Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Anleitung zur Verwendung der Gruppenrichtlinienobjekte für die Härtungs- und Protokollierungs-konfiguration von Windows 10

Version: 1.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Telefon: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Dieses Dokument stellt das Ergebnis von Arbeitspaket 12 des Projekts „SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10“ dar. Das Projekt wird durch die Firma ERNW Enno Rey Netzwerke GmbH im Auftrag des BSI durchgeführt.

Ziel dieses Dokuments ist die Erläuterung der bereitgestellten Gruppenrichtlinienobjekte, welche basierend auf dem Härtungs- und Protokollierungskonzept für die Konfiguration von Komponenten von Windows 10 erstellt wurden. Die Beschreibung und Erläuterung der gesetzten Konfigurationen sind in den zugehörigen Ergebnisdokumenten von Arbeitspaketen 10 (Protokollierungsempfehlungen) und 11 (Härtungsempfehlungen) beschrieben.

2 Allgemeines

Die bereitgestellten Gruppenrichtlinienobjekte sind separiert nach den Härtungsempfehlungen aus Arbeitspaket 11 (siehe (ERNW_WP11)) und den Protokollierungsempfehlungen aus Arbeitspaket 10 (siehe (ERNW_WP10)). Zusätzlich wurden bei den Härtungsempfehlungen drei unterschiedliche Nutzungsszenarien für Windows 10 definiert:

- Normaler Schutzbedarf Einzelrechner
- Normaler Schutzbedarf Domänenmitglied
- Hoher Schutzbedarf Domänenmitglied

Jede beschriebene Konfigurationsempfehlung wurde dabei mindestens einem Nutzungsszenario zugewiesen, mit Ausnahme der Protokollierungsempfehlungen aus Arbeitspaket 10, die für alle Szenarien gelten. Basierend auf der Zuordnung der Empfehlung zu den Nutzungsszenarien wurden dedizierte Gruppenrichtlinienobjekte erstellt. Dies ermöglicht eine feingranulare Implementierung der Härtungsempfehlung.

Nicht alle Einstellungen, welche in den Härtungs- und Protokollierungsempfehlungen sind, sind auch in den bereitgestellten Gruppenrichtlinienobjekten konfiguriert. Manche Einstellungen erfordern eine individuelle Betrachtung, beziehungsweise Konfiguration, und können nicht allgemeingültig vorkonfiguriert werden. Die folgende Tabelle enthält eine Auflistung der Einstellungen, welche nicht in den Gruppenrichtlinienobjekten konfiguriert sind:

Lfd. Nr. Härtungs-empfehlungen	Richtlinienname	Begründung
209	Interaktive Anmeldung: Nachrichtentitel für Benutzer, die sich anmelden wollen	Einstellung ist unternehmens- und sprachspezifisch.
231	Interaktive Anmeldung: Nachricht für Benutzer, die sich anmelden wollen	Einstellung ist unternehmens- und sprachspezifisch.
235	Konten: Administrator umbenennen	Individuelle Namensgebung erforderlich.
238	Konten: Gastkonto umbenennen	Individuelle Namensgebung erforderlich.
277-315	Zuweisen von Benutzerrechten	Individuelles Rollenkonzept erforderlich.
323, 326, 328, 331, 341, 342, 348, 356	Deaktivieren von Systemdiensten	Abhängig von installierten Rollen.

Tabelle 1 In Gruppenrichtlinienobjekten nicht enthaltene Härtungsempfehlungen

Zusätzlich ist ein größerer Teil der Empfehlungen aus Kapitel 5 der Härtungsempfehlungen und Kapitel 5.6.1.2 der Protokollierungsempfehlungen nicht enthalten, da hier ebenfalls Anpassungen an das konkrete Nutzungsszenario notwendig sind und die Einstellungen (auch aufgrund von Hardwareabhängigkeiten wie z. B. bei der „Virtualisierungsbasierten Sicherheit“) vorab ausführlich getestet werden müssen oder sich die konkreten Konfigurationen nicht über Gruppenrichtlinien (wie z. B. die Firmwarekonfiguration) abbilden lassen. Konkret bedeutet dies, dass die Empfehlungen der folgenden Einstellungskapitel manuell bzw. erst nach einer Evaluierung umgesetzt werden sollten (H – Härtungsempfehlung, P – Protokollierungsempfehlung):

