



# SICHERHEITSVORLAGEN IT-GRUNDSCHUTZ WINDOWS 8

Version 1.0

5. Oktober 2014

HiSolutions AG © 2014

– ÖFFENTLICH –





#### 1 ZUSAMMENFASSUNG

Basierend auf den bisher veröffentlichten IT-Grundschutz-Bausteinen für *Windows 7 (B 3.212)* und *Allgemeiner Client (B 3.201)* hat die HiSolutions AG administrative Vorlagen (Baselines) erstellt. Diese Vorlagen fassen die Sicherheitsanforderungen von Windows 8, für das bisher noch kein eigener Grundschutzbaustein veröffentlicht wurde, in Form von editierbaren Templates zusammen.

Bei der Erstellung der Templates wurden die Maßnahmen des Bausteins Windows 7 (B 3.212), welche ebenfalls für Windows 8 anwendbar sind, als Basis verwandt und zusätzlich neue Sicherheitsanforderungen von Windows 8 berücksichtigt.

Da sich Sicherheitsanforderungen häufig sinnvoll in computer- und nutzerbasierte Einstellungen unterteilen lassen, wurden zur einfacheren Administration zwei editierbare Template-Gruppen erstellt:

- Sicherheitsvorlage(n) für Computer
- Sicherheitsvorlage(n) für Benutzer

Zur Erstellung der Vorlagen wurde der Microsoft Security Compliance Manager (SCM) verwendet, da dieser ein mächtiges und 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 zu verwalten, und eignet sich daher für den Einsatz sowohl für Stand-Alone- als auch für Domänensysteme.

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

Für die Verwendung der Templates in produktiven Umgebungen ist es unbedingt notwendig, dass der jeweils zuständige Administrator sich mit den einzelnen Sicherheitseinstellungen unter Windows 8 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 der Vorlagen ohne vorherige Prüfung und adäquate Anpassung zu einem unerwünschten Verhalten der Systeme bis hin zum Ausfall von Funktionalität führen.





# INHALTSVERZEICHNIS

1	Z	ZUSAMMENFASSUNG						
IN	IHALTSVERZEICHNIS							
2	EINLEITUNG							
3	А	BGRENZUNG	4					
4	С	LIENT UNTER WINDOWS 8	6					
5	S	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	Aufbau der HiSolutions Baselines für Windows 8	10					
	6.4	Importieren der HiSolutions Baselines für Windows 8	10					
	6.5	Anpassen einer Baseline	13					
	6.6	15						
	6.7	15						
	6.8	16						
	6.9	Import der Baseline auf Stand-Alone-Systemen	17					
7	A	21						
	7.1	BSI	21					
	7.2	Microsoft	21					
	7.3	21						
	7.4	Tabellenverzeichnis	21					
	7.5	Begriffe	22					
KC	ONTAKT 2							



– ÖFFENTLICH –



### 2 EINLEITUNG

Das aktuell in vielen Unternehmen Einzug haltende Clientbetriebssystem Windows 8 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 verantwortliche 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 Sicherheitsvorlagen "IT-Grundschutz Windows 8" mit überschaubarem Aufwand eine IT-Grundschutz-konforme Basiskonfiguration erreicht werden kann.

Im Überblick stellt sich das Vorgehen des Einsatzes der Vorlagen – auch als Baselines, GPOs oder Policys bezeichnet – wie folgt dar:

Import des CAB	Anpassung	Versionskontrolle und Export	Import auf Zielsystem(en)
<ul> <li>Import des CAB in</li></ul>	<ul> <li>Anpassung der</li></ul>	<ul> <li>Abschließend Sperrung</li></ul>	<ul> <li>Import auf</li></ul>
den SCM	bestehenden Einstellungen	der Baseline	Zielsystem(en)
<ul> <li>Duplizierung gemäß</li></ul>	<ul> <li>Ggf. Zufügung eigener</li></ul>	<ul> <li>Export in gewünschtes</li></ul>	<ul> <li>Ggf. weiterer Export</li></ul>
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 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 den erstellten Grundschutz-Templates hingegen werden nur technische Maßnahmen umgesetzt, da eine Abbildung organisatorischer Aspekte mittels technischer Templates generell nicht möglich ist. Die Umsetzung der organisatorischen Aspekte des IT-Grundschutzes muss durch den Informationssicherheitsbeauftragten der Organisation ergänzend koordiniert werden.

