SICHERHEITSVORLAGE IT-GRUNDSCHUTZ WINDOWS 7

Version 1.0

24. März 2014

– ÖFFENTLICH –

1 ZUSAMMENFASSUNG

Ergänzend zum IT-Grundschutz-Baustein *Windows 7* hat die HiSolutions AG eine administrative Vorlage (Baseline) erstellt, die die Sicherheitsanforderungen der Grundschutzbausteine

- B 3.201 Allgemeiner Client und
- B 3.212 Client unter Windows 7

in Form eines editierbaren Templates zusammenfasst.

Zur Erstellung dieser Vorlage wurde der Microsoft Security Compliance Manager (SCM) verwendet, da dieser ein mächtiges, 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 für 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 sein, dass der zuständige Administrator sich mit den einzelnen Sicherheitseinstellungen unter Windows 7 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 Organisationen 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

2 EINLEITUNG

Das aktuell in Unternehmen am stärksten verbreitete Clientbetriebssystem Windows 7 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 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 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 einen bestimmten Sicherheitsstandard erfüllen.

Dieses Dokument beschreibt, wie mithilfe der „Sicherheitsvorlage IT-Grundschutz Windows 7“ eine IT-Grundschutz-konforme Basiskonfiguration erreicht werden kann.

Im Überblick stellt sich das Vorgehen des Einsatzes der Vorlage – auch als Baseline, GPO(s) oder Policy bezeichnet – 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 entbinden, die Einstellungen anforderungsgemäß und verantwortlich anzupassen.

Abweichungen von den Vorgaben der Maßnahmen des IT-Grundschutzes sind nach dem Vorgehensmodell 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. In dem hier erstellen Grundschutz-Template hingegen werden nur technische Maßnahmen umgesetzt, da eine Abbildung organisatorischer Aspekte mittels Template grundsätzlich nicht möglich ist. Die Umsetzung der organisatorischen Aspekte des IT-Grundschutzes für die jeweiligen Bausteine muss durch den IT-Sicherheitsbeauftragten der Organisation ergänzend koordiniert werden.

Das Template berücksichtigt grundsätzlich alle technischen Vorgaben der Maßnahmen der beiden Bausteine *Allgemeiner Client* und *Client unter Windows 7*. Allerdings besitzen einige Konfigurationswerte keine Wertzuweisung oder geben nur eine Basiskonfiguration vor, da bestimmte Einstellungen letztendlich nur gemäß den Vorgaben der jeweiligen Organisation zu spezifizieren sind. So bietet z. B. die 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 Einstellungen unterscheiden:

1. Einstellungen wie z. B. die Passwortlänge, die zugewiesene Werte besitzen. Diese Vorgaben müssen auf ihre Angemessenheit für die Organisation überprüft werden.
2. Einstellungen wie etwa zu BitLocker, denen keine konkreten Werte zugewiesen wurden. Sollte die Einstellungsgruppe benötigt werden, so sind adäquate Werte zu setzen, die die Anforderungen der Organisation widerspiegeln.

Active Desktop - Überprüfung erforderlich	1 Setting(s)	
Disable Active Desktop		Enabled
Administrative Freigaben - Überprüfung erforderlich	1 Setting(s)	
MSS: (AutoShareWks) Enable Administrative Shares	Not defined	Disabled

Abbildung 1: Überprüfung der Werte notwendig (Fall 1)

BitLocker - Wertzuweisung erforderlich	27 Setting(s)	
Choose default folder for recovery password	Not Configured	Not Configured
Prevent memory overwrite on restart	Not Configured	Not Configured
Choose drive encryption method and cipher strengt	Not Configured	Not Configured
Provide the unique identifiers for your organization	Not Configured	Not Configured
Validate smart card certificate usage rule complianc	Not Configured	Not Configured
Configure use of passwords for fixed data drives	Not Configured	Not Configured
Configure use of smart cards on fixed data drives	Not Configured	Not Configured
Choose how BitLocker-protected fixed drives can be	Not Configured	Not Configured

Abbildung 2: Zuweisung der Werte notwendig (Fall 2)

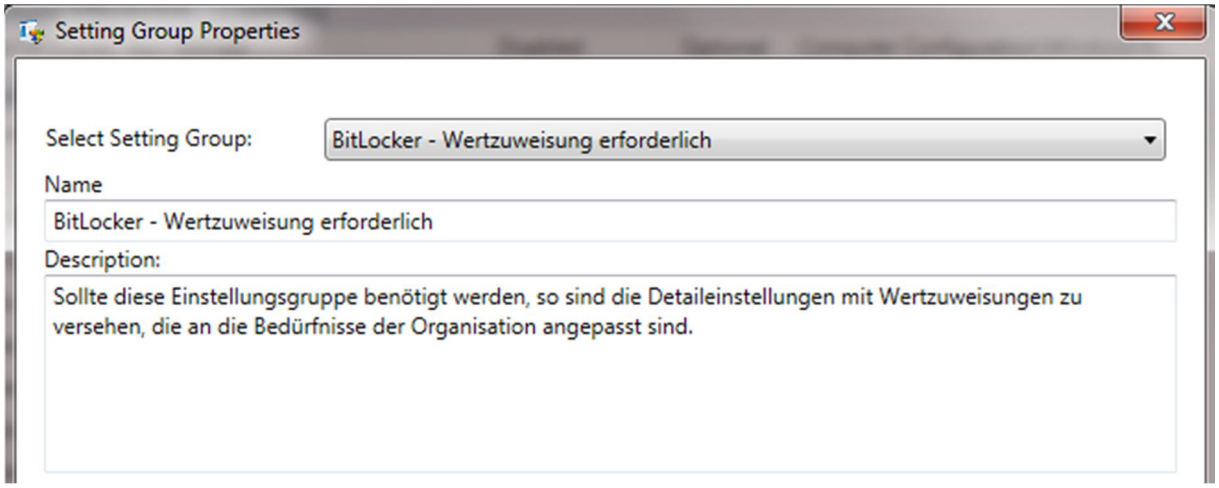


Abbildung 3: Beschreibung innerhalb der „Setting Group Properties“

Darüber hinaus werden bestimmte technische Einstellungen zur AD-Anbindung, zu speziellen Netzwerkfunktionen und zu Einzelanwendungen wie etwa Internet Explorer in diesem Template nicht vertieft, da sie nicht Teil der Bausteine *Allgemeiner Client* und *Client unter Windows 7* sind. Bei Bedarf können aber SCM-Einstellungen zu diesen Komponenten durch den Anwender des Templates zugefügt werden.

