



Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
**Digital•Sicher•BSI•**

# Hilfsmittel zur Umsetzung von Anforderungen des IT- Grundschutzes für Windows 10

Windows 10 20H2



# Änderungshistorie

<i>Version</i>	<i>Datum</i>	<i>Name</i>	<i>Beschreibung</i>
V 1.0		BSI	Initiale Version

*Tabelle 1: Änderungshistorie*

# Inhalt

1	Einleitung .....	6
2	Abgrenzung .....	8
3	Vorgehensweise („Best Practice“-Empfehlung).....	9
3.1	Vorbereitungen.....	9
3.1.1	Administrative Vorlagen (ADMX).....	9
3.1.1.1	Windows 10 20H2 .....	9
3.1.1.2	Microsoft Security Baselines.....	9
3.1.1.3	Microsoft Security Compliance Toolkit (SCT).....	10
3.2	Domänenverwalteter Client (Domain-joined Client).....	10
3.2.1	Zentraler Speicher für Gruppenrichtlinien .....	10
3.2.2	Zentrale Gruppenrichtlinienverwaltung.....	11
3.2.2.1	Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console).....	11
3.2.2.2	Gruppenrichtlinien-Objekteditor (Group Policy Object Editor) .....	11
3.2.3	Gruppenrichtlinieneinstellungen und Gruppenrichtlinienvoreinstellungen (Group Policy Preferences) .....	12
3.3	Nicht-Domänenverwalteter Client (Local Windows-based Client).....	12
3.3.1	Lokaler Speicher für Gruppenrichtlinien.....	12
3.3.2	Lokaler Gruppenrichtlinieneditor („gpedit“).....	13
3.3.3	Lokale Sicherheitsrichtlinie („secpol“).....	13
3.3.4	Microsoft Security Compliance Manager 3.0 .....	13
3.3.4.1	LocalGPO („LGPO.exe“).....	13
4	Konfiguration: SYS.2.1. Allgemeiner Client.....	15
4.1	Basis-Anforderungen.....	15
	SYS.2.1.A1 Sichere Benutzerauthentisierung (B).....	15
	SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen (B).....	28
	SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware (B).....	32
	SYS.2.1.A8 Absicherung des Bootvorgangs (B) .....	42
	SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen [Benutzer] (B).....	43
4.2	Standard-Anforderungen .....	49
	SYS.2.1.A10 Planung des Einsatzes von Clients (S) .....	49
	SYS.2.1.A11 Beschaffung von Clients (S) .....	50
	SYS.2.1.A13 Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (S) .....	50
	SYS.2.1.A14 Updates und Patches für Firmware, Betriebssystem und Anwendungen (S).....	50
	SYS.2.1.A15 Sichere Installation und Konfiguration von Clients (S).....	51
	SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen (S) ..	54
	SYS.2.1.A18 Nutzung von verschlüsselten Kommunikationsverbindungen (S) .....	81

SYS.2.1.A20	Schutz der Administrationsverfahren bei Clients (S) .....	86
SYS.2.1.A21	Verhinderung der unautorisierten Nutzung von Rechtermikrofonen und Kameras (S)..	93
SYS.2.1.A23	Bevorzugung von Client-Server-Diensten (S).....	94
SYS.2.1.A24	Umgang mit externen Medien und Wechseldatenträgern (S).....	98
SYS.2.1.A26	Schutz vor Ausnutzung von Schwachstellen in Anwendungen (S).....	104
SYS.2.1.A27	Geregelte Außerbetriebnahme eines Clients (S) .....	111
SYS.2.1.A34	Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten (S) .....	113
SYS.2.1.A43	Lokale Sicherheitsrichtlinien für Clients (S) .....	115
SYS.2.1.A44	Verwaltung der Sicherheitsrichtlinien von Clients (S).....	116
4.3	Anforderungen bei erhöhtem Schutzbedarf.....	116
SYS.2.1.A31	Einrichtung lokaler Paketfilter (H).....	116
SYS.2.1.A32	Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits (H).....	121
SYS.2.1.A33	Einsatz von Ausführungskontrolle (H).....	121
SYS.2.1.A35	Aktive Verwaltung der Wurzelzertifikate (H).....	125
SYS.2.1.A36	Selbstverwalteter Einsatz von SecureBoot und TPM (H).....	127
SYS.2.1.A37	Verwendung von Mehr-Faktor-Authentisierung (H) .....	133
SYS.2.1.A38	Einbindung in die Notfallplanung (H).....	134
SYS.2.1.A39	Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] (H).....	135
SYS.2.1.A41	Verwendung von Quotas für lokale Datenträger (H).....	135
SYS.2.1.A45	Erweiterte Protokollierung (H) .....	136
5	Konfiguration: SYS.2.2.3 Clients unter Windows 10 .....	138
5.1	Basis-Anforderungen.....	138
SYS.2.2.3.A1	Planung des Einsatzes von Cloud-Diensten unter Windows 10 (B) .....	138
SYS.2.2.3.A2	Auswahl und Beschaffung einer geeigneten Windows-10-Version (B).....	138
SYS.2.2.3.A4	Telemetrie und Datenschutzeinstellungen unter Windows 10 (B).....	138
SYS.2.2.3.A5	Schutz vor Schadsoftware unter Windows 10 (B) .....	140
SYS.2.2.3.A6	Integration von Online-Konten in das Betriebssystem [Benutzer] (B) .....	140
5.2	Standard-Anforderungen .....	141
SYS.2.2.3.A9	Sichere zentrale Authentisierung in Windows-Netzen (S).....	141
SYS.2.2.3.A12	Datei- und Freigabeberechtigungen unter Windows 10 (S).....	144
SYS.2.2.3.A13	Einsatz der SmartScreen-Funktion (S).....	147
SYS.2.2.3.A14	Einsatz des Sprachassistenten Cortana [Benutzer] (S).....	147
SYS.2.2.3.A15	Einsatz der Synchronisationsmechanismen unter Windows 10 (S) .....	148
SYS.2.2.3.A16	Anbindung von Windows 10 an den Microsoft-Store (S).....	150
SYS.2.2.3.A17	Keine Speicherung von Daten zur automatischen Anmeldung (S).....	151
SYS.2.2.3.A18	Einsatz der Windows-Remoteunterstützung (S).....	152
SYS.2.2.3.A19	Sicherheit beim Fernzugriff über RDP [Benutzer] (S) .....	153

---

SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten (S) .....	159
5.3 Anforderungen bei erhöhtem Schutzbedarf.....	162
SYS.2.2.3.A21 Einsatz des Encrypting File Systems (H).....	162
SYS.2.2.3.A22 Verwendung der Windows PowerShell (H).....	163
SYS.2.2.3.A23 Erweiterter Schutz der Anmeldeinformationen unter Windows 10 (H) .....	165
SYS.2.2.3.A24 Aktivierung des Last-Access-Zeitstempels (H).....	166
SYS.2.2.3.A25 Umgang mit Fernzugriffsfunktionen der „Connected User Experience and Telemetry“ (H).....	166
6 Konfigurationen zu weiteren Bausteinen .....	168
6.1 Basisanforderungen.....	168
6.1.1 SYS.3.1 Laptops .....	168
SYS.3.1.A3 Einsatz von Personal Firewalls (B).....	168
6.1.2 DER.1 Detektion von sicherheitsrelevanten Ereignissen .....	168
DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion [Fachverantwortliche] (B)...	168
6.1.3 OPS.1.1.4 Schutz vor Schadprogrammen .....	168
OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes (B).....	168
6.1.4 ORP.4 Identitäts- und Berechtigungsmanagement .....	171
ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen [IT-Betrieb] (B).....	171
6.1.5 CON.3 Datensicherungskonzept .....	179
CON.3.A5 Regelmäßige Datensicherung [IT-Betrieb] (B).....	179
6.2 Standardanforderungen .....	187
6.2.1 DER.1 Detektion von sicherheitsrelevanten Ereignissen .....	187
DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse [Fachverantwortliche] (S).....	187
6.2.2 OPS.1.1.4 Schutz vor Schadprogrammen .....	187
OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen [Benutzer] (S) .....	187
7 Überprüfung von angewendeten Gruppenrichtlinien .....	188
7.1 Resultant Set of Policy (RSoP).....	188
7.2 Berichtserstellung (GPResult) .....	188
8 Weiterführende Informationen und Hinweise .....	189
8.1 Problem- und Fehleranalyse .....	189
8.2 Unterstützung durch Microsoft.....	189
8.3 Vorschläge und Anregungen.....	189
9 Verzeichnisse und Anhänge.....	190
Literaturverzeichnis.....	191

# 1 Einleitung

Microsoft Windows 10 wird von Microsoft für Zielgruppen mit unterschiedlichen Einsatzzwecken und -szenarien als Standardsoftware bereitgestellt. Folglich ist Windows 10 auf ein breites Einsatzspektrum ausgerichtet und ist daher mit einem weitreichenden Funktionsumfang ausgestattet. Windows 10 enthält dabei nicht nur Betriebssystemfunktionalitäten, sondern in zunehmendem Maße auch weitere Softwarebestandteile auf Anwendungsebene. Hierzu zählen u. a. verschiedene Dienste, Treiber und Anwendungen. Windows 10 ist in diesem Sinne immer mehr als eine Distribution anzusehen, statt nur als ein Betriebssystem. Die unterschiedlichen Windows-Editionen (z. B. Home, Pro, Enterprise) unterscheiden sich vor allem in der Konfiguration<sup>1</sup> und der Verfügbarkeit von Softwarebestandteilen. Die voreingestellten Einstellungen („Standardkonfiguration“) der ausgelieferten Grundkonfiguration von Windows 10 haben das Ziel, möglichst breite Einsatzszenarien direkt zu unterstützen. Dies bedeutet, dass viele Softwarekomponenten bereits vorinstalliert und vorkonfiguriert sind. Da sowohl Windows 10 wie auch die Servervariante (Windows Server) die gleiche Softwarebasis haben, enthält der Client (Windows 10) denselben Kernel wie der Windows-Server sowie einige Serverdienste und Konfigurationen, wie beispielsweise DNS-Server, Fileserver, Druckserver, Mediaserver, RDP-Server, Zeitserver (NTP) und Routingdienste.

Entsprechend dem individuellen Bedarf sollten Anforderungen an das Betriebssystem formuliert werden, aus denen Anpassungen und Konfigurationen des Betriebssystems für das spezielle Einsatzszenario hervorgehen. Ziel sollte sein, möglichst nur solche Funktionalitäten des Betriebssystems zu aktivieren und zu konfigurieren, die für den tatsächlichen Einsatz erforderlich sind. Alle nicht benötigten Bestandteile und Komponenten sollten deaktiviert und nach Möglichkeit deinstalliert werden, wodurch die mögliche Angriffsfläche so gering wie möglich gehalten werden kann. Gleichzeitig muss stets die Bedienbarkeit des Betriebssystems berücksichtigt werden.

Diese grundsätzlichen Betrachtungen sollten zwar frühzeitig, aber nicht nur einmalig durchgeführt werden. Vielmehr sollte die Konfiguration in regelmäßigen Abständen (beispielsweise jährlich) hinsichtlich der Erfüllung aller Anforderungen überprüft werden.

Der IT-Grundschutz des BSI benennt mit den zugehörigen IT-Grundschutz-Bausteinen „Allgemeiner Client“ (SYS.2.1) und „Clients unter Windows 10“ (SYS.2.2.3) exemplarische Gefährdungen für einen Windows 10 Client und erläutert hiernach zugehörige Sicherheitsanforderungen, welche nach Basis-, Standard- sowie Anforderungen bei erhöhtem Schutzbedarf gegliedert sind. Über die bestehenden Umsetzungshinweise hinaus werden im Rahmen dieses Hilfsmittels Konfigurationsempfehlungen zu diesen Bausteinen sowie einigen wenigen Anforderungen von weiteren Bausteinen des IT-Grundschutzes (Edition 2022) bereitgestellt. Für die Basis- und Standard-Anforderungen werden konkrete Empfehlungen für die Konfiguration des normalen Schutzbedarfs angegeben. Zur Unterstützung der Risikoanalyse bei erhöhtem Schutzbedarf werden Hinweise zur Auswirkung von Konfigurationen beschrieben. Darüber hinaus werden für die im IT-Grundschutz-Baustein aufgeführten Anforderungen des erhöhten Schutzbedarfes Hinweise zur Umsetzung der Konfiguration gegeben.






Die Aussagen und Empfehlungen im Hilfsmittel wurden im Hinblick auf Windows 10 Version 20H2 in den Editionen Pro/Enterprise erarbeitet und sollen IT-Verantwortliche und Anwendende praxisnah bei der Umsetzung der Anforderungen aus dem IT-Grundschutz unterstützen. Grundsätzlich können die Empfehlungen aus dem Hilfsmittel auch für die derzeit aktuellen Versionen des Betriebssystems als Basis für die Absicherung herangezogen werden. Im Einzelfall können sich dabei das vordefinierte Verhalten sowie die Konfigurationspfade, -optionen und -möglichkeiten von den Ausführungen im Hilfsmittel geringfügig unterscheiden.

---

<sup>1</sup> Teilweise können Konfigurationsoptionen gewählt werden, die von der jeweiligen Komponente nicht übernommen werden.

Bei den hier dargestellten Konfigurationsempfehlungen werden sowohl ein Einsatz innerhalb einer Domäne als auch ein Stand-alone Betrieb von Windows 10 betrachtet. Dabei ergänzen diese Konfigurationsempfehlungen die veröffentlichten Umsetzungshinweise zu den entsprechenden Bausteinen. Sie erheben jedoch keinen Anspruch auf Vollständigkeit. Die Erstellung erfolgte auf Basis der Empfehlungen von Microsoft und anderer veröffentlichter Empfehlungen (CIS Benchmark<sup>2</sup>, SiSyPHuS Win 10<sup>3</sup> und der STIG Empfehlungen<sup>4</sup>). Zu verschiedenen Themengebieten wurden ergänzende Betrachtungen vorgenommen und Empfehlungen erarbeitet. Dabei wurde vorzugsweise auf eine Konfiguration über Gruppenrichtlinieneinstellungen hingearbeitet. Stehen keine Gruppenrichtlinieneinstellungen zur Verfügung, wird auf alternative Konfigurationswege, wie über die Windows Registry oder die Windows PowerShell verwiesen. Über die dargestellten Möglichkeiten hinaus kann es weitere und alternative Konfigurationswege geben, um die Anforderungen des IT-Grundschutzes zu erfüllen, die jedoch nicht näher beschrieben werden. Gruppenrichtlinien sollten auch dann gesetzt werden, wenn die konkrete Einstellung einer Konfiguration den voreingestellten Werten entspricht.

Das Dokument gibt in zwei Kapiteln für die Anforderungen der Bausteine „SYS.2.1 Allgemeiner Client“ und „SYS2.2.2.3 Clients unter Windows 10“ spezifische Hinweise und Empfehlungen zur Konfiguration. Hierbei werden die Umsetzungshinweise teilweise erweitert und konkretisiert. Anforderungen, zu denen keine spezifischen Hinweise gegeben werden können, sind nicht im Dokument enthalten. Im Dokument werden die folgenden Symbole verwendet:

<b>Gruppenrichtlinien</b>	
	Computer Configuration
	User Configuration
<b>Windows Registrierungsdatenbank (Registry)</b>	
	Windows Registry
<b>Grafische Oberfläche (User Interface)</b>	
	Windows Settings („Settings“-App)
	Control Panel

## Gendergerechte Sprache

Englischsprachige Begriffe werden, wie von Microsoft in Windows übersetzt verwendet, auch wenn es sich hierbei ausschließlich um eine maskuline Form handelt (z.B. bei Rollen- und Kontenbezeichnungen). Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter und beinhalten keine Wertung.

<sup>2</sup> [https://www.cisecurity.org/cis-benchmarks/#microsoft\\_windows\\_desktop](https://www.cisecurity.org/cis-benchmarks/#microsoft_windows_desktop)

<sup>3</sup> [https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS\\_Win10/SiSyPHuS\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/SiSyPHuS_node.html)

<sup>4</sup> [https://www.stigviewer.com/stig/windows\\_10/](https://www.stigviewer.com/stig/windows_10/)

## 2 Abgrenzung

Im Fokus der Konfigurationsempfehlungen des Hilfsmittels stehen Arbeitsplatzrechner (Desktop, Notebooks, Tablets) auf denen Windows 10 Pro/Enterprise Version 20H2, Stand-alone oder innerhalb einer On-Premises Windows-Domäneninfrastruktur betrieben werden. Bei Einsatz aktuellerer Windows Versionen lassen sich die Empfehlungen grundsätzlich für Entscheidungen zu einer Konfiguration unter Berücksichtigung möglicher Abweichungen ebenfalls heranziehen und anwenden. Viele Bestandteile des Funktionsumfangs wurden in den vergangenen Windows 10 Versionen lediglich erweitert. Die Empfehlungen im Hilfsmittel beziehen sich zudem auf viele grundlegende Bestandteile. Wesentlichen Aufschluss über Änderungen der Empfehlungen können dem jeweiligen Ankündigungsdokument („Announcement.pdf“) der Security Baselines zur entsprechenden Windows Version geben (siehe 3.1.1.2 Microsoft Security Baselines).

Nicht Gegenstand des Hilfsmittels sind Betrachtungen und Empfehlungen, die einen hybriden oder vollständigen Einsatz von Cloud-Diensten wie Azure AD voraussetzen. Sofern von diesem Szenario abgewichen wird, sollten die Konfigurationsempfehlungen individuell neu bewertet und angepasst werden.

Gruppenrichtlinienpfade sowie die Bezeichnungen der Gruppenrichtlinieneinstellungen werden in der Ausgangssprache des Betriebssystems (Englisch: Vereinigte Staaten) aufgeführt. Bei Verweisen auf Webseiten (z. B. Dokumentation) wird ebenfalls die Originalsprache gewählt.

Teilweise beinhalten Empfehlungen zu Windows 10 auch Konfigurationen zu weiteren nicht enthaltenen Software-Produkten von Microsoft, wie beispielsweise Microsoft Office. Im Rahmen dieses Hilfsmittels werden allerdings nur Empfehlungen zu Betriebssystembestandteilen von Windows 10 aufgeführt. Werden zusätzliche mit Windows 10 ausgelieferte Softwarekomponenten, wie der Webbrowser „Edge“, der E-Mail Client „Mail“-App, Texteditor, Multimedia oder Synchronisations-/Kollaborationsdienste genutzt, dann haben diese ggfs. auch Auswirkungen auf die Konfiguration des Betriebssystems und sind daher vergleichbar zu betrachten, wie die Installation weiterer Softwareprodukte (z.B. Office-Anwendungen, PDF-Betrachter, Webbrowser, Multimedia-Programme oder Bürokommunikationslösungen). Dies sollte dazu führen, dass bereits getroffene Einstellungen zu Windows 10 noch einmal überprüft und ggfs. geändert werden müssen.

Die Zusammenstellung der im Hilfsmittel aufgeführten Konfigurationsempfehlungen stellt eine aus Sicht des BSI wichtige Auswahl dar und hat daher nicht alle Konfigurationsmöglichkeiten von Windows betrachtet.

Der Umsetzungsgrad von IT-Grundschutz-Anforderungen durch die Konfiguration von Windows 10 ist individuell zu bestimmen und gegebenenfalls durch ergänzende und/oder zusätzliche technische und organisatorische Maßnahmen innerhalb der vorgesehenen Einsatzumgebung zu berücksichtigen.



## 3 Vorgehensweise („Best Practice“-Empfehlung)

### 3.1 Vorbereitungen

#### 3.1.1 Administrative Vorlagen (ADMX)

##### 3.1.1.1 Windows 10 20H2

Mit jeder Windows 10 Version veröffentlicht Microsoft sog. administrative Vorlagen mit welchen das Betriebssystem über Gruppenrichtlinien individuell konfiguriert werden kann. In domänenverwalteten Umgebungen werden die zugehörigen „Administrative Templates“ (ADMX) mit entsprechenden Sprachdateien (ADML) serverseitig importiert, um die Windows 10 spezifischen Einstellungen vornehmen und an die Clients verteilen zu können (siehe auch [2.2.1 Zentraler Speicher für Gruppenrichtlinien](#)).

Die jeweils aktuelle Version der administrativen Vorlagen für die verschiedenen Windows 10 Versionen können über die Webseiten von Microsoft bezogen werden.

Für Windows 10 Version 20H2 können die Vorlagen unter nachfolgendem Link abgerufen werden:

- Administrative Templates (.admx) for Windows 10 October 2020 Update (20H2)  
<https://www.microsoft.com/en-us/download/102157>

##### 3.1.1.2 Microsoft Security Baselines

Mit den Security Baselines stellt Microsoft sicherheitsrelevante Einstellungen in Form von importierbaren Gruppenrichtlinienobjekten bereit:

- Security baseline (FINAL) for Windows 10 and Windows Server, version 20H2  
<https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-final-for-windows-10-and-windows-server/ba-p/1999393>

Tabelle 2: Verzeichnisstruktur und Inhalt der Microsoft Security Baselines („Windows 10 Version 20H2 and Windows Server Version 20H2 Security Baseline.zip“)

Verzeichnisname	Beschreibung
Documentation	Das Ankündigungsdokument zu den Security Baselines („Announcement.pdf“) enthält eine Zusammenfassung der wesentlichen Neuerungen und Änderungen zur jeweiligen Version der Security Baselines. Übersicht der verfügbaren Gruppenrichtlinieneinstellungen für Windows 10 und Windows Server 20H2: <ul style="list-style-type: none"> <li>• „FINAL-MS Security Baseline Windows 10 and Windows Server v20H2.xlsx“</li> </ul> Neu hinzugefügte Gruppenrichtlinieneinstellungen in Windows 10 und Windows Server 20H2: <ul style="list-style-type: none"> <li>• „New Settings in Windows 10 and Windows Server v20H2.xlsx“</li> </ul>
GP Reports	In den Gruppenrichtlinienberichten (HTML-Format) sind die Einstellungen, der mit der Baseline bereitgestellten Gruppenrichtlinienobjekte, aus dem Verzeichnis „GPOs“ abrufbar.
GPOs	Enthält Gruppenrichtlinienobjekte für verschiedene Anwendungsbereiche (Einstellungen in der „Computerkonfiguration“ und „Benutzerkonfiguration“ für Windows 10 20H2, Internet Explorer, BitLocker, Microsoft Defender, Domain Security, Credential Guard, Domain Controller Virtualization Based Security, Domain Controller, Member Server), die in der Gruppenrichtlinienverwaltung (Group Policy Management Console) importiert werden können.

Verzeichnisname	Beschreibung
Scripts	<p>Mitgelieferte PowerShell Skripte importieren Gruppenrichtlinieneinstellungen der Security Baseline:</p> <ul style="list-style-type: none"> <li>• In ein Active Directory Verzeichnis („Baseline-ADImport.ps1“) oder</li> <li>• In nicht-domänenverwaltete Clients („Baseline-LocalInstall.ps1“).</li> </ul> <p>Mit dem Skript „Remove-EPBaselineSettings.ps1“ lassen sich Exploit-Schutz (Exploit Protection) Einstellungen, die durch frühere Security Baselines konfiguriert werden, gemäß Angabe von Microsoft<sup>5</sup> nahezu vollständig auf den Ursprungszustand zurücksetzen.</p> <p>Das Hilfsskript „MapGuidsToGpoNames.ps1“ verknüpft Gruppenrichtlinienamen mit den GUIDs eines GPO-Backups.</p>
Templates	<p>Die Gruppenrichtlinienvorlagen (Templates) für LAPS („AdmPwd.admx“), MSS-Einstellungen („MSS-legacy.admx“) und Security Guide („SecGuide.admx“) inkl. den zugehörigen Sprachdateien („*.adml“) im Verzeichnis „en-US“ enthalten zusätzliche Gruppenrichtlinieneinstellungen, die (je nachdem ob der Client Teil einer Domäne ist) in den zentralen Speicher für Gruppenrichtlinien (siehe 3.2.1) oder bei Stand-alone Clients in den lokalen Speicher „PolicyDefinitions“ (siehe 3.3.1) kopiert werden müssen.</p>

### 3.1.1.3 Microsoft Security Compliance Toolkit (SCT)

Das Security Compliance Toolkit umfasst mehrere Werkzeuge, mit denen sicherheitsrelevante Einstellungen in Windows 10 und weiteren Microsoft Produkten - vorzugsweise über Gruppenrichtlinien - konfiguriert, getestet und regelmäßig überprüft werden können.

- **Microsoft Security Compliance Toolkit 1.0**

<https://learn.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10>

## 3.2 Domänenverwalteter Client (Domain-joined Client)

### 3.2.1 Zentraler Speicher für Gruppenrichtlinien

Für eine zentrale Verwaltung und Konfiguration der Gruppenrichtlinien für Windows 10 wird die Verwendung des sog. zentralen Speichers (engl.: *Central Store*) empfohlen<sup>6,7</sup>. Beim Central Store handelt es sich um einen zentralen Ablageort für alle Gruppenrichtlinien, die im Active Directory-Verzeichnisdienst abgelegt werden.

Der Standardpfad zur Ablage der administrativen Vorlagen (ADMX) und der zugehörigen Sprachdateien (ADML) lautet:

```
\\<Domain Name>\SYSVOL\<Domain Name>\Policies\PolicyDefinitions
```

Hinweis: Ggfs. ist das Verzeichnis „PolicyDefinitons“ noch anzulegen.

<sup>5</sup> Siehe Beschreibung in „Remove-EPBaselineSettings.ps1“.

<sup>6</sup> <https://learn.microsoft.com/de-de/troubleshoot/windows-client/group-policy/create-and-manage-central-store>

<sup>7</sup> <https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-managing-windows-10-with-administrative-admx/ba-p/842926>

## 3.2.2 Zentrale Gruppenrichtlinienverwaltung

### 3.2.2.1 Gruppenrichtlinien-Verwaltungskonsole (Group Policy Management Console)

Über die Gruppenrichtlinien-Verwaltungskonsole lassen sich Gruppenrichtlinienobjekte u. a. erstellen, auflisten und Organisationseinheiten zuordnen.

Server-Manager → Tools → Group Policy Management

### 3.2.2.2 Gruppenrichtlinien-Objekteditor (Group Policy Object Editor)

Sollen Gruppenrichtlinienobjekte bearbeitet werden, ist der Gruppenrichtlinien-Objekteditor („Group Policy Management Editor“) zu verwenden:

Server-Manager → Tools → Group Policy Management → Group Policy Objects → Edit (im Kontextmenü des zu bearbeiteten Gruppenrichtlinienobjekts)

Gruppenrichtlinienobjekte im zentralen Gruppenrichtlinienverwaltungs-Editor weisen nachfolgende Struktur auf:

#### Gruppenrichtlinienobjektname

- **Computer Configuration**
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - Preferences
    - Windows Settings
    - Control Panel Settings
- **User Configuration**
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - Preferences
    - Windows Settings
    - Control Panel Settings

Im Vergleich zum lokalen Gruppenrichtlinieneditor erfolgt eine Aufteilung der „Computer Configuration“ sowie der „User Configuration“ in die Knoten „Policies“ und „Preferences“. In Abschnitt 3.2.3 (Gruppenrichtlinieneinstellungen und Gruppenrichtlinienvoreinstellungen) werden die Unterschiede erläutert. In den Eigenschaften eines Gruppenrichtlinienobjekts können dem Gruppenrichtlinienobjekt erläuternde Kommentare hinzugefügt werden. Werden nur Computer-spezifische bzw. ausschließlich Einstellungen in der „Benutzerkonfiguration“ vorgenommen, so können zur Verbesserung der Verarbeitungsperformance der Gruppenrichtlinie jeweils die Bereiche deaktiviert werden, zu denen im jeweiligen Gruppenrichtlinienobjekt keine Einstellungen vorgenommen werden.

**Hinweis:** Einstellungen zu „Preferences“ werden im Hilfsmittel nicht behandelt. Die Pfadangaben zu den Gruppenrichtlinien beziehen sich innerhalb des Hilfsmittels daher immer auf Einstellungen unter „Policies“.

### 3.2.3 Gruppenrichtlinieneinstellungen und Gruppenrichtlinienvoreinstellungen (Group Policy Preferences)

Gruppenrichtlinieneinstellungen sind Einstellungen, die grundsätzlich administrativ verbindlich vorgegeben werden. Das System soll davor geschützt werden, dass die Benutzenden eigenständig Änderungen an diesen Einstellungen vornehmen.

Gruppenrichtlinienvoreinstellungen sind Einstellungen, die dem System und Benutzenden vorgegeben werden können, allerdings nachträglich durch die Benutzenden veränderbar sind.

Dieser Unterschied sollte bei der Sicherheitskonfiguration berücksichtigt werden.

#### Zustände von Einstellungen bei Nichtkonfiguration von Gruppenrichtlinien

Gruppenrichtlinieneinstellungen weisen in der Regel folgende Konfigurationszustände auf:

- Nicht konfiguriert („Not Configured“)
- Aktiviert („Enabled“)
- Deaktiviert („Disabled“)

Darüber hinaus bieten eine Vielzahl von Gruppenrichtlinieneinstellungen zusätzlich die Möglichkeit, weitere Optionen zu konfigurieren. Hierbei kann es sich um Freitextfelder, Auswahllisten oder Auswahlkästchen handeln.

Zu einer Gruppenrichtlinieneinstellung kann der Beschreibung grundsätzlich entnommen werden, welche Konfiguration zu einem bestimmten Verhalten führt. Darüber hinaus beschreibt diese häufig auch das Verhalten, welches die Komponente oder Funktion aufweist, wenn die Gruppenrichtlinieneinstellung nicht konfiguriert ist („Not Configured“). Gruppenrichtlinieneinstellungen können Abhängigkeiten zu anderen Gruppenrichtlinieneinstellungen haben oder durch diese überschrieben werden. Viele Gruppenrichtlinieneinstellungen aktivieren oder deaktivieren nicht einfach nur eine Komponente oder Funktion, sondern sind in ihrer Wirkungsweise teilweise individuell. Teilweise liegt dies auch an der historischen Voreinstellung der Richtlinie<sup>8</sup>.

Alle Gruppenrichtlinieneinstellungen sollten stets explizit nach dem gewünschten Verhalten konfiguriert werden. Auf „nicht konfigurierte“ Einstellungen sollte verzichtet werden. Dies wirkt möglichen Änderungen des vordefinierten Verhaltens durch etwaige Updates entgegen.

Sollen Gruppenrichtlinieneinstellungen auf das durch Microsoft vordefinierte Verhalten in Windows 10 zurückgesetzt werden, sollte dieses explizit gesetzt werden.

## 3.3 Nicht-Domänenverwalteter Client (Local Windows-based Client)

### 3.3.1 Lokaler Speicher für Gruppenrichtlinien

Bei nicht domänenverwalteten Clients wird das lokale Gruppenrichtlinienobjekt, welches die Gruppenrichtlinieneinstellungen für die „Benutzerkonfiguration“ und „Computerkonfiguration“ enthält, im Dateisystem unterhalb des nachfolgenden Verzeichnisses gespeichert:

---

<sup>8</sup> <https://devblogs.microsoft.com/oldnewthing/20110606-00/?p=10493>

```
%systemroot%\System32\GroupPolicy
```

Standardpfad zur Ablage der administrativen Vorlagen (ADMX) und der zugehörigen Sprachdateien (ADML):

```
%systemroot%\PolicyDefinitions
```

### 3.3.2 Lokaler Gruppenrichtlinieneditor („gpedit“)

Der lokale Gruppenrichtlinieneditor in Windows 10 ist ein Snap-In für die Verwaltungskonsole (engl.: *Microsoft Management Console*, kurz: MMC) und ermöglicht Administrierenden eine Verwaltung der Gruppenrichtlinieneinstellungen des lokalen Gruppenrichtlinienobjekts:

```
%windir%\System32\gpedit.msc
```

Gruppenrichtlinienobjekte im lokalen Gruppenrichtlinieneditor weisen nachfolgende Struktur auf:

#### Gruppenrichtlinienobjektname

- **Computer Configuration**
  - Software Settings
  - Windows Settings
  - Administrative Templates
- **User Configuration**
  - Software Settings
  - Windows Settings
  - Administrative Templates

Im Gegensatz zu Gruppenrichtlinienobjekten die zentral verwaltet werden (siehe Abschnitt 3.2.2.2) wird die lokale Gruppenrichtlinie nicht in die Knoten „Policies“ und „Preferences“ unterteilt.

### 3.3.3 Lokale Sicherheitsrichtlinie („secpol“)

Die lokale Sicherheitsrichtlinie (engl.: *Local Security Policy*) ist eine Teilmenge der lokalen Gruppenrichtlinien und kann dediziert aufgerufen und bearbeitet werden:

```
%windir%\System32\secpol.msc
```

### 3.3.4 Microsoft Security Compliance Manager 3.0

#### 3.3.4.1 LocalGPO („LGPO.exe“)

- Erstellung eines lokalen Gruppenrichtlinienbackups (Export)
- Wiederherstellen (Import) von lokalen Gruppenrichtlinienbackups

Import von Gruppenrichtlinien mit dem LGPO-Werkzeug:

```
C:\> LGPO.exe /g "C:\<PFAD zu den Gruppenrichtlinien>
```

Für Clients mit erhöhtem Schutzbedarf sollte eine Referenzinstallation erstellt werden, in der die Grundkonfiguration und alle Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf den Client vorab getestet werden können (siehe SYS2.1.A30 Einrichten einer Referenzumgebung für Clients).

Es ist empfehlenswert, auch außerhalb des erhöhten Schutzbedarfes, die im Hilfsmittel empfohlenen Konfigurationseinstellungen innerhalb der vorgesehenen Einsatzumgebung vorab zu testen. Im Idealfall sollte hierzu eine Testumgebung genutzt werden, welche die produktive Einsatzumgebung möglichst genau abbildet. Mindestens sollte eine Referenzinstallation eingeplant und betrieben werden.

## 4 Konfiguration: SYS.2.1. Allgemeiner Client

### 4.1 Basis-Anforderungen

#### **SYS.2.1.A1 Sichere Benutzerauthentisierung (B)**

Die Identifikations- und Authentisierungsmechanismen von Windows 10 müssen so gestaltet sein, dass Benutzende sich eindeutig am IT-System authentisieren können. Passwörter, PINs, Token und Biometrie sind Techniken und Eigenschaften, über die sich Benutzende anmelden können. Die Verwendung von Windows 10 darf nicht ohne oder eine unzureichende Prüfung der Authentizität des Benutzenden durch die Administration erfolgen. Zur Umsetzung der Anforderung unterstützt Windows 10 die folgenden Authentisierungstechniken:

##### **Passwortbasierte Authentisierung (Standard)**

Die standardseitige Authentisierung von Benutzenden wird in Windows 10 durch Abfrage eines zugehörigen Passwortes durchgeführt. Es muss daher organisatorisch und technisch vorausgesetzt werden, dass durch Benutzende ein Passwort für ihr Konto zu setzen ist, welches den Sicherheitsrichtlinien der Institution entspricht.

Für die Umsetzung der Anforderung zur sicheren Benutzerauthentisierung sind die Anforderungen in ORP.4: Identität und Berechtigungsmanagement zu beachten. Insbesondere betrifft dies die Anforderungen:

- ORP.4.A8 Regelung des Passwortgebrauchs [Benutzer, IT-Betrieb] (B)
- ORP.4.A9 Identifikation und Authentisierung [IT-Betrieb] (B)
- ORP.4.A12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen [IT-Betrieb] (S)
- ORP.4.A22 Regelung zur Passwortqualität [IT-Betrieb] (B)
- ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme [IT-Betrieb] (B)


In den Umsetzungshinweisen<sup>9</sup> zum Baustein ORP4 Identitäts- und Berechtigungsmanagement können Richtwerte für die zu konfigurierenden Werte aus den Maßnahmen:

- ORP.4.M8 Regelung des Passwortgebrauchs (B)
- ORP.4.M9 Identifikation und Authentisierung (B)
- ORP.4.M12 Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen
- ORP.4.M22 Regelung zur Passwortqualität (B) und
- ORP.4.M23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme (B)

entsprechend den Regelungen und dem Einsatzzweck innerhalb der Organisation individuell abgeleitet werden.

Die Anforderungen an den Einsatz sicherer Passwörter lassen sich über die Kennwortrichtlinien festlegen. In domänenverwalteten Umgebungen müssen die Passwortrichtlinien über die „Default Domain Policy“ vorgenommen werden, damit sie global für alle Domänen-Konten angewendet werden.

<sup>9</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise 2021/Umsetzungshinweis zum Baustein ORP 4 Identitaets und Berechtigungsmanagement.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise%2021/Umsetzungshinweis%20zum%20Baustein%20ORP%204%20Identitaets%20und%20Berechtigungsmanagement.pdf)

 Computer Configuration/Windows Settings/Security Settings/Account Policies/Password Policy


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Enforce password history	Keep password history for: 24 passwords remembered	<p>Die Wiederholung alter Passwörter beim Passwortwechsel muss vom IT-System verhindert werden (Passworthistorie). Derzeit wird ein Maximalwert von 24 gespeicherten Passwörtern unterstützt (Voreingestellter Wert in domänenverwalteten Umgebungen). Ein hoher Wert soll verhindern, dass ein bereits verwendetes Passwort unmittelbar erneut vergeben werden kann.</p> <p>Wird keine Passworthistorie gespeichert (Wert: 0) können Benutzende bei einem Kennwortwechsel vormals genutzte Passwörter erneut vergeben. Der Wert sollte daher auf 24 gespeicherte Passwörter festgelegt werden.</p> <p>Der gesetzte Wert (24 gespeicherte Passwörter) bewirkt, dass erst nach 25 Passwortwechseln ein Passwort wiederverwendet werden kann. Daher muss die Länge der Historie in Zusammenhang mit dem minimalen Passwortalter betrachtet werden.</p> <p>Ein direkter Wechsel auf ein altes Passwort, welcher durch Benutzende absichtlich herbeigeführt wird, kann somit erschwert werden. Es bedarf einer zusätzlichen Sensibilisierung von Benutzenden, insbesondere wenn ein valider Grund für den Passwortwechsel vorgelegen hatte (z. B. Bekanntwerden des Passwortes gegenüber unautorisierten Personen).</p>
Maximum password age	365 days	<p>Die Notwendigkeit eines Passwortwechsels besteht nur mit einem validen Grund, beispielsweise wenn ein Passwort kompromittiert worden ist. Da nie vollständig ausgeschlossen werden kann, dass Passwörter abgegriffen worden sind, sollten präventiv regelmäßig Passwörter gewechselt werden. In der Praxis werden kompromittierte Anmeldeinformationen häufig für einen initialen Zugriff auf IT-Systeme durch Angreiferinnen und Angreifer ausgenutzt<sup>10</sup>.</p> <p>Häufige Passwortwechsel können Benutzende dazu verleiten, einfache Passwörter zu wählen. Daher sollte das Verhältnis</p>

<sup>10</sup> MITRE ATT&CK Technique T1078 (Valid Accounts) <https://attack.mitre.org/techniques/T1078/>



<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		<p>zwischen diesen Werten betrachtet werden.</p> <p>Es wird grundsätzlich empfohlen, Passwörter nach einem Jahr wechseln zu lassen.</p> <p>Bei Einsatz von Smartcards sollte darauf geachtet werden, dass die NT-Hashes regelmäßig geändert werden.</p>
Minimum password age	1 days	<p>Um zu verhindern, dass ein geändertes Passwort durch Benutzende unmittelbar auf ein bereits verwendetes Passwort zurück geändert werden kann, ist hier eine Zeitspanne von mind. einem Tag zu wählen.</p> <p>Je geringer der Wert des minimalen Passwortalters gewählt wird, desto kürzer ist die Zeitspanne, bis zu der ein altes Passwort durch Benutzende wiederverwendet werden könnte.</p>
Store passwords using reversible encryption	Disabled	<p>Die Empfehlung entspricht dem vordefinierten Verhalten.</p> <p>Passwörter werden bei aktivierter Gruppenrichtlinieneinstellung „Store passwords using reversible encryption“ mit dem in der Registry des Domänencontrollers gespeicherten SYSKEY ver- und entschlüsselt. „Domänenadministratoren“ und/oder mögliche Angreiferinnen und Angreifer, die über Zugriff auf den SYSKEY und die NTDS.dit verfügen, können hiermit die Klartextpasswörter von Konten ermitteln.</p> <p>Ein Aktivieren dieser Gruppenrichtlinie kann für Anwendungen erforderlich sein, die das Klartextpasswort von Konten zur Authentifizierung verwenden (z. B. MS-CHAP v1, SASL Digest Authentication, ältere macOS Clients, die sich an einer Domäne authentifizieren). Falls der Einsatz der umkehrbaren Verschlüsselung von Passwörtern zwingend notwendig sein sollte, sind vorher die Sicherheitsimplikationen genau zu evaluieren.</p>

## Anforderungen an die Passwortqualität

 Computer Configuration/Windows Settings/Security Settings/Account Policies/Password Policy

Gruppenrichtlinieneinstellung	Passwortphrasen (Option 1)	Komplexe Passwörter (Option 2)	Nutzung eines zweiten Faktors (z. B. Smartcard) für den interaktiven Logon (Option 3) <sup>11</sup>
Minimum password length	20-25 characters (Damit eine Mindestpasswortlänge von mehr als 14 Zeichen konfiguriert werden kann, muss zusätzlich die Richtlinieneinstellung „Relax minimum password length“) aktiviert werden).	10-12 characters	- Nicht erforderlich - Hinweis: Bei Option 3 wird systemseitig ein zufälliges 120 Zeichen langes Passwort gesetzt. Somit existiert weiterhin ein NT-Hash im AD, der verwendet wird. Dieser NT-Hash wird nicht automatisch regelmäßig geändert. Gemäß der Passwortrichtlinie ist eine Konfiguration vorzunehmen, um diesen 120-Zeichen NT-Hash analog zu den Kontenpasswörtern alle 365 Tage zu aktualisieren <sup>12</sup> .
Password must meet complexity requirements	Disabled	Enabled	Enabled

### Zusätzliche Konfiguration für Passwortlängen mit mehr als 14 Zeichen:


Um für domänenverwaltete Clients die minimale Passwortlänge konfigurieren zu können, muss die Konfiguration auf Domänencontrollern (vor Windows Server Version 20H1) über die PowerShell erfolgen, da die Bedienoberfläche des Group Policy Editors keine Eingabewerte von mehr als 20 Zeichen zulässt:

```
PS C:\> Set-ADDefaultDomainPasswordPolicy -MinPasswordLength [WERT] -Identity [DOMÄNE]
```

Ab Windows Version 20H1 existiert eine weitere Richtlinieneinstellung, mit der die Begrenzung auf 14 bzw. 20 maximale Zeichen für die minimale Passwortlänge über die GUI auf maximal 128 Zeichen festgelegt werden kann:

<sup>11</sup> Voraussetzung: Nutzung einer Public-Key-Infrastruktur (PKI) zur Verwaltung von (virtuellen) Smartcards  
Für den interaktiven Logon ist die Nutzung einer (virtuellen) Smartcard per Gruppenrichtlinieneinstellung zu erzwingen. Weitere Informationen: <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-require-smart-card> und <https://learn.microsoft.com/en-us/windows/security/identity-protection/virtual-smart-cards/virtual-smart-card-deploy-virtual-smart-cards>

<sup>12</sup> <https://learn.microsoft.com/en-us/archive/blogs/nextnextfinish/smart-card-logon-enforcement-long-edition>

 Computer Configuration Windows Settings/Security Settings/Account Policies/Password Policy

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Relax minimum password length	<b>Enabled</b>	Die mit Windows 10 Version 20H1 eingeführte Gruppenrichtlinieneinstellung legt fest, dass Vorgaben zur Mindestlänge der Passwörter über die GUI auch länger als 14 bzw. 20 Zeichen gewählt werden können. Normalerweise liegt die Grenze des Eingabefelds bei 14 bzw. 20 Zeichen. In domänenverwalteten Umgebungen müssen dafür alle Domänencontroller mindestens auf Windows Server Version 20H1 sein. Bei Einsatz der LTSC-Version des Servers, steht die Gruppenrichtlinieneinstellung ab Version 2022 zur Verfügung. Damit Passphrasen, wie in Option 1 der Anforderungen an die Passwortqualität mit mehr als 14 bzw. 20 Zeichen verwendet werden können, ist die Richtlinie zu aktivieren.

Administrierende haben in domänenverwalteten Umgebungen zwei Möglichkeiten, die Passwortanforderungen an Konten zu definieren: Die Anforderungen an die Passwortrichtlinie können über Group Policy Objects (GPOs) oder über Active Directory Objekte mit dem Namen „Fine grained password policies“ (FGPPs)<sup>13</sup> umgesetzt werden (verfügbar ab Domain Functional Level 2008). Bei beiden Ansätzen lassen sich dieselben Attribute konfigurieren, lediglich die Flexibilität sowie die Granularität der Anwendung unterscheiden sich.

Seit Einführung von Active Directory wird die Konfiguration der Passwortrichtlinien über GPOs von Microsoft empfohlen. In der Voreinstellung wird dies in der „Default Domain Policy“ umgesetzt, welche auf Domänenebene verlinkt wird. Die Passwortrichtlinie lässt sich zwar zusätzlich in weiteren GPOs setzen und in der Domäne untergeordneten OUs verlinken, allerdings wird für Domänenbenutzer die GPO, welche auf oberster Ebene auf die Domäne direkt verlinkt wurde, mit der höchsten Priorität bezogen und angewendet. Somit ist über die Konfiguration mittels GPOs nur eine globale Passwortrichtlinie für alle Konten in einer Domäne möglich.

