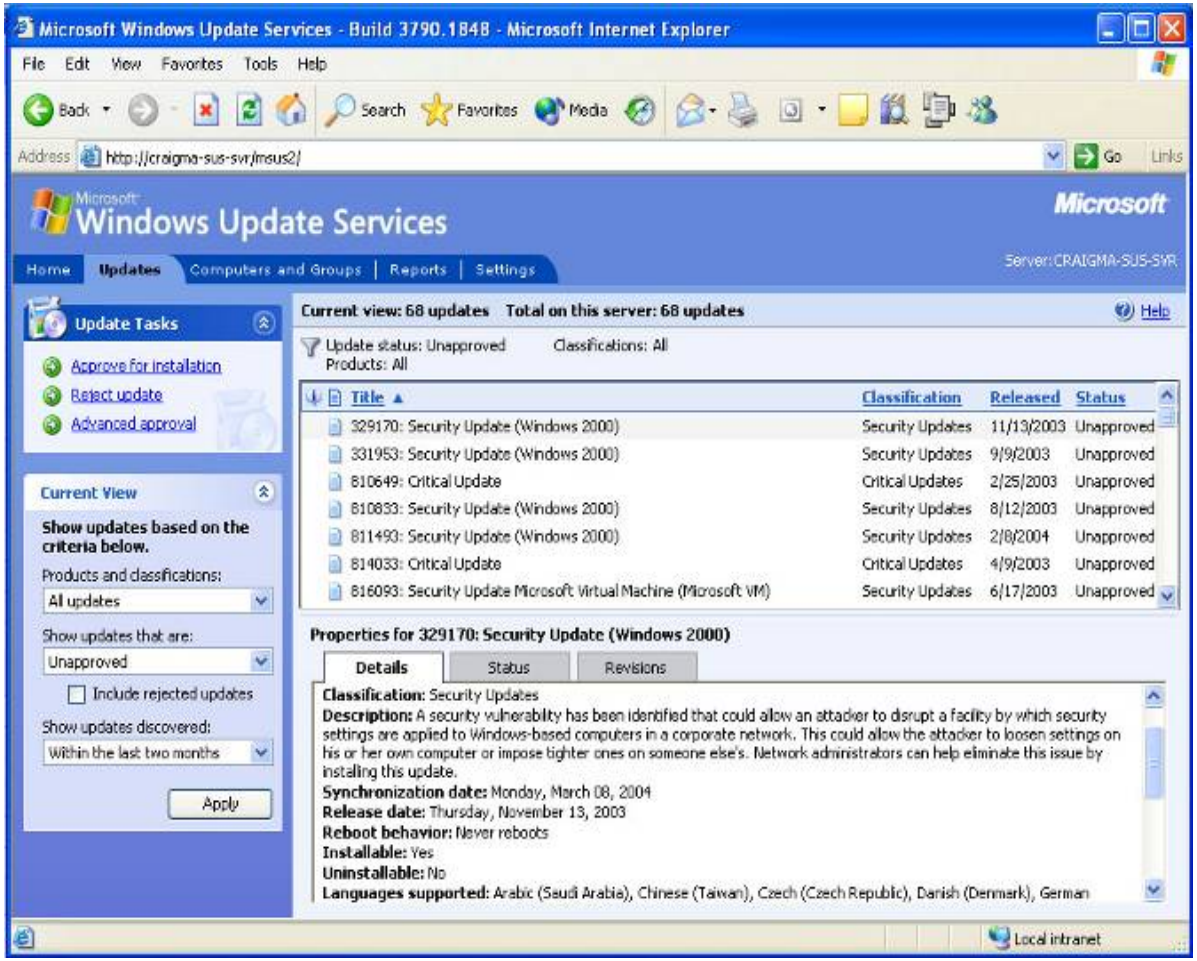
- Typische Benachrichtigung (nächste Folie):


Security Notification Service
Datei Bearbeiten Ansicht Einfügen Format Extras Tabelle Fenster ?
Antworten Allen Antworten Weiterleiten
Von: Microsoft Subscription [confirm@newsletters.microsoft.com]
An: Nigel Cair
Cc:
Betreff:: Security Notification Service
Thank you for subscribing to the Microsoft Security Notification Service. Please click the following link to confirm your subscription. http://register.microsoft.com/subscription/confirm.asp?guid=%7B8811097C-024B-41D9-AE7E-6BC9E9E7F6E7%7D&LCID=1033&ID=135&HASH=6179&WIZID=5759
If all or part of the above link does not work, please copy and paste the entire Web address into your Web browser's address bar. First, highlight the entire link which starts with http:// and may include more than one line. Next, copy the link by clicking on the Edit menu and then clicking Copy. Open your Web browser and click in the box where you usually see the Web page address. Paste the link into this box by clicking on the Edit menu and then click Paste. Finally, click Go or Enter.
If you do not wish to receive future Microsoft Security Notification E-mail from Microsoft, or believe you were subscribed in error, please delete this mail without taking any other action.
Please follow the link below for Microsoft.com's Privacy Statement. http://www.microsoft.com/info/privacy.htm

Patchmanagement – Microsoft Produkte

Fähigkeit	Windows-Update	WSUS	SMS 2003
Unterstützte Software Produkte	Windows 2000, Windows XP, Server 2003	Dito + Office (XP + 2003), Exchange 2003, SQL Server 2000, MSDE	Dito + NT 4.0, Windows 98, bel. Windows-Software
Updates von Erweiterungen	Alle Updates, Treiber Updates, Service Packs	Alle Updates f. unterst. Produkte, SPs, FPs, krit. Treiberupdates	Updates f. jede bel. Windows-basierte Software
Update-Management Fähigkeiten:			
Zielgerichtete Verteilung	n. a.	ja (grob)	ja (sehr granular)
Bandbreiten-Optimierung	ja	ja	ja

Das GUI von WSUS:



Neben Patchmanagement stellen starke Authentifizierungsmechanismen integralen Sicherheitsbestandteil dar

Implementierung einer guten Kennwortrichtlinie extrem wichtig

⇒ Nur: wie soll die Aussehen?

⇒ Vorschläge ??

- Nachteile eines komplexen Kennworts mit Sonderzeichen zusammen mit langer Kennwortchronik und niedriger Kontosperrungsschwelle (Microsoft-Empfehlung):
  - Kein technisches, sondern ‚menschliches' Problem
    - Motivationsproblem
  - Paßwort wird langsam eingetippt
  - Paßwort wird zugänglich niedergeschrieben
  - etc.
  - Häufiges Kennwortzurücksetzen (Helpdesk)
- Lan-Manager-Hash
  - Speicherung bei Kennwörtern bis zu 14 Zeichen (Grenze bei NT 4.0)
  - Umgehung: Deaktivierung im Gpo oder längeres Kennwort

Vorteile eines Paßsatzes statt Paßwortes

- 15 Zeichen schwer zu hacken
- Vergleich der Rechenzeiten zum Hacken (ca. 532.000 Jahrhunderte vs. ca. 4 Jahre!)
- Verzicht auf Komplexität des Paßsatzes

Fazit: mind. 15 Zeichen langes Paßwort:

- Verzicht auf Komplexität
- Mit schwacher Chronik (z. B. 2 Paßsätze pro 4 Monate)
- Kontosperrungsschwelle hoch (z. B. > 30 Versuche)

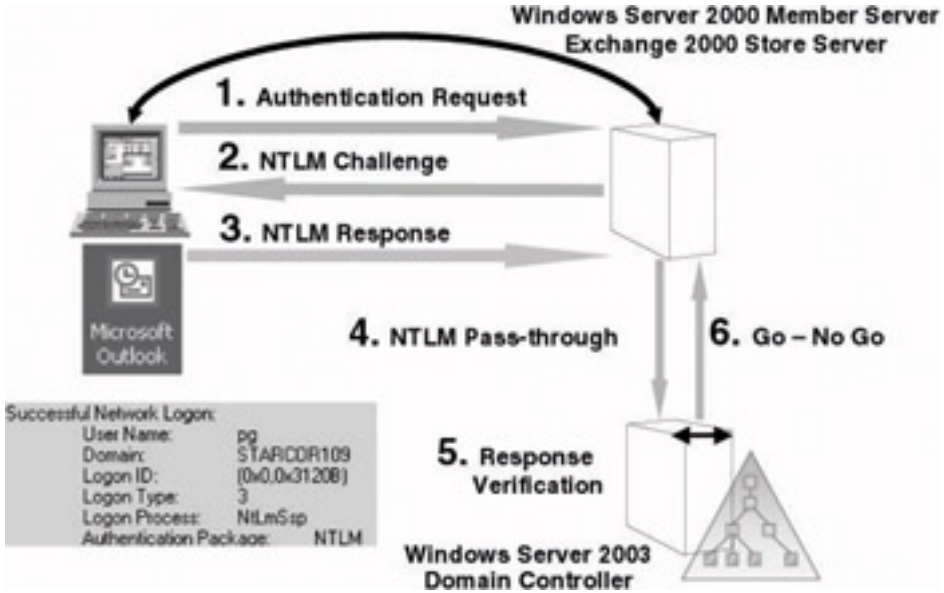
Problem der Implementierung im AD:

- Gui im Gpo lässt max. 14 Zeichen zu!
- Clients von Windows 2000
- Evtl. GUIs zur Paßsatzeingabe
- Lösung möglich per KB Artikel

Gängige Authentifizierungsprotokolle

Authentifizierungsprotokoll	Erläuterung
Basic Authentication	Teil der HTTP1-Spezifikation, Browserauthentifiz. gegen Webseite; Credentials gehen Base64-encodiert übers Netz; breite Unterstützung; sehr unsicher; kombinierbar mit SSL.
Digest Authentication (RFC 2617)	Als Ersatz zu Basic Authent. gedacht; HTTP-basierte Authentifiz., der ein Challenge-Response (CR)-Mechanis-mus unterliegt; Credentials nicht übers Netz, statt dessen mit Passwort gehashter Nonce; verwendet MD5. Anfällig gegenüber Replay-Attacken.
SSL /TLS (RFC 2246)	SSLv3 (von Netscape f. sichere Kommunik. über unsich. Kanal entwickelt) dient als Basis f. TLS; verwendet Zertifikate zur gegens. Authentifiz., kann starke Authentifiz. f. HTTP, SMTP, NNTP implementieren.
Kerberos (RFC 1510)	Sicheres Standardprotokoll im Active Directory; verwendet zur gegens. Authentifiz.; existiert auch in freien Versionen.
NTLM	Proprieträres Protokoll von MS; hauptsächl. Verwend. in Windows NT; verwendet CR-Mechanismus; existiert in den Versionen NTLM, NTLMv1, NTLMv2.

…am Beispiel der Authentifizierung eines Outlook 2003-Clients gegenüber einem Exchange 2000-Server (Verwendung des Challenge Response-Mechanismus):



NTLM-Authentifizierung absichern

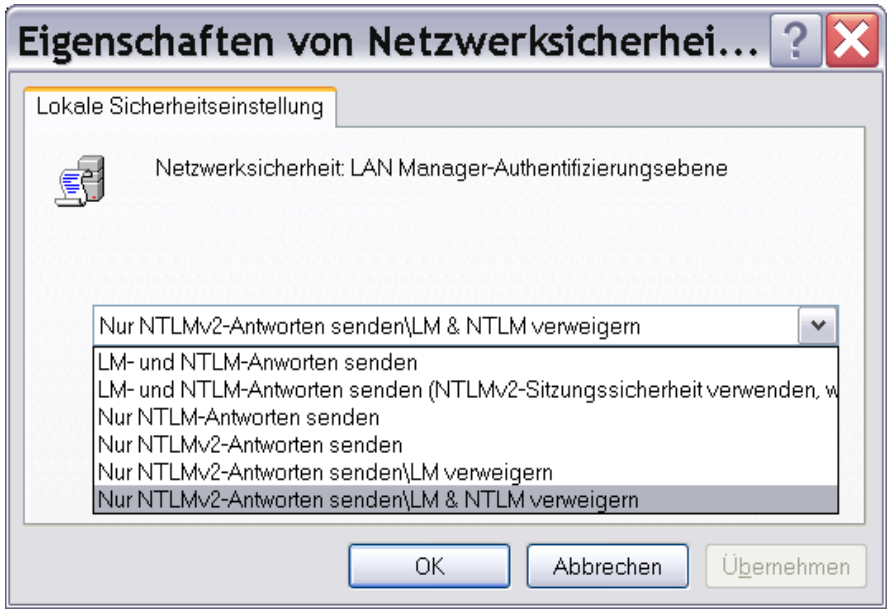
Absicherung der NTLM-Authentifizierung duch Anheben der LAN Manager-Authentifizierungsebene in Windows XP und Server 2003.

Lokal:

Gpedit.msc|
Computerconfiguration|
Windows-Einstellungen|
Sicherheitseinstellungen|Lokale Richtlinien|Sicherheitsoptionen

Im Active Directory:

Durch identische GPO-Einstellung (sollte auf Domänenebene sein).

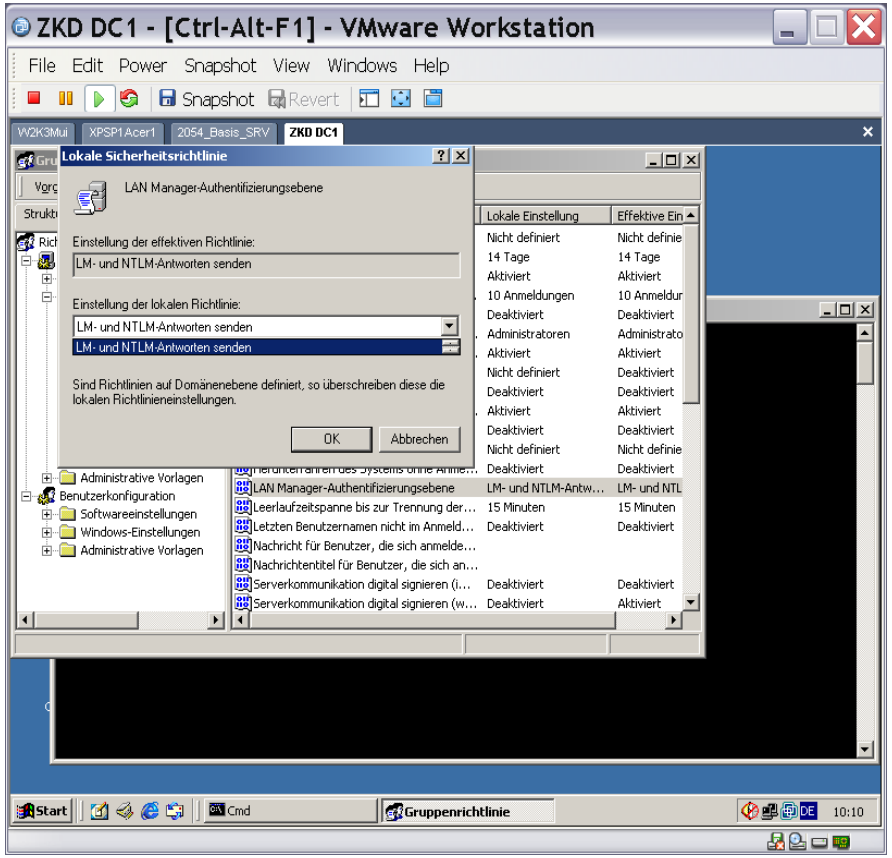


NTLM-Authentifizierung absichern

Absicherung der LAN Manager-Authentifizierungs Ebene in Windows 2000 nur durch Registry-Hack

- Die niedrigste Einstellung ist auf Windows 2000-Standalone-Systemen die Standardeinstellungen
- Damit Windows 2000-Benutzer auf Ressourcen von XP zugreifen können, müssen die Ebenen übereinstimmen
- Höhere Ebenen können bei NT 4.0 ab SP4 und bei Windows 2000 nur i. d. Registrierung konfiguriert werden unter:

  HKLM|System|CCS|Control|LSA| MSV1_0
- Weiteres Siehe RK.



