Leibniz Rechenzentrum

der Bayerischen Akademie der Wissenschaften

Windows 2000/XP Sicherheit in Kürze

Thomas Niedermeier

2004-12-26

Inhalt:

Alle folgende Sicherheits-Hinweise sind für Windows 2000/XP Maschinen gedacht, die Standalone betrieben werden. Besitzen Sie eine Maschine, die Teil einer Domäne oder eines anderen Verbundes von Maschinen ist, sprechen Sie dies bitte mit Ihrem zuständigen Administrator ab. Die Informationen sind möglichst allgemein gehalten und können deshalb nicht alle Gegebenheiten vor Ort berücksichtigen.

!!Achtung!!

Ein unsachgemäßer Umgang mit dem System kann zu dessen Unbrauchbarkeit führen.
Bedenken Sie auch, daß Bequemlichkeit und Sicherheit nicht immer vereinbar sind. Manche der Vorschläge auf dieser Seite bedeuten für den Benutzer Mehrarbeit zu Gunsten eines sicheren Systems.

!!Achtung!!

1. Physikalische Sicherheit

Das sicherste Betriebssystem nützt nichts wenn jemand von einem parallelen System auf die Daten Ihrer Platte zugreifen kann. Sie können im BIOS den Startvorgang Ihres Systems definieren. Erlauben Sie hier nur das Booten von der Festplatte. Setzen Sie ein BIOS-Passwort, damit nur Sie diese Einstellungen verändern können. Zusätzlich sollten Sie dafür sorgen, am Gehäuse Ihres Gerätes ein Schloss anzubringen, um ein Zurücksetzen des Passwortes oder gar einen Diebstahl der Platte zu verhindern.

2. Benutzerverwaltung

Auch für Windows gelten die gängigen Empfehlungen zu Passwörtern. Ein gutes Passwort besteht mindestens aus 8 Zeichen. Das Passwort umfasst eine Kombination von Klein-, Großbuchstaben, Ziffern und Sonderzeichen. Es dürfen keine Wortteile enthalten sein wie Dieter09 oder ähnlichem.

Bewahren Sie Ihr Passwort nur im Gedächtnis auf und nicht woanders.

In den Gruppenrichtlinien können Sie unter Richtlinien für Lokaler Computer - Computerkonfiguration - Windows Einstellungen - Sicherheitseinstellungen - Kontorichtlinien Richtlinien für Kennwörter und Konten Ihre Benutzer definieren:

Kennwortrichtlinien

Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert
Kennwortchronik erzwingen	5
Maximales Kennwortalter	42 Tage
Minimale Kennwortlänge	8 Zeichen

Kontosperrungsrichtlinien:

Kontensperrungsschwelle	5 ungültigen Anmeldeversuchen
Kontosperrdauer	30 Minuten
Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten

Legen Sie einen zweiten administrativen Benutzer an und sperren Sie den built-in Administrator, dadurch führen Sie einen etwaigen Angreifer in die Irre. Legen Sie für ihre alltäglichen Arbeiten einen Benutzer-Account an. Verwenden Sie Ihren Administrator-Account nur für administrative Tätigkeiten (Installation von Software). Beachten Sie hierbei, daß ältere Software eventuell nicht korrekt arbeitet, wenn Sie bestimmte Rechte auf das System nicht besitzen. Um Ihre Privilegien auf das System zu erhöhen, können Sie Ihr Benutzerkonto der Gruppe der Hauptbenutzer hinzufügen.

Definieren Sie, wer sich an der Maschine alles anmelden darf und gewähren Sie dieser Gruppe das Recht zur lokalen Anmeldung unter „Zuweisen von Benutzerrechten“. Verweigern Sie allen anderen den Zugriff. Ersetzen Sie die Gruppe Jeder durch die Gruppe Benutzer wo immer Sie Ihnen begegnet.

3. Dateisystem

Formatieren Sie Ihre lokalen Partitionen mit dem Dateisystem NTFS. Dadurch können Sie Dateirechte vergeben und erhöhen so die Sicherheit des Filesystems gegenüber Fat16 oder Fat32.
Löschen Sie unnötige Freigaben. Setzen Sie eindeutige Zugriffsrechte auf Freigaben und Dateisystem. Kontrollieren Sie regelmäßig die Anzahl der Freigaben.
Entfernen Sie die Gruppe Jeder von der obersten Ebene Ihrer Systempartition.
Um die Sicherheit Ihrer Daten auch bei einem Diebstahl der Platten (Notebook) zu gewähren, können Sie Ihre Dateien mit EFS verschlüsseln. Die Daten sind dann nur noch unter Ihrem Kennzeichen lesbar.