Die Templates berücksichtigen grundsätzlich alle technischen Vorgaben der Maßnahmen des Bausteins *Allgemeiner Client* und, soweit diese auf Windows 8 übertragbar sind, die Maßnahmen des Bausteins *Client unter Windows 7* sowie *neue Windows 8-spezifische Sicherheitseinstellungen*. 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 der Templates keine dedizierten organisationstypischen 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 einund ausgehenden Verkehr notwendig sind und ob diese auf Basis von Anwendungen oder von IP-Adressen und Ports erfolgen soll. Dies sollte dann über den "Group Policy Manager" im Pfad *Computer Configuration | Policies | Windows Settings | Security Settings | Windows Firewall with Advanced Security* 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.
- 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; Beispiel)

(	<ul> <li>BitLocker - Wertzuweisung erforderlich 27 S</li> </ul>	etting(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								
ŀ	Abbildung 2: Zuweisung der Werte notwendig (Fall 2; Beispiel)								





🙀 Setting Group Properties	Andrea Second Second Second Sector Sec.	×
Select Setting Group: Name	BitLocker - Wertzuweisung erforderlich	•
BitLocker - Wertzuweisung	erforderlich	
Description:		
Sollte diese Einstellungsgr versehen, die an die Bedür	uppe benötigt werden, so sind die Detaileinstellungen mit Wertzuweisungen zu fnisse der Organisation angepasst sind.	

Abbildung 3: Beschreibung innerhalb der "Setting Group Properties" (Beispiel)

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 zugrunde liegenden Grundschutz-Bausteine sind. Bei Bedarf können aber SCM-Einstellungen zu diesen Komponenten durch den Anwender des Templates hinzugefügt werden.

Entscheidend ist, dass die Templates erst auf ein System angewendet werden dürfen, nachdem sie zuvor durch einen zuständigen Administrator gesichtet und angepasst wurden. 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 CLIENT UNTER WINDOWS 8

Windows 8 stellt das aktuellste Client-Betriebssystem der Firma Microsoft dar. Es wurde am 26.10.2012 als Nachfolger von Windows 7 veröffentlicht und ist ein gleichermaßen für Desktop- wie für Touch-Geräte optimiertes Betriebssystem. Am 18.10.2013 veröffentlichte Microsoft Windows 8.1, welches ein kostenloses, umfangreiches Update für Windows 8 darstellt.

Dieses Dokument und die zugehörigen Vorlagen beschäftigen sich primär mit der Enterprise Version von Windows 8.1; für die Versionen Windows 8 Pro und Windows 8 sind ggf. Abweichungen zu beachten. Windows RT wird in diesem Dokument nicht betrachtet.

Der Schwerpunkt der Templates liegt zudem auf dem Einsatz von Client-Systemen in einer Domänenumgebung. Wichtige abweichende Sachverhalte, die speziell für Windows 8 auf Einzelplatzrechnern oder in einer Arbeitsgruppe gelten, werden ggf. hervorgehoben.

Derzeit wurde noch kein Grundschutz-Baustein für Windows 8 veröffentlicht. Da es jedoch viele Ähnlichkeiten zum Vorgängerbetriebssystem Windows 7 gibt, hat die HiSolutions AG auf Basis der IT-Grundschutz-Bausteine B 3.212 *Client unter Windows* 7 und B 3.201 *Allgemeiner Client* die für Windows 8 zutreffenden Maßnahmen und Gefährdungen bei der Erstellung der Templates berücksichtigt.

Der Baustein B 3.212 *Client unter Windows* 7 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 wirkende 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.

Der Baustein B 3.201 *Allgemeiner Client* zählt weitere 19 Maßnahmen auf und ist für alle Clientsysteme unabhängig vom Betriebssystem anzuwenden.