Entscheidend 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 CLIENT UNTER WINDOWS 7

Windows 7 stellt das vorletzte Client-Betriebssystem der Firma Microsoft dar. Es wurde am 22.10.2009 veröffentlicht und ist im Enterprise-Umfeld aktuell am weitesten verbreitet. Nachdem die Unterstützung für Windows 7 RTM ohne Service Pack am 9.4.2013 eingestellt wurde, ist Service Pack 1 die aktuelle Version mit einem Auslaufen des grundlegenden Supports am 13.1.2015 und des erweiterten Supports am 14.1.2020.[1]

Sowohl der Baustein als auch dieses Dokument und die zugehörige Vorlage beschäftigen sich primär mit der Windows 7 Enterprise Version; für die Versionen Windows 7 Professional und Windows 7 Ultimate sind ggf. Abweichungen zu beachten.

Der Schwerpunkt von Baustein und Template liegt zudem auf dem Einsatz von Clients in einer Domänenumgebung. Wichtige abweichende Sachverhalte, die speziell für Windows 7 auf Einzelplatzrechnern oder in einer Arbeitsgruppe gelten, werden ggf. hervorgehoben.

Der IT-Grundschutz-Baustein **B 3.212 Client unter Windows 7** stellt eine weitere Ergänzung zu den bereits in den IT-Grundschutz-Katalogen betrachteten Client-Betriebssystemen dar und wurde 2013 als Bestandteil der 13. Ergänzungslieferung der IT-Grundschutzkataloge des BSI veröffentlicht.[2] Der Baustein bietet einen Überblick über die aktuelle Gefährdungslage und liefert passende organisatorische sowie technische Maßnahmen zur Erlangung eines normalen Schutzbedarfs für Windows 7.

Der Baustein zählt 32 Gefährdungen aus allen Katalogen – Höhere Gewalt (1), Organisatorische Mängel (4), Menschliche Fehlhandlungen (10), Technisches Versagen (6) und Vorsätzliche Handlungen (11) – auf. Dem gegenübergestellt werden 45 dagegen gerichtete Maßnahmen für vier der fünf Phasen – Planung und Konzeption (22), Umsetzung (13), Betrieb (8) und Notfallvorsorge (2). Für die Phase der Aussonderung wird keine spezielle Maßnahme aufgeführt.

Im Vergleich zu den Bausteinen B 3.209 Client unter Windows XP und B 3.210 Client unter Windows Vista (beide im Stand der 11. Ergänzungslieferung von 2009) haben sich primär die folgenden Änderungen ergeben:

- Gefährdungen
  1. Höhere Gewalt
     - Wegfall aller Gefährdungen bis auf G 1.*2 Ausfall von IT-Systemen*; alle weiteren (Feuer, Wasser, Staub/Verschmutzung etc.) werden auf anderer Ebene betrachtet, nicht mehr am IT-System
  2. Organisatorische Mängel
     - Ergänzung zweier Gefährdungen im Vergleich mit Windows XP (G 2.19 *Unzureichendes Schlüsselmanagement* und G 2.62 *Ungeeigneter Umgang mit Sicherheitsvorfällen*)
     - Streichung einer rein Vista-spezifischen Gefährdung (G 2.146)
  3. Menschliche Fehlhandlungen
     - Ergänzung zweiter BitLocker-spezifischen Gefährdung von XP zu Vista (G 3.97 und G 3.98) und einer weiteren von Vista zu Windows 7 (G 3.112 zu Windows DISM[3])
  4. Technisches Versagen
     - Ergänzung zweier Gefährdungen von XP zu Vista (G 4.8 *Bekanntwerden von Softwareschwachstellen* und G 4.73 zu *Kompatibilitätsproblemen* von Vista/7)

[1] http://windows.microsoft.com/de-de/windows/products/lifecycle

[2] Es ist zu beachten, dass sich gegenüber der schon früher veröffentlichten Vorabversion des Bausteins (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Vorabversionen/Baustein_Win_7.pdf) erhebliche Änderungen ergeben haben. So finden sich etwa in der Phase Planung und Konzeption nun 22 statt vorher 9 Maßnahmen.

