



SICHERHEITSVORLAGE IT-GRUNDSCHUTZ WINDOWS SERVER 2008

Version 1.0 24. April 2013

HiSolutions AG © 2013

– ÖFFENTLICH –





1 ZUSAMMENFASSUNG

Ergänzend zum als Vorabversion erhältlichen IT-Grundschutz-Baustein *Windows Server 2008* hat die HiSolutions AG eine administrative Vorlage (Baseline) erstellt, die die Sicherheitsanforderungen der Grundschutzbausteine

- B 3.101 Allgemeiner Server und
- B 3.109 Windows Server 2008

in Form eines editierbaren Templates zusammenfasst.

Zur Erstellung dieser Vorlage wurde der Microsoft Security Compliance Manager (SCM) verwendet, da dieser ein mächtiges, aber kostenfreies Werkzeug ist, mit dem die Sicherheit von IT-Systemen und Anwendungen mittels Richtlinien optimiert werden kann. Ferner bietet dieses Werkzeug die Möglichkeit, Richtlinien zentral verwalten zu können, und eignet sich daher für den Einsatz sowohl auf Stand-Alone- als auch Domänensystemen.

Das folgende Dokument beschreibt, wie diese Vorlage durch die zuständigen Administratoren einer Organisation gemäß den Unternehmensanforderungen erweitert, angepasst und auf den jeweiligen Systemen installiert werden kann.

Ziel dieser Vorlage soll es sein, dass der zuständige Administrator sich mit den einzelnen Sicherheitseinstellungen unter Windows Server 2008 und Windows Server 2008 R2 auseinandersetzt und dementsprechend abwägt, ob die in der Vorlage vorgeschlagenen Sicherheitseinstellungen für den betrachteten Anwendungsfall sinnvoll sind, oder ob letzterer noch weitere Anpassungen erfordert.

Keinesfalls soll die Vorlage dazu dienen, "out-of-the-box" auf Produktivsystemen installiert zu werden. Dies ist aufgrund der unterschiedlichen Systemkonfigurationen von Windows-Systemen, die in Unternehmen zum Tragen kommen, nicht umsetzbar. In der Regel wird eine Installation dieser Vorlage ohne vorherige Prüfung und adäquate Anpassung zu einem unerwünschten Verhalten der Systeme führen.





INHALTSVERZEICHNIS

1	Ζl	JSAMMENFASSUNG	I				
INHA	LT	SVERZEICHNIS	2				
2	EI	INLEITUNG	3				
3	A	BGRENZUNG	4				
4	B	AUSTEIN WINDOWS SERVER 2008	6				
5	SI	ECURITY COMPLIANCE MANAGER (SCM)	7				
6	V	ORGEHENSWEISE	8				
6.	1	Voraussetzungen für den SCM	8				
6.	2	Aufbau des Security Compliance Managers	9				
6.	3	Importieren der HiSolutions Baseline für Windows Server 2008 R2	10				
6.	4	Anpassen einer Baseline	13				
6.	5	Exportieren einer angepassten Baseline	19				
6.	6	Sperren nach Export der Baseline (Versionsverwaltung)	20				
6.	7	Import der Baseline auf Domänen-Systeme	21				
6.	8	Import der Baseline auf Stand-Alone-Systemen	22				
7	A	NHANG	26				
7.	1	BSI	26				
7.	2	Microsoft	26				
7.	3	Abbildungsverzeichnis	26				
7.	4	Tabellenverzeichnis	26				
7.	7.5 Begriffe 26						
KON	TAł	ΥT	27				





2 EINLEITUNG

Das aktuelle Serverbetriebssystem Windows Server 2008 R2 bringt eine Vielzahl von Konfigurationsmöglichkeiten mit, die den Administratoren für den Einsatz in unterschiedlichsten Unternehmen und Organisationen Spielraum verschaffen, aber auch eine hohe Verantwortung aufbürden, insbesondere aufgrund der Implikationen für die Sicherheit der Systeme. Der Hersteller Microsoft hat zwar je nach ausgewählten Serverrollen bestimmte Voreinstellungen (Default-Werte) gesetzt, die bezüglich der Informationssicherheit bereits eine deutliche Verbesserung zu den Vorgängerversionen darstellen. Trotzdem kommt der Administrator keinesfalls umhin, die Konfiguration an die Bedürfnisse seiner Organisation bezüglich Funktionalität und vor allem Security anzupassen.

Insbesondere, wenn Anforderungen aus dem Bereich Governance, Risk und Compliance (GRC) zu bedienen sind, stellt sich schnell die Frage, welche Einstellungen der Gruppenrichtlinien (Group Policies, oft als "GPO" bezeichnet) einen bestimmten Sicherheitsstandard erfüllen.

Dieses Dokument beschreibt, wie mithilfe der "Sicherheitsvorlage IT-Grundschutz Windows Server 2008" eine IT-Grundschutz-konforme Basiskonfiguration erreicht werden kann.

Im Überblick stellt sich das Vorgehen des Einsatzes der Vorlage – auch Baseline, GPO(s) oder Policy – wie folgt dar:

Import des CAB	Anpassung	Versionskontrolle und Export	Import auf Zielsystem(en)
 Import des CAB in	 Anpassung der	 Abschließend Sperrung	 Import auf
den SCM	bestehenden Einstellungen	der Baseline	Zielsystem(en)
 Duplizierung gemäß	 Ggf. Zufügung eigener	 Export in gewünschtes	 Ggf. weiterer Export
Arbeitsweise des	Einstellungen oder	Format (GPO Backup	von Zielsystem zurück
SCM (siehe Hilfe)	Kategorien	oder SCCM)	in SCM

Dieses Benutzerhandbuch beschreibt die Schritte im Einzelnen. Für detaillierte Hinweise und Fragen zur Bedienung des Security Compliance Managers konsultieren Sie bitte die in diesen integrierte Online-Hilfe.

Es sind zwingend Kenntnisse zur Administration des Active Directory und von Gruppenrichtlinien erforderlich – weder die beschriebene Vorlage noch dieses Handbuch können den Administrator von seiner Pflicht, die Einstellungen anforderungsgemäß und verantwortlich anzupassen, entbinden.

Abweichungen vom IT-Grundschutz sind nach der Methodik des BSI (Standard 100-2) möglich und häufig sinnvoll. Sie sind an geeigneter Stelle zu begründen, etwa bei der Dokumentation der Umsetzung im ISMS-Tool.





3 ABGRENZUNG

Grundsätzlich werden in IT-Grundschutz-Bausteinen technische und organisatorische Maßnahmen betrachtet. Ziel des erstellten Grundschutz-Templates ist es, nur technische Maßnahmen umzusetzen, da eine Betrachtung und Umsetzung organisatorischer Aspekte mittels des Templates nicht möglich ist und auch nicht sinnvoll erscheint. Die Umsetzung organisatorischer Aspekte des Grundschutzes für die jeweiligen Bausteine muss durch den IT-Sicherheitsbeauftragten des jeweiligen Unternehmens ergänzend koordiniert werden.

Das Template berücksichtigt grundsätzlich technische Einstellungen der Maßnahmen des Bausteins.

Allerdings besitzen einige Konfigurationswerte keine Wertzuweisung oder stellen nur eine Basiskonfiguration dar, da letztendlich einige Einstellungen gemäß den Vorgaben des Unternehmens durchzuführen sind. So bietet z. B. die Windows Server 2008-Firewallkonfiguration innerhalb des Templates keine dedizierten Regeln zu IP-Adressen oder Ports an, da hier eine vorherige Betrachtung der auf dem System angebotenen Dienste durch den zuständigen Administrator erfolgen muss. Der Administrator muss dann entscheiden, welche Freigaben für ein- und ausgehenden Verkehr notwendig sind. Dementsprechend muss dies im Template konfiguriert werden.

Im Wesentlichen lassen sich zwei Gruppen von Einstellungsgruppen unterscheiden:

- 1. Einstellungen die zugewiesene Werte wie Passwortlänge besitzen. Diese vorhandenen Werte müssen auf die Umsetzbarkeit innerhalb der Organisation überprüft werden.
- 2. Einstellungen die keine Werte zugewiesen haben, zum Beispiel BitLocker oder NAP. Sollte die Einstellungsgruppe benötigt werden, so sind adäquate Werte zu setzen die die Anforderungen der Organisation berücksichtigen.

Authentication Types - Überprüfung erforderlich 21 Setting(s)		
Microsoft network client: Send unencrypted password to third-party SMB ser	Disabled	Disabled
Network security: Do not store LAN Manager hash value on next password cl	Enabled	Enabled
Interactive logon: Require Domain Controller authentication to unlock works	Disabled	Enabled
Network Security: Restrict NTLM: NTLM authentication in this domain	Not defined	Disable
Interactive logon: Number of previous logons to cache (in case domain contr	10 logons	0 logon(s)

Abbildung 1: Fall 1, Überprüfung der Werte notwendig

Biometrics - Wertzuweisung erforderlich 3 Setting(s)		
Allow users to log on using biometrics	Not Configured	None
Allow domain users to log on using biometrics	Not Configured	None
Allow the use of biometrics	Not Configured	None

Abbildung 2: Fall 2, Zuweisung der Werte notwendig





X

😼 Setting Group Properties

Select Setting Group: Windows Update - Wertzuweisung erforderlich
Name
Windows Update - Wertzuweisung erforderlich
Description:
Sollte diese Einstellungsgruppe benötigt werden, so sind die Detail-Einstellungen mit Wertzuweisungen zu
versehen, die an die Bedürfnisse der Organisation angepasst sind.

Abbildung 3: Beschreibung innerhalb der Setting Group "Properties"

Darüber hinaus werden die technischen Einstellungen der DNS-Server, IIS-Server oder wesentliche Einstellungen des Active-Directorys in diesem Template nicht vertieft, da sie nicht Teil des Bausteins Windows Server 2008 sind.

Bei Bedarf, können aber SCM-Einstellungen zu diesen Server-Rollen oder Erweiterungen durch den Anwender des Templates zugefügt werden.

Wichtig ist, dass das Template erst auf ein System angewendet werden darf, nachdem es zuvor durch einen zuständigen Administrator gesichtet und angepasst wurde. Die Installation auf einem Produktivsystem sollte erst nach vorheriger Prüfung auf einem Testsystem erfolgen.