Praktischer Teil (immer paarweise)

1. Erstellung einer Freigabe auf beiden Rechnern, überprüfen des Zugriffs
2. Anhebung der NTLM-Authentifizierungsebene auf einem der Paartner-Rechner
3. Überprüfung des Zugriffs in beide Richtungen
4. Anhebung der NTLM-Authentifizierungsebene auf dem zweiten Rechner
5. Überprüfung des Zugriffs in beide Richtungen
6. Erklärung der Phänomene

Definition: Privilegien sind Benutzerrechte im System

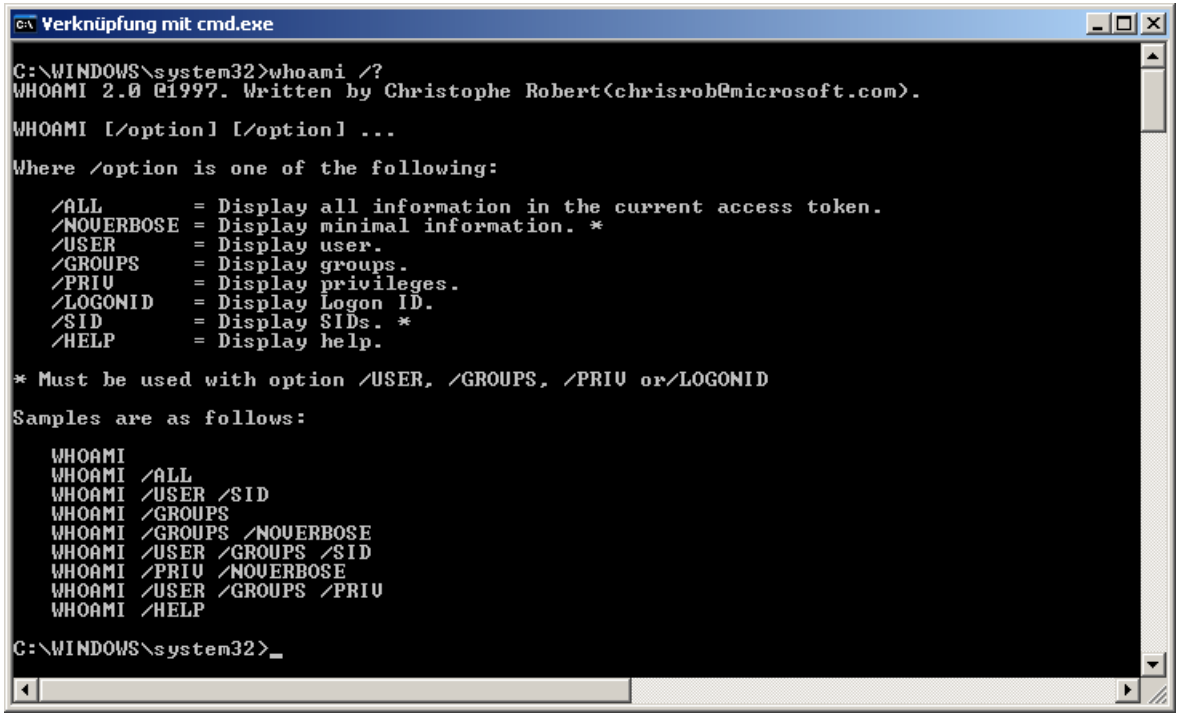
zu unterscheiden von NTFS- und AD-Zugriffsberechtigungen

Es gibt:

- Vordefinierte nicht veränderbare – gewissermaßen im System festverdrahtete – und nicht anzeigbare Zugriffsberechtigungen, die vordefinierten Konten (Administrator) und Gruppen (Administratoren, Hauptbenutzer etc.) zugewiesen sind
  - Beispiele: das Recht, die Festplatte zu formatieren; das Recht, Benutzerrechte zuzuweisen
- Veränderbare, d. h. von einem Administrator erteil- oder entziehbare Benutzerrechte
  - Das System vergibt per Default vordefinierten Benutzer- und Gruppenkonten bestimmte ‚Default'-Benutzerrechte
  - Beispiele: das Recht, sich lokal anzumelden; das Recht, die Systemzeit zu ändern

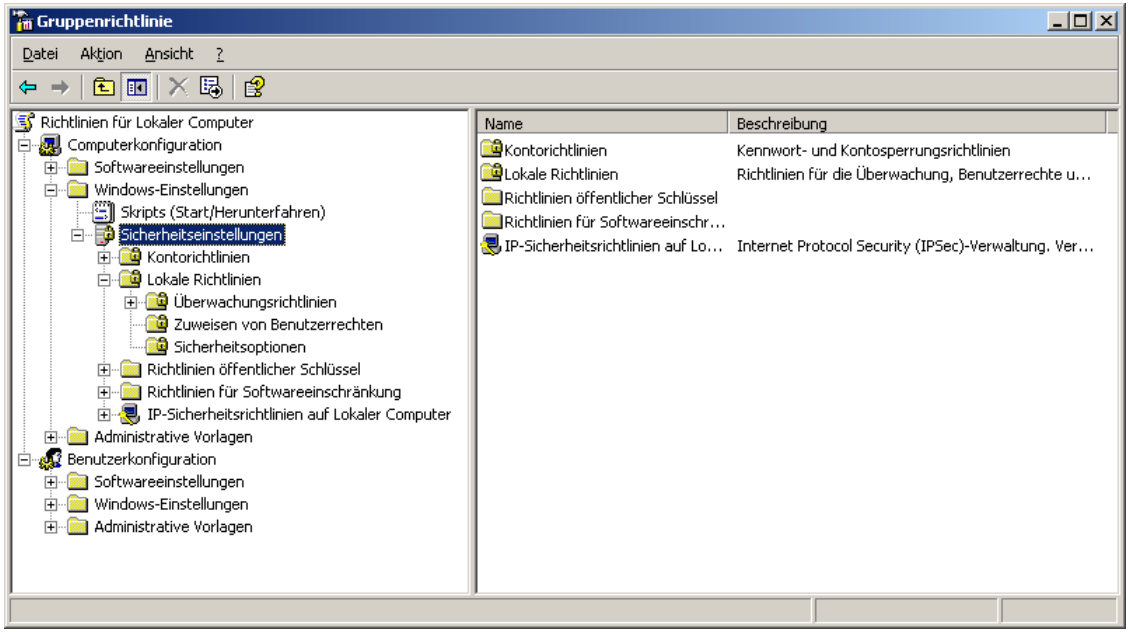
Ansicht von Privilegien

Kommandozeile mit dem Befehl ‚whoami /priv‘



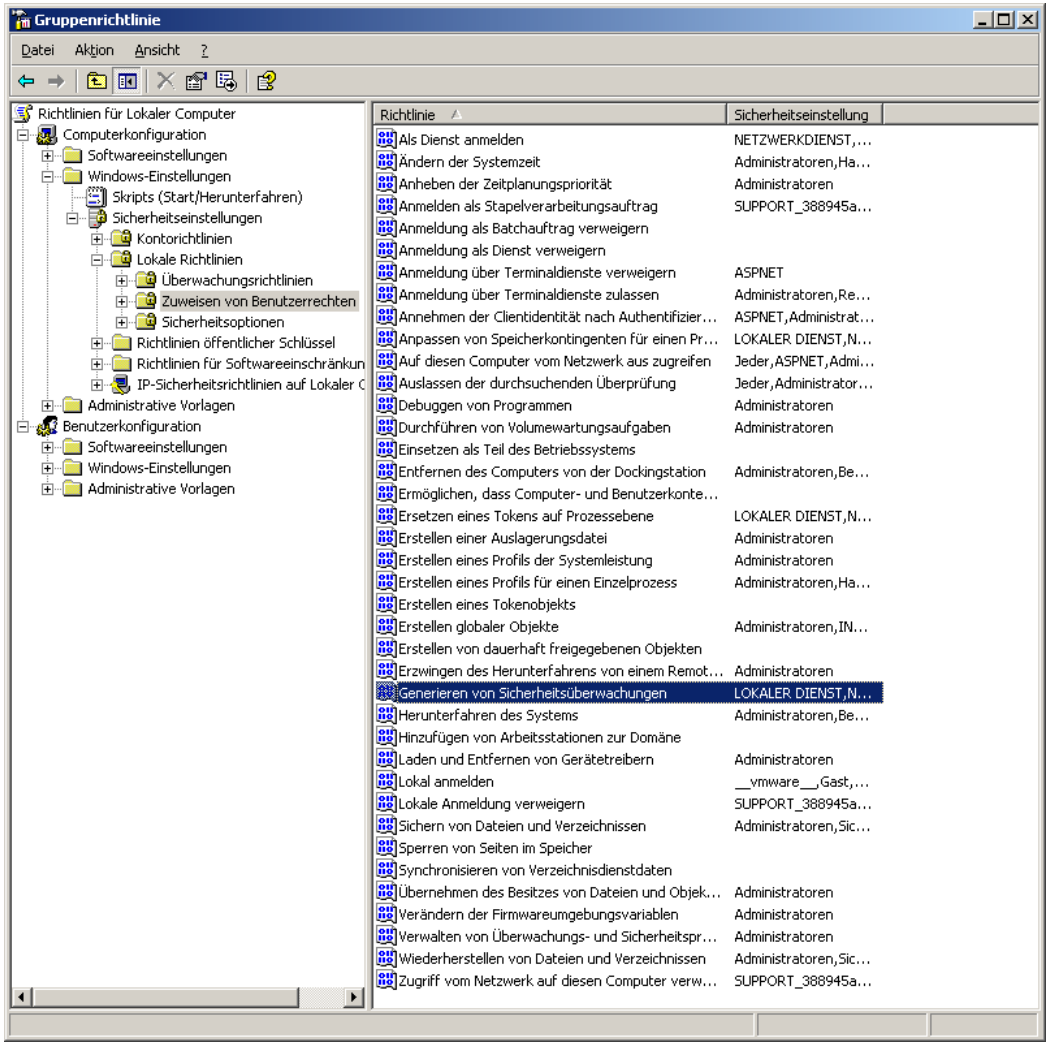
Ansicht und Konfiguration von Privilegien

Über den Gruppenrichtlinien-Editor mit dem Fokus ‚Lokale Sicherheitsrichtlinie‘:

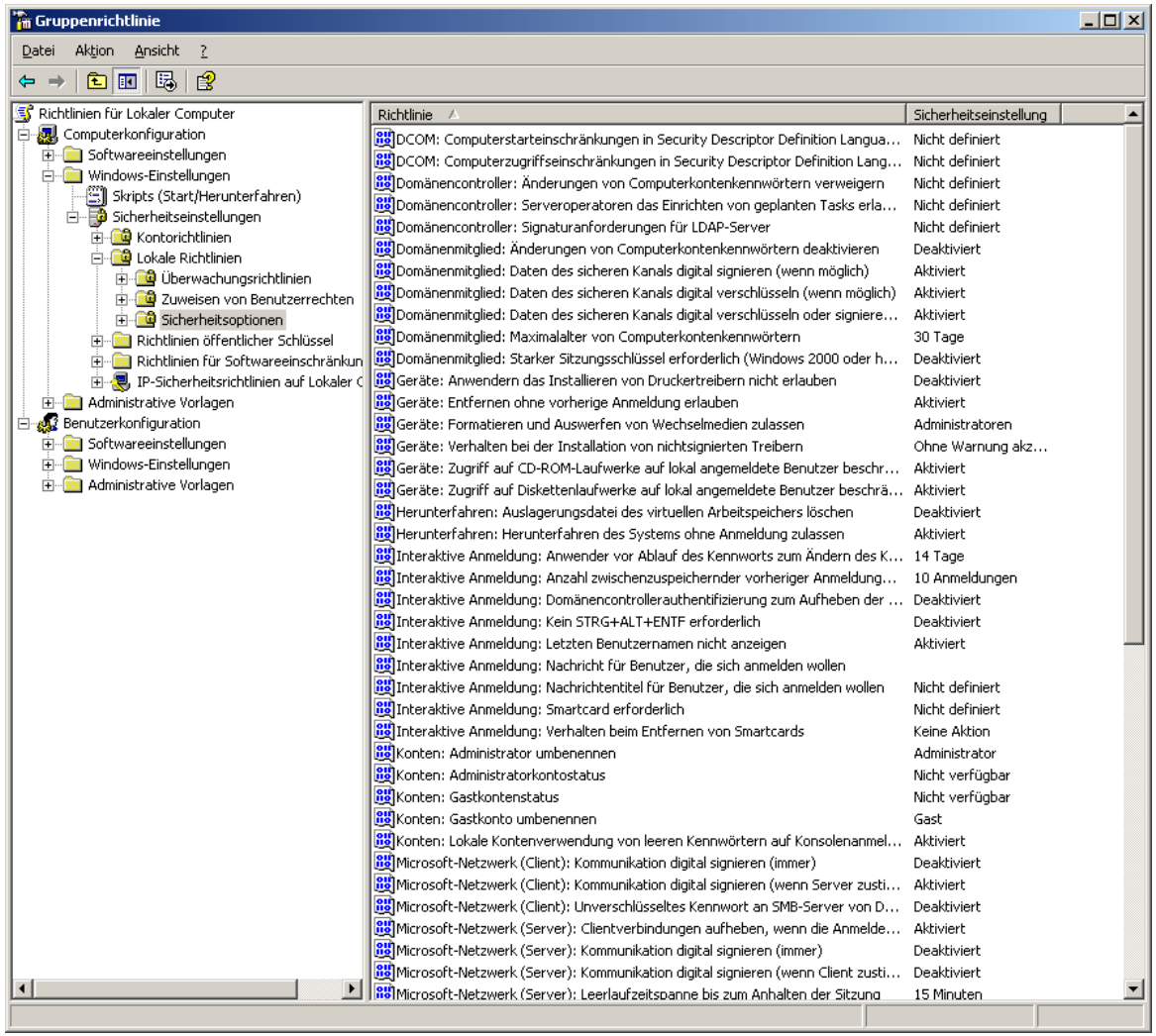


Ansicht und Konfiguration von Privilegien

Privilegien sind sichtbar unter dem Knoten ‚Zuweisen von Benutzerrechten‘:



Ansicht und Konfiguration von weiteren Sicherheitseinstellungen:



Das Problem

- Das Arbeiten als Administrator bzw. mit einem Account mit Administrator-Rechten unter Windows hat sich in vielen Firmen-Umgebungen und im privaten Bereich weitestgehend eingebürgert
- Windows XP z.B. versieht den ersten Benutzer-Account mit administrativen Rechten
  - Grund: Einem normalen Benutzer ist es nicht gestattet Software oder Treiber zu installieren oder die IP Adresse zu ändern – nicht einmal das Ändern der System-Zeit ist zulässig
- Im User-Alltag werden diese Funktionen sehr selten benötigt – für den Office-Einsatz und das Surfen im Internet sind keineswegs Administrator-Rechte erforderlich
- Gefahren der Arbeit mit administrativen Berechtigungen:
  - Alle Programme, die Sie starten, arbeiten unter dem mächtigsten Benutzer-Account
  - Diesen Programmen ist es gestattet auf Ihrem System beliebige Dateien zu lesen, hinzuzufügen oder zu löschen
  - Dies betrifft auch beliebige Registry-Schlüssel, Passwort-Dateien, System-Bibliotheken sowie Email und Internet Funktionalitäten

Die Lösung: Arbeiten mit einem gewöhnlichen Benutzer-Account über die sog. ‚sekundäre Anmeldung', i. e. der Befehl: ‚runas'

- Das Programm erfuhr bis zu Server 2003 eine immer bessere Integration von Anwendungen bis hin zum Internet Explorer.
- Syntax: Bei vielen MMC-Snap-Ins muss der Pfad mitgegeben werden:

  runas /user:K1\Administrator "mmc %systemroot%\system32\devmgmt.msc"

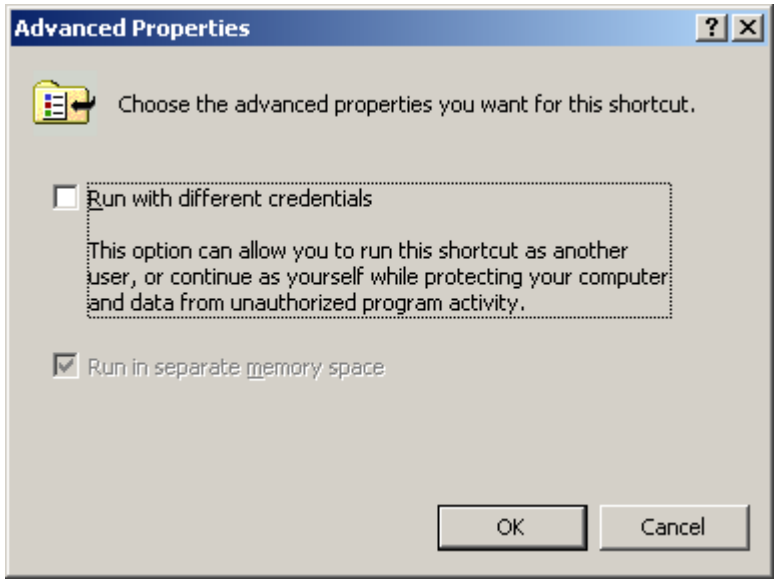
  …startet etwa den Gerätemanager auf dem Rechner K1 im Benutzerkontext des Administrators nach der Eingabe dessen Credentials.
- Anwendungsbeispiele

  Wärend der Administrator stets mit einem gewöhnlichen Benutzeraccount angemeldet ist, kann er administrative Aufgaben im Rahmen von *runas /user:* ausführen

  Der Browser kann in einem noch eingeschränkteren Sicherheitskontext ausgeführt werden

Das GUI


Run As
Which user account do you want to use to run this program?
Current user (HOME\dominick)
Run this program with restricted access
This option helps prevent programs from using administrator privileges to harm your computer. If you select this option, and the program relies on these privileges, it might behave improperly.
The following user:
User name:
Administrator
Password:
OK
Cancel


Advanced Properties
Choose the advanced properties you want for this shortcut.
Run with different credentials
This option can allow you to run this shortcut as another user, or continue as yourself while protecting your computer and data from unauthorized program activity.
Run in separate memory space
OK
Cancel

Praktischer Teil:

Den gewünschten Benutzer-Account anlegen.
Eine Gruppe „Trusted Users“ anlegen.
Den Benutzer-Account dieser Gruppe hinzufügen
Erstellen Sie sich ein Verzeichnis für Ihre privaten Dateien (z.B. d:\etc).
Erstellen sie dann unterhalb von etc ein Verzeichnis für Tools,
z.B. d:\etc\Tools.
Fügen Sie das „Tools“-Verzeichnis Ihrem Pfad hinzu
(Arbeitsplatz -> Rechte Maustaste -> Eigenschaften -> Erweitert -> Umgebungsvariablen)
Geben Sie der Gruppe ‚Trusted Users’ alle Rechte auf dieses Verzeichnis (und die Unterverzeichnisse) außer ‚Full Control’.
Erstellen Sie im „Tools“-Verzeichnis eine Batch-Datei mit Namen ‚su.cmd’ (Angelehnt an den Unix Befehl) mit folgendem Inhalt:

```
@runas /env /user:administrator "cmd.exe /k d:\etc\tools\admin.bat"
```

Erstellen Sie weiterhin eine admin.bat:

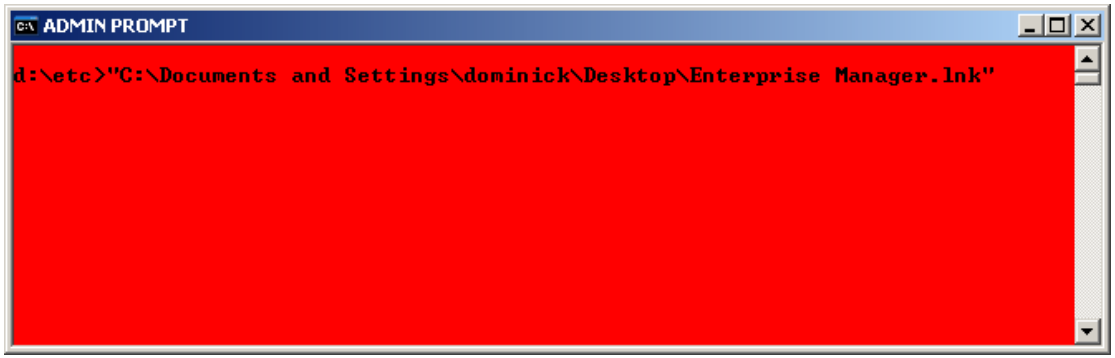
```
@cls
@title ADMIN Command Prompt
@color c0
```

Dies bewirkt, dass sie einen Command-Prompt öffnen und Ihr Admin-Passwort eingeben müssen. Danach läuft dieses Eingabe-Fenster als Administrator und sie können in diesem Fenster alle administrativen Tätigkeiten durchführen. Um konstant daran erinnert zu werden mit welchen Rechten dieses Fenster läuft, ist es rot eingefärbt und der Fenster-Titel wurde Dementsprechend modifiziert.

Arbeiten Sie gleichzeitig auch in einer Domain-Umgebung, können Sie runas so modifizieren, dass die Kommandozeile lokal als Administrator und in der Domäne als Benutzer gestartet wird. Modifizieren Sie dafür su.cmd folgendermaßen:

```
runas /u:administrator "runas /netonly /u:domain\user \"admin.bat\""
```

Das Ergebnis:



An welchen Stellen kann das Betriebsystem gehärtet werden?

- Durch den Einsatz importierbare .adm-Vorlagedateien
- Durch Gruppenrichtlinien
- Durch das Deaktivieren nicht benötigter Diensten
- Durch das Setzen von Registry-Parametern
- Durch das Setzen von Berechtigungen auf Registry-Schlüssel
- Durch das Setzen von NTFS-Berechtigungen

Überblick über die verschiedenen Installationsverfahren:

- Installation über 6 Setup-Disketten + CD-ROM
- Installation über Autostart der Installations-CD unter einem laufenden Windows
- Installation über ein bootfähiges CD-ROM-Laufwerk
- Installation über direkten Aufruf des Setup-Programms mit gewünschten Parametern (setzt eine beliebige laufende Windows-Version voraus): Winnt.exe /[Parameter], bzw. Winnt32.exe /[Parameter]
- Installation über eine Netzwerkfreigabe, auf der das \I386-Verzeichnis liegt (setzt Betriebssystem + Netzwerkclient auf Client voraus)
- Automatisierte Installation über Antwortdateien
- Automatisierte Installation mit Hilfe von RIS
- Installation mit Hilfe von /syspart
- Vorbereitung einer großflächigen Installation mit Sysprep

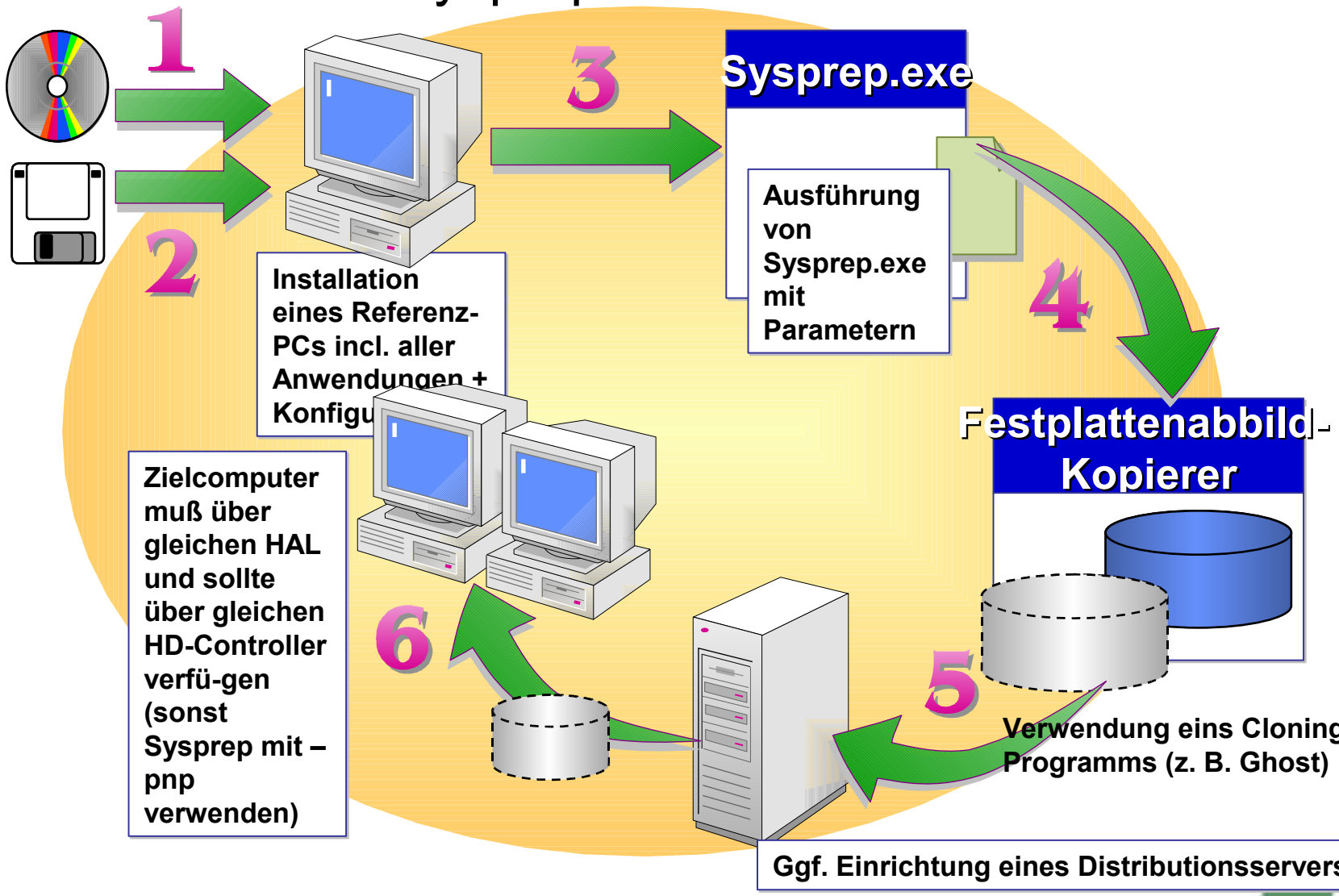
Windows kann nicht über Parameter oder direkt während der Installation gehärtet werden

deutlich weniger flexibel als die bei Unix-Systemen von vornherein festlegbaren Packages

Einzige Möglichkeit, ein schon gehärtetes Windows zu installieren besteht über manuell gehärtete Images über:

- Sysprep (alternativ dazu lässt sich auch newsid.exe von Sysinternals verwenden)
- RIS (Remote Installation Services)

Funktionsweise von Sysprep



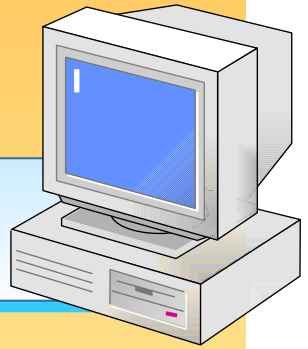
Funktionsweise von RIS

- Ein speziell konfigurierter RIS-Server verteilt Images von
  - Windows 2000 (Professional und Server)
  - Windows XP Professional
  - Windows Server 2003
- Es können nicht nur Images von Betriebssysteminstallation, sondern auch von Referenzrechnern, auf denen neben dem Betriebsystem noch Anwendungen installiert sein, verteilt werden
- RIS stellt neben einer bestehenden Active Directory-Infrastruktur, konfiguriertem DNS und DHCP noch folgende Anforderungen an RIS-Clients:

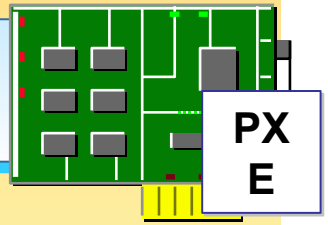
RIS-Client Voraussetzugen:

Clients für die Remoteinstallation müssen eine der folgenden Spezifikationen erfüllen

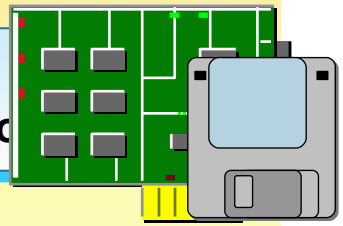
- Die Net PC-Spezifikation



- Einen Netzwerkadapter mit PXE



- Einen unterstützten Netzwerkadapter und eine Startdiskette für die Remoteinstallatio