[3] http://msdn.microsoft.com/en-us/library/windows/desktop/dd371719%28v=vs.85%29.aspx

sowie einer weiteren von Vista zu Windows 7 (G 4.55 *Datenverlust beim Zurücksetzen des Kennworts ab Windows Server 2003 und XP*)

5. Vorsätzliche Handlungen
   - Bündelung von drei Gefährdungen zu G 5.23 *Schadprogramme* von XP zu Vista, keine Änderungen zu Windows 7

- Maßnahmen
  1. Planung und Konzeption
     - Deutliche Erweiterung von 12 auf 21 Maßnahmen von XP zu Vista
     - Aufnahme von Maßnahme M 4.425 *Tresor- und Cardspace-Funktionen* von Vista zu Windows 7
  2. Umsetzung
     - Streichung zweier Maßnahmen von XP zu Vista (M 5.52 *Geräteschutz unter NT-basierten Windows-Systemen* und M 5.57 *Deaktivieren der automatischen CD-ROM-Erkennung*)
     - Erweiterung um vier Maßnahmen zu M 4.419 *AppLocker (Z)*, M 4.421 *PowerShell*, M 4.423 *Heimnetzgruppen-Funktion* sowie M 4.424 *Sicherer Einsatz älterer Software (Z)* von Vista zu Windows 7
  3. Betrieb
     - Streichung zweier XP-spezifischer Maßnahmen von XP zu Vista (M 2.329 *Windows XP Servicepack 2* und M 4.148 *Überwachung eines Windows 2000/XP Systems*)
     - Ergänzung dreier Maßnahmen von XP zu Vista (M 2.443 *Windows Vista SP1*, M 4.343 *Reaktivierung aus einem Volumenlizenzvertrag* und M 4.344 *Überwachung*)
     - Streichung der eben genannten Vista-spezifischen Maßnahme M 2.443 *Windows Vista SP1* von Vista zu Windows 7
     - Ergänzung zweier Maßnahmen von Vista zu Windows 7 (M 4.420 *Sicherer Einsatz des Wartungscenters (A)* und M 4.422 *BitLocker To Go (Z)*)
  4. Aussonderung
     - Unverändert keine Maßnahmen für diese Phase
  5. Notfallvorsorge
     - Unverändert zwei Maßnahmen für diese Phase (M 6.76 *Notfallplan* und M 6.78 *Datensicherung*)

Hinzu kommt, dass diverse Maßnahmen über die Ergänzungslieferungen aktualisiert wurden und nun auch in ihrem Inhalt an die neueren Windows-Clientbetriebssysteme angepasst sind.

Darüber hinaus wurde für das vorliegende Template auch der Baustein **B 3.201 Allgemeiner Client** herangezogen, welcher sich auf dem Stand der 12. Ergänzungslieferung von 2011 befindet. Er zählt weitere 19 Maßnahmen auf und ist für alle Clientsysteme unabhängig vom Betriebssystem anzuwenden.

Die 19 Maßnahmen des Bausteins B 3.201 *Allgemeiner Client* sowie die 45 Maßnahmen des Bausteins B 3.212 *Client unter Windows 7* beschreiben nur zum Teil technische Anforderungen oder Konfigurationen. Darüber hinaus werden organisatorische und prozessuale Schritte beschrieben und gefordert, die grundsätzlich nicht mit Hilfe von Gruppenrichtlinien umgesetzt werden können wie etwa die Forderung der Existenz eines Dokuments „Sicherheitsrichtlinie“. Jede Grundschutz-Maßnahme kann mehrere technische und organisatorische Teilmaßnahmen bzw. -anforderungen enthalten.

Bei den technisch umsetzbaren (Teil-)Maßnahmen wiederum gibt es solche, die durch das Setzen von Gruppenrichtlinienobjekten umgesetzt werden können (etwa eine Passwortrichtlinie) und solche, die prinzipiell anderer technischer Mittel bedürfen (z. B. die Installation einer Virenschutzlösung). Und schließlich spielt die „Siegelstufe“ der jeweiligen Maßnahme eine Rolle, also ob die Maßnahme in einer bestimmten Phase der Zertifizierung obligatorisch umzusetzen ist (A,B,C), ob diese bei Bedarf zusätzlich umgesetzt werden kann (Z) oder lediglich Wissen vermittelt (W). Dies ist im Template insofern berücksichtigt, dass Z-Maßnahmen als fakultativ gekennzeichnet sind.

5 SECURITY COMPLIANCE MANAGER (SCM)

Gruppenrichtlinien gehören zu den wichtigsten Werkzeugen 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 sowie die verschiedenen Versionen des Windows-Client-Betriebssystems und von Anwendungssoftware wie Internet Explorer, Microsoft Office oder Exchange Server. Die Ausführungen *Specialized Security – Limited Functionality* (für hohe Sicherheitsanforderungen) sowie *Enterprise Client* für Windows XP, Vista und 7 wurden aufgelöst zugunsten einheitlicher Templates mit einer Einstufung der Kritikalität vieler Settings nach folgender Tabelle:

SCM severity	DCM severity	SCAP severity
Critical	Critical	High
Important	Warning	Med
Optional	Informational	Info\Low
None	Other	Unknown

Tabelle 1: SCM Severity-Level

In der aktuellen Version 3 des SCM werden neben Windows 7 SP1 und Windows 2008 Server-Systemen mittlerweile auch Windows 8 und Windows Server 2012 unterstützt.

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

- Absicherung von Microsoft-Produkten (Windows Server, Windows Client, Office, Exchange Server, Internet Explorer)
- Zentrale Speicherung und Verwaltung von Baselines
- Möglichkeit der Nutzung von Baselines auf Stand-Alone- und Domänensystemen
- Vergleich und Zusammenführung (Merge) von Baselines
- Verschiedene Import- und Exportmöglichkeit
- Ausführliche integrierte Hilfe und Beschreibung der einzelnen Einstellmöglichkeiten

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 Version 2.5 als auch mit der aktuellen Version 3 des SCM bearbeiten.

Tabelle 2: Voraussetzungen 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[4]
	Microsoft Excel® 2007 oder später (optional für Export)
Rechte	Administratorrechte für die Installation des SCM. 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 kann der SCM über das Windows-Startmenü gestartet werden. Das erstmalige Einlesen der Vorlagen und Richtlinien nimmt gegebenenfalls einige Minuten in Anspruch.