Passwortbasierte Angriffe, wie bspw. Brute-Force-Angriffe<sup>14</sup>, können erschwert werden, in dem zusätzlich Kontosperrrichtlinien festgelegt werden<sup>15</sup>:

 Computer Configuration/Windows Settings/Security Settings/Account Policies/Account Lockout Policy


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Account lockout duration	15 minutes	Es handelt sich um die empfohlene Zeit, nach der ein gesperrtes Konto automatisch wieder entsperrt wird. Der Wert darf zwischen 1 und 99.999 Minuten

<sup>13</sup> [https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements-level-100-#fine\\_grained\\_pwd\\_policy\\_mgmt](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements-level-100-#fine_grained_pwd_policy_mgmt)

<sup>14</sup> MITRE ATT&CK Technique T1110 (Brute Force): <https://attack.mitre.org/techniques/T1110/>

<sup>15</sup> MITRE ATT&CK Mitigation M1036 (Account Use Policies) <https://attack.mitre.org/mitigations/M1036/>

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		liegen; sollte jedoch weder zu hoch noch zu niedrig gewählt werden. Bei Wert 0 wird das Konto solange gesperrt, bis es durch einen Administrierenden entsperrt wird.
Account lockout threshold	10 invalid logon attempts	Nach zehn fehlgeschlagenen Versuchen werden Konten gesperrt und entweder automatisch (nach festgelegter Zeit in der Gruppenrichtlinie „ <i>Account lockout duration</i> “) oder durch einen Administrierenden wieder entsperrt. Der Wert darf zwischen 1 und 999 Versuchen liegen. Der Wert sollte nicht auf 0 gesetzt werden, da ein Konto damit aufgrund fehlerhafter Anmeldeversuche nie gesperrt wird. Ein zu hoch gewählter Wert erleichtert passwortbasierte Angriffe, wie z. B. Brute-Force.
Reset account lockout counter after	15 minutes	Sofern der Kontosperrschwellwert („ <i>Account lockout duration</i> “) größer 0 gewählt wurde, muss diese Gruppenrichtlinieneinstellungen mindestens auf den Wert 1 Minute gesetzt sein. Mit einem Wert von 15 Minuten für den Kontosperrschwellwert sollte für den Wert ein Zeitraum bis 15 Minuten gewählt werden. Nach diesem Zeitraum wird der Zähler der fehlerhaften Anmeldeversuche zurückgesetzt. Beispiel: Benutzende lösen 9 von maximal 10 zulässigen Fehlversuchen bei der Kontenanmeldung aus. Nach Ablauf von 15 Minuten wird der Zähler auf 0 zurückgesetzt. Benutzenden stehen anschließend wieder 10 zulässige Fehlversuche zur Verfügung.

 Computer Configuration/Windows Settings/Security Settings/Account Policies/Account Lockout Policy

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Prevent the use of security questions for local accounts	<b>Enabled</b>  Da es sich um vorgegebene Sicherheitsfragen handelt, die durchaus auch von Dritten erraten werden könnten, ist es empfehlenswert generierte Passwörter als Antwort zu wählen.	Für das bei der Installation initial erstellte Konto müssen Sicherheitsfragen beantwortet werden. Für alle weiteren Konten, die über die Windows Einstellungen („Accounts → Family and other users“) angelegt werden, können ebenfalls Sicherheitsfragen festgelegt werden. Die Richtlinieneinstellung bezieht sich nur auf lokale Konten. Im Falle eines Zurücksetzens des Kontenkennworts,

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		können vorab beantwortete Sicherheitsfragen gestellt werden, um den Vorgang des Zurücksetzens des Kennworts zu autorisieren.

### Verbieten der Netzanmeldung mit lokalen Konten



Computer Configuration/Windows Settings/Local Policies/User Rights Assignment

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Access this computer from the network <sup>16</sup>	Administrators; Remote Desktop Users	Die Gruppenrichtlinieneinstellung legt fest, welche Konten und Gruppen über das Netz auf den Client zugreifen dürfen. Für einen Windows 10 Client sind hier die Gruppen „Administrators“ und „Remote Desktop Users“ (sofern RDP verwendet werden soll) ausreichend. Es sollten nur solche Konten und Gruppen aufgenommen werden, die einen Zugriff über das Netz auf den Client explizit erfordern.
Deny access to this computer from the network	Bei Nicht-Domänenmitgliedschaft: <ul style="list-style-type: none"> <li>• Guests</li> <li>• Local account</li> <li>• Anonymous logon</li> <li>• Alle selbst angelegten Dienstknoten (Service Accounts)</li> </ul> Bei Domänenmitgliedschaft zusätzlich: <ul style="list-style-type: none"> <li>• Hochprivilegierte Konten und Gruppen, z. B. „Domain Admins“, „Enterprise Admins“</li> </ul>	Durch das Verbot der Netzanmeldung mit lokalen Konten können bspw. keine Netzfregaben oder Remote Desktop Verbindungen verwendet werden, die durch Authentisierung eines lokal vorhandenen Kontos ggfs. möglich sind. Bei Clients, die Mitglied einer Domäne sind, sollten zusätzlich auch hochprivilegierte Konten und Gruppen, wie beispielsweise die „Enterprise Admins“ und „Domain-Admins“, für eine lokale Anmeldung ausgeschlossen werden.



Computer Configuration/Administrative Templates/MS Security Guide

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
WDigest Authentication	<b>Disabled</b>	Das Deaktivieren der <i>WDigest Authentication</i> erfordert möglicherweise die Berücksichtigung von KB2871997 <sup>17</sup> .

<sup>16</sup> <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/access-this-computer-from-the-network>

<sup>17</sup> <https://msrc-blog.microsoft.com/2014/06/05/an-overview-of-kb2871997/>

## Umgang mit alternativen Authentifizierungsmethoden und Mehr-Faktor-Authentisierung

Alternative und zusätzlich zum Passwort freigegebene Authentisierungstechniken innerhalb der Organisation können die Sicherheit erhöhen. Entsprechend der Anforderung ORP.4.A23 muss daher geprüft werden, ob andere Authentisierungsmerkmale bzw. -verfahren zusätzlich zu oder anstelle von Passwörtern verwendet werden können. Bei höherem Schutzbedarf (siehe auch [SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung](#)) sollte eine sichere Mehr-Faktor-Authentisierung konfiguriert und verwendet werden. Der Einsatz von Mehr-Faktor Authentisierung<sup>18</sup> richtet sich insbesondere an Techniken von möglichen Angreiferinnen und Angreifern, bei denen abgegriffenen Anmeldeinformationen (häufig: Anmelde-name und Passwort) auf einfache Weise missbräuchlich verwendet werden können, um sich initialen oder weiterführenden Zugriff auf (weitere) Systeme zu verschaffen. Die von Windows 10 angebotenen weiteren Authentifizierungsmethoden können für das lokale Anmelden am Client verwendet werden.

Windows 10 bietet die folgenden Authentifizierungsmethoden an:

Tabelle 3: Authentifizierungsmethoden in Windows 10

Methode	Beschreibung
Windows Hello Face	Benutzende werden mittels Gesichtserkennung über eine spezielle Near-Infrarot (IR) Kamera authentisiert.
Windows Hello Fingerprint	Benutzende authentifizieren sich mittels Fingerabdrucksensors
Windows Hello PIN	Eine PIN soll im Vergleich zu einem Passwort leichter zu merken sein (geringere Länge und Komplexität). Die PIN wird hierfür an das lokale Gerät gebunden.
Security Key	Für die Authentifizierung an weiteren Diensten kann ein Hardware-Sicherheitstoken (USB, NFC) verwendet werden.
Password	Klassisches Passwort
Picture password	Für die Anmeldung wird ein Bild eingeblendet, auf dem eine selbst zu definierende Geste eingegeben werden muss.

Die Bereitstellung und Verwaltung der Authentifizierungsmethoden wird in Windows 10 über Hello oder Hello for Business vorgenommen:

- **Windows Hello (nicht-domänenverwaltete Clients/lokale Konten)**  
In der Standardkonfiguration nicht-domänenverwalteter Windows 10 Clients sind alternative Authentifizierungsmethoden (z. B. Gesichtserkennung, Fingerabdruck, Windows Hello PIN, Security Key, Picture Password) für lokale Konten aktiviert und können durch die Benutzenden nach Einrichtung des Windows Hello PINs selbst eingerichtet werden.
- **Windows Hello for Business (domänenverwaltete Clients/Domänenkonten)**  
In domänenverwalteten Umgebungen wird eine zentrale Konfiguration von Windows Hello for Business vorausgesetzt, damit alternative und/oder zusätzlich Authentifizierungsmethoden verwendet werden dürfen. In der Dokumentation zu Hello for Business werden Voraussetzungen an die Infrastruktur sowie Informationen zur Einrichtung bereitgestellt:  
<https://learn.microsoft.com/de-de/windows/security/identity-protection/hello-for-business/>

### Persönliche Identifikationsnummer (PIN) für Windows Hello und Windows Hello for Business

Windows 10 bietet die Möglichkeit, sich mittels PIN zu authentisieren. Die PIN, als Ergänzung zum Passwort, ist eine Zahlenfolge oder eine Kombination aus Buchstaben, Zahlen und Sonderzeichen und ist an das Gerät gebunden, an dem sie eingerichtet wurde.

<sup>18</sup> MITRE ATT&CK Mitigation <https://attack.mitre.org/mitigations/M1032/>



## Computer Configuration/Administrative Templates/System/PIN Complexity

Gruppenrichtlinieneinstellung	Empfehlung / Konfigurationsoptionen	Erläuterung
Expiration	<b>Enabled</b>  <b>Options:</b> PIN Expiration: 0	Es handelt sich um die Voreinstellung. Da die PIN an das Gerät (2. Faktor) gebunden wird, ergibt sich keine Notwendigkeit einer regelmäßigen Änderung der PIN. Die PIN sollte besonders dann geändert werden, wenn die PIN-Eingabe durch Dritte beobachtet worden sein könnte.
History	<b>Enabled</b>  <b>Options:</b> PIN History: 0	Voreingestellt beträgt der Wert 0. Im Fall einer anlassbezogenen Änderung der PIN sollte sich die neue PIN jedoch von der vorherigen PIN unterscheiden.
Maximum PIN length	<b>Enabled</b>  <b>Options:</b> Maximum PIN length: 127 characters	Die Empfehlung entspricht dem voreingestellten Wert. Mit der Gruppenrichtlinieneinstellung kann die maximale PIN-Länge konfiguriert werden.
Minimum PIN length	<b>Enabled</b>  <b>Options:</b> Minimum PIN length: 6 characters	Voreingestellt ist eine minimale PIN-Länge von 4 Zeichen. Die Mindestlänge sollte entsprechend der Sicherheitsrichtlinie festgelegt werden.
Require digits	<b>„Enabled“</b> oder <b>„Disabled“</b> (entsprechend der Passwortrichtlinie der Institution)	Die Zeichenfolge kann durch Benutzende im vordefinierten Verhalten frei gestaltet werden und sollte gemäß der Passwortrichtlinie der Institution gestaltet sein.
Require lowercase letters		
Require special characters		
Require uppercase letters		

**Automatische Anmeldung von Konten**

## Computer Configuration/Administrative Templates/Windows Components/Windows Logon Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Sign-in and lock last interactive user automatically after a restart	<b>Disabled</b>	Durch das Deaktivieren der Richtlinieneinstellung wird verhindert, dass Konten automatisch gesperrt angemeldet werden, falls diese sich vor einem Herunterfahren (u.a. auch Cold Boot) nicht ordnungsgemäß abgemeldet haben sollten.




## Computer Configuration/Administrative Templates/MSS (Legacy)

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Eine automatische Anmeldung von Benutzerkonten, insb. der Administration, sollte nicht erlaubt werden.

**Sichere Anmeldung aktivieren**


Der sogenannte sichere Desktop (engl.: *Secure Desktop*) wurde mit Windows Vista gemeinsam mit der „Benutzerkontensteuerung“ (engl.: *User Account Control*, kurz: UAC) eingeführt und hat zum Ziel, die

Eingabe von Anmeldenamen / Passwörtern abzusichern, indem deren Eingabe auf einen separaten Desktop-Prozess erfolgt. Auf diese Weise kann gängige Keylogger-Malware daran gehindert werden, Zugangsinformationen auszulesen<sup>19</sup>.


 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Interactive logon: Do not require CTRL+ALT+DEL	<b>Disabled</b>	Sowohl bei Stand-alone Clients als auch bei domänenverwalteten Clients ist das vordefinierte Verhalten „Enabled“, sodass die Tastenkombination „STRG + ALT + ENTF“ nicht vor Eingabe der Kontennameinformationen auf der Windows-Anmeldemaske betätigt werden muss. Bei Deaktivierung der Richtlinieneinstellung (Auswahl von „Disabled“) wird die Betätigung der Tastenkombination erforderlich. Ursprünglich erforderte das vordefinierte Verhalten auf domänenverwalteten Clients die Betätigung der Tastenkombination. Die Richtlinieneinstellung soll die Aufmerksamkeit von Benutzenden auf den Anmeldeprozess richten, falls die Eingabe der Tastenkombination nicht vorab eingefordert wird. In diesem Fall könnte es sich um eine gefälschte Eingabemaske handeln. Bei Konfiguration der Richtlinieneinstellung sollte bei Bedarf eine barrierefreie Anmeldung berücksichtigt werden.

### Verhalten bei Inaktivität und Bildschirmsperre

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Interactive logon: Machine inactivity limit	600 bis 900 Sekunden, aber nicht 0	Der konkrete Wert ist von der jeweiligen Einsatzumgebung abhängig. Hier sind beispielsweise auch stationäre und mobile Clients zu unterscheiden. Unabhängig von einer organisatorischen Regelung, die zum Sperren bei Verlassen des Arbeitsplatzes verpflichtet.

 Computer Configuration/Administrative Templates/MSS (Legacy)

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	<b>Enabled</b> <b>Options:</b> ScreenSaverGracePeriod • 5 oder weniger Sekunden	Durch die Richtlinieneinstellung kann die Übergangszeit zwischen Aktivierung des Bildschirmschoners und der eigentlichen Aktivierung des Lockscreens konfiguriert

<sup>19</sup> <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-require-ctrl-alt-del>



		werden. Diese beträgt vordefiniert 5 Sekunden.
--	--	--

### Verhalten nach dem Bereitschaftsmodus (Standby)


Damit sich Benutzende auch nach dem Standby an Windows 10 authentisieren muss, sollte geprüft werden, ob die entsprechenden Gruppenrichtlinieneinstellung korrekt konfiguriert wurden:

 *Computer Configuration/Administrative Templates/System/Power Management/Sleep Settings*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Require a password when a computer wakes (on battery)	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten.
Require a password when a computer wakes (plugged in)	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten.


### Sonstiges

#### Zuletzt angemeldetes Konto nicht anzeigen

 *Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options*


<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoption</b>	<b>Erläuterung</b>
Interactive logon: Don't display last signed-in	Anlassbezogen sollte diese Einstellung aktiviert („ <b>Enabled</b> “) oder deaktiviert („ <b>Disabled</b> “) werden.	Zu den Logon-Szenarien zählen u. a. die lokale Anmeldung am Client, Nutzung von RDP in Virtual Desktop Infrastructures (VDI). Hinweis: Die Einstellung betrifft nicht die Nutzungshistorie des Terminal Server Clients (MSTSC), sodass dort das zuletzt verwendete Konto einer RDP-Verbindung hinterlegt wird. Diese werden in der Windows-Registry unter folgendem Pfad gespeichert: „HKCU\SOFTWARE\Microsoft\Terminal Server Client\Servers“ Der zuletzt verwendete RDP-Server wird in der Datei „Default.rdp“ im Dokumenten-Verzeichnis des jeweiligen Kontos („%USERPROFILE%\Documents“) als versteckte Datei gespeichert.

### Informationen über Konten auf dem Anmeldebildschirm

 *Computer Configuration/Administrative Templates/System/Logon*


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Block user from showing account details on sign-in	<b>Disabled</b>	Mit der Richtlinieneinstellung lässt sich die Anzeige von Konteninformationen auf dem Anmeldebildschirm deaktivieren. Hierdurch wird verhindert, dass Informationen, die nicht zur Anmeldung an Windows benötigt werden, durch unbefugte eingesehen werden können.

## Netzauswahl auf dem Anmeldebildschirm

 Computer Configuration/Administrative Templates/System/Logon


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Do not display network selection UI	<b>Enabled</b>	Durch die Richtlinieneinstellung lässt sich verhindern, dass der Client ohne vorherige Authentisierung mit (drahtlosen) Netzwerken verbunden wird. Das entsprechende Netzauswahlsymbol wird auf dem Anmeldebildschirm entfernt.

## Erinnerung vor Kennwortablauf

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Interactive logon: Prompt user to change password before expiration	Es sollte ein Wert zwischen 5 und 14 Tage gewählt werden.	Die Richtlinie sollte so konfiguriert werden, dass Benutzende frühzeitig an den bevorstehenden Kennwortwechsel ihres Kontos erinnert werden.

## Anzahl zwischengespeicherter Anmeldungen beschränken


 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	Es sollte ein Wert von 4 oder weniger Anmeldungen gewählt werden.	Bei einer Hochverfügbarkeit der Anmeldung an der Domäne kann der Wert auch auf 0 gesetzt werden. Wenn nur sichergestellt werden soll, dass das zuletzt verwendete Konto angemeldet werden kann, ist der Wert 1 ausreichend. Insbesondere ist die Zwischenspeicherung von Anmeldungen mit hohen Privilegien, wie denen von (Domänen)-Administrationskonten, kritisch zu betrachten.

 Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow log on locally	BUILTIN\Users, BUILTIN\Administrators	Nur Konten der der vordefinierten Built-In Gruppen „Users“ sowie „Administrators“ dürfen sich mit dieser Empfehlung lokal in Windows 10 anmelden.
Deny log on locally	BUILTIN\Guests	Konten, die Mitglied der vorkonfigurierten Built-In Gruppe „Guests“ sind, dürfen sich nicht lokal in Windows 10 anmelden.

## Auflistung von Konten


 Computer Configuration/Administrative Templates/System/Logon

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Do not enumerate connected users on domain-joined computers	<b>Enabled</b>	Domänenkonten werden nicht auf der Anmeldemaske aufgeführt.

		Je nach Einsatzszenario kann es hilfreich sein, wenn die Domänenkonten auf der Anmeldemaske aufgelistet werden.
Enumerate local users on domain-joined computers	<b>Disabled</b>	Lokale Konten werden nicht auf der Anmeldemaske angezeigt. Je nach Einsatzszenario kann es hilfreich sein, wenn die lokalen Konten auf der Anmeldemaske aufgelistet werden.

 *User Configuration/Administrative Templates/Start Menu and Taskbar/Notifications*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Turn off toast notifications on the lock screen	<b>Enabled</b>	Vordefiniert können PopUp-Benachrichtigungen von Anwendungen (sog. „Toast Notifications“) auch auf dem Sperrbildschirm angezeigt werden. Um zu verhindern, dass hierdurch möglicherweise sensible Informationen in Abwesenheit von Benutzerinnen und Benutzern auf dem Sperrbildschirm angezeigt werden, sollten die Toast-Notifications deaktiviert werden.

 *Computer Configuration/Administrative Templates/System/Logon*


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Turn off app notifications on the lock screen	<b>Enabled</b>	Im vordefinierten Verhalten können Benutzende selbstständig entscheiden, welche Benachrichtigungen von Apps auch auf dem Anmeldebildschirm angezeigt werden. Um zu verhindern, dass hierdurch möglicherweise sensible Informationen für unberechtigte Dritte einsehbar sind, sollte die Richtlinieneinstellung aktiviert werden.

### Hinweis bei Verwendung der Local Administrator Passwort Solution (LAPS)

Um LAPS nutzen zu können, müssen einige Konfiguration abweichend zu den Empfehlungen der Anforderungen

- [SYS.2.2.3.A9 Sichere zentrale Authentisierung in Windows-Netzen \(S\)](#)
- [SYS.2.2.3.A19 Sicherheit beim Fernzugriff über RDP \[Benutzer\] \(S\)](#)
- und [SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten \(S\)](#)

gesetzt werden<sup>20</sup>:

 *Computer Configuration/Administrative Templates/MS Security Guide*

<b>Gruppenrichtlinieneinstellung</b>	<b>Bei Verwendung von LAPS</b>	<b>Bisherige Empfehlung</b>
Apply UAC restrictions to local accounts on network logons	<b>Disabled</b>	Enabled

<sup>20</sup> <https://learn.microsoft.com/de-de/archive/blogs/secguide/remote-use-of-local-accounts-laps-changes-everything>

 Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment

Gruppenrichtlinieneinstellung	Bei Verwendung von LAPS	Bisherige Empfehlung
Deny log on through Remote Desktop Services	Keine Einträge	Guests, NT AUTHORITY\Local Account
Deny access to this computer from the network	Keine Einträge	Bei keiner Domänen-Mitgliedschaft: <ul style="list-style-type: none"> <li>• Guests</li> <li>• Local account</li> <li>• Anonymous logon</li> <li>• Alle selbst angelegten Dienstkonten (Service Accounts)</li> </ul> Bei Domänenmitgliedschaft zusätzlich: Hochprivilegierte Konten und Gruppen, z. B. „Domain Admins“, „Enterprise Admins“

### SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen (B)

Aus den Entscheidungen zur Umsetzung von Anforderungen aus dem Baustein OPS.1.1.3: Patch- und Änderungsmanagement sind in Windows 10 die Autoupdate-Mechanismen entsprechend zu konfigurieren. Hierbei zu berücksichtigen ist, ob ein selbstverwalteter Windows Service Update Server (WSUS) eingesetzt werden soll. In Infrastrukturen mit mehreren Windows 10 Clients kann es vorteilhaft sein, Windows Server Update Services (WSUS) zum Bezug und Verteilung der Updates für die Clients vorzusehen. Hierdurch können Updates an die Clients geplant und gestaffelt verteilt werden. Darüber hinaus lässt sich neben der Einsparung von Netzbandbreite eine direkte Kommunikation der Clients mit externen Diensten (wie Microsoft Update) einschränken.

Nach dem von Microsoft benannten Modell „Windows-as-a-service (WAAS)“ wird zwischen

- funktionalen Updates (engl.: *Feature Updates*) sowie
- monatlichen Qualitätsupdates (engl.: *Quality Updates*)

unterschieden.

(Sicherheits-)Updates für Windows 10 fallen in die Kategorie der monatlichen Qualitätsupdates und können über die Windows Updates, Windows Server Update Services (WSUS), eine Softwareverteilung (z. B. SCCM) oder manuell über den Update-Katalog<sup>21</sup> bezogen werden. Entsprechend des genutzten Bereitstellungsweges sollten in Windows 10 die automatischen Update-Mechanismen aktiviert und konfiguriert werden. Hierbei sollten die Updates und Patches vor dem Einspielen auf den Client vorab auf einer Referenzinstallation getestet werden (siehe SYS.2.1.A30 Einrichten einer Referenzumgebung für Clients).

#### Klassifizierung von Windows-Updates (Qualitätsupdates)

Tabelle 4: Updatekategorien in Windows

Kategorie	Beschreibung nach Microsoft
Wichtige Updates	Updates zur Verbesserung der Sicherheit und Zuverlässigkeit des Betriebssystems. Hierunter fallen u. a. die sogenannten monatlichen Rollup-Updates.
Empfohlene und optionale Updates	Beinhalten beispielsweise neue oder aktualisierte Treibersoftware für die am Client angeschlossenen Geräte

<sup>21</sup> <https://www.catalog.update.microsoft.com>

Die kumulativen Sicherheitsupdates (monatliches Rollup) werden einmal pro Monat am sogenannten „Patch Tuesday“ am jeweils zweiten Dienstag eines Monats über Windows Update sowie den Microsoft Update-Katalog veröffentlicht. In Ausnahmefällen, wie beispielsweise einer besonderen Bedrohungslage, werden Sicherheitsupdates auch außerhalb des „Patch Tuesday“ veröffentlicht (sog. „Out-of-Band-Updates“). Alle anderen Updates werden fortlaufend veröffentlicht.

Die funktionalen Updates des mit Windows 10 Version 21H2 eingeführten Bereitstellungskanals „General Availability Channel“ erscheinen jährlich und haben in der Pro-Edition einen 18-monatigen Lebenszyklus. In der Enterprise-Edition haben die Qualitätsupdates einen 30-monatigen Lebenszyklus<sup>22</sup>. Diese jährlichen Feature-Updates können bis zum Ende des jeweiligen Lebenszyklus der eingesetzten Windows 10 Version aufgeschoben werden.

**Hinweis:** Im vordefinierten Verhalten werden wichtige Updates automatisch heruntergeladen und installiert. Werden die zugehörigen Konfigurationseinstellungen über die Gruppenrichtlinie verwaltet, ist es Konten der Gruppe „Users“ nicht mehr möglich, diese über die Bedienoberfläche zu konfigurieren.

### Windows Updates (Qualitäts-Updates)

 Computer Configuration/Administrative Templates/Windows Components/Windows Update

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Configure Automatic Updates	<p><b>Enabled</b></p> <p><b>Options:</b> Configure automatic updating:</p> <ul style="list-style-type: none"> <li>4 – Auto download and schedule the install</li> </ul> <p>Scheduled install day:</p> <ul style="list-style-type: none"> <li>0 – Every day</li> </ul> <p><input type="checkbox"/> Install updates for other Microsoft products</p>	<p>Wenn Option 4 gewählt wurde, sollte ein Zeitplan (Wartungsfenster) festgelegt werden, in dem die Updates installiert werden. Bei aktivierter Richtlinieneinstellung wird in der Voreinstellung eine tägliche Installationszeit von 03:00 Uhr vorgesehen. Dies führt dazu, dass Windows in den meisten Fällen unmittelbar nach dem Einschalten des Clients (in der Regel morgens) Updates herunterlädt und installiert. Angemeldete Benutzende werden über einen bevorstehenden Neustart informiert und können die Zeit zum Neustart verschieben.</p> <p>Die Werte sollten nach den individuellen Anforderungen festgelegt werden. Es kann festgelegt werden, dass über die automatischen Updates des Betriebssystems auch Updates für weitere installierte Microsoft-Produkte bezogen und installiert werden sollen. Dies ist in den Sicherheitskonzepten der zu verwendeten Software zu betrachten.</p>
No auto-restart with logged on users for scheduled automatic updates installations	<p><b>Enabled</b></p>	<p>Angemeldete Benutzende werden über den anstehenden Neustart vorab informiert und können den Zeitpunkt des Neustarts nach hinten verschieben.</p> <p>Diese Einstellung setzt voraus, dass „Configure Automatic Updates“ konfiguriert wurde.</p>

<sup>22</sup> <https://learn.microsoft.com/de-de/lifecycle/faq/windows>

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		Microsoft empfiehlt diese Einstellung nicht mehr zu konfigurieren <sup>23</sup> .
Remove access to „Pause updates“ feature	<b>Enabled</b>	Im vordefinierten Verhalten können Benutzende können Updates pausieren. Durch die Richtlinieneinstellung kann der Zugriff durch Benutzende auf die Pausierungs-Funktion von Updateinstallationen verhindert werden.
Allow updates to be downloaded automatically over metered connections	<b>Enabled</b>	Windows Updates können ein großes Datenvolumen umfassen. Deckt ein Mobilfunkvertrag o.ä. diesen Bedarf nicht ab, können hier zusätzliche Kosten entstehen oder Datenvolumen vorzeitig aufgebraucht werden. Wird die Richtlinieneinstellung, „Deaktiviert“ (entspricht dem vordefinierten Verhalten) konfiguriert, werden nie Windows-Updates installiert, wenn ausschließlich eine getaktete Verbindung besteht. Trotz deaktivierter Richtlinieneinstellung können einige Windows Updates weiterhin heruntergeladen werden <sup>24</sup> . Getaktete Verbindungen müssen als solche gekennzeichnet werden <sup>25</sup> .
Do not include drivers with Windows Updates	<b>Disabled</b>	Durch eine Konfiguration der Richtlinieneinstellung mit „Deaktiviert“ werden auch Treiber über Windows Update bezogen.

### Einsatz von Windows Server Update Services (WSUS)

 Computer Configuration/Administrative Templates/Windows Components/Windows Update

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Specify intranet Microsoft Update service location	<b>Enabled</b>  In den Optionen zur Einstellung (Options) können bei Aktivierung nachfolgende Pfade zum WSUS-Server angegeben werden: <ul style="list-style-type: none"> <li>• Set the intranet update service for detecting updates</li> </ul>	Sofern ein WSUS-Server betrieben wird, sollten die Clients mit der Gruppenrichtlinie so konfiguriert werden, dass Updates ausschließlich über diesen Server bezogen werden.


<sup>23</sup> <https://techcommunity.microsoft.com/t5/windows-it-pro-blog/why-you-shouldn-t-set-these-25-windows-policies/ba-p/3066178>

<sup>24</sup> <https://support.microsoft.com/en-us/windows/why-can-t-i-change-the-metered-connection-setting-e2bb7d6e-2bd3-1b50-ea9c-ef813f3f58cf>


<sup>25</sup> <https://support.microsoft.com/en-us/windows/metered-connections-in-windows-7b33928f-a144-b265-97b6-f2e95a87c408>

	<ul style="list-style-type: none"> <li>Set the intranet statistics server</li> <li>Set the alternate download server (wenn ein alternativer WSUS-Server zur Verfügung steht)</li> </ul>	
Do not connect to any Windows Update Internet locations	<b>Enabled</b>	Mit der Konfiguration wird sichergestellt, dass die Clients ausschließlich eine Verbindung zum intern bereitgestellten WSUS-Server aufbauen.

### Microsoft Store Apps (nur GAC)

 Computer Configuration/Administrative Templates/Windows Components/Store


Gruppenrichtlinieneinstellung	Konfigurationsoptionen / Empfehlung	Erläuterung
Turn off Automatic Download and install of updates	„Enabled“ oder „Disabled“	Sofern Windows Apps, die über den App-Store aktualisiert werden, z.B. vorinstallierte Apps genutzt werden sollen, sollten automatische Updates hierfür aktiviert werden. Anderenfalls wird die Deaktivierung empfohlen.
Turn off the offer to update to the latest version of windows	<b>Enabled</b>	Mit dieser Einstellung werden über den Windows Store keine Vorschläge unterbreitet eine aktuellere Version von Windows 10 zu installieren.

 Computer Configuration/Administrative Templates/Windows Components/App runtime

Gruppenrichtlinieneinstellung	Konfigurationsoptionen / Empfehlung	Erläuterung
Block launching Universal Windows apps with Windows Runtime API access from hosted content	<b>Enabled</b>	Im vordefinierten Verhalten können alle Universal Windows Apps, die aus Webinhalten ausgeführt werden, auf die Windows Runtime API zugreifen. Sofern kein konkreter Anwendungsfall für solche UWP-Apps vorhanden ist, sollte die Ausführung durch die Richtlinieneinstellung blockiert werden.

### Feature Updates (nur GAC)

Feature Updates werden ebenfalls über Windows Update bereitgestellt. Alternativ ist eine Bereitstellung über die WSUS möglich. Um innerhalb der Organisation festzulegen und zu steuern, wann neue Windows 10 Version durch die Clients bezogen und installiert werden, können Konfigurationen der Gruppenrichtlinien von „Windows Update for Business“ vorgenommen werden:

 Computer Configuration/Administrative Templates/Windows Components/Windows Update/Windows Update for Business/

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Select the target Feature Update version	<b>Enabled</b>	Mit der Gruppenrichtlinieneinstellung wird die Windows 10 Zielversion festgelegt, die verwendet werden soll, um einen

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
	<b>Options:</b> <ul style="list-style-type: none"> <li>Target Version of Feature Updates: 20H2</li> </ul>	einheitlichen Versionsstand zu erreichen. Die Versionsnummer lässt sich über <a href="https://aka.ms/ReleaseInformationPage">https://aka.ms/ReleaseInformationPage</a> ermitteln. Sofern die Gruppenrichtlinieneinstellung nicht rechtzeitig aktualisiert wird, erfolgt möglicherweise eine automatische Aktualisierung auf die nächsthöhere Windows 10 Version nach Ablauf von 60 Tagen nach Ende des Supports.

### Verbindungskommunikationsendpunkte für Windows Update

Für Windows 10 Enterprise Version 20H2 werden von Microsoft nachfolgende Endpunkte angegeben<sup>26</sup>, zu denen das Betriebssystem eine Verbindung aufbauen kann, um Windows Updates herunterzuladen:

Tabelle 5: Verbindungskommunikationsendpunkte für Windows Update - Dienste

<b>Endpunkt(e)</b>	<b>Protokoll(e)</b>
*.prod.do.dsp.mp.microsoft.com	TLSv1.2/HTTPS/HTTP
emdl.ws.microsoft.com	HTTP
*.dl.delivery.mp.microsoft.com	TLSv1.2/HTTPS/HTTP
*.windowsupdate.com	HTTP
*.delivery.mp.microsoft.com	TLSv1.2/HTTPS/HTTP

### SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware (B)

Für einen Büroarbeitsplatz (normaler Schutzbedarf) mit wenigen, standardisierten Anwendungen kann der mitgelieferte Microsoft Defender verwendet werden. Dabei muss organisatorisch oder technisch sichergestellt werden, dass Sicherheitsereignisse zeitnah ausgewertet und bearbeitet werden (siehe DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion).

Im Stand-alone Betrieb oder in kleinen Arbeitsgruppen kann die Auswertung noch lokal über die Ereignisanzeige (Event Log) regelmäßig durch die Administration erfolgen.

In größeren Umgebungen ist eine dezentrale Auswertung auf vielen Clients nicht praktikabel, weshalb ein zentrales Monitoring und Reporting sowie eine zentrale Reaktion erforderlich werden (siehe DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse). Der Microsoft Defender selber enthält diese Funktionen nicht. Diese müssen bei Verwendung durch umliegende Maßnahmen umgesetzt werden oder alternative Produkte anderer Hersteller eingesetzt werden (siehe SYS.2.1.A10 Planung des Einsatzes von Clients).

Bei höherem Schutzbedarf muss aufgrund der Detektionsleistung gegebenenfalls ein anderes Schutzprogramm<sup>27</sup> oder eine andere Konfiguration des Microsoft Defenders ausgewählt werden (siehe [OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes \(B\)](#)).

Warnungen und gefundene Schadsoftware oder erkannte Angriffsversuche werden dem interaktiv angemeldeten Konto über eine PopUp-Benachrichtigung (sog. „Toast Notification“) angezeigt und zusätzlich in das Windows Event Log protokolliert (siehe Hinweis zu [OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen](#)).

<sup>26</sup> <https://learn.microsoft.com/en-us/windows/privacy/manage-windows-20h2-endpoints>

<sup>27</sup> MITRE ATT&CK Mitigation M1049 (Antivirus/Antimalware): <https://attack.mitre.org/mitigations/M1049/>



Microsoft stellt eine Liste der URLs zu Kommunikationsendpunkten zur Verfügung, die bei Nutzung des Microsoft Defender aufgerufen werden<sup>28</sup>.


Bei erhöhtem Schutzbedarf sollte die Anforderung SYS.2.1.A6 zusammen mit der Anforderung [SYS.2.1.A33 Einsatz von Ausführungskontrolle](#) betrachtet werden, um eine Ausführung schädlicher Software, über die noch keine Heuristik oder Signatur vorliegt, einzuschränken<sup>29</sup>.

Außerdem kann die Angriffsfläche durch Konfiguration des Microsoft Defender Exploit Guard Attack Surface Reduction reduziert werden, wenn der Microsoft Defender Antivirus Echtzeitschutz aktiviert ist (siehe [Empfehlungen zur Konfiguration der ASR-Regeln](#) unten). Mithilfe von Attack Surface Reduction (ASR) Regeln kann u.a. die initiale Kompromittierung durch die missbräuchliche Verwendung vertrauenswürdiger (System-)Programme und Werkzeuge erschwert oder verhindert werden (siehe MITRE ATT&CK Mitigation M1050 (Exploit Protection)<sup>30</sup>).

Die im Kapitel „Microsoft Defender Exploit Guard: Attack Surface Reduction“ genannten Regeln können einzeln auch nur im Audit Modus eingesetzt werden, beispielsweise um mögliche Auswirkungen einer Aktivierung bestimmter ASR-Regeln vorab zu testen. Anwendungen, z.B. zur Softwareverteilung oder Remote-Konfiguration können ggf. dem Einsatz mancher ASR-Regeln entgegenstehen. In diesen Fällen kann versucht werden, mit Ausnahmebehandlungen der ASR-Regeln zu arbeiten.

Schlägt eine Regel an, so erfolgt ein entsprechender Eintrag in der Windows Ereignisanzeige (Windows Defender/Operational). Es wird empfohlen, diese Einträge regelmäßig zu sichten und auszuwerten. Hierzu kann z.B. eine Ereignisweiterleitung genutzt werden.

### Early-Launch Anti-Malware

 *Computer Configuration/Administrative Templates/System/Early Launch Antimalware*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Boot-Start Driver Initialization Policy	<p><b>Enabled</b></p> <p><b>Options:</b> Choose the boot-start driver that can be initialized:</p> <ul style="list-style-type: none"> <li>• Good, unknown and bad but critical</li> </ul>	<p>Die Empfehlung entspricht der vordefinierten Konfiguration und sieht vor, dass auch als schädlich eingestufte Treiber geladen werden, ohne die jedoch das System nicht mehr starten würde. Es besteht das Risiko, dass schädliche Treiber nach Starten des Betriebssystems nicht als schädlich erkannt und entfernt werden können (z. B. Rootkits).</p> <p>Hinweis: Bei Einsatz von Antivirenlösungen anderer Hersteller müssen diese einen entsprechenden ELAM-Treiber mitliefern, damit die Einstellung angewendet wird<sup>31</sup>.</p>

<sup>28</sup> <https://download.microsoft.com/download/8/a/5/8a51eee5-cd02-431c-9d78-a58b7f77c070/mde-urls.xlsx>

<sup>29</sup> MITRE ATT&CK Mitigation M1038 (Execution Prevention): <https://attack.mitre.org/mitigations/M1038/>

<sup>30</sup> MITRE ATT&CK Mitigation M1050 (Exploit Protection): <https://attack.mitre.org/mitigations/M1050/>


<sup>31</sup> <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/elam-prerequisites>

## Umgang mit Dateien aus fremden und unbekanntem Quellen (Attachment Manager<sup>32</sup>)

 User Configuration/Administrative Templates/Windows Components/Attachment Manager

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Notify antivirus programs when opening attachments	<b>Enabled</b>	Ein in Windows 10 registriertes (Drittanbieter-)Schutzprogramm gegen Schadsoftware wird über den Vorgang informiert, dass ein Anhang geöffnet werden soll. Hierdurch soll ein On-Access Scan sichergestellt werden.
Do not preserve zone information in file attachments	<b>Disabled</b>	Entspricht den Vorgaben von Microsoft. Dateien werden um Zoneninformationen ergänzt, die den Ursprung der Datei kennzeichnen.
Hide mechanisms to remove zone information	<b>Enabled</b>	Damit die Zoneninformationen von gespeicherten Dateien nicht über die Dateieigenschaften entfernt werden können, empfiehlt es sich, die zugehörigen Funktionen aus der Oberfläche zu entfernen.

## Microsoft Defender Antivirus

 Computer Configuration/Administrative Templates/Windows Components/Windows Defender Antivirus


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off Windows Defender	<b>Disabled</b>	Im vordefinierten Verhalten wird durch den Microsoft Defender u. a. selbstständig entschieden, wie dieser sich nach der Installation eines Drittanbieterproduktes verhält. Vor der Installation eines Drittanbieterproduktes sollte entschieden werden, ob der Microsoft Defender über die Gruppenrichtlinie aktiviert oder deaktiviert werden soll.
Configure detection for potentially unwanted applications	<b>Enabled</b> <b>Options:</b> Block	Potenziell unerwünschte Anwendungen werden blockiert. Unterhalb dieser Kategorie fällt entsprechend der Definition von Microsoft jegliche Software, die zwar nicht explizit als Virus, Malware oder andere Form von Bedrohung bekannt ist, jedoch bspw. die Systemperformanz und Bedienbarkeit negativ beeinträchtigen können <sup>33</sup> .

<sup>32</sup> <https://support.microsoft.com/en-us/topic/information-about-the-attachment-manager-in-microsoft-windows-c48a4dcd-8de5-2af5-ee9b-cd795ae42738>

<sup>33</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/detect-block-potentially-unwanted-apps-microsoft-defender-antivirus?view=o365-worldwide>


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		Bevor die Einstellung aktiviert wird, sollte innerhalb eines Test-/Referenzsystems geprüft werden, ob für den Betrieb benötigte Software nicht durch die Funktion blockiert wird. Die Liste der potenziell unerwünschten Anwendungen wird von Microsoft gepflegt. Die zugehörigen Kriterien sind nicht veröffentlicht.

### Microsoft Defender Antivirus: Watson-Berichte

 *Computer Configuration/Administrative Templates/Windows Components/Microsoft Defender Antivirus/Reporting/*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Configure Watson events	<b>Disabled</b>	Durch Konfiguration der Richtlinieneinstellung werden keine Watson Ereignisse (Absturzinformationen über Anwendungen oder Dienste) an Microsoft gesendet.

### Microsoft Defender Antivirus Real-time Protection

 *Computer Configuration/Administrative Templates/Windows Components/Microsoft Defender Antivirus/Real-time Protection*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Turn off real-time protection	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten.
Turn on behavior monitoring	<b>Enabled</b>	Verhalten von Dateiprozessen sowie Änderungen von Dateien und der Windows-Registry werden vordefiniert hinsichtlich bekannten schädlichen Verhaltens überwacht.
Scan all downloaded files and attachments	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten.
Turn on process scanning whenever real-time protection is enabled	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten.
Monitoring file and program activity on your computer	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten.

### Microsoft Defender Antivirus: Microsoft Active Protection Service (MAPS)

Konfigurationsempfehlungen zum Microsoft Active Protection Service (MAPS) werden in den Empfehlungen zur Anforderung [OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes \(B\)](#) aufgeführt.

## Microsoft Defender Antivirus: Exploit Guard



Computer Configuration/Administrative Templates/Windows Components/Microsoft Defender Antivirus/Microsoft Defender Exploit Guard/Network Protection

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Prevent users and apps from accessing dangerous websites	<b>Enabled</b>  <b>Options:</b> Block	Diese Einstellung ist nur bei der Aktivierung von SmartScreen relevant <sup>34</sup> und kann nur konfiguriert werden, wenn die Cloud Protection (MAPS) genutzt wird (siehe <a href="#">Empfehlungen zu OPS.1.1.4.A3</a> ). Durch den „Netzwerkschutz“ des Microsoft Defender Exploit Guards lässt sich nach Aussage von Microsoft das Risiko minimieren, dass Benutzende durch Anwendungen auf bekannte maligne Inhalte im Internet zugreifen können <sup>35</sup> . Die Einstellung entspricht den Empfehlungen von Microsoft (siehe Security Baselines Windows 10 20H2).