Praktischer Teil

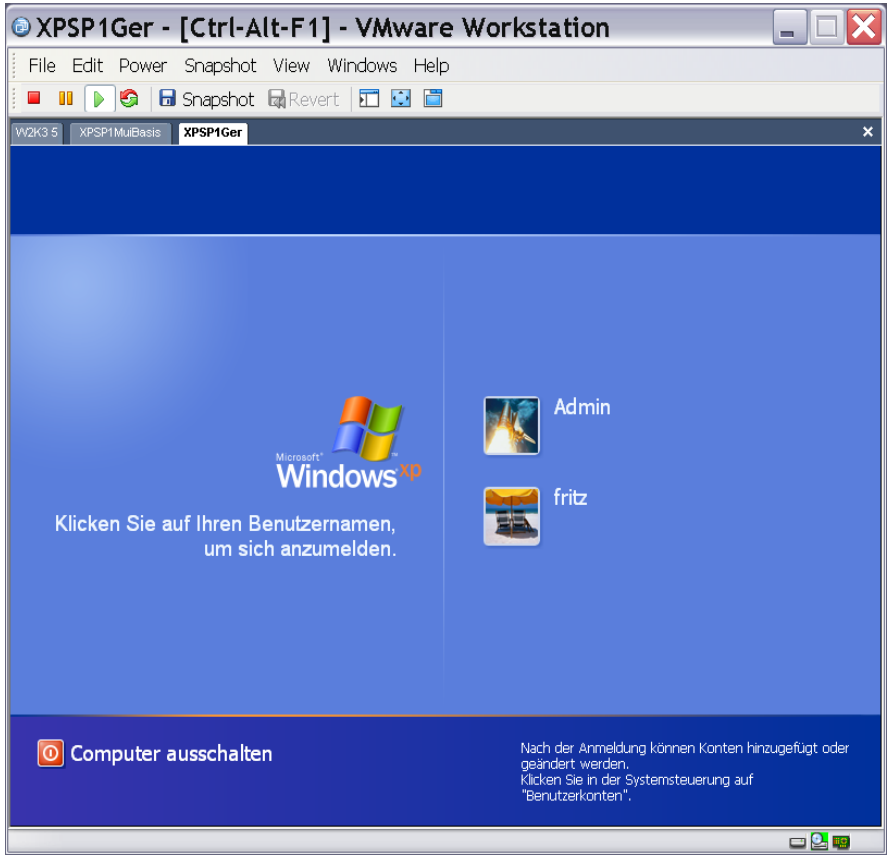
(Sollte nur an Rechnern durchgeführt werden, die nicht Mitglied einer Domäne sind):

1. Laden Sie newsid.exe von Sysinternals herunter
2. Geben Sie Ihrem Computer eine neue SID und einen neuen Namen unter der Verwendung von Newsid.exe; Sprechen Sie das Namensgebungsschema vorher mit dem Dozenten ab

Änderung der Standardbenutzeranmeldung

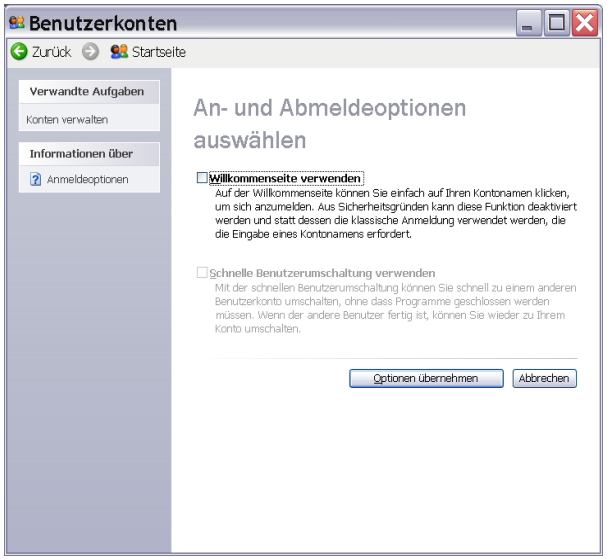
Es gibt die seit Windows NT bekannte klassische Benutzeranmeldung (Strg+Alt+Entf) und zusätzlich seit Windows XP die Anmeldung über die Willkommensseite. Die Anmeldung über die Willkommensseite ist die Standardanmeldung bei Windows XP, sie ist unsicherer.

Anmeldung über die Willkommensseite:



Änderung der Standardbenutzeranmeldung:

1. Aufruf von Benutzerkonten aus Systemsteuerung (nusrmgr.cpl)
2. *Willkommensseite verwenden* deaktivieren. Damit wird auch die schnelle Benutzerumschaltung deaktiviert. Für die schnelle Benutzerumschaltung gilt:
   1. Sie kann nicht zusammen mit der klassischen Anmeldung verwendet werden
   2. Sie kann nicht zusammen mit Offline-Dateien verwendet werden

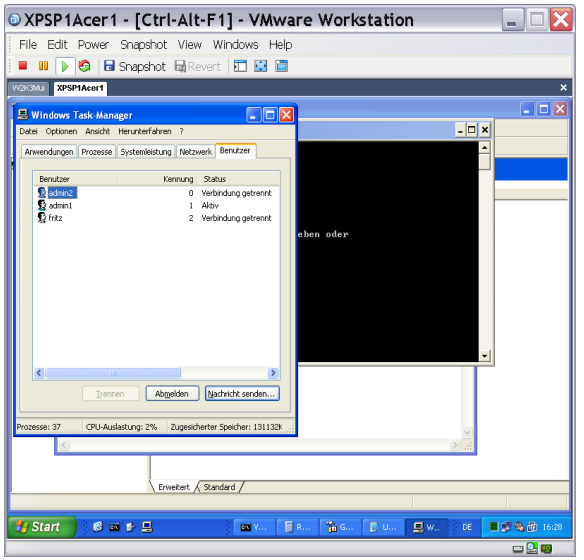


... Noch zur schnellen Benutzerumschaltung:

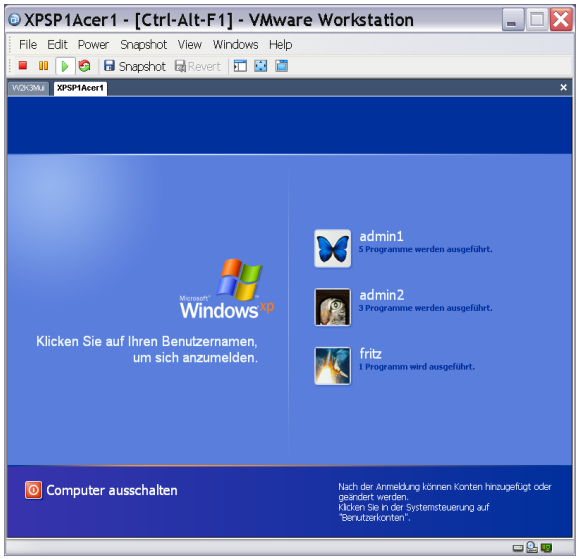
- Die schnelle Benutzerumschaltung ist in Windows XP Home und Professional verfügbar
- Die schnelle Benutzerumschaltung kann nicht aktiviert werden, wenn Windows XP (Prof.) Mitglied einer Domäne ist
- Wenn die schnelle Benutzerumschaltung aktiviert ist, steht im Taskmananger eine eigene Registerkarte *Benutzer* zur Verfügung in der die angemeldeten Benutzer und ihre Sitzungen eingesehen und von Mitgliedern der Gruppe Administratoren manipuliert werden können
- Ist die schnelle Benutzerumschaltung deaktiviert und ein Benutzer meldet sich ab, dann werden – anders als bei der schnellen Benutzerumschaltung – die laufenden Programme beendet
- Das Hochfahren des Systems – nicht der Anmelde- und Abmeldeprozeß – erfolgt schneller, wenn die schnelle Benutzerumschaltung deaktiviert ist
- Nur Mitglieder der Gruppe Administratoren können die schnelle Benutzerumschaltung (nusrmgr.cpl) aktivieren /deaktivieren

Absichern der Anmeldung

Taskmanager-Ansicht bei aktivierter schneller Benutzerumschaltung: nur Mitglieder der Gruppe Administratoren können parallel laufenden Sitzungen sehen und beenden

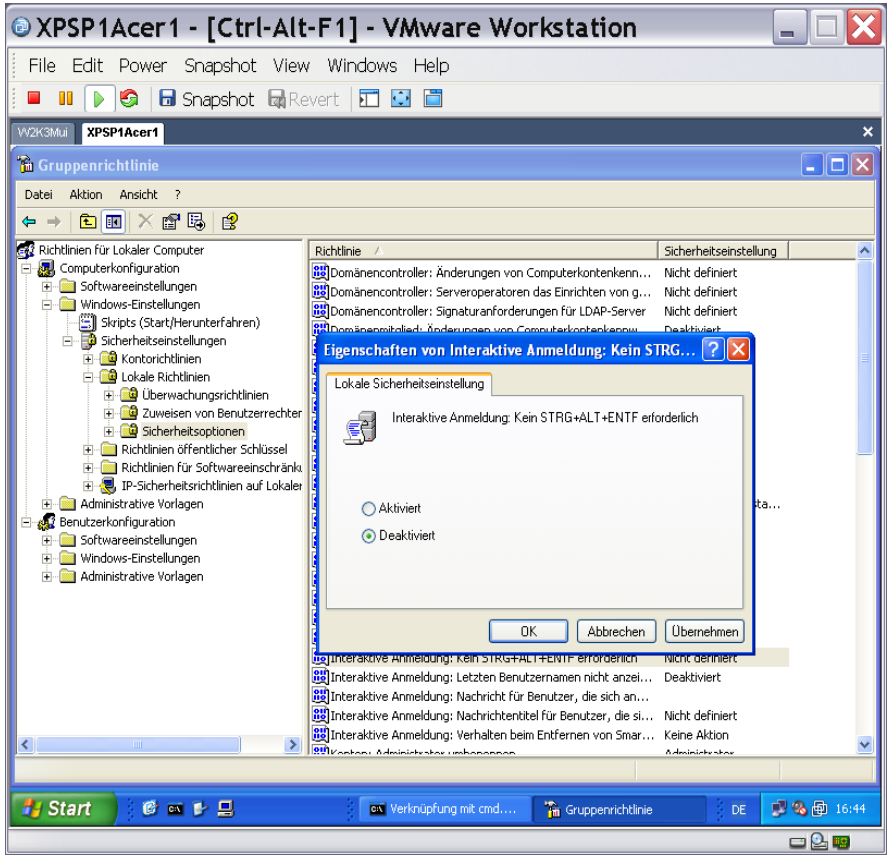


Anmeldebildschirm bei aktivierter schneller Benutzerumschaltung

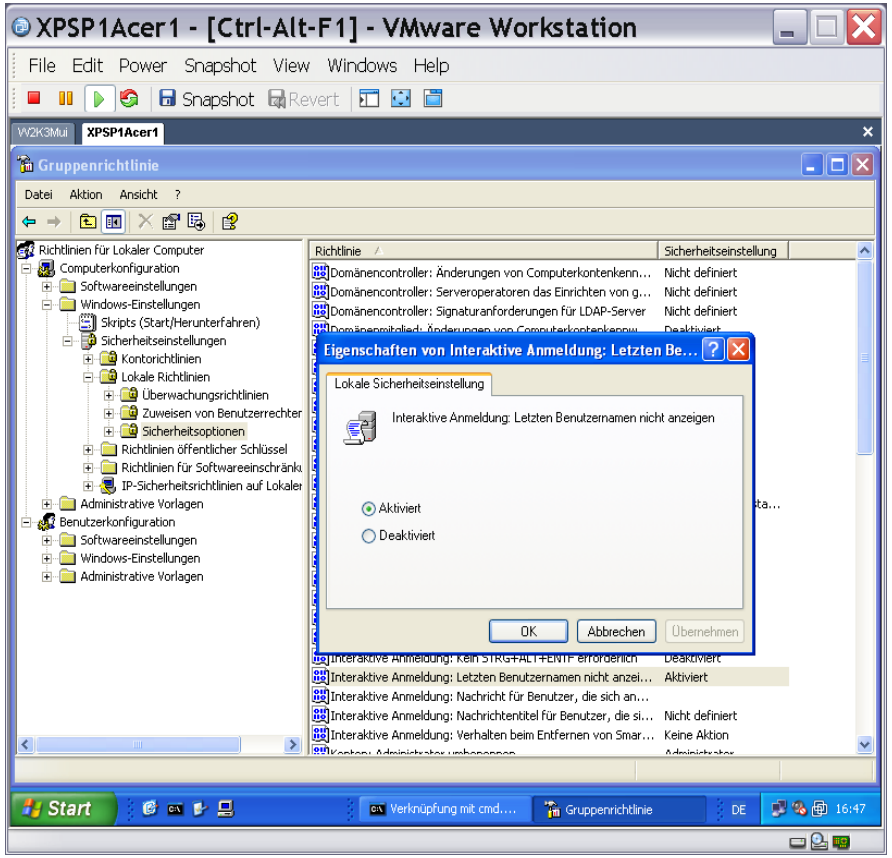


Absicherung der klassischen Benutzeranmeldung:

1. *Willkommensseite verwenden* deaktivieren
2. Damit ist aber noch keine Anmeldung über Strg+Alt+Entf ermöglicht und außerdem wird auch noch der Name des zuletzt angemeldeten Benutzers angezeigt
3. Anmeldung über Strg+Alt+Entf als Eintrag in einem GPO setzen



5. Zuletzt angemeldeten Benutzernamen nicht anzeigen
6. Konfigurieren einer Warnmeldung



Praktischer Teil

1. Stellen Sie von der schnellen auf die klassische Benutzer-Anmeldung um
2. Konfigurieren Sie die Erfordernis von Strg+Alt+Entf
3. Konfigurieren Sie eine Nachricht für Benutzer, die sich am System anmelden
4. Verhindern Sie das Anzeigen des Benutzernamens der letzten Anmeldung

Organisationen, die Sicherheitsvorlagen frei zur Verfügung stellen:

- **Microsoft Corporation**

  Per Default mit jeder Installation ausgelieferte Vorlagen

  Microsoft gibt Empfehlungen zum Schutz der von Microsoft entwickelten Betriebssysteme. Zu diesem Zweck verwendet Microsoft die drei folgenden Sicherheitsstufen :