Nach Ansicht der HiSolutions AG können diese Maßnahmen auch auf einen Windows 8 Client angewendet werden. Zusätzlich dazu ergeben sich aus der bisherigen Erfahrung und Untersuchungen die folgenden neuen Gefährdungen bei Windows 8:

- Lock-in-Effekt (bei Nutzung einer App oder eines Cloud-Dienstes)
- Integrierte Cloud-Funktionalität
- Integrierte TPM-Nutzung

Diese berücksichtigend, schlägt HiSolutions folgende neue Maßnahmen für Windows 8 vor:

- Beschaffung von Windows 8
- Gewährleistung des Datenschutzes unter Windows 8

Die Maßnahmen der Grundschutzbausteine 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 8/8.1 und Windows Server 2012 (auch R2) 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



– ÖFFENTLICH –



## 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	<b>?</b> • '	Voraussetzungen	zur	Installation	des	SCM
	<u> </u>	Volaussetzungen	zui	matanation	aco	CON

Betriebssystem	Windows® 7 x64 oder später			
	Windows Server® 2008 oder Windows Server® 2008 R2			
	Windows Server® 2012 oder Windows Server® 2012 R2			
Benötigter Arbeitsspeicher	500 MB			
Zusätzlich benötigte Software	Microsoft® .NET Framework 4			
	Microsoft SQL Server® 2005, SQL Server® 2008 oder SQL Server® 2008 R2 <sup>1</sup>			
	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 einem System mit mindestens Windows 7 oder Windows Server 2012 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.

<sup>&</sup>lt;sup>1</sup> 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.



– ÖFFENTLICH –



## 6.2 Aufbau des Security Compliance Managers

Die folgende Grafik illustriert den Aufbau des Security Compliance Managers:

12: Microsoft Security Compliance Manager								
File View Help							Global setting search	
Custom Baselines Undows 8 Microsoft Baselines Exchange Server 2007 SP3 Exchange Server 2007 SP3	Win8 Computer Security Compliance 1.0         3: <ul></ul>	Import     GPO Backup (folder)     SCM (.cab)						
Exchange Server 2010 SP2     Internet Explorer 10	Name	Default	Microsoft	Customized	Severity	Path	A Export	
Internet Explorer 8	Encryption Configuration 17 Setting(s)					*	Excel (.xism)	
Internet Explorer 9 Microsoft Office 2007 SP2	Microsoft network client: Digitally sign communication	Disabled	Enabled	Enabled	Critical	Computer Configuration\Windows Settings\Security Setting	GPO Backup (folder)	
Microsoft Office 2010 SP1	Microsoft network client: Send unencrypted passwor	Disabled	Disabled	Disabled	Critical	Computer Configuration\Windows Settings\Security Setting	SCAP v1.0 (.cab)	
Windows 7 SP1	Network security: Minimum session security for NTL	Require 128-bit e	Require NTLMv2	Require NTLMv2	Critical	Computer Configuration\Windows Settings\Security Setting	SCCM DCM 2007 (.cab)	
<ul> <li>Attachments \ Guides</li> </ul>	Domain member: Digitally sign secure channel data	Enabled	Enabled	Enabled	Critical	Computer Configuration\Windows Settings\Security Setting	SCM (.cab)	
Win8 BitLocker Security 1.0	System cryptography: Force strong key protection fo	Disabled	Not Defined	Not Defined	Important	Computer Configuration\Windows Settings\Security Setting	A Baseline	
Win8 Computer Security Compliance 1.0	Domain member: Require strong (Windows 2000 or	Disabled	Enabled	Enabled	Critical	Computer Configuration\Windows Settings\Security Setting	Compare / Merge	
Wine Domain Security Compliance 1.0 Wine Extended DCM Checks 1.0	Microsoft network server: Digitally sign communicati	Disabled	Enabled	Enabled	Critical	Computer Configuration\Windows Settings\Security Setting	Delete	
Win8 User Security Compliance 1.0	Network Security: Configure encryption types allowe	Not defined	RC4\AES128\AES2	RC4\AES128\AES	Important	Computer Configuration\Windows Settings\Security Setting	Duplicate	
<ul> <li>Windows Server 2003 SP2</li> <li>Windows Server 2008 R2 SP1</li> </ul>	System cryptography: Use FIPS compliant algorithms	Disabled	Enabled	Enabled	Important	Computer Configuration\Windows Settings\Security Setting	Properties	
Windows Server 2008 SP2	Microsoft network client: Digitally sign communication	Enabled	Enabled	Enabled	Critical	Computer Configuration\Windows Settings\Security Setting	Satting	
<ul> <li>Windows Server 2012</li> <li>Windows Vista SP2</li> </ul>	Allow unencrypted traffic	Not configured	Disabled	Disabled	Important	Computer Configuration\Administrative Templates\Window	Contraction of the second seco	
<ul> <li>Windows Vista SP2</li> <li>Windows XP SP3</li> </ul>	Set client connection encryption level	Not configured	Enabled	Enabled	Critical	Computer Configuration\Administrative Templates\Window	Setting Group	
4 Other Baselines	Allow unencrypted traffic	Not configured	Disabled	Disabled	Important	Computer Configuration\Administrative Templates\Window	(^) Help	
<ul> <li>Windows 8</li> <li>Windows 7 SP1</li> </ul>	Domain member: Digitally encrypt or sign secure cha	Enabled	Enabled	Enabled	Critical	Computer Configuration\Windows Settings\Security Setting	About	
	Network security: Minimum session security for NTL	Require 128-bit e	Require NTLMv2	Require NTLMv2	Critical	Computer Configuration\Windows Settings\Security Setting	Help Topics	
	Microsoft network server: Digitally sign communicati	Disabled	Enabled	Enabled	Critical	Computer Configuration\Windows Settings\Security Setting	Release Notes	
	Domain member: Digitally encrypt secure channel da	Enabled	Enabled	Enabled	Critical	Computer Configuration\Windows Settings\Security Setting	Send Feedback	
	Event Logging 58 Setting(s)						Privacy Statement	
	Audit: Force audit policy subcategory settings (Wind	Not defined	Enabled	Enabled	Critical	Computer Configuration\Windows Settings\Security Setting		
	Audit Policy: Privilege Use: Sensitive Privilege Use	No auditing	Success and Failur	Success and Failur	Critical	Computer Configuration\Windows Settings\Security Setting		
	Audit Policy: Account Management: Other Account M	No auditing	Success and Failur	Success and Failu	Critical	Computer Configuration\Windows Settings\Security Setting		
	Audit Policy: Logon-Logoff: IPsec Quick Mode	No auditing	No Auditing	No Auditing	Critical	Computer Configuration\Windows Settings\Security Setting		
	Audit: Audit the use of Backup and Restore privilege	Disabled	Not Defined	Not Defined	Critical	Computer Configuration\Windows Settings\Security Setting		
	Audit Policy: Detailed Tracking: RPC Events	No auditing	No Auditing	No Auditing	Critical	Computer Configuration\Windows Settings\Security Setting		
	Audit Policy: DS Access: Directory Service Access	No auditing	No Auditing	No Auditing	Critical	Computer Configuration\Windows Settings\Security Setting		
	Audit Policy: Policy Change: MPSSVC Rule-Level Policy	No auditing	No Auditing	No Auditing	Critical	Computer Configuration\Windows Settings\Security Setting		
	Audit Policy: Account Management: Distribution Gro	No auditing	No Auditing	No Auditing	Critical	Computer Configuration\Windows Settings\Security Setting +		
	· · · ·	-		-				

#### Abbildung 4: Aufbau des SCM

Auf der linken Seite erfolgt die Auswahl des abzusichernden Produkts. Nachdem ein entsprechendes Produkt ausgewählt worden ist (hier Windows 8), 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<sup>2</sup> verwiesen)
- Schwachstelle
- Auswirkungen
- Gegenmaßnahmen

<sup>&</sup>lt;sup>2</sup> Common Configuration Enumeration, siehe <u>http://cce.mitre.org/</u>.