## Microsoft Defender Exploit Guard: Attack Surface Reduction



Computer Configuration/Administrative Templates/Windows Components/Windows Defender Exploit Guard/Attack Surface Protection

Gruppenrichtlinieneinstellung	Empfehlung / Konfigurationsoptionen	Erläuterung
Configure Attack Surface Reduction rules	<b>Enabled</b>  <b>Options:</b> Set the state for each ASR rule: <ul style="list-style-type: none"> <li>Value name: GUID</li> <li>Value:               <ul style="list-style-type: none"> <li><b>1: Block</b></li> <li>0: Off</li> <li>2: Audit</li> </ul> </li> </ul> b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4 = <b>1</b> 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 = <b>1</b> d3e037e1-3eb8-44c8-a917-57927947596d = <b>1</b>	Die aufgelisteten Regeln entsprechen den Empfehlungen von Microsoft und sollen helfen, die Angriffsfläche zu reduzieren, um eine Infektion mit Schadsoftware zu verhindern. Microsoft stellt in der Dokumentation eine Übersicht über die zur Verfügung stehenden GUIDs bereit <sup>36</sup> . Mit den hier empfohlenen GUIDs soll die Angriffsfläche für folgende Bereiche reduziert werden: <ul style="list-style-type: none"> <li>Nicht vertrauenswürdige und nicht signierte Prozesse, die von USB ausgeführt werden, blockieren</li> <li>Diebstahl von Anmeldeinformationen aus dem Subsystem für die lokale</li> </ul>

<sup>34</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?ocid=cx-blog-mmpc&view=o365-worldwide>

<sup>35</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-network-protection?view=o365-worldwide>

<sup>36</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide>

Gruppenrichtlinieneinstellung	Empfehlung / Konfigurationsoptionen	Erläuterung
	<p>5beb7efe-fd9a-4556-801d-275e5ffc04cc = 1 e6db77e5-3df2-4cf1-b95a-636979351e5b = 1 d1e49aac-8f56-4280-b9ba-993a6d77406c = 0, 1 oder 2</p> <p><b>In Abhängigkeit davon, ob die Cloud-Protection (MAPS-Beitritt ist Voraussetzung) genutzt wird, können zusätzlich folgende ASR-Regeln konfiguriert werden:</b> c1db55ab-c21a-4637-bb3f-a12568109d35 = 0, 1 oder 2 01443614-cd74-433a-b99e-2ecdc07bfc25 = 0, 1 oder 2</p>	<p>Sicherheitsautorität (lsass.exe) blockieren</p> <ul style="list-style-type: none"> <li>• JavaScript und VBScript am Starten heruntergeladener ausführbarer Inhalte hindern</li> <li>• Ausführung potenziell verborgener Skripte blockieren</li> <li>• Persistenz durch WMI-Ereignisabonnement blockieren</li> <li>• Erstellung von Prozessen durch PSEXEC- und WMI-Befehle blockieren (Hinweis: Bei Konfiguration dieser ASR-Regel sollten mögliche Auswirkungen auf die IT-Infrastruktur (z.B. bei Einsatz einer Softwareverteilung o.ä., welche die WMI verwendet) geprüft werden<sup>37</sup>).</li> </ul> <p>Zusätzliche ASR-Regeln, die nur mit aktiver Cloud Protection (MAPS) (siehe <a href="#">Empfehlungen zu OPS.1.1.4.A3</a>) konfiguriert werden können:</p> <ul style="list-style-type: none"> <li>• Erweiterten Schutz vor Ransomware verwenden</li> <li>• Ausführbare Dateien an der Ausführung hindern, außer sie erfüllen ein Verbreitungs-, Alters- oder vertrauenswürdige Listen-Kriterium</li> </ul> <p>Um die Konfiguration der ASR-Regeln zu testen, werden von Microsoft einige Beispielszenarien bereitgestellt<sup>38</sup>.</p>

### Microsoft Defender Antivirus: Scan-Einstellungen und Updates

Nach Aktualisierung der Virenschutzdefinitionen (sog. „Security Intelligence Updates“) des Microsoft Defender führt dieser im Anschluss einen Quick Scan durch, sofern der letzte qualifizierte Quick Scan mehr als 7 Tage zurückliegt<sup>39</sup>. Dieses vordefinierte Verhalten kann entsprechend der Regelungen des festgelegten

<sup>37</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide>

<sup>38</sup> <https://demo.wd.microsoft.com>

<sup>39</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/schedule-antivirus-scans?view=o365-worldwide>

Konzepts für den Schutz vor Schadprogrammen (siehe [OPS.1.1.4 Schutz vor Schadprogrammen](#)) über die Gruppenrichtlinien<sup>40</sup> sowie die Aufgabenplanung (Task Scheduler)<sup>41</sup> angepasst werden.

Neben monatlichen Produktupdates für den Microsoft Defender (sog. „Platform Updates“), die über die Windows Updates bereitgestellt werden, veröffentlicht Microsoft in kürzeren Zeitabständen (i. d. R. mehrmals täglich) Aktualisierungen der Signaturdatenbank. Die Security Intelligence Updates werden vordefiniert über den Microsoft Defender bezogen. Alternativ können diese über die Webseite von Microsoft bezogen und manuell eingespielt werden: <https://www.microsoft.com/en-us/wdsi/defenderupdates>.



Computer Configuration/Administrative Templates/Windows Components/Microsoft Defender Antivirus/Scan

Gruppenrichtlinieneinstellung	Konfigurationsoptionen	Erläuterung
Specify the scan type to use for a scheduled scan	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Specify the scan type to use for a scheduled scan:</p> <ul style="list-style-type: none"> <li>Quick Scan (1)</li> <li>Full Scan (2)</li> </ul>	Im vordefinierten Verhalten ist in Windows 10 der Quick Scan (1) als Scan-Typ ausgewählt.
Specify the day of the week to run a scheduled scan	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Specify the day of the week to run a scheduled scan:</p> <ul style="list-style-type: none"> <li>(0x0) Every Day</li> <li>(0x1) Sunday</li> <li>(0x2) Monday</li> <li>(0x3) Tuesday</li> <li>(0x4) Wednesday</li> <li>(0x5) Thursday</li> <li>(0x6) Friday</li> <li>(0x7) Saturday</li> <li>(0x8) Never (default)</li> </ul>	Es kann ausgewählt werden, ob ein täglicher Scan erfolgen soll oder an einem bestimmten Wochentag durchgeführt wird. Durch Anpassung des geplanten Tasks für den Suchvorgang lassen sich Scans auch in größeren Zeitabständen festlegen. Bei nicht konfigurierter Richtlinieneinstellung werden geplante Scans in einem vordefinierten Intervall durchgeführt.
Specify the time of day to run a scheduled scan	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Specify the time of day to run a scheduled scan:</p> <ul style="list-style-type: none"> <li>0-1440 (Minuten)</li> </ul>	Vordefinierter Wert (bei nicht konfigurierter Richtlinieneinstellung): 120 (entspricht: 02:00 AM) Es kann ein Zeitpunkt gewählt werden, zu der ein geplanter Scan durchgeführt werden soll. Der eingetragene Wert repräsentiert die Minuten nach Mitternacht (00:00).
Start the scheduled scan only when computer is on but not in use	<p>„Enabled“ oder „Disabled“</p>	Es kann festgelegt werden, ob Scheduled Scans nur gestartet werden, wenn der Client nicht verwendet wird. Vordefiniert verhält sich Windows 10 bei nicht konfi-

<sup>40</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/use-group-policy-microsoft-defender-antivirus?view=o365-worldwide>

<sup>41</sup> <https://support.microsoft.com/en-us/windows/schedule-a-scan-in-microsoft-defender-antivirus-54b64e9c-880a-c6b6-2416-0eb330ed5d2d>

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
		guriertes Richtlinie, als wäre die Richtlinieneinstellung deaktiviert, sodass geplante Scans zur geplanten Zeit ausgeführt werden.
Specify the time for a daily quick scan	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Specify the time for a daily quick scan:</p> <ul style="list-style-type: none"> <li>• 0-1440 (Minuten)</li> </ul>	<p>Vordefinierter Wert (bei nicht konfigurierter Richtlinieneinstellung): 120 (entspricht: 02:00 AM)</p> <p>Es kann ein Zeitpunkt gewählt werden, zu dem ein Quick Scan durchgeführt werden soll.</p> <p>Der eingetragene Wert repräsentiert die Minuten nach Mitternacht (00:00).</p>
Specify the interval to run quick scans per day	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Specify the interval to run quick scans per day:</p> <ul style="list-style-type: none"> <li>• 1 (entspricht stündlich) bis 24 (entspricht einmal täglich)</li> </ul>	<p>Bei Quick Scans werden Verzeichnisse überprüft, in denen sich häufig Schadprogramme befinden können. Vordefiniert werden keine Intervall-basierten Quick Scans durchgeführt. Ein Intervall kann zwischen stündlich (1) und einmal täglich (24) festgelegt werden.</p>
Allow users to pause scan	„Enabled“ oder „Disabled“	<p>Es kann festgelegt werden, ob ein ausgeführter Scan unterbrochen bzw. pausiert werden kann.</p> <p>Durch Pausieren des Scans besteht grundsätzlich das Risiko, dass Gefahren nicht rechtzeitig erkannt werden. Bei nicht konfigurierter Richtlinieneinstellung können Scans durch Benutzer pausiert werden.</p>
Run full scan on mapped network drives	„Enabled“ oder „Disabled“	<p>Entweder sollte der Scan durch den Client erfolgen („Enabled“) oder durch den File-Server vorgenommen werden.</p> <p>Bei Konfiguration des Scans auf den Clients könnte dies bei gleichzeitigem Scandurchlauf zu einer höheren Auslastung des Netzes und des Dateiservers führen. Im vordefinierten Verhalten werden bei nicht konfigurierter Richtlinie verbundene Netzlaufwerke nicht durch Microsoft Defender auf dem Client mit in den Scan miteingeschlossen.</p>
Scan removable drives	„Enabled“ oder „Disabled“	<p>Bei aktivierter Einstellung werden alle angeschlossenen und eingebundenen Wechselmedien (z. B. USB-Sticks und -Festplatten) bei einem Scan automatisch mit einbezogen. Vordefiniert verhält sich Windows 10 so, als wäre die Einstellung deaktiviert, sodass Wechselmedien</p>

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
		grundsätzlich nur bei Quick Scans eingeschlossen werden.
Turn on catch-up full scan	„Enabled“ oder „Disabled“	Wird ein regulärer Full Scan nicht ausgeführt (bspw., wenn der Client zum festgelegten Zeitpunkt ausgeschaltet war), wird dieser nach dem zweiten verpassten Scan unmittelbar nach Anmeldung eines Kontos ausgeführt. Die Richtlinieneinstellung wird nur angewendet, wenn ein geplanter Suchvorgang (Scheduled Scan) besteht.
Turn on catch-up quick scan	„Enabled“ oder „Disabled“	Wird ein regulärer Quick Scan nicht ausgeführt (bspw. wenn der Client zum festgelegten Zeitpunkt ausgeschaltet war), wird dieser nach dem zweiten verpassten Scan unmittelbar nach Anmeldung eines Kontos ausgeführt. Die Richtlinieneinstellung wird nur angewendet, wenn ein geplanter Suchvorgang (Scheduled Scan) besteht. Bei nicht konfigurierter Richtlinie erfolgen vordefiniert keine Catch-Up Scans für geplante Quick Scans.
Turn on heuristics	„Enabled“ oder „Disabled“	Durch die Richtlinieneinstellung kann die Verwendung von Heuristiken durch den Microsoft Defender aktiviert oder deaktiviert werden. Bei nicht konfigurierter Richtlinie wird eine Heuristik durch den Windows Defender verwendet.
Define the number of days after which a catch-up scan is forced	„Enabled“ oder „Disabled“  <b>Options:</b> Define the number of days after which a catch-up scan is forced: <ul style="list-style-type: none"><li>• Angabe eines Wertes (Ganzzahl)</li></ul>	Durch die Einstellung kann festgelegt werden, nach wie vielen Tagen ein Scan erzwungen wird, wenn vorherige geplante Scans verpasst worden sind. Bei nicht konfigurierter Richtlinie erfolgt vordefiniert ein erzwungener Scan nach zwei verpassten Scans.
Scan packed executables	„Enabled“ oder „Disabled“	Durch die Richtlinieneinstellung kann festgelegt werden, ob gepackte ausführbare Dateien mit in den Scan eingeschlossen werden. Bei nicht konfigurierter Richtlinie werden gepackte ausführbare Dateien mit gescannt.
Scan archive files	„Enabled“ oder „Disabled“	Durch die Richtlinieneinstellung kann festgelegt werden, ob Archivdateien mit in den Scan eingeschlossen werden. Bei nicht konfigurierter Richtlinie werden Archivdateien mit gescannt.



<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
Specify the maximum depth to scan archive files	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Specify the maximum depth to scan archive files:</p> <ul style="list-style-type: none"> <li>• Angabe eines Wertes (Ganzzahl)</li> </ul>	Mit der Richtlinieneinstellung kann konfiguriert werden, dass geschachtelte Archivdateien mit gescannt werden. In den Konfigurationsoptionen kann eine Scan Tiefe angegeben werden. Bei nicht konfigurierter Richtlinie wird nur in der obersten Ebene von Archivdateien gescannt (entspricht Tiefe 0).
Check for the latest virus and spyware definitions before running a scheduled scan	<p>„Enabled“ oder „Disabled“</p>	Durch die Richtlinieneinstellung kann festgelegt werden, dass vor Ausführung eines geplanten Scans zunächst geprüft wird, ob aktuellere Definitionen zur Verfügung stehen. Bei nicht konfigurierter Richtlinie wird vor Ausführung des geplanten Scans nicht geprüft ob aktuellere Definitionen zur Verfügung stehen.

### Microsoft Defender Definition Updates



Computer Configuration/Administrative Templates/Windows Components/Microsoft Defender Antivirus/Security Intelligence Updates

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
Define the order of sources for downloading security intelligence updates	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Define the order of sources for downloading definition updates:</p> <ul style="list-style-type: none"> <li>• InternalDefinitionUpdate Server</li> <li>• FileShares</li> <li>• MicrosoftUpdateServer</li> <li>• MMPC</li> <li>• FileShares</li> </ul>	In verwalteten Umgebungen, in denen die Clients vom Internet gekapselt werden, können die Definitionsupdates für den Microsoft Defender auch von einer Netzfreigabe oder anderen Quellen bezogen werden.
Define file shares for downloading security intelligence updates	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Define file shares for downloading security intelligence updates:</p> <ul style="list-style-type: none"> <li>• \\UNC-Pfad</li> </ul>	Sofern die Definitionsupdates lokal im Netzwerk bereitgestellt werden sollen, ist in der Einstellung der Netzfreigabepfad (UNC-Pfad) anzugeben, in dem die Definitionsupdates hinterlegt werden. Es können auch mehrere Pfade angegeben werden (Trennzeichen: Pipe).
Turn on scan after security intelligence update	<p>„Enabled“ oder „Disabled“</p>	Durch die Richtlinie kann festgelegt werden, ob nach dem Update der Signaturendatenbank (Security Intelligence Update) ein Scan ausgeführt wird, sofern der letzte

Gruppenrichtlinieneinstellung	Konfigurationsoptionen	Erläuterung
		qualifizierte Quick Scan mehr als 7 Tage zurückliegt <sup>42</sup> .

Zum Bezug der Definitionsupdates gibt Microsoft nachfolgende Kommunikationsendpunkte an, die hierfür kontaktiert werden:

Tabelle 6: Verbindungskommunikationsendpunkte für Windows Defender Definition Updates

Verbindungsendpunkt(e)	Protokoll(e)
wdcp.microsoft.com	HTTPS/TLSv1.2
smartscreen-prod.microsoft.com	HTTPS
checkappexec.microsoft.com	HTTPS/HTTP

### Microsoft Defender SmartScreen

Die Konfigurationsempfehlungen zu Microsoft Defender SmartScreen werden in der Anforderung [SYS.2.2.3.A13 Einsatz der SmartScreen-Funktion](#) aufgeführt.

### SYS.2.1.A8 Absicherung des Bootvorgangs (B)

Die in Anforderung SYS.2.1.A8 geforderte Absicherung des Bootvorgangs wird nicht über Gruppenrichtlinieneinstellungen konfiguriert, sondern werden direkt in der UEFI-Firmware (Setup-Menü) vorgenommen.

Um von Windows 10 in die UEFI-Einstellungen zu gelangen, gibt es verschiedene Möglichkeiten, die nachfolgend kurz vorgestellt werden:

#### 1. Windows-Einstellungen (Windows Settings)

Windows-Settings/Update & Security/Recovery/Advanced startup:  
Auswahl von „Restart now“.

#### 2. Start-Menü

Im Start-Menü lässt sich nach Anklicken des Ein-/Aus-Buttons mit gehaltener Umschalttaste „Restart now“ auswählen.

#### 3. Anmelde-/Sperrbildschirm

Auf dem Anmelde-/Sperrbildschirm lässt sich nach Anklicken des Ein/Aus-Buttons mit gehaltener Umschalttaste „Restart now“ auswählen.

Unabhängig von der gewählten Möglichkeit wird anschließend ein Auswahlmenü angezeigt, bei dem folgende Optionen ausgewählt werden müssen:

#### 1. Troubleshoot (Reset your PC or see advanced options)

#### 2. Advanced options

#### 3. UEFI Firmware Settings

#### 4. „Restart“ auswählen, um in die UEFI-Firmwareeinstellungen zu booten.

#### • Secure Boot

Es sollte in der UEFI-Firmware überprüft werden, ob Secure Boot aktiviert ist. Das Kompatibilitätsunterstützungsmodul (engl.: *Compatibility Support Mode*) sollte nicht verwendet werden.

<sup>42</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/schedule-antivirus-scans?view=o365-worldwide>

- **Bootreihenfolge**  
Entsprechend der festgelegten Bootmedien ist die Bootreihenfolge in der Firmware so zu konfigurieren, dass keine Fremdmedien gebootet werden können. Für Windows 10 ist die Systempartition der Festplatte als Bootmedium ausreichend.
- **Bootmenü/Auflistung der angeschlossenen bootfähigen Geräte**  
Mit festgelegter Bootmenü-Tasten (z. B. F12) kann eine Übersicht der angeschlossenen bootfähigen Geräte beim Systemstart aufgerufen werden. Sofern die festgelegte Bootreihenfolge eingehalten werden soll und möglichst nicht durch einen Benutzenden ohne administrative Rechte beeinflusst wird, kann das Bootmenü in der Firmware deaktiviert werden.
- **Schutz vor unbefugtem Zugriff auf die Konfigurationseinstellungen der Firmware**  
Die Absicherung der Firmwareeinstellungen (BIOS/UEFI) vor unbefugtem Zugriff erfolgt durch einen Passwortschutz. Das hierfür gewählte Passwort richtet sich nach den Sicherheitsrichtlinien der Institution und ist für Anwendende nicht zur Verfügung zu stellen.
- **Nicht benötigte Funktionen der Firmware**  
Alle Funktionen sollten hinsichtlich ihrer Notwendigkeit für den Betrieb überprüft und entsprechend deaktiviert werden (siehe auch [SYS.2.1A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen](#)).

### SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen [Benutzer] (B)

In Windows 10 werden Komponenten mit ausgeliefert, die Cloud- und Online-Funktionen verwenden. Diese sind zum Teil fest im Betriebssystem integriert und können nicht deinstalliert werden. Es sollte daher festgelegt werden, welche dieser Funktionen genutzt und welche deaktiviert werden sollen.

Vor der Entscheidung zur Nutzung von Cloud- und Online-Funktionen muss bewertet werden, ob diese den Datenschutz- und Sicherheitsanforderungen genügen. Hierzu müssen alle grundlegenden technischen und organisatorische Sicherheitsanforderungen ausreichend berücksichtigt werden (siehe OPS.2.2.A1 Erstellung einer Strategie für die Cloud-Nutzung). Bei der Bewertung unterstützen können Veröffentlichungen des Herstellers, z. B. von Konformitätserklärungen zu IT-Sicherheitsstandards wie dem Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue)<sup>43</sup> des BSI. Die aktuellen Konformitätsberichte zu Microsoft Cloud-Diensten finden sich unter:

- <https://ms.portal.azure.com/#blade/Microsoft Azure Security/AuditReportsBlade>

Derzeit finden sich zu den Cloud-Diensten, die von in Windows 10 integrierten Funktionen genutzt werden, keine Konformitätsberichte.

Im Folgenden werden einige Online-Dienste behandelt, die Microsoft in Windows 10 nutzt:

#### Lokale Anmeldung am Client mit einem Microsoft-Konto

Der Umgang mit dem Microsoft-Konto sowie die zugehörigen Konfigurationsempfehlungen werden in der Anforderung [SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem](#) behandelt.

#### Erweiterte Online-Prüfungen des Microsoft Defenders

Die Online-Funktionalitäten des Microsoft Defenders Antivirus sollten konfiguriert werden ([siehe Konfigurationsempfehlungen zu SYS.2.1.A6](#)).

<sup>43</sup> [https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5\\_AktuelleVersion/C5\\_AktuelleVersion\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html)

## Erweiterung der Windows Desktop-Suche durch Online-Dienste



Computer Configuration/Administrative Templates/Windows Components/Search

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow Cloud Search	<b>Enabled</b>  <b>Options:</b> Cloud Search Setting: • Disable Cloud Search	Der Windows Suchfunktion („Windows Search“) und Cortana wird es unterbunden, in Cloud-Ressourcen wie z. B. OneDrive und SharePoint zu suchen.
Allow search and Cortana to use location	<b>Disabled</b>	Um zu verhindern, dass durch die Windows Suche und Cortana Standortinformationen des Geräts genutzt und verarbeitet werden, sollte die Richtlinie deaktiviert werden.
Do not allow web search	<b>Enabled</b>	Durch Aktivierung der Einstellung wird verhindert, das Internetsuchen über die Suchengine des Standard-Webrowsers durch die Windows Desktop-Suche vorgenommen werden können und hierdurch unabsichtlich Informationen an einen Suchanbieter abfließen könnten.
Don't search the web or display web results in Search	<b>Enabled</b>	Mit der Einstellung wird unterbunden, dass Suchergebnisse der Windows Suche auch Inhalte aus der Internetsuche abrufen und auflisten.
Allow indexing of encrypted files	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Verschlüsselte Dateien sollten nicht indiziert werden, da bei der Indizierung derartige Dateien entschlüsselt werden könnten.

### Sprachassistent Cortana

Die Konfigurationsempfehlungen zur Nutzung von Cortana werden in der Anforderung [SYS.2.2.3.A14 Einsatz des Sprachassistenten Cortana](#) erläutert.


### Abrufen von Tipps und Hilfe in den Windows-Einstellungen („Settings“-App)




Computer Configuration/Administrative Templates/Control Panel

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow Online Tips	<b>Disabled</b>	Durch das Abrufen von Tipps und der Hilfe in den Windows-Einstellungen (engl.: <i>Settings App</i> ) können Microsoft-Server kontaktiert werden. Um zu verhindern, dass unkontrollierte Anfragen zu den Servern gesendet werden, sollte die Richtlinie deaktiviert werden.


## Verwendung von Erkennungsdiensten für Sprache und Handschriften

 Computer Configuration/Administrative Templates/Control Panel/Regional and Language Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow users to enable online speech recognition services	<b>Disabled</b>	Durch das Deaktivieren der Richtlinie wird verhindert, dass Benutzende die Spracherkennungsdienste aktivieren und verwenden können. Durch Nutzung der Spracherkennungsdienste werden u. a. Sprach- und Eingabeverhaltensmuster mit der Cloud synchronisiert.

 Computer Configuration/Administrative Templates/Control Panel/Regional and Language Options/Handwriting personalization

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off automatic learning	<b>Enabled</b>	Diese Funktion erlaubt das Sammeln (möglicherweise sensibler) Informationen aus E-Mail- und Browser-Applikationen und überträgt diese potenziell zu Microsoft. Durch Konfigurieren dieser Richtlinie werden diese Informationen nicht mehr an Microsoft übermittelt.

 Computer Configuration/Administrative Templates/Windows Components/Text Input/Improve inking and typing recognition

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Improve inking and typing recognition	<b>Disabled</b>	Texteingaben können, beispielsweise zur Verbesserung der Spracherkennung, an Microsoft übermittelt werden und unter Umständen auch schutzbedürftige Informationen enthalten. Durch Konfigurieren dieser Richtlinie wird verhindert, dass Texteingaben vom Betriebssystem gesammelt und an Microsoft übertragen werden.

## Datensynchronisation zum OneDrive-Datendienst

Die Konfigurationsempfehlungen zur Nutzung von OneDrive zur Datensynchronisation wird in der Anforderung [SYS.2.2.3.A15 Einsatz von Synchronisationsmechanismen unter Windows 10](#) erläutert.

## KMS Client Online AVS Validation

 Computer Configuration/Administrative Templates/Windows Components/Software Protection Platform


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off KMS Client Online AVS Validation	<b>Enabled</b>	Um zu verhindern, dass „Key Management Services (KMS) Client-Aktivierungsdaten automatisch bei der Aktivierung an Microsoft gesendet werden, sollte die Richtlinie konfiguriert werden. In diesem

		Fall ist ggfs. ein lokaler KMS Dienst eigenständig zu betreiben, der dann die Verbindung zu Microsoft herstellt.
--	--	--

### Synchronisierung von Einstellungen zwischen mehreren Geräten (bei Nutzung von Microsoft Konten)

Die Synchronisierung von Einstellungen zwischen mehreren Geräten sollte angepasst werden. Die zugehörigen Konfigurationsempfehlungen befinden sich unter der Anforderung [SYS.2.2.3.A15 Einsatz der Synchronisationsmechanismen unter Windows 10](#).

### Find my Device (bei Nutzung von Microsoft-Konten)

 Computer Configuration/Administrative Templates/Windows Components/Find My Device


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn On/Off Find My Device	<b>Disabled</b>	Bei aktivierter Einstellung wird der Gerätestandort des Geräts mit der Microsoft Cloud synchronisiert. Benutzende können einen Suchbefehl aus der Microsoft Cloud heraus initiieren, um das Gerät zu orten.

### Cloudinhalte

 User Configuration/Administrative Templates/Windows Components/Cloud Content

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Configure Windows spotlight on lock screen	<b>Disabled</b>	Die Funktion „Windows Spotlight“ zeigt u. a. täglich wechselnde Hintergrundbilder, die aus externer Quelle abgerufen werden, auf dem Sperrbildschirm an.
Do not suggest third-party content in Windows spotlight	<b>Enabled</b>	Durch die Funktion „Windows Spotlight“ werden keine Drittanbieterempfehlungen angezeigt.
Do not use diagnostic data for tailored experiences	<b>Enabled</b>	Diagnosedaten aus der Verwendung von Browsern, Apps und Feature dürfen mit aktivierter Richtlinie nicht dazu verwendet werden, um auf das jeweilige Konto angepassten Inhalt anzuzeigen.
Turn off all Windows spotlight features	<b>Enabled</b>	Durch Aktivierung der Richtlinie lassen sich sämtliche „Windows Spotlight“-Funktionen deaktivieren und Netzwerkverkehr reduzieren. Hierzu zählen u. a. Sperrbildschirmfunktionen, Windows Tipps, Microsoft Verbraucherfunktionen.
Turn off the Windows Welcome Experience	<b>Enabled</b>	Nachdem ein funktionales Update in Windows 10 installiert wurde, wird nach der Anmeldung von Konten ggfs. die „Window Welcome Experience“ aufgerufen, in denen Veränderungen und Neuigkeiten vorgestellt werden und unter Umständen auch kontenspezifische Einstellungen vorgenommen werden können. Da der Endnutzende in vielen Fällen keine informierte

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		Entscheidung treffen kann, sollten die Datenschutzeinstellungen durch die Organisation vorgegeben werden.
Turn off Microsoft consumer experiences	<b>Enabled</b>	Den Benutzenden werden keine persönlichen Empfehlungen aufgrund erhobener „Benutzererfahrungen“ unterbreitet.
Turn off Windows Spotlight on Action Center	<b>Enabled</b>	Windows Spotlight Informationen werden nicht mehr im Action Center angezeigt.
Turn off Windows Spotlight on Settings	<b>Enabled</b>	Windows Spotlight lässt sich mit Aktivierung der Einstellung nicht mehr durch den Benutzenden in den Einstellungen konfigurieren.

 Computer Configuration/Administrative Templates/Windows Components/Cloud Content

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Do not show Windows tips	<b>Enabled</b>	Durch Aktivierung der Einstellung werden keine Hilfetext-Popups mehr angezeigt. Anderenfalls werden Tipps auf Grundlage gesammelter Diagnosedaten (engl.: <i>diagnostic data</i> ) angezeigt. Durch Konfiguration der Einstellung „Allow Telemetry“ (siehe <a href="#">SYS.2.2.3.A4</a> ) kann auch ein reduzierter Umfang der Tipps erfolgen, wenn weiterhin Windows Tipps angezeigt werden sollen.
Turn off cloud optimized content	<b>Enabled</b>	Cloudoptimierter Inhalt wird mit Aktivierung der Einstellung nicht mehr von Windows 10 abgerufen.
Turn off Microsoft consumer experiences	<b>Enabled</b>	Den Benutzenden werden keine persönlichen Empfehlungen aufgrund erhobener „Benutzererfahrungen“ unterbreitet.

## Internet Communication Management

 Computer Configuration/Administrative Templates/System/Internet Communication settings


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Turn off downloading of print drivers over HTTP	<b>Enabled</b>	Durch die Einstellung wird verhindert, dass Druckertreiber über nicht verschlüsselte Verbindungen (hier: HTTP) heruntergeladen werden und dabei potenziell sensible Informationen abfließen.
Turn off Internet download for Web publishing and online ordering wizards	<b>Enabled</b>	Die Einstellung verhindert, dass potenziell sensible Informationen abfließen können.
Turn off Event Viewer "Events.asp" links	<b>Enabled</b>	Durch die Einstellung werden Links innerhalb von Events der Ereignisanzeige deaktiviert. Bei Aufruf der Links werden Informationen über das Event zu Microsoft-Webseiten gesendet, um (sofern verfügbar)

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		weitere Erläuterungen zur Fehlermeldung anzuzeigen.
Turn off handwriting personalization data sharing	<b>Enabled</b>	Die Einstellung verhindert, dass Nutzungsdaten der Handschriftenerkennung an Microsoft gesendet werden.
Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	<b>Enabled</b>	Durch die Richtlinieneinstellung wird konfiguriert, dass der Internet Connection Wizard eine Liste von Internet Service Providern von Microsoft-Servern herunterlädt.
Turn off handwriting recognition error reporting	<b>Enabled</b>	Die Einstellung verhindert, dass Fehlerberichte zur Handschriftenerkennung an Microsoft gesendet werden können. Hinweis: Wenn die Einstellung „Turn off Windows Error Reporting“ aktiviert wurde, können auch keine Fehlerberichte zur Handschriftenerkennung versendet werden.
Turn off printing over http	<b>Enabled</b>	Die Richtlinie verhindert, dass Druckaufträge über http an einen Drucker übertragen werden und hierdurch potenziell sensible Informationen offengelegt werden.
Turn off Search Companion content file updates	<b>Enabled</b>	Um zu verhindern, dass Inhaltdateiupdates vom Such-Assistenten heruntergeladen werden, sollte die Einstellung deaktiviert werden.
Turn off the "Order Prints" picture task	<b>Enabled</b>	Über die „Photo Gallery“ in Windows 10 können Fotos zum Druck auch an externe Dienste gesendet werden. Um ein abfließen von möglicherweise sensiblen Informationen zu verhindern sollte die Funktion deaktiviert werden.
Turn off Windows Customer Experience Improvement Program	<b>Enabled</b>	Das „Windows Customer Experience Improvement Program“ sammelt Informationen zur verwendeten Hardwarekonfiguration und zur Softwarenutzung, um Verhaltens- und Nutzungsmuster zu bestimmen. Um zu verhindern, dass sensible Informationen zur Nutzung des Clients an Microsoft gesendet werden, sollte die Funktion deaktiviert werden.
Turn off Windows Error Reporting	<b>Enabled</b>	Die Einstellung verhindert, dass Fehlerberichte, die möglicherweise auch sensible oder persönliche Informationen von Benutzenden oder des Unternehmens/der Organisation beinhalten könnten, an Microsoft gesendet werden.
Turn off Windows Network Connectivity Status Indicator active tests	<b>Enabled</b>	Die Einstellung unterbindet Konnektivitätstests des Netzes in Windows.




<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Turn off Windows Update device driver searching	<b>Enabled</b>	Die Einstellung verhindert, dass nach Gerätetreibern über Windows Update gesucht wird, wenn lokale Treiber für das Gerät nicht gefunden wurden.

### Bezug von Schriftarten und -katalogdaten von einem Online-Schriftartenanbieter

 Computer Configuration/Administrative Templates/Network/Fonts


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Enable Font Providers	<b>Disabled</b>	Bei Bedarf können die in Windows bereits enthaltenen Schriftarten über weitere Schriftarten von einem Online-Schriftartenanbieter bezogen und nachinstalliert werden. Grundsätzlich können durch den Bezug von Schriftarten auch malizöse Inhalte nachgeladen werden. Die Funktion sollte daher deaktiviert werden.

### Benachrichtigungen über das Netzwerk senden und empfangen

 Computer Configuration/Administrative Templates/Windows Components/Start Menu and Taskbar

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Turn off notifications network usage	<b>Enabled</b>	Durch die Richtlinieneinstellung wird eine Synchronisierung zwischen Windows und den Push Notification Services (WNS) verhindert.

### Offline Maps

 Computer Configuration/Administrative Templates/Windows Components/Maps/Turn off Automatic Download and Update of Map Data

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Turn off Automatic Download and Update of Map Data	<b>Enabled</b>	Durch die Richtlinieneinstellung wird verhindert, dass die vorinstallierte Maps-App automatisch Daten herunterlädt oder das Kartenmaterial aktualisiert.
Turn off unsolicited network traffic on the Offline Maps settings page	<b>Enabled</b>	Durch die Richtlinieneinstellung wird verhindert, dass bereits auf der Konfigurationsoberfläche in den Windows-Einstellungen (Settings) ein Netzverkehr verursacht wird. Die Konfigurationsseite wird mit Aktivierung der Richtlinieneinstellung deaktiviert.

## 4.2 Standard-Anforderungen

### SYS.2.1.A10 Planung des Einsatzes von Clients (S)

In Windows-Umgebungen sind typischerweise für die Planung des Einsatzes die folgenden Aspekte besonders relevant:

- Vorgesehenes Einsatzszenario (mobil oder stationär, geschützt oder exponiert)
- Infrastruktur:
  - Stand-alone Betrieb
  - Kleine Arbeitsgruppen (Workgroup)
  - Domäne (z. B. Active Directory)

Einige Client-Richtlinien stehen in Bezug zur Netzkonzeption (NET.1.1 Netzarchitektur und -design) und unterstützen diese. Dies betrifft insbesondere das Zonenkonzept von Windows 10 (lokales Intranet, Internet). Die Intranetzone von Windows 10 sollte nur für Dienste im internen Netz erreichbar sein.

### **SYS.2.1.A11 Beschaffung von Clients (S)**

Abhängig von den vorgesehenen Funktionen sind zusätzliche Anforderungen an die Hardware zu berücksichtigen:

- Berücksichtigung von technischen Voraussetzungen, die durch die zu beschaffenden Produkte erfüllt werden müssen, um die geforderten Sicherheitsmaßnahmen umsetzen zu können
- Festlegen eines Nutzungszeitraumes und Einholen von Zusagen/Informationen über Bereitstellungszeitraum von Patches und Updates
- Kompatibilität zur eingesetzten Windows-Version (siehe Empfehlungen zu [SYS.2.2.3.A2 Auswahl und Beschaffung einer geeigneten Windows-10-Version](#))

### **SYS.2.1.A13 Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (S)**

Intel-Prozessoren bieten teilweise eine Funktion zur unbeobachteten Codeausführung (Intel Software Guard Extension, kurz: Intel SGX). Diese kann häufig in der Firmware konfiguriert werden:

- „Enabled“: Intel SGX steht zur Nutzung in Anwendungen zur Verfügung, sofern sie SGX unterstützen.
- „Software Controlled“ (auch „Software opt-in“): Auf Betriebssystemebene kann durch Software gesteuert werden, ob Intel SGX verwendet werden kann. Diese Option steht möglicherweise nicht auf allen Geräten zur Verfügung.
- „Disabled“: Intel SGX wird explizit deaktiviert und kann nicht außerhalb der Firmware aktiviert werden.

Wenn die Firmware-Einstellung „Enabled“ oder „Software Controlled“ gewählt ist, erkennt Windows 10 Intel SGX als Softwarekomponente, installiert einen Treiber und aktiviert diesen. Nicht alle Firmwareoberflächen bieten dieselben Konfigurationsmöglichkeiten für Intel SGX. Teilweise gibt es keine Option „Software Controlled“ und bei einigen Oberflächen überhaupt keine Möglichkeiten zur Konfiguration. Die Änderung der Treiberkonfiguration ist nur mit administrativen Berechtigungen möglich. Ebenfalls sollten Änderungen der Firmware auch nur durch berechtigte Personen möglich sein (siehe Anforderung [SYS.2.1.A8 Absicherung des Bootvorgangs](#)).

### **SYS.2.1.A14 Updates und Patches für Firmware, Betriebssystem und Anwendungen (S)**

Für Updates und Patches von Firmware, Betriebssystem und Anwendungen muss entschieden werden, wie diese innerhalb der IT-Infrastruktur bereitgestellt und installiert werden. Vor dem Einspielen sollten diese in einer Referenzumgebung getestet werden. In größeren Infrastrukturen mit mehreren Windows 10 Clients kann es vorteilhaft sein, Softwareverteilungssystem einzusetzen, die Anwendungen, Treiber und Betriebssysteme zentral bereitstellen und installieren.

## SYS.2.1.A15 Sichere Installation und Konfiguration von Clients (S)

Bei einer manuellen Installation von Windows 10 sollten folgende Aspekte beachtet werden:

- Es ist empfehlenswert, den Client während der Installationsroutine noch nicht mit dem Internet zu verbinden. Hierdurch lässt sich vermeiden, dass ein Microsoft-Konto eingerichtet oder mit dem Client zwingend verbunden wird.
- Das bei der Installation durch den Benutzenden eingerichtete Konto wird voreingestellt Mitglied der lokalen Gruppe „Administrators“, sodass dieses Konto vielmehr ein Konto zur Verwaltung des Clients ist. Im Anschluss an die Installation sollte daher mit Hilfe dieses Kontos ein weiteres Konto für die regelmäßige Benutzung angelegt werden, welches dann der lokalen Gruppe: „Users“ ausschließlich zugeordnet wird.
- Nach der Installation von Windows 10 bzw. bei vorinstallierten Systemen, können bereits nachfolgende Funktionen über die Out-Of-Box-Experience (OOBE) deaktiviert werden (die Einstellungen gelten nur für das initial erstellte Konto):
  - Das bei OOBE minimal auswählbare Telemetrielevel ist „Basic“. Um das geringere Telemetrielevel „Security“ einzustellen, ist eine Gruppenrichtlinie anzupassen (siehe [SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen unter Windows 10](#))
  - Aktivitätsverlauf
  - Verknüpfung von Smartphone und Windows 10
  - Nutzung von OneDrive („Dateien nur auf diesem PC speichern“)
  - Nutzung der digitalen Assistentin „Cortana“
  - Cloudbasierte Online-Sprachsteuerung
  - Verwenden des Standorts durch Microsoft und Apps
  - „Find-my-Device“ (Gerätesuche bei Verlust)
  - Verbesserung von Freihand und Eingabe
  - Tipps, Anzeigen und Empfehlungen
  - Nutzung der Werbe-ID durch Apps

Einzelne Konfigurationen können bei einer Neuinstallation des Systems auch mit in das Installationsmedium aufgenommen werden<sup>44,45</sup>. Darüber hinaus können die Konfigurationen zentral verwaltet werden (siehe [SYS.2.1.A44 Verwaltung der Sicherheitsrichtlinien von Clients](#)).

### Automatische Suche und Installation von Treibern

In Windows 10 werden passende Gerätetreiber in der Voreinstellung zweiphasig ausgewählt<sup>46</sup>. In der ersten Phase installiert Windows 10 den am besten geeigneten Treiber aus dem sog. „Driver Store“<sup>47</sup>, der eine vom Betriebssystem verwaltete Sammlung vertrauenswürdiger mitgelieferter und Drittanbieter-Treiberpakete darstellt. Hierdurch soll das Gerät zunächst schnell einsatzbereit gemacht werden. Anschließend wird in der

<sup>44</sup> <https://learn.microsoft.com/de-de/windows-hardware/manufacture/desktop/sysprep--system-preparation--overview>

<sup>45</sup> <https://learn.microsoft.com/de-de/windows-hardware/manufacture/desktop/sysprep--generalize--a-windows-installation>

<sup>46</sup> <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/how-windows-selects-a-driver-for-a-device>

<sup>47</sup> <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/driver-store>

zweiten Phase über Windows Update nach passenden Treiberpaketen für das Gerät gesucht, heruntergeladen und in den Driver Store abgelegt. Mit Windows 10 Version 20H1 wird durch Windows 10 automatisch der am besten passende Treiber zur Installation angeboten.



Computer Configuration/Administrative Templates/System/Device Installation

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Prevent device metadata retrieval from the internet	<b>Enabled</b>	Um zu verhindern, dass Gerätemetadaten für angeschlossene und installierte Geräte aus dem Internet regelmäßig durch Windows heruntergeladen werden, sollte die Richtlinie deaktiviert werden. Durch die Funktion könnten möglicherweise sensible Informationen über die Gerätekonfiguration abfließen.
Specify search order for device driver source locations	<b>Enabled</b>  <b>Options:</b> Specify search order for device driver source locations: <ul style="list-style-type: none"> <li>Do not search Windows Update</li> </ul>	Mit aktivierter Einstellung kann bestimmt werden, ob nach Gerätetreibern über Windows Update immer gesucht wird oder nur, wenn ein Treiber lokal nicht auf dem System zur Verfügung steht. Um die Suche nach Treibern über Windows Update vollständig zu unterbinden, sollte die Einstellung „Do not search Windows Update“ ausgewählt werden.

Laut Angaben von Microsoft werden zum Abruf der Metainformationen zu Gerätetreibern der nachfolgende Verbindungsendpunkt kontaktiert:

Tabelle 7: Verbindungskommunikationsendpunkt für den Abruf von Treibermetainformationen

Verbindungsendpunkt	Protokoll
dmd.metaservices.microsoft.com	HTTP

### Installation von Windows Apps durch Konten ohne administrative Berechtigung



Computer Configuration/Administrative Templates/System/Group Policy

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Prevent non-admin users from installing packaged Windows apps	<b>Disabled</b>	Softwareinstallationen sollten nur durch Konten mit administrativen Berechtigungen vorgenommen werden dürfen. Um zu verhindern, dass Konten ohne administrative Berechtigung eigenständig Windows Apps installieren können, sollte die Richtlinieneinstellung deaktiviert werden.

### Verarbeitung der Gruppenrichtlinie



Computer Configuration/Administrative Templates/System/Group Policy

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Configure registry policy processing	<b>Enabled</b>  <b>Options:</b> Configure registry policy processing	Die Richtlinieneinstellung legt fest, dass Gruppenrichtlinienobjekte auch verarbeitet werden, wenn sich keine Änderungen an den Richtlinien vorgenommen wurden. Die regelmäßige Aktualisierung

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
	<ul style="list-style-type: none"> <li>„Process even if the Group Policy objects have not changed“</li> </ul>	und Verarbeitung von Gruppenrichtlinien im Hintergrund beansprucht häufiger Rechenleistung auf dem Client, als wenn diese nur nach Anmeldung bzw. Neustart durchgeführt wird. Dies kann sich auf die Leistung des Clients auswirken.
Configure security policy processing	<b>Enabled</b>  <b>Options:</b> Configure security policy processing: <ul style="list-style-type: none"> <li>„Process even if the Group Policy objects have not changed“</li> </ul>	Bei Nicht-Konfiguration der Richtlinieneinstellung werden Gruppenrichtlinien, die keine Änderungen zur IST-Konfiguration beinhalten, nicht erneut auf dem Client verarbeitet. Die Empfehlung zur Richtlinieneinstellung legt fest, dass eine Verarbeitung der Gruppenrichtlinie auch ohne Änderungen der Gruppenrichtlinienobjekte vorgenommen wird.
Continue experiences on this device	<b>Disabled</b>	Sofern die Gruppenrichtlinieneinstellung nicht explizit konfiguriert wurde, ist das Standardverhalten von der eingesetzten Windows Edition abhängig und Benutzende können eigenständig entscheiden, ob diese Funktion aktiviert oder deaktiviert wird. Daher sollte die Einstellung durch Konfiguration der Richtlinieneinstellung vorgegeben werden.
Turn off background refresh of Group Policy	<b>Disabled</b>	Im vordefinierten Verhalten werden Hintergrundaktualisierungen der Gruppenrichtlinie in einem Abstand zwischen 90 und 120 Minuten durchgeführt. Durch die Deaktivierung der Richtlinieneinstellung wird verhindert, dass Aktualisierungen der Gruppenrichtlinie auch dann durchgeführt werden, wenn Benutzende den Client verwenden.



Computer Configuration/Administrative Templates/Windows Components/OOBE

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Don't launch privacy settings experience on user logon	<b>Enabled</b>	Durch die Einstellung wird bei erstmaliger interaktiver Anmeldung eines neuen Kontos keine Oberfläche zur Einstellung der Datenschutzoptionen angezeigt. Da der Endnutzende in vielen Fällen keine informierte Entscheidung treffen kann, sollten die Datenschutzeinstellungen durch die Organisation vorgegeben werden.

## SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen (S)

Wie in den Umsetzungshinweisen zum IT-Grundschutz-Baustein SYS.2.1 Allgemeiner Client in der Maßnahme SYS.2.1.M16 erläutert wird, wird im Rahmen der Standardinstallation eines Betriebssystems, wie Windows 10, eine größere Anzahl von Kennungen, Programmen, Diensten und sonstigen Komponenten eingerichtet, die für den Betrieb nicht in jedem Fall notwendig sind. Im Rahmen der Grundkonfiguration sollte daher geprüft werden, welche dieser Komponenten tatsächlich für den Betrieb benötigt werden.

### Advertising ID



Computer Configuration/Administrative Templates/System/User Profiles

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off the advertising ID	<b>Enabled</b>	Für zielgerichtete Werbung in Apps wird in Windows 10 eine sog. „Advertising ID“ vergeben, die eine eindeutige Identifizierung ermöglichen soll.

### Automatisches Ausführen und Wiedergabe von Medien und Anwendungen (Autoplay/Autorun)

Schadsoftware kann durch Wechseldatenträger übertragen werden und über diesen Weg auch auf Systeme gelangen, die netztechnisch gesondert geschützt oder abgeschottet werden. Um das Risiko einer automatischen Ausführung potenzieller Software zu verhindern, die sich auf angeschlossenen Wechseldatenträgern befinden kann, sollte das automatische Abspielen (Autoplay) deaktiviert werden<sup>48,49,50</sup>.



