



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	ZUSAMMENFASSUNG	1
	INHALTSVERZEICHNIS	2
2	EINLEITUNG	3
3	ABGRENZUNG	4
4	BAUSTEIN WINDOWS SERVER 2008	6
5	SECURITY COMPLIANCE MANAGER (SCM)	7
6	VORGEHENSWEISE	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	ANHANG	26
7.1	BSI	26
7.2	Microsoft	26
7.3	Abbildungsverzeichnis	26
7.4	Tabellenverzeichnis	26
7.5	Begriffe	26
	KONTAKT	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:



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

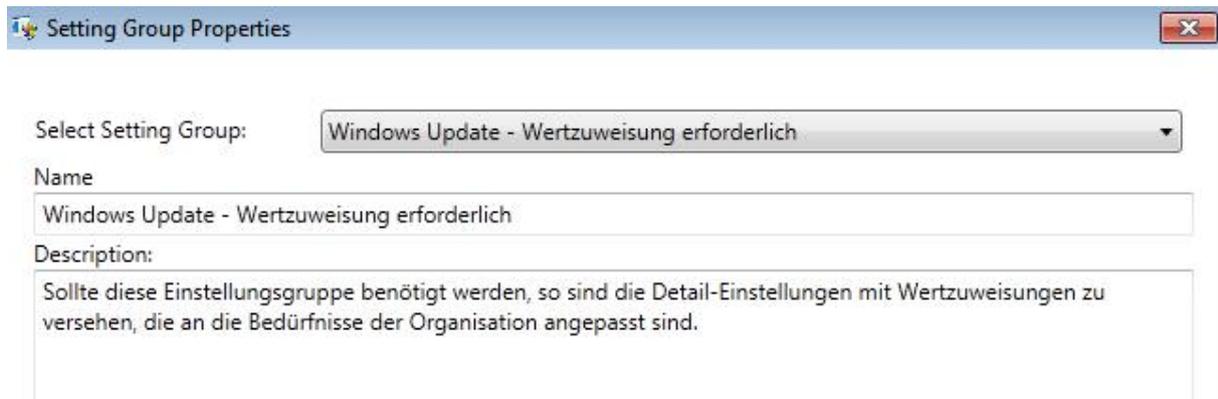


Abbildung 3: Beschreibung innerhalb der Setting Group "Properties"

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 Exportmöglichkeiten 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.

Tabelle 1: Voraussetzung zur Installation des SCM

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:

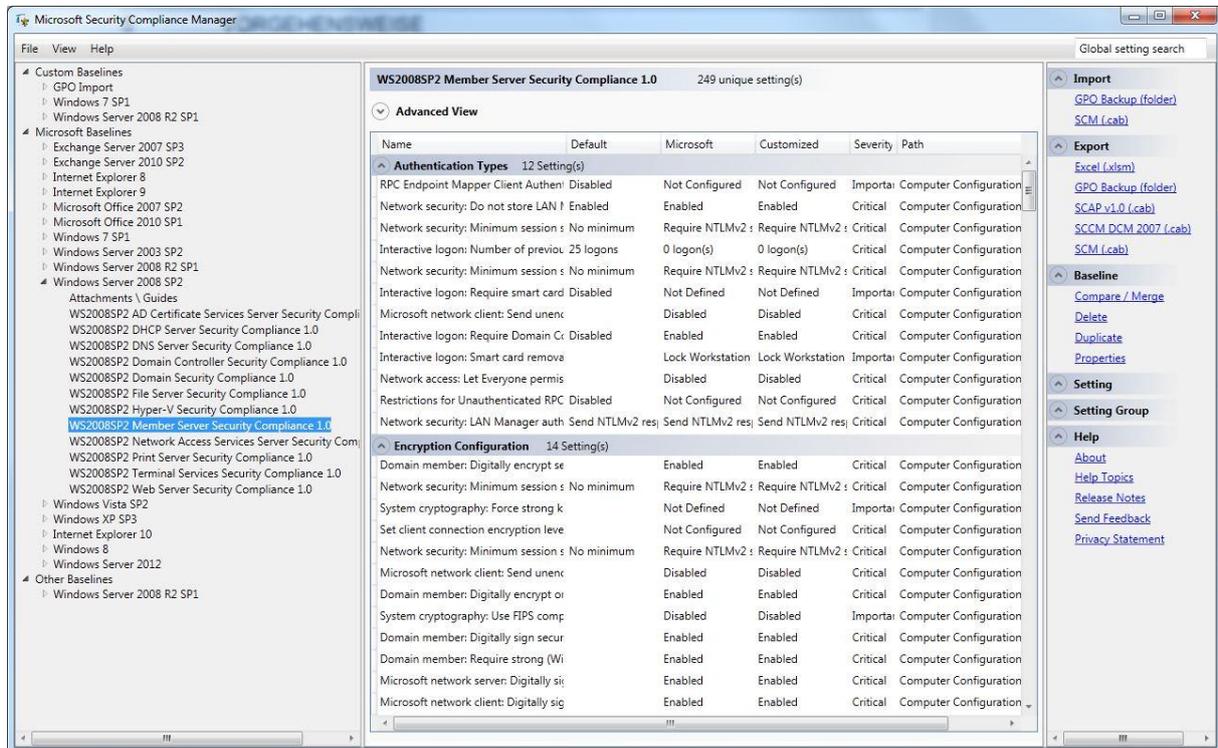


Abbildung 4: Aufbau des SCM

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 <http://cve.mitre.org/>.