Das vorliegende Dokument stellt kein Handbuch zur Bedienung des Security Compliance Managers dar. Hierfür bietet die in den Security Compliance Manager integrierte Hilfefunktion eine adäquate Grundlage.

Der Security Compliance Manager ist gegenwärtig nur in englischer Sprache erhältlich. Dies stellt allerdings kein Kompatibilitätsproblem dar, da bei einem Import der Vorlage auf einem System mit deutschen Regions- und Spracheinstellungen für alle Einstellungen automatisch ein Mapping erfolgt.





4 BAUSTEIN WINDOWS SERVER 2008

Der Baustein Windows 2008 ist eine weitere Ergänzung zu den bereits im IT-Grundschutz betrachteten Server-Betriebssystemen und wird als Bestandteil der 13. Ergänzungslieferung der IT-Grundschutzkataloge des BSI veröffentlicht werden. Momentan liegt er nur in einer im Juni 2012 veröffentlichten Vorabversion¹ vor, die noch nicht in der aktuellen Ausgabe (12. Ergänzungslieferung) der Kataloge enthalten ist.

Der Baustein bietet einen Überblick über die aktuelle Gefährdungslage und liefert passende organisatorische sowie technische Maßnahmen zur Erlangung eines normalen Schutzbedarfs sowohl für Windows Server 2008 als für das 2009 erschienene, parallel zu Windows 7 entwickelte Windows Server 2008 R2. Die vorliegende Sicherheitsbaseline konzentriert sich zwar auf letzteres, lässt sich aber auch für Windows Server 2008 anpassen und nutzen.

Im Vergleich zum bereits in der 12. Ergänzungslieferung vorhandenen Baustein "B 3.108 Windows Server 2003" sind zusätzlich im Baustein "Windows Server 2008" die folgenden neuen Maßnahmen vorhanden:

- M 2.x-1 (A) Planung der Systemüberwachung unter Windows Server 2008
- M 2.x-3 (C) Planung des Einsatzes von Virtualisierung durch Hyper-V
- M 4.x-1 (A) Planung des Einsatzes von Windows Server 2008
- M 4.x-2 (W) Übersicht über neue, sicherheitsrelevante Funktionen in Windows Server 2008
- M 4.x-3 (W) Beschaffung von Windows Server 2008
- M 2.x-4 (B) Nutzung von Rollen und Sicherheitsvorlagen unter Windows Server 2008
- M 4.W7-xx3 (Z) Anwendungssteuerung ab Windows 7
- M 4.x-4 (Z) Einsatz von Netzwerkzugriffsschutz unter Windows
- M 4.x-6 (Z) Sichere Migration von Windows Server 2003 auf Windows Server 2008
- M 4.x-7 (Z) Sicherer Einsatz von Virtualisierung mit Hyper-V
- M 4.x-5 (Z) Sichere Nutzung von DirectAccess unter Windows
- M 4.x-9 (Z) Sicherer Betrieb der biometrischen Authentisierung unter Windows
- M 4.x-10 (Z) Einsatz von Windows Server Core
- M 4.x-11 (B) Patch-Management mit WSUS ab Windows Server 2008





5 SECURITY COMPLIANCE MANAGER (SCM)

Gruppenrichtlinien sind mit die wichtigsten Werkzeuge in Windows-Umgebungen, um eine angemessene Absicherung der Systeme erzielen zu können. Ein Werkzeug für die Verwaltung von Gruppenrichtlinienobjekten unter Windows Client- und Serversystemen ist der Security Compliance Manager (SCM) von Microsoft. Dieser soll dabei unterstützen, von Microsoft und Drittanbietern empfohlene Sicherheitsrichtlinien unternehmens- oder organisationsweit durchzusetzen. Er gehört zur Gruppe der von Microsoft frei zum Download angebotenen "Solution Accelerators", welche Aufgaben rund um die Planung und das Deployment von Systemumgebungen und Anwendungen unterstützen.

Der SCM stellt bereits nach der Installation eine Vielzahl von aktuellen Baselines für Windows-Betriebssysteme und Anwendungen bereit, die entsprechend den Sicherheits- und Compliance-Anforderungen einer Organisation angepasst und erweitert werden können. Bei einer Baseline handelt es sich um eine Sammlung relevanter Sicherheits- und Konfigurationseinstellungen (engl. Configuration Items), die letztendlich zur Gesamtsicherheit des jeweiligen Systems beitragen sollen.

Die Auswahl an Baselines beschränkt sich nicht auf einzelne Produkte und Versionen, sondern ist zudem nach Anwendungsrollen und Sicherheitsanforderungen unterteilt. So gibt es eigene Vorlagen für File- und Web-Server, Hyper-V, Domänen-Controller oder die Remote Desktop Services. Außerdem liegen die Baselines für Windows XP, Vista und 7 in den Ausführungen *Specialized Security – Limited Functionality* (für hohe Sicherheitsanforderungen) sowie *Enterprise Client* oder auch für Notebooks vor.

In der für dieses Projekt verwendeten Beta Version 3 des SCM werden neben Windows 7 und Windows 2008 Server-Systemen mittlerweile auch Windows 8 und Windows Server 2012 unterstützt. Ebenfalls liegen diverse Baselines für verschiedene Versionen von Microsoft-Anwendungen wie den Internet Explorer, Microsoft Office und Exchange Server vor.

Die wichtigsten Funktionen des Security Compliance Managers sind im Folgenden dargestellt:

- Absicherung mehrerer Microsoft Produkte (Windows Server, Office, Exchange Server, Internet Explorer)
- Zentrale Speicherung und Verwaltung von Baselines
- Möglichkeit, die Baselines auf Stand-Alone- und Domänensystem zu nutzen
- Vergleich und Zusammenführung (Merge) von Baselines
- Verschiedene Import- und Exportmöglichkeit von Baselines





6 VORGEHENSWEISE

6.1 Voraussetzungen für den SCM

Die folgende Tabelle enthält die Systemanforderungen für den Security Compliance Manager:

Die erstellten CAB-Dateien lassen sich sowohl mit der aktuellen Version 2.5 als auch mit der Betaversion 3 des SCM bearbeiten.

Betriebssystem	Windows® 7 x64		
	Windows Server® 2008 oder Windows Server® 2008 R2		
Benötigter Arbeitsspeicher	500 MB		
Zusätzlich benötigte Software	Microsoft® .NET Framework 4		
	Microsoft SQL Server® 2005, SQL Server® 2008 oder SQL		
	Server® 2008 R2 ²		
	Microsoft Excel® 2007 oder später (optional für Export).		
Rechte	Administratorrechte werden für die Installation des SCM benötigt.		
	Des Weiteren benötigt auch das Tool LocalGPO für den Import von Vorlagen administrative Rechte.		

Es wird empfohlen, den SCM auf Windows 7 oder Windows Server 2008 R2 zu installieren.

Nach der Installation muss der SCM über das Windows-Startmenü gestartet werden. Das erstmalige Einlesen der Vorlagen und Richtlinien nimmt gegebenenfalls einige Minuten in Anspruch.

² Sofern kein Microsoft SQL Server oder SQL Server Express auf dem Zielsystem vorhanden ist, wird letzterer während der SCM-Installation mitinstalliert, und es wird eine Instanz für den SCM eingerichtet.





6.2 Aufbau des Security Compliance Managers

Die folgende Grafik illustriert den Aufbau des Security Compliance Managers:

Microsoft Security Compliance Manager	VEISE						
ile View Help							Global setting search
Custom Baselines IF GPO Import IF Windows 7 SP1 IF Windows Gener 2008 R2 SP1 IF Windows Gener 2007 SP3 IF Exchange Server 2007 SP3	WS2008SP2 Member Server Securit Advanced View Name	WS2008SP2 Member Server Security Compliance 1.0 249 unique setting(s) Advanced View Image: Severity Path					Import <u>GPO Backup (folder)</u> <u>SCM (cab)</u> Export
Exchange Server 2010 SP2 Internet Explorer 8 Internet Explorer 7 Microsoft Office 2007 SP2 Microsoft Office 2010 SP1 Windows Server 2008 R2 SP1 Windows Server Security Compliance 1.0 WS20085P2 DNC Server Security Compliance 1.0 WS20085P2 DDC Server Security Compliance 1.0 WS20085P2 DDC Server Security Compliance 1.0 WS20085P2 DNC Server Security Compliance 1.0 WS20085P2 Pile Server Security Compliance 1.0 WS20085P2 Pile Server Security Compliance 1.0 WS20085P2 Pile Server Security Compliance 1.0 WS20085P2 Hencer Server Security Compliance 1.0 WS20085P2 Immediate Services Server Security Compliance 1.0 WS20085P2 Immediate Services Server Security Compliance 1.0 WS20085P2 Immediate Services Service Server Security Compliance 1.0 WS20085P2 Immediate Services Security Compliance 1.0 Windows VS4 SP3 Windows Server 2028 R2 SP1 Windows Server 2008 R2 SP1	Authentication Types 12 Settin RPC Endpoint Mapper Client Authent Network security: Do not store LAN N Network security: Minimum session s Interactive logon: Number of previou Network security: Minimum session s Interactive logon: Require smart card Microsoft network client. Send unenc Interactive logon: Require Domain Cc Interactive logon: Require Domain Cc Interactive logon: Require Domain Cc Interactive logon: Smart card remove Network security: LAN Manager auth Control Configuration 14 S Domain member: Digitally encrypt os System cryptography: Force strong k Set client connection encryption leve Network security: Minimum session s Microsoft network client: Send unenc Domain member: Digitally sign secur Domain member: Digitally sign	g(s) Disabled Enabled No minimum 25 logons No minimum Disabled Disabled Send NTLMv2 resj Setting(s) No minimum	Not Configured Enabled Require NTLMv2 : 0 logon(s) Require NTLMv2 : Not Defined Disabled Lock Workstation Disabled Not Configured Send NTLMv2 rest Enabled Require NTLMv2 rest Disabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled	Not Configured Require NTLMv2 : 0 logon(s) Require NTLMv2 : Not Defined Disabled Lock Workstation Disabled Not Configured Send NTLMv2 resp Enabled Require NTLMv2 resp Not Defined Not Configured Require NTLMv2 : Disabled Enabled Enabled Enabled Enabled Enabled Enabled Enabled	Importan Critical Critical Critical Importan Critical Importan Critical	Computer Configuration Computer Configuration	Excel (xism) GPO Backup (folder) SCAP v10 (cab) SCM (cab) SCM (cab) Baseline Compare / Merge Pelete Puplicate Properties Setting Setti

Abbildung 4: Aufbau des SCM

Auf der linken Seite erfolgt die Auswahl des abzusichernden Produkts. Nachdem ein entsprechendes Produkt ausgewählt worden ist (hier Windows Server 2008 SP2), erscheinen im mittleren Bereich die gesetzten Einstellungen.