Computer Configuration/Administrative Templates/Windows Components/AutoPlay Policies

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Disallow Autoplay for non-volume devices	<b>Enabled</b>	Das automatische Abspielen von Medien aus MTP-Geräten, wie z. B. Kameras oder Mobiltelefonen, birgt das Risiko, dass Inhalte ohne Bestätigung automatisch ausgeführt werden und sollte daher deaktiviert werden.
Set the default behavior for Autorun	<b>Enabled</b> <b>Options:</b> Set the default behavior for Autorun: <ul style="list-style-type: none"> <li>Do not execute any autorun commands</li> </ul>	Das automatische Ausführen von Autorun-Befehlen, welche typischerweise in der auf Datenträgern und Medien abgelegten Datei „autorun.inf“ hinterlegt werden können, sollte deaktiviert werden, um zu verhindern, dass Inhalte ohne Interaktion des Benutzenden ausgeführt werden können.
Turn off Autoplay	<b>Enabled</b> <b>Options:</b> Turn off Autoplay: <ul style="list-style-type: none"> <li>All drives</li> </ul>	Das automatische Abspielen von Inhalten von angeschlossenen Geräten führt dazu, dass eine Ausführung automatisch stattfindet. Hieraus ergibt sich ein Risiko, dass

<sup>48</sup> MITRE ATT&CK Technique T1092 (Communication Through Removable Media)

<https://attack.mitre.org/techniques/T1091/>

<sup>49</sup> MITRE ATT&CK Technique T1091 (Replication Through Removable Media)

<https://attack.mitre.org/techniques/T1092/>

<sup>50</sup> MITRE ATT&CK Technique T1052 (Exfiltration Over Physical Medium)

<https://attack.mitre.org/techniques/T1052/>

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		durch die Deaktivierung des Autoplays entgegengewirkt wird.

### **Automatischer Start von Anwendungen nach interaktiver Kontenanmeldung (Autostart)**

Mögliche Angreiferinnen und Angreifer sowie Schadsoftware verschaffen sich häufig Persistenz in Systemen, indem in betroffenen Systemen die Einträge des Autostarts geändert oder hinzugefügt werden. Hierdurch soll sichergestellt werden, dass eine schädliche Software auch nach einem Neustart des Systems oder einer erneuten interaktiven Kontenanmeldung wieder ausgeführt wird. Werden über den Autostart ausführbare Dateien privilegiert ausgeführt, ist auch eine Ausweitung der Rechte möglich.

Mit der Technique T1547 („Boot or Logon Autostart Execution“) in der MITRE ATT&CK Enterprise Matrix wird darauf aufmerksam gemacht, dass eine präventive Gegenmaßnahme aufwendig ist<sup>51</sup>. Die Autostart-Funktion ist eine Betriebssystemfunktion in Windows 10, die sich nicht deaktivieren lässt. Daher ist ein regelmäßiges Monitoring auf mögliche Manipulationen der Autostart-Einträge unerlässlich. Legitime Änderungen durch Softwareinstallation oder -updates sollten entsprechend dokumentiert werden und mit den vorliegenden Zuständen auf den Zielsystemen abgeglichen werden.

Im Gegensatz zu den Richtlinieneinstellungen für das Autorun-Verhalten beim Anschluss von Wechselmedien und Datenträgern gibt es über die Gruppenrichtlinie keine Einstellungen für das Verhalten zur automatischen Ausführung von Anwendungen nach einer interaktiven Kontenanmeldung.

Sofern bei der Installation ein automatischer Programmstart (Autorun) nicht konfiguriert werden kann, sollte nach der Installation von Anwendungen geprüft werden, ob diese einen Eintrag in die Liste der Autostart-Anwendungen angelegt hat.

Auf einem Referenzsystem lässt sich über die grafische Bedienoberfläche im Reiter „Autostart“ des Task-Managers für das jeweilige Konto überprüfen, ob und welche Anwendungen automatisch nach Kontenanmeldung gestartet werden.

In der Windows-Registry lassen sich die zugehörigen Einträge in nachfolgenden Schlüsselpfaden einsehen bzw. auflisten<sup>52,53</sup>:

- ❏ HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
- ❏ HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- ❏ HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- ❏ HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx (werkseitig nicht vorhanden)

Um das Autostart-Verhalten in domänenverwalteten Umgebungen über die Gruppenrichtlinie einheitlich festzulegen, empfiehlt sich eine Konfiguration der Registry, z. B. über die Group Policy Preferences, durch Änderung der Schlüsselwerte (Löschen zum Deaktivieren von Anwendungen).

Zusätzlich zur Windows-Registry sollten ebenfalls die Verzeichnisse „Startup“ überprüft werden:

<sup>51</sup> MITRE ATT&CK Technique T1547 („Boot or Logon Autostart Execution“)

<https://attack.mitre.org/techniques/T1547/001/>

<sup>52</sup> <https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1060-registry-run-keys-startup-folder>

<sup>53</sup> <https://learn.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys>

- **Konten-spezifisches Verzeichnis:**

„C:\Users\{Anmeldename des Kontos}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\  
(Das angemeldete Konto und die Konten in der Gruppe „Administrators“ haben Schreibrechte).

- **Konten-übergreifendes Verzeichnis:**

„C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Autostart“  
(Konten in der Gruppe „Users“ haben nur Leseberechtigung).

**Hinweis:** Die genannten Pfade können durch mögliche Angreiferinnen und Angreifer über die Windows-Registry manipuliert werden, sodass die Startup-Verzeichnisse auf einen anderen Ort verweisen. Die Pfade der Startup-Verzeichnisse sind in der Windows-Registry hinterlegt:

- ☛ HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- ☛ HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- ☛ HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- ☛ HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

In der Voreinstellung befinden sich im Autostart bereits Einträge zu Cortana, OneDrive, Skype und den Windows Security Notifications. Sofern bei der Installation eine Nutzung von Cortana und OneDrive abgelehnt wurde, sind die zugehörigen Einträge bereits deaktiviert.

### Aufgabenplanung (Geplante Tasks/Task Scheduler)

Durch die Aufgabenplanung (Task Scheduler) in Windows 10 lassen sich geplante Aufgaben („Scheduled Tasks“) anlegen und verwalten, die zu einem bestimmten Zeitpunkt oder Ereignis eine festgelegte Aktion, wie bspw. die Ausführung eines Programms oder Skripts, mit den Rechten verschiedener Konten auslösen. Mögliche Angreiferinnen und Angreifer können diese Betriebssystemfunktionalität dazu missbrauchen, um sich Persistenz zu verschaffen, eine Privilegienerweiterung herbeizuführen oder beliebigen Programm- und Skriptcode auszuführen<sup>54</sup>. Aus diesem Grund sollten die in Windows 10 bereits vorhandenen geplanten Aufgaben in der Aufgabenverwaltung hinsichtlich ihrer betrieblichen Notwendigkeit überprüft und ggfs. deaktiviert werden. Nach Softwareinstallation und Updates sollte die Aufgabenplanung hinsichtlich geänderter oder hinzugefügter Einträge kontrolliert und mit dem dokumentierten Ausgangszustand abgeglichen werden. Zugehörige Ereignisse können hierüber auch im Event Log protokolliert worden sein<sup>55</sup>.

### Konten

Die in Windows 10 bereits vorhandenen und vordefinierten Konten sollten in der „Computerverwaltung“ hinsichtlich ihrer Rechte und Gruppenmitgliedschaften überprüft werden:

- **„Computer Management“**  
Computer Management („compmgmt.msc“) → System Tools → Local Users and Groups → Users
- PowerShell

- PS C:\> Get-LocalUser

Nachfolgend genannte Konten sollten wie folgt behandelt werden:

<sup>54</sup> MITRE ATT&CK Technique T1053 (Scheduled Task/Job): <https://attack.mitre.org/techniques/T1053/>

<sup>55</sup> <https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-other-object-access-events>



Tabelle 8: Übersicht der Konten in Windows 10

<b>Kontoname</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Administrator	<b>Disabled</b> (Zusätzlich sollte der Kontenname individuell umbenannt werden.)	Vordefiniertes Konto für die lokale Administration, welches voreingestellt deaktiviert ist. Das Konto kann nicht gelöscht oder gesperrt werden.
DefaultAccount	<b>Disabled</b>	Es handelt sich um ein vordefiniertes Dienstkonto, das in Windows 10 nicht verwendet wird. Das Konto wird beispielsweise in der Xbox verwendet. Voreingestellt ist das Konto deaktiviert und sollte auch nicht aktiviert werden.
Guest	<b>Disabled</b> (Zusätzlich sollte der Kontenname individuell umbenannt werden.)	Das „Gastkonto“ ist in der Voreinstellung deaktiviert und verfügt über ein leeres Kennwort. Über das „Gastkonto“ kann ein anonymer Zugriff erfolgen, der ein Sicherheitsrisiko darstellen kann.
WDAGUtilityAccount	<b>Disabled</b>	Das Konto ist Teil des Microsoft Defender Application Guard (WDAG) und wird automatisch aktiviert, sobald WDAG aktiviert wird. Sofern WDAG nicht verwendet wird, sollte das Konto deaktiviert werden.

## Gruppen

Die Mitgliedschaften der Gruppen sollten überprüft und hierdurch sollte sichergestellt werden, dass Konten nur über die erforderlichen Berechtigungen verfügen. Built-In Gruppen können nicht deaktiviert oder entfernt werden.

- „Computer Management“  
Computer Management (compmgmt.msc) → System Tools → Local Users and Groups → Groups
- PowerShell

```
PS C:\> Get-LocalGroup
```

Tabelle 9: Übersicht der Gruppen in Windows 10

<b>Gruppenanzeigename</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Access Control Assistance Operators	Es sollten keine Konten von Benutzenden der Gruppe zugordnet werden.	Mitglieder der Gruppe dürfen Remoteabfragen zu Attributen und Rechten für Ressourcen auf dem Client abfragen.
Administrators	Die in der Gruppe enthaltenen Mitglieder sollten überprüft werden. Es sollte sichergestellt sein, dass nur solche Mitglieder enthalten sind, die Administrationsrechte zwingend benötigen. Benutzende sollten nicht über administrative Rechte verfügen. Zur Administration des Clients sollte	Vorkonfigurierte lokale Gruppe der „Administrators“. Es handelt sich um eine Built-In Gruppe.

<b>Gruppenanzeigename</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
	ein dediziertes administratives Konto vorgesehen werden. Hinweis: In der Voreinstellung wird das bei Installation angelegte Konto automatisch Mitglied der Gruppe „Administrators“.	
Backup Operators	Vordefiniert enthält die Gruppe keine Mitglieder. Maximal sollten der Gruppen dedizierte Konten für die Datensicherung zugeordnet werden. Benutzende sollten nicht in die Gruppe der Sicherungsoperatoren aufgenommen werden.	Mitglieder dieser Gruppe verfügen über weitreichende Zugriffsrechte auf Dateien und Verzeichnisse. Außerdem dürfen sie Datensicherungen und Wiederherstellungen durchführen. Damit sind Mitglieder dieser Gruppe indirekt in der Lage beliebige Systemveränderungen durchzuführen, die sonst nur mit Systemrechten möglich sind.
Cryptographic Operators	Vordefiniert enthält die Gruppe keine Mitglieder. Falls die Rolle des „Crypto Officers“ gemäß FIPS-140-2 nicht benötigt wird, sollte diese Gruppe leer bleiben.	Mitglieder dieser Gruppe sind für die Konfiguration von IPSec zuständig („Crypto Officer“), um FIPS-konform zu bleiben <sup>56</sup> .
Device Owners	Vordefiniert enthält die Gruppe keine Mitglieder. Es sollten keine Mitglieder der Gruppe hinzugefügt werden.	Mitglieder dieser Gruppe dürfen beispielsweise auf den Client über das Netz zugreifen oder die lokale Zeitzone ändern. Die Gruppe wird für besonders eingeschränkte Nutzungsszenarien von Windows, beispielsweise „HoloLens“ <sup>57</sup> .
Distributed COM Users	Vordefiniert enthält die Gruppe keine Mitglieder. Sofern kein konkreter Anwendungsfall vorliegt, sollten keine Mitglieder der Gruppe hinzugefügt werden.	Mitglieder der Gruppe dürfen verteilte COM-Objekte aktivieren, ausführen und verwenden <sup>58</sup> . DCOM wird vorrangig im Serverbereich eingesetzt. Risiken entstehen durch einen entfernten Zugriff auf COM-Objekte <sup>59</sup> .
Event Log Readers	Vordefiniert dürfen Konten die über eine Mitgliedschaft in der Gruppe „Users“ verfügen, bereits die Windows-Protokolle Anwendung, Installation und System lesen. Sofern kein konkreter Anwendungsfall	Mitglieder der Gruppe dürfen die ausgezeichneten Events des lokalen Clients in der Ereignisanzeige auslesen. Diese Built-In-Gruppe wird beispielsweise dazu verwendet, um eine Weiterleitung von

<sup>56</sup> <https://web.archive.org/web/20130203064043/http://blogs.technet.com/b/lrobbins/archive/2011/06/23/quot-admin-free-quot-active-directory-and-windows-part-1-understanding-privileged-groups-in-ad.aspx>

<sup>57</sup> <https://learn.microsoft.com/en-us/hololens/security-adminless-os>

<sup>58</sup> <https://learn.microsoft.com/en-us/windows/win32/com/dcom-security-enhancements-in-windows-xp-service-pack-2-and-windows-server-2003-service-pack-1>

<sup>59</sup> <https://attack.mitre.org/techniques/T1021/003/>

<b>Gruppenanzeigename</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
	vorliegt, sollten keine Mitglieder der Gruppe hinzugefügt werden.	Ereignissen („Windows Event Forwarding“) zu konfigurieren <sup>60</sup> .
Guests	Vordefiniert enthält die Gruppe nur das bereits deaktivierte Gastkonto („Guest“). Es sollten keine Konten aufgenommen werden.	Durch Konten, die über eine Mitgliedschaft in der „Guests“-Gruppe verfügen, kann ein anonymer Zugriff erfolgen, der ein Sicherheitsrisiko darstellen kann.
Hyper-V Administrators	Nur bei der Nutzung von Hyper-V wird diese Gruppe benötigt. In die Gruppe sollten nur solche Konten aufgenommen werden, die Hyper-V verwalten. Diese Möglichkeit sollte vorrangig zur Verwaltung von Hyper-V genutzt werden, anstatt die Hyper-V Nutzenden in die Gruppe „Administrators“ aufzunehmen.	Die Gruppe kann im Rahmen der Verwaltung von Hyper-V genutzt werden. Hyper-V ist eine zusätzliche Funktion, die nachinstalliert werden kann.
IIS_IUSRS	Ein Betrieb der sog. „Internet Information Service (IIS)“ – Dienste auf dem Client ist wie ein Webserver zu behandeln. Hierzu ist der IT-Grundschutz-Baustein „APP.3.2 Webserver“ zusätzlich zu modellieren. Microsoft liefert zu den Identitäten und Berechtigungen umfangreiche Informationen <sup>61,62</sup> .	Die Gruppe wird durch den Internet Information Service (IIS) genutzt, der nachinstalliert werden muss.
Network Configuration Operators	Sofern Benutzende die Änderungen der Netzkonfiguration selbst vornehmen sollen dürfen, sollten die zugehörigen Konten in die Gruppe der Network Configuration Operators aufgenommen werden, anstatt sie zu Administrierenden zu machen.	Durch Aufnahme eines Kontos in die Gruppe können Berechtigungen zur Konfiguration der Netzchnittstellen delegiert werden <sup>63</sup> .
Performance Log Users	Es sollten keine Konten von Benutzenden der Gruppe zugeordnet werden.	Die Mitglieder dieser Gruppe können leistungsbezogene Logdateien und Alarmer auf Domänencontroller der Domäne

<sup>60</sup> <https://learn.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection>

<sup>61</sup> <https://learn.microsoft.com/de-de/troubleshoot/iis/understanding-identities>

<sup>62</sup> <https://learn.microsoft.com/de-de/troubleshoot/iis/default-permissions-user-rights>

<sup>63</sup> [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754921\(v=ws.10\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754921(v=ws.10))

<b>Gruppenanzeigename</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		verwalten, ohne Mitglied der „Administrationsgruppe“ zu sein.
Performance Monitor Users	Es sollten keine Konten von Benutzenden der Gruppe zugeordnet werden.	Die Mitglieder dieser Gruppe können ein Leistungsmonitoring auf Domänencontroller durchführen, ohne Mitglied der „Administrators-“ oder „Performance Log“ Gruppe zu sein.
Power Users	Die Gruppe ist wahrscheinlich aus Kompatibilitätsgründen noch in Windows 10 enthalten und beinhaltet keine Mitglieder. Es sind keine Anwendungsfälle bekannt, in denen Benutzende der Gruppe hinzugefügt werden sollten.	Es handelt sich eine Gruppe, die in vorherigen Windows-Versionen teilweise erhöhte Rechte bereitstellte. Seit Windows Vista wurden diese erhöhten Rechte der Gruppe entzogen und sie verfügt über vergleichbare Rechte mit der Gruppe „Users“.
Remote Desktop Users	In der Gruppe der „Remote Desktop Users“ sollten nur die Konten und Gruppen enthalten sein, die einen Remotezugriff auf den Client benötigen.	In der Gruppe aufgenommene Mitglieder dürfen sich über Remote Desktop auf das IT-System verbinden. Zusätzlich muss Remote Desktop aktiviert sein (Standard: Deaktiviert). Weitere Informationen hierzu sind in den Empfehlungen zur Anforderung <a href="#">SYS.2.2.3.A19 Sicherheit beim Fernzugriff über RDP</a> zu entnehmen.
Remote Management Users	In der Gruppe der „Remote Management Users“ sollten nur die Konten und Gruppen enthalten sein, die einen Remotezugriff über das Windows Remote Management auf den Client benötigen.	Mitglieder der Gruppe können auf WMI-Ressourcen über Managementprotokolle wie das WS-Management über das Windows Remote Management zugreifen
Replicator	Entsprechend den Empfehlungen von Microsoft sollten keine Mitglieder der Gruppe hinzugefügt werden.	Die Gruppe wird vom File Replication Service auf dem Domänencontroller verwendet und ist in Windows 10 nicht relevant.
System Managed Accounts Group	Es sollten keine Konten der Gruppe zugordnet werden.	Die Mitglieder dieser Gruppe werden durch das System verwaltet.
Users	In der Gruppe „Users“ sollten alle Konten aufgenommen werden, die für die regelmäßige Nutzung des Systems vorgesehen sind.	Microsoft bezeichnet die Konten in dieser Gruppe auch als „Standardbenutzer“. Nach Installation des Betriebssystems sind lediglich die Gruppen „NT-AUTHORITY\Authenticated Users“ sowie „NT-AUTHORITY\INTERACTIVE“ Mitglieder der Gruppe. Hierbei handelt es sich um System-interne Gruppen, die für Ressourcenzugriffe benötigt werden <sup>64</sup> .

<sup>64</sup> <https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/special-identities>

## Auswertung von zugeordneten Rechten und Privilegien von Konten (User Rights Assignment)

Um die tatsächlich zugeordneten Rechte und Privilegien von Konten auszuwerten, bietet sich ein Export mittels des in Windows 10 mitausgelieferten Werkzeugs „secedit“ in die Datei „Ausgabe.txt“ an:

### Command Line (CMD) mit administrativen Rechten:

```
C:\> secedit /export /areas USER_RIGHTS /cfg Ausgabe.txt
```

**Hinweis:** Es werden nur Einträge gelistet, für die auch eine Zuordnung von Privilegien und Rechten besteht. Die zugehörigen Bezeichner werden nur teilweise aufgelöst, weshalb eine manuelle Zuordnung zu den SIDs vorgenommen werden muss. Eine Übersicht u. a. zu den sog. „Well-Known SIDs“ werden in der Dokumentation zum Betriebssystem bereitgestellt<sup>65</sup>.

## Debugrechte

 Computer Configuration/Windows Settings/Security Settings Local Policies/User Rights Assignment

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Debug programs	<b>Enabled</b>  <b>Anmerkung:</b> Die in der Gruppenrichtlinie aufgeführte Liste der Konten und Gruppen sollte leer sein.	Das Debug-Privileg wird voreingestellt. Konten von Administrierenden zugewiesen. Debugrechte werden in der Regel nur für Entwicklungstätigkeiten benötigt, die native Anwendungen im Speicher nachverfolgen müssen. Mit Debug-Privilegien können beispielsweise potenziell sensible Informationen aus dem Arbeitsspeicher ausgelesen werden. Dieses wird durch Programme wie bspw. „Mimikatz“ genutzt. Mit diesem Privileg wird der Zugriff auf jeden Prozess oder Thread unabhängig von den Security-Deskriptoren erlaubt. Dies trifft nicht auf geschützte Prozesse (engl.: <i>Protected Processes</i> ) zu.

## Game Recording und Broadcasting-Funktionen

 Computer Configuration/Windows Components/Windows Game Recording and Broadcasting

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Enables or disables Windows Game Recording and Broadcasting	<b>Disabled</b>	Mit der Game Recording und Broadcast-Funktion können Benutzende den Bildschirminhalt aufzeichnen und Live-Sitzungen in das Internet übertragen. Um zu verhindern, dass Benutzende oder Malware möglicherweise sensible Informationen an unberechtigte Dritte übertragen, sollte die Funktion deaktiviert werden.

<sup>65</sup> <https://learn.microsoft.com/en-us/windows/security/identity-protection/access-control/security-identifiers>

## Lokalisierungsinformationen

 Computer Configuration/Windows Settings/Security Settings Local Policies/User Rights Assignment

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off location	Enabled	Um zu verhindern, dass Standortinformationen von Programmen verwendet werden, sollte die Richtlinie konfiguriert werden.

## Windows-Dienste

(System-)Dienste sind Programme, die Windows 10 im Hintergrund und in der Regel mit privilegierten Rechten ausführt. Aus Sicht von möglichen Angreifenden stellen Windows-Dienste eine gängige Praxis dar, um sich Persistenz oder erhöhte Rechte in einem System zu verschaffen<sup>66</sup>. Die bereits nach Betriebssysteminstallation vorhandenen (System-)Dienste, aber auch die durch Softwareinstallationen und Updates hinzugefügten Dienste in Windows 10 sollten daher regelmäßig gesichtet und hinsichtlich ihrer betrieblichen Notwendigkeit geprüft werden. Nicht für den Betrieb erforderliche Dienste sollten deaktiviert oder deaktiviert werden. Außerdem sollten die Rechte für die Erstellung und Modifikation von Diensten auf ausschließlich administrative Konten beschränkt werden. Eine Übersicht der installierten und ausgeführten Dienste sowie ihrer zugehörigen Startmodi lässt sich im „Computer Management“ entnehmen:

- „Computer Management“  
Computer Management (compmgmt.msc) → System Tools → Services and Applications → Services

Alternativ kann eine Liste der Dienst auch über die Windows PowerShell ermittelt werden:

- PowerShell

```
PS C:\> Get-Service
```

Ob und zu welchem Zeitpunkt (während des Bootens/nach dem Booten/bei Bedarf) ein Dienst gestartet wird, wird durch den sog. „Startup-Typ“ festgelegt:

## Startup-Types

Tabelle 10: Starttypen der Windows-Dienste

Typ	Erläuterung
Automatisch („Automatic“)	Der Dienst wird während des Bootvorgangs gestartet.
Automatisch (Verzögerter Start) („Automatic – Delayed Start“)	Der Dienst wird im Anschluss an den Bootvorgang gestartet.
Manuell („Manual“)	Der betroffene Dienst kann manuell durch Benutzende- oder automatisch durch Systeminteraktion (z. B. Abhängigkeit eines/r anderen Dienstes/Anwendung) bei Bedarf gestartet werden.
Deaktiviert („Disabled“)	Der jeweilige Dienst ist deaktiviert und kann nicht mehr gestartet werden.

Die in Windows 10 vorinstallierten und ggfs. ausgeführten Dienste sollten in der „Computerverwaltung“ hinsichtlich ihrer Notwendigkeit für den Betrieb überprüft werden. Dazu ist es ratsam, die Liste der installierten Dienste inkl. der zugehörigen Beschreibung auf einer Referenzinstallation zu exportieren:

- **Dienste (MMC)**
  1. Action → Export

<sup>66</sup> MITRE ATT&CK Technique T1543 (Create or Modify System Process)  
<https://attack.mitre.org/techniques/T1543/>

2. Auswahl eines Dateityps (.txt oder .csv) und Speichern der Liste (Tipp: Da die Beschreibungstexte Kommata enthalten, sind Tabulatoren getrennte Listen möglicherweise besser für eine Weiterverarbeitung geeignet: Unicode Text → Tab Delimited).
3. Mit Tabellenkalkulationssoftware o. ä. lässt sich die Übersicht der Dienste sortieren und um individuelle Spalten, z. B. zur Kommentierung ergänzen.

- PowerShell (PS)

```
PS C:\> Get-Service | Export-Csv -path "C:\services.csv"
```

- Command Line (CMD)

```
C:\> sc query state=all > services.txt
```

- Windows Management Instrumentation (WMI)

```
PS C:\> Get-WmiObject win32_service | select Name, DisplayName, State, PathName | Export-Csv -path "C:\services.csv"
```

Die Liste der Dienste sollte nach entsprechender Durchsicht und Kommentierung hinsichtlich der Notwendigkeit der Dienste der Dokumentation hinzugefügt werden. Nach Neuinstallationen von Software oder Veränderungen durch (Betriebssystem-)Updates sollten Veränderungen an den Diensten geprüft werden. In der Regel werden Windows Updates monatlich am zweiten Dienstag eines Monats, dem sog. „Patch Tuesday“ veröffentlicht. Außer der regulären Veröffentlichung können Updates oder Patches aber auch unregelmäßig als sog. „Out-of-Band-Release“ bereitgestellt werden.

Die nachfolgende Liste einer Auswahl der vorhandenen Systemdienste soll helfen, eine Einschätzung zu Diensten zu geben, die, wenn sie nicht benötigt werden, abgeschaltet werden können. Die Tabelle orientiert sich dabei am Nutzungsszenario eines verwalteten Bürokommunikationsclients.



Computer Configuration/Windows Settings/Security Settings/System Services

Dienst	Empfehlung für den „StartupType“	Erläuterung
Application Layer Gateway Service	<b>Disabled</b>	Der Dienst wird u. a. für das Teilen einer Internetverbindung (Internet Connection Sharing) durch Drittanbieterwerkzeuge benötigt.
AllJoyn Router Service (AJRouter)	<b>Disabled</b>	Der AllJoyn-Dienst kann u. a. zur Vernetzung bspw. mit IoT-Geräten verwendet werden.
Background Intelligence Transfer Service (BITS)	<b>Disabled</b> (wenn die Windows Updates nicht direkt über Microsoft Update Server bzw. WSUS verteilt werden)	Der Dienst wird zur Übertragung von Dateien im Hintergrund verwendet und kann für das Nachladen schädlicher Inhalte missbraucht werden. Daher sollte der Dienst deaktiviert werden. Der Dienst wird u. a. benötigt, um Windows Updates von Microsoft Update Servern bzw. WSUS herunterzuladen. Wird der Dienst deaktiviert, können Windows Updates nicht mehr automatisch heruntergeladen werden. Um einer missbräuchlichen Verwendung des BITS durch einen möglichen

<i>Dienst</i>	<i>Empfehlung für den „StartupType“</i>	<i>Erläuterung</i>
		Angreifenden oder Malware, wie in der MITRE ATT&CK Technique T1197 „BITS Jobs“ beschrieben werden <sup>67</sup> , entgegen zu wirken, sollten ggfs. weitere Maßnahmen, wie eine Nutzungsbeschränkung auf bestimmte Konten/Gruppen oder netzseitige Begrenzung auf ausschließlich bekannte Endpunkte, erfolgen.
Bluetooth Audio Gateway Service (BTAGService)	<b>Disabled</b>	Diese Dienste werden u. a. zur Verbindung mit anderen Bluetooth-Geräten, wie bspw. Kopfhörern benötigt. Über die Bedienoberfläche kann die Nutzung der Bluetooth-Schnittstelle per Schaltfläche aktiviert oder deaktiviert werden.
Bluetooth Support Service (bthserv)	<b>Disabled</b>	Darüber hinaus kann auch die Deaktivierung einer nicht benötigten Bluetooth-Schnittstelle in vielen Fällen zusätzlich in der Firmware vorgenommen werden.
BranchCache	<b>Disabled</b>	Der BranchCache dient dazu, Windows Updates über ein Peer-to-Peer Protokoll zu verteilen.
Connected User Experiences and Telemetry (Startup Mode: Disabled)	<b>Disabled</b>	Der Windows-Dienst „Benutzererfahrung und Telemetrie im verbundenen Modus“ (Connected User Experiences and Telemetry Service), auch DiagTrack genannt, ist der zentrale Baustein der Windows Telemetrie-Komponente. Durch Deaktivierung des Dienstes „Benutzererfahrung“ und Telemetrie im verbundenen Modus, wird die Initiierung der DiagTrack-Listener Session verhindert, die einen Teil der Quellen für Telemetrie-Daten darstellt, sowie eine Übertragung der protokollierten Daten an das Telemetrie-Backend unterbunden. Siehe auch <a href="#">SYS.2.2.3.A25 Umgang mit Fernzugriffsfunktionen der „Connected User Experience and Telemetry“</a> .
Device Management Wireless Application Protocol (WAP) Push Message Routing Service	<b>Disabled</b>	Der Dienst wird für eine Verwaltung von Windows 10 mittels Mobile Device Management verwendet.

<sup>67</sup> MITRE ATT&CK Technique T1197 (BITS Jobs) <https://attack.mitre.org/techniques/T1197/>



<b>Dienst</b>	<b>Empfehlung für den „StartupType“</b>	<b>Erläuterung</b>
Downloaded Maps Manager (MapsBroker)	<b>Disabled</b>	Der Dienst „MapsBroker“ wird u. a. gestartet, wenn Anwendungen auf heruntergeladene Karten zugreifen möchten. In der Grundkonfiguration greift keine Anwendung auf diesen Dienst zu.
Fax	<b>Disabled</b>	Der Dienst wird zum Senden und Empfangen von Fax benötigt.
Geolocation Service (lfsvc) (Startup Mode: Disabled)	<b>Disabled</b>	Der Dienst „lfsvc“ verfolgt den aktuellen Gerätestandort und kann Ereignisse auslösen, die bestimmten Standorten zugeordnet worden sind.
Internet Connection Sharing (ICS) (SharedAccess)	<b>Disabled</b>	Der Dienst „SharedAccess“ stellt Netzwerke, wie u. a. NAT, Namensauflösung oder Intrusion-Prevention-Dienste zur Verfügung. Es wird empfohlen, den Dienst zu deaktivieren, da der Client nicht als Router eingesetzt werden sollte, um bspw. mit weiteren IT-Systemen einen Internetanschluss zu teilen. Zusätzlich widerspricht dies der Anforderung <a href="#">SYS.2.1.A23 Bevorzugung von Client-Server-Diensten</a> .
Link-Layer Topology Discovery Mapper (lltdsvc)	<b>Disabled</b>	Der Dienst „lltdsvc“ erstellt eine Übersicht über das Netz, der verbundenen PCs und Geräte sowie den zugehörigen Metainformationen, die bspw. im „Netzwerk- und Freigabecenter“ eingesehen werden können.
Microsoft iSCSI Initiator Service (MSiSCSI)	<b>Disabled</b>	In der Regel wird das iSCSI-Protokoll im Serverumfeld verwendet.
Microsoft Store Install Service (InstallService)	<b>Disabled</b>	Der Dienst ist Teil der Microsoft Store – Infrastruktur und wird für Store-App-Installationen benötigt. Sofern Installationen von Apps aus dem Microsoft Store nicht durchgeführt werden, sollte der Dienst deaktiviert werden.
Payments and NFC/SE Manager (SEMGrSvc)	<b>Disabled</b>	Der Dienst verwaltet die NFC-Schnittstelle.
Peer Name Resolution Protocol (PNRPsvc)	<b>Disabled</b>	Siehe auch <a href="#">SYS.2.1.A23 Bevorzugung von Client-Server-Diensten</a> . Die Dienste ermöglichen eine dezentrale Namensauflösung.
Peer Networking Grouping (p2psvc)	<b>Disabled</b>	
Peer Networking Identity Manager (p2pimsvc)	<b>Disabled</b>	
PNRP Machine Name Publication Service (PNRPAutoReg)	<b>Disabled</b>	
Printer Spooler	<b>Enabled</b>	Der Dienst ermöglicht die Nutzung von Druckern. Ist die Datei- und Druckerfreigabe eingeschaltet, ist der Dienst

<i>Dienst</i>	<i>Empfehlung für den „StartupType“</i>	<i>Erläuterung</i>
		auch von extern erreichbar, ohne dass ein Drucker auch freigegeben sein muss.
Problem Reports and Solutions Control Panel Support (wercplsupport)	<b>Disabled</b>	Der Dienst ist Teil der Windows Error Reporting Funktion, mit der Systemfehler an Microsoft berichtet werden können. Siehe auch Empfehlungen zum Internet Communication Management zu <a href="#">SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen</a> .
Remote Access Auto Connection Manager (RasAuto)	<b>Disabled</b>	Der Dienst verwaltet automatische RAS-Verbindungen und kann automatisch Verbindungen aufbauen, ohne dass eine „Benutzerinteraktion“ erforderlich ist.
Remote Access Connection Manager	<b>Disabled</b>	Der Dienst verwaltet Einwahlverbindungen und VPN-Verbindungen zu anderen IT-Systemen und Netzen.
Remote Desktop Configuration (SessionEnv)	<b>Disabled</b>	Sofern die Möglichkeit zum Fernzugriff auf den Client (RDP Server) nicht verwendet wird, sollte der Remote Desktop Konfigurationsdienst deaktiviert werden.
Remote Desktop Services (TermService)	<b>Disabled</b>	Sofern die Möglichkeit zum Fernzugriff auf den Client (RDP Server) und auf entfernte IT-Systeme (als RDP Client) nicht verwendet wird, sollte der Remote Desktop Konfigurationsdienst deaktiviert werden.
Remote Desktop Services UserMode Port Redirector (UmRdpService)	<b>Disabled</b>	Der Dienst ist für die Umleitung von angeschlossenen Geräten (Drucker, Laufwerke) am RDP Client zum RDP Server zuständig. Sollte die Funktionalität der Geräteumleitung nicht benötigt werden, sollte der Dienst abgeschaltet werden. Auswirkungen: Angeschlossene Geräte am RDP Client können nicht zum RDP Server umgeleitet werden.
Remote Procedure Call (RPC) Locator (RpcLocator)	<b>Disabled</b>	Der Dienst erfüllt in Windows 10 keine Funktion und wird lediglich zur Kompatibilität von (älteren) Anwendungen vorgehalten.
Remote Registry (RemoteRegistry)	<b>Disabled</b>	Der Dienst ermöglicht einen entfernten Zugriff auf die Registrierungsdatenbank des Clients. Verschiedene Management-Tools wie z. B. der System Center Configuration Manager als auch Schwachstellen-

<i>Dienst</i>	<i>Empfehlung für den „StartupType“</i>	<i>Erläuterung</i>
		Scanner sind auf diesen Dienst möglicherweise angewiesen.
Retail Demo Service	<b>Disabled</b>	Der Retail Demo Service wird für einen Demomodus von Windows 10 für den Einzelhandel benötigt.
Routing and Remote Access (RemoteAccess)	<b>Disabled</b>	Der Dienst stellt Routing-Funktionalitäten zur Verfügung, die eher im Serverumfeld angesiedelt sind.
Server (LanmanServer)	<b>Disabled</b> (Stand-alone Clients, nicht-domänenverwaltete Clients) oder <b>Enabled</b> (Domänenverwaltete Clients)	Der Dienst ermöglicht das Teilen von Dateien, Druckern, Named-Pipes über ein Netz. Dies bedeutet, dass Datei- und Druckerfreigaben von diesem Dienst abhängen, die u. a. von verschiedenen Management-Tools wie z. B. System Center Configuration Manager (SCCM) für Zugriffe auf den Client verwendet werden.
Smart Card	<b>Disabled</b>	Der Dienst wird für die Nutzung von Smart Cards benötigt.
Smart Card Device Enumeration Service	<b>Disabled</b>	Der Dienst stellt WinRT eine Schnittstelle zur Smart Card Nutzung zur Verfügung.
SNMP Trap (SNMPTRAP)	<b>Disabled</b>	Der Dienst empfängt SNMP-Benachrichtigungen und reicht diese weiter an ein SNMP-Management.
SSDP Discovery (SSDPSRV)	<b>Disabled</b>	Durch den Dienst werden Geräte und Dienste, die das SSDP Discovery Protokoll unterstützen (Universal Plug and Play, UPnP) automatisch im Netz gesucht und lokal angeschlossene Geräte veröffentlicht.
UPnP Device Host (upnphost)	<b>Disabled</b>	Der Dienst verwaltet Universal Plug and Play (UPnP) Geräte.
Windows Event Collector (Wecsvc)	<b>Disabled</b>	Der Dienst ist ein Serverdienst, der Ereignisse von anderen Clients entgegennimmt und diese lokal abspeichert.
Windows Error Reporting Service (WerSvc)	<b>Disabled</b>	Der Dienst ermöglicht eine Berichterstattung über abgestürzte Anwendungen und sucht nach automatischen Lösungsvorschlägen. Es können außerdem Logdateien für Diagnose und Reparatur-Dienste generiert werden.
Windows Insider Service	<b>Disabled</b>	Der Windows Insider Service wird für die Teilnahme am gleichnamigen Programm von Microsoft verwendet.
Windows Media Player Network Sharing Service (WMPNetworkSvc)	<b>Disabled</b>	Der Dienst ermöglicht es, Windows Media Player Bibliotheken über das


<i>Dienst</i>	<i>Empfehlung für den „StartupType“</i>	<i>Erläuterung</i>
		Netz freizugeben, damit sie von anderen Multimediageräten verwendet werden können.
Windows Mobile Hotspot Service (icssvc)	<b>Disabled</b>	Mit dem Dienst lassen sich mobile Datenverbindungen für andere Geräte verfügbar machen.
Windows Push Notifications System Service (WpnService)	<b>Disabled</b>	Durch den Dienst können Benachrichtigungen und Updates von Drittanbietern über das Internet empfangen werden.
Windows PushToInstall Service (PushToInstall)	<b>Disabled</b>	Der Dienst verwaltet Apps, die aus der Microsoft Store App eines anderen Geräts zur Installation auf das lokale Gerät bestimmt wurden.
Windows Remote Management (WS-Management) (WinRM)	<b>Disabled</b>	Der Dienst Windows Remote Management (WinRM) empfängt über das Netz WS-Management-Anfragen und verarbeitet diese. Mögliche Angreiferinnen und Angreifer können mit kompromittierten Anmeldeinformationen die Schnittstellen von WinRM verwenden, um aus der Ferne bestimmte Aktionen auf dem lokalen System auszuführen <sup>68</sup> . Verschiedene Management-Tools wie z. B. der System Center Configuration Manager (SCCM) sind auf diesen Dienst angewiesen.
Xbox Live Auth Manager (XblAuthManager)	<b>Disabled</b>	Die Xbox-Dienste stellen Funktionen (z. B. Authentisierung, Speichersynchronisierung, Netzdienste, etc.) für die Xbox Spieleplattform auf Windows 10 bereit.
Xbox Live Game Save (XblGameSave)	<b>Disabled</b>	
Xbox Live Game Save (XboxGipSvc)	<b>Disabled</b>	
Xbox Live Networking Service (XboxNetApiSvc)	<b>Disabled</b>	

### Windows-Features


Windows-Features sind teilweise optionale (Zusatz-)Funktionen, die durch den Benutzenden hinzugefügt oder entfernt bzw. deaktiviert werden können, sofern sie nicht benötigt werden. Es wird empfohlen, die Liste der bereits installierten Programme sowie der aktivierten Windows-Features zu sichten und zu prüfen, welche der Programme und Funktionen deaktiviert bzw. deinstalliert werden können. Dies ist vom tatsächlichen Einsatzszenario abhängig. Windows-Features können nicht zentral über die Gruppenrichtlinie verwaltet werden. Alternativ ist dies über (PowerShell-)Skripte vorzunehmen, die über die Gruppenrichtlinien verteilt werden.

<sup>68</sup> MITRE ATT&CK Technique T1021.006 (Remote Services: Windows Remote Management)  
<https://attack.mitre.org/techniques/T1021/006/>

Die in Windows 10 vorinstallierten und ggfs. ausgeführten Programme können in der „Computerverwaltung“ überprüft werden:

 Control Panel → Programs → Programs and Features → Uninstall or change a program

Die in Windows 10 aktivierten Windows-Features können in der „Computerverwaltung“ überprüft werden:

 Control Panel → Programs → Programs and Features → Turn Windows features on or off

<b>Windows Feature</b>	<b>Voreinstellung</b>	<b>Erläuterung</b>
.NET Framework 3.5 (includes .NET 2.0 and 3.0)	Off	Das .NET-Framework wird von Software benötigt, die als .NET-Anwendung entwickelt wurden. In der Regel wird bei der Installation von Software, die Abhängigkeiten zum .NET-Framework hat, das .NET-Framework nachinstalliert.
.NET Framework 4.6 Advanced Services	On (nur TCP Port Sharing der WCF Services)	
Active Directory Lightweight Directory Services	Off	Die AD LDS Dienste sind unabhängig von Active Directory und stellen Verzeichnisdienstfunktionen für Anwendungen zur Verfügung. In der Regel werden sie nicht auf einem Client benötigt.
Containers	Off	Das Feature stellt Dienste und Werkzeuge bereit, um Windows Server Container zu erstellen und zu verwalten. In der Regel werden sie nicht auf einem Client benötigt.
Data Center Bridging	Off	Durch das Feature werden Funktionen zur Nutzung der DCB Suite der IEEE-Standards bereitgestellt. In der Regel wird das Feature nicht auf dem Client benötigt.
Device Lockdown	Off	Das Device Lockdown Feature wird beispielsweise zur Konfiguration von Kiosk-PCs verwendet. Mit den Funktionen ist es möglich, unerwünschte Tastatureingaben (z. B. STRG-ALT-ENTF) zu unterbinden oder Schreibzugriffe auf Laufwerke zu verhindern.
Guarded Host	Off	Das Feature wird beim Einsatz von Shielded-VMs und Guardian Host Service in Hyper-V benötigt.
Hyper-V	Off	Die Hyper-V Funktionen umfassen die Management-Werkzeuge und Tools sowie die Hyper-V Plattform mit dem Hyper-V Hypervisor und Hyper-V Services. Die Dienste sollten nur aktiviert werden, wenn sie benötigt werden.
Internet Explorer 11	On	Die Internet Explorer Desktopanwendung wird zum 15.06.2022 eingestellt und nicht

<b>Windows Feature</b>	<b>Voreinstellung</b>	<b>Erläuterung</b>
		mehr unterstützt. Wird die Desktopanwendung nicht benötigt, sollte sie deaktiviert werden. <sup>69</sup>
Internet Information Services	Off	Durch das Feature können IIS-Webserver oder FTP-Server bereitgestellt werden. Ein Client-System sollte nicht als Server fungieren.
Internet Information Services Hostable Web Core	Off	Durch das Feature kann es Anwendungen ermöglicht werden, eigenständig Webserver zu hosten. Ein Client-System sollte nicht als Server fungieren.
Legacy Components	Off	Zu den Legacy Components zählt DirectPlay, ein Netzdienst für Multiplayer-Spiele.
Media Features	On	Das Feature umfasst den Windows Media Player. Sollte der Windows Media Player nicht benötigt werden, lässt er sich durch Deaktivieren des Features abschalten.
Microsoft Message Queue (MSMQ) Server	Off	Durch die MSMQ-Technik können Anwendungen in heterogenen Netzen auch mit Systemen kommunizieren, die zeitweise offline sind. Die Funktion wird von veralteten Anwendungen verwendet. Das Feature sollte nur bei Bedarf aktiviert werden.
Microsoft Print to PDF	On	Windows 10 verfügt über einen integrierten PDF-Drucker, mit dem Ausdrücke in das PDF-Format umgewandelt werden können.
Microsoft XPS Document Writer	On	Dokumentenbetrachter für das XPS-Format. Sollte das Dateiformat nicht verwendet werden, kann das Feature deaktiviert werden.
MultiPoint Connector	Off	Ermöglicht die Verwaltung und Überwachung des Clients durch MultiPoint Manager und Dashboard Anwendungen.
Print and Document Services	On (nur der Internet Printing Client)	Der Internet Printing Client ermöglicht HTTP-Verbindungen zu Webdruckservern. Sollte die Funktion nicht für Drucker benötigt werden, sollte sie deaktiviert werden.
Remote Differential Compression API Support	On	Das Feature wird von bestimmten Drittanbieter-Anwendungen zur Komprimierung von Dateien benötigt. Sollten keine Anwendungen eingesetzt werden, die das Feature benötigen, sollte es deaktiviert werden.