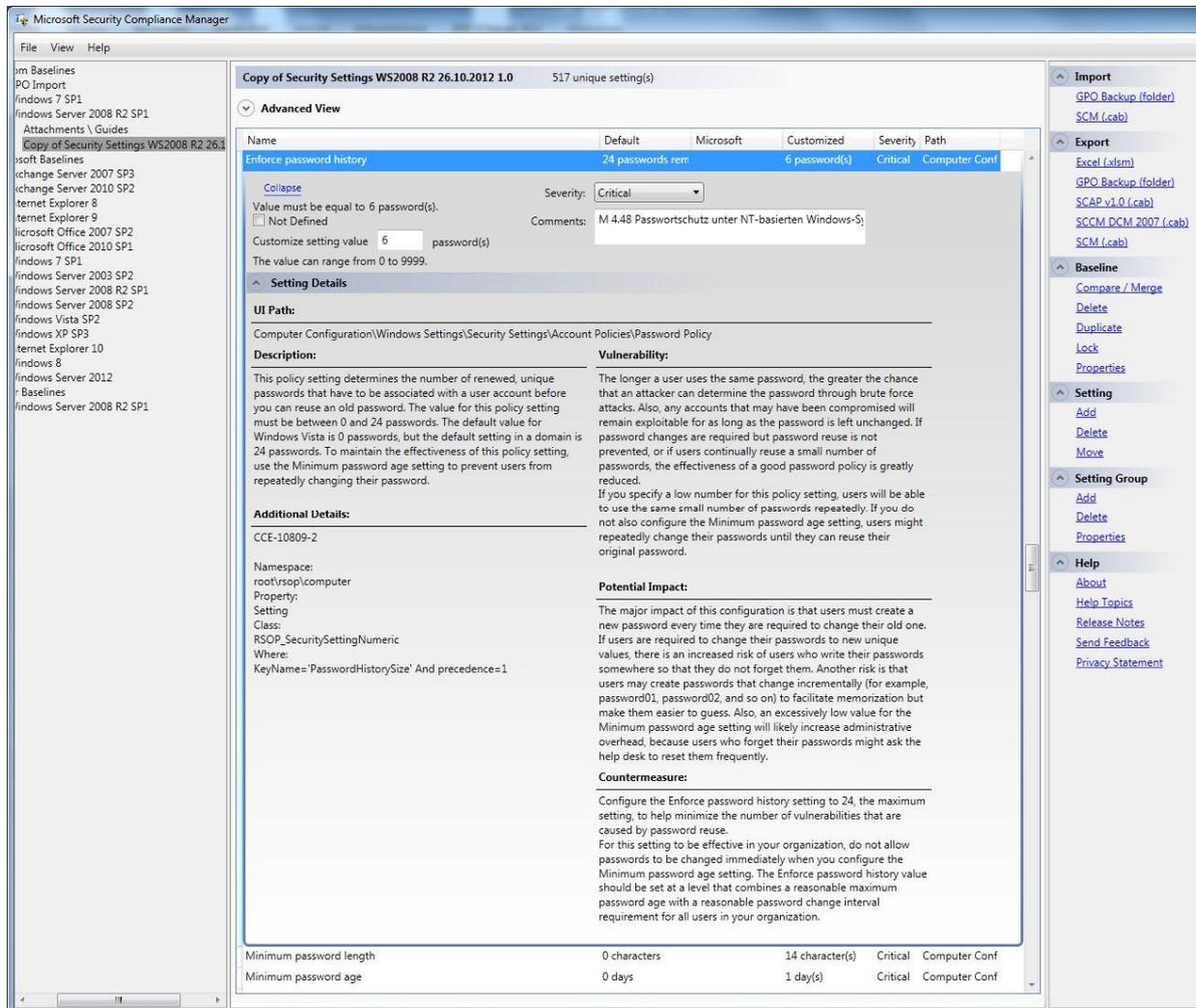


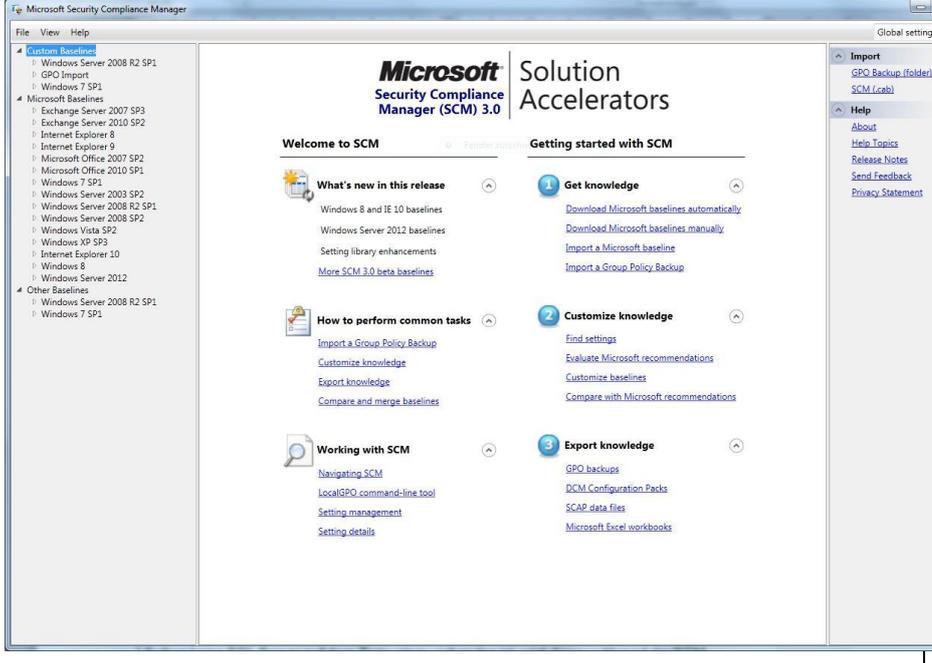
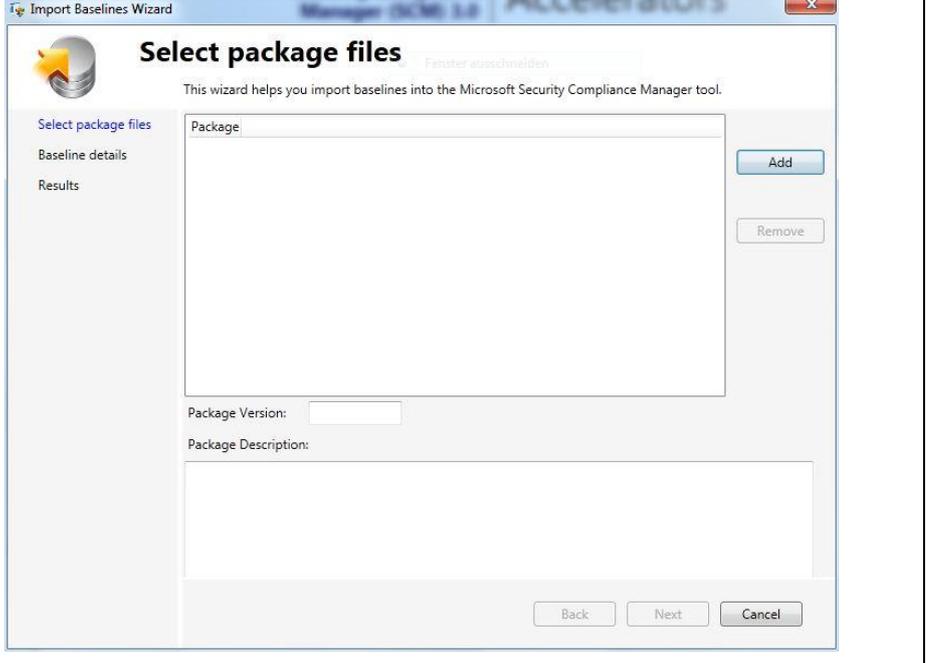
Abbildung 5: Detaillierte Konfigurationseinstellungen