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

6.2 Aufbau des Security Compliance Managers

Die folgende Grafik illustriert den Aufbau des Security Compliance Managers:

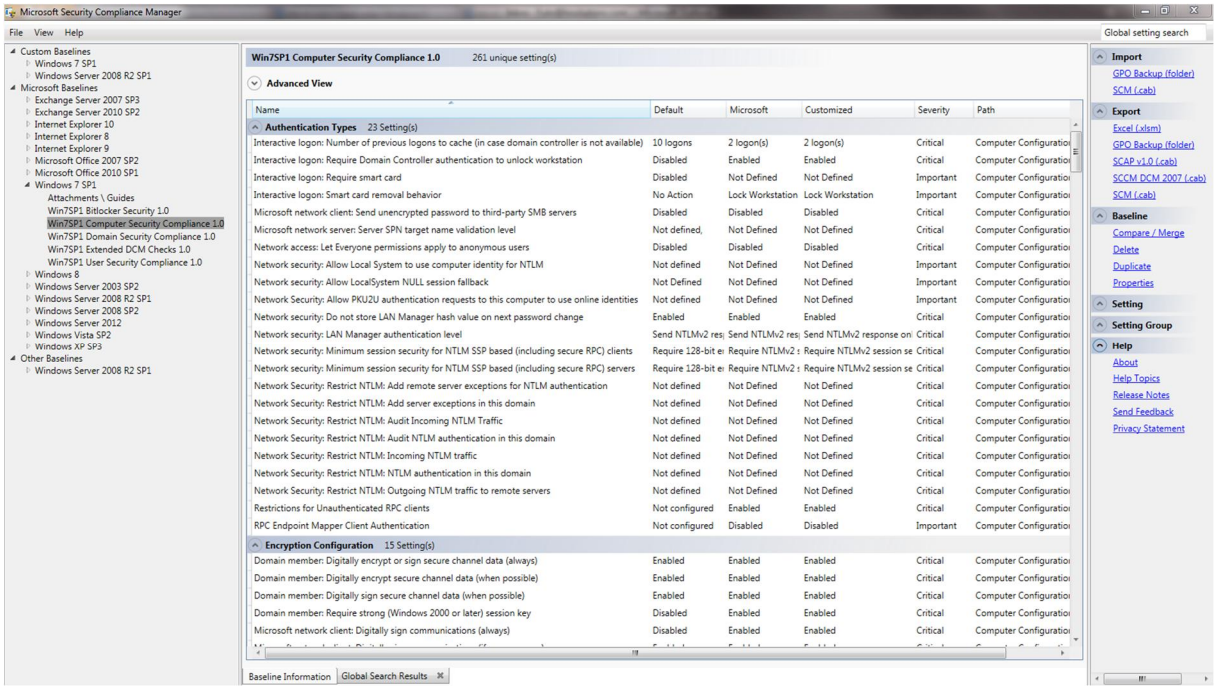


Abbildung 4: Aufbau des SCM

Auf der linken Seite erfolgt die Auswahl des abzusichernden Produkts. Nachdem ein entsprechendes Produkt ausgewählt worden ist (hier Windows 7 SP1), 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-ID[5] verwiesen)
- Schwachstelle
- Auswirkungen
- Gegenmaßnahmen

[5] Common Configuration Enumeration, siehe http://cce.mitre.org/.

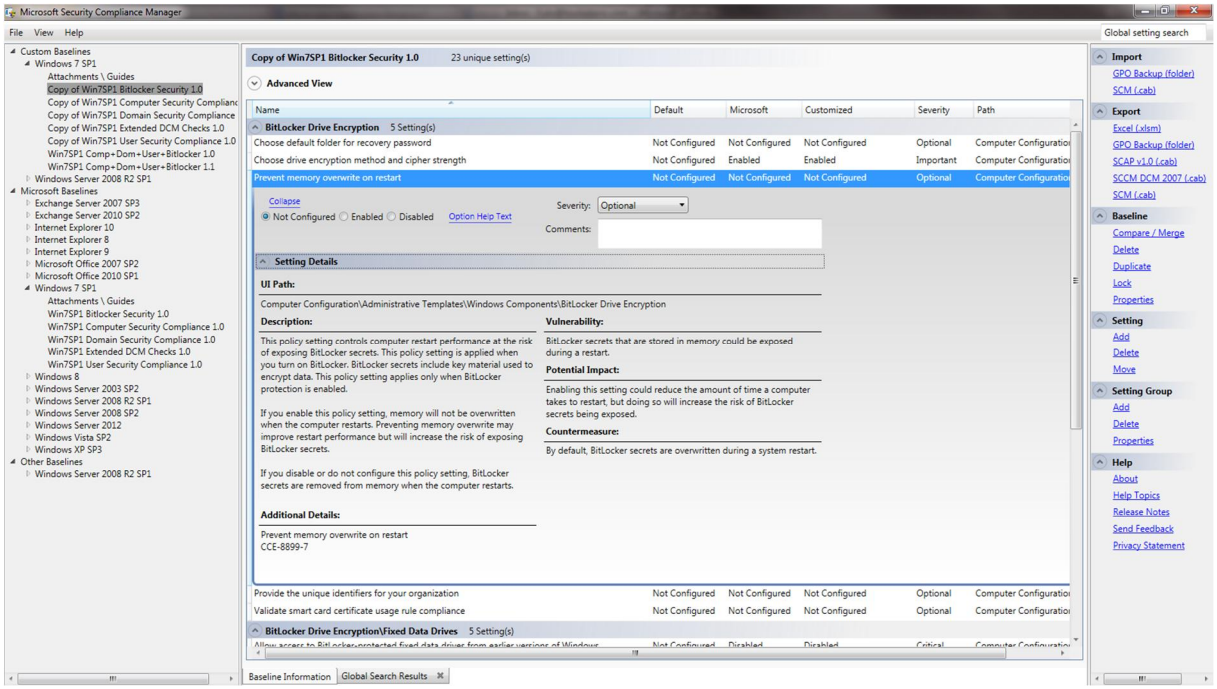


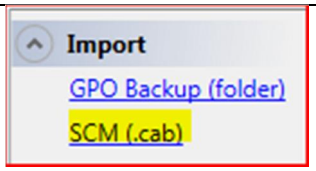
Abbildung 5: Detaillierte Konfigurationseinstellungen