<sup>69</sup> <https://learn.microsoft.com/de-de/troubleshoot/browsers/disable-internet-explorer-windows>

<b>Windows Feature</b>	<b>Voreinstellung</b>	<b>Erläuterung</b>
Services for NFS	Off	Das Feature enthält Dienste und Werkzeuge zum Zugriff auf Dateien über das Network File System (NFS)-Protokoll. Wird NFS nicht eingesetzt, sollte das Feature deaktiviert sein.
Simple TCP/IP Services (echo, daytime etc.)	Off	Das Feature umfasst Netzfunktionen, wie „echo“, „daytime“, etc. und wird in der Regel nicht benötigt.
SMB 1.0/CIFS File Sharing Support	Off	Ermöglicht Datei- und Druckerfreigaben mit älteren Windows-Versionen (Windows NT 4.0 bis XP und Server 2003 R2). Sollte eine Abwärtskompatibilität nicht benötigt werden, sollte das Feature deaktiviert werden.
SMB Direct	On	SMB (Server Message Block) über RDMA (Remote Direct Access Memory) Netzdaten werden direkt in den Speicher des entfernten Hosts gesendet, ohne CPU-Kerne für Berechnungen beim TCP/IP-Stack hier groß in Anspruch zu nehmen. Dies setzt RDMA-fähige Netzwerkkadapters voraus. Diese Funktion wird hauptsächlich nur bei Servern eingesetzt.
Telnet Client	Off	Das Feature stellt eine Telnet-Kommandozeile bereit, um sich zu Telnet-Servern zu verbinden. Telnet ist veraltet und nicht sicher. Der Client sollte daher nur hinzugefügt werden, wenn ein konkreter Anwendungsfall dies erfordert.
TFTP Client	Off	Das Trivial File Transfer-Protokoll gilt als veraltet und nicht sicher. Der TFTP-Client sollte daher nur hinzugefügt werden, wenn ein konkreter Anwendungsfall dies erfordert.
Virtual Machine Platform	Off	Das Feature ermöglicht eine Unterstützung für virtuelle Maschinen unter Windows 10 (Voraussetzung für den Einsatz des „Windows Subsystem for Linux“). Mit der Virtual Machine Platform können MSIX-Anwendungspakete für APP-V/MSI erstellt werden.
Windows Hypervisor Platform	Off	Das Feature stellt ein User-Mode API für Drittanbieter-Virtualisierung und Anwendungen bereit, damit diese Aktionen am Hyper-V Hypervisor vornehmen können (z. B. Konfigurationen von Partitionen, Speicherzuordnung oder virtuellen Prozessoren)

<b>Windows Feature</b>	<b>Voreinstellung</b>	<b>Erläuterung</b>
Windows Identity Foundation 3.5	Off	Ältere .NET-Anwendungen benötigen ggf. das Feature. In .NET 4 ist ein neues Identity Framework bereits integriert.
Windows PowerShell 2.0	On	Die PowerShell 2.0 Engine ist veraltet und abgekündigt. Aus Kompatibilitätsgründen ist sie noch enthalten. Im Gegensatz zu PowerShell Version 5.1 (und aufwärts) werden in PowerShell Version 2.0 keine relevanten Sicherheitsfunktionalitäten implementiert, z. B. die Unterstützung des Anti-Malware Scan Interface (AMSI) oder die Protokollierung von PowerShell-Skriptblöcken. Daher stellt die PowerShell Version 2.0 ein Sicherheitsrisiko dar und sollte deaktiviert werden, wenn sie nicht explizit durch einen Anwendungsfall benötigt wird.
Windows Process Activation Service	Off	Das Feature wird von den Internetinformationsdiensten (IIS) verwendet. Sollte das Feature nicht benötigt werden, sollte es deaktiviert werden.
Windows Projected File System	Off	Das Windows Projected File System (ProjFS) ermöglicht einer User-Mode Anwendung virtuelle Dateisysteme zu erstellen <sup>70</sup> .
Windows Subsystem for Linux	Off	Durch das Feature kann eine Linux Bash (z.Zt. Ubuntu-Distribution) in Windows ausgeführt werden. Außerdem lassen sich Linux-Anwendungen in Windows 10 ausführen.
Windows TIFF iFilter	Off	Mit dem Feature lassen wird der Windows Indexdienst befähigt, TIFF-Dateien zu analysieren und eine (Text-)OCR-Erkennung durchzuführen, damit beispielsweise Inhalte gescannter Dokumente mit der Windows Suche durchsucht werden können.
Work Folders Client	On	Das Feature synchronisiert Ordnerinhalte und stellt sie Offline zur Verfügung <sup>71</sup> . Sollte die Funktion nicht benötigt werden, sollte das Feature deaktiviert werden.

### Vorinstallierte Apps (Apps, System-Apps und Features)

In Windows 10 sind einige Apps (APPX-Pakete) und sog. „Windows-Features“ bereits vorinstalliert. Die vorinstallierten Apps sind kontenspezifisch, sodass diese automatisch in der Umgebung des Kontos installiert und zur Verfügung gestellt werden. Sie befinden sich im Verzeichnis C:\Program Files\WindowsApps. System-Apps werden im Verzeichnis C:\Windows installiert und sind Teil des Betriebssystems.

<sup>70</sup> <https://learn.microsoft.com/en-us/windows/win32/projfs/projected-file-system>

<sup>71</sup> <https://learn.microsoft.com/de-de/windows-server/storage/work-folders/work-folders-overview>



Auf einem Referenzsystem sollte nach der Installation für ein Referenzkonto eines Benutzenden die Liste der bereitgestellten Windows-Apps ermittelt werden:

- ⚙️ *Windows-Settings* → *Apps & Features*
- ⚙️ *Windows-Settings* → *Apps & Features* → *Optional Features*

**Hinweis:** Nicht alle Apps lassen sich über die UI deinstallieren<sup>72</sup>.

**PowerShell:** Ermitteln der vorinstallierten (System-)Apps (administrative Rechte erforderlich)

```
PS C:\> Get-AppxProvisionedPackage -Online | Format-Table DisplayName, PackageName
```

Die Liste der vorinstallierten (System-)Apps kann in ein kommentierbares Datenformat gebracht werden, um zu Dokumentationszwecken die Entscheidung für das Beibehalten oder Entfernen einer App zu hinterlegen.

Da sich über die Bedienschnittstelle nicht alle Apps entfernen lassen und diese immer nur für das angemeldete Konto entfernt werden, wird empfohlen die PowerShell zu verwenden:

**PowerShell:** Entfernen vorinstallierte (System-)Apps für neue Konten

```
PS C:\> Remove-AppxProvisionedPackage -Online -PackageName [PACKAGENAME_EINFUEGEN]
```

**Hinweis:** Durch diesen Befehl werden die provisionierten Appx-Pakete entfernt. Bereits installierte Appx-Packe müssen mit `Remove-AppxPackage` entfernt werden.

**PowerShell:** Entfernen vorinstallierte (System-)Apps für ein bestehendes Konto:

```
PS C:\> Remove-AppxPackage -Package [PACKAGENAME_EINFUEGEN]
```

## IP-Protokollfamilien

Die Konfiguration der Netzadapter hängt stark von der Netzkonfiguration ab. Sollte ein spezifisches Protokoll wie z. B. ausschließlich IPv4 verwendet werden, sollte IPv6 auf demselben Adapter deaktiviert werden. Der Einsatz von Tunnelprotokollen oder der Mischbetrieb der Protokollfamilien sollte vermieden werden, da hierdurch eine zusätzliche Komplexität bei der Absicherung der Netzkommunikation hinzukommt.

 *Computer Configuration/Administrative Templates/Network/TCPIP Settings/IPv6 Transition Technologies*


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Set Teredo State	Disabled	Teredo (RFC 4380) baut einen IPv6-Tunnel über eine IPv4-Sitzung auf. Durch derartige Tunneltechniken können Sicherheitsmaßnahmen umgangen werden, wie z. B. Firewalls oder IDS. Weiterführende Informationen können aus Kapitel 3.7 des Leitfadens für eine sichere IPv6-Netzarchitektur <sup>73</sup> entnommen werden.

<sup>72</sup> <https://learn.microsoft.com/de-de/windows/application-management/apps-in-windows-10>


<sup>73</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi\\_lana\\_leitfaden\\_ipv6\\_pdf.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_leitfaden_ipv6_pdf.pdf?__blob=publicationFile)

Gegebenenfalls können nicht alle für alle Netzadapter die Protokollfamilien festgelegt werden. Dies trifft insbesondere für Schnittstellen zu unterschiedlich konfigurierten Netzen zu, wie dies typischerweise bei mobilen Einsatzszenarien der Fall ist.

### Funkprotokolle: WLAN-Funktionen


 Computer Configuration/Administrative Templates/Network/Network Connection Manager

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Prohibit connection to non-domain networks when connected to domain authenticated network	<b>Enabled</b>	Sofern eine aktive Netzverbindung zu einem Domänennetz besteht, sollten weitere Verbindungen zu anderen Netzen, die nicht Teil des Domänennetzes sind, unterbunden werden.

 Computer Configuration/Administrative Templates/Network/WLAN Service/WLAN Settings

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services	<b>Disabled</b>	Im vordefinierten Verhalten können Benutzende die Funktion („Wi-Fi Sense“) selbstständig ein- oder ausschalten. Um zu verhindern, dass automatisch eine Verbindung zu offenen oder von geteilten WiFi-Hotspots („Mobile Hotspot“) durch Windows 10 hergestellt wird, sollte die Richtlinieneinstellung deaktiviert werden. Hierdurch lässt sich verhindern, dass Verbindungen zu potenziell unsicheren Netzen aufgebaut wird und hierbei möglicherweise sensible Daten abfließen können.

### Projektornutzung

 Computer Configuration/Administrative Templates/Windows Components/Connect

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Don't allow this PC to be projected to	<b>Enabled</b>	Vordefiniert können andere Geräte den Client nur als Anzeigebildschirm verwenden (projizieren), wenn das optionale Feature „Wireless Display“ nachinstalliert wird. Durch die Richtlinieneinstellung wird verhindert, dass der Client als Projektor genutzt werden kann (Anzeigebildschirm kann von anderen Clients über das Netz/andere Funkprotokolle verwendet werden) <sup>74</sup> .


<sup>74</sup> <https://support.microsoft.com/en-us/windows/screen-mirroring-and-projecting-to-your-pc-5af9f371-c704-1c7f-8f0d-fa607551d09c>

## Treiber

Eine Liste der vorinstallierten Gerätetreiber kann mittels Kommandozeilenbefehl „driverquery“ ausgegeben werden<sup>75</sup>:

```
C:\> driverquery /V
```

Die vorinstallierten Treiber sollten hinsichtlich ihrer Notwendigkeit für den Betrieb überprüft werden. Nicht benötigte Treiber sollten ggfs. deinstalliert werden.

 Computer Configuration/Administrative Templates/MS Security Guide

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Configure SMB v1 client driver	<b>Enabled</b>  <b>Options:</b> Configure MrxSmb10 driver: • Disable driver	Durch die Richtlinieneinstellung wird der Startup-Typ des SMBv1 Kernel-Mode Treibers im Client festgelegt. Wichtiger Hinweis: „Disabled“ sollte nicht für die Einstellung insgesamt gewählt werden, da dies den Wert des Startup-Typs in der Registry löscht.
Configure SMB v1 server	<b>Disabled</b>	Die Richtlinieneinstellung deaktiviert die serverseitige Verarbeitung des SMBv1-Protokolls.

## Mapper und Responder-Treiber für das Link-Layer Topology Discovery

 Computer Configuration/Administrative Templates/Network/Link-Layer Topology Discovery

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn on Mapper I/O (LLTDIO) driver	<b>Disabled</b>	Die Empfehlung entspricht der Voreinstellung.
Turn on Responder (RSPNDR) driver	<b>Disabled</b>	Durch die Link-Layer Topologie Discovery wird ein grafischer Netzplan erstellt, in dem eine Übersicht über das Netz, der verbundenen PCs und Geräte sowie den zugehörigen Metainformationen dargestellt wird.

## Entwicklermodus

Der Entwicklermodus ermöglicht u. a. die Installation von Apps aus unbekanntem Quellen (sog. „Side-loading“) und sollte deaktiviert werden, sofern er nicht explizit durch einen Anwendungsfall benötigt wird. In der Voreinstellung ist der Entwicklermodus deaktiviert und kann durch Benutzende nur mit Konten, die über Administrationsrechte verfügen, in der „Settings“-App aktiviert werden:

 Windows-Settings/Update & Security/For developers/Developer Mode

Über nachfolgende Gruppenrichtlinieneinstellung kann der Entwicklermodus auch systemweit deaktiviert werden:

 Computer Configuration/Administrative Templates/Windows Components/App Package Deployment

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
-------------------------------	------------	-------------

<sup>75</sup> <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/driverquery>

Allow development of Windows Store apps and installing them from an integrated development environment (IDE)	<b>Disabled</b>	Die Einstellung verhindert, dass Apps aus unbekanntem Quellen installiert werden.
--	-----------------	---

### Fernwartung (Remote Assistance)


Die Remoteunterstützung ist in der Voreinstellung aktiviert, sodass Benutzende Einladungen zur Remoteunterstützung erstellen können. Konfigurationsempfehlungen werden zur Anforderung [SYS.2.2.3.A18 Einsatz der Windows-Remoteunterstützung](#) bereitgestellt.

### Energieoptionen: Standby-Modus<sup>76</sup>

 Computer Configuration/Administrative Templates/System/Power Management/Sleep Settings


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow standby states (S1-S3) when sleeping (plugged in)	<b>Disabled</b>	Bei Verwendung der Standby-Modi S1 bis S3 werden Anwendungsdaten und ggfs. vertrauenswürdige Daten oder Anmeldeinformationen im Arbeitsspeicher gehalten. Mögliche Angreiferinnen und Angreifer, die einen Client im Standby vorfinden, können potenziell sensible Informationen aus dem Arbeitsspeicher stehlen.
Allow standby states (S1-S3) when sleeping (on battery)		
Require a password when a computer wakes (plugged in)	<b>Enabled</b>	Es handelt sich um die Voreinstellung. Bei Reaktivierung des Clients aus dem Standby ist die Eingabe des Passworts zum Entsperren notwendig.
Require a password when a computer wakes (on battery)	<b>Enabled</b>	

### Insider Preview (Experimentiermodus)

 Computer Configuration/Administrative Templates/Windows Update for Business

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Manage preview builds	<b>Disabled</b>	Durch Konfiguration der Richtlinie wird verhindert, dass Benutzende dem Windows Insider Program über „Settings → Update and Security“ beitreten können. In verwalteten und produktiven Umgebungen sollten Benutzende nicht experimentelle Versionen von Windows beziehen und einsetzen. Durch Fehler und Bugs können Sicherheitsrisiken bestehen.

### Windows Connect Now

 Computer Configuration/Administrative Templates/Network/Windows Connect Now

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Configuration of wireless settings using Windows Connect Now	<b>Disabled</b>	

<sup>76</sup> <https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/system-sleeping-states>

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Prohibit access of the Windows Connect Now wizards	<b>Enabled</b>	Durch den Assistenten können Wireless Router oder Access-Point eingerichtet werden. In zentral verwalteten Umgebungen sollten mögliche Schattennetze abseits der vorgesehenen Infrastruktur unterbunden werden.

### Microsoft Support Diagnostic Tool



Computer Configuration/Administrative Templates/System/Troubleshooting and Diagnostics/Microsoft Support diagnostic Tool

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider	<b>Disabled</b>	Das Microsoft Support Diagnostic Tool (MSDT) sammelt Diagnosedaten zur Analyse für Supportanbieter. Um zu verhindern, dass möglicherweise sensible Daten gesammelt und versendet werden, sollte das Tool über die Richtlinie deaktiviert werden.

### Windows Performance PerfTrack



Computer Configuration/Administrative Templates/System/Troubleshooting and Diagnostics/Windows Performance PerfTrack

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Enable/Disable PerfTrack	<b>Disabled</b>	PerfTrack ist in der Voreinstellung aktiviert und erfasst Events zur Leistung und Performance. Um zu verhindern, dass über die Funktion möglicherweise sensible Informationen an Microsoft übertragen werden, sollte die Richtlinie konfiguriert werden.

### Windows Script Host (WSH) und Windows Script Host Remoting

Als Laufzeitumgebung für Skriptsprachen kann der Windows Script Host (WSH) von Benutzenden und Administrierenden verwendet werden, um Aufgaben zu automatisieren. Gleichzeitig werden Skripte auch von möglichen Angreiferinnen und Angreifern verwendet, um beispielsweise bestimmte Aktionen auf dem Opfersystem auszuführen. Aus diesem Grund sollte nur die Ausführung vertrauenswürdiger Skripte ermöglicht werden oder der Windows Script Host deaktiviert werden, wenn eine Skriptausführung nicht benötigt wird. In der Voreinstellung ist der Windows Script Host aktiviert. Entsprechende Empfehlungen können aus den Kapiteln 5.5.2.1 („Ausführung von vertrauenswürdigen Skripten“), 5.2.2 („Deaktivierung von Windows Script Host“) sowie 5.5.2.3 („Deaktivierung von Windows Script Host Remoting“) der Konfigurationsempfehlungen zur Härtung von Windows 10 mit Bordmitteln angewendet werden<sup>77</sup>.


<sup>77</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen\\_zur\\_Haertung\\_von\\_Windows\\_10.pdf?blob=publicationFile&v=3](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen_zur_Haertung_von_Windows_10.pdf?blob=publicationFile&v=3)

## Lokale Namensauflösung durch LLMNR und NetBIOS


Durch die lokale Namensauflösung mit dem Link-Local Multicast Name Resolution (LLMNR)-Protokoll und NetBIOS können mögliche Angreiferinnen und Angreifer Informationen der IT-Infrastruktur sammeln und für mögliche Spoofing- oder Relay-Angriffe verwenden<sup>78</sup>.

 *Computer Configuration/Administrative Templates/Network/DNS-Client*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off multicast name resolution	<b>Enabled</b>	Die Multicast-Namensauflösung ist in der Voreinstellung für alle Netzadapter aktiviert.

 *Computer Configuration/Administrative Templates/Network/Network Connections*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
NetBT NodeType configuration	<b>Enabled</b>  <b>Options:</b> • Configure NetBT NodeType: P-node	Vordefiniert verwendet Windows 10 Broadcasts (B-Node), wenn kein WINS-Server für ein Netzinterface angegeben wurde. Bei Angabe eines WINS-Servers wird zunächst dieser kontaktiert und anschließend ein Broadcast gesendet. Durch die empfohlene Einstellung wird verhindert, dass das System NetBIOS Broadcasts versendet.

 *Computer Configuration/Administrative Templates/MSS (Legacy)*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. NetBIOS Name Release-Anfragen werden von Windows 10 Clients ignoriert. Ausgenommen hiervon sind anfragende WINS-Server.


## Einrichtung von Bridges im Netz

 *Computer Configuration/Administrative Templates/Network/Network Connections*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Prohibit installation and configuration of Network Bridge on your DNS domain network	<b>Enabled</b>	Im vordefinierten Verhalten können Benutzende, die über Konten mit administrativen Berechtigungen verfügen, Netzbrücken oder die Konfiguration von Netzbrücken ändern. Um zu verhindern, dass Netzbrücken in fremde Netze konfiguriert werden können, sollte die Richtlinieneinstellung aktiviert werden. Die Richtlinieneinstellung hat nur Auswirkung auf domänenverbundene Clients.
Prohibit use of Internet Connection Sharing on your DNS domain network	<b>Enabled</b>	In der Voreinstellung dürfen Benutzende mit Hilfe der Funktion „Mobile Hotspot“ (auch ohne Administrationsrechte) ein ad


<sup>78</sup> MITRE ATT&CK Technique T1557.001 (Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay) <https://attack.mitre.org/techniques/T1557/001/>

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
		hoc WLAN für weitere IT-Systeme erstellen. Um zu verhindern, dass hierdurch Verbindungen zu weiteren Geräten erfolgt, sollte die Funktion über die Gruppenrichtlinieneinstellung deaktiviert werden.

 Computer Configuration/Administrative Templates/Network/Windows Connection Manager

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Minimize the number of simultaneous connections to the Internet or a Windows Domain	<b>Enabled</b>  <b>Options:</b> Minimize Policy Options: • 3 = Prevent Wi-Fi when on Ethernet	Die Richtlinieneinstellung verhindert, dass neben einer drahtgebundenen Verbindung zusätzlich eine WLAN-Verbindung aufgebaut werden kann.

## Netzdienste

 Computer Configuration/Administrative Templates/MSS (Legacy)

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten.
MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	<b>Enabled</b>  <b>Options:</b> DisableIPSourceRouting: • Highest protection, source routing is completely disabled.	Zum Schutz vor Spoofing-Angriffen sollte die Richtlinieneinstellung entsprechend der Empfehlung konfiguriert werden, sodass das IP-Source Routing abgeschaltet wird.
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	DisableIPSourceRouting IPv6: • Highest protection, source routing is completely disabled	
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	<b>Disabled</b>	Im vordefinierten Verhalten sind in Windows 10 Änderungen der Routing-Tabelle durch ICMP-Redirects möglich. Nach Ablauf einer Zeitspanne von 10 Minuten wird eine durch ICMP-Redirect erlernte Route zwar wieder aus der Routingtabelle entfernt, allerdings ist der Client für diesen Zeitraum für Routingprobleme anfällig. Um zu verhindern, dass mittels OSPF erzeugte Routen durch ICMP-Redirect überschrieben werden, sollte die Richtlinieneinstellung deaktiviert werden.

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds	<b>Enabled</b>  <b>Options:</b> KeepAliveTime • 300,000 or 5 minutes (recommended)	In Windows 10 werden Keep-Alive-Packages im Regelfall nicht versenden. Anwendungen ist es jedoch möglich, diese entsprechend über ein TCP Stack Flag anzufordern. Zur Reduzierung des Risikos von möglichen Denial-of-Service-Angriffen sollte der Abstand (Keep Alive Time) verringert werden.
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	<b>Disabled</b>	Das Internet Router Discovery Protocol (IRDP) ermöglicht dem Client eine Erkennung eines Gateways und konfiguriert dieses entsprechend RFC 1256 automatisch als Gateway-Adresse in der Netzkonfiguration.  In Angriffen mit Zugriff auf das Netz, können Clients gefälschte Gateways vorgegeben werden. Aus diesem Grund sollte die Funktion deaktiviert werden.
MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted	<b>Enabled</b>  <b>Options:</b> TcpMaxDataRetransmissions • 3	Durch die Richtlinieneinstellung kann festgelegt werden, wie häufig durch TCP Datensegmente erneut versendet werden, wenn der Empfang nicht durch den Empfänger quittiert wurde. Anschließend wird die Verbindung bei Erreichen des Höchstwertes erfolgloser Versuche abgebrochen. Der Wert sollte nicht zu hoch gewählt werden, damit die Ressourcen des Clients durch Angriffe nicht zu stark ausgelastet werden können.
MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted		

### Deaktivierung nicht benötigter Funktionen in der Firmware

Werden (Hardware-)Funktionen nicht benötigt, werden diese in den Firmwareeinstellungen deaktiviert. Nicht abschließende Auflistung möglicherweise nicht benötigter Funktionen:

- **Schnittstellen**
  - Funk (WLAN, Bluetooth, NFC)
  - Ein-/Ausgabeports (USB Port, Memory Card Slot, ExpressCard, Camera, Microphone, Firewire, Thunderbolt)
- **(Peripherie-)Geräte**
  - Sensoren (Fingerabdruckleser, GPS, Lagesensoren, ...)
  - Trusted Platform Module (TPM)
- **Funktionen**
  - Bootmenü (F10/F12)
  - Wake On LAN
  - Preboot Execution Environment (PXE)



- Intel Active Management Technology (AMT)
- (Firmware-)Update (z. B. Windows UEFI Update)
- Diebstahlsicherung (z. B. Computrace)

### SYS.2.1.A18 Nutzung von verschlüsselten Kommunikationsverbindungen (S)

Der sog. „Secure Channel“ (auch: „SChannel“) in Windows 10 ist ein Security Support Provider (SSP), der eine Sammlung von Sicherheitsprotokollen zur Authentifizierung und sicheren, verschlüsselten Kommunikation bereitstellt. Der SChannel wird häufig von Anwendungen und Diensten in Windows 10 genutzt, die abgesicherte HTTP-Verbindungen benötigen.

Tabelle 11: Exemplarischer Aufbau der Bezeichnung von Cipher Suites

Protokoll	Schlüssel-austausch-algorithmus	Signatur-algorithmus		Sitzungsverschlüsselung, Schlüsselgröße und Verschlüsselungstyp	Nachrichten-authentifizierungs-algorithmus mit Digestgröße	Elliptic Curve (optional)
TLS_	ECDHE_	ECDSA_	WITH_	AES_256_GCM_	SHA384_	P384

 Computer Configuration/Administrative Templates/Network/SChannel Configuration Settings/Cipher Suite Order

Gruppenrichtlinieneinstellung	Empfehlung
SSL Cipher Suites	<p><b>Enabled</b></p> <p><b>Options:</b></p> <p>TLS_DHE_DSS_WITH_AES_128_CBC_SHA256            TLS_DHE_DSS_WITH_AES_256_CBC_SHA256            TLS_DHE_RSA_WITH_AES_128_GCM_SHA256            TLS_DHE_RSA_WITH_AES_256_GCM_SHA384            TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384            TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256            TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384            TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256            TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384            TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256            TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384            TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256</p>

Die nachfolgenden SChannel-Konfigurationen<sup>79,80</sup> der Ciphers, Hashalgorithmen, Schlüsselaustauschalgorithmen und Protokolle können ohne Erstellung einer selbstdefinierten ADMX/ADML-Vorlage nur über das Setzen von Registrierungswerten in der Windows-Registry von Windows 10 konfiguriert werden. In verwalteten Umgebungen ist die Erstellung einer solchen Gruppenrichtlinienvorlage zu empfehlen. Microsoft stellt hierfür keine ADMX/ADML-Vorlage zur Verfügung. Wenn keine Vorlage erstellt werden soll, können in verwalteten Umgebungen auch die Registrierungswerte über die Gruppenrichtlinie konfiguriert werden.

<sup>79</sup> <https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/restrict-cryptographic-algorithms-protocols-schannel>

<sup>80</sup> <https://learn.microsoft.com/en-us/windows-server/security/tls/tls-schannel-ssp-changes-in-windows-10-and-windows-server>

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers

Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)	Registrierungsschlüssel	Wertname (REG_DWORD)	Empfohlener Datenwert
Enable AES 128/128	AES 128/128	Enabled	0xffffffff
Enable AES 256/256	AES 256/256	Enabled	0xffffffff
Enable DES 56/56	DES 56/56	Enabled	0x00000000
Enable NULL	NULL	Enabled	0x00000000
Enable RC2 40/128	RC2 40/128	Enabled	0x00000000
Enable RC2 56/128	RC2 56/128	Enabled	0x00000000
Enable RC2 128/128	RC2 128/128	Enabled	0x00000000
Enable RC4 40/128	RC4 40/128	Enabled	0x00000000
Enable RC4 56/128	RC4 56/128	Enabled	0x00000000
Enable RC4 64/128	RC4 64/128	Enabled	0x00000000
Enable RC4 128/128	RC4 128/128	Enabled	0x00000000
Enable Triple DES 168/168	Triple DES 168/168	Enabled	0x00000000

Wert 0xffffffff repräsentiert den aktivierten Zustand, Wert 0x00000000 bedeutet, dass die Cipher deaktiviert wird.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes

Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)	Registry-Key	ValueName	Value
Enable the MD5 Hash	MD5	Enabled	0x00000000
Enable the SHA Hash	SHA	Enabled	0x00000000
Enable the SHA256 Hash	SHA256	Enabled	0xffffffff
Enable the SHA384 Hash	SHA384	Enabled	0xffffffff
Enable the SHA512 Hash	SHA512	Enabled	0xffffffff

Wert 0xffffffff repräsentiert den aktivierten Zustand, Wert 0x00000000 bedeutet, dass der Hashalgorithmus deaktiviert wird.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms

Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)	Registry-Key	ValueName	Value
Diffie-Hellman Settings	Diffie-Hellman	ClientMinKeyBitLength	0x00000800 (2048)* 0x00000bb8 (3000)
		ServerMinKeyBitLength	0x00000800 (2048)* 0x00000bb8 (3000)
Enable Elliptic curve Diffie-Hellman	ECDH	Enabled	0xffffffff
Enable public-key cryptography standards	PKCS	ClientMinKeyBitLength	0x00000bb8 (3000)

\*Nach der BSI TR-02102-1 bis Ende 2022 verwendbar<sup>81</sup>.

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)	Registry-Key	ValueName	Value
Enable Multi-Protocol Unified Hello for Servers (IIS)	MultiProtocol Unified Hello\Server	Enabled	0x00000000

<sup>81</sup> <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?blob=publicationFile>

<b>Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)</b>	<b>Registry-Key</b>	<b>ValueName</b>	<b>Value</b>
	MultiProtocol Unified Hello\Server	DisabledByDefault	0x00000001
Enable Private Communications Technology (PCT) 1.0 for Clients	PCT 1.0\Server	Enabled	0x00000000
	PCT 1.0\Server	DisabledByDefault	0x00000001
Enable Private Communications Technology (PCT) 1.0 for Servers	PCT 1.0\Client	Enabled	0x00000000
	PCT 1.0\Client	DisabledByDefault	0x00000001
Secure Sockets Layer (SSL) 2.0 for Clients	SSL 2.0\Client	Enabled	0x00000000
		DisabledByDefault	0x00000001
Secure Sockets Layer (SSL) 2.0 for Servers	SSL 2.0\Server	Enabled	0x00000000
		DisabledByDefault	0x00000001
Secure Sockets Layer (SSL) 3.0 for Clients	SSL 3.0\Client	Enabled	0x00000000
	SSL 3.0\Client	DisabledByDefault	0x00000001
Secure Sockets Layer (SSL) 3.0 for Servers	SSL 3.0\Server	Enabled	0x00000000
	SSL 3.0\Server	DisabledByDefault	0x00000001
Transport Layer Security (TLS) 1.0 for Clients	TLS 1.0\Client	Enabled	0x00000000
	TLS 1.0\Client	DisabledByDefault	0x00000001
Transport Layer Security (TLS) 1.0 for Server	TLS 1.0\Server	Enabled	0x00000000
	TLS 1.0\Server	DisabledByDefault	0x00000001
Transport Layer Security (TLS) 1.1 for Clients	TLS 1.1\Client	Enabled	0x00000000
	TLS 1.1\Client	DisabledByDefault	0x00000001
Transport Layer Security (TLS) 1.1 for Server	TLS 1.1\Server	Enabled	0x00000000
	TLS 1.1\Server	DisabledByDefault	0x00000001
Transport Layer Security (TLS) 1.2 for Clients	TLS 1.2\Client	Enabled	0x00000000
	TLS 1.2\Client	DisabledByDefault	0x00000001
Transport Layer Security (TLS) 1.2 for Servers	TLS 1.2\Server	Enabled	0x00000001
	TLS 1.2\Server	DisabledByDefault	0x00000000

Wert 0x00000001 repräsentiert den aktivierten Zustand, Wert 0x00000000 bedeutet, dass das Protokoll deaktiviert wird.





Computer Configuration/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel/Advanced Page

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Turn off encryption support	Only use TLS 1.2	Transport Layer Security (TLS) 1.0, TLS 1.1, TLS 1.2, Secure Sockets Layer (SSL) 2.0, or SSL 3.0 werden deaktiviert. Der Mindeststandard des BSI zur Verwendung von Transport Layer Security <sup>82</sup> erlaubt TLS 1.2 oder TLS 1.3, allerdings unterstützt Windows 10 nur TLS 1.2.


Dienste, die den Empfehlungen des Mindeststandards des BSI zur Verwendung von Transport Layer Security<sup>82</sup> nicht entsprechen, sind nach Umsetzung der Konfigurationseinstellungen möglicherweise nicht mehr nutzbar. Bei Abweichungen sollte berücksichtigt werden, dass diese Einstellungen systemweit gültig sind, d. h. alle Anwendungen, die die TLS Funktionalität des Betriebssystems nutzen, sind hiervon betroffen.

<sup>82</sup> [https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll\\_node.html](https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html)

 Computer Configuration/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Client

 Computer Configuration/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Service

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow Basic authentication	<b>Disabled</b>	Vordefiniert nutzt der WinRM Client keine Basic Authentication.
Disallow Digest authentication	<b>Enabled</b>	Digest Authentication sollte nicht zur Authentisierung in WinRM verwendet werden.
Allow unencrypted traffic	<b>Disabled</b>	WinRM Client und Service dürfen keine unverschlüsselten Informationen austauschen. Häufig wird WinRM nicht direkt verwendet, sondern auch durch weitere Funktionen, wie PowerShell Remoting oder Windows Event Forwarding.
Disallow WinRM from storing RunAs credentials	<b>Disabled</b>	Anmeldeinformationen sollten nicht durch WinRM zwischengespeichert werden.

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Konfigurationsparameter	Empfehlung	Erläuterung
Network security: Configure encryption types allowed for Kerberos	AES128_HMAC_SHA1, AES256_HMAC_SHA1 Future encryption types	Erläuterung siehe <a href="#">SYS.2.2.3.A9 Sichere zentrale Authentisierung in Windows-Netzen</a> .
Microsoft network client: Send unencrypted password to third-party SMB servers	<b>Disabled</b>	Verhindern des Sendens von unverschlüsselten Kennwörtern an SMB-Server von Drittanbietern. Die Einstellung ist heute praktisch nicht mehr relevant, da die relevanten Implementierungen von SMB (z. B. Samba) verschlüsselte Passwörter unterstützen.
Microsoft network client: Digitally sign communications (always)	<b>Enabled</b>	Mit aktivierter Einstellung fordert die SMB Clientkomponente, dass die SMB-Datenpakete signiert sein müssen. Anderenfalls ist die Kommunikation mit einem SMB-Server nicht möglich. Hierdurch lassen sich Man-in-the-Middle Angriffe verhindern, bei denen bspw. SMB-Datenpakete durch unberechtigte Dritte manipuliert werden.
Microsoft network client: Digitally sign communications (if server agrees)	<b>Enabled</b>	Der Microsoft Network Client fragt den beteiligten SMB-Server an, ob dieser SMB Signing unterstützt. Falls ja, werden die SMB-Datenpakete signiert.
Microsoft network server: Digitally sign communications (always)	<b>Enabled</b>	Mit aktivierter Einstellung fordert die SMB-Serverkomponente, dass die SMB-Datenpakete signiert sein müssen. Anderenfalls ist die Kommunikation mit einem SMB-Client nicht möglich. Hierdurch lassen sich Man-in-the-Middle Angriffe verhindern, bei denen bspw.

<b>Konfigurationsparameter</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		SMB-Datenpakete durch unberechtigte Dritte manipuliert werden.
Microsoft network server: Digitally sign communications (if client agrees)	<b>Enabled</b>	Der Microsoft Network Server fragt den beteiligten SMB-Client an, ob dieser SMB Signing unterstützt. Falls ja, werden die SMB-Datenpakete signiert.
Network security: LDAP client signing requirements	Required Signing	Die LDAP-Kommunikation sollte immer signiert werden. Sollten im lokalen Netz Systeme betrieben werden, die LDAP Signing noch nicht unterstützen, muss überprüft werden, welche Zugriffsmöglichkeiten genutzt werden können. Entweder kann das betroffene System solange nicht genutzt werden, bis LDAP Signing umgesetzt ist oder die Sicherheitseinstellung muss für alle Zugriffe in der Infrastruktur heruntergesetzt werden („Negotiate signing“).
Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM	Für die vom LAN-Manager geforderte Authentifizierungsebene sollte das Authentifizierungsprotokoll für Netzanmeldungen festgelegt werden. Veraltete Protokolle sollten dafür nicht mehr verwendet werden. Die Gruppenrichtlinieneinstellung legt fest, dass nur noch NTLMv2 eingesetzt wird.
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security and Require 128-bit encryption	Es handelt sich um das vordefinierte Verhalten. Server setzen eine 128-Bit Verschlüsselung und NTLMv2 voraus.
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security and Require 128-bit encryption	
Domain member: Digitally encrypt or sign secure channel data (always)	<b>Enabled</b>	Wird ein Windows 10 Client in eine Windows-Domäne aufgenommen, wird ein Objekt für diesen Client erstellt. Das zugehörige Kennwort wird dafür genutzt, um eine sichere Verbindung (engl.: <i>Secure Channel</i> ) zwischen Domänencontroller und Client aufzubauen. Durch die Einstellung wird sichergestellt, dass alle Kommunikation über den Secure Channel verschlüsselt oder signiert sein muss. Mit aktivierter Einstellung wird sichergestellt, dass der Secure Channel nur aufgebaut wird, wenn die Signierung-/

<b>Konfigurationsparameter</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		Verschlüsselung der gesamten Kommunikation über den Secure Channel ausgehandelt ist. Unabhängig von dieser Einstellung werden Anmeldeinformationen, die über den sicheren Kanal übertragen werden, immer verschlüsselt.
Domain member: Digitally encrypt secure channel data (when possible)	<b>Enabled</b>	Es handelt sich um das vordefinierte Verhalten. Mit aktivierter Einstellung wird vom Domänenmitglied (Windows 10 Client) die Verschlüsselung der Kommunikation innerhalb des Secure Channels gefordert. Unterstützt der Domänencontroller die Verschlüsselung der gesamten Kommunikation über den Secure Channel, wird der Netzverkehr verschlüsselt. Falls der Domänencontroller nicht die Verschlüsselung des gesamten Netzverkehrs unterstützt, werden zumindest die Anmeldeinformationen (Logon Information) verschlüsselt über den Secure Channel übertragen.
Domain member: Digitally sign secure channel data (when possible)	<b>Enabled</b>	Mit aktivierter Einstellung wird vom Domänenmitglied (Windows 10 Client) die Signierung der Kommunikation innerhalb des Secure Channels gefordert. Unterstützt der Domänencontroller die Signierung der gesamten Kommunikation über den Secure Channel, wird der Netzverkehr signiert.
Domain member: Maximum machine account password age	30	Das Kennwort des Computerobjekts im Active Directory sollte regelmäßig geändert werden. Die Änderung des Kennworts erfolgt in der Standardkonfiguration im Abstand von 30 Tagen automatisch.
Domain member: Disable machine account password changes	<b>Disabled</b>	
Domain member: Require strong (Windows 2000 or later) session key	<b>Enabled</b>	Mit aktivierter Einstellung wird eine Schlüssellänge von 128 Bit für die Verschlüsselung der Daten, die über den Secure Channel ausgetauscht werden, gefordert.

### SYS.2.1.A20 Schutz der Administrationsverfahren bei Clients (S)

In Windows 10 wird zwischen lokaler Administration und Remote-Administration (über das Netz) unterschieden. Hierbei sollte zuerst festgelegt werden, ob der Client mit lokalen oder domänenverwalteten Konten administriert werden soll. Bei der Nutzung von domänenverwalteten Konten sollte berücksichtigt werden, dass die Clients nicht mit dem Konto des „Domänenadministrators“ verwaltet werden, sondern ein

gesondertes Konto verwendet wird, welches über eine Mitgliedschaft in der lokalen Gruppe der „Administrators“ verfügt. Wenn ein zur Administration verwendetes Konto („Administrationskonto“) für mehrere Clients verwendet wird, besteht das Risiko, dass sich mögliche Angreiferinnen und Angreifer bei Übernahme dieses Kontos auf andere Clients ausbreiten können. Um dieses Risiko auszuschließen, sollten unterschiedliche Administrationskonten bzw. unterschiedliche Passwörter für die Clients gewählt werden. Um die Verwaltung von mehreren Clients in domänenverwalteten Umgebungen zu unterstützen, kann LAPS verwendet werden (siehe [SYS.2.1.A1 Sichere Benutzerauthentisierung](#)).

Anmerkung: Das Built-In Administrationskonto, also das Konto mit dem Anzeigenamen „Administrator“ und der SID, die auf 500 endet (RID 500), sollte deaktiviert werden. Für die Administration des Clients sollte ein zusätzliches separates Konto angelegt werden.

Die neben den in Windows 10 verfügbaren Administrationsschnittstellen möglicherweise zusätzlich eingesetzten (Drittanbieter-)Werkzeuge sollten mit in der aufgestellten Übersicht, entsprechend der Empfehlung aus den Umsetzungshinweisen, berücksichtigt werden.

Entsprechend der erstellten Übersicht über die verschiedenen Administrationstätigkeiten, welche Arbeiten auf welchem Weg durchgeführt werden, sollte eine organisatorische und technische Absicherung der verwendeten Schnittstellen und Verfahren erfolgen. Nicht verwendete Schnittstellen sollten entsprechend [SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen](#) deinstalliert oder deaktiviert werden.

### Lokale Administration

In Windows 10 lassen sich unterschiedliche Verfahren und Methoden zur Administration verwenden. Über die Windows-Settings als auch die Systemsteuerung werden in Windows 10 häufig verwendete und benötigte Konfigurationsmöglichkeiten zusammengefasst. Hierbei wird nicht zwischen gesonderten Ansichten für Benutzende und Administrierende unterschieden. Änderungen von systemweit geltenden Konfigurationseinstellungen können i. d. R. nur mit administrativen Rechten vorgenommen werden. Spezifische Konfigurationen zu bestimmten Betriebssystemkomponenten und eine Feinjustierung wird in der Regel über Gruppenrichtlinien oder die Windows-Registry vorgenommen.

### Vorinstallierte administrative (Verwaltungs-)Werkzeuge

Die administrativen Werkzeuge in Windows 10<sup>83</sup> können beispielsweise über die Systemsteuerung („control.exe“) auf dem lokalen System aufgelistet werden. Einige der Werkzeuge können als Snap-In über die Microsoft Management Console (MMC) geöffnet werden. Die Verknüpfungen verweisen auf nachfolgende administrative Verwaltungs- und Diagnosewerkzeuge:

Tabelle 12: Übersicht der vorinstallierten (Verwaltungs-)Werkzeuge

Administratives Werkzeug	Kurzbeschreibung
<a href="#">Component Services</a>	Administrationsmöglichkeit zur Verwaltung von Component Object Model (COM) Komponenten, COM+ Anwendungen und Distributed Transaction Coordinator (DTC).
<a href="#">Computer Management</a>	In der „Computerverwaltung“ werden verschiedene Verwaltungskonsolen zusammengefasst: Geplante Aufgaben (engl.: <i>Task Scheduler</i> ), Ereignisanzeige (engl.: <i>Event Viewer</i> ), Freigegebene Ordner (engl.: <i>Shared Folders</i> ), „Benutzer-/Gruppenverwaltung“ (engl.: <i>Local Users and Groups</i> ), Leistungsmonitoring (engl.: <i>Performance</i> ), Geräte-Manager (engl.: <i>Device Manager</i> ), Datenträgerverwaltung (engl.: <i>Disk Management</i> ) sowie Dienste und Anwendungen (engl.: <i>Service and Applications</i> ).
<a href="#">Defragment and Optimize Drives</a>	Werkzeuge und Einstellungen zur (regelmäßigen) Optimierung von Laufwerken.

<sup>83</sup> <https://learn.microsoft.com/en-us/windows/client-management/administrative-tools-in-windows-10>

<b>Administratives Werkzeug</b>	<b>Kurzbeschreibung</b>
<a href="#">Disk Cleanup</a>	Mit Hilfe der Datenträgerbereinigung in Windows 10 lassen sich möglicherweise nicht mehr benötigte Dateien ermitteln, die entfernt werden können, um freien Speicherplatz zu schaffen.
<a href="#">Event Viewer</a>	Die Ereignisanzeige dient der Betrachtung von Logdateien, wie bspw. der Windows-Protokolllogbücher: Application, Security, Installation, System oder weitergeleitete Ereignisse.
<a href="#">iSCSI Initiator</a>	Mittels des iSCSI Initiators lassen sich u. a. Laufwerke über das iSCSI Protokoll verbinden.
<a href="#">Local Group Policy Editor</a>	Anzeigen und Bearbeiten der lokalen Gruppenrichtlinien (Teilmenge der lokalen Gruppenrichtlinien).
<a href="#">Local Security Policy Editor</a>	Anzeigen und Bearbeiten der lokalen Sicherheitsrichtlinien (Teilmenge der lokalen Gruppenrichtlinien).
<a href="#">Microsoft Management Console (MMC)</a>	Administrative Verwaltungstools lassen sich auch in der Microsoft Management Console (MMC) über sog. „Snap-Ins“ hinzufügen. Für einige der verfügbaren Snap-Ins steht zudem beim Hinzufügen ein Assistent zur Verfügung, der durch die Konfiguration des Snap-Ins navigiert. Snap-Ins sind insbesondere aus dem Windows-Server-Umfeld bekannt. Es können auch entfernte Windows-Systeme administriert werden. Es kann ein Konsolenstamm mit den zur Administration benötigten Verwaltungskonsolen erstellt und für eine spätere Verwendung abgespeichert werden.
<a href="#">ODBC Data Sources</a>	Verwaltung von Datenbanktreibern und -quellen.
<a href="#">Performance Monitor</a>	Umfangreiche Visualisierungsmöglichkeiten für leistungsbezogenes Monitoring in Echtzeit oder aus gespeicherten Logdateien.
<a href="#">PowerShell</a>	Mit der PowerShell können über eine Vielzahl vorhandener Commandlets (Cmdlets) Konfigurationen des Clients ausgelesen oder verändert werden. Es ist auch eine skriptbasierte automatisierte Verwaltung möglich. Hinweise zur Konfiguration bzw. Verwendung der PowerShell werden in den Empfehlungen zur Anforderung <a href="#">SYS.2.2.3.A22 Verwendung der Windows PowerShell</a> bereitgestellt.
<a href="#">Print Management</a>	Verwaltung von Druckern, Druckertreibern und -servern.
<a href="#">Recovery Drive</a>	Erstellung eines Wiederherstellungslaufwerkes.
<a href="#">Registry Editor</a>	Die Windows-Registry ist eine hierarchische Konfigurationsdatenbank, die sowohl von Windows 10 als auch installierten Anwendungen verwendet wird. In der Registrierungsdatenbank werden neben Einstellungen, die betriebssystemweit gültig sind auch Einstellungen für die einzelnen Konten hinterlegt. Auf die kontenspezifischen Einstellungen hat das jeweilige Konto voreingestellt Schreibrechte. Mit dem Windows-Registry Editor kann die Windows-Registry interaktiv verwaltet werden.
<a href="#">Resource Monitor</a>	Umfangreiche Visualisierungsmöglichkeiten für leistungsbezogenes Monitoring der Auslastung von Systemressourcen (Prozessorleistung, Datenträgerzugriffen, Arbeitsspeicherauslastung oder Netzbandbreite).
<a href="#">Services</a>	Verwaltung von (System-)Diensten.
<a href="#">System Configuration (MSCONFIG)</a>	Konfiguration des Systemstartverhaltens von Windows und (System-) Diensten.
<a href="#">System Information</a>	Zusammenfassung über vorhandene Hard- und Softwareressourcen, Komponenten sowie Eigenschaften der Systemumgebung.