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.

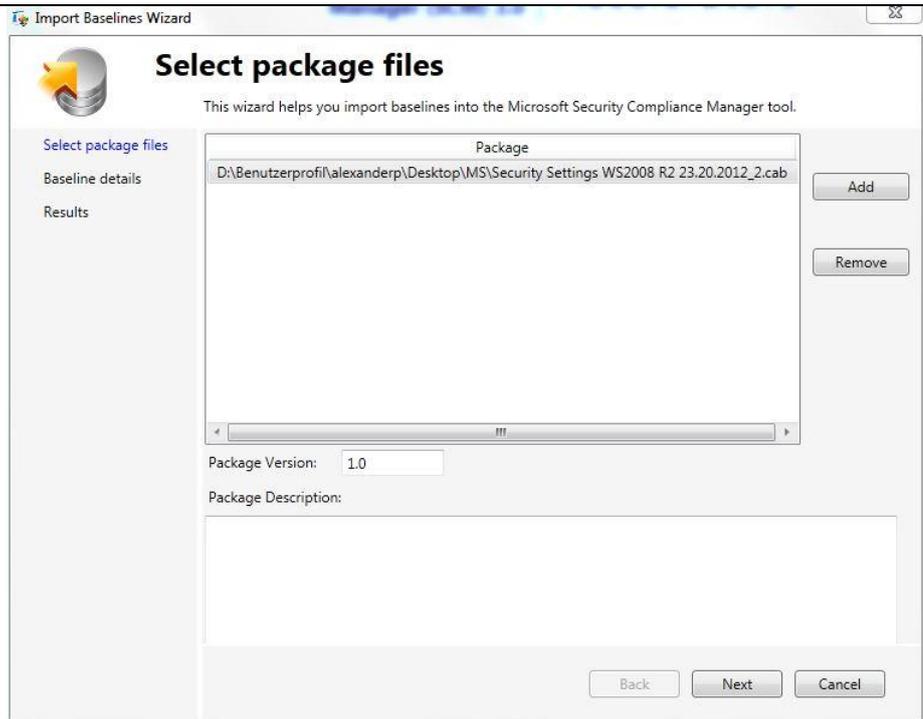
6.3 Importieren der HiSolutions Baseline für Windows Server 2008 R2