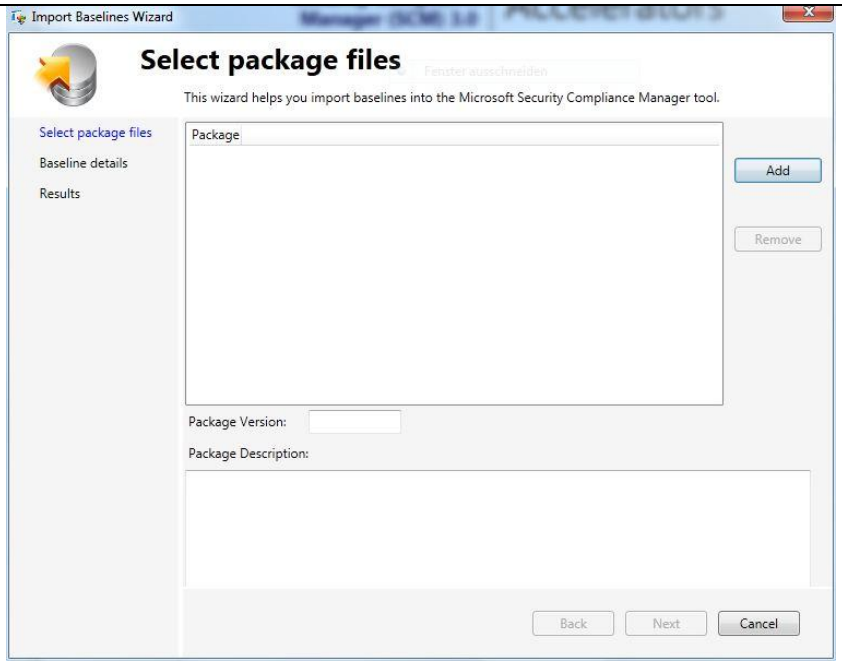
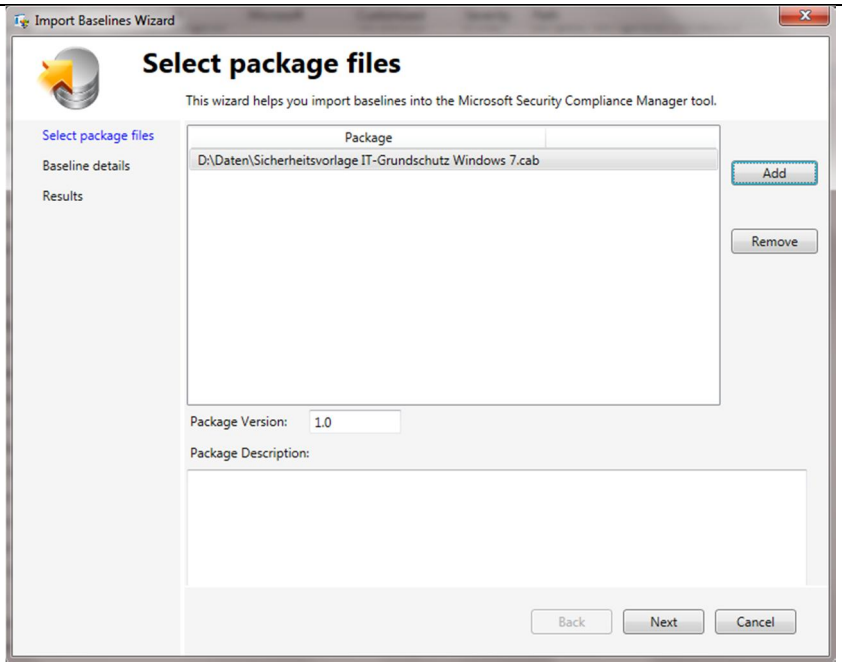
Es empfiehlt sich immer, eine bereits bestehende Baseline anzupassen, da bei dieser im Vergleich zu einer leeren Gruppenrichtlinie bereits Sicherheitsempfehlungen von Microsoft enthalten sind, welche zu einer Grundsicherheit des Systems beitragen.

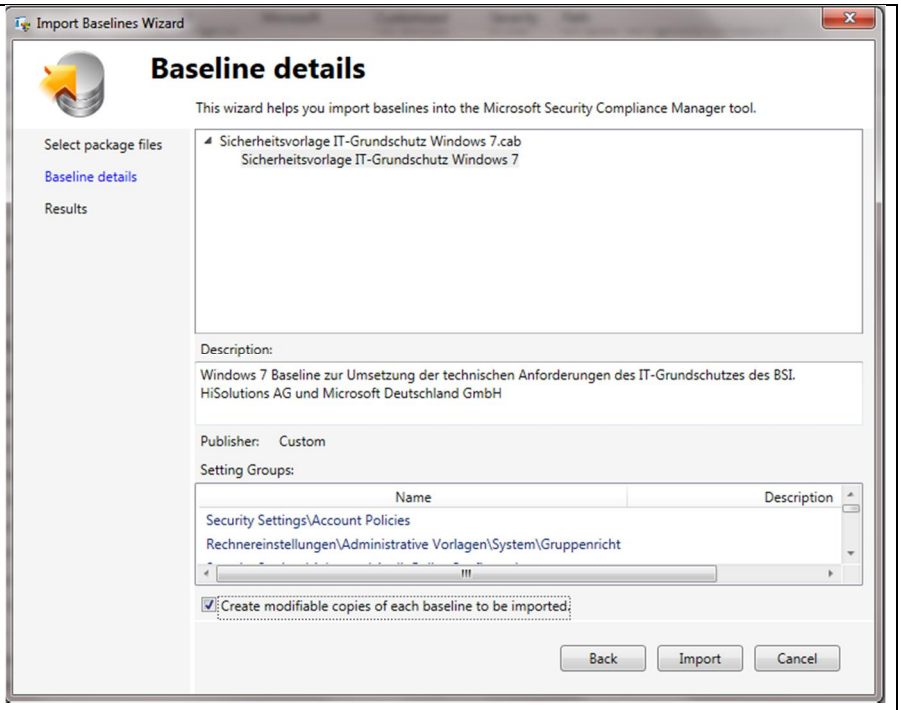
6.3 Importieren der HiSolutions Baseline für Windows 7

