

Windows Server 2003/XP

Security Hardening

Jiří Hýzler, MCT, MVP

OKsystem s.r.o.

30/11/06

O čem bude seminář

- **Úvod do bezpečnosti**
- **Baseline security**
 - Group Policy
 - Bezpečnostní šablony
 - Administrativní šablony
 - Security Configuration Wizard
 - Další bezpečnostní nastavení
- **Live technologie**
- **Diskuse**

Security Threats to Servers / Workstations

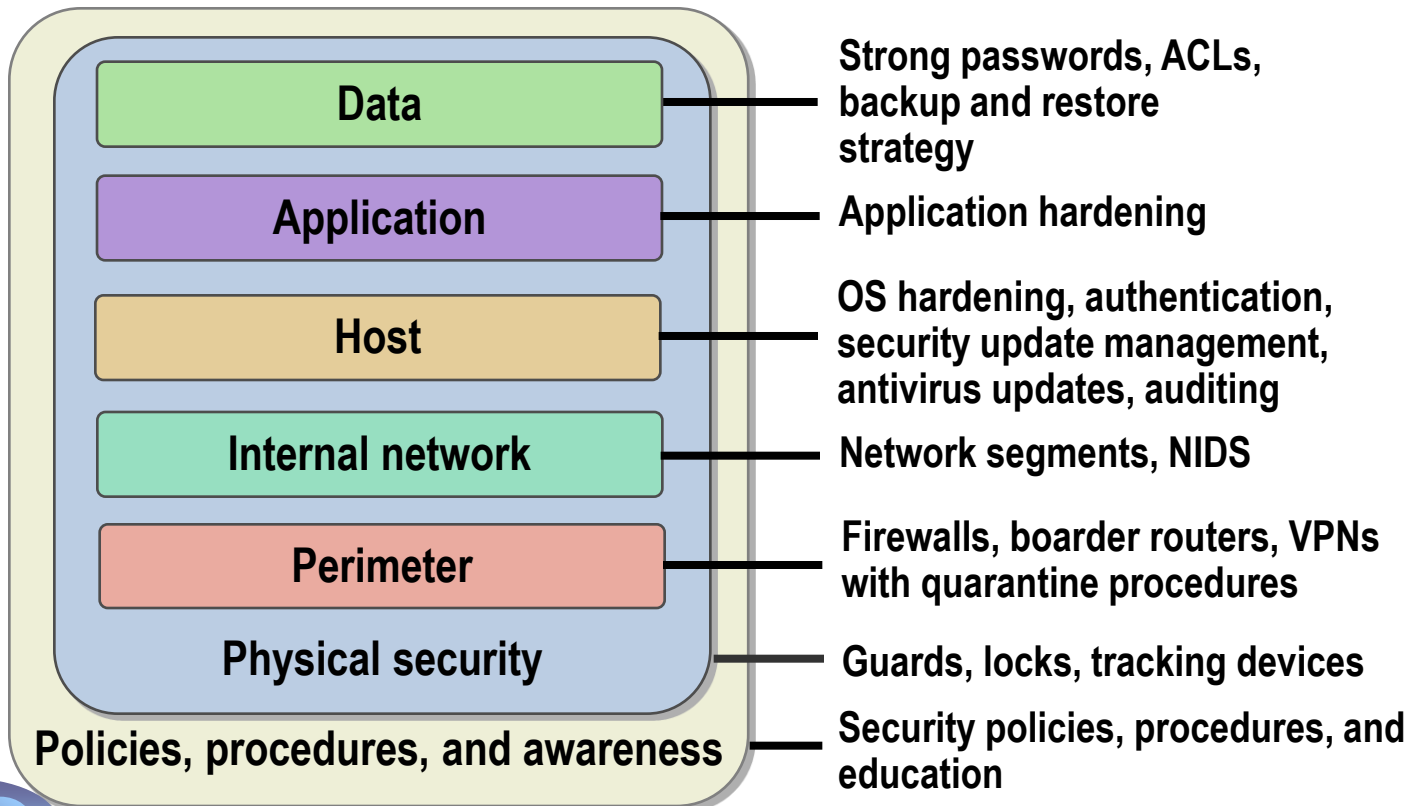
- **Malicious users with physical access to the computers**
- **Denial of service attack**
- **Buffer overrun attack**
- **Viruses, Worms**
- **Trojan horses**
- **Back door attack**
- **Password guessing / Password dictionary / Brute force attack**
- **Logic bomb**
- **Rootkits**
- **Replay attack**
- **Man-in-the-middle attack**
- **Spoofing**
- **Sniffing**
- **Social engineering, ...**

What Is a Defense-in-Depth Approach to computer Security?