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

<p>Zum Importieren der Baseline im Import-Bereich auf <i>SCM (cab)</i> klicken. Der <i>Import Baselines Wizard</i> öffnet sich.</p>	
<p>Auf „Add“ klicken und die zu importierende Baseline auswählen.</p>	

Weiter mit „Next“



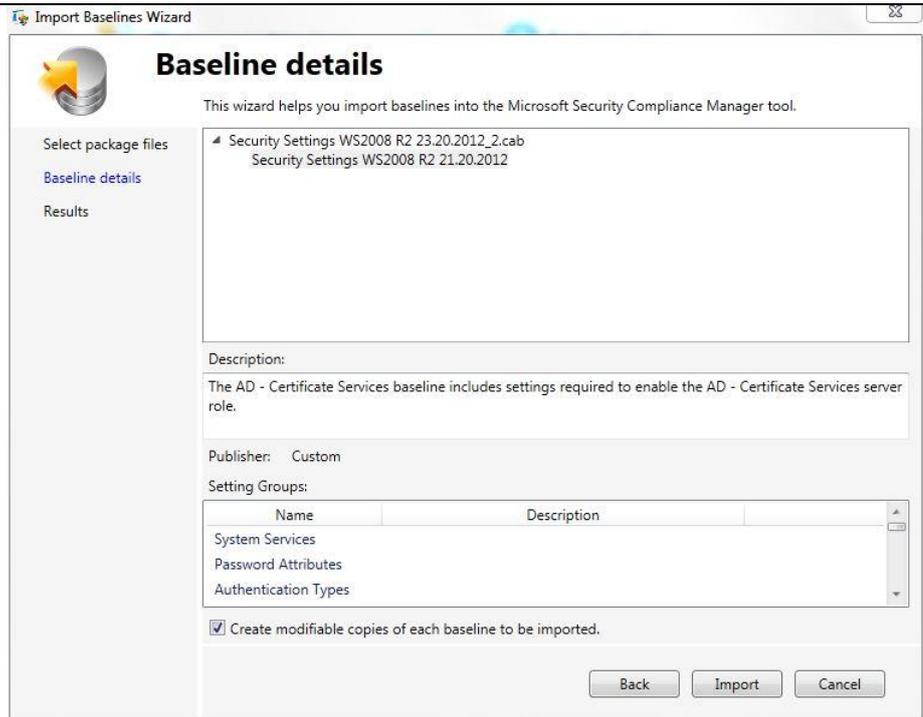
Es folgt eine Zusammenfassung der Baseline-Details.

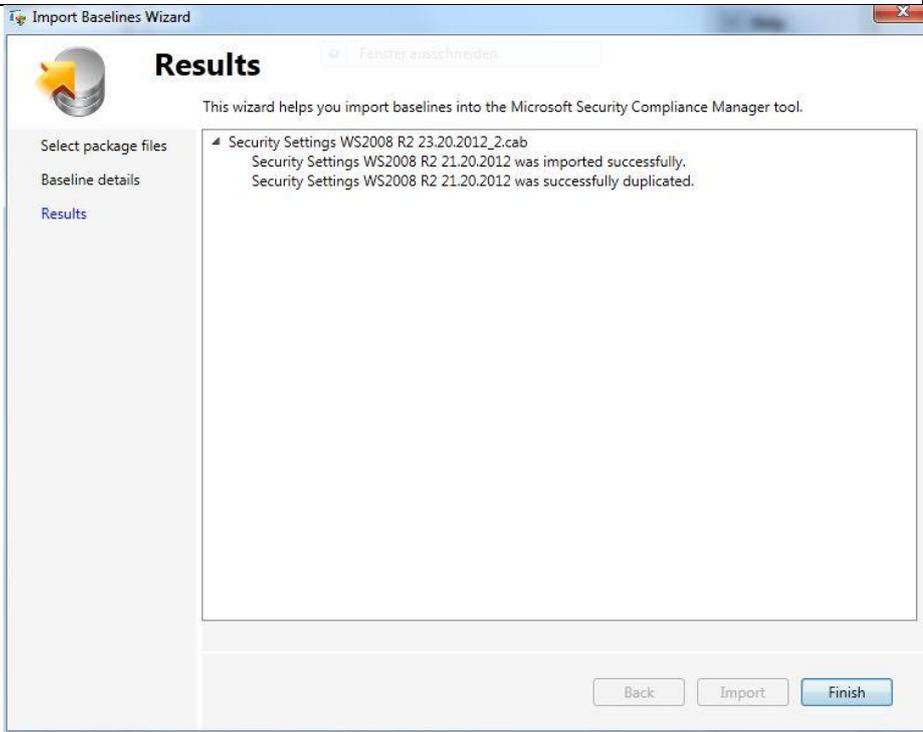
Die Option „*Create modifiable copies of each baseline to be imported*“ auswählen.