Um die Konfigurationseinstellungen der gewählten Baseline anpassen zu können, muss diese zunächst mit dem Befehl "*Duplicate*" im rechten Bereich *Baseline* dupliziert werden. Die neue Richtlinie erscheint dann abschließend im Bereich "Custom Baselines" im oberen Bereich des linken Fensters.

Anschließend können die Einstellungen in der Richtlinie gemäß den jeweiligen Sicherheitsanforderungen angepasst werden. Durch Klicken auf eine Zeile innerhalb des SCM werden die einzelnen Konfigurationseinstellungen für das gewählte Objekt eingeblendet (siehe Abbildung 5). Microsoft stellt für jede Einstellung ausführliche Informationen bereit, die sich folgendermaßen untergliedern lassen:

- UI-Pfad
- Beschreibung
- Weitere Details (meist wird hier auf eine entsprechende CCE-ID³ verwiesen)
- Schwachstelle
- Auswirkungen
- Gegenmaßnahmen

³ Common Configuration Enumeration, siehe <u>http://cce.mitre.org/</u>.





Tre Microsoft Security Compliance Manager	the second se		
File View Help			
pm Baselines PO Import findows 7 SP1 findows Server 2008 R2 SP1 Attachments \ Guides Form of Serving Settinger WC2008 R2 26 1	Copy of Security Settings WS2008 R2 26.10.2012 1.0 517 unic 	que setting(s) Default Microsoft Customized Severity Path	Import GPO Backup (folder) SCM (cab) Export
Eggy of Security Settings WS2008 R2 261 soft Baselines cchange Server 2007 SP3 (change Server 2000 SP2 ternet Explorer 8 ternet Explorer 8 licrosoft Office 2007 SP2 licrosoft Office 2007 SP2 findows Server 2008 SP1 findows Server 2008 R2 SP1 findows Vista SP2 findows Vista SP2 findows Vista SP2 ternet Explorer 10 findows Server 2012 r Baselines findows Server 2012 r Baselines	Name Enforce password history Collapse Value must be equal to 6 password(s). Not Defined Comments: Customize setting value passwords arrange from 0 to 9999. Setting Details UI Path: Computer Configuration\Windows Settings\Security Settings\Account Description: This policy setting determines the number of renewed, unique passwords hat have to be associated with a user account before you can reuse an old passwords. The value for this policy setting must be between 0 and 24 passwords. The value for this policy setting windows Yotis is 0 passwords. The default value for Windows Yotis is 0 passwords. The default value for Windows Yotis is 0 passwords. The default value for windows Yotis is 0 passwords. But the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting repeatedly changing their password. Additional Details:	Default Microsoft Curtomized Severity Path 24 passwords rem 6 passwords Critical Computer Cont Critical • • • • M 4.48 Passwords ruter NT-basierten Windows-5; • • • Policies/Password Policy • • • • Vulnerability: The longer a user uses the same password, the greater the chance that an attacker can determine the password hough brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password ruse is not prevented, or if users continually reuse as mall number of passwords repasted). If you specify a low number for this policy setting, users will be able to use the same small number of passwords repasted). If you on tha loo configure the Minimum password as exiting, users might	Export Excel (Jam) GPD Backup (folder) SCAP VL0 (Loab) SCM (Loab) SCM (Loab) SCM (Loab) Compare/Merge Delete Duplicate Lock Properties Setting Add Delete Move Setting Group Add Delete Properties Add Delete Properties Add Delete Properties About Help About Help About Help About Help About Help About Help Settement
	CCE-10809-2 Namespace: rootirsopicomputer Property: Setting Class: RSOP_SecuritySettingNumeric Where: KeyName='PasswordHistorySize' And precedence=1	repeatedly change their passwords until they can reuse their original password. Potential Impact: The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords, somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password) assword age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently. Countermeasure:	
	Minimum parenueri leeeth	Configure the Enforce password history setting to 24, the maximum setting, to help minimize the number of vulnerabilities that are caused by password reuse. For this setting to be effective in your organization, do not allow passwords to be changed immediately when you configure the Minimum password age setting. The Enforce password history value should be set at a level that combines a reasonable maximum password age with a reasonable password change interval requirement for all users in your organization.	
4 <u>m</u> >	Minimum password age	0 days 1 day(s) Critical Computer Conf	

Abbildung 5: Detaillierte Konfigurationseinstellungen

Es empfiehlt sich immer, eine bereits bestehende Baseline anzupassen, da bei dieser im Vergleich zu einer leeren Gruppenrichtlinie bereits Sicherheitsempfehlungen von Microsoft enthalten sind, welche zu einer Grundsicherheit des Systems beitragen.

6.3 Importieren der HiSolutions Baseline für Windows Server 2008 R2

Nach der Installation des SCM muss die von HiSolutions in Form einer CAB-Datei bereitgestellte Baseline für Windows Server 2008 R2 in den SCM importiert werden. Die Grafiken in Tabelle 2 veranschaulichen die Vorgehensweise.





Tabelle 2: Vorgehensweise zum Import einer Baseline

Zum Importieren der	Ty Microsoft Security Compliance Mana	ger	ارما
Baseline im Import-	File View Help		Global setting :
Bereich auf SCM (cab)	Windows Server 2008 R2 SP1 GPO Import	Microsoft Solution	GPO Backup (folder)
klicken. Der Import	Windows 7 SP1 Microsoft Baselines Exchange Server 2007 SP3	Security Compliance Manager (SCM) 3.0 Accelerators	SCM (.cab) Help
Baselines Wizard öffnet	Exchange Server 2010 SP2 Internet Explorer 8 Internet Explorer 8	Welcome to SCM Getting started with SCM	About Help Topics
sich.	Microsoft Office 2007 SP2 Microsoft Office 2010 SP1 Microsoft Office 2010 SP1		Release Notes Send Feedback
	Windows Server 2003 SP2 Windows Server 2008 R2 SP1 Windows Server 2008 R2 SP1	What's new in this release Windows 8 and IE 10 baselines	Privacy Statement
	Windows Server 2008 SP2 Windows Vista SP2 Windows XP SP3	Windows Server 2012 baselines Download Microsoft baselines manually	
	▷ Internet Explorer 10 ▷ Windows 8	Setting library enhancements Import a Microsoft baseline More SCM 3.0 beta baselines Import a Group Policy Backup	
	Windows Server 2012 Other Baselines Windows Server 2008 R2 SP1		
	Windows 7 SP1	How to perform common tasks 💿 🕝 Customize knowledge 💿	
		Import a Group Policy Backup ring settings Customize knowledge Evaluate Microsoft recommendations	
		Export knowledge Customize baselines Compare with Microsoft recommendations	
		Compare and merge baselines	
		Working with SCM 💿 🥝 Export knowledge 🔗	
		Navigating SCM GPO backups LocalGPO command-line tool DCM Configuration Packs	
		Setting management SCAP data files	
		Setting details Interosoft excel workbooks	
Auf Add" klicken und	Ty Import Baselines Wizard		
die zu importierende	6	last naskana filas	
Baseline auswählen.	Se Se	lect package files	
		This wizard helps you import baselines into the Microsoft Security Compliance Manager tool.	
	Select package files	Package	
	Baseline details	Add	
	Results		
		Remove	
		Package Version:	
		Package Description:	
		Back Next Cancel	





Moitor mit Novt"	Import Baselines Wizard		23				
		last naskana filas					
	Se Se	нест раскаде files					
	9	This wizard helps you import baselines into the Microsoft Security Compliance Manager tool.					
	Select package files	Package D\\Benutzerprofil\alexanderp\Desktop\MS\Security_Settings_WS2008_R2_23_20_2012_2.cab					
	Baseline details		Add				
	Nesuits						
			Remove				
		× [] >					
		Package Version: 1.0					
		Package Description:					
		Back Next	Cancel				
Es folgt eine	🙀 Import Baselines Wizard	1					
Zusammenfassung der	Baseline details						
Baseline-Details.	N						
Die Option "Create	Select package files	Security Settings WS2008 R2 23.20.2012_2.cab					
modifiable copies of	Baseline details	Security Settings WS2008 R2 21.20.2012					
imported" auswählen	Results						
erlaubt es die							
importierte Baseline							
gemäß den		Description:					
Sicherheitsanforderung		The AD - Certificate Services baseline includes settings required to enable the AD - Certificate role.	Services server				
en des Unternehmens							
Standard-Baselines		Publisher: Custom					
schreibgeschützt sind		Name Description	*				
und immer unverändert		System Services					
bleiben. Die editierbare		Password Attributes Authentication Types	Ψ.				
dann unter der Rubrik		Create modifiable copies of each baseline to be imported.					
"Custom Baselines".							
Abschließend die		Back Import	Cancel				
Baselines mittels des							
"Import" Befehls							
importieren.							
Ggf. muss eine							
Abfrage, ob die							
Baseline importiert							
werden soll, obwohl sie							
dem System							
dom bystom	I						





vorhanden ist, mit "OK" bestätigt werden.							
Nachdem der Import erfolgreich abgeschlossen ist, erscheint die entsprechende	Ty Import Baselines Wizard Results Penter auschmeden This wizard helps you import baselines into the Microsoft Security Compliance Manager tool. 4 Council: Continue Microsoft Da 23 20 2012 3 art						
Statusmeldung. Zum Beenden auf <i>"Finish"</i> klicken.	Baseline details Results	 Security Settings WS2008 R2 22.20.2012 was imported successfully. Security Settings WS2008 R2 21.20.2012 was successfully duplicated. 					
		Back	Import Finish				

6.4 Anpassen einer Baseline

Nachdem die im vorherigen Abschnitt beschriebenen Schritte zum Importieren der Baseline durchgeführt worden sind, müssen die in der Grundschutz-Vorlage vorkonfigurierten Einstellungen durch den zuständigen Server-Administrator überprüft und bei Bedarf an den Unternehmenseinsatz und die entsprechenden Unternehmensrichtlinien (z. B. die Passwortrichtlinie) angepasst werden.