aselines		210						treast
ows 8 tachments \ Guides py of Win8 Computer Security Compliance 1	Advanced View	310 unique	setting(s)					GPO Backup SCM (.cab)
Baselines nge Server 2007 SP3	Name	Default	Microsoft	Customized	Severity	Path		A Export
nge Server 2010 SP2 et Explorer 10 et Explorer 8	Accounts: Administrator account status Interactive logon: Machine account lockout threshold	Disabled Not defined	Disabled 10 invalid logon a	Disabled 10 invalid logon a	Critical Critical	Computer Configuration\Windows Settings\Security Setting Computer Configuration\Windows Settings\Security Setting	*	Excel (.xlsm) GPO Backup
et Explorer 9	Allow the use of biometrics	Not configured	Not Configured	Not Configured	Important	Computer Configuration\Administrative Templates\Window		SCAP v1.0 (.
oft Office 2007 SP2 oft Office 2010 SP1 wws 7 SP1	Collapse Not Configured  Enabled Disabled Option	n Help Text	Severity: Imp	oortant 🔻				SCCM DCM SCM (.cab)
ns o chments \ Guides			Comments:					A Baseline
8 BitLocker Security 1.0								Compare /
8 Computer Security Compliance 1.0	<ul> <li>Setting Details</li> </ul>							Delete
8 Domain Security Compliance 1.0 8 Extended DCM Charles 1.0	UI Path:							Duplicate
8 User Security Compliance 1.0	Computer Configuration\Administrative Templates\Windows Component\Biometrics							Lock
vs Server 2003 SP2	Description:		Vulnerability:					Properties
vs Server 2008 R2 SP1 vs Server 2008 SP2 vs Vista SP2 vs Vista SP2 vs XP SP3 lines	If you enable (or do not configure) this policy setting Biometric Service will be available, and users will be applications that use biometrics on Windows. If you the ability to log on with biometrics, you must also o "Allow users to no on uring biometrics" policy cetter	g, the Windows able to run want to enable configure the	Biometric authen however if low qu be less secure the Potential Impact	tication is often mo vality biometric tecl an password auther t:	ore robust the hnology is us ntication.	an passwords, ed it may actually		Setting     Add     Delete     Move
	If you disable this policy setting, the Windows Biome not be available, and users will be unable to use any features in Windows. Note: Users who log on using biometrics should cre-	etric Service will biometric ate a password-	If you mable (or do not configure) this policy setting, the Windows Biometric Service will be available and users will be able to run applications that use biometrics on Windows If you want to enable the ability to log on with biometrics, you must also configure the "Allow users to log on using biometrics" policy setting.				Setting Gro     Add     Delete     Properties	
	recovery disk; this will prevent data loss in the event forgets their logon credentials.	that someone	If you disable this not be available, features in Windo	s policy setting, the and users will be un ows.	Windows Bio nable to use a	ometric Service will any biometric		About
	Additional Details:		Countermeasure					Help Topics
	Allow the use of biometrics CCE-22729-8		Enable or disable your organization	this policy setting uses biometrics.	depending o	n whether or not		Release Not Send Feedb Privacy Stat

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 Aufbau der HiSolutions Baselines für Windows 8

Die HiSolutions Grundschutz-Templates für Windows 8 sind zurzeit aufgeteilt in fünf .cab-Dateien.

Eine grundlegende Unterteilung ist diejenige in Computereinstellungen vs. Benutzereinstellungen. Dies hat sich als Basis bewährt, um die Komplexität ein Stück weit zu reduzieren. In der Praxis wird in der Regel eine wesentlich feingliedrigere Einteilung nach Gebieten und Rollen erfolgen, um die Richtlinien auch über längere Zeit wartbar zu halten.

Darüber hinaus erfolgte eine weitere Trennung jedoch außerdem aus technischen Gründen: Notwendig war eine Aufteilung in Settings für Windows 8 und solche für Windows 8.1, wobei letztere .cab-Dateien nur die Delta-Settings zu Windows 8 enthalten. Dies war unumgänglich, da aufgrund eines Bugs im aktuellen SCM keine Windows 8.1-spezifischen Einstellungen zu einer Windows 8-GPO hinzugefügt werden können. Zudem hat dies den Vorteil, das Nutzer von Windows 8 die schlankeren Richtlinien ohne Fehlermeldungen nutzen können.<sup>3</sup>

Eine fünfte .cab-Datei enthält unsere Empfehlungen bezüglich Client-Chiffren. Diese konnte aufgrund von softwaretechnischen Beschränkungen des Tools nicht im SCM gesetzt werden und sollte in jedem Fall auf Kompatibilität mit allen Client-Anwendungen inkl. Browser und Plugins getestet werden.