Diese Einstellung erlaubt es, die importierte Baseline gemäß den Sicherheitsanforderungen des Unternehmens anzupassen, da Standard-Baselines schreibgeschützt sind und immer unverändert bleiben. Die editierbare Baseline erscheint dann unter der Rubrik „*Custom Baselines*“.

Abschließend die Baselines mittels des „*Import*“ Befehls importieren.

Ggf. muss eine Abfrage, ob die Baseline importiert werden soll, obwohl sie im Original nicht auf dem System



<p>vorhanden ist, mit „OK“ bestätigt werden.</p>	
<p>Nachdem der Import erfolgreich abgeschlossen ist, erscheint die entsprechende Statusmeldung. Zum Beenden auf „Finish“ klicken.</p>	

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.

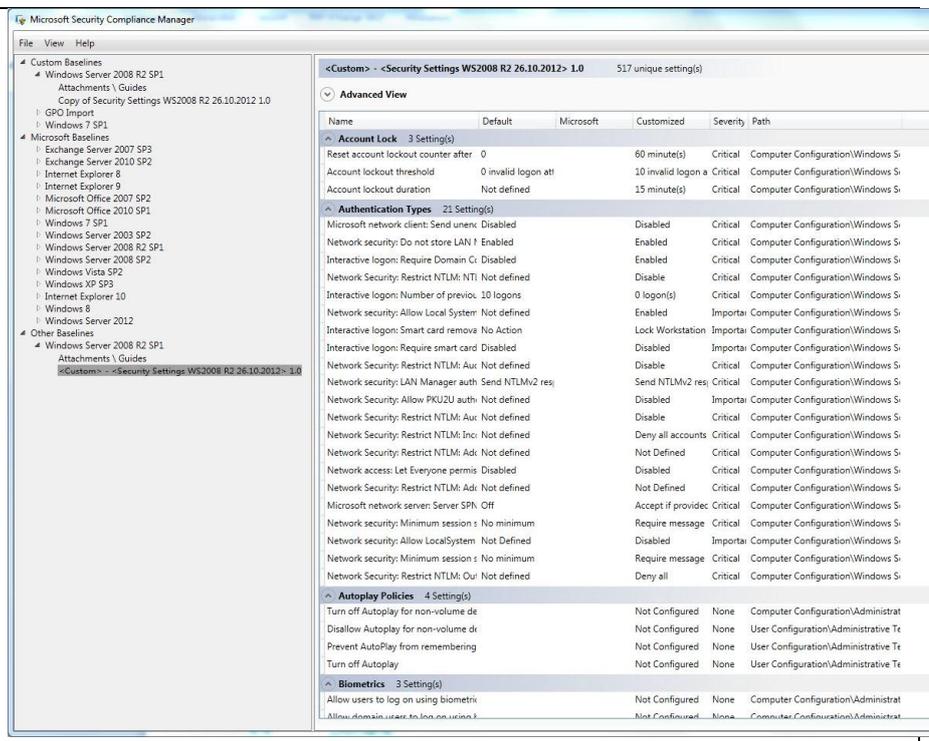
WARNUNG: Vor Applizieren einer Baseline auf einem Produktivsystem müssen sämtliche Einstellungen durch den Systemadministrator verifiziert werden. Eine Verteilung der Baseline ohne vorherige Prüfung kann die Funktionalität der betroffenen Systeme beeinträchtigen. Es wird daher dringend empfohlen, eine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

Der nächste Schritt besteht darin, dass die Einstellungen der Richtlinie an die Bedürfnisse der Organisation angepasst werden.



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.

Tabelle 4: Konfigurationskategorien der Baseline

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

	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 lokalen 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 Virenschernern 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.

		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 (SCCM) 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 Menü einer einzelnen Baseline (siehe Abbildung 6: Lock Funktion einer Baseline). Eine ausführliche Beschreibung der Sperrfunktion findet sich in der Hilfe des SCM.