4. Windows Update - SUS

Viele Einbrüche in Systeme nutzen Sicherheitslücken, die oft monatelang bekannt waren, die aber vom Administrator nicht geschlossen wurden. Halten Sie Ihr System deshalb auf einem aktuellen Stand mit der Windows Update Funktion. Warten Sie aber ein paar Tage bevor Sie den aktuellsten Hotfix oder ein Service Pack einspielen, um Ihr System nicht unnötig zu gefährden. Informieren Sie sich über aktuelle Sicherheitsprobleme mit Ihrem Betriebssystem und der Software die Sie nutzen. Informationen über aktuelle Sicherheitsprobleme finden Sie bei:

Microsoft (http://www.microsoft.com/security/)
Cert Stuttgart (http://cert.uni-stuttgart.de/os/ms/index.php)

Mitglieder des MWN können den SUS des LRZ (http://www.lrz-muenchen.de/services/security/mwnsus/) nutzen. Außerhalb des MWN können Sie die automatische Update Fuktion für Windows konfigurieren.

5. MBSA (Microsoft Baseline Security Analyzer)

Um eine Übersicht über Sicherheitsrelevante Aspekte Ihres Systems zu bekommen, laden Sie sich den MBSA (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP) von Microsoft herunter. Scannen Sie damit regelmäßig Ihr System. Sie erhalten damit detailliert Auskunft über fehlende Hotfixes, Windows, SQL und IIS Schwachstellen, sowie über schwache Passwörter. Der MBSA bietet auch weiterführende Informationen zu den angezeigten Sicherheitsproblemen Ihres Systems.

6. Virenscanner

Installieren Sie auf Ihrem System einen aktuellen Virenscanner. Damit alleine ist es aber nicht getan. Um auch gegen die neuesten Viren geschützt zu sein, müssen sie auch regelmäßig die aktuellsten Virenpatterns in Ihren Scanner einpflegen. Näheres finden sie bei Ihrem Virenscanner-Hersteller. Angehörige der Universitäten LMU und TUM können den Virenscanner Sophos über das LRZ (http://www.lrz-muenchen.de/services/security/antivirus/) nutzen. Informationen zu aktuellen Viren finden Sie bei den Herstellern:

Sophos (http://www.sophos.com/)
Symantec (http://www.symantec.com/region/de/avcenter/)

7. Personal Firewall

Weitere Sicherheit bietet eine personal Firewall, die Sie auf Ihrer lokalen Maschine installieren. Über diese Firewall können Sie sehr feingranular steuern, von welchen Maschinen mit welchem Protokoll und über welche Ports auf Ihre Maschine zugegriffen werden darf und welche Informationen Ihre Maschine nach außen gibt.

Windows XP SP2 Nutzer sollten die mitgelieferte Firewall einschalten. Damit werden standardmäßig alle Verbindungsversuche von außen geblockt. Für alle anderen Windows-Versionen empfiehlt sich der Einsatz eines Produktes eines Drittherstellers wie Zonealarm. Eine Liste von aktuellen Firewalls finden Sie hier. (http://www.microsoft.com/germany/consumer/sicherheit/content/protect/windows2000/firewall.aspx)

8. Spyware-Adware-Browser Hijacking

Ein in den letzten Monaten wachsendes Problem sind Spy- und Adware. Während Adware den Nutzer nur mit Reklame belästigt, spioniert Spyware den Nutzer aus und überträgt sensible Daten (Nutzungsverhalten, Passwörter, Bankverbindung, Kreditkartennummern...) ins Internet. In diesem Zusammenhang tritt auch immer wieder das "Browser Hijacking", also eine Übernahme des Browsers. Dies macht sich meist durch das zurücksetzen der Startseite, oder immer wieder begleitende Popups bemerkbar.

Ähnlich wie für Viren gibt es auch hierfür Tools um diese unliebsamen Gäste zu entfernen und sich davor zu schützen. Sehr gute Erfahrungen haben wir mit nachfolgenden Produkten gemacht. Vergessen Sie aber nicht auch diese Tools müssen auf dem aktuellsten Stand gehalten werden.