  Ältere Systeme

  Unternehmen

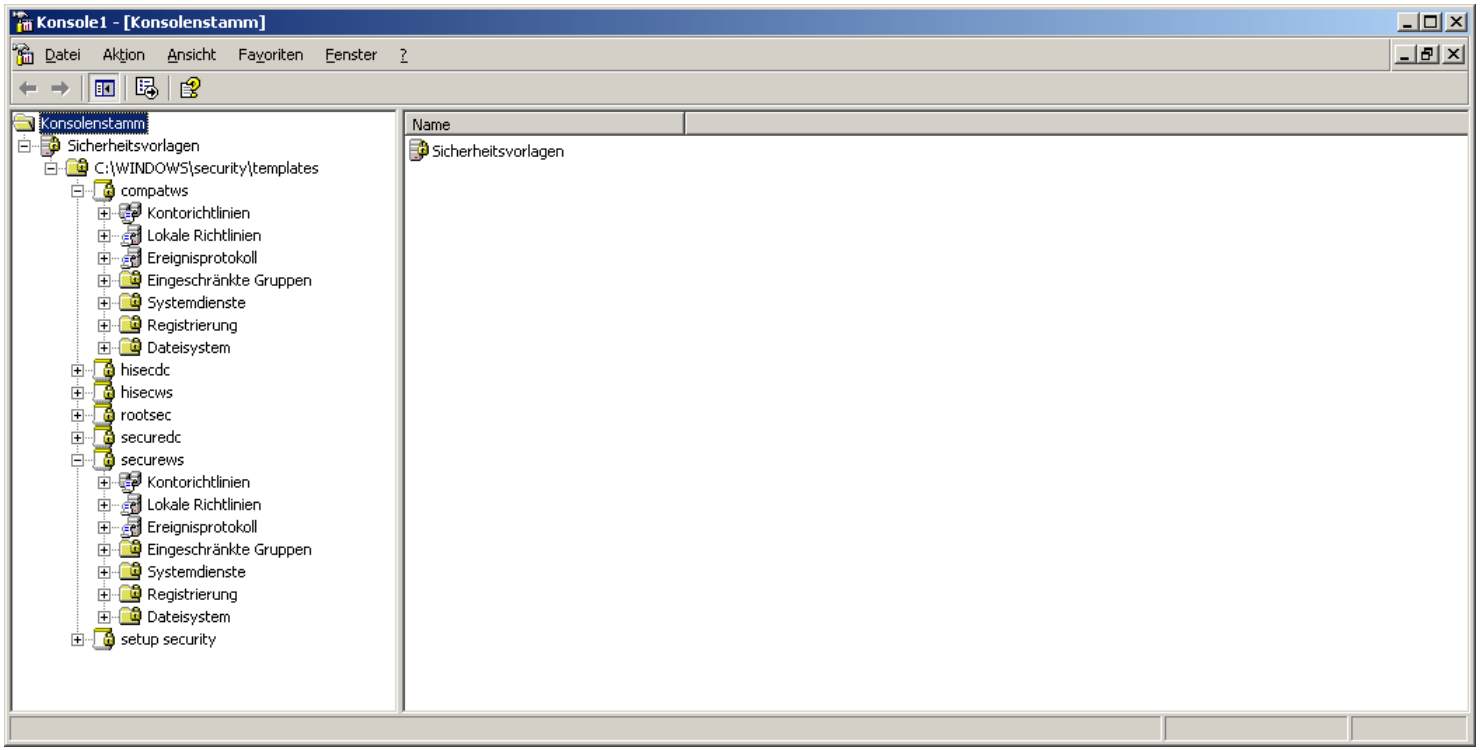
  Hohe Sicherheit

  Diese Sicherheitsstufen wurden für viele verschiedene Kundenszenarios ausführlich getestet. Sie sind für alle Organisationen geeignet, die vorhandene Windows-Computer schützen möchten.

  Werden mit dem Sicherheitshandbuch für Windows XP ausgeliefert

(Importierbare) Vorlagen

- Mit jeder XP-Installation ausgelieferte Vorlagen:



Center for Internet Security (CIS)

- Das Center for Internet Security (Zentrum für Internetsicherheit) hat Benchmarks zum Sammeln von Informationen entwickelt, anhand derer Organisationen fundierte Entscheidungen über die verfügbaren Sicherheitsoptionen treffen können. Das CIS hat drei von Sicherheits-Stufen entwickelt (die sich stark an Microsoft orientieren):
  - Ältere Systeme
  - Unternehmen
  - Hohe Sicherheit

National Institute of Standards and Technology (NIST)

- Das National Institute of Standards and Technology (Nationales Institut für Standardisierung und Technologie) ist für die Erarbeitung von Sicherheitsempfehlungen für die Regierung der Vereinigten Staaten von Amerika zuständig. Das NIST hat vier Sicherheitsstufen entwickelt, die von den Bundesbehörden der Vereinigten Staaten sowie von privaten und öffentlichen Organisationen verwendet werden:
  - SoHo (Small Office/Home Office)
  - Ältere Systeme
  - Unternehmen
  - Spezielle Sicherheit mit eingeschränkter Funktionalität (Vorlage sollte ausführlich getestet werden)

…Security Guides werden zur Verfügung gestellt von:

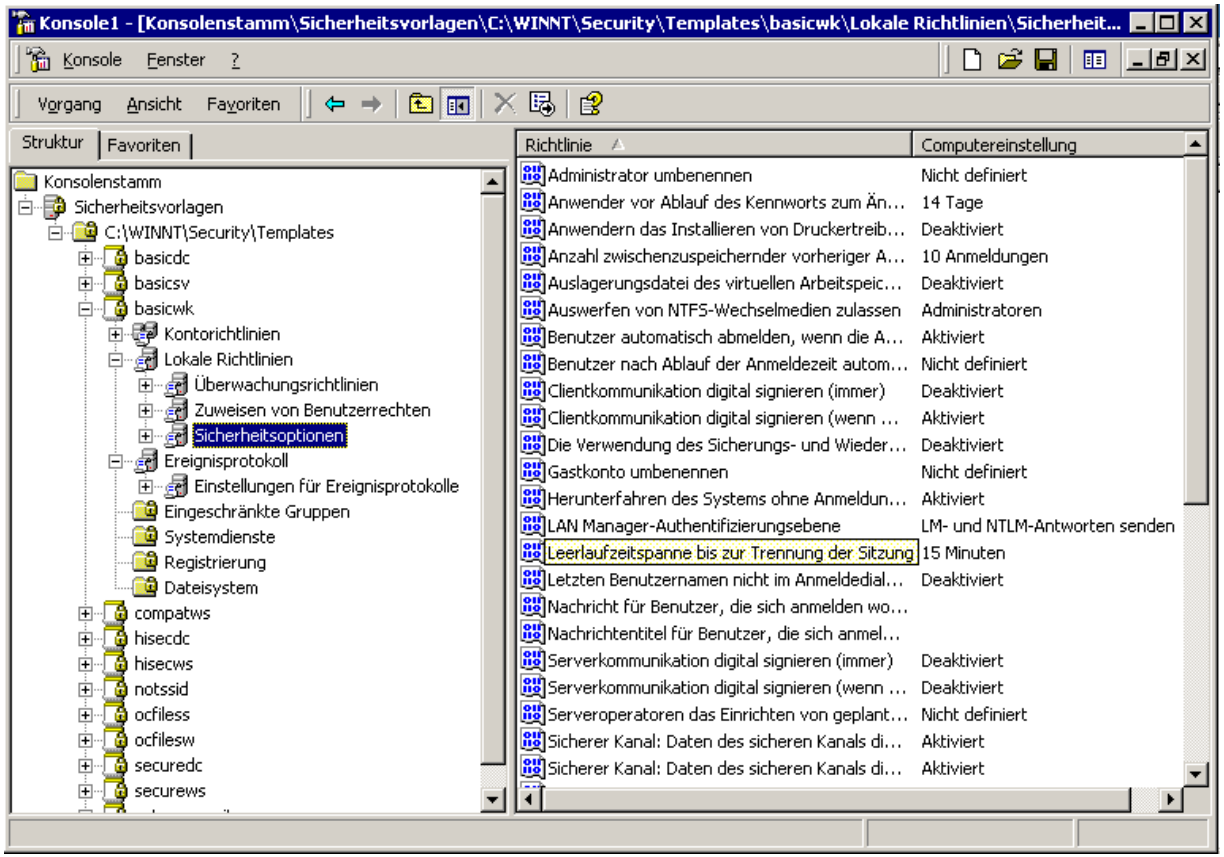
- Defense Information Systems Agency (DISA)

  Die Defense Information Systems Agency (Behörde für die Sicherheit von Informationssystemen im Verteidungssektor) erarbeitet Sicherheitsempfehlungen für das Verteidigungsministerium der USA

- National Security Agency (NSA)

  Die National Security Agency (Nationale Sicherheitsbehörde) entwickelt Sicherheitsempfehlungen zum Schutz von hochgefährdeten Computern im Verteidigungsministerium der USA. Sie hat eine Sicherheitsstufe erarbeitet, die in etwa mit der Sicherheitsstufe "Hoch" anderer Organisationen vergleichbar ist.

Sicherheitsvorlagen können mit dem Snap-In *Sicherheitsvorlagen* erstellt und bearbeitet werden:



Anwenden von Sicherheitsvorlagen

- Sicherheitsvorlagen können importiert und angewendet werden
  - In die lokale Sicherheitsrichtlinie
  - In Active Directory Gruppenrichtlinienobjekten
  - Mit dem Tool „Sicherheitskonfiguration und –analyse entweder über die grafische Oberfläche oder an der Eingabeaufforderung

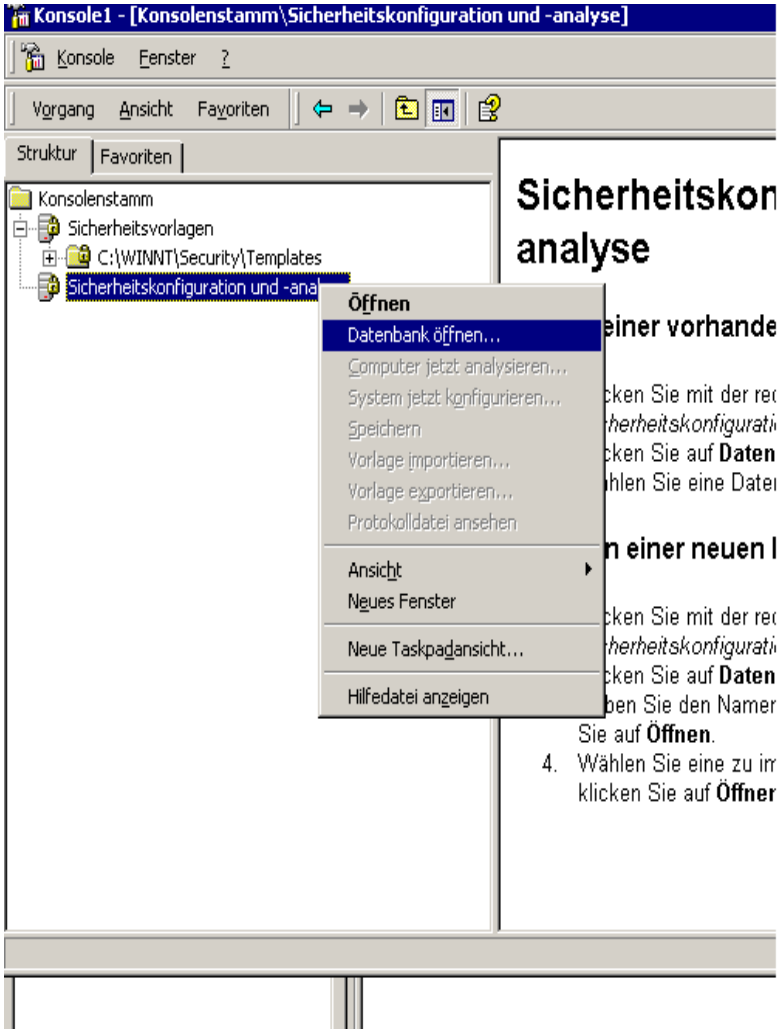
Grundsätzlich sollten Sicherheitsvorlagen auf nicht produktiven Systemen getestet werden, bevor sie ausgerollt werden

Das Snap-In *Sicherheitskonfiguration- und Analyse*

- Zum Nachvollziehen von Änderungen nutzt der Administrator das Tool „sicherheitskonfiguration und –analyse
- Die Sicherheitseinstellungen werden gegen eine Datenbank geprüft

  Datenbank (.*sdb*) und Logdatei werden im Benutzerprofil gespeichert
- Sicherheitsvorlagen können kumulativ importiert werden
- Änderungen werden hervorgehoben dargestellt
- Mit demselben Tool kann die Sicherheitskonfiguration erneut implementiert werden

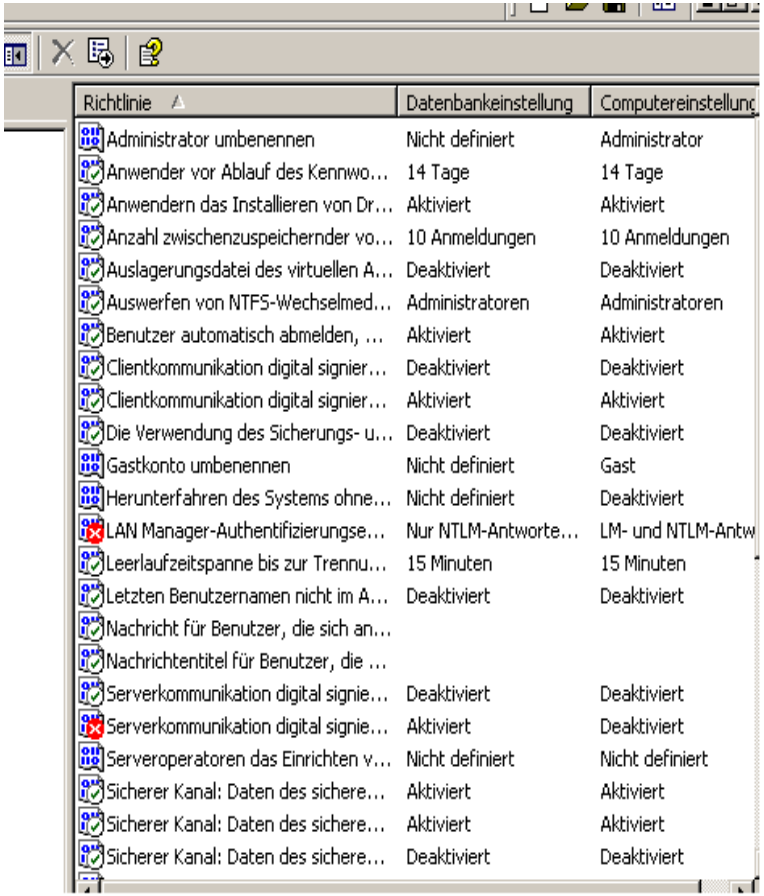
Sicherheitskonfiguration- und Analyse



Beim Ausführen der Sicherheitskonfiguration und –analyse sind folgende Angaben notwendig:

- Name der Datenbank (neuer Name erstellt neue DB)
- Name der Logdatei
- Name einer Vorlagendatei

Sicherheitskonfiguration- und Analyse



Richtlinie	Datenbankeinstellung	Computereinstellung
Administrator umbenennen	Nicht definiert	Administrator
Anwender vor Ablauf des Kennwo...	14 Tage	14 Tage
Anwendern das Installieren von Dr...	Aktiviert	Aktiviert
Anzahl zwischenzuspeichernder vo...	10 Anmeldungen	10 Anmeldungen
Auslagerungsdatei des virtuellen A...	Deaktiviert	Deaktiviert
Auswerfen von NTFS-Wechselmed...	Administratoren	Administratoren
Benutzer automatisch abmelden, ...	Aktiviert	Aktiviert
Clientkommunikation digital signier...	Deaktiviert	Deaktiviert
Clientkommunikation digital signier...	Aktiviert	Aktiviert
Die Verwendung des Sicherungs- u...	Deaktiviert	Deaktiviert
Gastkonto umbenennen	Nicht definiert	Gast
Herunterfahren des Systems ohne...	Nicht definiert	Deaktiviert
LAN Manager-Authentifizierungse...	Nur NTLM-Antworte...	LM- und NTLM-Antw
Leerlaufzeitspanne bis zur Trennu...	15 Minuten	15 Minuten
Letzten Benutzernamen nicht im A...	Deaktiviert	Deaktiviert
Nachricht für Benutzer, die sich an...		
Nachrichtentitel für Benutzer, die ...		
Serverkommunikation digital signie...	Deaktiviert	Deaktiviert
Serverkommunikation digital signie...	Aktiviert	Deaktiviert
Serveroperatoren das Einrichten v...	Nicht definiert	Nicht definiert
Sicherer Kanal: Daten des sichere...	Aktiviert	Aktiviert
Sicherer Kanal: Daten des sichere...	Aktiviert	Aktiviert
Sicherer Kanal: Daten des sichere...	Deaktiviert	Deaktiviert