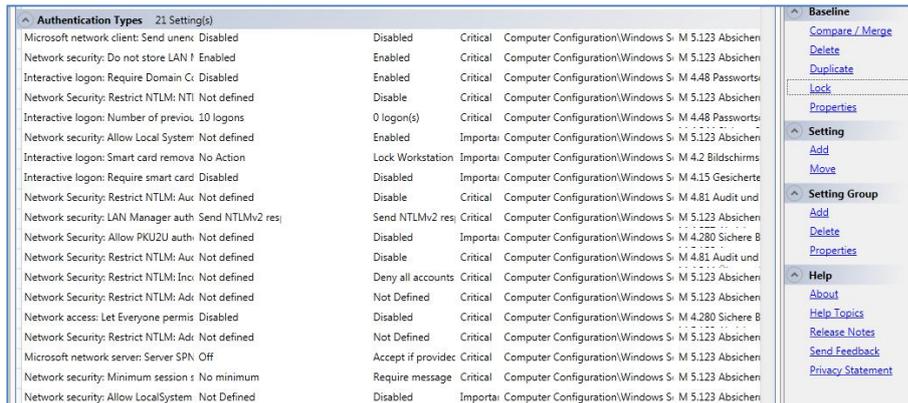


Abbildung 6: Lock Funktion einer Baseline

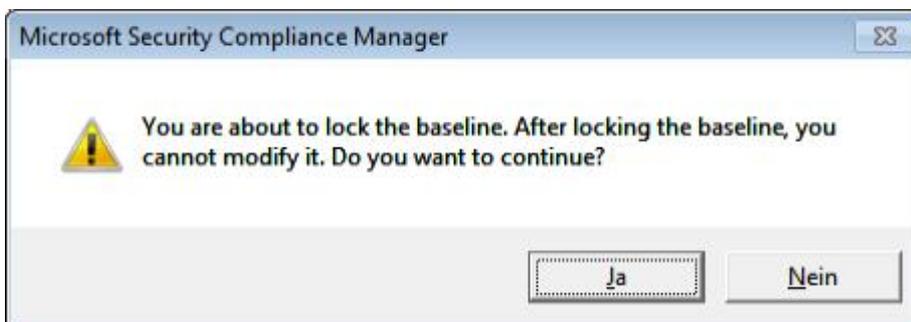


Abbildung 7: Hinweis zur Sperrung über die „Lock“ Option.

Nach erfolgreicher 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).

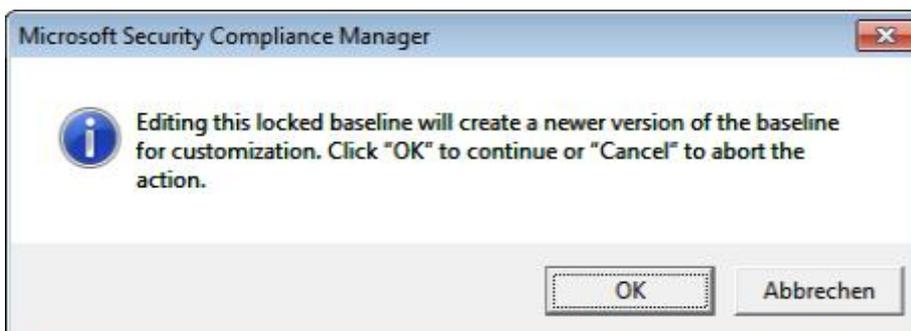


Abbildung 8: Erstellung einer Kopie

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.