Es empfiehlt sich hierbei, schrittweise alle im Template vorhandenen Kategorien (siehe Tabelle 4) mitsamt allen Einstellungen durchzugehen, diese zu evaluieren und gegebenenfalls auf einen adäquaten Wert anzupassen.

Diese Vorgehensweise ist insofern notwendig, da in dem entsprechenden Grundschutz-Baustein diverse Neuerungen beschrieben werden, diese aber nicht immer unbedingt auf den jeweiligen Systemen benötigt werden. Aus diesem Grund sind für solche Fälle meist noch die Default-Einstellungen oder von HiSolutions empfohlene Einstellungen aktiv bzw. noch nicht konfiguriert und benötigen daher eine weitere Anpassung. Dies betrifft zum Beispiel die Einstellungen in den Kategorien Biometrie, IPsec, Network Access Protection etc.

Um den Bezug zu den BSI-Grundschutzbausteinen kenntlich zu machen, erfolgt innerhalb des Templates im Kommentarfeld (*Comments*) zu jeder Konfigurationseinstellung eine Zuordnung der Einstellung zu einer oder mehreren Grundschutzmaßnahmen der beiden BSI-Bausteine B 3.101 Allgemeiner Server und B 3.109 Windows Server 2008.





WARNUNG: Vor Applizieren einer Baseline auf einem Produktivsystem müssen sämtliche Einstellungen durch den Systemadministrator verifiziert werden. Eine Verteilung der Baseline ohne vorherige Prüfung kann die Funktionalität der betroffenen Systeme beeinträchtigen. Es wird daher dringend empfohlen, eine Baseline und sämtliche Änderungen von Einstellungen vorher auf einem Testsystem umfassend zu testen.

Siehe dazu auch: G 3.81 Unsachgemäßer Einsatz von Sicherheitsvorlagen ab Windows Server 2003

Wenn Sicherheitsvorlagen auf einem Server eingespielt und aktiviert werden, dann besteht die Gefahr, dass bestimmte Funktionen oder der ganze Server nicht mehr verfügbar sind. Werden Sie mit Hilfe von Gruppenrichtlinien oder Skripten automatisch auf mehrere Server ausgerollt, kann der Betrieb im betrachteten IT-Verbund gestört werden und sogar vollständig ausfallen.

