



# Sicherheits-Schulung

## Security Benchmarks

# Sicherheits-Schulung

## Gesamtüberblick

### *Sicherheitsbenchmarks setzen Sicherheitsstandards*

- Center for Internet Security
  - Ziele
  - Plattformen
  - Was wird getestet?
- Microsoft Management Console
  - Security analysis and configuration
  - Hfnetchk
- Microsoft Baseline Security Analysis 1.2.1

lessus

# Sicherheits-Schulung

## Ziele

### *Sicherheitsbenchmarks setzen Sicherheitsstandards*

- Soll Standards setzen
- Soll Druck ausüben
  - OS Herstellerfirmen
  - SW Herstellerfirmen
  - Firmen, die die SW, das OS einsetzen (KontragG)
- Soll einfach zu bedienen sein
- Soll Wettbewerb auslösen
- Zertifikate fördern
- Soll, natürlich, das Netz sicherer machen

Zielerreichung: Stelle Benchmark zur Verfügung!

# Sicherheits-Schulung

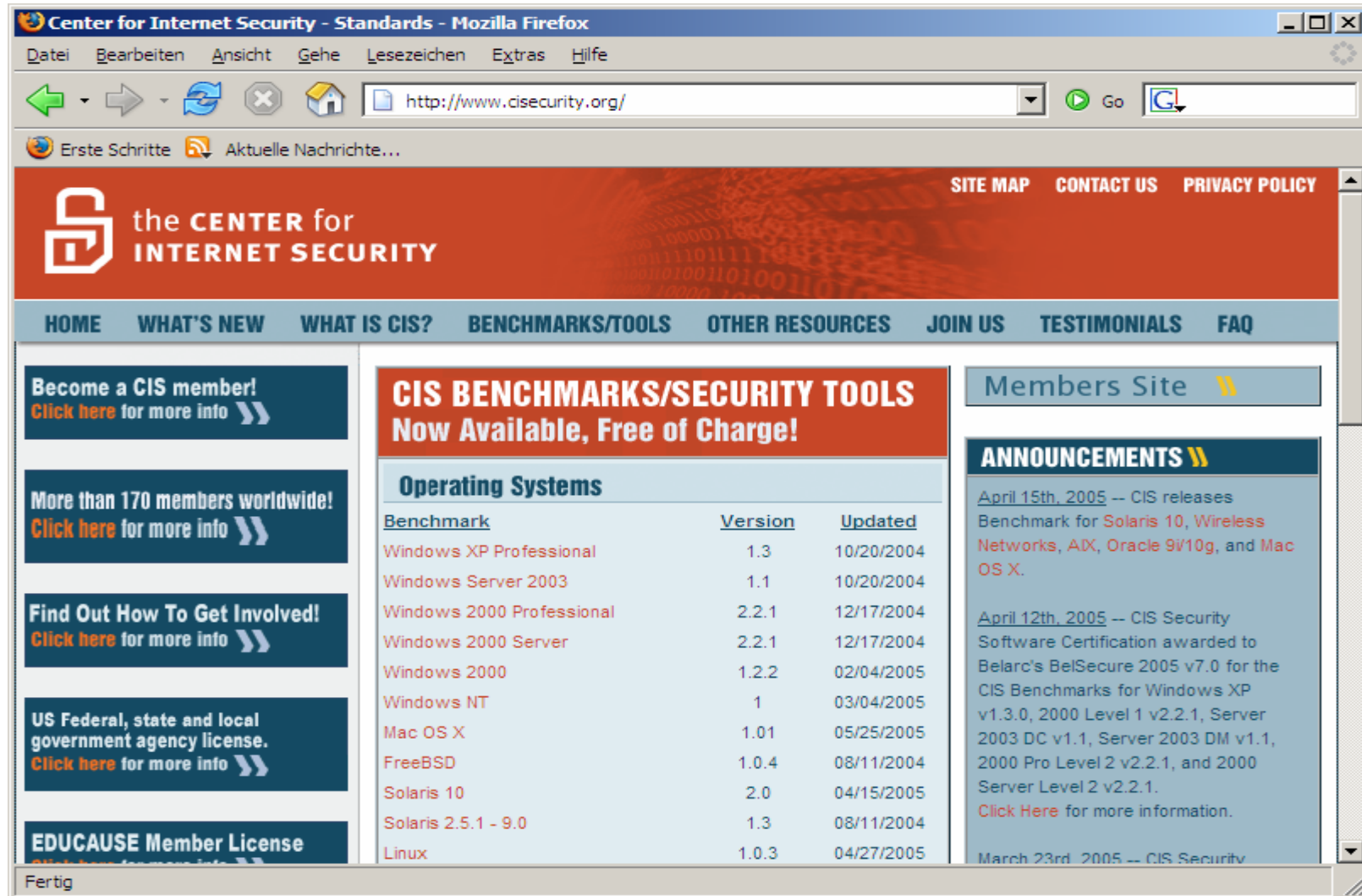
## Security Benchmarks Standards

### *CIS Foundation Standards*

- BS7799
- IETF site security handbook (rfc2196)
- The Information Systems Audit and Control Association (ISACA)
- FISCAM (Federal Information System Controls Audit Manual)
- Generally Accepted System Security Principles sponsored by the International Information Security Foundation (I<sup>2</sup>SF)
- NIST Principles and Practices for Securing IT Systems
- SysTrust™ Principles and Criteria for Systems Reliability (AICPA), Version 2.0
- NSA
- FBI / DOD

# Sicherheits-Schulung

## Center for Internet Security



Center for Internet Security - Standards - Mozilla Firefox

http://www.cisecurity.org/

Erste Schritte Aktuelle Nachrichte...

SITE MAP CONTACT US PRIVACY POLICY

the CENTER for INTERNET SECURITY

HOME WHAT'S NEW WHAT IS CIS? BENCHMARKS/TOOLS OTHER RESOURCES JOIN US TESTIMONIALS FAQ

Become a CIS member!  
Click here for more info >>

More than 170 members worldwide!  
Click here for more info >>

Find Out How To Get Involved!  
Click here for more info >>

US Federal, state and local government agency license.  
Click here for more info >>

EDUCAUSE Member License  
Click here for more info >>