Abbildung 9: Editierung einer Kopie

6.7 Import der Baseline auf Domänen-Systeme

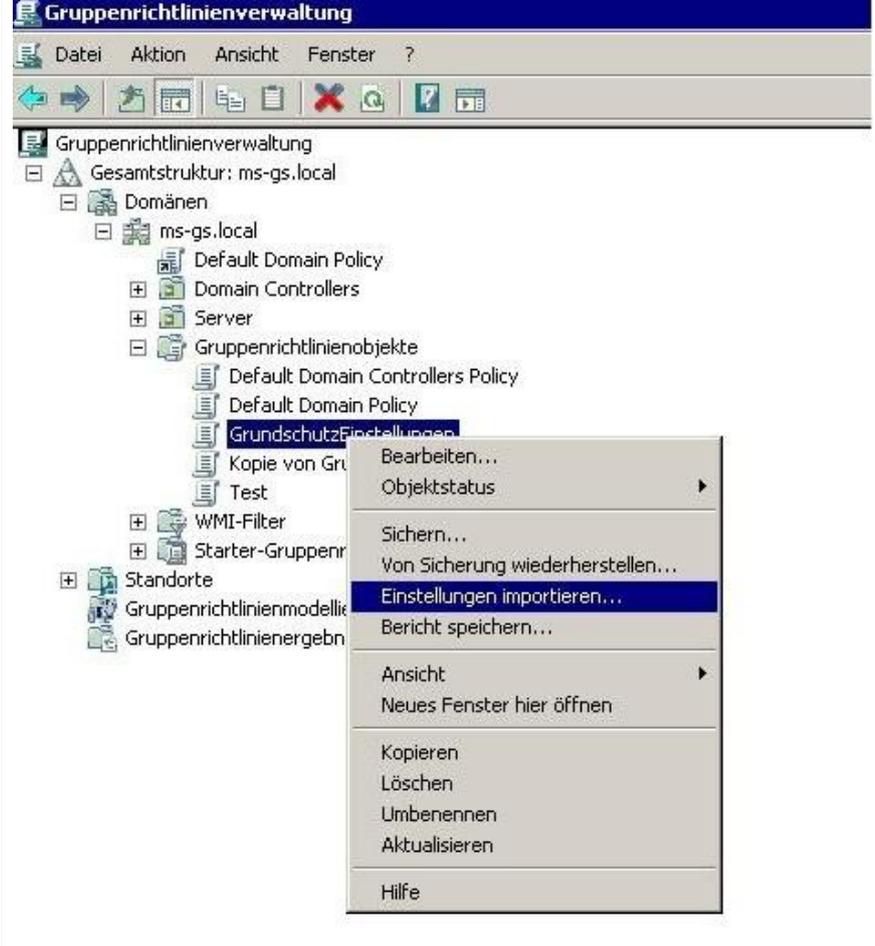
Im folgenden Abschnitt wird die Vorgehensweise für Serversysteme beschrieben, die ihre Gruppenrichtlinieneinstellungen zentral über einen Domain Controller beziehen.

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 Gruppenrichtlinienverwaltungskonsolle kann die exportierte Gruppenrichtlinie durch den Menüpunkt „*Einstellungen importieren*“ importiert werden.

Tabelle 5: Importieren von Einstellungen auf einem Domänencontroller

<p>Durch Rechtsklick auf ein bestehendes Gruppenrichtlinienobjekt können im Kontextmenü die Einstellungen importiert werden.</p>	 <p>The screenshot shows the 'Gruppenrichtlinienverwaltung' (Group Policy Management) console. The tree view is expanded to 'ms-gs.local' > 'Gruppenrichtlinienobjekte'. The 'Grundsicherungseinstellungen' (Security Settings) object is selected, and a context menu is open. The 'Einstellungen importieren...' (Import Settings...) option is highlighted in blue. Other options in the menu include 'Bearbeiten...', 'Objektstatus', 'Sichern...', 'Von Sicherung wiederherstellen...', 'Bericht speichern...', 'Ansicht', 'Neues Fenster hier öffnen', 'Kopieren', 'Löschen', 'Umbenennen', 'Aktualisieren', and 'Hilfe'.</p>
----------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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 [Microsoft-Link](#) ist ausführlich beschrieben, wie eine Verknüpfung von Gruppenrichtlinienobjekten durchzuführen ist.

6.8 Import der Baseline auf Stand-Alone-Systemen

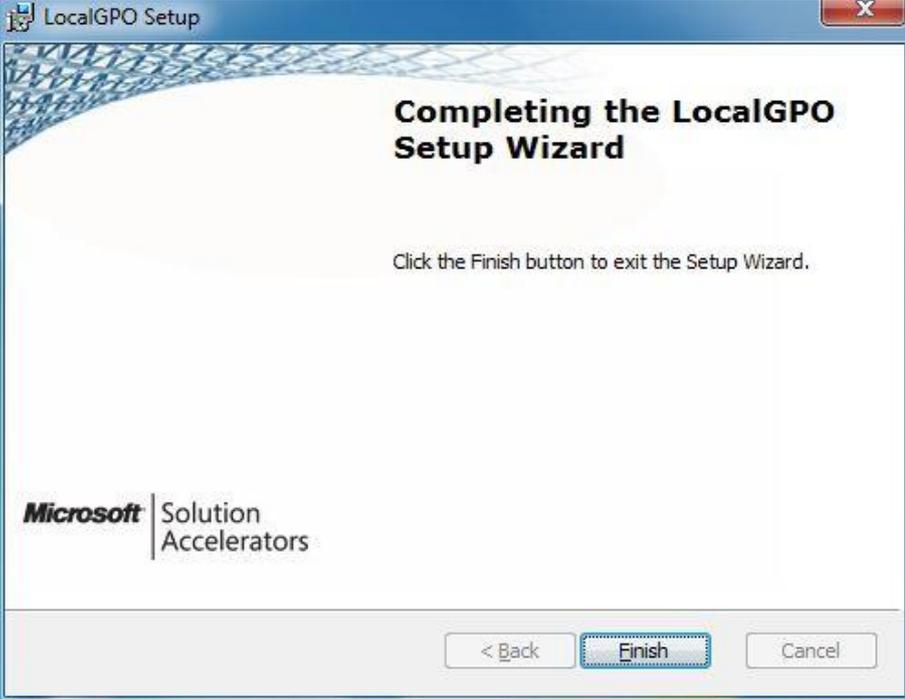
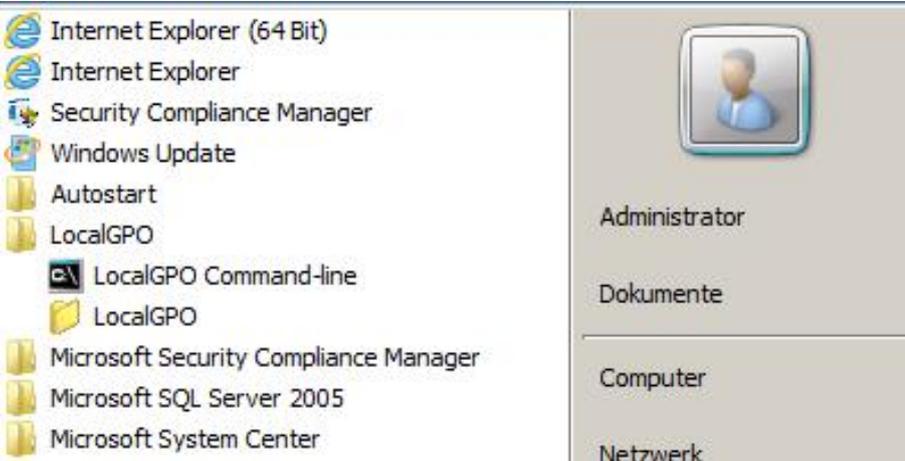
Sofern kein Active Directory (AD) im Unternehmen eingesetzt wird oder das System keine Anbindung an ein AD besitzt, weil es sich z. B. um ein DMZ System handelt, besteht auch die Möglichkeit, die Baseline als lokale Sicherheitsrichtlinie auf dem System zu integrieren.