Tabelle 3: Anpassen einer Baseline

besteht darin, dass die Einstellungen der Richtlinie an die Bedürfnisse der Organisation angepasst werden.	Der nächste Schritt							
Description Understand * Windows 2012 Statements Statemen	hastaht darin dass dia	File View Help						
Einstellungen der Richtlinie an die Bedürfnisse der Organisation angepasst werden.	Desterit darin, dass die	Custom Baselines Custom> - <security 26.10.2012="" r2="" settings="" ws2008=""> 1.0 517 unique s</security>				517 unique setting(s)		
Richtlinie an die Bedürfnisse der Organisation angepasst werden. I weicher 39t Bedürfnisse der Organisation Bedürfnisse der Organisation Bedürfnisse der Die State Bedürfnisse der Die State Bedürfn	Einstellungen der	Attachments \ Guides Copy of Security Settings WS2008 R2 26.10.2012 1.0	Advanced View					
A monost fiscation Bedürffnissee der Organisation angepasst werden. A monost fiscation A monost fiscation <p< th=""><th>Richtlinie an die</th><th>P GPO Import Vindows 7 SP1</th><th>Name</th><th>Default</th><th>Microsoft</th><th>Customized</th><th>Severity</th><th>Path</th></p<>	Richtlinie an die	P GPO Import Vindows 7 SP1	Name	Default	Microsoft	Customized	Severity	Path
Bedurfmisse der Organisation angepasst werden. Extrage Amer 2003 93 Extrage Amer 2003 93 Marre Extrage 1000 Marre Extrage 1000 Marre Extrage 1000 Marre Extrage 1000 Marre Extrage 1000 Marre Extrage 1000 Marre Extrage 1000 Marre Extrage 1000 Marre Extrage 1000 Marre Extrage 1000 Marre Extrage 10000 Marre Extrage 10000 Marre Extrage 100000 Marre Extrage 1000000 Marre Extrage 1000000000000000000000000000000000000		 Microsoft Baselines 	Account Lock 3 Setting(s)					
Organisation Accurt lockst threshold 0 mail logons at 10 ma	Bedurfnisse der	 Exchange Server 2007 SP3 Exchange Server 2010 SP2 	Reset account lockout counter after	r O		60 minute(s)	Critical	Computer Configuration\Windows Si
Accurat locked duration Note defined 15 minutely Cited Computer Configuration/Windo angepasst werden. Interactive logon Statustion Note defined Daabed Cited Computer Configuration/Windo Windows Server 2008 52 591 Win	Organization	Internet Explorer 8	Account lockout threshold	0 invalid logon at!		10 invalid logon a	Critical	Computer Configuration\Windows S
Angepasst werden. I Moroso Tolice 200 SP1 Vindows 789 Vindows	Organisation	Internet Explorer 9 Microsoft Office 2007 SP2	Account lockout duration	Not defined		15 minute(s)	Critical	Computer Configuration\Windows S
Image process in work control Image process in work control based Daabed Critical Computer Configuration/Windo Image process in work control based Daabed Critical Computer Configuration/Windo Image process in work control based Daabed Critical Computer Configuration/Windo Image process in work control based Daabed Critical Computer Configuration/Windo Image process in work control based Daabed Critical Computer Configuration/Windo Image process in work control based Daabed Critical Computer Configuration/Windo Image process in work control based Daabed Critical Computer Configuration/Windo Image process in work control based Daabed Critical Computer Configuration/Windo Image process in work control based Daabed Critical Computer Configuration/Windo Image process in work control based Daabed Image process in an intervant Collabled Daabed Importal Configuration/Windo Image process in work control based Daabed Image process in an intervant Collabled Daabed Importal Configuration/Windo Image process in work control based Daabed Importal Configuration/Windo Network security Relin Window Relin work security Relin Window Relin work security Relin Window Relin work security Relin	angenasst werden	Microsoft Office 2010 SP1	Authentication Types 21 Sett	ing(s)				
Network security. Divideous Server 2008 82 971. Nindeous Server 2008 82 971. Nindeous Server 2008 82 973. Nindeous Server 2008 82 971. Attechment LyGoudes Divideous Server 2008 82 971. Attechment LyGoudes Server 2008 82 972. <	angepassi werden.	 Windows 7 SP1 Windows Server 2003 SP2 	Microsoft network client: Send uner	nc Disabled		Disabled	Critical	Computer Configuration\Windows Si
Interactive logon: Require Domain C. Disabled Enabled C. Circuit Computer Configuration/Window Sivers 2018 572 Interactive logon: Number of previos. 20 goon(s). Circuit Computer Configuration/Window Sivers 2018 1/W indows Severs 2018 1/W indo		Windows Server 2008 R2 SP1	Network security: Do not store LAN	1 Enabled		Enabled	Critical	Computer Configuration\Windows S
Pundows V3 93 Pundows V3 94 Pundows		 Windows Server 2008 SP2 Windows Vista SP2 	Interactive logon: Require Domain C	Cr Disabled		Enabled	Critical	Computer Configuration\Windows Si
Interactive logen Kunner of previo. 20 logens. 0 lo		Windows XP SP3	Network Security: Restrict NTLM: N	11 Not defined		Disable	Critical	Computer Configuration\Windows Si
Nondow Server 2012 Other Baselines Windows Server 2018 2 591; Attachments V Suides Machanisms Katadements V Suides Machanisms Ma		 Internet Explorer 10 Windows 8 	Interactive logon: Number of previo	Interactive logon: Number of previoe. 10 logons Network security: Allow Local System: Not defined Interactive logon: Smart card remova. No Action			Critical	Computer Configuration Windows Si
		 Windows Server 2012 	Network security: Allow Local System				Importa	Computer Configuration/Windows Si
Attachments Vouldes " Indextools leggin Require strukt caldo Utaboled Datable Indextools (engineeric configuration) Windo Network Security: Lestinger WS2008 R2 26 10 2012 31 21 Retwork Security: Lestinger WS2008 R2 26 10 2012 31 21 Retwork Security: Lestinger WS2008 R2 26 10 2012 31 21 Network Security: Lestinger WS2008 R2 26 10 2012 31 21 Retwork Security: Lestinger WS2008 R2 26 10 2012 31 21 Retwork Security: Lestinger WS2008 R2 26 10 2012 31 21 Network Security: Restrict NTLM: Are Not defined Datable Computer Configuration/Windo Network Security: Restrict NTLM: Are Not defined Deny all accounts: Critical Computer Configuration/Windo Network Security: Restrict NTLM: Are Not defined Datable Critical Computer Configuration/Windo Network Security: Restrict NTLM: Are Not defined Not Defined Critical Computer Configuration/Windo Network Security: Restrict NTLM: Are Not defined Not Defined Critical Computer Configuration/Windo Network Security: Restrict NTLM: Are Not defined Not Defined Critical Computer Configuration/Windo Network Security: Restrict NTLM: Are Not defined Not Defined Critical Computer Configuration/Windo Network Security: Allow LocalSystem Not Defined Disabled Imputer Configuration/Windo Network Security Rev		4 Other Baselines 4 Windows Senser 2008 P2 SP1	Interactive logon: Smart card remov				Importa	Computer Configuration Windows S
Indications Catalog Catalog </th <th></th> <th>Attachments \ Guides</th> <th>Interactive logon: Require smart car</th> <th>nd Disabled</th> <th></th> <th>Disabled</th> <th>Importa</th> <th>Computer Configuration Windows Si</th>		Attachments \ Guides	Interactive logon: Require smart car	nd Disabled		Disabled	Importa	Computer Configuration Windows Si
Network Security, Allow PRU2D auth: Not defined Diasbled Dinasbled Din		<custom> - <security 26-10-2012="" r2="" settings="" ws2008=""> 1.0</security></custom>	Network security: LAN Manager aut	th Sand NTI My2 rec		Send NTLMv2 rec	Critical	Computer Configuration/Windows St
Netvork Security, Retrict NTLM Au, Not defined Disable Critical Computer Configuration/Windo Netvork Security, Retrict NTLM Au, Not defined Deny all accursts: Critical Computer Configuration/Windo Netvork Security, Retrict NTLM Au, Not defined Not Defined Critical Computer Configuration/Windo Netvork Security, Retrict NTLM Au, Not defined Not Defined Critical Computer Configuration/Windo Netvork Security, Retrict NTLM Au, Not defined Not Defined Critical Computer Configuration/Windo Netvork Security, Retrict NTLM Au, Not defined Not Defined Critical Computer Configuration/Windo Netvork Security, Nimrum Sesses: Let Veryone permit Disabled Critical Computer Configuration/Windo Netvork Security, Nimrum Sesses: No minimum Require message Critical Computer Configuration/Windo Netvork Security, Nimrum Session: No minimum Require message Critical Computer Configuration/Windo Netvork Security, Nimrum Session: No minimum Require message Critical Computer Configuration/Windo Netvork Security, Nimrum Session: No minimum Require message Critical Computer Configuration/Windo Netvork Security, Nimrum Session: No minimum Require message Critical Computer Configuration/Windo Netvork Security, Nimrum Session: No minimum Require message			Network Security: Allow PK1211 aut	hi Not defined		Disabled	Importa	Computer Configuration/Windows St
Network Security, Restrict NTUM Adr. Not defined Denyil accounts Computer Configuration/Windo Network Security, Restrict NTUM Adr. Not defined Not Defined Critical Computer Configuration/Windo Network Security, Restrict NTUM Adr. Not defined Not Defined Critical Computer Configuration/Windo Network Security, Restrict NTUM Adr. Not defined Not Defined Critical Computer Configuration/Windo Network Security, Restrict NTUM Adr. Not defined Not Defined Critical Computer Configuration/Windo Network Security, Restrict NTUM Adr. Not defined Not Defined Critical Computer Configuration/Windo Network Security, Minimum session No minimum Require message Critical Computer Configuration/Windo Network Security, Restrict NTUM Adr. Not Defined Diabiled Inoputer Configuration/Windo Network Security, Restrict NTUM Adr. Not Defined Diabiled Computer Configuration/Windo Network Security, Restrict NTUM Adr. Not Defined Diabiled Critical Computer Configuration/Windo Network Security, Restrict NTUM Adr. Not Defined Diabiled Critical Computer Configuration/Windo Network Security, Restrict NTUM Adr. Not Defined Diabiled Not Configured Not Network Security, Restrict NTUM Adr. Not Defined Not Critical Computer Configuration/Minitrat<			Network Security: Restrict NTLM: Au	w. Not defined		Disable	Critical	Computer Configuration/Windows St
Network Security: Restrict NTLM: Adt. Not defined Not Defined Critical Computer Configuration/Windo Network security: Restrict NTLM: Adt. Not defined Disabled Critical Computer Configuration/Windo Network security: Netwini TATL: Adt. Not defined Not Defined Critical Computer Configuration/Windo Microsoft: network server: SPN: Off Accept if provides: Critical Computer Configuration/Windo Microsoft: network server: SPN: Off Accept if provides: Critical Computer Configuration/Windo Network security: Minimum session: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session: No minimum Require message Critical Computer Configuration/Windo Network Security: Retrict: TTLM: CV: Not defined Draw Critical Computer Configuration/Windo Network Security: Retrict: TTLM: CV: Not defined Draw Critical Computer Configuration/Windo Network Security: Retrict: TTLM: CV: Not defined Draw Critical Computer Configuration/Windo Network Security: Retrict: TTLM: CV: Not defined Not Critical Computer Configuration/Mindo Network Security: Retrict: TTLM: CV: Not defined Not Critical <td< th=""><th></th><th></th><th>Network Security: Restrict NTLM: In</th><th>c: Not defined</th><th></th><th>Denv all accounts</th><th>Critical</th><th>Computer Configuration/Windows St</th></td<>			Network Security: Restrict NTLM: In	c: Not defined		Denv all accounts	Critical	Computer Configuration/Windows St
Network scess: Let Everyone permis Disabled Critical Computer Configuration/Windo Network Security: Retrict NTLM Adx Not defined Not Defined Critical Computer Configuration/Windo Network Security: Retrict NTLM Adx Not defined Not Defined Critical Computer Configuration/Windo Network Security: Retrict NTLM Adx Not defined Not Defined Critical Computer Configuration/Windo Network Security: Minimum session No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session No minimum Require message Critical Computer Configuration/Windo Network security: Retrict NTLM CV Not defined Deny all Critical Computer Configuration/Windo Network security: Retrict NTLM CV Not defined Not Configured None Leer Configuration/Administration/Definition Database Setting(s) Not Leer Configuration/A			Network Security: Restrict NTLM: Ac	dr Not defined		Not Defined	Critical	Computer Configuration/Windows Su
Network Security: Restrict NTLM: Adt. Not defined Not Defined Critical Computer Configuration/Windo Network Security: Minimum sessions 1No minimum Require message Critical Computer Configuration/Windo Network Security: Allow LocalSystem Not Defined Diasbled Incord Computer Configuration/Windo Network Security: Allow LocalSystem Not Defined Diasbled Computer Configuration/Windo Network Security: Restrict NTLM: Our Not defined Diasbled Computer Configuration/Windo Network Security: Restrict NTLM: Our Not defined Diasbled Computer Configuration/Windo Network Security: Restrict NTLM: Our Not defined Diasbled Computer Configuration/Windo Network Security: Restrict NTLM: Our Not defined Diasbled Computer Configuration/Windo Network Security: Restrict NTLM: Our Not defined Not Computer Configuration/Windo Network Security: Restrict NTLM: Our Not defined Not Computer Configuration/Minima Diaslow Autoplay Policies 4 Settings) Turn off Autoplay for non-volume de Not Dreversh Autoplay for non-volume de Not Nore User Configuration/Administrati Dreversh Autoplay for non-volume de Not Computer Configuration/Administrati Dreversh Autoplay for non-volume de Not Nore User Configuration/Administrati			Network access: Let Everyone permi	mis Disabled Adr. Not defined		Disabled	Critical	Computer Configuration\Windows St
Microsoft network servers SPN-Off Accept if provide: Critical Computer Configuration/Windo Network security: Minimum session : No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session : No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session : No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session : No minimum Require message Critical Computer Configuration/Windo Network Security: Metricita: NTLM: Ou: Not defined Databatel Importal Computer Configuration/Windo Network Security: Politics: 4 Security: Politics: Accept Politics: Security: Network Computer Configuration/Windo Natophy for non-volume de Not Configured Nore Gradinal Administration Disalion: Autophy for non-volume dat Not Configured Nore Leer Configuration/Administration Turn off Autophy for non-volume dat Not Configured Nore Leer Configuration/Administration Turn off Autophy for non-volume dat Not Configured Nore Leer Configuration/Administration Turn off Autophy Not Configured Nore Leer Configuration/Administration Not Configured Nore Leer Configuration/Administration Not Configur			Network Security: Restrict NTLM: Ac			Not Defined	Critical	Computer Configuration\Windows St
Network security: Minimum session 1: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session 1: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session 1: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session 1: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session 1: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session 2: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session 2: No minimum Not Configured Nore Computer Configuration/Administrati Or Autoplay Policies 4 Setting(s) Nore Computer Configuration/Administrati Disalion Autoplay for non-volume dic Not Configured Nore User Configuration/Administrati Prevent Autoplay for non-volume Nort Grifigured Nore User Configuration/Administrati Minimum Session 2: Nort Grifigured in Administrati Sitesting(s) Nore Computer Configuration/Administrati Minimum Session 2: Nort Grifigured in Administrati Nort Gorn Grifigured in Administrati Nort Gorn Grifigured in Administrati			Microsoft network server: Server SP	N Off		Accept if provided	Critical	Computer Configuration\Windows S
Network security: Allow LocalSystem: Not Defined Disabled Importa: Computer Configuration/Windo Network security: Minimum session: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session: No minimum Require message Critical Computer Configuration/Windo Network security: Minimum session: No minimum Require message Critical Computer Configuration/Windo Network Security: Minimum session: No minimum Require message Not Computer Configuration/Windo Network Security: Minimum session: No minimum Not Configured None Letre Configuration/Minimistration/Administrat			Network security: Minimum session	s No minimum		Require message	Critical	Computer Configuration\Windows Si
Network security: Minimum session : No minimum Require message Critical Computer Configuration/Windo Network Security: Retrict XTUL® Ou: Not defined Day Critical Computer Configuration/Windo Natopolay Folicies Astemptor Policies Not Not Computer Configuration/Windo Turn off Autopolay for non-volume de Not Nor Computer Configuration/Administrati Diallow Autoplay for non-volume de Not Nor User Configuration/Administrati Trun off Autoplay for non-volume de Not Computer Configuration/Administrati Diallow Autoplay Not Computer Configuration/Administrati Turn off Autoplay Not Computer Configuration/Administrati Turn off Autoplay Not User Configuration/Administrati Turn off Autoplay Not User Configuration/Administrati Turn off Autoplay Not Setting(s) Turn off Autoplay Not User Configuration/Administrati Turn off Autoplay Not Not User Configuration/Administrati Turn off Autoplay Not Not User Configuration/Administrati Turn off Autoplay Not Not Computer Configuration/Administrati Turn off Autoplay Not Not Computer Configuration/Administrati		Network security: Allow LocalSyster	n Not Defined		Disabled	Importa	Computer Configuration\Windows Si	
Network Security: Restrict NTLM: Our Not defined Deny all Critical Computer Configuration/Windo • Autoplay Folicies 4 Setting(s) Turn off Autoplay for non-volume de Not Computer Configuration/Administrati Tourn off Autoplay for non-volume de Not Computer Configuration/Administrati None User Configuration/Administrati Dealow Not Configured None User Configuration/Administrati Turn off Autoplay Not Configured None User Configuration/Administrati • Biometrics 3 Setting(s) None User Configuration/Administrati			Network security: Minimum session	s No minimum		Require message	Critical	Computer Configuration\Windows S
Autoplay Policies 4 Setting(s) Turn off Autoplay Policies 4 Setting(s) Turn off Autoplay for non-volume de Not Configured None User Configuration/Administrati Prevent AutoPlay from remembering Not Configured None User Configuration/Administrati Turn off Autoplay on Non-volume (setting(s) None Gramma Setting(s) Not Configured None User Configuration/Administrati None User Configuration/Administrati None User Configuration/Administrati None Gramma Setting(s)			Network Security: Restrict NTLM: Or	ut Not defined		Deny all	Critical	Computer Configuration\Windows Si
Turn off Autoplay for non-volume de Not Configured None Computer Configuration/Administration Diallow Autoplay for non-volume de Not Configured None User Configuration/Administration Prevent Autoplay Not Configured Not User Configuration/Administration Turn off Autoplay Not Configured None User Configuration/Administration Wind Gamma Stating(s) None User Configuration/Administration Allow users to log on using biometrix Not Configured None Computer Configuration/Administration			Autoplay Policies 4 Setting(s)					
Disallow Autoplay for non-volume dk Not Configured None User Configuration/Administrati Prevent Autoplay Not Configured None User Configuration/Administrati Turn off Autoplay Not Configured None User Configuration/Administrati Biometrics Stating(s) None User Configuration/Administrati Allow users to log on using biometrix Not Configured None Computer Configuration/Administrati			Turn off Autoplay for non-volume d	non-volume de		Not Configured	None	Computer Configuration\Administrat
Prevent AutoPRay from remembering Not Configured None User Configuration/Administrati Turn off Autoplay Not Configured None User Configuration/Administrati Biometrics 3 Setting(c) Not Computer Configuration/Administrati Allow users to log on using biometrix Not Configured None Computer Configuration/Administrati			Disallow Autoplay for non-volume of	de		Not Configured	None	User Configuration\Administrative Te
Turn off Autoplay Not Configured None User Configuration/Administratic Biometrics 3 Setting(s) None Computer Configuration/Administratic Allow users to log on using biometrix Not Configured None Computer Configuration/Administratic			Prevent AutoPlay from rememberin	g		Not Configured	None	User Configuration\Administrative Te
Allow users to log on using biometrix Not Configured None Computer Configuration/Admin			Turn off Autoplay			Not Configured	None	User Configuration\Administrative Te
Allow users to log on using biometrix Not Configured None Computer Configuration/Admin			Biometrics 3 Setting(s) Allow users to log on using biometric					
						Not Configured	None	Computer Configuration\Administrat
Allow domain users to lon on using k Not Configured None Connected Configuration Admin			Allow domain users to log on using	. 6		Not Configured	None	Computer Confinuation\Administrat