## 6.4 Importieren der HiSolutions Baselines für Windows 8

Nach der Installation des SCM müssen die von HiSolutions in Form von CAB-Dateien bereitgestellten Baselines für Windows 8 in den SCM importiert werden. Die Grafiken in Tabelle 3 veranschaulichen die Vorgehensweise.

<sup>&</sup>lt;sup>3</sup> Dabei ist jedoch zu beachten, dass der Support für Windows 8 bereits im Oktober 2015 auslaufen wird.





#### Tabelle 3: Vorgehensweise zum Import einer Baseline

Zum Importieren der Baseline im Import- Bereich auf SCM (cab) klicken. Der Import Baselines Wizard öffnet sich.	Import <u>GPO Backup (folder)</u> <u>SCM (.cab)</u>
Auf "Add" klicken und die gewünschten zu	Select package files
importierenden	This wizard helps you import baselines into the Microsoft Security Compliance Manager tool.
Baselines auswahlen.	Select package files     Package       Baseline details     Add       Results     Remove
	Package Version: Package Description:
	Back Next Cancel
Weiter mit <i>"Next"</i>	Compared Baselines Wizard      Select package files     Baseline details     Results      Results      Compared Results      Co
	Package Version: 1.0 Package Description:
	Back Next Cancel







Es folgt eine	🖙 Import Baselines Wizard		X						
Zusammenfassung der Baseline-Details.	Baseline details This wizard helps you import baselines into the Microsoft Security Compliance Manager tool.								
Die Option "Create modifiable copies of each baseline to be imported" auswählen.	Select package files Baseline details Results	Sicherheitsvorlage IT-Grundschutz Windows 8 Benutzer.cab     Sicherheitsvorlage IT-Grundschutz Windows 8 Benutzereinstellunge     Sicherheitsvorlage IT-Grundschutz Windows 8 Computer.cab     Sicherheitsvorlage IT-Grundschutz Windows 8 Computereinstellunge							
Diese Einstellung erlaubt es, die importierten Baselines gemäß den									
Sicherheitsanforderunge		Description: The User baseline includes settings such as screen saver polic	v settings.						
n des Unternehmens anzupassen, da		······································	,g.						
Standard-Baselines		Publisher: Custom							
schreibgeschutzt sind		Name	Description						
bleiben. Die editierbaren		Administrative Templates\System for user setting	The system for user setting policy CI cont						
Baselines erscheinen		Windows Components\Windows Media Player\Playback     III							
dann unter der Rubrik " <i>Custom Baselines</i> ".		Create modifiable copies of each baseline to be imported.							
Abschließend die			Back Import Cancel						
Baselines mittels des									
<i>"Import"</i> Befehls importieren.									
Gof, muss eine Abfrage.									
ob die Baselines									
importiert werden sollen,									
nicht auf dem System									
vorhanden sind, mit "OK"									
bestätigt werden.									







## 6.5 Anpassen einer Baseline

Nachdem die im vorherigen Abschnitt beschriebenen Schritte zum Importieren der Baselines 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 in den Templates 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 verwendeten 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