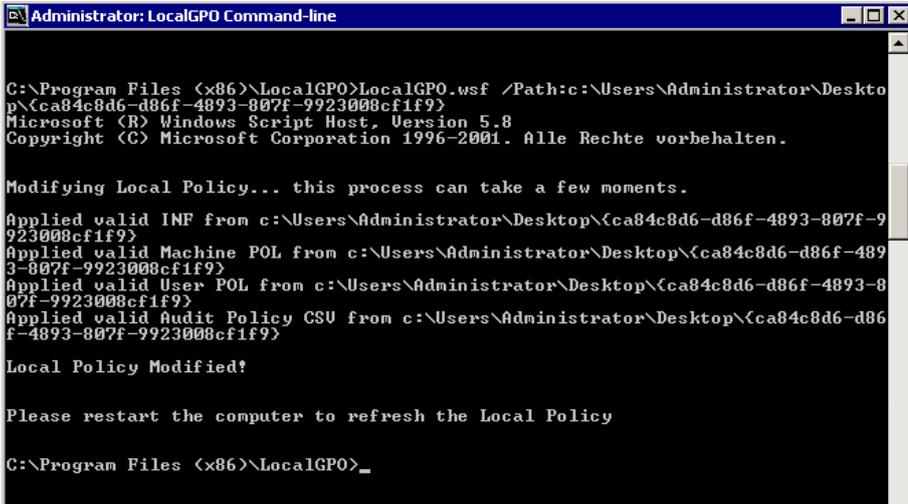
Für diesen Zweck stellt der Security Compliance Manager das Befehlszeilen-Tool *LocalGPO* zur Verfügung. Hiermit kann man die lokalen Richtlinien eines PCs in ein GPO-Backup exportieren und umgekehrt das exportierte GPO-Backup einer Baseline als lokalen Richtlinienatz anwenden. Das Tool wird bei der 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

<p>Sofern noch nicht auf dem Stand-Alone-System vorhanden, muss das Tool LocalGPO installiert werden.</p> <p>Die gewünschte Baseline ist aus dem Security Compliance Manager zu exportieren (GPO Backup-Folder) und auf das Zielsystem zu übertragen.</p>	
<p>Der LocalGPO Installations-Wizard führt den Administrator durch die Installation.</p>	

	
<p>Das Tool LocalGPO Command-line muss als Administrator ausgeführt werden. Nachdem sich das Kommandozeilenfenster geöffnet hat, kann mit dem Befehl im nächsten Fenster die Baseline auf das System appliziert werden.</p>	

<p>Zum Applizieren der in Abschnitt 6.4 überprüften Baseline ist folgende Kommandozeile auszuführen:</p>	
<p>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.</p>	

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	https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b03/b03101.html
Vorabversion Baustein B 3.109 Windows Server 2008	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Vorabversionen/Baustein_Win_Server_2008.pdf?blob=publicationFile

7.2 Microsoft

Security Compliance Manager	http://technet.microsoft.com/en-us/library/cc677002.aspx
Verknüpfen einer GPO mithilfe der Gruppenrichtlinienkonsole	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

info@hisolutions.com

www.hisolutions.com

Fon +49 30 533 289 0

Fax + 49 30 533 289 900