Using a layered approach:

Increases an attacker's risk of detection

Reduces an attacker's chance of success



What Is a Secure Member Server Baseline?

A secure baseline:

- Is a detailed description of all relevant configuration settings for a specific computer

Core Server Security Practices :

- Apply the latest service pack and all available security updates
- Use Group Policy to harden servers
- Use MBSA to scan server security configurations
- Restrict physical and network access to servers / Decommission computers securely



Guidelines for Creating a Strong Password Policy

When implementing a password policy:

- Educate users about password requirements
- Consider the use of pass phrases rather than passwords

When enforcing a password policy:

- Use password complexity
- Use Group Policy to control:
 - Maximum password age
 - Password history
 - Minimum password age
 - Password length

Account Lockout Policies vs. DoS

Group Policy Setting	Description
Account lockout threshold	The number of logon attempts that can be made before the account is locked out
Account lockout duration	The number of minutes a locked out account will remain disabled before being automatically enabled
Reset account lockout counter after	The number of minutes that must elapse after a failed logon attempt before the counter is reset to 0 bad logon attempts

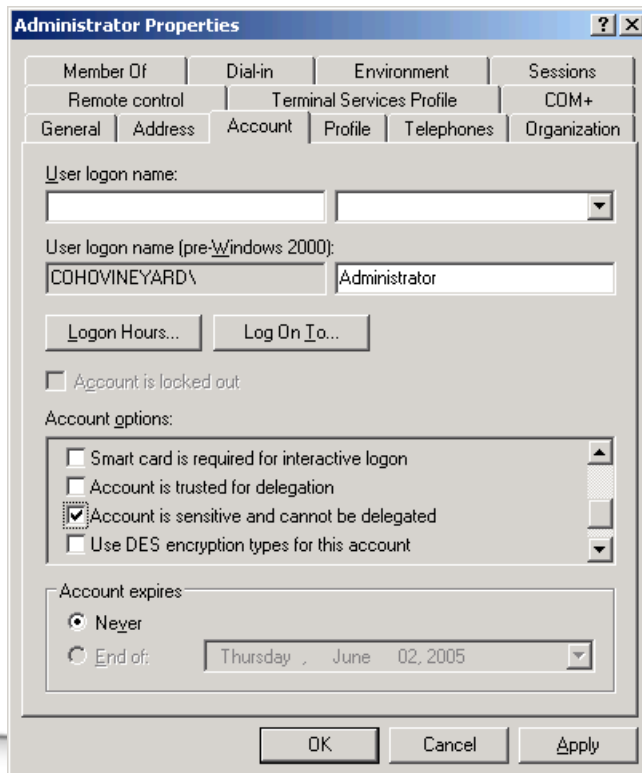
Guidelines for Setting Security for Administrator Accounts

Methods to increase the security of administrative accounts include:

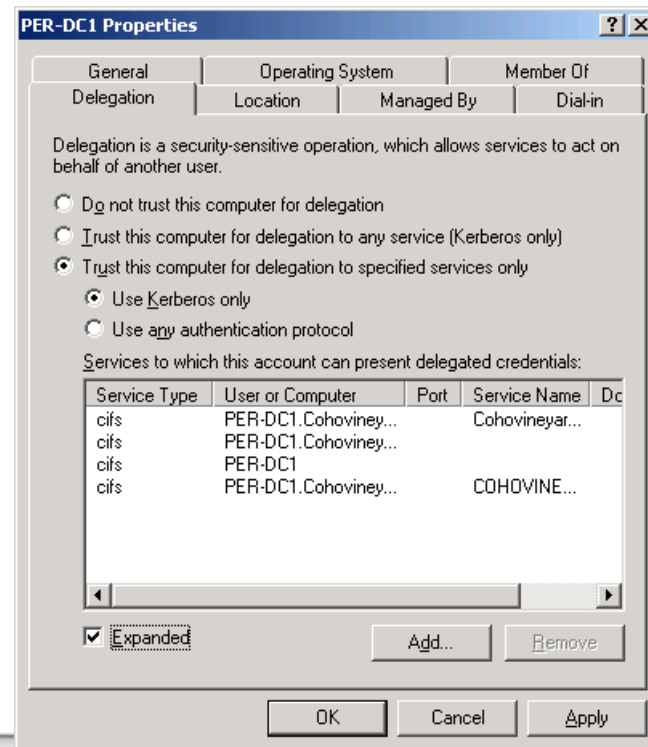
- Limiting the number of administrator accounts to highly trusted personnel
- Separating user and administrative accounts
- Using the secondary logon service
- Disabling the built-in administrator account
- Enforcing strong passwords
- Implementing two-factor authentication