Abweichungen von den Datenbankeinstellungen sind hervorgehoben

Sicherheitskonfiguration- und Analyse

- Zur Automatisierung – z.B. in Batchdateien – kann secedit.exe verwendet werden
- Syntax:
  `secedit /configure [/DB` *`Dateiname`* `] [/CFG` *`Dateiname`* `] [/overwrite][/areas` *`Bereich1 Bereich2...`*`] [/log` *`Protokollpfad`*`] [/verbose] [/quiet]`
- Die Auswertung der Protokolldatenbank erfolgt dann über die GUI

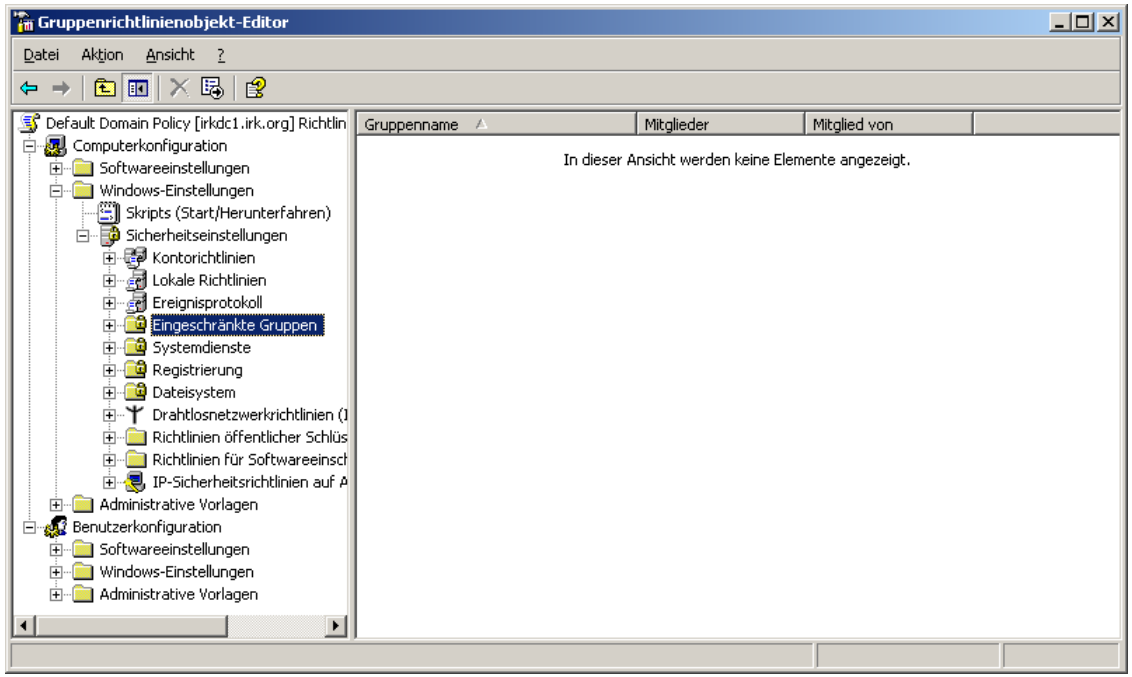
Praktischer Teil:

- Siehe Word-Dokument

Richtlinien

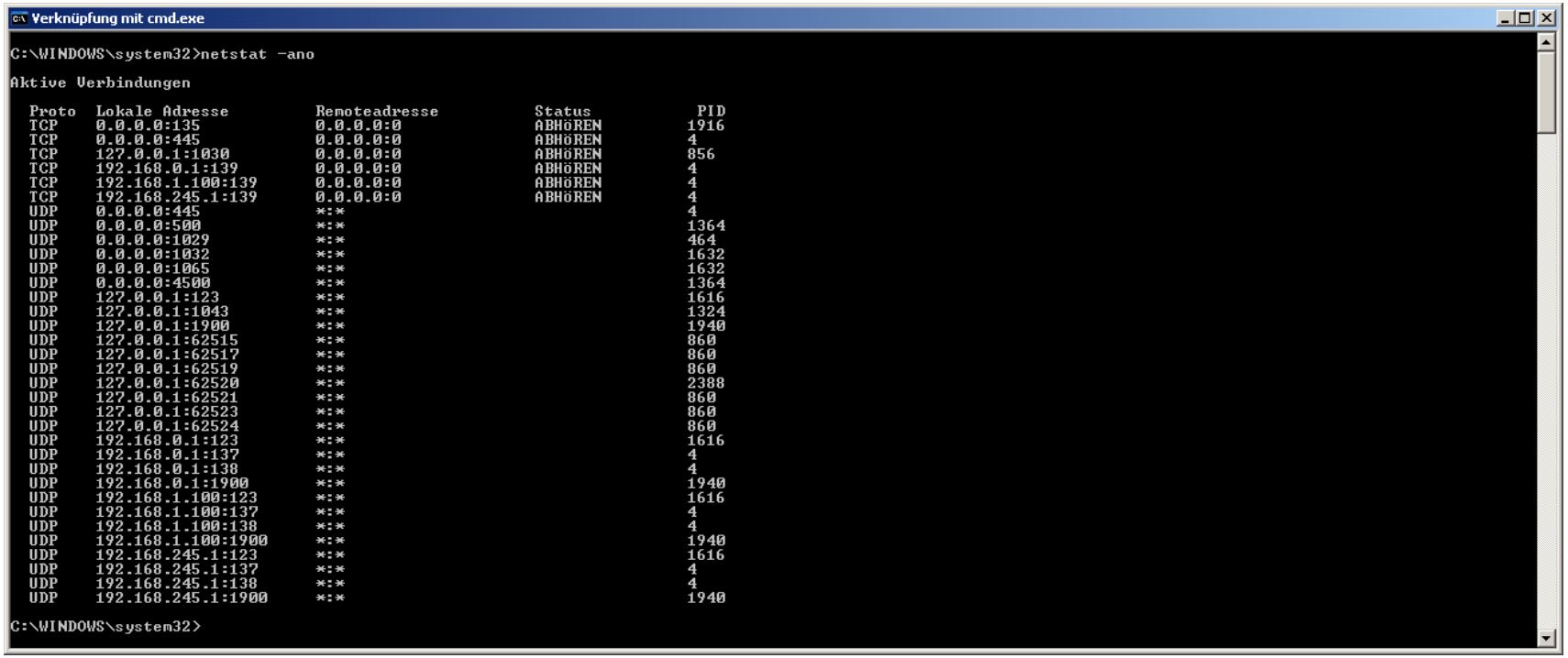
- Auf Workstations max. einen administrativen Account
- Ggf. Administrator- und Gast-Konto umbenennen
  - Möglich in den Sicherheitseinstellungen
  - Verhindert nicht das Identifizieren dieser Konten über die SID (nur mit professionellen Tools möglich)
- Gewöhnliche Benutzer nur zum Mitglied der Gruppe ‚Benutzer' machen
- Sich vor dem Kauf neuer Software informieren, ob diese für Windows XP SP2 (und Server 2003) designed ist
- Verwendung von Hauptbenutzern möglichst vermeiden
  - Falls Anwendungen unter dem Benutzer-Konto nicht laufen, zunächst Anwendungskompatibilitäts-Modus verwenden (und nicht die Gruppe Hauptbenutzer)

Mitgliedschaft in Sicherheits-relevanten Gruppen kann in AD-Umgebungen einfach per GPO gesteuert werden:



Identifizierung von Diensten auf einem System

- Eine Möglichkeit: ‚netstat –ano‘ (auf Windows XP und Server 2003 verfügbar)

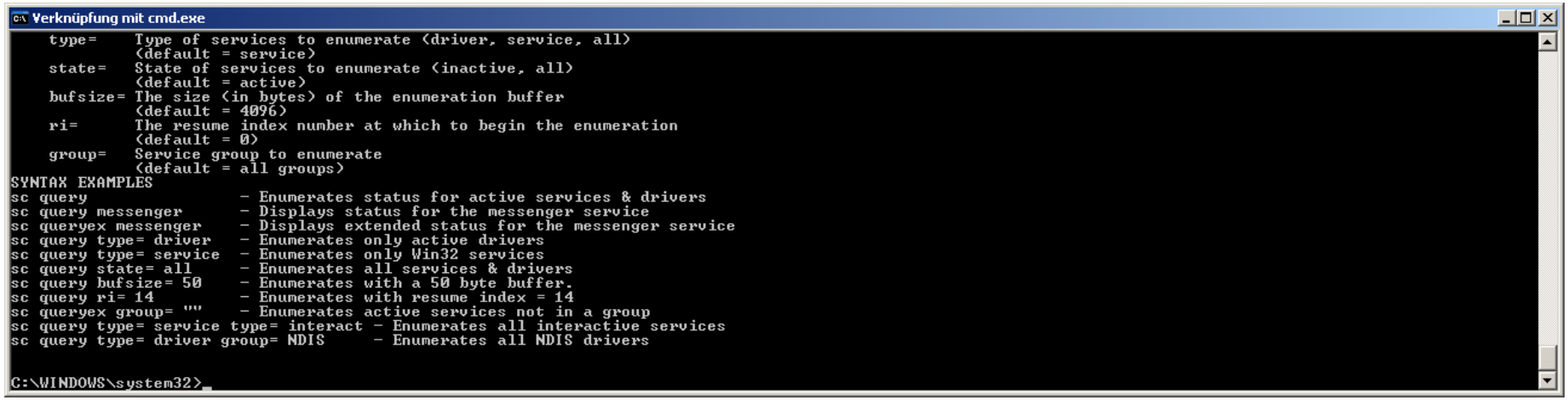


Identifizierung von Diensten auf einem System

- Bessere Möglichkeit: ‚netstat –**b**ano‘ (auf Windows XP SP2 und Server 2003 verfügbar)

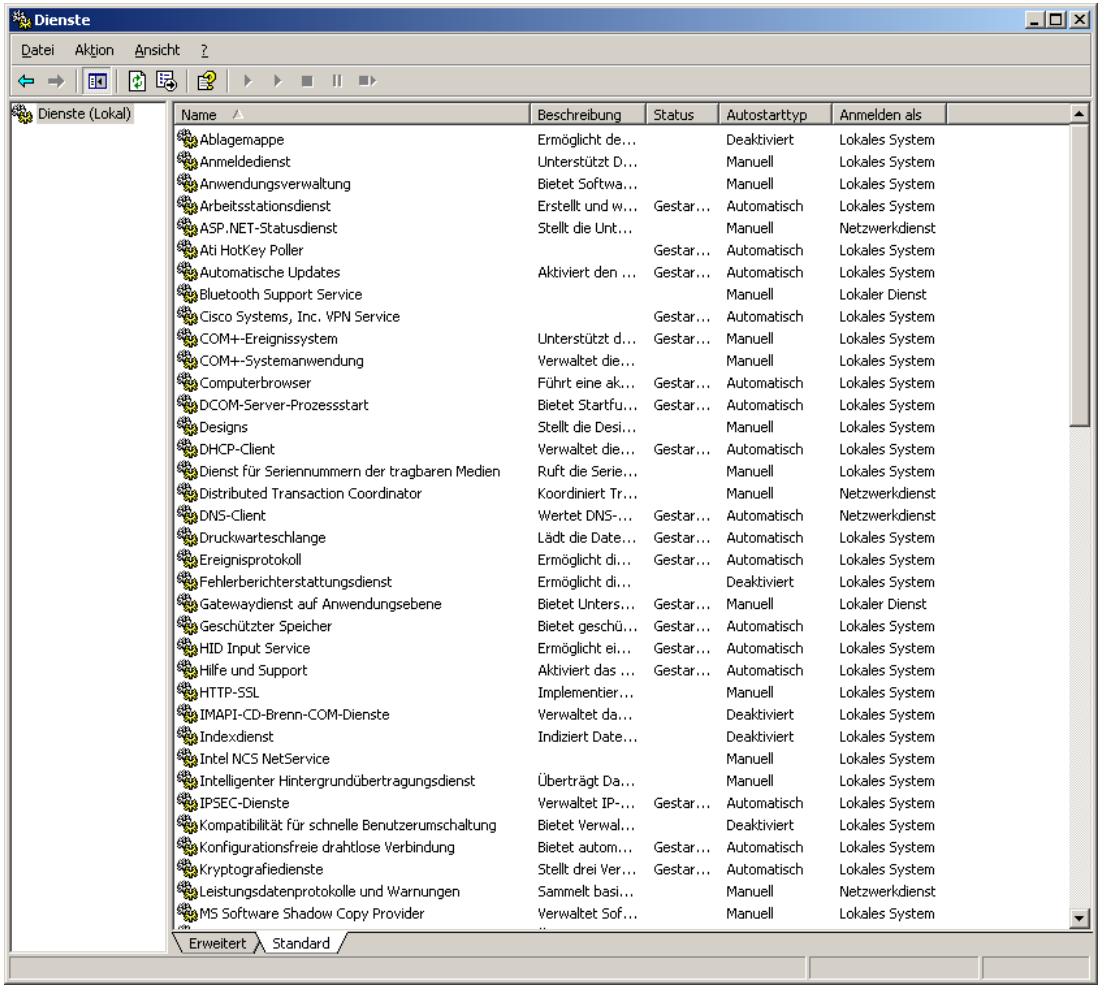
  Listet Dienste und von diesen geladene Dlls auf

- Weitere Möglichkeit: ‚sc query‘:



Identifizierung von Diensten auf einem System

- Über das GUI: ‚services.msc‘



Die Default-Einstellungen entnimmt man:

Windows Default Security and Services Configuration.xls aus dem Windows Security Guide

Dienste, die problemlos in Windows XP deaktiviert werden können:

- Ablagemappe
- Bluetooth Support Service (wenn Bluetooth nicht verwendet wird)
- Designs
- Distributed Transaction Coordinator
- Fehlerberichterstattungsdiestn
- Ggf. HID Input Service
- Imapi-CD-Brenn-Com-Dienste
- Routing und RAS (wenn keine RAS-Funktionalität verwendet wird)
- Sitzungsmanager für Remotedesktop-Hilfe (wenn diese nicht verwendet wird)
- Smartcard (wenn keine Smartcard verwendet wird)
- Telnet

Achtung bei folgenden Diensten:

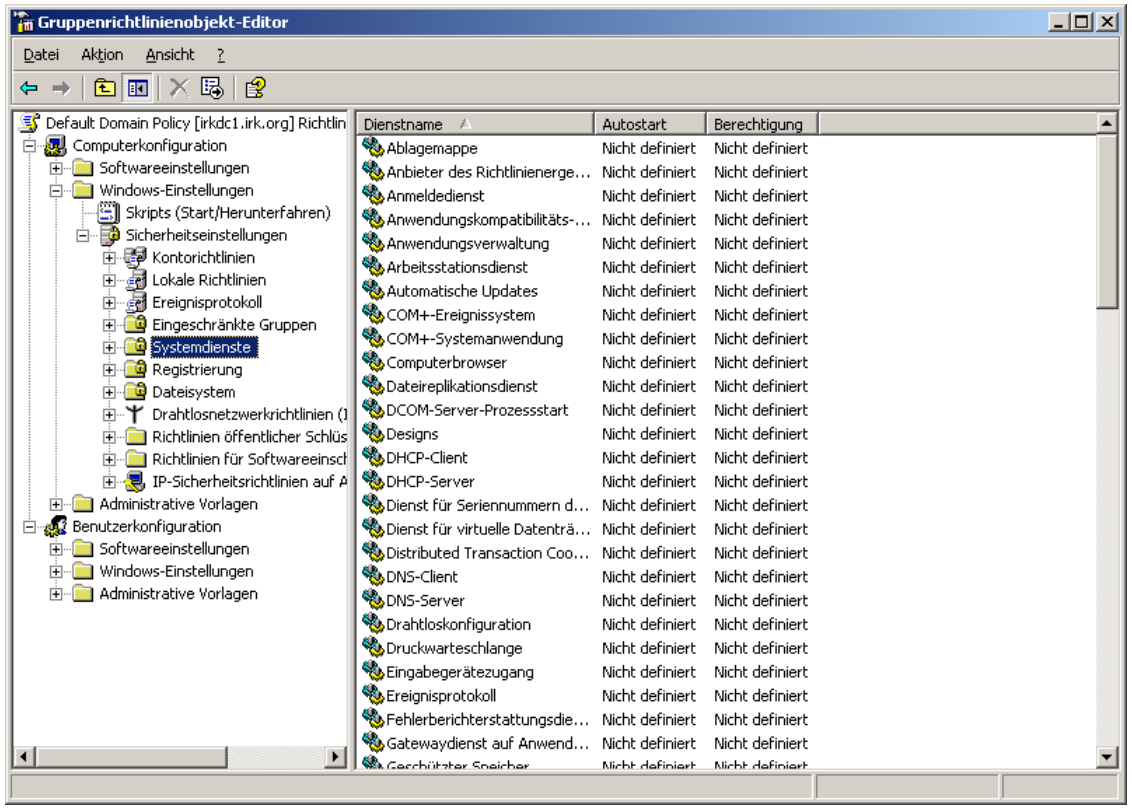
Arbeitsstationsdienst: Verantwortlich für das Zugreifen auf (SMB-) Freigaben

Server: Verantwortlich für das Erstellen und Freigeben von (SMB-) Freigaben

Computerbrowser: Verantwortlich für das Auflösen von NetBIOS-Namen in nicht-WINS-Umgebungen; wird u. a. von Office 2000 benötigt

Remote Registrierung: ermöglicht den remoten Zugriff auf Registry-Hives; wenn der Dienst deaktiviert wird, funktionieren einige MMC-Snap Ins nicht mehr remote (z. B. der Gerätemanager)

Dienstekonfiguration ist über GPO-Einstellungen in AD-Umgebungen deutlich besser zu verwalten:



Praktischer Teil

- Siehe ausgeteiltes Word-Dokument

Es gibt eine Reihe von sog. Registry-Hacks, mit denen Bereiche abgedeckt werden können, die (noch) nicht durch GPOs behandelt werden

- Sinnvolle Literatur dazu:

  Bedrohungen und Gegenmassnahmen – Sicherheitseinstellungen unter Windows Server 2003 und Windows XP (downloadbar auf den Technetseiten von Microsoft)

  Preston Gralla: *Windows XP Hacks, 2nd. Edition*, O'Reilly (2005)

Beispiel für sinnvollen guten Registriy-Hack

- Verhinderung des Schreibens auf USB-Sticks (von WinTotal-Webseite)

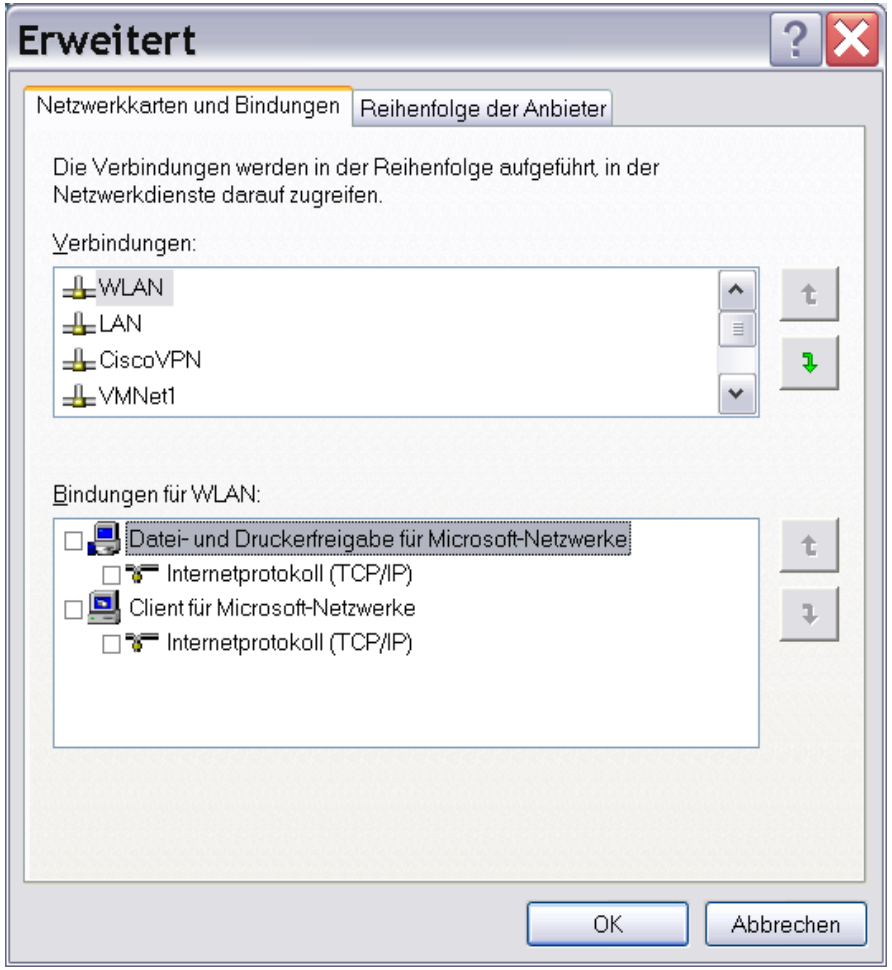
  Dazu muss ein neuer Eintrag angelegt werden unter:

  HKEY_LOCAL_MACHINE\System\ CurrentControlSet\ Control\ StorageDevicePolicies
  Name: **WriteProtect**
  Typ: DWord-Wert
  Wert **0** = Schreibschutz ist deaktiviert
  Wert 1 = Schreibschutz ist aktiviert

  Ergebnis:

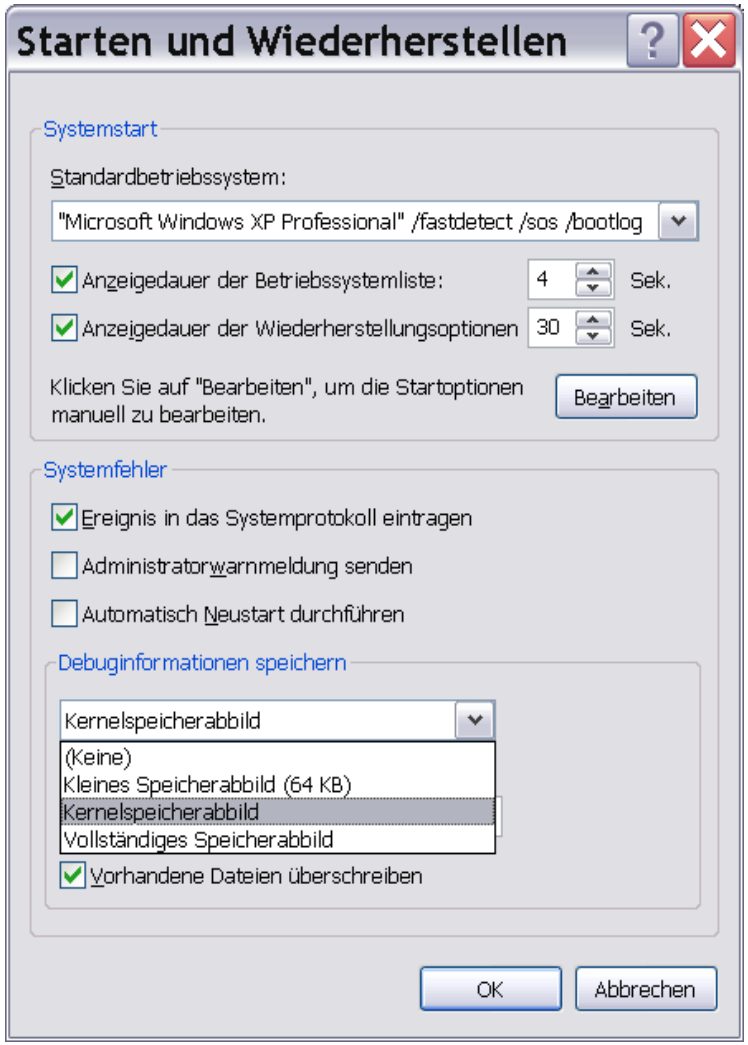
Anpassen der Bindungen zwischen NIC, Protokoll und Netzwerkdienst für verschiedene Adapter in ncpa.cpl| Erweitert|Erweiterte Einstellungen:

- Unterschiedliche Sicherheitslevels für WLAN, LAN und VPN
- Außer im LAN ggf. Client für Microsoft-Netzwerke nicht an den Adapter binden



Anpassung der Startoptionen:

- Per Hand: Hinzufügen der Parameter /sos /bootlog in Boot.ini und Anpassen der Anzeige von OS-Auswahl im Bootmenü und per default zu bootendes OS
- In den Systemeigenschaften:
  - Systemfehler
  - Debuginformationen:
    - Kleines Speicherabbild
    - Kernelspeicherabbild ca. 50-800 MB
    - Vollst. Speicherabbild (pagefile mind. RAM+1MB)
  - Supptools-Tool: *Dumpchk.exe*



Kleines Absturz-Speicherabbild mit *dumpchk.exe* betrachtet:

Verknüpfung mit cmd.exe

```
DebuggerDataSize      00000290
DataBlocksOffset      000073b0
DataBlocksCount       00000003


Windows XP Kernel Version 2600 (Service Pack 1) UP Free x86 compatible
Built by: 2600.xpsp2.030422-1633
Kernel base = 0x804d4000 PsLoadedModuleList = 0x80543530
Debug session time: Fri Jan 23 13:38:48 2004
System Uptime: 0 days 4:01:01
start    end        module name
804d4000 806aab00   nt            Checksum: 001E3FB0  Timestamp: Thu Apr 24 16:57:43 2003 (3EA80977)

Unloaded modules:
b1305000 b1548000   w70n51.sys    Timestamp: unavailable (00000000)
b1968000 b1978000   NAVENG.Sys    Timestamp: unavailable (00000000)
b1003000 b1094000   NavEx15.Sys    Timestamp: unavailable (00000000)
b2058000 b2068000   NAVENG.Sys    Timestamp: unavailable (00000000)
b1134000 b11c5000   NavEx15.Sys    Timestamp: unavailable (00000000)
b1928000 b1938000   NAVENG.Sys    Timestamp: unavailable (00000000)
b156f000 b1600000   NavEx15.Sys    Timestamp: unavailable (00000000)
b1871000 b1898000   kmixer.sys    Timestamp: unavailable (00000000)
f7301000 f7544000   w70n51.sys    Timestamp: unavailable (00000000)
b2402000 b2412000   NAVENG.Sys    Timestamp: unavailable (00000000)
b1740000 b17d1000   NavEx15.Sys    Timestamp: unavailable (00000000)
b2ab6000 b2ac6000   NAVENG.Sys    Timestamp: unavailable (00000000)
b19ff000 b1a90000   NavEx15.Sys    Timestamp: unavailable (00000000)
b19d8000 b19ff000   kmixer.sys    Timestamp: unavailable (00000000)
b1a90000 b1ab7000   kmixer.sys    Timestamp: unavailable (00000000)
b23c2000 b23d2000   NAVENG.Sys    Timestamp: unavailable (00000000)
b1ab7000 b1b48000   NavEx15.Sys    Timestamp: unavailable (00000000)
b1a90000 b1ab7000   kmixer.sys    Timestamp: unavailable (00000000)
b1a90000 b1ab7000   kmixer.sys    Timestamp: unavailable (00000000)
b1b78000 b1b88000   NAVENG.Sys    Timestamp: unavailable (00000000)
b1ab7000 b1b48000   NavEx15.Sys    Timestamp: unavailable (00000000)
b2168000 b218f000   kmixer.sys    Timestamp: unavailable (00000000)
```

Auditing stellt eine der wichtigsten Methoden zur Kontrolle eines lauffähigen und abgesicherten Systems dar.

Zum Auditing gehört nicht nur die richtige Auswahl der Auditkategorien, sondern ebenso das Prüfen und Auswerten der Auditlogs.

Eine sorgfältige Auswahl der Auditkategorien ist wesentlich, um eine sinnvolle Anzahl von aufgezeichneten Ereignissen zu erhalten

- Das Aktivieren von zu vielen Auditkategorien führt zu einer nicht mehr auswertbaren Anzahl von Ereignissen.
- Ein zu Wenig führt zu Auslassung der Protokollierung wichtiger Ereignisse und damit zu einer Fehleinschätzung des Gesamt- - und hier besonders – des Sicherheitszustandes des Systems.

Es gibt 9 Audit-Kategorien, jede von diesen Kategorien wird einzeln in dem entsprechenden GPO aktiviert

Überwachungsrichtlinien müssen grundsätzlich dort implementiert werden, wo das Ereignis eintritt

Z.B. Anmeldeversuche auf OU „Domain Controllers“;
Anmeldeereignisse auf OU „Workstations“

Richtlinieneinstellung „Ereignisanzeige“ steuert die Größe der Protokolldateien und deren Aufbewahrung.