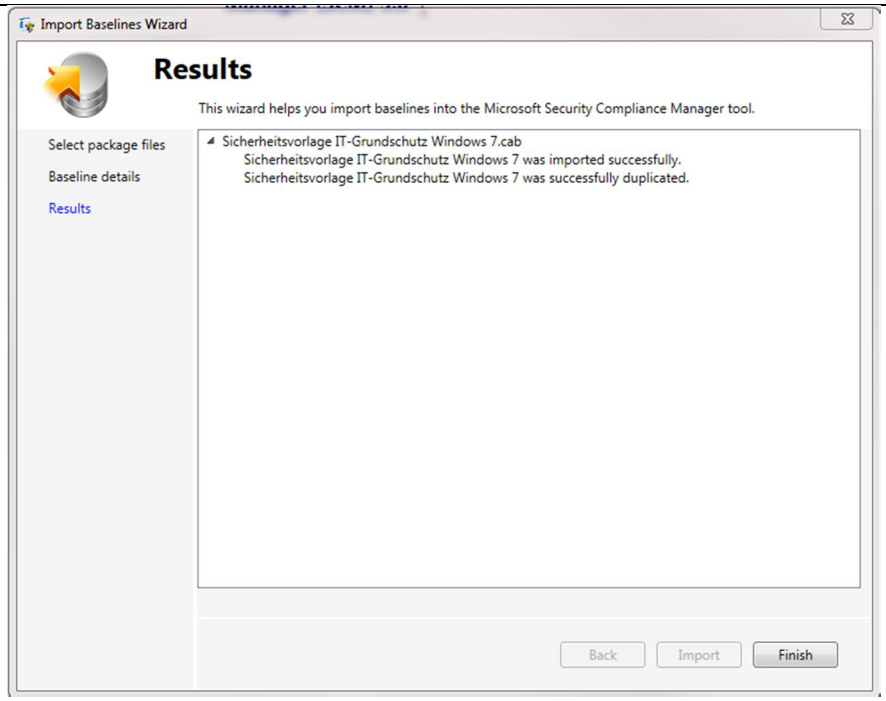
Nach der Installation des SCM muss die von HiSolutions in Form einer CAB-Datei bereitgestellte Baseline für Windows 7 in den SCM importiert werden. Die Grafiken in Tabelle 3 veranschaulichen die Vorgehensweise.

Tabelle 3: Vorgehensweise zum Import einer Baseline

Zum Importieren der Baseline im Import-Bereich auf *SCM (cab)* klicken. Der *Import Baselines Wizard* öffnet sich.	

Auf *„Add“* klicken und die zu importierende Baseline auswählen.	
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 vorhanden ist, mit „OK“ bestätigt werden.	

Nachdem der Import erfolgreich abgeschlossen ist, erscheint die entsprechende Statusmeldung. Zum Beenden auf *„Finish“* klicken.	

6.4 Anpassen einer Baseline

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

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

Diese Vorgehensweise ist insofern notwendig, als dass in den beiden IT-Grundschutz-Bausteinen diverse Anforderungen beschrieben werden, die nicht immer unbedingt auf zu den fachlichen Anforderungen der Organisation kompatibel sein müssen. Aus diesem Grund sind für solche Fälle meist noch die Default-Einstellungen oder von HiSolutions empfohlene Einstellungen aktiv, bzw. es sind noch gar keine Werte konfiguriert und die Einstellung benötigt daher eine weitere Anpassung. Dies betrifft zum Beispiel die Einstellungen in den Kategorien BitLocker, Firewall oder Startmenü und Taskleiste.

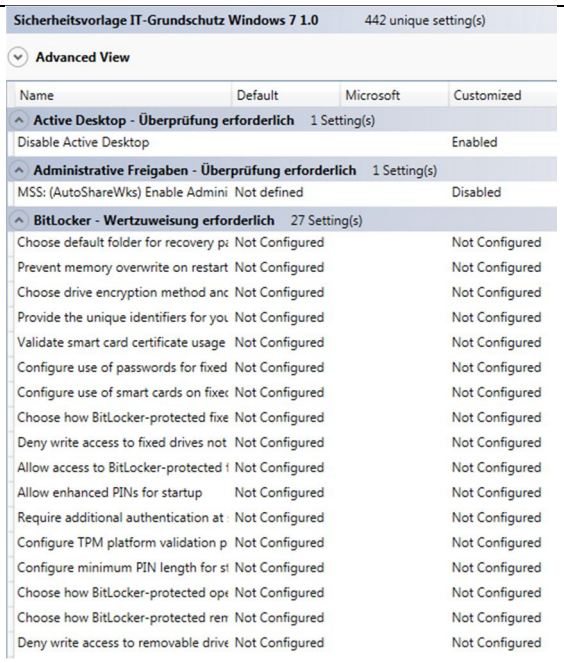
Um den Bezug zu den IT-Grundschutzbausteinen deutlich zu machen und eine Nachvollziehbarkeit zu bieten, erfolgt innerhalb des Templates im Kommentarfeld (*Comments*) zu jeder Konfigurationseinstellung eine Zuordnung der Einstellung zu einer oder mehreren Maßnahmen der Bausteine B 3.201 *Allgemeiner Client* und B 3.212 *Client unter Windows 7*.