<b>Administratives Werkzeug</b>	<b>Kurzbeschreibung</b>
<a href="#">Task Scheduler</a>	Verwaltung von geplanten Aufgaben, die bestimmte Ereignisse nach einem festgelegten Auslöser starten.
<a href="#">Windows Management Instrumentation (WMI)</a>	Bei der Windows Management Instrumentation (WMI) handelt es sich um eine Implementierung des Web Based Enterprise Management (WBEM) auf Basis des Common Information Models (CIM). Durch die WMI können administrative Aufgaben, sowohl auf dem lokalen, als auch auf entfernten Clients automatisiert werden oder Verwaltungsinformationen ausgetauscht werden.
<a href="#">Windows Firewall with Advanced Security</a>	Verwaltungskonsole der Windows Firewall mit erweiterter Sicherheit.
<a href="#">Windows Memory Diagnostic</a>	Werkzeuge zur Arbeitsspeicherdiagnose.

## Remote-Administration

Bei der Remote-Administration werden die Clients häufig von Administrationsarbeitsplätzen aus der Ferne über das Netz administriert. Hierfür stehen in Windows 10 zum einen interaktive Methoden, wie Remote-Desktop-Sitzungen (engl.: *RDP-Session*) oder die Remote-Unterstützung (engl.: *Remote Assistance*) und zum anderen unterschiedliche Protokolle sowie Schnittstellen zur Verfügung, die für administrative Tätigkeiten verwendet werden können.

### Interaktive Remote-Administration mit Zugriff auf die Bedienoberfläche

Sowohl die Remoteunterstützung (engl.: *Windows Remote Assistance*, kurz RA) als auch das Remotedesktopprotokoll (engl.: *Windows Remote Desktop Protocol*, kurz RDP) bieten einen entfernten Zugriff auf das Zielsystem mit vollständiger Bedienoberfläche. Die Remoteunterstützung ist in der Voreinstellung aktiviert. Benutzende müssen jedoch eine Unterstützungseinladung versenden. Remote Desktop ist in der Voreinstellung deaktiviert. Konfigurationsempfehlungen zum Einsatz von Remote Desktop und der Remote Assistance werden unter [SYS.2.2.3.A18 Einsatz der Windows-Remoteunterstützung \(S\)](#) beschrieben. Die Administration erfolgt dann analog zu der oben beschriebenen lokalen Administration.

### Protokolle und Schnittstellen zur Remote-Administration:

#### Windows Remote Management (WinRM)

Bei der Windows Remoteverwaltung (WinRM) handelt es sich um eine Implementierung des WS-Verwaltungsprotokolls<sup>84</sup>, das u. a. auf dem Simple Object Access Protokoll (SOAP) basiert. WinRM wird u. a. dazu verwendet, um mit der Windows Management Instrumentation (WMI) über das Netz interagieren zu können. In der Voreinstellung ist der Dienst nicht aktiv. Für die Nutzung der Schnittstelle sind mehrere Schritte erforderlich:

1. Aktivierung des Dienstes „WinRM“ und Auswahl des Startup-Types: „Automatic (Delayed Start)“
2. Aktivieren/Anlegen der vordefinierten eingehenden Ausnahmeregel „Windows Remote Management (HTTP-In)“ in der Windows Firewall für die Profile „Domain, Private“
3. Konfiguration des WinRM-Listeners über die PowerShell oder die GPO<sup>85</sup>

<sup>84</sup> <https://learn.microsoft.com/de-de/windows/win32/winrm/portal>

<sup>85</sup> <https://learn.microsoft.com/de-de/archive/blogs/wmi/three-ways-to-configure-winrm-listeners>

Alternativ ist die Einrichtung von WinRM über einen Konfigurationsassistenten möglich<sup>86</sup>:

```
C:\> winrm quickconfig
```


Dabei ist die automatisch vorgenommene Konfiguration von WinRM zu prüfen:

```
C:\> winrm get winrm/config
```

Insbesondere sollten hierbei auch die Wahl des WinRM Listener überprüft werden:

```
C:\> winrm enumerate winrm/config/listener
```

Verfügen mögliche Angreiferinnen und Angreifer über Anmeldeinformationen, können diese über WinRM aus der Ferne Aktivitäten mit den Rechten des jeweiligen Kontos durchführen<sup>87</sup>.

 Computer Configuration/Administrative Templates/Windows Components/Windows Remote Management (WinRM)/WinRM Service

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow remote server management through WinRM	„ <b>Enabled</b> “, wenn WinRM als Administrationsschnittstelle verwendet wird. In diesem Fall sollten über den IPv4/IPv6-Filter nur die IP-Adressen der Netzstellen des Clients zugelassen werden, über die eine Administration erfolgen soll (z. B. Management-Netz). Wichtig: Die Angabe erfolgt zwingend als Range x.x.x.x-x.x.x.x, auch wenn nur eine IP-Adresse des Clients über WinRM erreichbar gemacht werden soll.	Sofern die Richtlinieneinstellung nicht konfiguriert wurde, antwortet der WinRM-Service, der voreingestellt nicht automatisch gestartet wird, keinen Remotesystemen.

 Computer Configuration/Administrative Templates/Windows Components/Windows Remote Shell

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow Remote Shell Access	„ <b>Disabled</b> “, wenn ein Zugriff über die Windows Remote Shell (WinRS) nicht benötigt wird.	Sofern die Richtlinieneinstellung nicht konfiguriert wurde, ist der Zugriff über eine Windows Remote Shell (WinRS) möglich, wenn das Windows Remote Management eingerichtet ist. Sofern ein Remoteshellzugriff nicht benötigt wird, sollte dieser deaktiviert werden.

Wird WinRM zur Remote-Administration verwendet, sollten die Konfigurationsempfehlungen zur Anforderung [SYS.2.1.A18 Nutzung von verschlüsselten Kommunikationsverbindungen](#) betrachtet werden.

<sup>86</sup> <https://learn.microsoft.com/en-us/windows/win32/winrm/installation-and-configuration-for-windows-remote-management>

<sup>87</sup> MITRE ATT&CK Technique T1021.006 (Remote Services: Windows Remote Management): <https://attack.mitre.org/techniques/T1021/006/>

Administrationsverfahren wie Desired State Configuration (DSC) oder auch das PowerShell Remoting nutzen WinRM:

Tabelle 13: Protokolle und Schnittstellen von Desired State Configuration (DSC) und PowerShell Remoting

<b>Protokoll/Schnittstelle</b>	<b>Erläuterungen</b>
<a href="#">Desired State Configuration (DSC)</a>	<p>Desired State Configuration (DSC) ist eine Plattform zur Konfiguration, Bereitstellung und Verwaltung von Systemen. Es handelt sich um eine Funktion, die als Teil des Windows Management Frameworks mit der PowerShell Version 4.0 eingeführt worden ist. DSC erweitert die PowerShell um Methoden zur Konfigurationsverwaltung über mehrere Geräte.</p> <p>Hierbei können Konfigurationen entweder von einer Freigabe abgerufen (Pull) oder auf den Client verteilt werden (Push)<sup>88</sup>.</p>
<a href="#">PowerShell Remoting</a>	<p>Durch das PowerShell Remoting lassen sich Befehle auf entfernten IT-Systemen ausführen. Das PowerShell Remoting ist in der Voreinstellung nicht aktiviert. Sofern es aktiviert werden soll, wird das Windows Remote Management konfiguriert (WinRM) und verwendet. Dabei erfolgt unabhängig vom verwendeten Transportprotokoll (HTTP-5985/HTTPS-5986) die gesamte PowerShell-Remoting Kommunikation im Anschluss an die initiale Authentisierung verschlüsselt<sup>89</sup>.</p> <p>Einige der PowerShell Cmdlets, die über einen Parameter zur Angabe des Clients verfügen, können auch ohne PowerShell Remoting zur Remote-Administration u. a. verwendet werden<sup>90</sup>:</p> <ul style="list-style-type: none"> <li>• Restart-Computer</li> <li>• Test-Connection</li> <li>• Clear-EventLog</li> <li>• Get-EventLog</li> <li>• Get-HotFix</li> <li>• Get-Process</li> <li>• Get-Service</li> <li>• Set-Service</li> <li>• Get-WinEvent</li> <li>• Get-WmiObject</li> </ul> <p>PowerShell Remoting kann von möglichen Angreiferinnen und Angreifern missbraucht werden. Sofern PowerShell Remoting zu Administrationszwecken verwendet werden soll, sollte die Nutzung entsprechend eingeschränkt werden. Hilfreiche Vorgehensweisen, u. a. die Verwendung von Just Enough Administration (JEA), lassen sich Kapitel 5.5.1.4.2 der Konfigurationsempfehlungen zur Härtung von Windows 10 mit Bordmitteln entnehmen<sup>91</sup>.</p>

<sup>88</sup> <https://learn.microsoft.com/en-us/powershell/dsc/pull-server/enactingconfigurations?view=dsc-1.1>

<sup>89</sup> <https://learn.microsoft.com/en-us/powershell/scripting/learn/remoting/winrmsecurity?view=powershell-5.1>

<sup>90</sup> <https://learn.microsoft.com/en-us/powershell/scripting/learn/remoting/running-remote-commands?view=powershell-5.1>

<sup>91</sup> [https://www.bsi.bund.de/EN/Topics/Cyber-Security/Recommendations/SiSyPHuS\\_Win10/AP11/SiSyPHuS\\_AP11\\_node.html](https://www.bsi.bund.de/EN/Topics/Cyber-Security/Recommendations/SiSyPHuS_Win10/AP11/SiSyPHuS_AP11_node.html)

## Distributed Component Object Model (DCOM)

DCOM ist ein Dienst, der über Port 135 über das Netz angesprochen werden kann. Nach einem initialen Kommunikationsaufbau wird je nach angesprochener Komponente eine individuelle Kommunikation auf einem anderen Port (RPC High-Port) dynamisch aufgebaut. Die verfügbaren Komponenten können in der Management Console über das Component Services Snap-In aufgelistet und konfiguriert werden<sup>92</sup>.

Nachfolgend werden beispielhaft einige Protokolle bzw. Schnittstellen aufgeführt, die zur Verwaltung des Clients eingesetzt werden können:

Tabelle 14: Protokolle und Schnittstellen von Windows Script Host Remoting und Windows Remote WMI

Protokoll/Schnittstelle	Erläuterungen
Windows Script Host Remoting	Empfehlungen zur Konfiguration werden zur Anforderung <a href="#">SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen</a> beschrieben.
Windows Remote WMI	Die Windows Management Instrumentation (WMI) kann auch über das Netz verwendet werden. Empfehlungen zur Konfiguration können über die Betriebssystem-Dokumentation abgerufen werden <sup>93</sup> .

## Windows-Remote Registry

Die Registrierungsdatenbank von Windows 10 lässt sich auch aus der Ferne verwalten. Der Start-Typ des zugehörigen Windows-Dienstes „Remote Registry“ (RemoteRegistry) ist voreingestellt „manual“, sodass die Remoteregistrierung im vordefinierten Verhalten nicht aktiviert ist. Die Windows Remote Registry verwendet das Windows Remote Registry Protocol (MS-RRP)<sup>94</sup>, welches auf Remote Procedure Call (RPC) basiert.



Computer Configuration/Windows Settings/Local Policies/Security Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Network access: Remotely accessible registry paths	<b>Enabled</b>  <b>Options:</b> Kein Eintrag	Durch die Richtlinieneinstellung kann eine selbst zu definierende Liste von Pfaden angegeben werden, auf die über das Netzwerk zugegriffen werden darf (ACL). Hinweis: Für einen netzbasierten Zugriff auf die Registry muss der Dienst „Remote Registry“ ausgeführt werden <sup>95</sup> .
Network access: Remotely accessible registry paths and sub-paths	<b>Enabled</b>  <b>Options:</b> Kein Eintrag	Siehe Erläuterung zu „Network access: Remotely accessible registry paths“

## Gruppenrichtlinien

Gruppenrichtlinieneinstellungen stellen umfangreiche Anpassungs- und Konfigurationsmöglichkeiten für die Administration von Windows 10 dar. Hierbei wird unterschieden zwischen:

<sup>92</sup> [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731901\(v=ws.11\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731901(v=ws.11)?redirectedfrom=MSDN)

<sup>93</sup> <https://learn.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista>

<sup>94</sup> [https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-rrp/0fa3191d-bb79-490a-81bd-54c2601b7a78](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rrp/0fa3191d-bb79-490a-81bd-54c2601b7a78)

<sup>95</sup> <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-remotely-accessible-registry-paths>

- **Lokale Gruppenrichtlinie (Richtlinien für den Client)**  
Das lokale Gruppenrichtlinienobjekt kann mit administrativer Berechtigung durch das Snap-In „Group Policy Object Editor“ über die MMC editiert werden.
- **Zentral verwaltete Gruppenrichtlinien**  
Die Gruppenrichtlinienobjekte innerhalb der Domäne werden im Active Directory über den zentralen Gruppenrichtlinieneditor („Group Policy Editor“) verwaltet.

Über die Gruppenrichtlinienobjekte lässt sich sowohl die „Computerkonfiguration“ als auch die „Benutzerkonfigurationen“ vornehmen.

### Einschränkungen der Remotedienste für administrative Zwecke


Die Abschaltung der in Windows 10 integrierten Administrationsschnittstellen ist sehr aufwändig. Außerdem hat Microsoft in vielen Fällen Funktionen so implementiert, dass ein Abschalten der Remotedienste für administrative Zwecke dazu führt, sodass auch hiermit nicht in Bezug stehende interne Client-Funktionen eingeschränkt sein können. Da diese Aspekte von Microsoft teilweise nicht dokumentiert sind, ist eine Bewertung und Empfehlung nicht verlässlich möglich. Daher sollte anstelle des Deaktivierens der zugehörigen Dienste eine Einschränkung der Kommunikation über die Windows-Firewall konfiguriert werden.

### SYS.2.1.A21 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras (S)

Über die Firmware lassen sich in der Regel ein eingebautes Mikrofon und/oder eine eingebaute Kamera deaktivieren. In Windows 10 lässt sich für Apps (Appx-Pakete) individuell festlegen, welche auf Mikrofon oder Kamera zugreifen dürfen. Für alle anderen Programme lässt sich mittels Gruppenrichtlinieneinstellung im Gegensatz dazu keine individuelle Einschränkung der Kamera- und Mikrofonnutzung vornehmen. Hier verbleibt nur die Möglichkeit einer pauschalen Aktivierung oder Deaktivierung.

Um eine Geräteinstallation vom Benutzenden angeschlossenes Mikrofon bzw. Webcam einzuschränken, kann eine Geräteinstallationsrichtlinie konfiguriert werden<sup>96</sup>.

#### Mikrofon

 *Computer Configuration/Administrative Templates/Windows Components/App Privacy*


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Let Windows apps access the camera	<b>Enabled</b> <b>Options:</b> <ul style="list-style-type: none"> <li>• Default for all apps: Force Deny</li> <li>• Force allow these specific apps (use Package Family Names): z. B. Microsoft.SkypeApp_kzft8qxf38zg5c</li> </ul>	Die Richtlinie gilt nur für Windows (Store) Apps. Im vordefinierten Verhalten dürfen Benutzende selbst entscheiden, welche Apps auf die Kamera zugreifen dürfen. Mit der Richtlinie sollten Organisationen den Kamerazugriff durch Apps einschränken.
Let Windows apps activate with voice while the system is locked	<b>Enabled</b> <b>Options:</b> <ul style="list-style-type: none"> <li>• Default for all apps: Force Deny</li> </ul>	Durch die Richtlinieneinstellung wird festgelegt, ob Spracheingaben über das Mikrofon von Windows Apps verarbeitet werden, wenn der Client gesperrt ist. Eine Nutzung eines gesperrten Clients

<sup>96</sup> <https://learn.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy>

	widerspricht den Anforderungen SYS.2.1.A1.
--	---

## Kamera


Über Gruppenrichtlinieneinstellung lässt sich die Kameranutzung softwareseitig verhindern oder einschränken:

 *Computer Configuration/Administrative Templates/Windows Components/App Privacy*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Let Windows apps access the microphone	<b>Enabled</b>  <b>Options:</b> <ul style="list-style-type: none"> <li>• Default for all apps: Force Deny</li> <li>• Force allow these specific apps (use Package Family Names); z. B. Microsoft.SkypeApp_kzft8qxf38zg5c</li> </ul>	Die Richtlinie gilt nur für Windows (Store) Apps. Vordefiniert dürfen Benutzende selbst darüber entscheiden, welche Apps auf das Mikrofon zugreifen dürfen. Mit der Richtlinie sollten Organisationen den Mikrofonzugriff durch Apps einschränken.

 *Computer Configuration/Administrative Templates/Windows Components/Camera*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow Use of Camera	<b>Disabled</b>	Durch diese Einstellung wird die Verwendung der Kamera pauschal verhindert. Erlaubte Apps in der Richtlinie „Let Windows apps access the microphone“ dürfen weiterhin auf die Kamera zugreifen.

 *Computer Configuration/Administrative Templates/Control Panel/Personalization*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Prevent enabling lock screen camera	<b>Enabled</b>	Durch diese Einstellung wird die Verwendung der Kamera auf dem Sperrbildschirm verhindert.

## SYS.2.1.A23 Bevorzugung von Client-Server-Diensten (S)

Grundsätzlich sollte der Windows 10 Client keine Serverdienste anbieten. Falls doch Serverdienste angeboten werden, müssen im Einzelfall auch die entsprechenden IT-Grundschutz-Bausteine berücksichtigt werden.

### Datei- und Druckerfreigaben


Der LanmanServer-Dienst ist immer aktiv, da insbesondere in einer Windows-Domäne viele Verwaltungsdienste hierauf beruhen. Eine Abschaltung des Dienstes für Windows 10 Clients, die Teil einer Windows-Domäne sind, wird daher allgemein nicht empfohlen.

Für Stand-alone Installationen sollte geprüft werden, ob der Dienst abgeschaltet werden kann. In diesem Fall kann der Dienst „LanmanServer“ mit dem Anzeigenamen „Server“ gestoppt werden und der Startup-Typ des Dienstes auf „Disabled“ festgelegt werden. Nach einem Neustart von Windows 10 ist der Port 445

nicht mehr geöffnet. Alternativ kann anstelle des Deaktivierens des Dienstes eine Einschränkung der Kommunikation über die Windows-Firewall konfiguriert werden.

### Administrative Freigaben


Die administrativen Freigaben sind voreingestellt und nach Aktivierung der Datei- und Druckerfreigabe über die Windows-Firewall auch über das Netz erreichbar. Richten Administrierende darüber hinausgehende Freigaben ein, werden diese ebenfalls über die Windows-Firewall zugelassen. Diese können auch zentral über die folgende GPO gesetzt werden.

 Computer Configuration/Administrative Templates/MS Security Guide

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure environments)	<b>Disabled</b>	Die administrativen Freigaben sollten über die Richtlinieneinstellung deaktiviert werden.

### Drucker

Angeschlossene Drucker am Client sollten nur im Bedarfsfall für andere Clients freigegeben werden. Vorzuziehen sind dedizierte Druckserver, um direkte Verbindungen zwischen Clients zu vermeiden.


 Computer Configuration/Administrative Templates/Printers

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow Print Spooler to accept client connections	<b>Disabled</b>	Im Standardfall (die Richtlinieneinstellung wurde nicht konfiguriert), lässt der Druckerspooler keine Clientverbindungen zu, bis ein lokaler Drucker im Netz freigegeben wird. Durch die Richtlinieneinstellung wird verhindert, dass der Druckerspooler Clientverbindungen zulässt. Konten aus der Gruppe „Users“ können außerdem keine Drucker freigeben. Der Druckerspooler-Dienst muss nach Konfiguration der Richtlinieneinstellung neu gestartet werden. Hinweis: Die Richtlinieneinstellung bezieht sich nicht auf bereits freigegebene Drucker.
Package Point and print - Approved servers	<b>Enabled</b> <b>Options:</b> Unter „Enter fully qualified server names“ sollte eine Liste der Server angegeben werden, von denen Clients Drucker installieren dürfen.	Über die Einstellung lassen sich die Server konfigurieren, von denen Drucker über Point and Print installiert werden dürfen. Durch Angabe einer Liste von gültigen Druckservern wird die Installation von Druckern über beliebige Server verhindert.
Point and Print Restrictions	<b>Enabled</b> <b>Options:</b>	Mit der Gruppenrichtlinie können die Point and Print Restrictions konfiguriert werden <sup>97</sup> , sodass Benutzenden eine

<sup>97</sup> <https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7>

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
	Aktivieren der Option: „Users can only point and print to these servers:“ sowie Angabe von Servernamen der in der Infrastruktur gültigen Druckserver. <ul style="list-style-type: none"> <li>• <b>Security Prompts:</b> „When installing drivers for a new connection:“ <b>Show warning and elevation prompt</b></li> <li>• „When updating drivers for an existing connection:“ <b>Show warning and elevation prompt</b></li> </ul>	Warnmeldung sowie eine Aufforderung der „Benutzerkontensteuerung für erhöhte Rechte“ angezeigt wird, um Druckertreiber zu installieren <sup>98</sup> . Alternativ können alle Einstellungen dieser Gruppenrichtlinie über folgenden Windows-Registry-Eintrag überschrieben werden: “HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint RestrictDriverInstallationTo Administrators = 1“ Mit dieser Registry-Einstellung können nur noch Administrierende bei Verwendung von „Point and Print“ einen Druckertreiber installieren <sup>99</sup> .

### Update Delivery Optimization

 Computer Configuration/Administrative Templates/Windows Components/Delivery Optimization

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Download Mode	<b>Enabled</b>  <b>Options:</b> Download Mode: <ul style="list-style-type: none"> <li>• LAN (1) oder</li> <li>• Simple (99)</li> </ul> alternativ: <ul style="list-style-type: none"> <li>• Bypass (100)</li> </ul>	Windows Updates, Apps und App-Updates werden nicht zwischen Arbeitsplätzen innerhalb eines Netzes ausgetauscht. Durch Konfiguration der Richtlinieneinstellung soll verhindert werden, dass externe Quellen (z.B. Cloud-Dienste) kontaktiert werden.

### Peer-to-Peer Protokolle zur Namensauflösung

 Computer Configuration/Administrative Templates/Network/Microsoft Peer-to-Peer Networking Services


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off Microsoft Peer-to-Peer Networking Services	<b>Enabled</b>	Das Peer Name Resolution Protocol (PNRP) wird in Peer-to-Peer-Szenarien als Protokoll zur Namensauflösung verwendet, um erreichbare Clients zu erkennen, mit denen eine direkte Kommunikation geführt werden kann (z. B. Chat). Vor eingestellt sind die Dienste aktiviert. Um zu verhindern, dass Peer-to-Peer-Verbindungen zur Namensauflösung aufgebaut

<sup>98</sup> <https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7>


<sup>99</sup> <https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872>




<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		werden, sollte die Richtlinieneinstellung aktiviert werden.

 *Computer Configuration/Administrative Templates/Network/Microsoft Peer-to-Peer Networking Services/Peer Name Resolution Protocol/Global Clouds*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Set PNRP cloud to resolve only	<b>Enabled</b>	Das Peer Name Resolution Protocol (PNRP) wird in Peer-to-Peer-Szenarien als Protokoll zur Namensauflösung verwendet, um erreichbare Clients zu erkennen, mit denen eine direkte Kommunikation geführt werden kann (z. B. Chat). Das Aktivieren der Einstellung verhindert, dass der Client PNRP-Namen registriert, um anderen Clients eine Namensauflösung zu ermöglichen. Das Auflösen von Namen anderer Clients über PNRP bleibt weiterhin möglich.
Turn off PNRP cloud creation	<b>Enabled</b>	Durch die Einstellung wird verhindert, dass durch das PNRP eine Cloud erstellt wird, die von Anwendungen verwendet werden könnte, um Hostnamen zu veröffentlichen oder aufzulösen.

 *Computer Configuration/Administrative Templates/Network/Microsoft Peer-to-Peer Networking Services/Peer Name Resolution Protocol/Link-Local Clouds*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Set PNRP cloud to resolve only	<b>Enabled</b>	Das Peer Name Resolution Protocol (PNRP) wird in Peer-to-Peer-Szenarien als Protokoll zur Namensauflösung verwendet, um erreichbare Clients zu erkennen, mit denen eine direkte Kommunikation geführt werden kann (z. B. Chat). Das Aktivieren der Einstellung verhindert, dass der Client PNRP-Namen registriert, um anderen Clients eine Namensauflösung zu ermöglichen. Das Auflösen von Namen anderer Clients über PNRP bleibt weiterhin möglich.
Turn off PNRP cloud creation	<b>Enabled</b>	Durch die Einstellung wird verhindert, dass durch das PNRP eine Cloud erstellt wird, die von Anwendungen verwendet werden könnte, um Hostnamen zu veröffentlichen oder aufzulösen.

 *Computer Configuration/Administrative Templates/Network/Microsoft Peer-to-Peer Networking Services/Peer Name Resolution Protocol/Site-Local Clouds*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Set PNRP cloud to resolve only	<b>Enabled</b>	Das Peer Name Resolution Protocol (PNRP) wird in Peer-to-Peer-Szenarien als

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		Protokoll zur Namensauflösung verwendet um erreichbare Clients zu erkennen, mit denen eine direkte Kommunikation geführt werden kann (z. B. Chat). Das Aktivieren der Einstellung verhindert, dass der Client PNRP Namen registriert, um anderen Clients eine Namensauflösung zu ermöglichen. Das Auflösen von Namen anderer Clients über PNRP bleibt weiterhin möglich.
Turn off PNRP cloud creation	<b>Enabled</b>	Durch die Einstellung wird verhindert, dass durch das PNRP eine Cloud erstellt wird, die von Anwendungen verwendet werden könnte, um Hostnamen zu veröffentlichen oder aufzulösen.

### SYS.2.1.A24 Umgang mit externen Medien und Wechseldatenträgern (S)

Mit Hilfe von Gruppenrichtlinieneinstellungen zur Geräteinstallation lässt sich die Installation von Gerätetreibern und der Zugriff auf externe Schnittstellen konfigurieren.

Eine restriktive Konfigurationsmöglichkeit stellt die Verhinderung der Installation von Gerätetreibern von entfernbaren Geräten (Wechselgeräte) dar. Hierbei ist zu beachten, dass sich die Richtlinieneinstellungen nicht auf bereits installierte Geräte auswirken. Geräte mit bereits installierten Gerätetreibern können weiterhin verwendet werden. Die Information, ob es sich um ein Wechselgerät (Plug and Play) handelt, wird durch ein Gerät eigenständig vorgegeben. Manipulierte USB-Geräte können die Gruppenrichtlinieneinstellungen daher grundsätzlich auch umgehen.



Computer Configuration/Administrative Templates/System/Device Installation/Device Installation Restrictions

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
Prevent installation of removable devices	„Enabled“ oder „Disabled“	Mit aktivierter Einstellung wird pauschal verhindert, dass entfernbare Geräte (i.d.R. USB-Geräte, wie Tastaturen, Mäuse, Webcams, USB-Headsets, USB-Datenträger und Festplatten), die nach Aktivierung dieser Richtlinie angeschlossen werden, installiert und verwendet werden können. Die Richtlinieneinstellung ist nur zu empfehlen, wenn die anzuschließende Hardware insgesamt bekannt ist und sich nicht häufig verändert. Vor Aktivierung der Richtlinieneinstellung müssen die erlaubten Geräte ordnungsgemäß installiert worden sein. Diese Richtlinie wird vorrangig gegenüber allen anderen Richtlinien zur Geräteinstallation (wie z.B. der Verhinderung von Geräten mit Angabe von Geräte- oder Instanz-ID angewendet. Durch Umsetzung der sehr restriktiven Richtlinie ist es auch Administrierenden nicht mehr

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
		möglich, neue Geräte zu installieren. Damit Administrationskonten weiterhin eine Geräteinstallation angeschlossener Geräte durchführen können, kann zusätzlich die Richtlinieneinstellung „Allow administrators to override Device Installation Restriction policies“ konfiguriert werden. Benutzende halten bei Anschluss eines Wechselgeräts die Information, dass die Installation des angeschlossenen Gerätes durch eine Gruppenrichtlinie blockiert wurde und die Systemadministration kontaktiert werden sollte. Der Text und der Titel zur Hinweismeldung kann über die Gruppenrichtlinieneinstellung „Display a custom message (title) when installation is prevented by a policy setting“.
Allow administrators to override Device Installation Restriction policies.	„Enabled“ oder „Disabled“	Sofern Administrierende weiterhin Geräte installieren können sollen, ist die entsprechende Ausnahme mit der Einstellung festzulegen. Per Richtlinie blockierte Geräteinstallationen können über den Gerätemanager aktiviert werden (z.B. mittels „Update Driver Software“, um die Geräteinstallation neu zu initiieren.).
Display a custom message when installation is prevented by a policy setting	„Enabled“ oder „Disabled“	Für den Benutzenden kann ein individueller Text (max. 128 Zeichen) festgelegt werden, der auf die Gründe der fehlgeschlagenen Geräteinstallation hinweist und ggfs. einen Ansprechpartner benennt, an den sich gewendet werden kann. Wird die Richtlinie nicht konfiguriert oder deaktiviert, wird ein Standardtext angezeigt.

Neben der aufgezeigten sehr restriktiven Möglichkeit können über Gruppenrichtlinien auch eine Liste erlaubter Geräte als auch eine Liste nicht erlaubter Geräte gepflegt werden. Microsoft stellt über die Dokumentation zu Windows 10 eine entsprechende und detaillierte Schritt-für-Schritt-Anleitung mit Betrachtung verschiedener Szenarien zur Verfügung<sup>100</sup>.


An Windows 10 angeschlossene Geräte werden Anhand der vom Geräteherstellenden vergebenen Geräteinformationen (u. a. Device Instance ID, Device ID, Device Setup Class, Device Type) identifiziert. Diese können beispielsweise über den Gerätemanager oder dem Werkzeug „pnputil“ bzw. über das PowerShell cmdlet Get-PnpDevice für angeschlossene Geräte ausgelesen werden.

<b>Geräteidentifikationsmerkmal</b>	<b>Beschreibung</b>
Geräte-ID (engl.: <i>Device ID</i> ) und kompatible ID (engl.: <i>Compatible ID</i> ).	Die Geräte-ID soll ein Gerät eindeutig identifizieren und wird durch Geräteherstellende vergeben. Die Geräte-ID kann unter Hardware-IDs

<sup>100</sup> <https://learn.microsoft.com/en-us/windows/client-management/manage-device-installation-with-group-policy>

<b>Geräteidentifikationsmerkmal</b>	<b>Beschreibung</b>
	(HWID) in den Eigenschaften eines Gerätes im Gerätemanager aufgelistet werden.
Geräteinstanz-ID (engl.: <i>Device Instance ID</i> )	Durch den Geräteinstanzpfad wird ein Gerät eindeutig im System identifiziert. Durch den Plug & Play (PnP)-Manager wird jedem Geräteknoten in der Gerätestruktur eines Systems eine eindeutige Geräteinstanz-ID zugewiesen (siehe Eigenschaft eines Gerätes im Gerätemanager: „Device instance path“). Der Geräteinstanzpfad besteht aus der Device ID und der Geräteinstanz-ID (Beispiel: Device-ID\Geräteinstanz-ID). Der Pfad kann sich ändern, wenn ein Gerät an einen anderen Anschlussport verbunden wird. Der Geräteinstanzpfad ist spezifischer als die Geräte-ID.
Geräteeinrichtungsklassen (engl.: <i>Device setup classes</i> )	Die Geräteeinrichtungsklasse umfasst eine Sammlung von Geräten einer bestimmten Kategorie (z.B. Bluetooth-Geräten, Mäusen, Tastaturen) und kann in den Eigenschaften eines Gerätes im Gerätemanager unter „Class Guid“ eingesehen werden.

Nachfolgende Übersicht gibt einen Überblick, über die zugehörigen Gruppenrichtlinieneinstellung zur Konfiguration einer Erlaubt- und Blockierliste. Bei der Konfiguration ist zu beachten, dass eine konfigurierte Blockierliste immer Vorrang hat. Dabei ist zu berücksichtigen, dass die zur Identifizierung der genutzten Geräte Merkmale auch vorgetäuscht werden können.

 *Computer Configuration/Administrative Templates/System/Device Installation/Device Installation Restrictions*

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
Prevent installation of devices not described by other policy setting	„Enabled“ oder „Disabled“	Durch Aktivierung der Richtlinieneinstellung wird verhindert, dass Gerätetreiber von Geräten installiert werden können, die nicht explizit in der Erlaubtliste aufgeführt sind. Installationen (eingeschlossen Updates für Gerätetreiber) von Geräten, die nicht in der Geräteliste der Gruppenrichtlinieneinstellung: „Allow installation of devices that match any of these device IDs“, „Allow installation of devices that match any of these device instance IDs“ oder „Allow installation of devices for these device classes“, können nicht mehr durchgeführt werden.
Allow installation of devices that match any of these device IDs	„Enabled“ oder „Disabled“  <b>Options:</b> Allow installation of devices that match any of these device IDs • Angabe von Device-ID(s)	Die Konfiguration einer Erlaubtliste von Geräten durch Angabe der Geräte-ID, setzt voraus, dass die Richtlinieneinstellung „Prevent installation of devices not described by other policy setting“ aktiviert wurde. Alle Gerätetreiber zu Geräten, deren Geräte-ID (engl.: <i>Device ID</i> ) oder der kompatiblen ID (engl.: <i>Compatible ID</i> , in der Erlaubtliste enthalten sind, dürfen automatisch installiert werden, sobald das Gerät an den Client angeschlossen wurde.

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
Allow installation of devices that match any of these device instance IDs	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Allow installation of devices that match any of these device instance IDs</p> <ul style="list-style-type: none"> <li>• Angabe von Device Instance-ID(s)</li> </ul>	Die Konfiguration einer Erlaubtliste von Geräten durch Angabe der Geräteinstanz-ID, setzt voraus, dass die Richtlinieneinstellung „Prevent installation of devices not described by other policy setting“ aktiviert wurde. Alle Gerätetreiber zu Geräten, deren Geräteinstanz-ID (engl.: <i>Device instance path</i> ), in der Erlaubtliste enthalten sind, dürfen automatisch installiert werden, sobald das Gerät an den Client angeschlossen wurde.
Allow installation of devices using drivers that match these device setup classes	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Allow installation of devices using drivers for these device classes</p> <ul style="list-style-type: none"> <li>• Angabe von Device Classes</li> </ul>	Die Konfiguration einer Erlaubtliste von Geräten durch Angabe der Geräteinstallationsklasse, setzt voraus, dass die Richtlinieneinstellung „Prevent installation of devices not described by other policy setting“ aktiviert wurde. Mittels der Richtlinieneinstellung kann die Gerätetreiberinstallation von Geräten aus einer Geräteklasse erlaubt werden. In der Liste anzugeben sind die Geräteklassen. Eine Übersicht der Geräteklassen kann in der zugehörigen Dokumentation eingesehen werden <sup>101,102</sup> .
Prevent installation of devices that match any of these device IDs	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Prevent installation of devices using drivers for these device IDs</p> <ul style="list-style-type: none"> <li>• Angabe von Device -ID(s)</li> </ul>	Mit Hilfe der Gruppenrichtlinieneinstellung lassen sich Geräte IDs einer Blockierliste hinzufügen, deren Gerätetreiber nicht installiert werden. Die Richtlinieneinstellung hat Vorrang vor den anderen Richtlinieneinstellungen zum Erlauben der Installation von Geräten.
Prevent installation of devices that match any of these device instance IDs	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Prevent installation of devices using drivers for these device instance IDs</p> <ul style="list-style-type: none"> <li>• Angabe von Device Instance-ID(s)</li> </ul>	Mit Hilfe der Gruppenrichtlinieneinstellung lassen sich Geräteinstanzpfade von Geräten einer Blockierliste hinzufügen, deren Gerätetreiber nicht installiert werden. Die Richtlinieneinstellung hat Vorrang vor den anderen Richtlinieneinstellungen zum Erlauben der Installation von Geräten.
Prevent installation of devices using drivers that match these device setup classes	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Prevent installation of</p>	Mit Hilfe der Gruppenrichtlinieneinstellung lassen sich Gerätesetupklassen einer Blockierliste hinzufügen. Treiber von Plug and Play-Geräten der zugehörigen Klasse

<sup>101</sup> <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/system-defined-device-setup-classes-reserved-for-system-use>

<sup>102</sup> <https://learn.microsoft.com/en-us/windows-hardware/drivers/install/system-defined-device-setup-classes-available-to-vendors>

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
	devices using drivers for these device setup classes <ul style="list-style-type: none"> <li>• Angabe von Device Setup Classes</li> </ul>	werden nicht installiert. Die Richtlinieneinstellung hat Vorrang vor den anderen Richtlinieneinstellungen zum Erlauben der Installation von Geräten.

Neben der Möglichkeit zur Einschränkung der Gerätetreiberinstallation kann auch der Zugriff auf Wechseldatenträgerspeicher restriktiv konfiguriert werden. Ausnahmen für bestimmte Geräte können hierbei nicht getroffen werden:



Computer Configuration/Administrative Templates/System/Removable Storage Access

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
All Removable Storage classes: Deny all access	„Enabled“ (sofern der Zugriff auf Wechselmedien vollständig verhindert werden soll) oder „Disabled“	Es handelt sich um die restriktivste Einstellung, bei der ein Zugriff auf sämtliche Wechselmedien unterbunden wird.
CD and DVD: Deny execute access	„Enabled“ oder „Disabled“	CDs und DVDs sind heutzutage nur noch selten im Einsatz. Sofern ein expliziter Einsatz nicht vorgesehen ist, sollte ein möglicher Zugriff auf CDs/DVDs eingeschränkt werden.
CD and DVD: Deny read access		
CD and DVD: Deny write access		
Custom Classes: Deny execute access	„Enabled“ oder „Disabled“	Es kann eine Liste von GUIDs von Wechseldatenträgerklassen hinterlegt werden, auf welche die Richtlinie angewendet wird.
Custom Classes: Deny write access		
Floppy Drives: Deny execute access	„Enabled“ oder „Disabled“	Physische Diskettenlaufwerke sind heutzutage nicht mehr im Einsatz. Sofern ein expliziter Einsatz nicht vorgesehen ist, sollte ein möglicher Zugriff durch ein Diskettenlaufwerk eingeschränkt werden.
Floppy Drives: Deny read access		
Floppy Drives: Deny write access		
Removable Disks: Deny execute access	„Enabled“ oder „Disabled“	Die Richtlinie bezieht sich auf Wechseldatenträger (z. B. USB-Sticks).
Removable Disks: Deny read access		
Removable Disks: Deny write access		
Tape Drives: Deny execute access	„Enabled“ oder „Disabled“	Bandlaufwerke werden selten an Clients betrieben. Sofern ein Einsatz nicht vorgesehen ist, sollte ein möglicher Zugriff auf ein Bandlaufwerk eingeschränkt werden.
Tape Drives: Deny read access		
Tape Drives: Deny write access		
WPD Devices: Deny read access	„Enabled“ oder „Disabled“	Windows Portable Device (WPD) ermöglicht die Kommunikation mit angeschlossenen Medien- und Speichergeräten, wie bspw. Music-Player, Smartphones oder Kameras.
WPD Devices: Deny write access		

Um das Risiko von Angriffen über DMA ausgehend von angeschlossenen (externen) Geräten zu reduzieren, sollte Kernel DMA Protection genutzt werden:

### Kernel DMA Protection<sup>103</sup>




Computer Configuration/Administrative Templates/System/Kernel DMA Protection

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Enumeration policy for external devices incompatible with Kernel DMA Protection	<p><b>Enabled</b></p> <p><b>Options:</b> Enumeration Policy:</p> <ul style="list-style-type: none"> <li>Block all</li> </ul>	<p>Die Empfehlung entspricht dem vordefinierten Verhalten ab Windows 10 Version 1803, sofern die Hardwarevoraussetzungen erfüllt werden. Ggfs. sind in den Firmwareeinstellungen die Hyper-V Virtualisierungsfunktionen (IOMMU) zu aktivieren. Ob die die Kernel DMA Protection aktiviert ist, kann zur Laufzeit überprüft werden<sup>104</sup>.</p> <p>Der Kernel DMA (Direct Memory Access)-Schutz bietet keinen Schutz vor Angriffen die von 1394/FireWire-, PCMCIA-, ExpressCard-Geräten, dem CardBus oder weiteren Geräten ausgehen.</p> <p>Der Schutz besteht nur für DMA-Angriffe, die nach dem Ladevorgang des Betriebssystems von PCI/PCIe-Geräten, wie Thunderbolt 3 oder CFexpress) erfolgen.</p>

Sofern die technischen Voraussetzungen nicht gegeben sind, um die Gruppenrichtlinieneinstellung zur „Kernel DMA Protection“ umzusetzen, lässt sich mit nachfolgender Gruppenrichtlinieneinstellung verhindern, dass Gerätetreiber von SBP-2 und Thunderbolt Controllern installiert werden:

<sup>103</sup> <https://learn.microsoft.com/en-us/windows/security/information-protection/kernel-dma-protection-for-thunderbolt>

<sup>104</sup> <https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-kernel-dma-protection>

 Computer Configuration/Administrative Templates/System/Device Installation/Device Installation Restrictions

Gruppenrichtlinieneinstellung	Konfigurationsoptionen	Erläuterung
Prevent installation of devices that match any of these device IDs	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Prevent installation of devices that match any of these device IDs:</p> <ul style="list-style-type: none"> <li>• "PCI\CC_0C0A" als Eintrag der Liste hinzufügen. (Es handelt sich um Thunderbolt-Controller.)</li> </ul> <p><input checked="" type="checkbox"/> Also apply to matching devices that are already installed</p>	<p>Diese Einstellung verhindert eine Installation von Thunderbolt-Controllern und somit auch die Nutzung von USB Type-C. Auf Geräten, die die technischen Voraussetzungen erfüllen, sollte deshalb stattdessen der sog. „Kernel-DMA-Schutz“ verwendet werden.</p> <p>Hinweis: Vor allem relevant bei Nutzung einer Festplattenverschlüsselung ohne sog. „Prä-Boot-Authentisierung“.</p>
Prevent installation of devices using drivers that match these device setup classes	<p>„Enabled“ oder „Disabled“</p> <p><b>Options:</b> Prevent installation of devices that match any of these device setup classes:</p> <ul style="list-style-type: none"> <li>• {d48179be-ec20-11d1-b6b8-00c04fa372a7} {7ebefbc0-3200-11d2-b4c2-00a0C9697d07} {c06ff265-ae09-48f0-812c-16753d7cba83} {6bdd1fc1-810f-11d0-bec7-08002be2092f}</li> </ul> <p><input checked="" type="checkbox"/> Also apply to matching devices that are already installed</p>	<p>Diese Einstellung verhindert eine Installation von Gerätetreibern aus den Gerätesetupklassen SBP2-Protokoll, IEC-6188, AVC und IEEE1394 Host Bus Controller.</p> <p>Auf Geräten, die die technischen Voraussetzungen erfüllen, sollte deshalb stattdessen der sog. Kernel-DMA-Schutz verwendet werden.</p> <p>Hinweis: Vor allem relevant bei Nutzung einer Festplattenverschlüsselung ohne sog. „Prä-Boot-Authentisierung“.</p>

### SYS.2.1.A26 Schutz vor Ausnutzung von Schwachstellen in Anwendungen (S)

Der Funktionsumfang von Windows 10 umfasst einen voreingestellten Exploit-Schutz (engl.: *exploit protection*) mit unterschiedlichen Mitigationen, die einem Risiko der Ausnutzung von Schwachstellen entgegenwirken sollen. Die folgenden Mitigationen zum Schutz vor Ausnutzung von Schwachstellen in der Voreinstellung bereits voreingestellt aktiviert:

- Data Execution Prevention (DEP)
- Adress Space Layout Randomization (ASLR) (ohne Mandatory ASLR)
- Structured Exception Handling Overwrite Protection (SEHOP)

Für 64-Bit Anwendungen wird DEP im vordefinierten Verhalten durch das Betriebssystem aktiviert, auch wenn die entsprechende Linker-Option (/NXCOMPAT) nicht gesetzt wurde. Bei 32-Bit Anwendungen ohne



die Linker-Option ist DEP nicht aktiv. Damit Anwendungen durch ASLR geschützt werden, müssen die zugehörigen ausführbaren Dateien (Images) mit der Linker-Option (/DYNAMICBASE) kompiliert worden sein.