Dokument	Kapitelnummer	Kapitelüberschrift
H	5.1	Windows Defender-Anwendungssteuerung
H	5.2	Virtualisierungsbasierte Sicherheit
H	5.3.3	Anforderungen für den sicheren Einsatz des TPM
H	5.4.1.2	Deaktivierung Autologger-Diagtrack-Listener
H	5.5.1.1	Deaktivierung von PowerShell Version 2.0
H	5.5.1.3	Einschränkung der PowerShell-Skriptsprache (lokaler Computer)
H	5.5.1.4	Sichere Verwendung von PowerShell-Remoting
H	5.5.2	Windows Script Host
H	5.6	Firmware
P	5.6.1.2	Stellen Sie sicher, dass für sicherheitsrelevante Registrierungsobjekte eine SACL konfiguriert ist. *Hinweis: Betrifft nur Benutzerspezifische Registrierungsschlüssel.*

Tabelle 2 Zusätzlich zu konfigurierende Einstellungsempfehlungen

2.1 Gruppenrichtlinienobjekte

Die Konfigurationsempfehlungen wurden einerseits nach dem jeweiligen Nutzungsszenario und andererseits nach der jeweiligen Einstellungskategorie (Einstellungen für Computer oder Benutzer), aufgeteilt. Daraus resultieren für die Härtungsempfehlungen insgesamt 5 verschiedene Gruppenrichtlinienobjekte, die eingesetzt werden können. Die folgenden Tabellen stellen eine Zuordnung der Gruppenrichtlinienobjekte zum jeweiligen Nutzungsszenario dar.

Die folgende Tabelle listet die bereitgestellten Gruppenrichtlinienobjekte für die Computerkonfiguration auf:

Nr.	Name
1	Normaler Schutzbedarf Einzelrechner (NE) - Computer
2	Normaler Schutzbedarf Domänenmitglied (ND) - Computer
3	Hoher Schutzbedarf Domänenmitglied (HD) - Computer

Tabelle 3 Gruppenrichtlinienobjekte für Computerkonfiguration

Die folgende Tabelle listet die bereitgestellten Gruppenrichtlinienobjekte für die Benutzerkonfiguration auf:

Nr.	Name
4	Normaler Schutzbedarf (ND, NE) - Benutzer

5	Hoher Schutzbedarf (HD) - Benutzer

Tabelle 4 Gruppenrichtlinienobjekte für Benutzerkonfiguration

Für die Protokollierungsempfehlungen aus Arbeitspaket 10 existiert nur 1 Gruppenrichtlinienobjekt, da keine Unterscheidung zwischen unterschiedlichen Nutzungsszenarien und Einstellungskategorien getroffen werden muss:

Nr.	**Name**
6	Protokollierung (ND, NE, HD) - Computer

3 Importieren der Gruppenrichtlinienobjekte

Die folgenden Abschnitte beschreiben beispielhaft das Vorgehen, um die bereitgestellten Gruppenrichtlinienobjekte auf Einzelrechnern oder im Active Directory anzuwenden.

3.1 Einzelrechner

Gruppenrichtlinienobjekte können über das Tool *Local Group Policy Object Utility* (LGPO) (siehe (ms_lgpo, 2020)) lokal exportiert und importiert werden. Für dieses Szenario sind die Gruppenrichtlinienobjekte *Normaler Schutzbedarf Einzelrechner (NE)* (Gruppenrichtlinienobjekt Nr. 1), *Normaler Schutzbedarf (NE, ND)* (Gruppenrichtlinienobjekt Nr. 4) und *Protokollierung (NE, ND, HD)* (Gruppenrichtlinienobjekt Nr. 6) relevant. Im Folgenden werden die einzelnen Schritte beschrieben, um die bereitgestellten Gruppenrichtlinienobjekte lokal zu importieren:

1. Laden Sie das Tool *LGPO.exe* bei Microsoft herunter.
2. Entpacken Sie den Ordner, der die Datei *LGPO.exe* enthält, aus dem heruntergeladenen Archiv.
3. Starten Sie eine administrative Kommandozeile:
    a. Starten Sie das Programm *Eingabeaufforderung* (cmd.exe) oder *PowerShell* (powershell.exe).
4. Führen Sie das Programm *LGPO.exe* mit dem Parameter */g* und dem Pfad zum jeweiligen Gruppenrichtlinienobjekt aus:
    a. `C:\>LGPO.exe /g „C:\<Pfad>\Normaler Schutzbedarf Einzelrechner (NE) – Computer“`
    b. `C:\>LGPO.exe /g „C:\<Pfad>\Normaler Schutzbedarf (NE, ND) – Computer“`
    c. `C:\>LGPO.exe /g „C:\<Pfad>\Protokollierung (NE, ND, HD) – Computer“`
5. Führen Sie einen Neustart durch, um die Konfigurationen anzuwenden:
    a. `C:\>shutdown.exe /r /t 0`