Microsoft



- ÖFFENTLICH -



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	<custom> - <delta_sicherheitsvorlage_it-grundschutz_window< th=""><th>s-8.1_Computer</th><th>&gt; 1.0 110 un</th><th>ique setting(s)</th><th></th></delta_sicherheitsvorlage_it-grundschutz_window<></custom>	s-8.1_Computer	> 1.0 110 un	ique setting(s)	
besteht darin, dass die	Advanced View				
Einstellungen der	Name	Default	Microsoft	Customized	Severity Path
Diabtlinia an dia	EMET "Überprüfung erforderlich" 5 Setting(s)				
Richulmie an die	Default Action and Mitigation Settings			Not Configured	Importar Computer Configuration\Administrat
Bedürfnisse der	Application Configuration			Not Configured	Importar Computer Configuration\Administrat
Organisation	Default Protections for Internet Explorer			Enabled	Critical Computer Configuration\Administrat
Organisation	Default Protections for Popular Software			Enabled	Critical Computer Configuration\Administrat
angepasst werden.	Default Protections for Recommended Software			Enabled	Critical Computer Configuration\Administrat
	Malware - Analyse "Überprüfung erforderlich" 93 Setting(s)				
	Allow antimalware service to remain running always			Not Configured	Importar Computer Configuration\Administrat
	Allow antimalware service to startup with normal priority			Not Configured	Importar Computer Configuration\Administrat
	Allow definition updates from Microsoft Update			Not Configured	Importar Computer Configuration\Administrat
	Allow definition updates when running on battery power			Not Configured	Importar Computer Configuration\Administrat
	Allow notifications to disable definitions based reports to Microsoft	M		Not Configured	Importar Computer Configuration\Administrat
	Allow real-time definition updates based on reports to Microsoft M	ЧÞ		Not Configured	Importa: Computer Configuration\Administrat
	Allow users to pause scan			Disabled	Importar Computer Configuration\Administrat
	Always automatically restart at the scheduled time			Not Configured	Importar Computer Configuration\Administrat
	Check for the latest virus and spyware definitions before running a	ch		Enabled	Importal Computer Configuration\Administrat
	Check for the latest virus and spyware definitions on startup			Enabled	Importar Computer Configuration\Administrat
	Configure local setting override for maximum percentage of CPU ut	iliz		Not Configured	Importar Computer Configuration\Administrat
	Configure local setting override for monitoring file and program act	ivi		Not Configured	Importal Computer Configuration\Administrat
	Configure local setting override for monitoring for incoming and ou	tg		Not Configured	Importal Computer Configuration\Administrat
	Configure local setting override for reporting to Microsoft MAPS			Not Configured	Importal Computer Configuration\Administrat
	Configure local setting override for scanning all downloaded files an	d		Not Configured	Importal Computer Configuration\Administrat
	Configure local setting override for schedule scan day			Not Configured	Importal Computer Configuration\Administrat
	Configure local setting override for scheduled quick scan time			Not Configured	Importal Computer Configuration\Administrat
	Configure local setting override for scheduled scan time			Not Configured	Importar Computer Configuration\Administrat
	Configure local setting override for the removal of items from Quar	an		Not Configured	Importal Computer Configuration\Administrat
	Configure local setting override for the scan type to use for a sched	ule		Not Configured	Importar Computer Configuration\Administrat
	Configure local setting override for the time of day to run a schedul	ed		Not Configured	Importa: Computer Configuration\Administrat
	Configure local setting override for turn on behavior monitoring			Not Configured	Importal Computer Configuration\Administrat
	Configure local setting override to turn off Intrusion Prevention Syst	er		Not Configured	Importal Computer Configuration\Administrat
	Configure local setting override to turn on real-time protection			Not Configured	Importal Computer Configuration\Administrat

Nachdem alle Einstellungen überprüft und angepasst worden sind, kann die Baseline nun entweder auf mehreren Clients in einer Domäne verteilt (siehe Abschnitt 6.8) oder auf ein Stand-Alone-System (siehe Abschnitt 6.9) angewandt werden.

Zunächst muss allerdings ein Export der Baseline in ein dafür benötigtes Format erfolgen. Abschnitt 6.6 beschreibt den Export einer angepassten Baseline, Abschnitt 6.7 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.





### 6.6 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.

## 6.7 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.

▲ Baseline	Microsoft Security Compliance Manager 83	
<u>Compare / Merge</u> <u>Delete</u> <u>Duplicate</u>	You are about to lock the baseline. After locking the baseline, you cannot modify it. Do you want to continue?	
Lock Properties	JaNein	1

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: Bearbeiten einer Kopie). Diese Baseline kann nun als Basis weiterer Konfigurationen verwendet werden.

Sicherheitsvorlag	ge IT-Grundschu	utz Windows 8 Co	omputer		
Version major:	1	<ul> <li>Image: A state</li> <li>Image: A state<th>Version minor:</th><th>1</th><th></th></li></ul>	Version minor:	1	
The Computer b	aseline includes	settings to confi	gure desktop and mobile	computers.	
The Computer b	aseline includes	settings to confi	gure desktop and mobile	computers.	
The Computer b	aseline includes	settings to confi	gure desktop and mobile	computers.	