### CIS BENCHMARKS/SECURITY TOOLS Now Available, Free of Charge!

#### Operating Systems

Benchmark	Version	Updated
Windows XP Professional	1.3	10/20/2004
Windows Server 2003	1.1	10/20/2004
Windows 2000 Professional	2.2.1	12/17/2004
Windows 2000 Server	2.2.1	12/17/2004
Windows 2000	1.2.2	02/04/2005
Windows NT	1	03/04/2005
Mac OS X	1.01	05/25/2005
FreeBSD	1.0.4	08/11/2004
Solaris 10	2.0	04/15/2005
Solaris 2.5.1 - 9.0	1.3	08/11/2004
Linux	1.0.3	04/27/2005

Members Site >>

#### ANNOUNCEMENTS >>

April 15th, 2005 -- CIS releases Benchmark for Solaris 10, Wireless Networks, AIX, Oracle 9i/10g, and Mac OS X.

April 12th, 2005 -- CIS Security Software Certification awarded to Belarc's BelSecure 2005 v7.0 for the CIS Benchmarks for Windows XP v1.3.0, 2000 Level 1 v2.2.1, Server 2003 DC v1.1, Server 2003 DM v1.1, 2000 Pro Level 2 v2.2.1, and 2000 Server Level 2 v2.2.1.  
Click Here for more information.

March 23rd, 2005 -- CIS Security

Fertig

# Sicherheits-Schulung

## Security Benchmarks CIS W2K

Eigenschaften der Benchmark Sicherheitseinstellungen

- Auch von unerfahrenen Administratoren zu realisieren
- Umsetzung stört den „normalen“ Betrieb nicht
- Können mit dem Benchmark scoring tool evaluiert werden

Level I Benchmarks testen das Betriebssystem

Level II Benchmarks testen Applikationen

Zur Zeit sind alle Testgruppen gleich gewichtet.

# Sicherheits-Schulung

## Security Benchmarks CIS W2K cis.inf

Windows 2000 Level I Security Scoring Tool v1.0.0

**THE CENTER FOR INTERNET SECURITY<sup>SM</sup>**

Windows 2000 Level I Security Scoring Tool - Host Based - v1.0.0

Computer:  **OVERALL SCORE:**

Scan Time:

**Scoring**

Select Security Template:

**Reporting**

**Service Packs and Hotfixes**

Service Pack:  Score:

Hotfixes Needed:  Score:

**Account and Audit Policies**

Non-Expiring Passwords:  Score:

Policy Mismatches:  Score:

**Security Options**

Restrict Anonymous:  Score:

Security Options Mismatches:  Score:

Designed by Kerry Steele, Paul Bible, Corey Badeaux, and Ron King.  
Please direct all technical feedback to [win2k-scan@cisecurity.org](mailto:win2k-scan@cisecurity.org).