Strategies for Supplemental Authentication

- **Delegated authentication**—Windows services impersonate clients when accessing resources on clients' behalf
- **Constrained delegation**—Computer account is configured so it is delegated for only specific services on the network



The Administrator Properties dialog box is shown with the 'Account' tab selected. The 'User logon name' is set to 'COHOVINEYARD\Administrator'. The 'Account options' section has 'Account is sensitive and cannot be delegated' checked, and 'Account expires' is set to 'Never'.



The PER-DC1 Properties dialog box is shown with the 'Delegation' tab selected. The 'Trust this computer for delegation to specified services only' radio button is selected, with 'Use Kerberos only' chosen. A table lists the services to which this account can present delegated credentials.

Service Type	User or Computer	Port	Service Name	Dc
cifs	PER-DC1.Cohoviney...		Cohovineyar...	
cifs	PER-DC1.Cohoviney...			
cifs	PER-DC1			
cifs	PER-DC1.Cohoviney...		COHOVINE...	

Recommendations for Configuring Auditing on Domain Controllers

Audit policy	Recommended minimum settings
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Only if required by threat model
Audit policy change	Success
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success

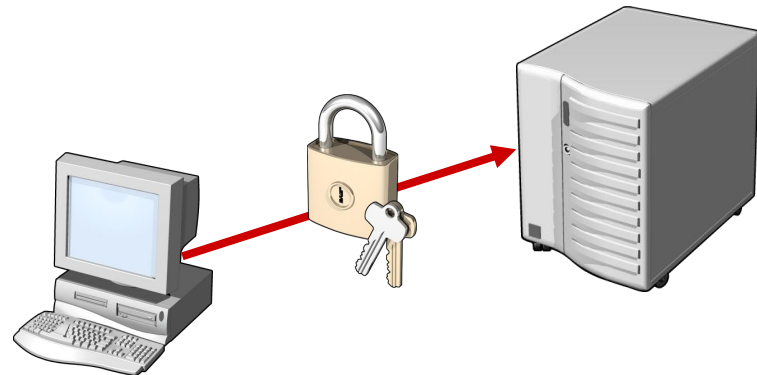
Guidelines for Managing User Rights Assignments

User rights	Add the following members:
Deny access to this computer from the network	<ul style="list-style-type: none">• Built-in Administrator• Support_388945a0• Guest• NON-Operating System service accounts
Deny logon as a batch job	<ul style="list-style-type: none">• Built-in Administrator• Support_388945a0• Guest• NON-Operating System service accounts
Deny logon through Terminal Services	<ul style="list-style-type: none">• Built-in Administrator• Support_388945a0• Guest• NON-Operating System service accounts

Guidelines for Security Options

Secure communication between client and server by configuring the following:

- **SMB signing**
- **LDAP signing**
- **Disable anonymous SAM and share enumeration**
- **Disable caching passwords**
- **Set appropriate NTLM level**



What Is a Restricted Group Policy?

- **Use restricted group policy to control membership**

 - Specify members of a group

 - Members that are not specified in the policy are removed during configuration or refresh

- **To apply restricted group policy**

 - Define the policy using the local computer security policy

 - Define the policy in a GPO that is linked to an organizational unit that contains computer accounts to manage local groups

 - Define the policy in a GPO that is linked to the Domain Controllers OU to manage domain groups

Guidelines for Other Security Settings



Disable unnecessary services / components



Resizing event logs



Use NTFS permissions to secure files and folders



Software Restriction Policy

What Are Software Restriction Policies?