Die Mitigationen des (inzwischen nicht mehr weiterentwickelten) Enhanced Mitigation Experience Toolkit (EMET) wurden größtenteils als Exploit-Schutz mit in Windows 10 aufgenommen und integriert<sup>105</sup>. Eine Übersicht des in Windows 10 enthaltenen Schutzes sowie eine detaillierte Gegenüberstellung zu den Mitigationen in EMET kann auf den Webseiten von Microsoft abgerufen werden:

- <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/exploit-protection?view=o365-worldwide>

Der Exploit-Schutz in Windows 10 kann für das System („Systemeinstellungen“), aber auch für einzelne Programme („Programmeinstellungen“) individuell konfiguriert werden. Vordefiniert ist hier bereits nachfolgende Konfiguration der Systemeinstellungen:

Tabelle 15: Voreinstellungen des Exploit-Schutzes (Systemeinstellungen)

<b>Mitigation</b>	<b>Voreinstellung</b>	<b>Erläuterung</b>
<a href="#">Control Flow Guard (CFG)</a>	Use default (On)	Durch einen Schutz der Programmablaufsteuerung werden gültige Aufrufadressen einer Funktion in einer Erlaubtliste gepflegt. Bei indirekten Funktionsaufrufen (engl.: <i>indirect calls</i> ) muss das Aufrufziel in der Erlaubtliste enthalten sein. Stellt die Prüfung durch CFG einen nicht in der Erlaubtliste vorhandenes Aufrufziel fest, wird der Prozess durch Windows terminiert. CFG muss (sofern vom Compiler unterstützt) durch die Compiler- und Linker-Optionen explizit aktiviert werden, damit Anwendungen durch CFG geschützt werden können.
<a href="#">Data Execution Prevention (DEP)</a>	Use default (On)	Durch die Datenausführungsverhinderung kann das Betriebssystem bestimmte Speicherbereiche (engl.: <i>memory pages</i> ) des virtuellen Adressraums von Prozessen als nicht ausführbar markieren (engl.: <i>no execute</i> , kurz: <i>nx</i> ). Der Prozessor kann keinen Code innerhalb dieser markierten Regionen mehr ausführen.
<a href="#">Force randomization for images (Mandatory ASLR)</a>	Use default (Off)	Die zufällige Zuordnung von Speicheradressen im virtuellen Adressraum kann für Images (.DLL/.EXE), die in den Speicher geladen werden sollen, erzwungen werden. Hierdurch werden zufällige „Base“-Adressen vergeben. Voreingestellt wird Mandatory ASLR („Force-Relocate“) in Windows 10 allerdings nicht für alle Anwendungen erzwungen. Anwendungen müssen über die Compiler- und Linker-Optionen explizit den ASLR-Schutz in den Linker-Optionen aktiviert haben („/DYNAMICBASE“). Durch Aktivierung der Funktion „Mandatory ASLR“ über die Bedienoberfläche oder mittels des PowerShell Commands:

<sup>105</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/import-export-exploit-protection-emet-xml?view=o365-worldwide>

<b>Mitigation</b>	<b>Voreinstellung</b>	<b>Erläuterung</b>
		„Set-ProcessMitigation -System -Enable ForceRelocateImages“ können alle Anwendungen systemweit geschützt werden. Im Einzelfall sind die Auswirkungen auf die Kompatibilität und mögliche Beeinträchtigungen zu überprüfen. Alternativ kann die Mitigation auch anwendungsspezifisch konfiguriert werden.
<a href="#">Randomize memory allocations (Bottom-up ASLR)</a>	Use default (On)	Durch die zufällige Verwürfelung des Speicheradressraums werden Adressbereiche im Speicher zufällig an Prozesse zugewiesen. Hierdurch soll eine Vorhersage von Speicherbereichen, die durch Programme regelmäßig verwendet werden, erschwert bzw. praktisch nicht mehr möglich sein. Bottom-Up ASLR wird nur von Anwendungen genutzt, bei denen die Compiler- und Linker-Optionen explizit den ASLR-Schutz in den Linker-Optionen aktiviert haben („/DYNAMICBASE“). 64-Bit Anwendungen, die nicht mit dem ASLR Schutz (/DYNAMICBASE) kompiliert worden sind, sind in der Voreinstellung nicht mittels ASLR geschützt. In diesem Fall ist „Mandatory ASLR“ in den Systemeinstellungen oder anwendungsspezifisch zusätzlich zu aktivieren, damit derartige Anwendungen ebenfalls durch Bottom-Up ASLR geschützt werden <sup>106,107</sup> .
<a href="#">High-entropy ASLR</a>	Use default (On)	Damit der vollständige 64-Bit Adressraum von ASLR verwendet werden kann, sollten die entsprechenden Compiler und Linker-Optionen (/HIGHENTROPYVA und /LARGEADDRESSAWARE) aktiviert werden. Durch die höhere Entropie wird eine Vorhersage von verwendeten Speicheradressen erschwert. Die Mitigation setzt voraus, dass Bottom Up-ASLR aktiv ist.
<a href="#">Validate exception chains (SEHOP)</a>	Use default (On)	Durch die sog. „Structured Exception Handling Overwrite Protection (SEHOP)“ können Exploits mitigiert werden, die den strukturierten Ausnahmehandler ( <i>engl.</i> : Structured Exception Handler) überschreiben.
<a href="#">Validate heap integrity</a>	Use default (On)	Werden Manipulationen des Heap festgestellt, soll der betroffene Prozess terminiert werden.

Die Unterschiede bei der zur Auswahl stehenden Konfigurationsoptionen sollen nachfolgend erläutert werden:

<sup>106</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/exploit-protection-reference?view=o365-worldwide#randomize-memory-allocations-bottom-up-aslr>

<sup>107</sup> <https://msrc-blog.microsoft.com/2017/11/21/clarifying-the-behavior-of-mandatory-aslr/>

Tabelle 16: Möglichkeiten zur Konfiguration der systemweiten Mitigationen in den Systemeinstellungen

<b>Einstellung</b>	<b>Erläuterung</b>	<b>Empfehlung</b>
On by default	Die betroffene Mitigation des Exploit-Schutzes wird auch für Anwendungen aktiviert, welche nicht explizit mit den zugehörigen Linker- und Compiler-Einstellungen kompiliert wurden.	Die Einstellung „On by default“ sollte nur gewählt werden, wenn die Kompatibilität zu allen betroffenen Anwendungen sichergestellt wurde.
Off by default	Die betroffene Mitigation des Exploit-Schutzes wird für alle Anwendungen deaktiviert.	Die Einstellung „Off by default“ sollte nicht ausgewählt werden, da hierdurch Mitigationen des Exploit-Schutzes außer Kraft gesetzt werden.
Use default (On) / Use default (Off)	Voreingestellt wird für die System-weiten Einstellungen des Exploit-Schutzes die Konfiguration „Use default (On)“ bzw. „Use default (Off)“ verwendet. Dies bedeutet, dass das vordefinierte Verhalten umgesetzt wird.	Die Voreinstellung zu den jeweiligen Mitigationen des Exploit-Schutzes entsprechen den Empfehlungen von Microsoft und können grundsätzlich beibehalten werden. Abweichungen bzw. Ausnahmen sollten Anwendungs-spezifisch vorgenommen werden <sup>108</sup> . Hier können systemseitig vorgegebene Mitigationskonfigurationen auch überschrieben werden. Dies kann beispielsweise auf Anwendungen zutreffen, die einem erhöhten Risiko der Ausnutzung von Exploits unterliegen.

Im Folgenden sollen die Auswirkungen auf die Konfiguration (am Beispiel von ASLR, DEP und SEHOP in einer Matrix veranschaulicht werden:

Tabelle 17: Unterschiede der Konfigurationsoptionen im Hinblick auf ASLR, DEP und SEHOP

	<b>DEP oder SEHOP (nur für 64-Bit)</b>	<b>Linkeroption On</b>	<b>Linkeroption Off</b>
On by default	Funktion an	Funktion an	Funktion an
Off by default	Funktion an	Funktion aus	Funktion aus
Use default (On) / Use default (Off)	Funktion an	Funktion an	Funktion aus

**Linkeroption bedeutet hier:** /DYNAMICBASE (32/64-Bit), /NXCOMPAT (32-Bit) oder /SAFESEH (32-Bit)

In den Programmeinstellungen sind für Anwendungen vordefiniert bereits nachfolgende individuelle Konfigurationen vorgegeben:

Tabelle 18: Voreinstellungen des Exploit-Schutzes (Programmeinstellungen)

<b>Programm</b>	<b>Voreinstellung, welche die Systemeinstellungen überschreiben</b>
ExtExport.exe	Force randomization for images (Mandatory ASLR): On
ie4uinit.exe	Force randomization for images (Mandatory ASLR): On
ieinstal.exe	Force randomization for images (Mandatory ASLR): On
ielowutil.exe	Force randomization for images (Mandatory ASLR): On
ueUnatt.exe	Force randomization for images (Mandatory ASLR): On
ieexplore.exe	Force randomization for images (Mandatory ASLR): On

<sup>108</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide>

Programm	Voreinstellung, welche die Systemeinstellungen überschreiben
mscorsvw.exe	Disable extension points: On
msfeedssync.exe	Force randomization for images (Mandatory ASLR): On
mshta.exe	Force randomization for images (Mandatory ASLR): On
ngen.exe	Disable extension points: On
ngentask.exe	Disable extension points: On
PresentationHost.exe	Data Execution Prevention (DEP): On Force randomization for images (Mandatory ASLR): On Randomize memory allocations (Bottom-up ASLR): On Validate exception chains (SEHOP): On Validate heap integrity: On
PrintDialog.exe	Disable extension points: On
PrintIsolationHost.exe	keine
runtimebroker.exe	Disable extension points: On
splwow64.exe	keine
spoolsv.exe	keine
SystemSettings.exe	Disable extension points: On

Um zu prüfen, welche Prozessspeicherschutzmechanismen für einen Prozess einer ausgeführten Anwendung aktiviert sind, kann beispielsweise der Process Explorer aus der Sysinternals-Suite (nur für ASLR und DEP) herangezogen werden<sup>109</sup>. Eine Auswertung des PE-Headers von ausführbaren Dateien, beispielsweise mit Hilfe des dumpbin-Werkzeugs und dem /HEADERS-Parameter, das Teil der Visual Studio Entwicklungsumgebung ist, kann Aufschluss darüber geben, welche Linker-Optionen gesetzt wurden<sup>110</sup>.

Bei Anpassungsbedarf kann über die Einstellung zum Exploit-Schutz („Exploit protection“) für einzelne ausführbare Dateien von Anwendungen eine Konfiguration vorgenommen werden. Microsoft empfiehlt individuelle Anpassungen vor produktiven Einsatz in einer Test-/Referenzumgebung hinsichtlich ihrer Auswirkungen und Beeinträchtigungen zu testen.

Insbesondere Anwendungen, die Daten aus nicht vertrauenswürdigen Quellen verarbeiten oder mit erhöhten Rechten ausgeführt werden, sollten hinsichtlich eines ausreichenden Exploit-Schutzes geprüft werden. Sollten keine Informationen über die genutzten Linker- und Compiler-Einstellungen vorliegen, sind neben einer Risikobetrachtung ggfs. weitergehende Analysen durchzuführen.

Eine Konfigurationsänderung der Systemeinstellungen erfordert in der Regel einen Systemneustart. Bei Anpassung von Programmeinstellungen ist der Neustart der betroffenen Anwendung ausreichend. Administrative Berechtigungen sind für die Änderung der Konfiguration erforderlich. Änderungen an der Konfiguration zu DEP und SEHOP wirken sich nur auf 32-Bit Anwendungen aus.

Die System- und Programmeinstellungen des Exploit-Schutzes können mittels grafischer Bedienoberfläche über die Windows-Einstellungen aufgerufen und bei Bedarf angepasst werden:

⚙️ *Windows Settings* → *Update & Security* → *Windows Security* → *App & browser control* → *Exploit protection* → *Exploit protection settings*

Alternativ lässt sich die Konfiguration des Exploit-Schutzes mittels des PowerShell cmdlets „Set-ProcessMitigation“ und „Get-ProcessMitigation“ mit administrativen Rechten abrufen oder bearbeiten:

#### Systemeinstellungen auslesen:

```
PS C:\> Get-ProcessMitigation -System
```

<sup>109</sup> <https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer>

<sup>110</sup> <https://learn.microsoft.com/en-us/cpp/build/reference/dumpbin-command-line?view=msvc-170>

**Systemeinstellungen anpassen:**

```
PS C:\> Set-ProcessMitigation -System <-Enable oder -Disable> <Mitigation cmdlet parameter keyword111>
```

**Programmeinstellungen auslesen:**

```
PS C:\> Get-ProcessMitigation -Name Prozessname.exe
```

**Programmeinstellungen anpassen:**

```
PS C:\> Set-ProcessMitigation -Name Prozessname.exe <-Enable oder -Disable> <Mitigation cmdlet parameter keyword>
```


Abweichende Einstellungen von der vordefinierten Konfiguration sollten vorab auf einem Referenzsystem erstellt, getestet und über o.g. Konfigurationspfad in den Windows-Einstellungen in das XML-Format exportiert werden:

 *Windows Settings* → *Update & Security* → *Windows Security* → *App & browser control* → *Exploit protection* → *Exploit protection settings* → *Export settings*

Mit der PowerShell kann über den Parameter `-RegistryConfigFilePath` ein Export in das XML-Format durchgeführt werden:

```
PS C:\> Get-ProcessMitigation -RegistryConfigFilePath C:\ExploitConfigfile.xml
```

Die Konfiguration kann in domänenverwalteten Umgebungen über die Gruppenrichtlinie verteilt werden:

 *Computer Configuration/Administrative Templates/Windows Components/Microsoft Defender Exploit Guard/Exploit Protection*


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Use a common set of exploit protection settings	<p><b>Enabled</b></p> <p><b>Options:</b> Type the location (local path, UNC path, or URL) of the mitigation settings configuration XML file: z. B. \\Server\Share\ExploitConfig.xml</p>	<p>Damit durch die Richtlinieneinstellung eine Konfiguration von Maßnahmen zum Schutz von System und Anwendungen bereitgestellt werden kann, sind folgende Vorbereitungen vorzunehmen<sup>112</sup>:</p> <ul style="list-style-type: none"> <li>• Eine spezifische Konfiguration muss auf einem Referenzsystem, bspw. mit dem PowerShell cmdlet „Set-ProcessMitigation“ oder „ConvertTo-ProcessMitigationPolicy“ oder über das Windows Security Center vorgenommen werden.</li> <li>• Aus dieser Konfiguration lässt sich eine XML-Datei exportieren (z. B. über „Get-ProcessMitigation“ in der PowerShell</li> </ul>

<sup>111</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide#powershell>

<sup>112</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/import-export-exploit-protection-emet-xml?view=o365-worldwide>


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
		oder über das Windows Security Center (Export-Button) <ul style="list-style-type: none"> <li>Die XML-Datei muss entweder auf einer Freigabe abgelegt werden, zu der die Clients lesenden Zugriff haben oder lokal auf die Clients verteilt werden. Hat der Client keinen Zugriff auf die XML-Datei mit der Konfiguration, so wird die Einstellung nicht angewendet. Beispiele:                          C:\MitigationSettings\ExploitConfig.xml                          \\Server\Share\ExploitConfig.xml                          https://server/ExploitConfig.xml</li> </ul>

Neben der Bereitstellung einer Konfiguration mittels XML-Datei über o.g. Gruppenrichtlinie, kann alternativ durch die Gruppenrichtlinieneinstellung „Process Mitigation Options“ im Pfad:

 *Computer Configuration/Administrative Templates/System/Mitigation Options*

für einzelne Anwendungen individuell DEP, SEHOP oder ASLR definiert werden<sup>113</sup>. Hierzu wird eine Liste über Prozessnamen von Anwendungen gepflegt, denen über ein Bitmuster zusätzliche Mitigationen zugeordnet werden können. Die hier aufgenommenen Einträge finden sich im Anschluss auch in der Liste zu den Programmeinstellungen des Exploit-Schutzes wieder:

 *Windows Settings → Update & Security → Windows Security → App & browser control → Exploit protection settings → Program settings*

 *Computer Configuration/Administrative Templates/Windows Components/File Explorer*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off Data Execution Prevention for Explorer	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten: Die Aktivierung der Datenausführungsverhinderung (Data Execution Prevention) des Windows-Explorers bietet Schutzmechanismen, die eine Ausnutzung von möglichen Schwachstellen des Windows-Explorers unterbinden können. Hinweis: Auf 64-Bit Versionen von Windows 10 ist DEP und auch die Heap Termination aktiv und lassen sich über diese Richtlinie nicht deaktivieren <sup>114</sup> .
Turn off heap termination on corruption	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten: Die Heap Termination verhindert eine weitere Ausführung von Prozessen (Legacy Plug-Ins) des Windows-

<sup>113</sup> <https://learn.microsoft.com/en-us/windows/security/threat-protection/override-mitigation-options-for-app-related-security-policies>

<sup>114</sup> <https://devblogs.microsoft.com/oldnewthing/20170620-00/?p=96435>

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		Explorers, wenn die zugehörige Sitzung korrupt wird. Hinweis: Auf 64-Bit Versionen von Windows 10 ist DEP und auch die Heap Termination aktiv und lassen sich über diese Richtlinie nicht deaktivieren <sup>115</sup> .
Turn off shell protocol protected mode	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten: Der geschützte Modus für das Shell-Protokoll ist aktiviert. Durch diesen Modus werden Funktionen des Protokolls reduziert. Beispielsweise wird für Anwendungen, die das Protokoll verwenden, der Zugriff auf Verzeichnisse eingeschränkt.



Computer Configuration/Administrative Templates/MS Security Guide

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Enable Structured Exception Handling Overwrite Protection (SEHOP)	<b>Enabled</b>	Durch die Einstellung wird SEHOP auch für 32-bit Prozesse unabhängig der Linker-Optionen aktiviert.

### SYS.2.1.A27 Geregelte Außerbetriebnahme eines Clients (S)

Vor einer Außerbetriebnahme sollten die auf dem Client gespeicherten noch benötigten Daten gesichert werden. Hierzu sollten insbesondere die vordefinierten Speicherorte von Windows 10 bei der Datensicherung berücksichtigt werden. Anschließend kann der Client sowohl lokal, wie auch mit seiner Verknüpfung in einem Verzeichnisdienst gelöscht werden.

#### Datensicherung

Voreingestellt werden Konten-spezifische Daten in Windows 10 besonders unter den folgenden Speicherorten abgespeichert:

Tabelle 19: Voreingestellte Speicherorte in Windows 10 für Konten-spezifische Daten

<b>Daten</b>	<b>Umgebungsvariable</b>	<b>Standard-Verzeichnispfad</b>
Informationen und (Programm-) Dateien, die von allen Konten zugreifbar sind	%ALLUSERSPROFILE%	C:\ProgramData
Windows AppData Roaming: Einstellungen und Konten-spezifische Daten von Anwendungen, die bei einer Anmeldung an einem weiteren Gerät übertragen werden (erfordert Roaming-Profile)	%APPDATA%	C:\Users\*Kontoname*\AppData\Roaming
Windows AppData Local: Temporäre Einstellungen und (kontenspezifische) Daten, die nur lokal auf dem jeweiligen Gerät gespeichert werden.	%LOCALAPPDATA%	C:\Users\*Kontoname*\AppData\Local
Kontenprofilverzeichnis	%HOMEPATH%	C:\Users\*Kontoname*

<sup>115</sup> <https://devblogs.microsoft.com/oldnewthing/20170620-00/?p=96435>

 Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
<a href="#">Back up files and directories</a>	Es sollten nur Administrierende oder spezifische Dienstkonten bei Einsatz einer Backupsoftware in die Liste aufgenommen werden.	Konten, die über das Privileg <i>SeBackupPrivilege</i> verfügen, können auf Dateien, Verzeichnisse, Registry und andere Objekte zu Backupzwecken zugreifen. Dieses Privileg sorgt dafür, dass NTFS die folgenden Zugriffsberechtigungen für jede Datei und jeden Ordner unabhängig vom Security Descriptor setzt: READ_CONTROL, ACCESS_SYSTEM_SECURITY, FILE_GENERIC_READ, FILE_TRAVERSE
<a href="#">Restore files and directories</a>	Es sollten nur Administrierende oder spezifische Dienstkonten bei Einsatz einer Backupsoftware in die Liste aufgenommen werden.	Konten, die über das Privileg <i>SeRestorePrivilege</i> verfügen, können auf Dateien, Verzeichnisse, Registry und andere Objekte zu Wiederherstellungszwecken zugreifen. Dieses Privileg sorgt dafür, dass NTFS die folgenden Zugriffsberechtigungen für jede Datei und jeden Ordner unabhängig vom Security Descriptor setzt: WRITE_DAC, WRITE_OWNNER, ACCESS_SYSTEM_SECURITY, FILE_GENERIC_RIGHT, FILE_ADD_FILE, FILE_ADD_SUBDIRECTORY, DELETE

**Austragen des Clients aus Verzeichnisdiensten und Datenbanken**

Wenn ein Client außer Betrieb genommen wird, sollte auf dem Client die Mitgliedschaft zur Domäne ausgetragen werden. Hierdurch wird das zugehörige Objekt im Active Directory deaktiviert.

**Clientseitig kann dies mit administrativen Rechten erfolgen:**

 Windows-Settings/Account/Access Work or school → Disconnect

 Control Panel/System/Advanced system settings/Computer name, domain, and workgroup settings/Change settings → Computer Name → Change... → Member of → Workgroup (z. B. WORKGROUP)

**Serverseitig kann dies über die Verwaltung der „Active Directory Benutzer und Computer“ erfolgen:**

Server Manager → Tools → Active Directory Users and Computers

**Löschen der Daten auf dem IT-System**

Das Leeren des Papierkorbes in Windows 10 sowie das unwiderrufliche Löschen von Dateien (mit Hilfe der Tastenkombination Shift + ENTF) führt nicht dazu, dass derart gelöschte Dateien ganz oder teilweise wiederhergestellt werden können. Sensible Daten sollten daher vor Außerbetriebnahme mit geeigneten Werkzeugen und Methoden sicher gelöscht werden. Es ist empfehlenswert, den sicheren Löschvorgang über den gesamten Datenträger auszuführen.



## SYS.2.1.A34 Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten (S)

In Windows 10 werden Dienste und Programme, wie bei anderen Betriebssystemen auch, in Prozessen ausgeführt. Diese bieten bereits eine gewisse Kapselung des Prozesses zum Betriebssystem und anderen Prozessen an. Zusätzlich unterteilt Windows 10 die Prozesse anhand der Zugehörigkeit zum User- und Kernel-Mode und weist diesen weitere Zugriffsregeln zu. Dies wird auch als Integritätsstufe (engl.: *Integrity Level*) bezeichnet. Neben dieser Form der Isolierung gibt es weitergehende Kapselungsmöglichkeiten, die zusätzlich genutzt werden können.

### Einsatz des Microsoft Defender Credential Guard zum Schutz der Anmeldeinformationen

Der Virtual Secure Mode (VSM)<sup>116</sup> stellt Hypervisor-Funktionalitäten zur Verfügung, mit denen eine virtuelle Separierung von sicherheitskritischen Bereichen des Betriebssystems innerhalb von Windows 10 erfolgt. Dies wird im Folgenden als Secure-Kernel bezeichnet. Das Konzept von VSM sowie eine technische Analyse werden im Arbeitspaket 6 des SiSyPHuS Projekts erläutert<sup>117</sup>.

Es bestehen folgende Hardwarevoraussetzungen, damit Anmeldeinformationen unter Windows 10 mit Credential Guard geschützt werden können:

- Unterstützung der Virtualisierungs-basierten Sicherheit (VBS)
  - UEFI Firmware (Version 2.3.1.c oder höher) mit UEFI Secure Boot
  - 64-bit CPU
  - CPU Virtualisierungserweiterungen (Intel VT-x/AMD-v) mit Second Level Address Translation (SLAT)
  - Windows Hypervisor (Installation des Windows-Features „Hyper-V“ ist nicht erforderlich)

Zum Schutz der Anmeldeinformationen unter Windows 10 kann der Microsoft Defender Credential Guard aktiviert werden (siehe auch Kapitel 5.2 der Konfigurationsempfehlungen zur Härtung von Windows 10 des SiSyPHuS Win10 Projekts)<sup>118</sup>:



Computer Configuration/Administrative Templates/System/Device Guard

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn On Virtualization Based Security	<p><b>Enabled</b></p> <p><b>Options:</b></p> <ul style="list-style-type: none"> <li>• Select Platform Security Level: Secure Boot and DMA Protection</li> <li>• Virtualization Based Protection of Code Integrity: Enabled with UEFI lock</li> <li>• Require UEFI Memory Attributes Table: Disabled</li> </ul>	<p>Credential Guard verwendet VBS zum sicheren Speichern und Verwalten von Windows-Anmeldedaten von Domänenkonten im Secure-Kernel. Lokale Konten und Microsoft-Konten werden hiervon nicht erfasst<sup>119</sup>.</p> <p>Der Wert mit UEFI-Sperre aktiviert Credential Guard und weist Windows an, relevante Credential Guard-Konfigurationsparameter im sicheren Speicher des UEFIs abzulegen.</p>

<sup>116</sup> <https://learn.microsoft.com/en-us/virtualization/hyper-v-on-windows/tlfs/vsm>

<sup>117</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHuS/Workpackage6\\_Virtual\\_Secure\\_Mode.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHuS/Workpackage6_Virtual_Secure_Mode.pdf)

<sup>118</sup> [https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS\\_Win10/AP11/SiSyPHuS\\_AP11\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/AP11/SiSyPHuS_AP11_node.html)

<sup>119</sup> <https://learn.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-protection-limits>

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
	<ul style="list-style-type: none"> <li>Credential Guard Configuration: Enabled with UEFI lock</li> <li>Secure Launch Configuration: Enabled</li> </ul>	


**Schutz des Local Credential Store LSA (Protected Mode Light, PPL)<sup>120</sup>**

Falls der Microsoft Defender Credential Guard nicht eingesetzt werden soll, kann alternativ auch der LSA-Prozess durch den Protected Mode Light (PPL) zusätzlich geschützt werden. Der Prozess läuft dann weiterhin im normalen Kernel-Modus und nicht im Secure-Kernel.

Eine Konfiguration kann entweder durch nachfolgenden Registrierungsschlüssel oder die Gruppenrichtlinieneinstellung des MS Security Guides vorgenommen werden:

 HKLM\SYSTEM\CurrentControlSet\Control

Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)	Registry-Key	ValueName	Value (DWORD)
Run Lsa as PPL	Lsa	RunAsPPL	0x00000001

 Computer Configuration/Administrative Templates/MS Security Guide

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
LSA Protection	<b>Enabled</b>	<p>Die Local Security Authority (LSA), die im Local Security Authority Server Service (LSASS)-Prozess läuft, verarbeitet und validiert lokale und Netzanmeldungen. Ab Windows 8.1 stellt das Betriebssystem erweiterte Schutzmechanismen für den LSASS-Prozess bereit. Ein Teilaspekt dieser Schutzmechanismen ist, den LSASS-Prozess als geschützten Prozess auszuführen.</p> <p>Die Aktivierung des zusätzlichen LSA-Schutzes erhöht das Schutzniveau des LSASS-Prozesses in der Form, dass lediglich mit einer validen Microsoft-Signatur signierte LSA-Plug-Ins und -Treiber geladen werden können. Dies kann gängiger Schadsoftware erschweren, auf die im LSASS-Prozess vorgehaltenen kryptografischen Informationen zuzugreifen.</p> <p>Ist der zusätzliche LSA-Schutz aktiv, ist es nicht mehr möglich, den LSASS-Prozess oder vom Benutzenden definierte LSA-Plug-Ins zu debuggen.</p>

<sup>120</sup> <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection# to-disable-lsa-protection>

**Hinweise:**

- Vor Aktivierung sollten alle verwendeten LSA Plug-Ins identifiziert werden, um zu prüfen, ob diese von Microsoft signiert wurden. Anderenfalls werden die LSA Plug-Ins (z. B. für eine Smart Card Anmeldung) nicht mehr geladen.
- Bei Einsatz von Secure Boot muss für eine etwaige spätere Deaktivierung der LSA Protection das Tool „Local Security Authority (LSA) Protected Process Opt-out“ verwendet werden. Hierdurch wird die UEFI Variable gelöscht, ohne Secure Boot deaktivieren zu müssen (Bei der Deaktivierung von Secure Boot werden alle Secure Boot und UEFI-bezogenen Konfigurationen zurückgesetzt.)
- Um zu prüfen, ob LSA als Protected Process korrekt gestartet wurde, kann in der Ereignisanzeige unterhalb von „Windows Logs“ unter „System“ nach dem WinInit-Ereignis: „12: LSASS.exe was started as a protected process with level: 4“ gesucht werden.

**Microsoft Defender: Application Guard<sup>121</sup>**

Der Microsoft Defender Application Guard (MDAG) ist eine Sandboxlösung, die derzeit nur von Microsoft-eigenen Anwendungen wie dem Edge-Browser oder Microsoft Office genutzt werden kann. Eine Entscheidung, ob diese Funktion erforderlich ist, muss im Kontext der jeweiligen Anwendung getroffen werden. Für andere Anwendungen oder falls WDAG nicht verwendet werden soll, muss auf Lösungen von Drittanbietern zurückgegriffen werden. Bei erhöhtem Schutzbedarf sollte WDAG oder vergleichbare Drittanbieterprodukten genutzt werden.

**SYS.2.1.A43 Lokale Sicherheitsrichtlinien für Clients (S)**

Das Verhalten der Windows-Funktionen ist abhängig von deren Konfiguration, dabei kann das voreingestellte Verhalten sich durch Updates verändern. Daher sollten möglichst alle sicherheitsrelevanten Einstellungen explizit gesetzt werden, um wenigstens Änderungen des Standardverhaltens durch Nicht-Konfiguration (engl.: *Not Configured*) auszuschließen. Die Konfiguration kann dabei über Änderungen der Windows-Registry, der (lokalen) Gruppenrichtlinienverwaltung, der grafischen Oberfläche, von kommandozeilenbasierten Parametern (Command Line bzw. PowerShell) oder Konfigurationsdateien erfolgen. Es wird zwischen Einstellungen unterschieden, die das gesamte Betriebssystem betreffen und Einstellungen, die nur kontenspezifisch gelten. Änderungen an der „Computerkonfiguration“ kann nur mit administrativen Rechten durchgeführt werden, während die „Benutzerkonfiguration“ immer auch selbst durch Benutzende geändert werden kann. Durch Benutzende geänderte zentral konfigurierte Einstellungen werden bei der nächsten Aktualisierung der Richtlinien überschrieben. Wichtige sicherheitsrelevante Einstellungen sollten in der „Computerkonfiguration“ eingestellt werden, wenn es dazu auch eine Einstellungsmöglichkeit in der „Benutzerkonfiguration“ gibt.

Die Empfehlungen zu sicherheitsrelevanten Einstellungen aus Sicht von Microsoft werden zum einen über die veröffentlichte Dokumentation zu Windows 10 und zum anderen in Form sogenannter Microsoft Security Baselines mit konkreten Konfigurationsempfehlungen bereitgestellt:

- <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines>

Hierbei sollten diese als Ausgangspunkt für die Konfiguration genommen werden und nochmals kritisch hinterfragt werden, ob diese passend für die vorhandene IT-Infrastruktur sind. Dabei können auch weitere Quellen hinzugezogen werden, wie beispielsweise:

- **Windows 10 Security Technical Implementation Guide (STIG)**  
[https://www.stigviewer.com/stig/windows\\_10/](https://www.stigviewer.com/stig/windows_10/)

<sup>121</sup> <https://learn.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-application-guard/md-app-guard-overview>

- **CIS Microsoft Windows 10 Enterprise (Release 20H2 or older) Benchmark**  
[https://www.cisecurity.org/cis-benchmarks/#microsoft\\_windows\\_desktop](https://www.cisecurity.org/cis-benchmarks/#microsoft_windows_desktop)
- **Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10 (SiSyPHuS Win10)**  
[https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS\\_Win10/SiSyPHuS\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/SiSyPHuS_node.html)

Mit Hilfe von Werkzeugen (wie bspw. dem PolicyAnalyzer als Bestandteil des Microsoft Security Compliance Toolkits) können Einstellungen eines Systems mit den Security Baselines oder selbst definierten Richtlinienvorlagen abgeglichen werden.

In den Empfehlungen von Microsoft werden einige Konfigurationen für Komponenten empfohlen, die Anforderungen betreffen, welche beim allgemeinen Client nicht in den Basis- oder Standard-Anforderungen enthalten sind. Falls es daher in den Empfehlungen von Microsoft korrespondierende Anforderungen zum erhöhten Schutzbedarf gibt, sind diese wie Basis- oder Standard-Anforderungen zu behandeln. Dies betrifft u. a. die Windows Firewall (bezogen auf SYS2.1.A31) und den Credential Guard (bezogen auf SYS2.2.3.A23).

### **SYS.2.1.A44 Verwaltung der Sicherheitsrichtlinien von Clients (S)**

Viele Windows Clients werden in Windows-Domänen über Active Directory Domain Services (ADDS) verwaltet. Über diese werden die Konfigurationen in Form von Gruppenrichtlinien an die Clients verteilt (siehe 3.2.2 Zentrale Gruppenrichtlinienverwaltung). Die Gruppenrichtlinien können dabei zentral in den Verwaltungskonsolen des ADDS konfiguriert werden.

Alternativ können Windows Clients sowohl in Windows-Domänen als auch Workgroups über Desired State Configuration (DSC) konfiguriert werden<sup>122</sup>.

## **4.3 Anforderungen bei erhöhtem Schutzbedarf**

### **SYS.2.1.A31 Einrichtung lokaler Paketfilter (H)**

In den Umsetzungshinweisen zum Baustein SYS.2.1 Allgemeiner Client werden bereits allgemeine Strategien vorgestellt, mit der die Paketfilter-Regeln implementiert werden können. Es sollte die dort beschriebene restriktive Strategie gewählt werden und hierdurch nur explizit erlaubte Verbindungen und Kommunikation zugelassen werden.

Die in Windows 10 enthaltene Windows Firewall ist ein hostbasierter Paketfilter und voreingestellt aktiviert. Ein- und ausgehende Datenpakete werden nach Status und dem Kontext der Netzverbindung gefiltert. In den voreingestellten Regeln sind ausgehende Verbindungen zunächst erlaubt und eingehende Verbindungen werden blockiert. Eine Protokollierung ist nicht konfiguriert. Diese Konfiguration umfasst daher nicht eine strikte Filterung auf Basis einer Erlaubt-Liste.

Die Windows Firewall unterscheidet zwischen drei Profilen, die je nach zugeordnetem Profil der Netz-schnittstellen angewendet werden:

---

<sup>122</sup> <https://learn.microsoft.com/de-de/powershell/scripting/dsc/getting-started/wingettingstarted?view=powershell-7.1>

## Windows Firewall: Profile

*Domänenprofil (engl.: Domain Profile)*

**Das Domain Profile wird auf Netze angewendet, zu denen der Client eine authentifizierte Verbindung zu einem Domänencontroller herstellen kann.**

*Privates Profil (engl.: Private Profile)*

**Das Private Profile wird verwendet, wenn keine Verbindung zu einem Domänencontroller besteht und das angeschlossene Netz als privat klassifiziert wurde.**

*Öffentliches Profil (engl.: Public Profile)*

**Für (noch) nicht identifizierten Netze wird zunächst das öffentliche Profil (Public Profile) verwendet. Dies trifft beispielsweise auf WLAN-Verbindungen zu.**

Windows 10 ordnet ein Netzprofil automatisch zu, wenn eine neue Verbindung zu einem Netz über eine Netzchnittstelle hergestellt wird. Zur Identifikation von Netzen wird der Dienst „Network Level Awareness (NLA)“ verwendet. Netze, die von Windows anhand von Merkmalen nicht eindeutig identifiziert werden können, werden als nicht identifiziertes Netz behandelt. Häufig ist dies der Fall, wenn für die Netzverbindung kein Gateway angegeben wurde.

Beim erstmaligen Verbindungsaufbau zu einem identifizierten Netz erfolgt eine grafisch geführte Konfigurationsabfrage des sog. „Network Location Wizards“, ob der Client durch andere Geräte im Netz erkannt werden soll. Bei positiver Bestätigung wird das private Netzprofil verwendet. Anderenfalls verbleibt das Profil zunächst öffentlich. Ein Wechsel zwischen den Profilen „Private“ und „Public“ kann über die Windows-Einstellungen auch von Konten aus der Gruppe „Users“ vorgenommen werden. Um dies zu verhindern, kann mit Hilfe folgender Richtlinieneinstellung für Domänenkonten eine Einschränkung getroffen werden:



Computer Configuration/Administrative Templates/Network/Network Connections

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Require domain users to elevate when setting a network's location	<b>Enabled</b>	Durch die Richtlinieneinstellung ist ein Wechsel der Netzprofile nur noch für Konten mit administrativen Berechtigungen möglich.

Ist Windows 10 Teil einer domänenverwalteten Umgebung und besteht eine aktive Verbindung zum Domänennetz, wird der Netzverbindung durch Network Level Awareness das Profil „Domain“ der Netzchnittstelle fest zugeordnet. In diesem Fall können mit Konten aus der Gruppe „Users“ nicht zu den Profilen „Private“ oder „Public“ gewechselt werden. Wird die Verbindung zu einem anderen Netz hergestellt, das nicht Teil der Domäne ist, kann zwischen den Profilen „Public“ und „Private“ gewählt werden.

In den Gruppenrichtlinien zum „Network List Manager“ sollte konfiguriert werden, ob die Konten der Gruppe „Users“ bei identifizierten Netzen zum „Private“-Profil wechseln dürfen. Im Fall von Verbindungen in öffentlichen Netzen (z. B. WLAN-Hotspots) besteht bei Auswahl des privaten Profils das Risiko, dass unberechtigte Zugriffe auf freigegebene Dienste erfolgen könnten.



Computer Configuration/Administrative Templates/Windows Settings/Security Settings/Network List Manager Policies

Für jedes Firewall-Profil kann das Verhalten für ein- und ausgehende Verbindungen festgelegt werden:

- **Inbound connections**

- **Block (default)**

Alle eingehenden Verbindungen, für die im Regelwerk keine Regel existiert, die solche Verbindungen explizit zulässt, werden blockiert.

- **Block all connections**  
Alle eingehenden Verbindungen werden blockiert, selbst wenn im Regelwerk eine Regel existiert, die eine solche Verbindung zulassen würde.
- **Allow**  
Alle eingehenden Verbindungen werden zugelassen, sofern im Regelwerk keine Regel existiert, die eine solche Verbindung blockieren würde.
- **Outbound connections**
  - **Block**  
Alle ausgehenden Verbindungen werden blockiert, sofern im Regelwerk keine Regel existiert, die eine solche Verbindung zulassen würde.
  - **Allow (default)**  
Alle ausgehenden Verbindungen werden erlaubt, sofern im Regelwerk keine Regel existiert, die eine solche Verbindung explizit blockieren würde.

### Windows Firewall: Regelarten für ein- oder ausgehende Verbindungen

Über die Microsoft Defender Firewall mit erweiterter Sicherheit kann ein Wizard zur Erstellung von Regeln verwendet werden. Regeln können auch über die PowerShell erzeugt werden. Es stehen nachfolgende Regelarten zur Auswahl:

- **Program**  
Durch Angabe des Pfades zu einer Anwendung können Regeln erstellt werden, die sich nur auf die Verbindungen einer bestimmten Anwendung beschränken sollen. (Anmerkung: Die entsprechenden Anwendungen müssen hierzu Windows Sockets (Winsock) verwenden, um durch eine Programm-Regel der Windows Firewall erfasst werden zu können).
- **Port**  
Durch Port-Regeln können für die Protokolle TCP und UDP einzelne Ports oder Portbereiche angegeben werden, auf die sich die Regelaktion beschränken soll.
- **Predefined**  
In Windows 10 sind vordefinierte Firewall-Regeln enthalten, die eine Konfiguration der Firewall unterstützen sollen. Vordefinierte Regeln sollten hinsichtlich ihres Umfangs überprüft werden und ggfs. angepasst oder reduziert werden.
- **Custom**  
Durch selbstdefinierte Regeln können die bereits genannten Arten direkt im Wizard kombiniert werden. Nachträglich können alle Konfigurationsmöglichkeiten der Regeln umfassend über die Regeleigenschaften bearbeitet werden. Die Kombination von Regelarten, wie beispielsweise von Programmen und Port, kann dazu verwendet werden, um einem bestimmten Programm die Kommunikation nur über die festgelegten Ports zu ermöglichen.

Für die Konfiguration der Windows-Firewall Regeln werden durch Microsoft Best-Practice-Empfehlungen sowie Anleitungen bereitgestellt:

- <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring>
- Erstellen einer Programm- oder Dienst-Regel, die sich auf eingehende Verbindungen bezieht:  
<https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-inbound-program-or-service-rule>
- Erstellen einer Programm- oder Dienst-Regel, die sich auf ausgehende Verbindungen bezieht:  
<https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-outbound-program-or-service-rule>

## Auswirkungen durch Regeln auf ein- und ausgehende Verbindungen

Auswirkungen von Regeln, welche auf die ausgehenden Verbindungen angewendet werden:

Tabelle 20: Auswirkungen der Firewallregeln (Matrix) auf ausgehende Verbindungen

	<i>Allow the connection</i>	<i>Block the connection</i>	<i>Disabled rule</i>	<i>No rule</i>
Outbound: Block	✓	✗	✗	✗
Outbound: Allow	✓	✗	✓	✓

✓ Verbindung wird zugelassen, ✗ Verbindung wird blockiert

Auswirkungen von Regeln, welche auf die eingehenden Verbindungen angewendet werden:

Tabelle 21: Auswirkungen von Allow-/ Block-Regeln (Matrix) auf eingehende Verbindungen

	<i>Allow the connection</i>	<i>Block the connection</i>	<i>Disabled rule</i>	<i>No rule</i>
Inbound: Block (default)	✓	✗	✗	✗
Inbound: Allow	✓	✗	✓	✓
Inbound: Block all connections	✗	✗	✗	✗

✓ Verbindung wird zugelassen, ✗ Verbindung wird blockiert

Windows 10 nutzt die Funktionen der Windows Firewall teilweise auch, um Konfigurationen für netzfähige Windows-Funktionen und Anwendungen umzusetzen. Hierbei handelt es sich ausschließlich um Erlaubt-Regeln. Beispielsweise nutzt die Datei- und Druckerfreigabe die Windows-Firewall, um das „Ein- und Abschalten“ der Funktion umzusetzen. Dabei führt ein „Einschalten“ zum Aktivieren der bereits angelegten Firewallregeln. Beim „Abschalten“ werden diese Regeln wieder deaktiviert. Deaktivierte Regeln werden in der Windows Firewall so behandelt, als wären sie nicht angelegt. Nur wenn eine Regel aktiviert ist (grüner Kontrollhaken vor der Regel), wird sie auch berücksichtigt.

Bei der Installation netzfähiger Anwendungen und Dienste kann durch Entwickler eine Liste von Protokoll- und Portinformationen angegeben werden, die für eine Netzkommunikation erforderlich sind. Durch die Installation mit administrativen Rechten können Firewallregeln auch automatisiert in der Windows Firewall angelegt werden. Üblicherweise wird während der Installationsroutine ein Dialogfenster angezeigt, die eine Bestätigung für das Anlegen der zugehörigen Regeln einfordert.

Für den normalen Schutzbedarf ist die voreingestellte Firewallkonfiguration ausreichend. Die Firewallkonfiguration der Microsoft Defender Firewall mit erweiterter Sicherheit lässt sich über den folgenden Gruppenrichtlinienpfad aufrufen und sollte hinsichtlich der vorkonfigurierten Regeln überprüft werden. Hierbei kann es nach Aussage in der Dokumentation von Microsoft zu ungewollten Änderungen der Standardkonfiguration kommen, da netzabhängige Funktionen ggfs. die Firewallinstellungen nachträglich anpassen können<sup>123</sup>.



*Computer Configuration/Administrative Templates/Windows Settings/Security Settings/Windows Firewall with Advanced Security/*

Bei nicht-domänenverwalteten Clients kann die Firewallkonfiguration entweder über die lokale Gruppenrichtlinie oder über das Windows Firewall Snap-In in der Microsoft Management Console (MMC) aufgerufen werden. Eine Konfiguration ist ebenfalls mit der PowerShell möglich.