# Sicherheits-Schulung

## Security Benchmarks CIS W2K workstation

Windows 2000 Level I Security Scoring Tool v1.0.0

**THE CENTER FOR INTERNET SECURITY<sup>SM</sup>**

Windows 2000 Level I Security Scoring Tool - Host Based - v1.0.0

Computer:  **OVERALL SCORE:**

Scan Time:

**Scoring**

Select Security Template:

**Reporting**

**Service Packs and Hotfixes**

Service Pack:  Score:

Hotfixes Needed:  Score:

**Account and Audit Policies**

Non-Expiring Passwords:  Score:

Policy Mismatches:  Score:

**Security Options**

Restrict Anonymous:  Score:

Security Options Mismatches:  Score:

Designed by Kerry Steele, Paul Bible, Corey Badeaux, and Ron King.  
Please direct all technical feedback to [win2k-scan@cisecurity.org](mailto:win2k-scan@cisecurity.org).

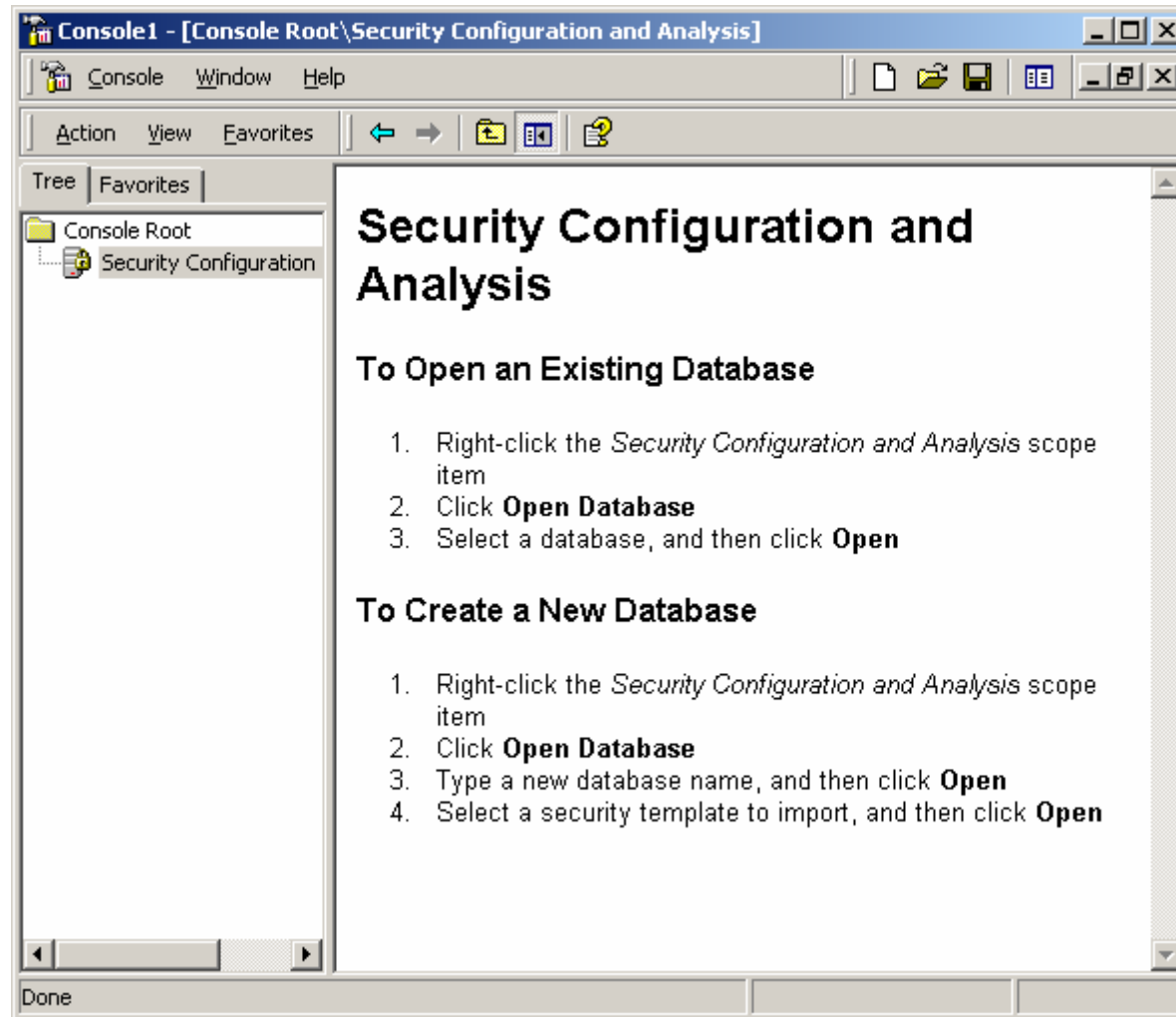
# Sicherheits-Schulung

## Security Benchmarks CIS W2K

```
C:\Program Files\CIS\SECDIT.TXT
File Edit View Favorites Tools Help
← Back → Search Favorites History
Address C:\Program Files\CIS\SECDIT.TXT
Analyze SeNetworkLogonRight.
Mismatch - SeNetworkLogonRight.
Analyze SeTcbPrivilege.
Analyze SeMachineAccountPrivilege.
Analyze SeBackupPrivilege.
Analyze SeChangeNotifyPrivilege.
Mismatch - SeChangeNotifyPrivilege.
Analyze SeSystemtimePrivilege.
Analyze SeCreatePagefilePrivilege.
Analyze SeCreateTokenPrivilege.
Analyze SeCreatePermanentPrivilege.
Analyze SeDebugPrivilege.
Mismatch - SeDebugPrivilege.
Analyze SeRemoteShutdownPrivilege.
Analyze SeAuditPrivilege.
Analyze SeIncreaseQuotaPrivilege.
Analyze SeIncreaseBasePriorityPrivilege.
Analyze SeLoadDriverPrivilege.
Analyze SeLockMemoryPrivilege.
Analyze SeBatchLogonRight.
Analyze SeServiceLogonRight.
Analyze SeInteractiveLogonRight.
Mismatch - SeInteractiveLogonRight.
Analyze SeSecurityPrivilege.
```