With software restriction policies, you can:

- **Control the ability of software to run on your system**
- **Permit users to run only specific files on multiuser computers**
- **Decide who can add trusted publishers to your computer**
- **Control whether software restriction policies affect all users or just certain users on a computer**
- **Prevent a specific file from running on a local computer, organizational unit, site, or domain**

Rules to Identify Software

Rule	Description
Hash	<ul style="list-style-type: none">● When a software program is opened, a hash of the program is compared to existing hash rules
Certificate	<ul style="list-style-type: none">● Identifies software by its signing certificate
Path	<ul style="list-style-type: none">● Identifies software by its file path
Internet zone	<ul style="list-style-type: none">● Identifies software from a zone that is specified through Internet Explorer

Software Restriction Policy Options

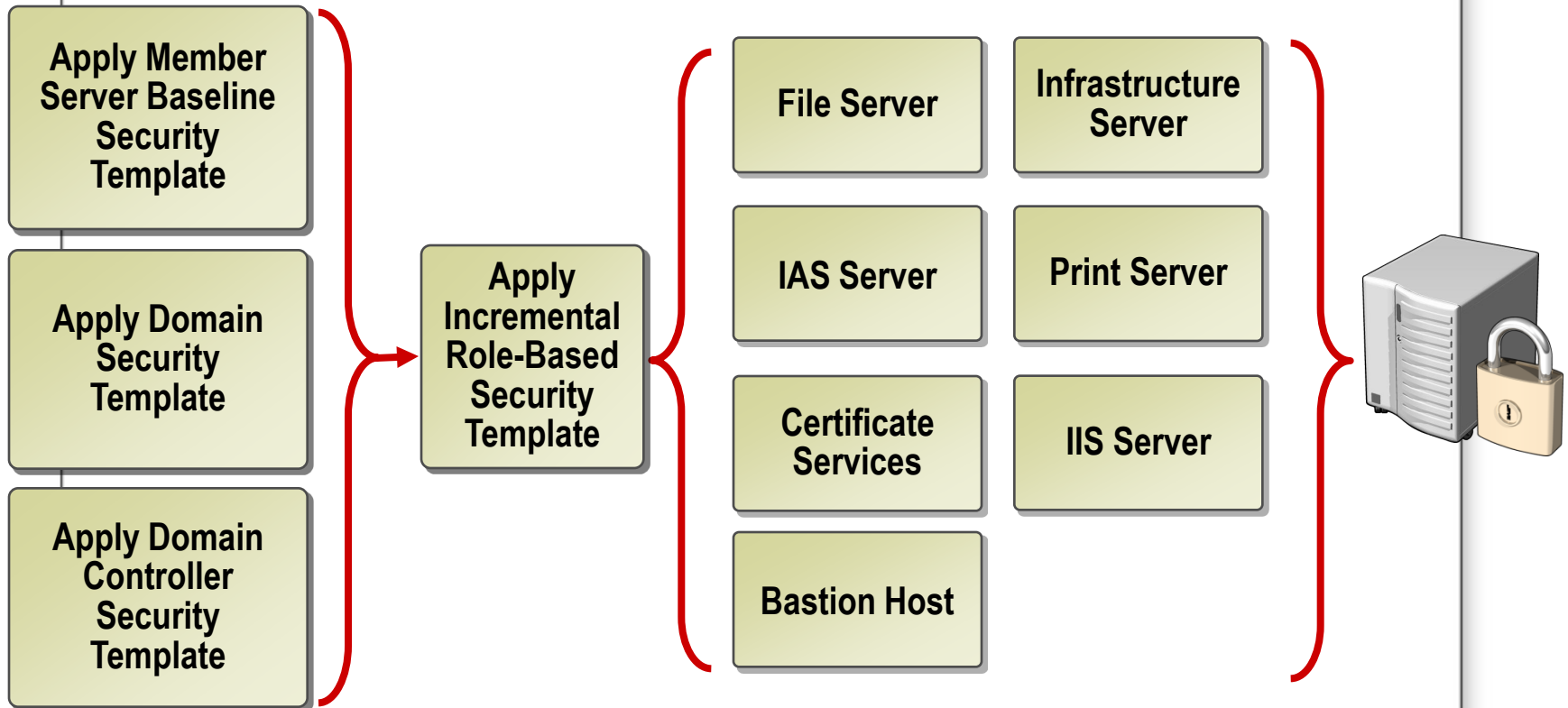
Option	Description
DLL checking	<ul style="list-style-type: none">● Used to ensure that the programs running in your environment are secure
Skip administrators	<ul style="list-style-type: none">● Allows all administrators to run all programs
File types designated as executables	<ul style="list-style-type: none">● Software restrictions can be applied to a file type by adding it to the Designated file types list
Trusted publishers	<ul style="list-style-type: none">● Used to configure which users can select trusted publishers