Audit-Kategorien

Active Directory-Zugriff überwachen	Zugriff auf ein AD-Objekt (SACL)
Anmeldeereignisse überwachen	An-/Ameldung an Ressource („where the logon occurs“)
Anmeldeversuche überwachen	An-/Abmeldung am Domänencontroller („where the acount lives“)
Kontenverwaltung überwachen	Ändern, Erstellen, Löschen von Sicherheitsprincipals
Objektzugriffsversuche überwachen	Zugriff auf Datei, Drucker, Ordner (SACL)
Prozessverfolgung überwachen	Ein Prozess/eine Anwendung führt einen Vorgang aus (für Entwickler)
Rechteverwendung überwachen	Verwenden eines Benutzerrechts
Richtlinienänderungen überwachen	Bearbeiten von Policies
Systemereignisse überwachen	z.B. Herunterfahren eines Systems

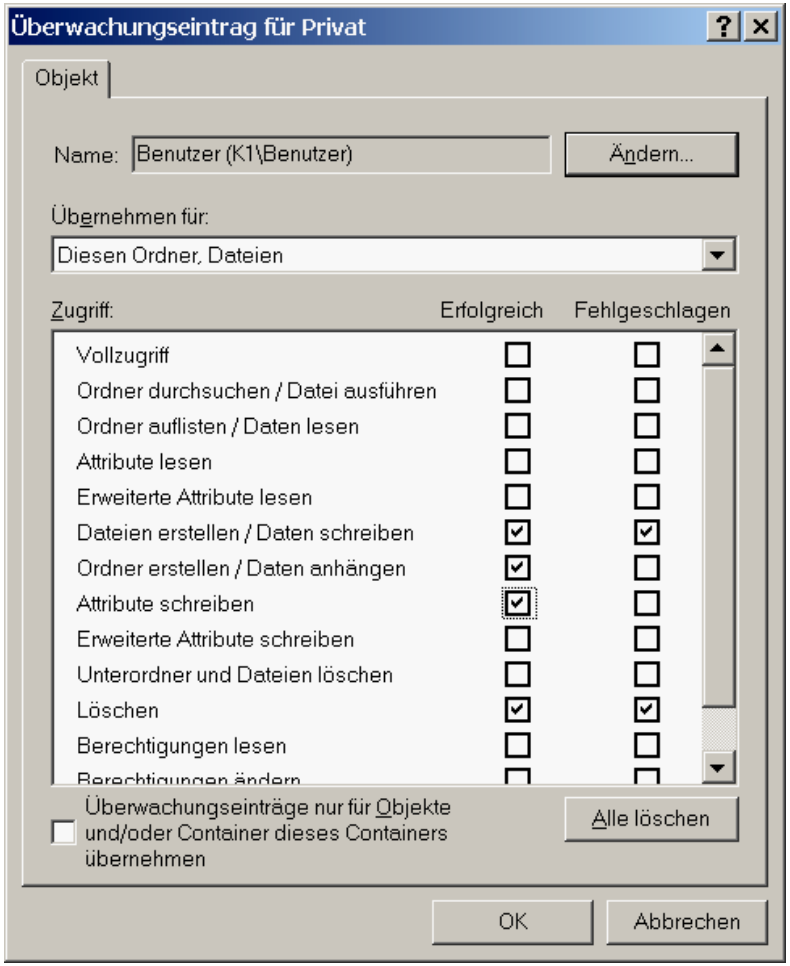
Nach der Aktivierung (im GPO) kann für die beiden Kategorien

- Active Directory-Objekte
- NTFS-Objekte

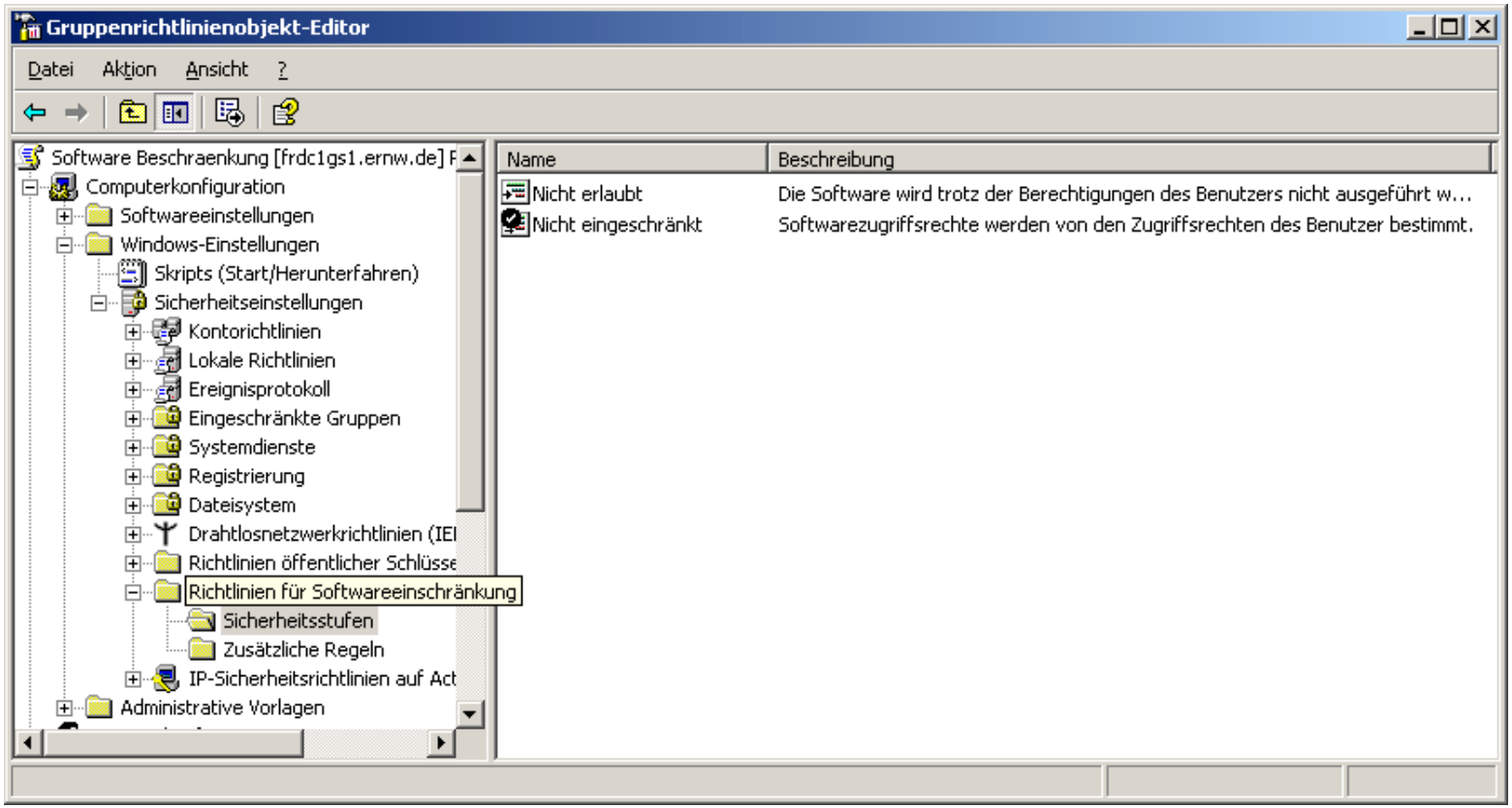
die Überwachung in der zugehörigen Objekt-SACL granular konfiguriert werden:

Sinnvolle Einstellungen entnimmt man

z. B. dem *Windows XP-Sicherheitshandbuch.*



Wichtiges neues Sicherheitsmerkmal von Windows XP und Server 2003: Richtlinien für Softwarebeschränkung:



Möglichkeiten

- Schutz des Rechners vor bösartigem Code
- Kontrolle, welcher Benutzer welche Software ausführen darf
- Schutz vor gewöhnlichem Code

Unterstützte Betriebssysteme:

- Windows 2000, Windows XP, Server 2003 (Bearbeitung kann nicht auf Windows 2000-Rechnern erfolgen)

Konfiguration (Überblick):

- Sicherheitsstufen:

  Nicht erlaubt: erfordert zusätzliche Definition von Ausnahmen in *Zusätzliche Regeln*

  Nicht eingeschränkt: erfordert zusätzliche Definition von einzuschränkender Software in *Zusätzliche Regeln*

- Zusätzliche Regeln:
  - Hashregel
  - Zertifikatregel
  - Internetzonenregel

  Rangfolge der Regeln: im Konfliktfall i. A. die speziellste Regel

Grenzen der Softwarebeschränkung

- Regeln gelten ggf. nicht für:
  - Treiber und Software im Kernelmodus
  - Code, der unter *System*-Konto läuft
  - *.NET Common Language Runtime*
  - Code in einer NTVDM (vgl. KB319458)

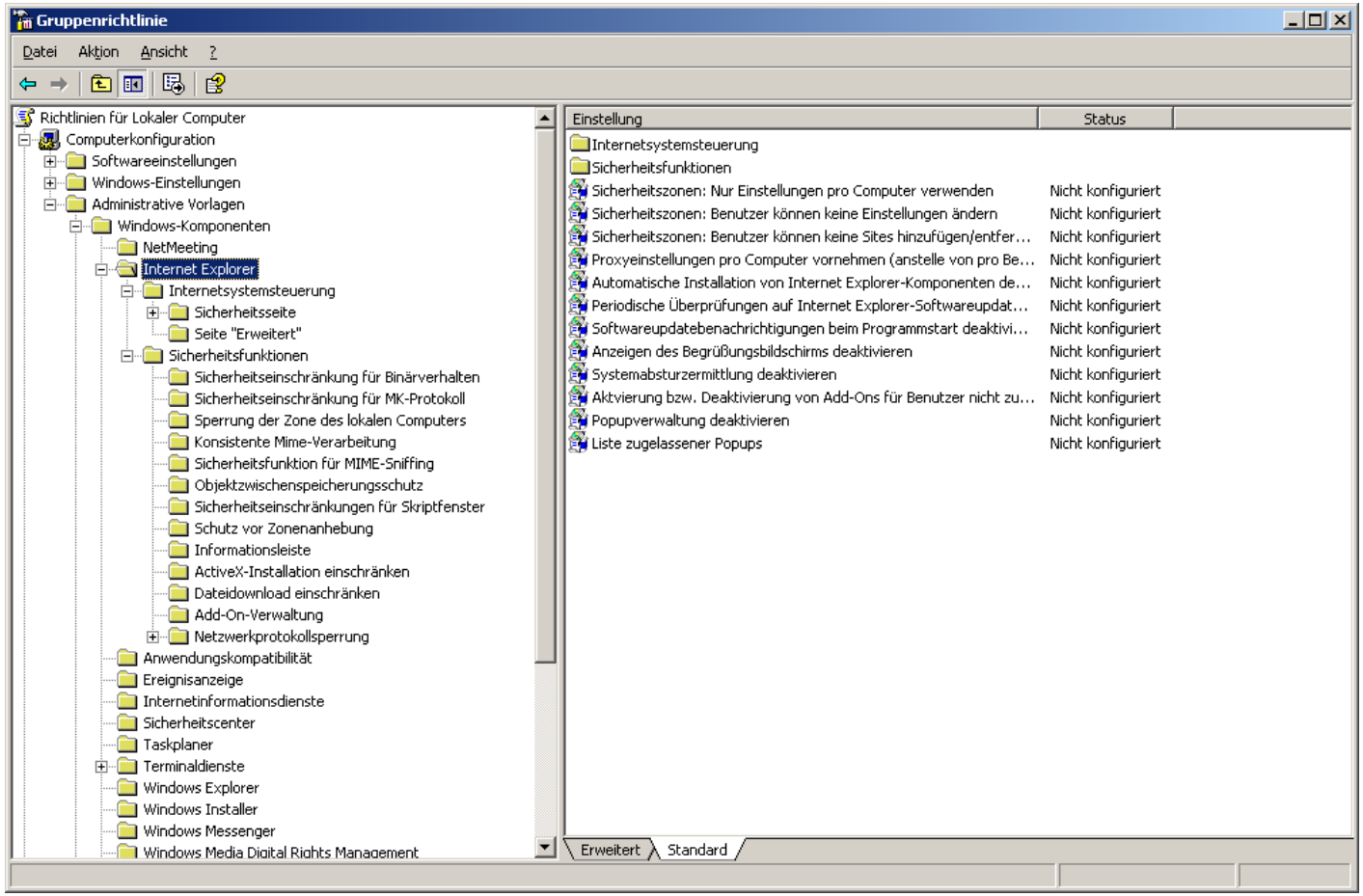
Wenn möglich einen anderen Browser als den IE verwenden

- Meister Schadcode für IE geschrieben
- Sinnvoller Ersatz für viele Zwecke Firefox
  - Achtung: Nicht immer einsetzbar; z. B. nicht bei der Zertifikatsbearbeitung einer Windows CA

Bändigungsmöglichkeiten des IE im GPO

- Jede Seite der Internetoptionen kann über eine GPO-Einstellung gesteuert werden
- Weitere Konfigurationsmöglichkeiten über das bei Microsoft herunterladbare IEAK (Internet Explorer Administration Kit)

Bändigungsmöglichkeiten des IE im GPO



Technologien für eine sichere Email-Verarbeitung (hierüber gibt es noch keine präzisen Informationen)

Technologien für sicheres Browsen (eine Auswahl):

- Detaillierte Add-On-Verwaltung für den IE durch Benutzer (Benutzer können sich Listen anzeigen lassen und Add-Ons per Mausklick deaktivieren, entfernen, es läßt sich anzeigen, welche geladen sind, welche verwendet werden. Add-Ons umfassen: Active-X-Controls, Symbolleistenerweiterungen, Browsererweiterungen. Administratoren können Allowlists und Denylists definieren)
- Add-On-Absturzerkennung für den IE: bei jedem Absturz des IE wird das Add-On-Absturzerkennungsprogramm gestartet, das eine Fehleranalyse durchführt und versucht, das den Absturz verursachende Add-On zu identifizieren

Technologien für sicheres Browsen:

Strengere Sicherheitseinstellungen für die Zone *Eingeschränkte Sites* (erfordert evtl. Anpassung des HTML-Codes von in dieser Site ausgeführten Seiten)

Einschränkung der IE-Zone *Lokaler Computer*: ab SP2 wird die Zone *Lokaler Computer* auf alle Dateien und Inhalte angewendet, die vom IE verarbeitet werden; früher wurden lokale Inhalte als sicher betrachtet und es wurde keine zonenbasierte Sicherheit auf sie angewendet; jetzt werden Webanwendungen mit geringen Einschränkungen ausgeführt (z. B. werden Active-X-Scripts in lokalen HTML-Seiten, die im IE angezeigt werden, nicht ausgeführt)

Sicherheitskontext wird bei der Navigation in eine andere Domäne ab jetzt ungültig

Popup-Manager im IE (standardmäßig deaktiviert): Bei Aktivierung werden automatische Popup-Fenster und Popup-Fenster im Hintergrund blockiert

Technologien für sicheres Browsen:

- Fenstereinschränkungen im IE:

  Skripte können die Fenstereinstellungen nicht mehr so ändern, dass Titel-, Adress- oder Statusleiste nicht mehr angezeigt werden können

  Der Befehl *fullscreen* wird umdefiniert: Fenster wird maximiert angezeigt mit stets sichtbarer Titel-, Adress- und Statusleiste

  Positionierung von Fenstern: keine Erweiterung über das übergeordnete Fenster hinaus, Verankerung mit dem übergeordneten Fenster (untergeordnete Fenster werden mit verschoben), Anzeige über dem übergeordneten Fenster, damit Dialogfelder nicht verdeckt werden können

- Verhindern der Zonenheraufstufung im IE: Webinhalt kann sich künftig nicht mehr in eine andere Sicherheitszone eintragen, um die Wahrscheinlichkeit der Ausführung von malicious Code zu erhöhen

…vom Dozenten vorgeschlagene Übungen