3.2 Active Directory

Gruppenrichtlinienobjekte werden in Active Directory-Umgebungen über die *Gruppenrichtlinienverwaltung* (gpmc.msc) konfiguriert, verwaltet und entsprechenden Organisationseinheiten zugewiesen. Im Folgenden werden die einzelnen Schritte beschrieben, um die bereitgestellten Gruppenrichtlinienobjekte in die Gruppenrichtlinienverwaltung zu importieren:

1. Öffnen Sie die *Gruppenrichtlinienverwaltung* der entsprechenden Active Directory-Domäne:
    a. Starten Sie dazu das Programm *Gruppenrichtlinienverwaltung* (gpmc.msc) auf einem Domänencontroller oder Mitgliedssystem.
2. Erstellen Sie ein neues Gruppenrichtlinienobjekt und benennen Sie es entsprechend:

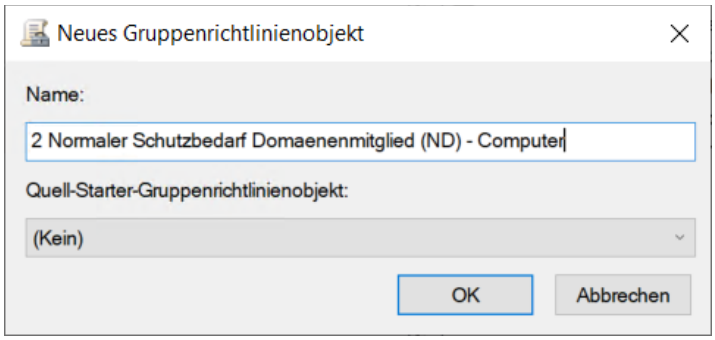

Abbildung 1 Erstellung eines neuen Gruppenrichtlinienobjekts

3. Klicken Sie mit der rechten Maustaste auf das neu erstellte Gruppenrichtlinienobjekt und wählen Sie die Option *Einstellungen importieren...* aus:

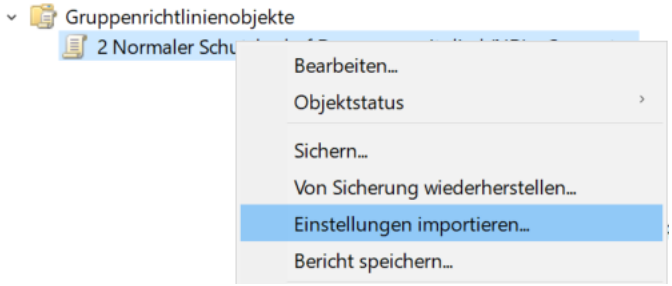

Abbildung 2 Importieren der Einstellungen

4. Klicken Sie weiter, bis zur Auswahl des Sicherungsordners (der Ordner, der das bereitgestellte Gruppenrichtlinienobjekt enthält):