In der folgenden Tabelle 4 erfolgt eine Auflistung der Einstellungskategorien der Baseline. Sofern in der entsprechenden Kategorie noch Default-Werte vorhanden sind oder diese gemäß den Unternehmensrichtlinien angepasst werden müssen, erfolgt hier ebenfalls der entsprechende Vermerk in der Kommentarspalte.

Kategorie	Beschreibung	Kommentar
Account Lock	Erlaubt es, Werte für das Aussperren von Benutzern nach mehrmaliger falscher Eingabe des Passwortes festzulegen	Die Kategorie spiegelt die Anforderungen des Grundschutzes wieder und muss ggf. den eigenen Anforderungen angepasst werden.
Authentication Types	In diesem Abschnitt werden sämtliche Authentifizierungseinstellungen für NTLM,	Der Einsatz von NTLM und LAN Manager wird nicht

Tabelle 4: Konfigurationskategorien der Baseline





	LAN Manager und das interaktive Logon konfiguriert.	empfohlen. Durch die Einstellungen in diesem Abschnitt wird nur NTLMv2 erlaubt. Sofern Applikationen oder andere Systeme auf den Einsatz von NTLM- oder LM- Hashes angewiesen sind, ist die entsprechende Konfiguration notwendig.
Autoplay Policies	Autoplay-Einstellungen z. B. für MTP- Geräte, die etwa AutoPlay für Kameras oder Telefone unterbinden.	In diesem Abschnitt sind keine feingranularen Autoplay- Policies definiert, da diese an die Sicherheitsanforderungen des Unternehmens angepasst werden müssen.
Biometrics	Konfiguriert die Authentifizierung mittels biometrischer Merkmale, sofern die eingesetzte Hardware dies unterstützt.	Biometrische Einstellungen sind im Template nicht konfiguriert und müssen bei Bedarf entsprechend angepasst werden.
BitLocker	BitLocker ist die integrierte Festplattenverschlüsselung unter Windows Server 2008. Der Einsatz hängt meist vom Schutzbedarf der gespeicherten Daten ab und ist je nach Unternehmensanforderungen an die Vertraulichkeit zu konfigurieren.	Einstellungen für BitLocker sind im Template nicht konfiguriert, da der Einsatz von BitLocker sehr individuell gestaltbar ist. Sofern Festplattenverschlüsselung erwünscht ist, muss ein entsprechendes Konzept durch den zuständigen Administrator erarbeitet und umgesetzt werden.
DirectAccess	DirectAccess ermöglicht es Benutzern, aus der Ferne auf Dateifreigaben, Websites und Anwendungen im Unternehmen zuzugreifen, ohne eine dedizierte VPN-Verbindung herzustellen. Als Netzwerkprotokoll wird IPv6 eingesetzt, welches durch IPsec abgesichert wird.	DirectAccess ist im Prinzip eine Technologie, um ein VPN abzulösen, erfordert aber auch einige technische Änderungen an der Netzwerkinfrastruktur, da diese Lösung auf IPv6 aufbaut. Sofern der Einsatz von DirectAccess erwünscht ist, muss dies entsprechend im Template konfiguriert werden. Als Minimalanforderung werden mindestens zwei Server mit Windows Server 2008 R2, mindestens zwei, besser vier öffentliche IPv4- Adressen sowie Clients mit Windows 7 in der Enterprise- oder Ultimate-Edition benötigt.
Driver Installation	Konfiguration, ob die Abfrage erfolgen soll, Windows Update zur Suche von Treibern zu benutzen.	In der gegenwärtigen Einstellung erfolgt keine Aufforderung, Windows Update zur Suche von





		Treibern zu benutzen.
Encrypted File System (EFS)	Encrypted File System bietet eine Dateiverschlüsselung auf NTFS- Datenträgern	Da für EFS eine PKI erforderlich ist, wurden im Template keine Konfigurationseinstellungen vorgenommen. Encrypted File System ist in der Vorlage nicht aktiv und muss bei Bedarf entsprechend konfiguriert werden.
Encryption Configuration	In dieser Sektion werden die Verschlüsselungs- und digitalen Signaturmechanismen festgelegt, die zur Absicherung der Netzwerkkommunikation mit anderen IT-Systemen dienen.	Die Einstellungen in diesem Abschnitt sind dahingehend zu prüfen, ob diese mit der bereits bestehenden Infrastruktur kompatibel sind.
Event Logging	In diesem Abschnitt wird die Protokollierungsrichtlinie für das IT- System festgelegt.	Es wurde eine Grundkonfiguration durchgeführt, die dem BSI Grundschutz entspricht. Sofern die Anforderung an ein detaillierteres Logging besteht, sind die Logging-Parameter entsprechend anzupassen.
Identity Management	Umbenennung der lokalen Konten für Administrator und Gast.	Der Grundschutz empfiehlt die Umbenennung der beiden Iokalen Konten. In der Vorlage wurden entsprechende Werte gesetzt, die aber gemäß den Unternehmensvorgaben anzupassen sind.
Internet Communication Settings	Deaktiviert sämtliche Datenübertragungen an Microsoft, die im Rahmen des Produktverbesserungsprozesses verschickt werden.	Alle Dienste, welche Diagnose- oder Benutzerdaten an Microsoft versenden und keine Notwendigkeit auf einem Serversystem darstellen, sind deaktiviert.
IPsec	Sofern Datenübertragungen verschlüsselt über IPsec erfolgen sollen, kann dies in diesem Abschnitt erfolgen.	IPsec ist nicht aktiviert und je nach den Anforderungen des Unternehmens zu konfigurieren.
Key Management	Konfiguriert einen sicheren Kanal mit 128 Bit Verschlüsselungsstärke zwischen Member Server und Domänencontroller.	Diese Einstellung ist entsprechend anzupassen. Es wird mindestens Windows 2000 benötigt. Erfolgt keine Konfiguration, so wird die Verschlüsselungsstärke ausgehandelt.
Least Functionality	Einstellungen, die vorhandene Funktionen einschränken oder nur für bestimmte Benutzergruppen erlauben.	Die Kategorie spiegelt die Anforderungen des Grundschutzes wieder und muss ggf. den eigenen Anforderungen angepasst