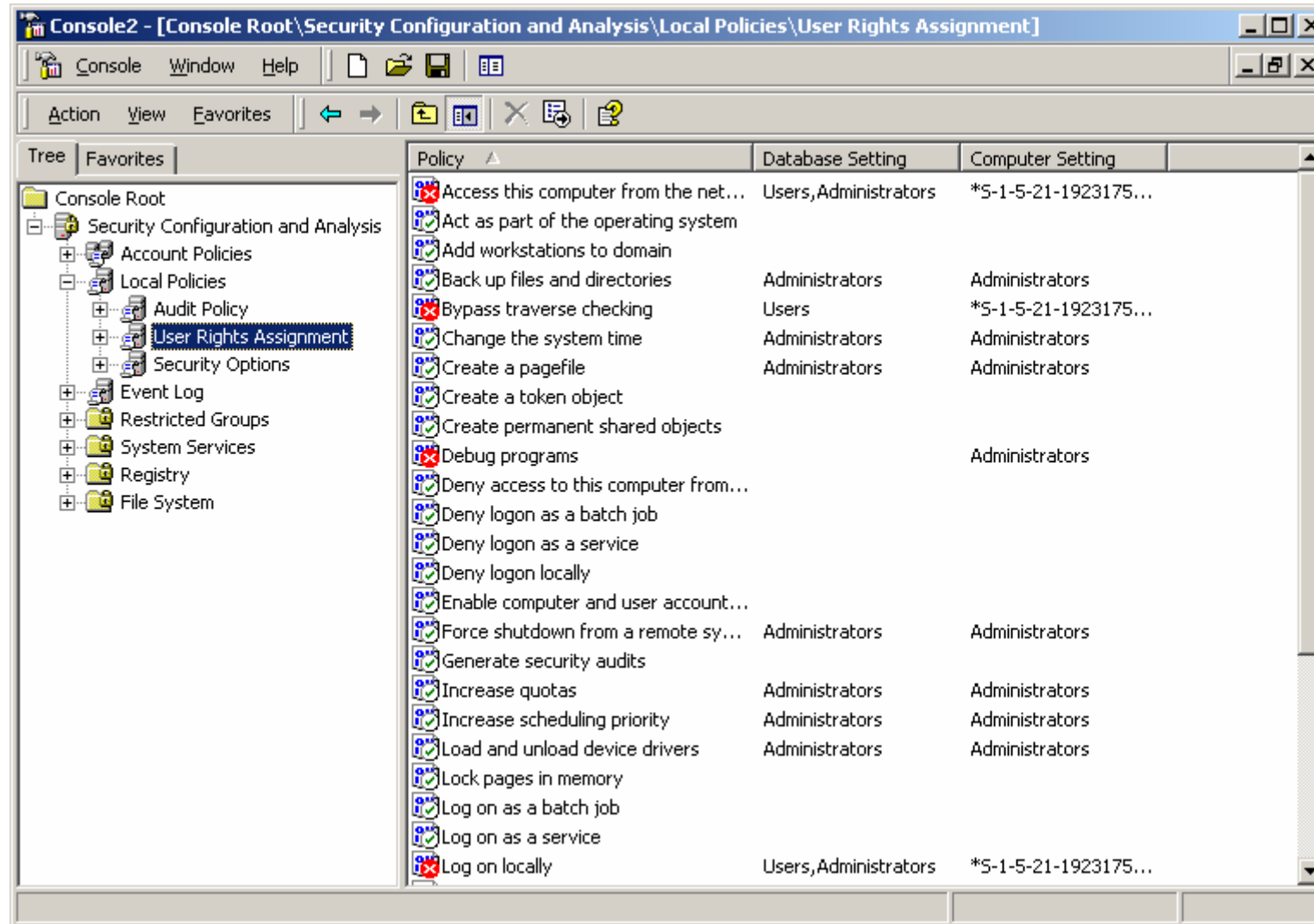
# Sicherheits-Schulung

## Security Benchmarks mmc I



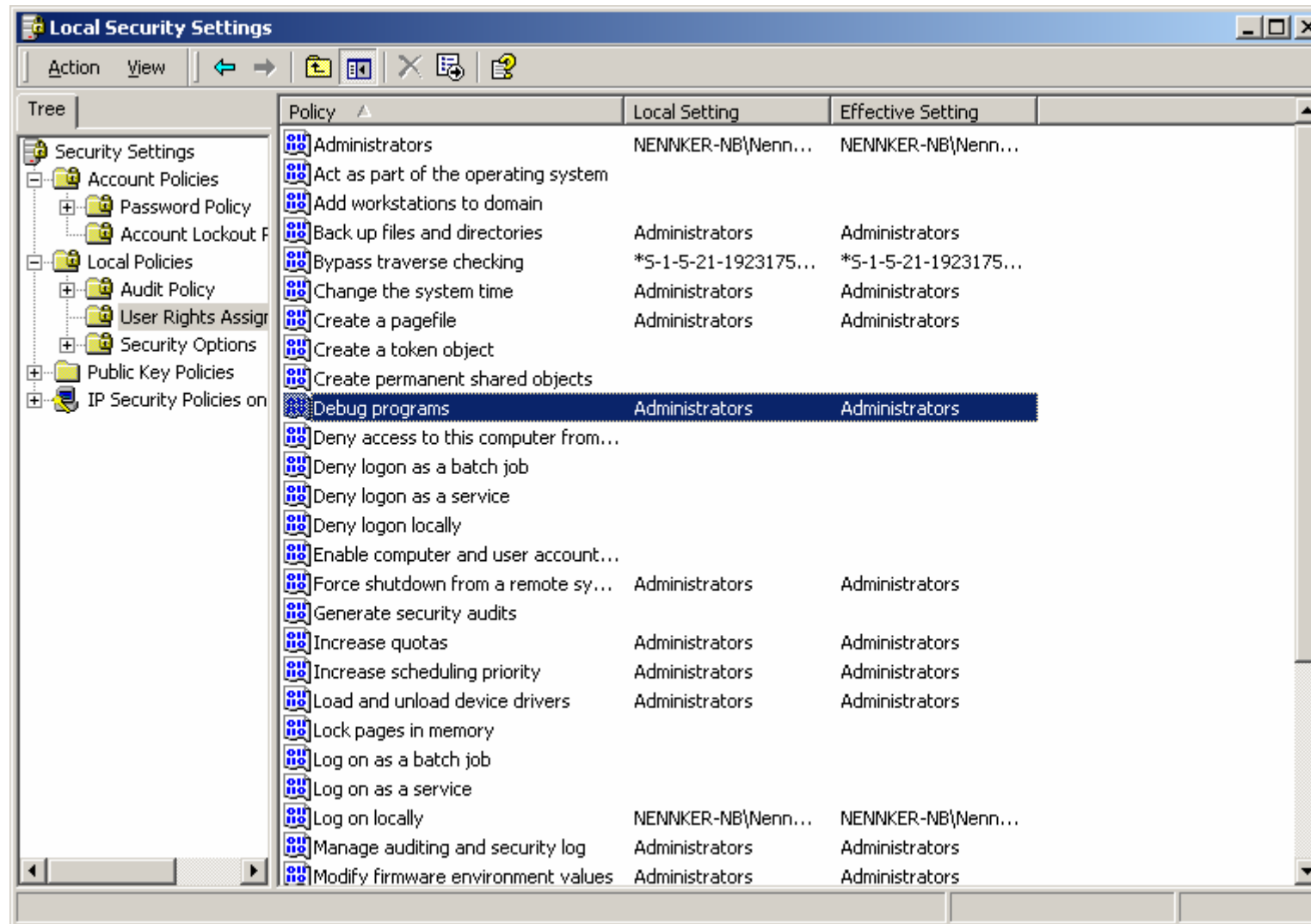
# Sicherheits-Schulung