Abbildung 8: Bearbeiten einer Kopie

### 6.8 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.



- ÖFFENTLICH -



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.

#### 6.9 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*<sup>4</sup> zur Verfügung. Hiermit kann man die lokalen Richtlinien eines PCs in ein GPO-Backup exportieren und

<sup>&</sup>lt;sup>4</sup> Das mit dem SCM aktuell (Stand September 2014) mitgelieferte Tool LocalGPO läuft nicht auf Windows 8.1. Für dieses System sind die entsprechenden Tools aus dem folgenden von Microsoft





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.	Microsoft Solution Accelerators	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	

bereitgestellten Download zu verwenden, bis eine aktualisierte Version des SCM zur Verfügung steht: <u>http://blogs.technet.com/b/secguide/archive/2014/08/13/security-baselines-for-windows-8-1-windows-server-2012-r2-and-internet-explorer-11-final.aspx</u>.





	tel LocalGDO Setup	X
	LocalGPO Setup  Completing the Setup Wizard  Click the Finish button to exit  Microsoft Solution	e LocalGPO : the Setup Wizard.
	< Back En	ish 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.	<ul> <li>Internet Explorer (64 Bit)</li> <li>Internet Explorer</li> <li>Security Compliance Manager</li> <li>Windows Update</li> <li>Autostart</li> <li>LocalGPO</li> <li>LocalGPO Command-line</li> <li>LocalGPO</li> <li>Microsoft Security Compliance Manager</li> <li>Microsoft SQL Server 2005</li> <li>Microsoft System Center</li> </ul>	Administrator Dokumente Computer Netzwerk
Zum Applizieren der in Abschnitt 6.5 überprüften Baseline ist folgende Kommandozeile auszuführen:	Administrator: LocalGPO Command-line C:\Program Files (x86>\LocalGPO>LocalGPO.wsf / p\{ca84c8d6-d86f-4893-807f-9923008cf1f9> Microsoft (R) Windows Script Host, Version 5.8 Copyright (C) Microsoft Corporation 1996-2001. Modifying Local Policy this process can tak Applied valid INF from c:\Users\Administrator\ 923008cf1f9> Applied valid Machine POL from c:\Users\Administrator\ 97f-9923008cf1f9> Applied valid User POL from c:\Users\Administr 97f-9923008cf1f9> Applied valid Audit Policy CSU from c:\Users\A f-4893-807f-9923008cf1f9> Local Policy Modified! Please restart the computer to refresh the Loc C:\Program Files (x86>\LocalGPO>_	■         Path:c:\Users\Administrator\Deskto         Alle Rechte vorbehalten.         e a few moments.         Desktop\(ca84c8d6-d86f-4893-807f-9         strator\Desktop\(ca84c8d6-d86f-4893-8         ator\Desktop\(ca84c8d6-d86f-4893-8         dministrator\Desktop\(ca84c8d6-d86f-d866         all Policy
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 Baustein B 3.212 Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kataloge/Inhalt/\_content/baust/b03/b03201.html https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz Kataloge/Inhalt/\_content/baust/b03/b03212.html

## 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: Überprüfung der Werte notwendig (Fall 1; Beispiel)	4
Abbildung 2: Zuweisung der Werte notwendig (Fall 2; Beispiel)	4
Abbildung 3: Beschreibung innerhalb der "Setting Group Properties" (Beispiel)	5
Abbildung 4: Aufbau des SCM	9
Abbildung 5: Detaillierte Konfigurationseinstellungen	10
Abbildung 6: Lock-Funktion einer Baseline	15
Abbildung 7: Erstellung einer Kopie	15
Abbildung 8: Bearbeiten einer Kopie	16

## 7.4 Tabellenverzeichnis

Tabelle 1: SCM Severity-Level	7
Tabelle 2: Voraussetzungen zur Installation des SCM	8
Tabelle 3: Vorgehensweise zum Import einer Baseline	11
Tabelle 4: Anpassen einer Baseline	14
Tabelle 5: Importieren von Einstellungen auf einem Domänencontroller	17
Tabelle 6: Absicherung von Stand-Alone-Systemen	18



- ÖFFENTLICH -



# 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