		werden.
Least Privilege	In diesem Abschnitt erfolgt die Zuweisung von Benutzerrechten.	Die Einstellungen müssen entsprechend überprüft und ggf. an weitere administrative Gruppen, die möglicherweise im Unternehmen bestehen, angepasst werden.
Log Access Limitation	Zuweisung der Berechtigung für das Ändern der Protokollierungseinstellungen für Dateien und Ordner sowie das Löschen des Sicherheitslogs.	Jeder, der diese Berechtigung besitzt, ist in der Lage, kritische Informationen oder Beweismittel zu löschen. Diese Berechtigung sollte nur der Gruppe der lokalen Administratoren eingeräumt werden.
Logging Configuration	In diesem Abschnitt können Dateigrößen für Logdateien festgelegt werden und wie sich das System zu verhalten hat, wenn nicht mehr ausreichend Speicherplatz für das Logging vorhanden ist.	Je nach Bedarf muss die Logging-Konfiguration des Systems angepasst werden.
Microsoft Peer-to-Peer Networking Services	Diese Einstellung deaktiviert den Microsoft Peer-to-Peer Networking Service.	Sofern Anwendungen vom Peer-to-Peer Networking Service abhängig sind, ist dieser Dienst wieder zu aktivieren.
Network Access Protection (NAP)	Durch Network Access Protection kann der Clientzugriff auf das Netzwerk mit entsprechenden Richtlinien oder so genannten Health Policies kontrolliert werden. Solche Richtlinien erlauben es z. B., die Konfigurationseinstellungen zu analysieren oder den Status von Virenscannern zu ermitteln. Je nach Ergebnis der Prüfung kann dem Client der Zugriff erlaubt oder verweigert werden.	Network Access Protection ist in der Vorlage nicht konfiguriert, da hierzu noch weitere Infrastrukturkomponenten wie z. B. ein Network Policy Server notwendig sind.
Network Protection	In diesem Abschnitt wird die Konfiguration der Windows Firewall vorgenommen. Es werden diverse Netzwerk-Registry-Werte festgelegt, die vom BSI empfohlen sind.	Die Firewall ist im Template so konfiguriert, dass alle eingehenden Verbindungen erst einmal geblockt werden. Da hier von einem Betrieb des Servers in einer Domäne ausgegangen wird, ist nur das Domänenprofil aktiv. Die anderen Profile sind identisch konfiguriert, aber nicht aktiv. Eine Anpassung ist demnach in der Regel erforderlich.
Password Attributes	In diesem Abschnitt kann die Passwortrichtlinie des Unternehmens umgesetzt werden.	Die Einstellungen sind in Anlehnung an die Passwortrichtlinie des Unternehmens zu wählen und





		entsprechend zu konfigurieren.
Protocol Configuration	Sichere Konfiguration von Protokollen. In diesem Abschnitt werden z. B. LDAP, ICMP, Kanalverschlüsselungsoptionen etc. definiert.	Die Kategorie spiegelt die Anforderungen des Grundschutzes wieder und muss ggf. den eigenen Anforderungen angepasst werden.
Remote Assistance	Konfiguration, ob Remoteunterstützung erlaubt ist oder nicht.	In diesem Template wird davon ausgegangen, dass die Remoteunterstützung auf Servern nicht benötigt wird.
Remote Desktop Connection Client	Sichere Einstellung für RDP- Verbindungen.	Passwörter dürfen bei Remote Desktop Sessions nicht gespeichert werden. Die Einstellung deaktiviert die "Passwort speichern"- Checkbox bei zugreifenden Clients.
Remote Desktop Session Security	Sicherheitskonfiguration für Remote Desktop Sessions bzw. Konfiguration der Authentifizierung für Remotedesktopdienste (z. B. Authentifizierung auf Netzwerkebene).	Diese Einstellung verschlüsselt die RDP Session mit 128 Bit. Sofern Clients dies nicht unterstützen, schlägt eine Verbindung via RDP fehl.
Server Manager	Einstellung, ob der Server Manager direkt nach einer Anmeldung am System erscheint oder nicht.	Der Server Manager startet nicht direkt nach einer erfolgreichen Anmeldung am Server.
Session Configuration	Einstellungen für die Bildschirmsperre, Anmelden zu bestimmten Zeiten, Anzeigen von zuletzt angemeldeten Benutzern und die Nutzung von Chipkarten.	Die Kategorie spiegelt die Anforderungen des Grundschutzes wieder und muss ggf. den eigenen Anforderungen angepasst werden.
System Defaults ⁴	Umbenennung von administrativen und Gastkonten.	Die Kategorie spiegelt die Anforderungen des Grundschutzes wieder und muss ggf. den eigenen Anforderungen angepasst werden.
System Integrity	Hier werden Einstellungen zur Benutzerkontensteuerung durchgeführt.	Die UAC ist in der Vorlage aktiv konfiguriert. Gemäß den Richtlinien eines Unternehmens müssen die Einstellungen entsprechend angepasst werden.
System Services	Konfiguration von Systemdiensten, die unter Windows 2008 vorhanden sind.	Eine entsprechende Rollenauswahl muss für das System mittels des Server

⁴ Einige hier aufgelistete Einstellungen wurden bereits in einem anderen Konfigurationsabschnitt konfiguriert, werden aber redundant aufgelistet. Sofern die Konfiguration schon vorher erfolgt ist, sind die Werte hier identisch.

– ÖFFENTLICH –





		Managers erfolgen, damit nur benötigte Dienste gestartet werden und somit die Angriffsfläche minimiert wird.
		Zusätzlich sollten alle weiteren Dienste auf deren Erforderlichkeit geprüft und ggf. deaktiviert werden.
Windows Media Digital Rights Management	Sofern Windows Media Player auf einem Server installiert ist, kann hier konfiguriert werden, ob dieser eine Internetverbindung nach extern aufbauen darf, um DRM Informationen abzurufen.	Mit der momentanen Einstellung ist es Windows Media Player ⁵ nicht erlaubt, DRM Information direkt von Microsoft zu beziehen.
Windows Updates	Abschnitt zur Konfiguration von Windows Updates.	Der Grundschutz empfiehlt einen eigenen WSUS Server im Netzwerk des Unternehmens zu betreiben. Dieser muss entsprechend konfiguriert werden.

Nachdem alle Einstellungen überprüft und entsprechend angepasst worden sind, kann die Baseline nun entweder auf einem Domänensystem oder einem Stand-Alone Server verteilt werden. Wie eine Verteilung auf einem Domänensystem erfolgt, ist im Abschnitt 6.6 beschrieben. Abschnitt 6.8 beschreibt die Vorgehensweise zur Applizierung einer Baseline auf einem Stand-Alone System. Zunächst muss allerdings erst ein Export der Baseline in ein dafür benötigtes Format erfolgen. Abschnitt 6.5 beschreibt den Export einer angepassten Baseline.

AppLocker ist ein weiteres erwähnenswertes Feature, welches nicht über den Security Compliance Manager konfiguriert werden kann, aber dennoch zur Sicherheit des Systems beiträgt, da Administratoren mittels AppLocker-Richtlinien einzelne Anwendungen sperren können. Die AppLocker-Richtlinien müssen direkt auf dem Domain Controller oder in der lokalen Sicherheitsrichtlinie eines Stand-Alone Systems konfiguriert werden.

Bei neu installierten Windows Systemen ist IPv6 bereits im Default-Modus aktiviert. Sofern keine Mechanismen zur Blockierung und Kontrolle von IPv6 existieren, wird empfohlen, dieses Protokoll komplett zu deaktivieren, da dieses sonst als Einfallstor für Angriffe ausgenutzt werden kann. Die Deaktivierung von IPv6 kann gegenwärtig nicht durch den SCM erfolgen. Folgender Web-Link beschreibt, wie eine manuelle Deaktivierung von IPv6-Komponenten durchzuführen ist.

6.5 Exportieren einer angepassten Baseline

Wurden alle Einstellungen überprüft und gegebenenfalls bearbeitet, so muss im nächsten Schritt die angepasste Baseline aus dem SCM exportiert werden, damit der Import auf dem Zielsystem erfolgen kann. Dies geschieht über die Export Funktion des SCM.

Für den späteren Import auf dem Zielsystem wird der Export mittels Gruppenrichtlinie – *GPO Backup (folder)* empfohlen. Nachdem der Ordner erstellt worden ist, muss er auf das entsprechende Zielsystem (entweder auf ein Domänen- oder ein Stand-Alone-System) transferiert werden.

⁵ Um den Media Player oder die Rolle Streaming Media Services zu nutzen, ist das optional erhältliche Paket Windows Media Services 2008 für Windows Server 2008 R2 zu installieren.





Sofern im Unternehmen der System Center Configuration Manager (SSCM) eingesetzt wird, kann der Export der Baseline auch im SCCM-Format DCM erfolgen.

6.6 Sperren nach Export der Baseline (Versionsverwaltung)

Der SCM bietet die Möglichkeit, importierte Baselines zu sperren. Die Sperrung erfolgt über die Option "Lock" im rechten Menu einer einzelnen Baseline (siehe Abbildung 6: Lock Funktion einer Baseline). Eine ausführliche Beschreibung der Sperrfunktion findet sich in der Hilfe des SCM.

Authentication Types 21 Setting(s)				Baseline
Microsoft network client: Send unenc Disabled	Disabled	Critical	Computer Configuration\Windows Sr M 5.123 Absichen	Compare / Merge
Network security: Do not store LAN / Enabled	Enabled	Critical	Computer Configuration\Windows Sr M 5.123 Absichen	Delete
Interactive logon: Require Domain Cc Disabled	Enabled	Critical	Computer Configuration\Windows Sr M 4.48 Passworts	Duplicate
Network Security: Restrict NTLM: NTI Not defined	Disable	Critical	Computer Configuration\Windows Sr M 5.123 Absichen	LOCK Deservation
interactive logon: Number of previou 10 logons	0 logon(s)	Critical	Computer Configuration\Windows Sr M 4.48 Passworts	Propercies
Network security: Allow Local System Not defined	Enabled	Importa	Computer Configuration\Windows Sr M 5.123 Absichen	Setting
interactive logon: Smart card remova No Action	Lock Workstation	Importa	Computer Configuration\Windows Sr M 4.2 Bildschirms	Add
nteractive logon: Require smart card Disabled	Disabled	Importa	Computer Configuration\Windows Sr M 4.15 Gesicherte	Move
Network Security: Restrict NTLM: Auc Not defined	Disable	Critical	Computer Configuration\Windows Sr M 4.81 Audit und	Setting Group
Network security: LAN Manager auth Send NTLMv2 res	Send NTLMv2 res	Critical	Computer Configuration\Windows Sr M 5.123 Absichen	Add
Network Security: Allow PKU2U auth: Not defined	Disabled	Importa	Computer Configuration\Windows Sr M 4.280 Sichere B	Delete
Network Security: Restrict NTLM: Auc Not defined	Disable	Critical	Computer Configuration\Windows Sr M 4.81 Audit und	Properties
Network Security: Restrict NTLM: Inc: Not defined	Deny all accounts	Critical	Computer Configuration\Windows Sr M 5.123 Absichen	A Help
Network Security: Restrict NTLM: Adv Not defined	Not Defined	Critical	Computer Configuration\Windows Sr M 5.123 Absicher	About
Network access: Let Everyone permis Disabled	Disabled	Critical	Computer Configuration\Windows Sr M 4.280 Sichere B	Help Topics
Network Security: Restrict NTLM: Adv Not defined	Not Defined	Critical	Computer Configuration\Windows Sr M 5.123 Absichen	Release Notes
Microsoft network server: Server SPN Off	Accept if providec	Critical	Computer Configuration\Windows Sr M 5.123 Absichen	Send Feedback
Network security: Minimum session s No minimum	Require message	Critical	Computer Configuration\Windows Sr M 5.123 Absicher	Privacy Statement
Network security: Allow LocalSystem Not Defined	Disabled	Importa	Computer Configuration\Windows Sr M 5.123 Absicher	

Abbildung 6: Lock Funktion einer Baseline

Microsoft	Security Compliance Manager	83
<u> </u>	You are about to lock the baseline. After locking the baseline cannot modify it. Do you want to continue?	e, you
	[]	<u>N</u> ein

Abbildung 7: Hinweis zur Sperrung über die "Lock" Option.