## Security Benchmarks mmc II



# Sicherheits-Schulung

## Security Benchmarks mmc III



# Sicherheitsbenchmarks

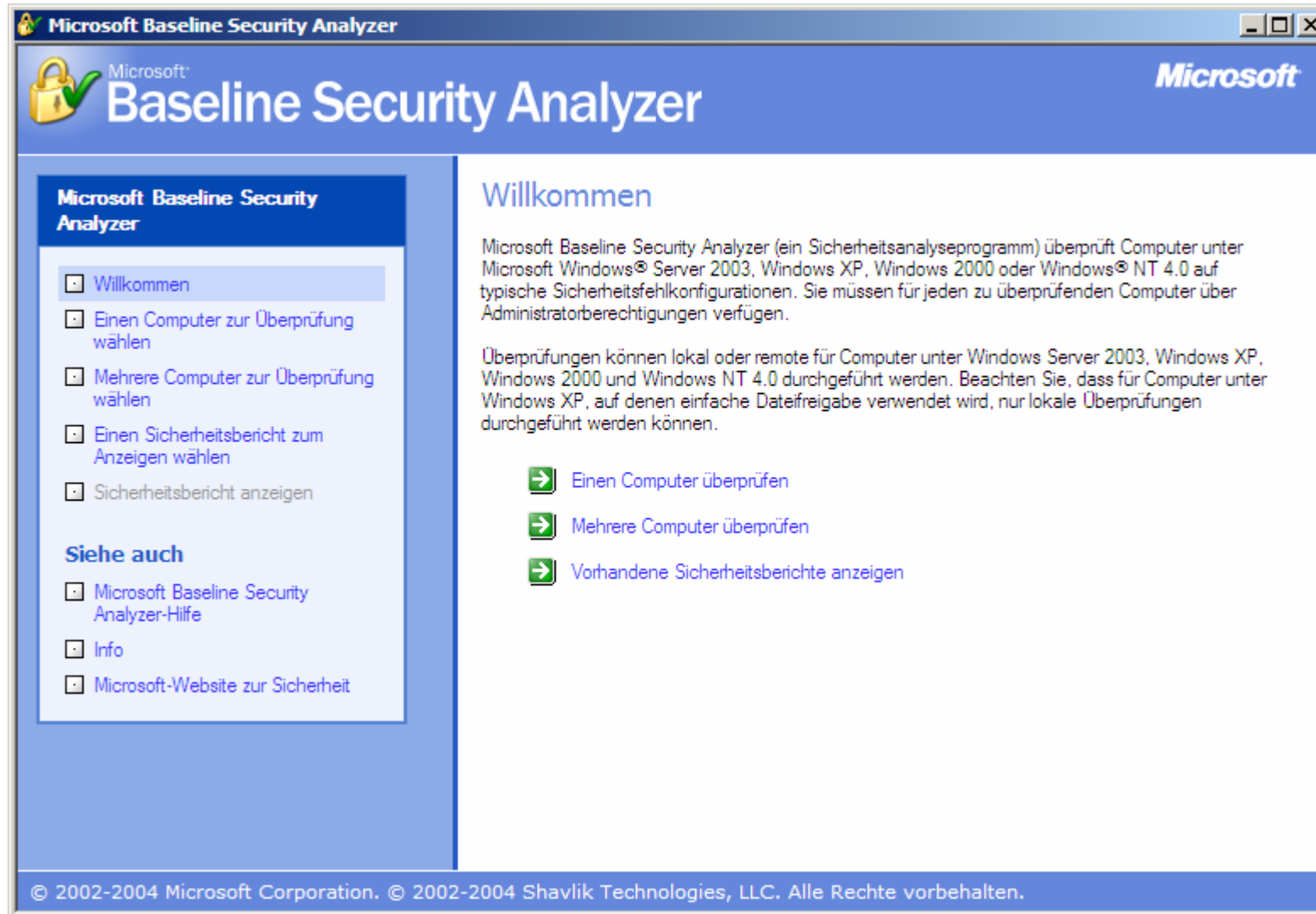
## Microsoft Baseline Security Analyser

- Seit 8. April 2002 verfügbar
- Benutzt ebenfalls hfnetchk (dll)
- Englisch
- Remote scan ist möglich !
- Scan nur mit Administrator Rechten