Spybot Search and Destroy (http://security.kolla.de/)
Ad-aware von Lavasoft
(http://www.lavasoft.de/)

9. Überwachung einschalten

Schalten Sie die Überwachung ein um einen besseren Überblick zu bekommen, was auf Ihrer Maschine geschieht. In den Gruppenrichtlinen - Richtlinien für Lokaler Computer - Computerkonfiguration - Windows Einstellungen - Sicherheitseinstellungen - Lokale Richtlinien - Überwachungsrichtlinien sollte Sie folgende Ereignisse auf erfolgreich/fehlgeschlagen überwachen:

Anmeldeereignisse
Anmeldeversuche
Kontenverwaltung
Objektzugriffsversuche
Rechteverwendung
Richtlinienveränderung

Die einzelnen Ereignisse werden in der Ereignisanzeige im Sicherheitsprotokoll angezeigt. Erhöhen Sie über die Eigenschaften (rechte Maustaste auf das gewünschte Protokoll) auch die Größe des Sicherheitsprotokolls auf mindestens 2 MB und stellen Sie Bei Bedarf überschreiben ein.

10. Unnötige Dienste deaktivieren

Jeder Dienst, der auf Ihrer Maschine läuft, bietet einen Angriffspunkt. Deaktivieren Sie alle nicht benötigten Dienste. Vorsicht! Sollten Sie einen für das System wichtigen Dienst deaktivieren kann Ihr System unbrauchbar werden. Berücksichtigen Sie auch Dienste, die nachträglich durch Softwareinstallationen hinzugefügt wurden. Die folgende Liste kann also nicht vollständig sein. Bevor Sie einen Dienst deaktivieren informieren Sie sich (siehe unten). Deaktivieren Sie immer nur einen Dienst. Wenn Sie die Möglichkeit haben, probieren Sie das vorher in einer Testumgebung aus

Weitere Informationen zu den einzelnen Diensten können Sie hier nachlesen:

Liste bekannter Dienste für Windows XP auch auf Win 2000 übertragbar (http://www.beemerworld.com/tips/servicesxp.htm)
Liste bekannter Prozesse auf Windows-Systemen (http://www.reger24.de/prozesse.html)

Zu den Kerndiensten von Windows zählen:

Standalone Maschine:

Dienst "Ausführen als"
DNS-Client
Druckwarteschlange
Ereignisprotokoll
Plug & Play
Remoteprozeduraufruf (RPC)
Sicherheitskontenverwaltung
Verwaltung logischer Datenträger
Windows Verwaltungsinstrumentation

Netzwerkverbindungen (Startart manuell, bei Anbindung ans Netz über Modem oder Lan)

optional:
Task Planer (um zeitgesteuerte Aufträge auszuführen)
Geschützter Speicher (Hinterlegt Passwörter)
Windows Installer (um Software auf WindowsInstaller Technologie zu installieren)

Im Verbund Arbeitsgruppe/Domäne kommen zu den obigen Diensten hinzu:

Arbeitsstationsdienst
TCP/IP NetBIOS Hilfsprogramm
Netzwerkverbindungen (manuell)

optional:
IPSec Policy-Agent (für sichere Kommunikation innerhalb einer Domäne)
Remote Registry Service (Software die über das Netz auf Ihre Registry zugreift, Virenscanner)

Für Server kommen noch hinzu:
Anmeldedienst
Dateireplikationsdienst
Kerberos-Schlüsselverteilungscenter
Remote Procedure Call (RPC) Locator
Systembenachrichtigung
Server
TCP/IP NetBIOS Hilfsprogramm
Windows-Zeitgeber

11. Unnötige Komponenten entfernen

IIS (Internet Information Server):
Eine der Komponenten, die sich häufig unbemerkt auf W2K-Maschinen findet, ist der IIS von Microsoft. Da ein unkonfigurierter und ungepflegter IIS ein bedeutendes Sicherheitsrisiko darstellt, empfehlen wir diesen zu deinstallieren, wenn nicht explizit benötigt. Um einen IIS abzusichern gibt es Tools wie IISlockdown oder UrlScan. Zahlreiche Patches und sehr gute Dokumentation findet man bei Microsoft. Überprüfen Sie auch die Installation mit dem MBSA [S.3] .

MS Dokumentation zu IIS
(http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/DEFAULT.asp)

MSDE/SQL-Server:
Kontrollieren Sie mit dem MBSA [S.3] ob auf Ihrem System eine SQL-Datenbank läuft und ob etwaige Sicherheitslücken bestehen. Bei der Installation von unterschiedlichster Software wird gelegentlich eine MSDE im Hintergrund mitinstalliert. Häufig sind diese Komponenten nicht auf dem aktuellsten Stand. Tragen Sie deshalb dafür Sorge, das aktuellste Service Pack zu installieren. Entfernen Sie die Software, wenn Sie nicht mehr benötigt wird.