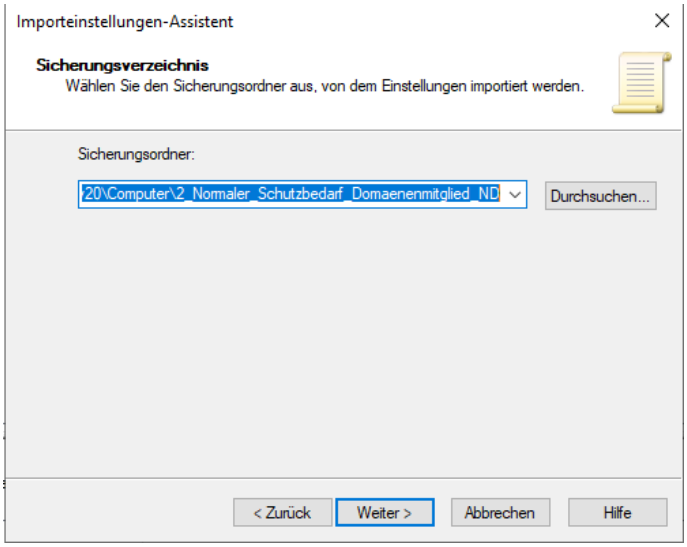

Abbildung 3 Auswahl des Sicherungsverzeichnisses

5. Anschließend wählen Sie das gewünschte Gruppenrichtlinienobjekt aus:

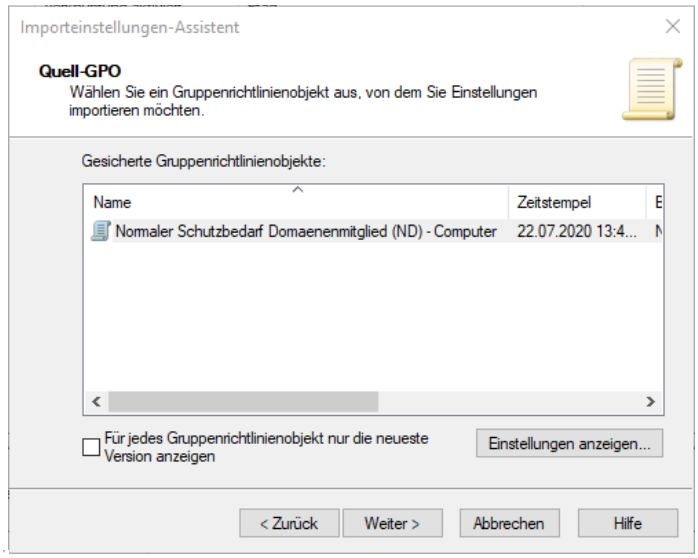

Abbildung 4 Auswahl des zu importierenden Gruppenrichtlinienobjekts

6. Anschließend muss das Gruppenrichtlinienobjekt noch mit der gewünschten Organisationseinheit verknüpft werden.

3.2.1 Verknüpfung von Gruppenrichtlinienobjekten

Um die Gruppenrichtlinienobjekte effektiv anzuwenden, müssen diese noch mit den entsprechenden Objekten im Active Directory verknüpft werden. Dazu werden typischerweise individuelle Organisationseinheiten angelegt (eine Verknüpfung mit dem Domänen-Objekt oder sog. *Sites* ist jedoch auch möglich). Diese enthalten idealerweise entweder nur Benutzer- oder Computer-Objekte. Daraus resultieren aus dem Einsatzszenario *Normaler Schutzbedarf Domänenmitglied* mindestens zwei Organisationseinheiten (die jeweils Benutzer und Computer enthalten) mit einer Verknüpfung zu dem entsprechenden Gruppenrichtlinienobjekt.

Die Gruppenrichtlinienobjekte des hohen Schutzbedarfs enthalten dediziert nur die Einstellungen für den hohen Schutzbedarf. Das bedeutet, dass auf den Organisationseinheiten des hohen Schutzbedarfs auch die Gruppenrichtlinienobjekte des normalen Schutzbedarf angewendet werden müssen. Computer- und Benutzer-Objekte mit hohen Schutzbedarf müssen dabei jeweils in einer eigenen Organisationseinheit sortiert werden. Der folgende Screenshot stellt exemplarisch die Verknüpfung der Gruppenrichtlinienobjekte zu den beiden Nutzungsszenarien in Active Directory-Umgebungen dar:

Abbildung 5 Verknüpfung der Gruppenrichtlinienobjekte

Das Gruppenrichtlinienobjekt für die Protokollierung betrifft nur die Computerkonfiguration. Da keine Unterscheidung hinsichtlich des Schutzbedarfs getroffen wird, kann das importierte Objekt mit der Computer-Organisationseinheit für den normalen und den hohen Schutzbedarf verknüpft werden.

Appendix

Werkzeuge

Werkzeug	Verfügbarkeit und Beschreibung
`Local Group Policy Object Utility`	*Verfügbarkeit:* Download unter https://www.microsoft.com/en-us/download/details.aspx?id=55319 *Beschreibung:* Lokale Verwaltung von Gruppenrichtlinienobjekten
`Gruppenrichtlinienverwaltung`	*Verfügbarkeit:* Aktivierbares Windows Feature *Beschreibung:* Verwaltung von Gruppenrichtlinienobjekte in Active Directory-Umgebungen

Referenzen

ERNW_WP10. (kein Datum). SiSyPHuS Win10 (Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10): Work Package 10.

ERNW_WP11. (kein Datum). SiSyPHuS Win10 (Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10): Work Package 11.

ms_lgpo. (7. Oktober 2020). Von https://www.microsoft.com/en-us/download/confirmation.aspx?id=55319 abgerufen

Abkürzungen

BSI: Bundesamt für Sicherheit in der Informationstechnik 5
TPM: Trusted Platform Module 7