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

Tabelle 4: Anpassen einer Baseline

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

Nachdem alle Einstellungen überprüft und angepasst worden sind, kann die Baseline nun entweder auf mehreren Clients in einer Domäne verteilt (siehe Abschnitt 6.7) oder auf ein Stand-Alone-System (siehe Abschnitt 6.8) angewandt werden.

Zunächst muss allerdings ein Export der Baseline in ein dafür benötigtes Format erfolgen. Abschnitt 6.5 beschreibt den Export einer angepassten Baseline, Abschnitt 6.6 das Sperren für die Versionsverwaltung von Baselines.

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.

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.

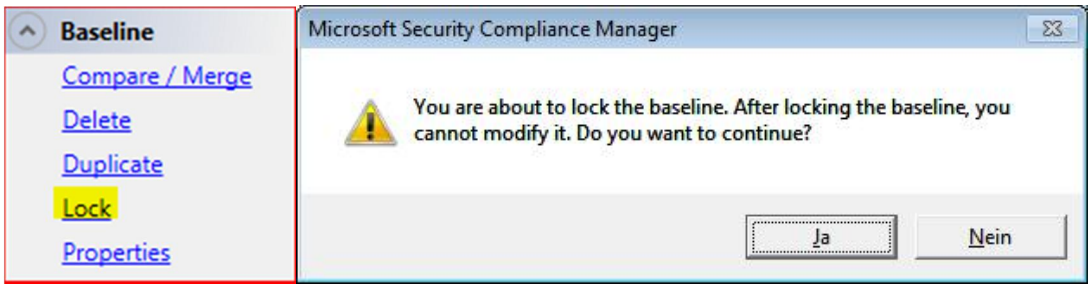


Abbildung 6: Lock-Funktion einer Baseline

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 7: Erstellung einer Kopie).

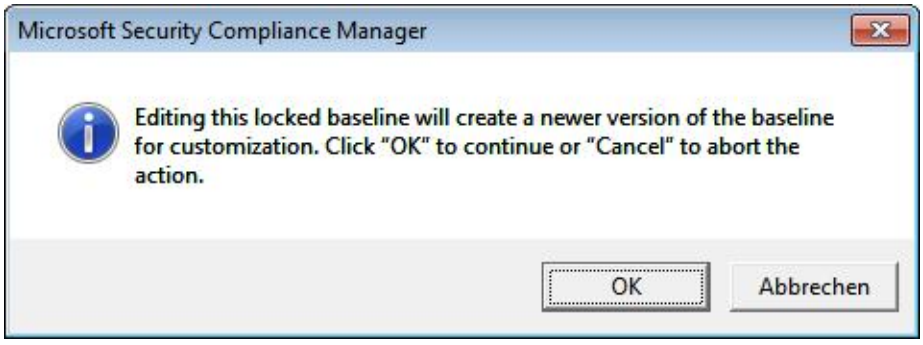


Abbildung 7: Erstellung einer Kopie

Durch die Edit-Funktion wird automatisch eine neue *Minor-Version* der Baseline erstellt (siehe Abbildung 8: Editierung einer Kopie). Diese Baseline kann nun als Basis weiterer Konfigurationen verwendet werden.