Nach erfolgter Sperrung ist eine Bearbeitung der Baseline nicht mehr möglich. Über die Option "Edit" muss zuerst eine Kopie einer gesperrten Baseline erstellt werden (siehe Abbildung 8: Erstellung einer Kopie).



Abbildung 8: Erstellung einer Kopie





Durch die "Edit"-Funktion wird automatisch eine neue *Minor-Version* der Baseline erstellt (siehe Abbildung 9: Editierung einer Kopie). Diese Baseline kann nun als Basis weiterer Konfigurationen verwendet werden.

Luit				
Baseline Name:				
HiS-Windows-2	800			
Version major:	1	Version minor:	1	
Description:				

Abbildung 9: Editierung einer Kopie

6.7 Import der Baseline auf Domänen-Systeme

Im folgenden Abschnitt wird die Vorgehensweise für Serversysteme beschrieben, die ihre Gruppenrichtlinieneinstellungen zentral über einen Domain Controller beziehen.

Das Verzeichnis mit dem Gruppenrichtlinien-Export kann entweder als neue Richtlinie verwendet werden, oder die Einstellungen können in eine bereits bestehende Richtlinie übernommen werden.

Um eine exportierte SCM-Richtlinie in eine Gruppenrichtlinie zu importieren, muss der Gruppenrichtlinienverwaltung-Editor genutzt werden. Entweder kann dies durch die Erstellung einer neuen GPO erfolgen, oder die Einstellungen können in eine bestehende GPO integriert werden.

Im Kontextmenü der Gruppenrichtlinienverwaltungskonsole kann die exportierte Gruppenrichtlinie durch den Menüpunkt "Einstellungen importieren" importiert werden.





Tabelle 5: Importieren von Einstellungen auf einem Domänencontroller



Nach dem Import können die Einstellungen auf der Registerkarte des Gruppenrichtlinienverwaltungs-Editors angezeigt werden.

Sofern eine Gruppenrichtlinie innerhalb derselben Domäne wieder importiert werden soll (z. B. nach Anpassung der Baseline im SCM), ist die Funktion *"Von Sicherung wiederherstellen"* zu verwenden.

Abschließend muss das Gruppenrichtlinienobjekt noch mit einem AD-Ast (z. B. einer OU) verknüpft werden, damit die Einstellungen wirksam werden. Solange das Gruppenrichtlinienobjekt noch nicht verknüpft ist, sind die Einstellungen auch nicht aktiv. Unter dem folgenden <u>Microsoft-Link</u> ist ausführlich beschrieben, wie eine Verknüpfung von Gruppenrichtlinienobjekten durchzuführen ist.

6.8 Import der Baseline auf Stand-Alone-Systemen

Sofern kein Active Directory (AD) im Unternehmen eingesetzt wird oder das System keine Anbindung an ein AD besitzt, weil es sich z. B. um ein DMZ System handelt, besteht auch die Möglichkeit, die Baseline als lokale Sicherheitsrichtlinie auf dem System zu integrieren.

Für diesen Zweck stellt der Security Compliance Manager das Befehlszeilen-Tool *LocalGPO* zur Verfügung. Hiermit kann man die lokalen Richtlinien eines PCs in ein GPO-Backup exportieren und umgekehrt das exportierte GPO-Backup einer Baseline als lokalen Richtliniensatz anwenden. Das Tool wird bei der Installation des Security Compliance Managers nicht komplett installiert, sondern als MSI-Paket zur nachträglichen Installation abgelegt, so dass man es auch auf anderen PCs einsetzen





kann. Die einzelnen Schritte zum Importieren einer Baseline auf einem Stand-Alone-System sind in der folgenden Tabelle beschrieben:

Tabelle 6: Absicherung von Stand-Alone-Systemen

Sofern noch nicht auf dem Stand-Alone- System vorhanden, muss das Tool LocalGPO installiert werden.		
Die gewünschte Baseline ist aus dem Security Compliance Manager zu exportieren (GPO Backup-Folder) und auf das Zielsystem zu übertragen.		
Der LocalGPO Installations-Wizard führt den Administrator durch die Installation.	设 LocalGPO Setup	Welcome to the LocalGPO Setup Wizard
		The Setup Wizard will allow you to change the way LocalGPO features are installed on your computer or even to remove LocalGPO from your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	Microsoft Solution Accelerators	< Back Next > Cancel





	E LocalGPO Setup	
	C S	ompleting the LocalGPO etup Wizard
	Clie	ck the Finish button to exit the Setup Wizard.
	Microsoft Solution Accelerators	< Back Finish Cancel
Das Tool LocalGPO Command-line muss als Administrator ausgeführt werden. Nachdem sich das Kommandozeilenfenste r geöffnet hat, kann mit dem Befehl im nächsten Fenster die Baseline auf das System appliziert werden.	 Internet Explorer (64 Bit) Internet Explorer Security Compliance Manager Windows Update Autostart LocalGPO LocalGPO LocalGPO Microsoft Security Compliance Ma Microsoft SQL Server 2005 Microsoft System Center 	Administrator Dokumente Computer Netzwerk





Zum Applizieren der in	Administrator: LocalGPO Command-line	×
Abschritt 6.4 überprüften Baseline ist folgende Kommandozeile auszuführen:	C:\Program Files (x86)\LocalGPO}LocalGPO.wsf /Path:c:\Users\Administrator\Deskto p\{ca84c8d6-d86f-4893-807f-9923008cf1f9} Microsoft (R) Windows Script Host, Uersion 5.8 Copyright (C) Microsoft Corporation 1996-2001. Alle Rechte vorbehalten. Modifying Local Policy this process can take a few moments. Applied valid INF from c:\Users\Administrator\Desktop\{ca84c8d6-d86f-4893-807f-9 923008cf1f9} Applied valid Machine POL from c:\Users\Administrator\Desktop\{ca84c8d6-d86f-4893-807f-9 3-807f-9923008cf1f9} Applied valid User POL from c:\Users\Administrator\Desktop\{ca84c8d6-d86f-4893-8 97f-9923008cf1f9} Applied valid Audit Policy CSU from c:\Users\Administrator\Desktop\{ca84c8d6-d86f-4893-8 07f-9923008cf1f9} Local Policy Modified! Please restart the computer to refresh the Local Policy C:\Program Files (x86)\LocalGPO>_	
Nach dem Applizieren der Baseline auf dem System ist dieses neu zu starten, um die neuen Einstellungen wirksam werden zu lassen. Die Einstellungen können in der lokalen Sicherheitsrichtlinie des Systems eingesehen werden.		

LocalGPO kann auch in die andere Richtung benutzt werden, um die Konfiguration der lokalen Gruppenrichtlinien zu exportieren, so dass diese weiter im Security Compliance Manager bearbeitet werden können.





7 ANHANG

7.1 BSI

Baustein B 3.101 Allgemeiner Server

Vorabversion Baustein B 3.109 Windows Server 2008 https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b0 3/b03101.html https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundsch utz/Download/Vorabversionen/Baustein Win Server 2008.pdf? blob=publicationFile

7.2 Microsoft

Security Compliance Manager Verknüpfen einer GPO mithilfe der Gruppenrichtlinienkonsole http://technet.microsoft.com/en-us/library/cc677002.aspx http://technet.microsoft.com/de-de/library/cc778387(v=ws.10).aspx

7.3 Abbildungsverzeichnis

Abbildung 1: Fall 1, Überprüfung der Werte notwendig	4
Abbildung 2: Fall 2, Zuweisung der Werte notwendig	4
Abbildung 3: Beschreibung innerhalb der Setting Group "Properties"	5
Abbildung 4: Aufbau des SCM	9
Abbildung 5: Detaillierte Konfigurationseinstellungen	10
Abbildung 6: Lock Funktion einer Baseline	20
Abbildung 7: Hinweis zur Sperrung über die "Lock" Option	20
Abbildung 8: Erstellung einer Kopie	20
Abbildung 9: Editierung einer Kopie	21

7.4 Tabellenverzeichnis

Tabelle 1: Voraussetzung zur Installation des SCM	8
Tabelle 2: Vorgehensweise zum Import einer Baseline	11
Tabelle 3: Anpassen einer Baseline	14
Tabelle 4: Konfigurationskategorien der Baseline	14
Tabelle 5: Importieren von Einstellungen auf einem Domänencontroller	22
Tabelle 6: Absicherung von Stand-Alone-Systemen	23

7.5 Begriffe

Abkürzung	Erläuterung
SCM	Security Compliance Manager
SSCM	System Center Configuration Manager
NAP	Network Access Protection
EFS	Encrypting File System
IPsec	Internet Protocol Security





RDP	Remote Desktop Protocol
CCE	Common Configuration Enumeration

KONTAKT

HiSolutions AG Bouchéstraße 12 12435 Berlin

<u>info@hisolutions.com</u> <u>www.hisolutions.com</u> Fon +49 30 533 289 0 Fax + 49 30 533 289 900