MS Dokumentation zu SQL
(http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/DEFAULT.asp)

Unnötige Protokolle deaktivieren bzw. deinstallieren:
Entfernen oder deaktivieren Sie alle unnötigen Netzwerk-Protokolle von Ihrer Netzwerkkarte. Generell benötigen Sie nur das TCP/IP Protokoll für den Zugang zum WWW. Betreiben Sie eine Standalone Maschine, sollten Sie andere Protokolle wie NetBios oder IPX entfernen. Geben Sie keine Dateien oder Drucker frei, können Sie auch "Datei und Druckerfreigabe" und den "Client für MS-Netzwerke" deaktivieren.

OS2 und POSIX Komponenten entfernen
Entfernen Sie den Registryschlüssel
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems]. Starten Sie hierzu das Programm c:\winnt\regedit.exe unter Windows 2000 bzw. unter Windows XP c:\windows\regedit.exe.
Lassen Sie danach Ihr System nach Dateien os2*.dll, posix*.dll und psx*.dll suchen. Entfernen Sie zuerst die Dateien im Unterordner dllcache und danach den Rest, da die gelöschten Dateien sonst wieder hergestellt werden.

12. Sicherheitsoptionen

Über die Gruppenrichtlinen - Richtlinien für Lokaler Computer - Computerkonfiguration - Windows Einstellungen - Sicherheitseinstellungen - Lokale Richtlinien - Sicherheitsoptionen können Sie allgemeine Einstellungen zur Sicherheit Ihres Systems einstellen, die für die Maschine und alle Benutzer gelten.

Richtlinie	Einstellung
Anzahl zwischenzuspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist)	0 Anmeldungen
Auslagerungsdatei des virtuellen Arbeitspeichers beim Herunterfahren des Systems löschen	Aktiviert
Clientkommunikation digital signieren (wenn möglich)	Aktiviert
LAN Manager-Authentifizierungsebene	Nur NTLMv2-Antworten senden LM- und NTLM verweigern
Letzten Benutzernamen nicht im Anmeldedialog anzeigen	Aktiviert
Serverkommunikation digital signieren (wenn möglich)	Aktiviert
Sicherer Kanal: Daten des sicheren Kanals digital signieren (wenn möglich)	Aktiviert
Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)	Aktiviert
STRG+ALT+ENTF-Anforderung zur Anmeldung deaktivieren	Aktiviert
Unverschlüsseltes Kennwort senden, um Verbindung mit SMB-Servern von Drittanbietern herzustellen	Aktiviert
Verhalten bei der Installation von nichtsignierten Dateien (außer Treibern)	Warnen, aber Installation zulassen
Verhalten bei der Installation von nichtsignierten Treibern	Warnen, aber Installation zulassen
Weitere Einschränkungen für anonyme Verbindungen	Kein Zugriff ohne explizite anonyme Berechtigung
Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen	Deaktiviert
Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Zugriff auf globale Systemobjekte prüfen	Aktiviert

Um die Sicherheit weiter zu erhöhen kann man noch Folgende Einstellungen tätigen:

Anwendern das Installieren von Druckertreibern nicht erlauben	Aktiviert
Clientkommunikation digital signieren (immer)	Aktiviert
Die Verwendung des Sicherungs- und Wiederherstellungsrechts überprüfen	Aktiviert
Herunterfahren des Systems ohne Anmeldung erlauben	Aktiviert
Serverkommunikation digital signieren (immer)	Aktiviert
Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)	Aktiviert
Sicherer Kanal: Starker Sitzungsschlüssel erforderlich (Windows 2000 oder höher)	Aktiviert

13. Internet Explorer

Für den Internet Explorer gelten die selben Regeln wie für das Betriebssystem. Ein schlecht gepflegter oder falsch konfigurierter Browser kann eine ernsthafte Bedrohung für die Sicherheit Ihres Systems sein. Die Gefahr geht hierbei von bestimmten Websites aus, die Sie besuchen. Beim Öffnen der Site im Browser starten Skripte oder Java-Aplets, die unter umständen Ihr System beschädigen können. Setzen Sie die Sicherheitsstufe Ihres IE für die Webinhaltszone Internet auf hoch. Deaktivieren Sie alle Aktive-X und Scriptingeinstellungen. Sperren Sie alle Cookies unter Datenschutz. Sollten Sie dennoch Cookies für einzelne Seiten benötigen, können Sie die Seite in eine Ausnahmeliste mit geringer Sicherheitsstufe aufnehmen.