nessus

# Sicherheitsbenchmarks

## MBSA Welcome



# Sicherheitsbenchmarks

## MBSA Pick a computer to scan

The screenshot shows the Microsoft Baseline Security Analyzer (MBSA) interface. The title bar reads 'Microsoft Baseline Security Analyzer'. The main window has a blue header with the Microsoft logo and the text 'Microsoft Baseline Security Analyzer'. On the left, there is a sidebar with a list of options: 'Willkommen', 'Einen Computer zur Überprüfung wählen' (highlighted), 'Mehrere Computer zur Überprüfung wählen', 'Einen Sicherheitsbericht zum Anzeigen wählen', and 'Sicherheitsbericht anzeigen'. Below this is a section 'Siehe auch' with links to 'Microsoft Baseline Security Analyzer-Hilfe', 'Info', and 'Microsoft-Website zur Sicherheit'. The main area is titled 'Einen Computer zur Überprüfung wählen' and contains the following fields and options:

- Computename:** A dropdown menu showing 'BU-TZ\W4DE3ESY0069028' with '(dieser Computer)' next to it.
- IP-Adresse:** A field with four empty boxes separated by dots, followed by a dropdown arrow.
- Name des Sicherheitsberichts:** A text box containing '%D% - %C% (%T%)'. Below it, a legend explains: '%D% = Domäne, %C% = Computer, %T% = Datum und Uhrzeit, %IP% = IP-Adresse'.
- Optionen:** A list of checkboxes:
  - Überprüfung auf Windows-Anfälligkeiten
  - Auf schwache Kennwörter überprüfen
  - Auf IIS-Anfälligkeiten überprüfen
  - Auf SQL-Anfälligkeiten überprüfen
  - Auf Sicherheitsupdates überprüfen
  - SUS-Server verwenden:
    - A dropdown menu showing 'http://berkom-sus.bln05.telekom.de'.

At the bottom of the main area, there is a link 'Weitere Informationen über Überprüfungsoptionen' and a green button with a right-pointing arrow labeled 'Überprüfung starten'. The footer of the window contains the text: '© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. Alle Rechte vorbehalten.'

# Sicherheitsbenchmarks

## MBSA Sicherheitsbericht

Microsoft Baseline Security Analyzer

Microsoft  
**Baseline Security Analyzer**

Microsoft

**Microsoft Baseline Security Analyzer**

- Willkommen
- Einen Computer zur Überprüfung wählen
- Mehrere Computer zur Überprüfung wählen
- Einen Sicherheitsbericht zum Anzeigen wählen
- Sicherheitsbericht anzeigen

**Siehe auch**

- Microsoft Baseline Security Analyzer-Hilfe
- Info
- Microsoft-Website zur Sicherheit

**Aktionen**

Drucken

**Sicherheitsbericht anzeigen**

Sortierreihenfolge: Wertung (schlechteste zuerst)

**Überprüfungsergebnisse für Sicherheitsupdates**

Wertung	Rubrik	Ergebnis
	Windows-Sicherheitsupdates	Einige Sicherheitsupdates konnten nicht bestätigt werden (Anzahl: 1). <a href="#">Gegenstand der Überprüfung</a> <a href="#">Ergebnisdetails</a> <a href="#">Vorgehensweise zur Behebung</a>
	Office-Updates	Es fehlt kein kritisches Sicherheitsupdate. <a href="#">Gegenstand der Überprüfung</a>
	MDAC-Sicherheitsupdates	Es fehlt kein kritisches Sicherheitsupdate. <a href="#">Gegenstand der Überprüfung</a>
	MSXML-Sicherheitsupdates	Es fehlt kein kritisches Sicherheitsupdate. <a href="#">Gegenstand der Überprüfung</a>

**Überprüfungsergebnisse für Windows**

Anfälligkeiten

Wertung	Rubrik	Ergebnis
---------	--------	----------

Vorheriger Sicherheitsbericht Nächster Sicherheitsbericht

© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. Alle Rechte vorbehalten.