Predefined Security Templates

Template	Description
Setup security.inf	Specifies default security settings
DC security.inf	Specifies default security settings for a domain controller
Compatws.inf	Modifies permissions and registry settings to enable maximum application compatibility
Securedc.inf and Securews.inf	Enhances security settings that are least likely to affect application compatibility
Hisecdc.inf and Hiseaws.inf	Increases the restrictions on security settings
Rootsec.inf	Specifies permissions for the root of the system drive

Microsoft Windows Server 2003 Security Guide Templates

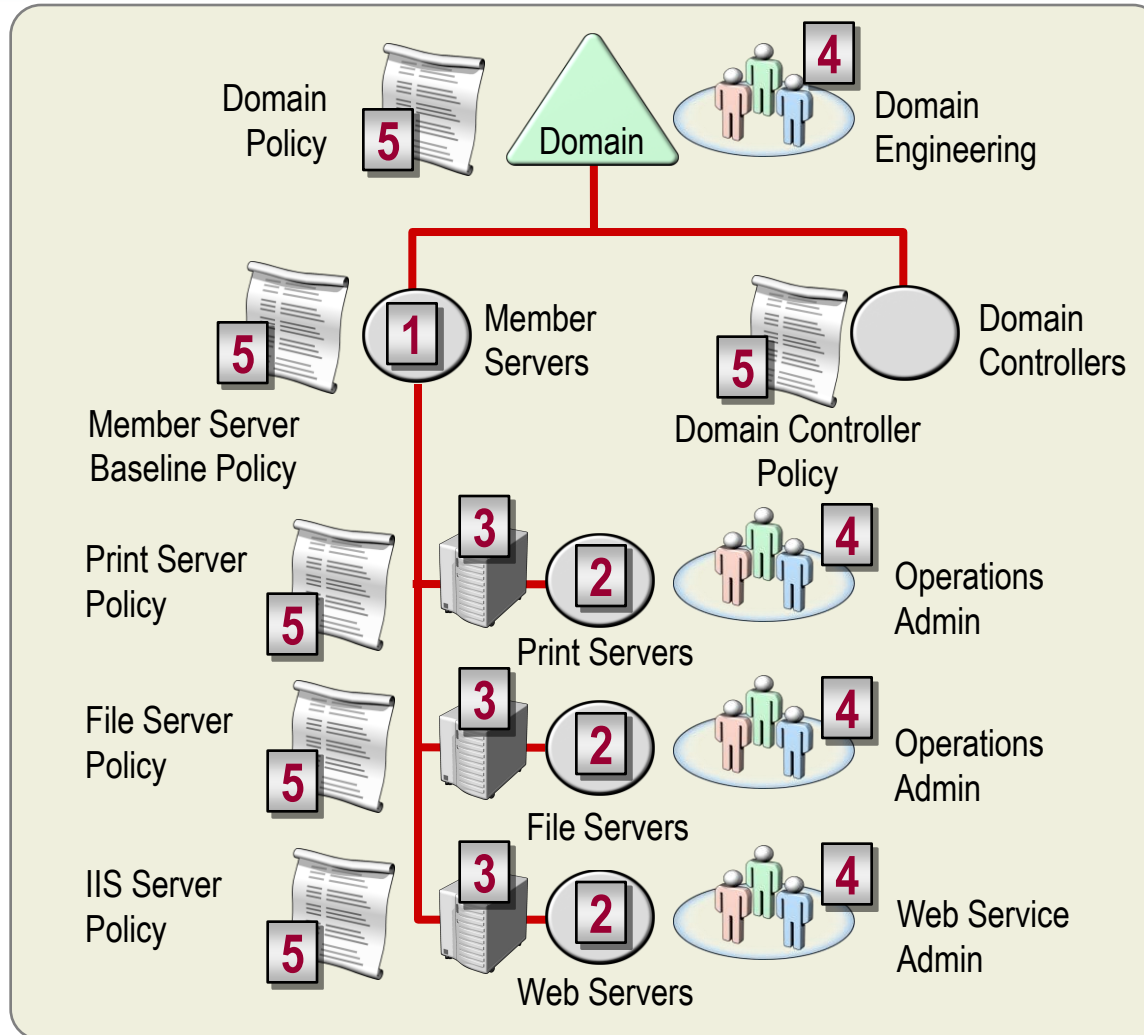
The Windows Server 2003 Security Guide includes the following practices and templates:



Windows XP Security Guide Templates

Template	Description
Enterprise client	Enterprise Client – Desktop.inf Enterprise Client – Laptop.inf
High security	High Security – Desktop.inf High Security – Laptop.inf
Stand-alone	Legacy Enterprise Account.inf Legacy Enterprise Client – Desktop.inf Legacy Enterprise Client – Laptop.inf Legacy High Security Account.inf Legacy High Security – Desktop.inf Legacy High Security – Laptop.inf

Designing a Role-Based OU Hierarchy



Internet Explorer Administrative Templates

Contain a number of security features, such as:






- Security Zone configurations
- Authenticode settings
- Add-on management and restrictions
- File download restrictions
- Pop-up blocker management

- Internet Explorer 7 .adm:

http://www.microsoft.com/downloads/details.aspx?familyid=11AB3E81-6462-4FDA-8EE5-FCB8264C44B1&mg_id=10050&displaylang=en



Internet Explorer Zones

Internet Explorer security zone	Default setting in Windows XP SP2
Internet 	Medium
Local intranet 	Medium-Low
Trusted sites 	Low
Restricted sites 	High
My Computer 	Low

Microsoft Office Administrative Templates

- Enable you to set policies globally for Microsoft Office users connected to a network
- Allow an administrator to quickly enforce a particular user configuration on client computers
- Administrative templates in Office include:

Access11.adm

Excel11.adm

FP11.adm

GAL11.adm

INF11.adm

PUB11.adm

OUTLK11.adm

...



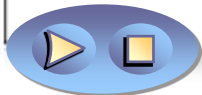
What Is the Security Configuration Wizard?

SCW provides guided attack surface reduction for servers running Windows

- Disables unnecessary services and IIS Web extensions
- Blocks unused ports and secure ports that are left open by using IPSec
- Reduces protocol exposure (LDAP, NTLM, SMB)
- Configures audit settings

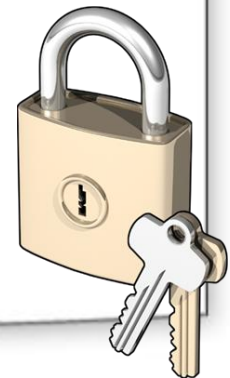
SCW supports:

- Rollback
- Analysis
- Remote configuration
- Command-line support
- Active Directory integration
- Policy editing



Additional Security Settings

- **Disabling error reporting**
- **Disable dump file creation**
- **Support for „no execute“ hardware**
- **TCP/IP Hardening**
<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/HTHardTCP.asp>
- **Desktop firewall**
- **Autoruns, Process Explorer, Rootkit Revealer, ...**
- **AVO, Anti-spyware**
 - Forefront Client Security, Windows Defender



Live technologie



Windows Live™ OneCare™

• <http://safety.live.com>

Odkazy

- **How to use the SysKey utility to secure the Windows Security Accounts Manager database:**
<http://support.microsoft.com/default.aspx?scid=kb;en-us;310105>
- **Windows Deployment and Resource Kits:**
<http://www.microsoft.com/windows/reskits/default.asp>
- **Microsoft Security Home Page:** <http://www.microsoft.com/security/default.msp>
- **Windows Security Home Page:**
<http://www.microsoft.com/windows/security/default.msp>
- **Threats and Countermeasures :**
<http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch00.msp>
- **Software ke stažení:** <http://blogs.technet.com/technetzsk/pages/software-ke-sta-en-z-ms-kuchyn.aspx>
- **„Nové“ sysinternals:** <http://www.microsoft.com/technet/sysinternals/default.msp>
- **Microsoft Forefront Client Security:**
<http://www.microsoft.com/forefront/clientsecurity/default.msp>
- **Windows Defender:**
<http://www.microsoft.com/athome/security/spyware/software/default.msp>

Diskuse

- **Otázky ?**

- **Další informace najdete na:**

<http://www.microsoft.com/cze/technet/chat/default.mspx>

<https://blogs.technet.com/technetczsk/>

<http://support.microsoft.com/newsgroups/>

Školení 2823: Implementace a administrace ve Windows Server 2003 síti



OKsystem

Microsoft
Small Business
Specialist

Microsoft
GOLD CERTIFIED
Partner

Learning Solutions
Networking Infrastructure Solutions