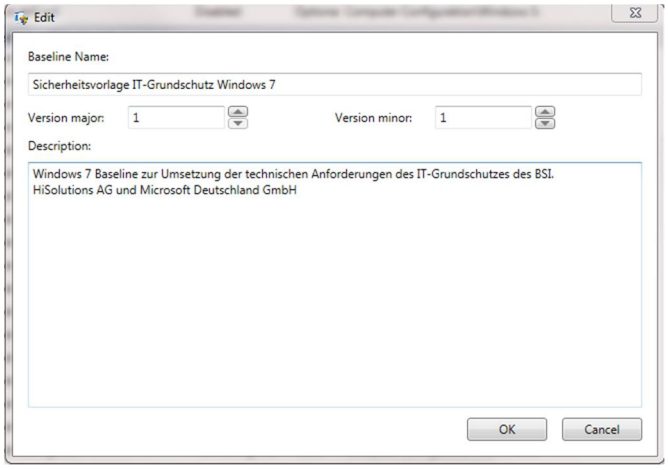


Abbildung 8: Editierung einer Kopie

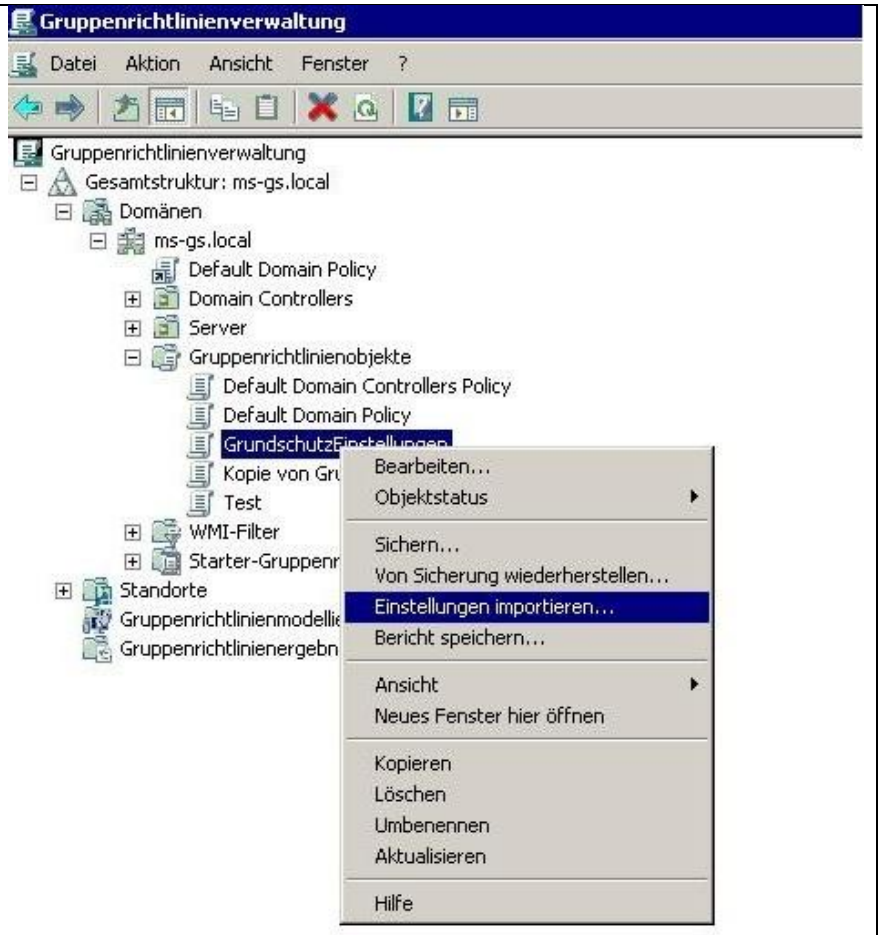
6.7 Import der Baseline auf Domänen-Systeme

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

Um eine exportierte SCM-Richtlinie in eine Gruppenrichtlinie zu importieren, muss der Gruppenrichtlinienverwaltung-Editor genutzt werden. Das Verzeichnis mit dem Gruppenrichtlinien-Export kann entweder als neue Richtlinie verwendet werden, oder die Einstellungen können in eine bereits bestehende Richtlinie übernommen werden.

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

Tabelle 5: Importieren von Einstellungen auf einem Domänencontroller

Durch Rechtsklick auf ein bestehendes Gruppenrichtlinienobjekt können im Kontextmenü die Einstellungen importiert werden.	

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

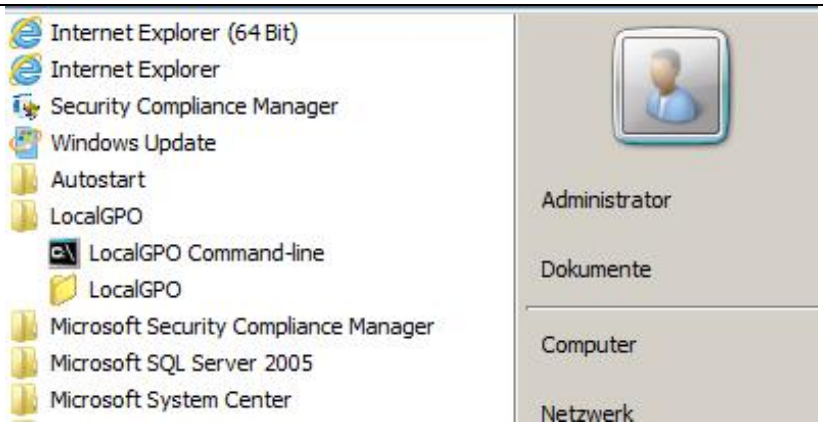
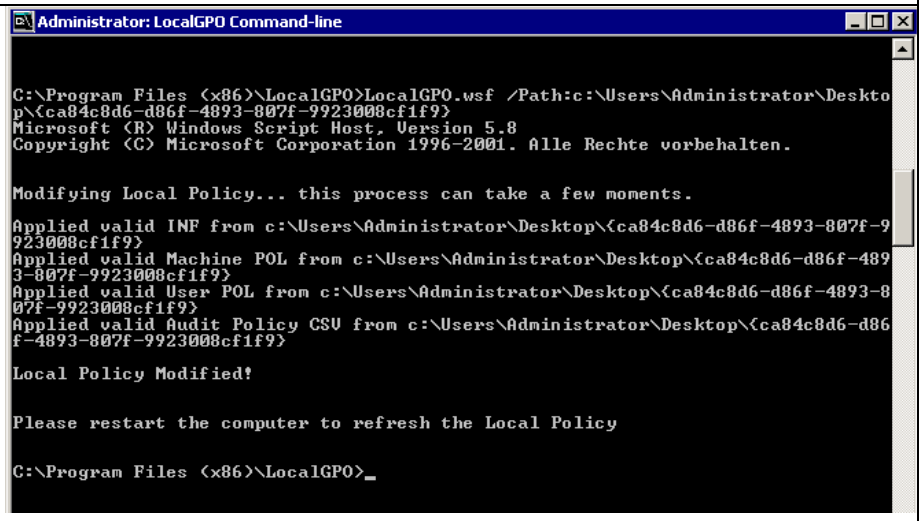
Wenn kein Active Directory (AD) im Unternehmen eingesetzt wird oder das System keine Anbindung an ein AD besitzt, besteht auch die Möglichkeit, die Baseline als lokale Sicherheitsrichtlinie auf das System aufzuspielen.

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, sodass 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.	
	

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.	
Zum Applizieren der in Abschnitt 6.4 überprüften Baseline ist folgende Kommandozeile auszuführen:	
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, sodass diese im Security Compliance Manager weiterbearbeitet werden können.

7 ANHANG

7.1 BSI

Baustein B 3.201 Allgemeiner Client	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03201.html
Baustein B 3.212 Windows 7	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b03/b03212.html

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

7.4 Tabellenverzeichnis

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