# Sicherheitsbenchmarks

## Security Benchmark CIS Solaris

- Der älteste der CIS Benchmarks
- SUN Package
- Gutes Abstimmung zwischen Ergebnisdarstellung und Benchmark Dokumentation

nessus

# Sicherheitsbenchmarks

## Security Benchmark CIS Solaris

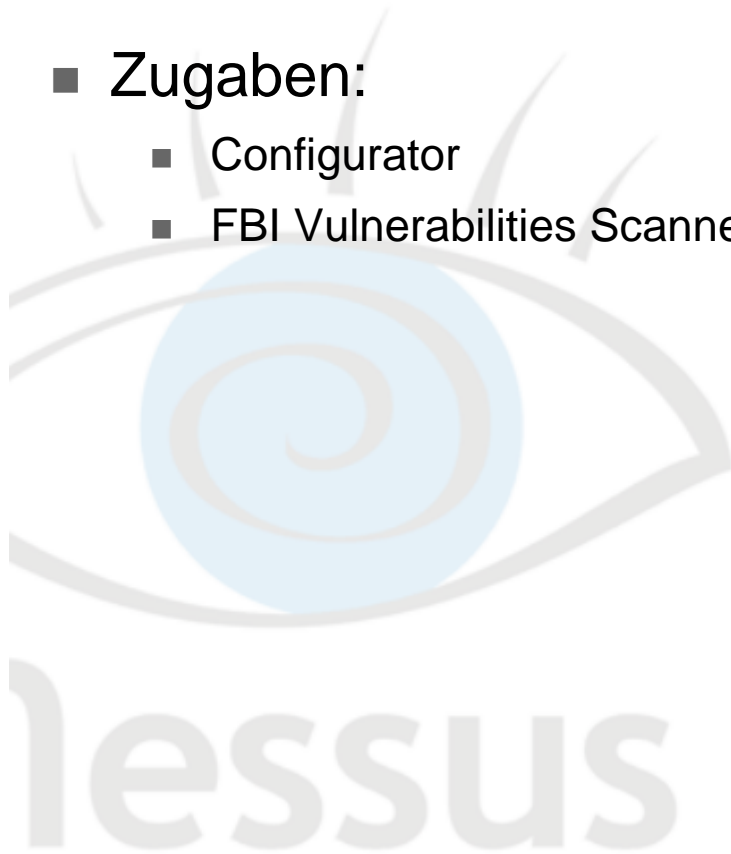
```
*** CIS Ruler Run ***
Starting at time 20020409-14:07:24

Negative: 1.1 System appears not to have been patched within
the last month.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 network printing is deactivated.
Positive: 2.7 rquotad is deactivated.
Positive: 2.8 CDE-related daemons are deactivated.
Positive: 2.9 kerberos net daemons are deactivated.
Positive: 3.1 Miscellaneous scripts are all turned off.
Positive: 3.2 NFS Server script nfs.server is deactivated.
Positive: 3.3 This machine isn't being used as an NFS client.
Positive: 3.4 rpc rc-script is deactivated.
Positive: 3.5 ldap cache manager is deactivated.
Positive: 3.6 The printer init scripts are deactivated.
Positive: 3.7 volume manager is deactivated.
Positive: 3.8 Graphical login is deactivated.
Positive: 3.9 Mail daemon is not listening on TCP 25.
Negative: 3.10 Apache web server rc-script not deactivated.
Negative: 3.11 snmp daemon should be deactivated.
Negative: 3.13 Serial login prompt not disabled.
Negative: 3.12 inetd is still active.
```

# Sicherheitsbenchmarks

## Security Benchmark CIS Solaris

- Zugaben:
  - Configurator
  - FBI Vulnerabilities Scanner



# Sicherheitsbenchmarks

## Zusammenfassung

### *Sicherheit ist ein Prozess*

Standards für die Organisation setzen

Wettbewerb zwischen den Administratoren

Best-practice, Due Diligence, KontrakG, Industriestandard



lessus

# Sicherheitsbenchmarks

Ansprechpartner

Axel Nennker

T-Systems International GmbH

SSC ENPS / Technologiezentrum

Tel: 030 / 34 97 - 3256

Fax: 030 / 34 97 - 3257

email: [axel.nennker@t-systems.com](mailto:axel.nennker@t-systems.com)

lessus Fragen???