Für den höheren Schutzbedarf sollten diese vordefinierten Konfigurationen kritisch geprüft werden. Die Regeln der eingehenden Verbindungen sollten auf das erforderliche Maß reduziert werden. Ausgangspunkt

<sup>123</sup> <https://support.microsoft.com/en-us/topic/preventing-smb-traffic-from-lateral-connections-and-entering-or-leaving-the-network-c0541db7-2244-0dce-18fd-14a3ddeb282a>


hierfür könnte eine Kommunikationsmatrix des Clients darstellen. Hierzu können alle vordefinierten Regeln bis auf solche Verbindungen, die explizit benötigt werden, gelöscht oder deaktiviert werden. Ein Löschen hat den Vorteil, dass die Konfiguration übersichtlich wird. Dagegen können ggfs. zukünftige Konfigurationen dazu führen, dass gelöschte Regeln wieder neu angelegt werden. Hierzu können die vordefinierten Regeln einfach aus einer Liste wieder ausgewählt werden.

Durch Aktualisierung können Netzregeln wieder verändert werden, daher sollten in regelmäßigen Abständen die Netzregeln der Windows Firewall überprüft werden.


Außerdem sollten die Einstellungen für ausgehende Verbindungen auf „blockiert“ geändert werden:

-  *Computer Configuration/Administrative Templates/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Public Profile/State*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Windows Firewall: Public: Outbound connections	Block	Ausgehende Verbindungen werden grundsätzlich blockiert. Ausnahmen bestehen für aktive Regeln, die eine Verbindung explizit zulassen.


-  *Computer Configuration/Administrative Templates/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Private Profile/State*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Windows Firewall: Private: Outbound connections	Block	Ausgehende Verbindungen werden grundsätzlich blockiert. Ausnahmen bestehen für aktive Regeln, die eine Verbindung explizit zulassen.


-  *Computer Configuration/Administrative Templates/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Domain Profile/State*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Windows Firewall: Domain: Outbound connections	Block	Ausgehende Verbindungen werden grundsätzlich blockiert. Ausnahmen bestehen für aktive Regeln, die eine Verbindung explizit zulassen.

Darüber hinaus empfiehlt Microsoft die Protokollierung zu aktivieren und die Speichergröße der Logdateien anzupassen:

-  *Computer Configuration/Administrative Templates/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Public Profile/Logging*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>
Size limit	16384 KB
Log dropped packets	Yes
Log successful connections	Yes

-  *Computer Configuration/Administrative Templates/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Private Profile/Logging*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>
Size limit	16384 KB
Log dropped packets	Yes
Log successful connections	Yes





Computer Configuration/Administrative Templates/Windows Settings/Security Settings/Windows Firewall with Advanced Security/Domain Profile/Logging

Gruppenrichtlinieneinstellung	Empfehlung
Size limit	16384 KB
Log dropped packets	Yes
Log successful connections	Yes

### SYS.2.1.A32 Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits (H)

Mit dem in Windows 10 enthaltenen Exploit-Schutz werden wesentliche Maßnahmen zum Schutz vor Exploits getroffen. Empfehlungen zu DEP, ASLR und SEHOP werden zur Anforderung SYS.2.1.A26 Schutz vor Ausnutzung in Anwendungen beschrieben. Weitergehende Prozessmitigationen dokumentiert Microsoft unter:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/customize-exploit-protection?view=o365-worldwide>

Beim erhöhtem Schutzbedarf können die beschriebenen weiteren Maßnahmen zur Verhinderung der Ausnutzung von Schwachstellen zusätzlich genutzt werden.

Darüber hinaus kann auch die Verarbeitung von Daten, die potenziell Exploits beinhalten, eingeschränkt werden oder besonders auffälliges Verhalten zusätzlich protokolliert werden. Hinweise können den Umsetzungshinweisen zum Baustein SYS.2.1 Allgemeiner Client entnommen werden (siehe SYS.2.1.M32 Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits).

### SYS.2.1.A33 Einsatz von Ausführungskontrolle (H)

Die Einführung einer Ausführungskontrolle für Anwendungen bedarf über die technische Umsetzung hinaus ein umfangreiches Konzept, in dem die Bedingungen und Konditionen organisatorisch festgelegt werden:

- Gestaltung und Beschreibung einheitlicher Prozesse für die
  - Erstellung und die Verwaltung der Regelwerke
  - Erfassung ausführbarer Dateien von neuer Software und -updates
  - Qualitätssicherung (Test- und Evaluierung der Regelwerke)
- Integration der Anwendungsausführungskontroll-Prozesse in die Softwareverteilung
- Festlegen von Kriterien für die Einsatzstrategie der zur Verfügung stehenden Regelarten (z. B. Herausgeber (zertifikatsbasiert), Dateihash, Pfad) und die zur Umsetzung notwendigen Schritte, z. B.:
  - bei zertifikatsbasierten Regeln müssen die vertrauenswürdigen Herausgebendenzertifikate ermittelt und verteilt werden
  - bei der Nutzung von Dateiprüfsummen muss für jede ausführbare Datei der Dateihash für die Konfiguration erstellt werden
  - bei Pfadregeln müssen alle Pfade ermittelt und in die Konfiguration aufgenommen werden, in denen ausführbare Dateien liegen, die ausgeführt werden sollen. Als Ausgangspunkte können hier die Default-Regeln von Windows verwendet werden.

Das Risiko, dass unerwünschte ausführbare Dateien ausgeführt werden, hängt stark von der gewählten Konfiguration ab. Während bei einem Dateihash immer individuell genau die gewünschte Datei freigegeben wird, führen Regeln auf der Basis von Ausstellerzertifikaten dazu, dass neben der gewünschten Datei auch alle anderen Dateien, die mit dem gleichen Zertifikat signiert wurden, freigegeben werden. Dies kann dazu führen, dass hierunter auch unerwünschte Dateien sind. Falls diese bekannt sind, können diese auch mit

Sperrregeln gesperrt werden oder aber ergänzende Parameter für die Freigabe der gewünschten Dateien hinzugefügt werden. Daher empfiehlt es sich aus Sicht der Informationssicherheit, möglichst die niedrigste Ebene der Zertifikatskette zu verwenden. Allerdings führt dies möglicherweise dazu, dass die Konfiguration der Zertifikate häufiger angepasst werden muss. Bei der Nutzung von Pfadregeln sollte geprüft werden, ob alle Dateien unterhalb des Pfades erlaubt werden sollen. Außerdem sollten kritisch die Dateisystemberechtigungen für die jeweiligen Konten geprüft werden, um zu verhindern, dass mittels vorhandener Schreibrechte ausführbare Dateien innerhalb der freigegebenen Pfade anlegen und somit ausführen können.

Die technische Umsetzung in Windows 10 ist abhängig von der eingesetzten Windows 10 Edition. AppLocker und Microsoft Defender Application Control (MDAC) stehen erst mit der Enterprise Edition zur Verfügung. Daneben existieren noch die Software Restriction Policies (SRP), die allerdings nicht mit dem Funktionsumfang von AppLocker/ MDAC vergleichbar sind und voreingestellt nicht nach dem Erlaubt-Prinzip konfiguriert sind. Ebenfalls wurden die SRP mit Windows 10 Version 22H2 von Microsoft abgekündigt und können ab dieser Version nicht mehr verwendet werden.

### a Microsoft AppLocker<sup>124</sup>

#### 1. Schritt: Autostart des System-Dienstes „Application Identity Service“ festlegen



Computer Configuration/Windows Settings/Security Settings/System Services

Dienst	Startup type	Erläuterung
Application Identity (AppIDSvc)	Automatic	Der AppIDSvc wird von AppLocker benötigt, um Software zu identifizieren und die Regelwerke anzuwenden. Der Dienst muss automatisch gestartet werden, da sonst die Applocker-Regeln nicht angewendet werden.

#### 2. Anlegen von Standardregeln in AppLocker



Computer Configuration/Windows Settings/Security Settings/Application Control Policies/AppLocker

Im Kontextmenü zu den Regelwerken in AppLocker kann das jeweilige Standardregelwerk angelegt werden („Create Default Rules“). Hierbei handelt es sich um nachfolgende Pfadregeln:

- Executable Rules
  - %PROGRAMFILES%\\*
  - %WINDIR%\\*
  - \* (nur für Administrationskonten)
- Windows Installer Rules
  - Alle signierten Installer-Dateien
  - Alle Installer-Dateien im Pfad %SYSTEMDRIVE%\Windows\Installer
  - Alle Installer-Dateien (nur Administrationskonten)
- Script Rules
  - Alle Skriptdateien im Verzeichnis %PROGRAMFILES%\\*
  - Alle Skriptdateien im Verzeichnis %WINDIR%\\*
  - Alle Skriptdateien (nur für Administrationskonten)

<sup>124</sup> <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>

- Packaged App Rules
  - Alle signierten Appx-Packages
- 3. **Optional: Einschließen von Programmbibliotheken (.DLL)**  
 Über das Kontextmenü von AppLocker kann in den erweiterten Eigenschaften auch die Überwachung von Programmbibliotheken (.DLL) miteinbezogen werden. Nach entsprechender Aktivierung wird AppLocker um ein weiteres Regelwerk „DLL Rules“ erweitert. Auch hier können folgende Standardregeln angelegt werden:
  - Microsoft Windows DLLs (Pfadregel %WINDIR%)
  - DLLs im Verzeichnis %PROGRAMFILES%
  - Alle DLLs (nur für Administrationskonten)
- 4. **Aktivieren von AppLocker und Erzwingen oder Überwachen der Regelwerke**  
 Über das Kontextmenü von AppLocker kann in den Eigenschaften unter „Enforcement“ für die einzelnen Regelarten festgelegt werden, ob diese durch AppLocker kontrolliert oder nur überwacht werden. Damit AppLocker nur erlaubte Software anhand der Regeln in den Regelwerken ausführt, ist hier „Enforce rules“ für die Regelwerke zu wählen.
- 5. **Neustart der Clients**  
 Windows 10 Clients, auf denen erstmals die AppLocker Richtlinien angewendet werden, müssen neu gestartet werden.

#### b Microsoft Defender Application Control (WDAC)<sup>125</sup>

##### 1. Schritt: Erstellen eines Regelwerks (engl.: *Code Integrity Policy*, CIP)

**PowerShell:** Durchführung eines System-Scans zur Erfassung der Softwareherausgeber von ausführbaren Dateien (mit alternativer Erfassung der Prüfsummen)

```
PS C:\> New-CIPolicy -FilePath Policy-Audit.xml -Level FilePublisher -Fallback Hash -UserPEs
```

**PowerShell:** Entfernen der Option „Audit Mode Enabled“

```
PS C:\> Set-RuleOption -FilePath Policy-Audit.xml -Option 3 -Delete
```

**PowerShell:** Konvertierung des Ergebnisses in eine Binärdatei

```
PS C:\> ConvertFrom-CIPolicy -XmlFilePath Policy-Audit.xml -BinaryFilePath Policy-Enforced.p7b
```

##### 2. Schritt: Bereitstellung der Code Integrity Policy (CIP)



Computer Configuration/Administrative Templates/System/Device Guard

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Deploy Windows Defender Application Control	Code Integrity Policy file path: [FILEPATH]	Angabe eines Dateipfades zur „Policy-Enforced.p7b“ im Netz oder lokal


<sup>125</sup> <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/select-types-of-rules-to-create>

Ausführliche Informationen zur Konfiguration von WDAC werden in den Konfigurationsempfehlungen zur Härtung von Windows 10 mit Bordmitteln im Kapitel 5.1 „Microsoft Defender Application Control“<sup>126</sup> des SiSyPHuS-Projektes bereitgestellt.

### c Microsoft Software Restriction Policies (SRP)<sup>127</sup>


#### 1. Schritt: Anlegen der Software Restriction Policies

(Kontextmenü: New Software Restriction Policies)

 Computer Configuration/Windows Settings/Security Settings/Software Restriction Policies

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Enforcement Properties	Apply software restriction policies to the following: „All software files“ Apply software restriction policies to the following users: „All users“ When applying software restriction policies: “Ignore certificate rules”	Durch die Gruppenrichtlinieneinstellung wird festgelegt, ob SRP auf alle Dateien von Software angewendet werden oder Dateien von Programmbibliotheken (z. B. DLL) ausgenommen werden. Darüber hinaus wird festgelegt, ob SRP nur auf Konten der Gruppe „Users“ oder auch der Gruppe „Administrators“ angewendet wird. Für eine restriktivere Konfiguration können zusätzlich Programmbibliotheken mit in die Überprüfung eingeschlossen werden. Sofern Software nicht mittels Hashwerten oder anhand von Dateipfaden identifiziert wird, können zusätzlich Zertifikatsregeln erzwungen werden. In diesem Fall ist die Richtlinie „Trusted Publishers Properties“ zu berücksichtigen.

#### 2. Schritt: Auswahl von zu prüfenden Dateien anhand des Dateityps

 Computer Configuration/Windows Settings/Security Settings/Software Restriction Policies/

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Designated File Type	Zur bestehenden Liste können ggfs. noch weitere Dateitypen, wie z. B. PowerShell-Skriptdateien, hinzugefügt werden.	Hier können Dateitypen ausgewählt werden, die durch SRP kontrolliert werden sollen.

<sup>126</sup> <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Cyber-Security/SiSyPHuS/AP10/Logging-Configuration-Guideline.pdf?blob=publicationFile&v=5>

<sup>127</sup> <https://learn.microsoft.com/en-us/windows-server/identity/software-restriction-policies/software-restriction-policies>

### 3. Schritt: Auswahl eines Standardsicherheitsniveaus (Security Level)



Computer Configuration/Windows Settings/Security Settings/Software Restriction Policies/Security Levels

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Disallowed	Für eine Anwendungsrestriktion nach dem „Erlaubt“-Prinzip sollte diese Einstellung mit „Set as Default“ als Standardsicherheitsniveau gewählt werden.	Es handelt sich um das „Erlaubt“-Prinzip, nach dem nur explizit in der Liste aufgeführte Software ausgeführt werden darf.
Basic User	Das Security Level „Basic User“ sollte nicht verwendet werden.	Die Funktion wird in SRP nicht mehr unterstützt.
Unrestricted	Bei einem „Erlaubt“-Prinzip sollte die Einstellung nicht konfiguriert werden.	Voreingestelltes Sicherheitsniveau. Es handelt sich um das „Blockieren“-Prinzip, nach dem explizit aufgeführte Software nicht ausgeführt werden darf.

### 4. Schritt: Überprüfen und ggfs. Anpassen des Standardregelwerks sowie Ergänzung weiterer Einträge (falls erforderlich)

Bei den Standardregeln sind bereits zwei Einträge (Pfadregeln) mit dem Sicherheitsniveau „Unrestricted“ vorhanden: Software aus den Verzeichnissen %SYSTEMROOT% und %PROGRAMFILES% dürfen ausgeführt werden. Die bereits angelegten Standardregeln erlauben bei ausgewähltem Standardsicherheitsniveau „Disallowed“ jedoch keine Ausführung von x86-Anwendungen, sodass die erforderlichen Verzeichnisse, z.B. %SYSTEMROOT%\system32 und %PROGRAMFILES(x86)%, noch hinzugefügt werden sollten.

Unterhalb des Gruppenrichtlinienpfades können über das Kontextmenü weitere Einträge zu folgenden Regelarten hinzugefügt werden. Diese stellen jeweils Ausnahmen zum empfohlenen Standardsicherheitsniveau dar und müssen für ein „Erlaubt“-Prinzip mit Sicherheitslevel „Unrestricted“ gewählt werden:



Computer Configuration/Windows Settings/Security Settings/Software Restriction Policies/Additional Rules

- Certificate Rule
- Hash Rule
- Network Zone Rule
- Path Rule

Weiterführende Informationen zu den Software Restriction Policies (SRP) können über die Dokumentation abgerufen werden<sup>128</sup>.

### SYS.2.1.A35 Aktive Verwaltung der Wurzelzertifikate (H)

Mechanismen im Betriebssystem und von Anwendungen überprüfen die Vertrauenswürdigkeit von Softwarekomponenten anhand der vorliegenden Zertifikatsketten (Zertifikatsvalidierung). Gelangen gestohlene Zertifikate in die Hände von möglichen Angreiferinnen und Angreifern oder stellen Zertifizierungsstellen ohne eine sorgfältige Überprüfung großzügig Zertifikate aus, so lassen sich diese missbräuchlich einsetzen,

<sup>128</sup> <https://learn.microsoft.com/en-us/windows-server/identity/software-restriction-policies/software-restriction-policies>


um beispielsweise Schadsoftware zu signieren und eine Vertrauenswürdigkeit gegenüber dem Betriebssystem und Benutzenden vorzutäuschen<sup>129,130</sup>.

Für die organisatorische Umsetzung dieser Anforderung sollte ein umfangreiches Konzept erstellt werden, das den Umgang mit nachfolgenden Aspekten und Fragestellungen beschreibt:


- Etablierung einheitlicher Prozesse für das Zertifikatsmanagement
- Berücksichtigung bei Request for Changes (RFCs) im Change-Management
- Kriterien, die vertrauenswürdige (Wurzel-)Zertifikate und Herausgeber festlegen (siehe auch Technische Richtlinie TR-03116-4<sup>131</sup>)
- Welche (Wurzel-) Zertifikate sind vertrauenswürdig und sollen in der Certificate Trust List (CTL) bereitgestellt werden?
- Wie erfolgt die Verwaltung von Zertifikatssperrlisten?
- Online Certificate Status Protocol (OCSP)
- Certificate Revocation List (CRL)

Zur aktiven Verwaltung der Wurzelzertifikate in Windows 10 lässt sich an nachfolgender technischer Vorgehensweise orientieren:

**Schritt 1:** Deaktivierung des automatischen Nachladens von Wurzelzertifikaten

 Computer Configuration/Administrative Templates/System/Internet Communication Management/Internet communication settings

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off Automatic Root Certificates Update	<b>Enabled</b>	Durch die Deaktivierung der automatischen Updates der Wurzelzertifikate werden die Windows Update Webseiten durch Windows 10 nicht kontaktiert, um zu prüfen, ob Microsoft ein CA-Zertifikat zur Liste der vertrauenswürdigen Zertifizierungsstellen zur Verfügung stellt.

 HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\

Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)	Registry-Key	ValueName	Value
CTL RootDirUrl	AutoUpdate	RootDirUrl	URL (HTTP) oder Dateipfad
CTL Synchronization	AutoUpdate	DisallowedCertLastSyncTime	1

**Schritt 2:** Erzeugung der Liste der vertrauenswürdigen (Wurzel-)Zertifikate (Certificate Trust List, CTL)

```
C:\> Certutil -generateSSTFromWU WURoots.sst
```

**Schritt 3:** Anpassung der Liste der vertrauenswürdigen (Wurzel-) Zertifikate (Certificate Trust List, CTL), sodass nur noch die für den Betrieb benötigten Zertifikate enthalten sind.

<sup>129</sup> MITRE ATT&CK Technique T1587.002 (Develop Capabilities: Code Signing Certificates) <https://attack.mitre.org/techniques/T1587/002>

<sup>130</sup> MITRE ATT&CK Technique T1553 (Subvert Trust Controls) <https://attack.mitre.org/techniques/T1553/>

<sup>131</sup> <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.html>


Der Zertifikatsmanager wird geöffnet, um die gewünschten Zertifikate auszuwählen und anschließend in eine .sst-Datei zu exportieren:

```
C:\> explorer.exe WURoots.sst
```

Zur Überprüfung und der Dokumentation der im UEFI-Zertifikatsspeicher enthaltenen Zertifikate können die Empfehlungen zur Anforderung [SYS.2.1.A36 Selbstverwalteter Einsatz von SecureBoot und TPM \(H\)](#) (Schritt 1-4) herangezogen werden.

### Sperren von einzelnen nicht-vertrauenswürdigen Zertifikaten

Das Sperren einzelner, nicht-vertrauenswürdiger Zertifikate kann in nachfolgendem Gruppenrichtlinienpfad durch Aufnahme der entsprechenden Zertifikate vorgenommen werden:

 *Computer Configuration/Administrative Templates/Windows Settings/Public Key Policies/Untrusted Certificates*

## SYS.2.1.A36 Selbstverwalteter Einsatz von SecureBoot und TPM (H)

Auf UEFI-basierten Systemen schützt die Funktion Secure Boot die Integrität des Bootvorgangs. Die hierfür benötigten Schlüsselspeicher können selbst verwaltet werden. Hierzu können die folgenden Schritte genutzt werden:

1. Einrichtung eines USB-Bootsticks (UEFI Shell und Efitools), falls die Firmware nicht bereits die benötigten Werkzeuge zur Verwaltung der UEFI Schlüsseldatenbanken bereitstellt.

- 1.1. Starten von DISKPART (Windows-Kommandozeilenwerkzeug)

```
C:\> diskpart
DISKPART>
```

- 1.2. Übersicht der angeschlossenen Laufwerke ausgeben lassen

```
DISKPART> list disk
```

- 1.3. Auswahl des angeschlossenen USB-Sticks (hier: Disk 1)

```
DISKPART> sel disk 1
Disk 1 is now the selected disk.
```

- 1.4. Löschen der Informationen zur Konfiguration

```
DISKPART> clean
DiskPart succeeded in cleaning the disk.
```

- 1.5. Erstellen einer primären Partition

```
DISKPART> create part primary
DiskPart succeeded in creating the specified partition.
```

- 1.6. Auswahl der Partition 1

```
DISKPART> sel part 1
Partition 1 is now the selected partition.
```

- 1.7. Formatieren des Laufwerkes (Dateisystem: FAT32)

```
DISKPART> format quick fs=fat32 label="Bootstick"
DiskPart successfully formatted the volume.
```

- 1.8. Die Partition als aktiv markieren

```
DISKPART> active
DiskPart marked the current partition as active.
```

## 1.9. Zuweisen eines Laufwerksbuchstaben

```
DISKPART> assign
DiskPart successfully assigned the drive letter or mount point.
```

## 1.10. Diskpart beenden

```
DISKPART> exit
Leaving DiskPart...
```

## 1.11. Anlegen der Verzeichnisstruktur auf dem Bootstick (hier: Laufwerk F:)

```
C:\> mkdir F:\efi
C:\> mkdir F:\efi\boot
C:\> mkdir F:\efi\tools
```

## 1.12. Herunterladen und Entpacken des EFI Dev Kit (Edk):

<https://sourceforge.net/projects/efidevkit/files/Releases/Official%20Releases/Edk%201.06.zip/download>

1.13. Aus dem Verzeichnis *Edk/Other/Maintained/Application/UefiShell/bin/x64* die Datei *Shell\_Full.efi* in das Unterverzeichnis *efi/boot* auf den USB-Bootstick kopieren und umbenennen in *bootx64.efi*

```
C:\> copy Edk\Other\Maintained\Application\UefiShell\bin\x64\Shell_Full.efi F:\efi\boot\bootx64.efi
```

## 1.14. Herunterladen der Efitools (Version: 1.9.2 – Autor: James Bottomley):

<https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git>

1.15. Entpacken der Efitools (*efitools-1.9.2.tar.gz*) in das Unterverzeichnis *efi/tools* auf dem USB-Bootstick (Hinweis: Der Windows-Explorer kann das Format *tar.gz* nicht entpacken. Es ist ein Drittanbieter-Werkzeug erforderlich.)

```
C:\> xcopy /s efitools-1.9.2.tar.gz\efitools-1.9.2.tar\efitools-1.9.2 F:\efi\tools
```

## 1.16. Den Anweisungen der README folgen und die efitools in einer Linux-Umgebung kompilieren (Hinweis: Neben Entwicklungswerkzeugen sind dafür u. a. Perl, Perl-Modul: Slurp und gnu-efi erforderlich). Alternativ bieten viele Linux-Distributionen bereits kompilierte Pakete (efitools) an, die direkt genutzt werden können.

## 2. Konfigurieren der Firmware zum Starten der EFI Shell

Die nachfolgenden Schritte sind abhängig vom Gerät bzw. Herstellenden. Damit die EFI Shell gestartet werden kann, muss Secure Boot ausgeschaltet werden, da die zu startenden Dateien unsigned sind.

## 2.1. In die Firmwareeinstellungen booten

## 2.2. Setzen eines Supervisor-Passworts (i. d. R. unter „Security“)

## 2.3. Ausschalten von „Secure Boot“ (i. d. R. unter „Security\Boot“)

## 2.4. Einschalten des Bootmenüs „F12 Boot Menu“ (o. ä., i. d. R. unter „Main“)

## 2.5. Beenden der Konfiguration und Speichern der Einstellungen (i. d. R. „Exit and Save changes“)

## 3. Starten der EFI Shell

## 3.1. Bootmenü öffnen (i. d. R. im obigen Beispiel über Taste F12)

## 3.2. Auswahl „USB HDD“, damit vom USB-Bootstick gebootet werden kann

## 3.3. Es sollte die EFI Shell gestartet sein:

```
EFI Shell version 2.70 [0.4000]
Current running mode 1.1.2
[...]
Shell>
```



1. Sichern des vorhandenen Schlüsselmaterials, um die enthaltenen Zertifikate im UEFI Zertifikatsspeicher zu prüfen.

**Hinweis:** Möglicherweise ist die Tastaturbelegung in einem fremdsprachigen Layout (geräteabhängig) konfiguriert.

- 3.4. Auswahl des USB-Bootsticks

Anhand der aufgelisteten „Device Mapping Table“ der EFI-Shell lässt sich der Bezeichner des Gerätes entnehmen (hier: fs0, es kann aber auch anders lauten, z. B. fs1)

```
Shell> fs0:
```

- 3.5. Wechsel in das Verzeichnis efi/tools

```
fs0:\> cd efi
fs0:\efi> cd tools
```

- 3.6. Starten des KeyTools

```
fs0:\efi\tools> KeyTool.efi
```

- 3.7. Auswahl „Save Keys“ und Auswahl des USB-Bootsticks. Die folgenden Schlüssel werden in das Root-Verzeichnis gesichert: \PK.esl, \KEK.esl, \db.esl, \dbx.esl.

- 3.8. Beenden des KeyTools im Hauptmenü mit der Auswahl „Exit“

- 3.9. Beenden der der EFI-Shell

```
fs0:\efi\tools> exit
```

- 3.10. Der USB-Bootstick kann entfernt werden

- 3.11. Konvertierung des Schlüsselmaterials unter Linux mit Hilfe der efitools in das standardisierte X509-Zertifikatsformat (DER)

```
root@linux:/ sig-list-to-certs PK.esl PK
root@linux:/ sig-list-to-certs KEK.esl KEK
root@linux:/ sig-list-to-certs db.esl db
root@linux:/ sig-list-to-certs dbx.esl dbx
```

- 3.12. Optional: Konvertierung des Schlüsselmaterials unter Linux mit Hilfe von OpenSSL in eine direkt lesbare Textform

```
root@linux:/ openssl x509 -text -inform DER -in PK-0.der > PK-0.txt
root@linux:/ openssl x509 -text -inform DER -in KEK-0.der > KEK-0.txt
root@linux:/ openssl x509 -text -inform DER -in KEK-1.der > KEK-1.txt
root@linux:/ openssl x509 -text -inform DER -in db-0.der > db-0.txt
root@linux:/ openssl x509 -text -inform DER -in db-1.der > db-1.txt
root@linux:/ openssl x509 -text -inform DER -in db-2.der > db-2.txt
root@linux:/ for f in dbx* ; do printf "$f\t" ; cat "$f" | xxd -c 256 -p -l 256 ; done > dbx.txt
```

Anmerkung: Die Einträge der UEFI Revocation List (DBX) über die Signaturen der zurückgerufenen bzw. gesperrten UEFI-Module werden als einzelne Dateien (Schema: dbx-[0..n].hash) extrahiert, die jeweils eine SHA256-Prüfsumme beinhalten. Einfachheitshalber werden die Inhalte der Dateien (ASCII) hexadezimal umgewandelt und als Liste in die Datei dbx.txt zusammengeführt.

- 3.13. Sichtung der enthaltenen Zertifikate (in der Textform oder mit Hilfe eines Zertifikatbetrachters). Hierbei sollte anhand von öffentlich verfügbaren Informationen geprüft werden, ob die Zertifikate

von den angegebenen Ausstellern stammen. Für Microsoft sind diese Informationen über die Dokumentation zu Windows abrufbar<sup>132</sup>. Außerdem sollte geprüft werden, ob die in KEK und DB enthaltenen Zertifikate überhaupt benötigt werden. Falls die Verwaltung der Schlüsselspeicher an das Betriebssystem ausgelagert wird, muss das Zertifikat des Betriebssystemherausgebenden (Microsoft Corporation KEK CA 2011) im KEK vorhanden sein:

- Microsoft Corporation KEK CA 2011<sup>133</sup>  
SHA1-Zertifikatshash: 31 59 0b fd 89 c9 d7 4e d0 87 df ac 66 33 4b 39 31 25 4b 30.  
SignatureOwner GUID: {77fa9abd-0359-4d32-bd60-28f4e78f784b}

Die Prüfsummen der zurückgerufenen bzw. gesperrten UEFI Module können teilweise über die Dokumentation recherchiert werden (sog. „Update to Revoke Non-compliant UEFI Modules“).

- <https://learn.microsoft.com/en-us/security-updates/securityadvisories/2014/2871690>
- <https://learn.microsoft.com/en-us/security-updates/securityadvisories/2014/2962824>

## 1. Selbstverwaltetes Schlüsselmaterial erzeugen und signieren

Anmerkungen: Die erzeugten geheimen Schlüssel sollten vor missbräuchlicher Verwendung entsprechend geschützt werden. Sie sollten zudem im Backupkonzept berücksichtigt werden.

### 3.14. Erzeugen eines eigenen Plattform Keys (PK)

```
root@linux:/ openssl req -new -x509 -newkey rsa:2048 -subj "/CN=OWN Platform Key 2021/" -keyout PK.key -out PK.crt -days 3650 -nodes -sha256
```

### 3.15. Erzeugen eines eigenen Key Exchange Keys (KEK)

```
root@linux:/ openssl req -new -x509 -newkey rsa:2048 -subj "/CN=OWN KEK 2021/" -keyout KEK.key -out KEK.crt -days 3650 -nodes -sha256
```

### 3.16. Erzeugen eines eigenen Schlüssels für die Authorized Database (db)

```
root@linux:/ openssl req -new -x509 -newkey rsa:2048 -subj "/CN=OWN UEFI 2021/" -keyout db.key -out db.crt -days 3650 -nodes -sha256
```

### 3.17. Konvertierung des X509-Zertifikats des PK in eine EFI-Signature-List-Datei

```
root@linux:/ cert-to-efi-sig-list -g [selbsterzeugte GUID] PK.crt PK.esl
```

### 3.18. Konvertierung des X509-Zertifikats des KEK in eine EFI-Signature-List-Datei

```
root@linux:/ cert-to-efi-sig-list -g [selbsterzeugte GUID] KEK.crt KEK.esl
```

### 3.19. Konvertierung des X509-Zertifikats der DB in eine EFI-Signature-List-Datei

```
root@linux:/ cert-to-efi-sig-list -g [selbsterzeugte GUID] db.crt db.esl
```

### 3.20. Signieren der EFI-Signaturliste (PK)

```
root@linux:/ sign-efi-sig-list -k PK.key -c PK.crt PK PK.esl PK.auth
```

### 3.21. Signieren der EFI-Signaturliste (KEK)

```
root@linux:/ sign-efi-sig-list -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

### 3.22. Umbenennen der in Schritt 4.4 gesicherten *db.esl* zu *db\_old.esl*

### 3.23. Neu erzeugte *db.esl* aus Schritt 5.6 umbenennen zu *db\_new.esl*

### 3.24. Zusammenführen der beiden Listen

<sup>132</sup> <https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-secure-boot-key-creation-and-management-guidance>

<sup>133</sup> <https://go.microsoft.com/fwlink/?LinkId=321185>

```
root@linux:/ cat db_old.esl db_new.esl > db.esl
```

### 3.25. Signieren der EFI-Signaturlisten

```
root@linux:/ sign-efi-sig-list -k KEK.key -c KEK.crt db db.esl db.auth
```

### 3.26. Kopieren der Dateien *PK.auth*, *KEK.esl* und *db.esl* auf den USB-Bootstick

## 4. Kopieren der Schlüssel in den Schlüsselspeicher

Durch das Kopieren der Schlüssel in die Schlüsselspeicher wird die Konfiguration angewendet.

### 4.1. In die Firmwareeinstellungen booten

### 4.2. Einschalten von „Secure Boot“ (i. d. R. unter „Security\Boot“)

### 4.3. Löschen aller Secure Boot Einstellungen (i. d. R. unter „Security\Boot“)

### 4.4. Beenden der Konfiguration und Speichern der Einstellungen (i. d. R. „Exit and Save changes“)

### 4.5. Bootmenü öffnen (i. d. R. im obigen Beispiel Taste F12)

### 4.6. Auswahl „USB HDD“, damit vom USB-Bootstick gebootet wird

### 4.7. Es sollte die EFI Shell gestartet sein

```
EFI Shell version 2.70 [0.4000]
Current running mode 1.1.2
[...]
Shell>
```

### 4.8. Auswahl des USB-Bootsticks (anhand der aufgelisteten Device Mapping Table in der EFI-Shell lässt sich der Bezeichner des Gerätes entnehmen; hier: fs0, es kann aber auch anders lauten, z. B. fs1)

```
Shell> fs0:
```

### 4.9. Wechsel in das Verzeichnis efi/tools

```
fs0:\> cd efi
fs0:\efi> cd tools
```

### 4.10. Starten des KeyTools

```
fs0:\efi\tools> KeyTool.efi
```

### 4.11. Zunächst KEK.esl bzw. db.esl als KEK bzw. db durch Auswahl einfügen („Replace Key“)

### 4.12. Anschließend PK.auth als PK durch Auswahl einfügen („Replace Key“)

### 4.13. Reset-Befehl durchführen, um den Rechner neu zu starten

## 5. Ausrollen der "Secure Boot"-Konfiguration auf beliebigen Rechnern

### 5.1. In die Firmwareeinstellungen booten

### 5.2. Einschalten des Bootmenüs „F12 Boot Menu“ (o. ä., i. d. R. i. d. R. unter „Main“)

### 5.3. Setzen eines Supervisor-Passworts (i. d. R. unter „Security“)

### 5.4. Löschen aller Secure Boot Einstellungen (i. d. R. unter „Security\Boot“)

### 5.5. Beenden der Konfiguration und Speichern der Einstellungen (i. d. R. „Exit and Save changes“)

### 5.6. Bootmenü öffnen (im obigen Beispiel i. d. R. Taste F12)

### 5.7. Auswahl „USB HDD“, damit vom USB-Bootstick gebootet wird

5.8. Es sollte die EFI Shell gestartet sein:

```
EFI Shell version 2.70 [0.4000]
Current running mode 1.1.2
[...]
Shell>
```

5.9. Auswahl des USB-Bootsticks (anhand der aufgelisteten Device Mapping Table in der EFI-Shell lässt sich der Bezeichner des Gerätes entnehmen; hier: fs0, es kann aber auch anders lauten, z. B. fs1)

```
Shell> fs0:
```

5.10. Wechsel in das Verzeichnis efi/tools

```
fs0:\> cd efi
fs0:\efi> cd tools
```

5.11. Starten des KeyTools

```
fs0:\efi\tools> KeyTool.efi
```

5.12. Zunächst KEK.esl bzw. db.esl als KEK bzw. db durch Auswahl einfügen („Replace Key“)

5.13. Anschließend PK.auth als PK durch Auswahl einfügen („Replace Key“)

5.14. Reset-Befehl durchführen, um den Rechner neu zu starten


**Hinweis: Auswirkungen bei Firmware-Update**

Bei einem Firmware-Update können ggfs. alle Schlüssel mit voreingestellten Schlüsselmaterial überschrieben werden. In diesem Fall muss das selbstverwaltete Schlüsselmaterial erneut eingespielt werden.

Neben der hier gezeigten Anleitung für die Konfiguration gibt es im Internet noch viele weitere Hilfestellungen zum selbstverwalteten Einsatz von Secure Boot, z. B. auch von der NSA<sup>134</sup>, welche zum Teil auch andere Werkzeuge verwenden, wie PowerShell-Skripte.

**Umgang mit dem Zugriff auf Firmwarevariablen**

Sofern Firmwarevariablen aus Windows 10 heraus konfiguriert werden sollen, sind hierfür entsprechende Berechtigungen erforderlich:

 Computer Configuration/Security Settings/User Rights Assignments


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Modify firmware environment values	<b>Administrators</b> oder <b>keine Einträge</b>	Mit dem Privileg dürfen Umgebungsvariablen in der Firmware verändert werden, die im NVRAM persistent gespeichert sind. Wenn von Seiten des Betriebssystems die Firmwarekonfiguration verwaltet werden soll, dann wird empfohlen, die Einstellung auf dem voreingestellten Wert „Administrators“ zu belassen. Wird die Funktion nicht benötigt, sollte das Privileg an keine Gruppe bzw. Konto vergeben sein.

<sup>134</sup> UEFI Secure Boot Customization (<https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF>)

## SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung (H)

Windows 10 bietet als Möglichkeit eines zweiten Faktors für die Authentisierung die Nutzung von Smart Cards an:

### Zwei-Faktor Authentisierung mit Smart Cards

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options/

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Interactive logon: Require Windows Hello for Business or smart card	<b>Enabled</b>	Mit aktivierter Einstellung ist eine Anmeldung an Windows 10 nur noch mittels Smart Card möglich. Voraussetzung: Für den Benutzenden ist eine Smart Card eingerichtet worden.
Interactive logon: Smart card removal behavior	Lock Workstation	Wird die Smart Card des Benutzenden aus dem Smart-Card-Leser gezogen, wird die aktive Sitzung des angemeldeten Kontos automatisch gesperrt. Die Funktion sollte verwendet werden, wenn Benutzende angehalten werden, ihre Smart Card nicht unbeaufsichtigt zu lassen.

Windows 10 bietet als alternatives Anmeldeverfahren die Kombination von mehreren Anmeldeinformationen zur lokalen Anmeldung an, welches Microsoft als „mehrstufiges Entsperren“ bezeichnet:

### Mehrstufiges Entsperren in Windows 10

Beim mehrstufigen Entsperren in Windows 10 (engl.: *Multi-factor Unlock*) ist eine Anmeldung oder das Entsperren des Geräts erst nach erfolgreicher Eingabe bzw. Vorlage der Authentifizierungsmerkmale möglich. Das Kontenpasswort oder eine Smart Card kann als Fallback-Option gewählt werden, falls das mehrstufige Entsperren fehlschlägt. Optional können sowohl die Anmeldung mit Kontenpasswort als auch mit Smart Card deaktiviert werden, sodass eine Anmeldung nur noch über das mehrstufige Entsperren möglich ist<sup>135</sup>. Unabhängig davon, dass das Sicherheitsniveau für netzbasierte Angriffe dem Niveau des Kennworts oder der Smart Card entspricht, können die Anmeldeinformationen nicht an einem anderen Gerät zur (missbräuchlichen) Anmeldung verwendet werden. Zusätzlich sind die biometrischen Merkmale Fingerabdruck und Gesichtserkennung im Vergleich zu Kennwörtern nicht einfach reproduzierbar.

### In Windows 10 unterstützte Anmeldeinformationsanbieter (engl.: *Credential Provider*)

Tabelle 22: Unterstützte Anmeldeinformationsanbieter in Windows 10

Credential Provider	GUID
PIN	{D6886603-9D2F-4EB2-B667-1971041FA96B}
Fingerabdruck	{BEC09223-B018-416D-A0AC-523971B639F5}
Gesichtserkennung	{8AF662BF-65A0-4D0A-A540-A338A999D36F}
Verbindung zu einem als vertrauenswürdig festgelegten und in Reichweite befindlichen Mobiltelefon oder einem Netz (Trusted Signal)	{27FBDB57-B613-4AF2-9D7E-4FA7A66C21AD}

<sup>135</sup> <https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/feature-multifactor-unlock>


 Computer Configuration/Administrative Templates/Windows Components/Windows Hello for Business

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Configure device unlock factors	<b>Enabled</b>	In der Standardkonfiguration ist die Richtlinie nicht aktiviert („Not Configured“). Wird die Richtlinie aktiviert, ist für den ersten Faktor PIN, Fingerabdruck oder Gesichtserkennung voreingestellt. Für den zweiten Faktor ist das vertrauenswürdige Signal (Trusted Signal) und PIN konfiguriert. Für das vertrauenswürdige Signal ist eine XML-Datei zu erstellen. Die Möglichkeiten zur Konfiguration können der Dokumentation entnommen werden.

### SYS.2.1.A38 Einbindung in die Notfallplanung (H)

Die Aspekte zur Systemwiederherstellung und Datensicherung werden unter den Empfehlungen zur Anforderung [CON.3.A5 Regelmäßige Datensicherung](#) beschrieben.

Bei Netzstörungen bietet Windows 10 die Möglichkeit, Daten von Dateifreigaben weiterhin zu verwenden, indem sie regelmäßig lokal gespiegelt werden<sup>136</sup>. Eine Möglichkeit, die mit Windows 10 mit ausgeliefert wird, sind die „Offline Files“:


 Computer Configuration/Administrative Templates/Network/Offline Files

Gruppenrichtlinieneinstellung	Konfigurationsoptionen	Erläuterung
Allow or Disallow use of the Offline Files feature	„Enabled“ oder „Disabled“	Die Funktion muss durch einen Administrierenden einmalig aktiviert werden. Wird die Richtlinieneinstellung explizit auf „Enabled“ gesetzt, können „Offline Files“ verwendet werden. Konten der Gruppe „Users“ können die Funktion nicht selbstständig deaktivieren.

Benutzende können über den Aufruf des Kontextmenüs einer Netzfreigabe in einem verbundenen Netzwerk über die Schaltfläche „Always available offline“ für Dateien und Verzeichnisse festlegen, ob diese offline synchronisiert werden. Handelt es sich beim Fileserver um einen Windows Server, ist serverseitig das Zwischenspeichern von Freigaben zu aktivieren („Allow caching of share“ in den Einstellungen der Dateifreigabe). Synchronisationskonflikte können entstehen, wenn Dateien durch mehrere Benutzende gleichzeitig Offline bearbeitet werden.

Die Offline-Dateien werden clientseitig voreingestellt im Verzeichnis „C:\Windows\CSC“ gespeichert.

Die Konfiguration der Offline Files kann über die Gruppenrichtlinieneinstellungen in den nachfolgenden Pfaden der „Computer Configuration“ oder in der „User Configuration“ vorgenommen werden:

 Computer Configuration/Administrative Templates/Network/Offline Files

 User Configuration/Administrative Templates/Network/Offline Files

<sup>136</sup> <https://learn.microsoft.com/en-us/windows-server/storage/folder-redirection/folder-redirection-rup-overview>

### SYS.2.1.A39 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] (H)

Ein IT-System mit Windows 10 kann entweder über einen verbauten bzw. wechselbaren Akku (i. d. R. mobiles Gerät) verfügen oder als stationäres System (i. d. R. Desktop) an eine unterbrechungsfreie Stromversorgung angeschlossen werden. Hierbei sollte sichergestellt werden, dass Windows 10 über einen kritisch niedrigen Batteriezustand rechtzeitig informiert wird, um entsprechende Maßnahmen zu treffen, die einem Datenverlust vorbeugen. Bei integriertem Akku, wie es bei Notebooks der Fall ist, kann Windows 10 den Batteriestand über die Hardwareschnittstelle unmittelbar erfassen. Bei kleineren USV-Geräten wird häufig eine Treibersoftware mitgeliefert, mit welcher Windows 10 über eine USB-Verbindung zum Batterie- und Betriebszustand der USV informiert wird. Bei größeren USV-Anlagen, die den Notstrom zentral für mehrere Geräte bereitstellen, sollte eine Information zum Herunterfahren des Systems über das Netz erfolgen, sofern die Versorgung nicht ausreichend sichergestellt werden kann.


In Windows 10 kann über die Energieoptionen festgelegt werden, welche Aktion bei einem kritischen Batteriestand (z. B. bei einem Notebook oder lokal angeschlossener USV) ausgeführt werden soll:

 Computer Configuration/Administrative Templates/System/Power Management/Notification Settings

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Critical battery notification action	<b>Enabled</b>  <b>Options:</b> <ul style="list-style-type: none"> <li>Critical battery notification action: Hibernate</li> </ul>	Befindet sich der Akku des Rechners in einem kritisch niedrigen Zustand, sollte der Rechner automatisch in den Ruhezustand (Suspend-to-Disk, Power State S4) überführt werden, um einem möglichen Datenverlust vorzubeugen.

### SYS.2.1.A41 Verwendung von Quotas für lokale Datenträger (H)

In Windows 10 können Laufwerkskontingente mit dem sog. „Disk Quota Management“ für NTFS-formatierte Datenträger eingerichtet werden, um den verwendeten Speicherplatz auf der lokalen Festplatte zu begrenzen. Eine über die Gruppenrichtlinieneinstellungen konfigurierte Quota wird auf alle Laufwerke des Clients angewendet. Es können keine spezifischen Konfigurationen für einzelne Laufwerke oder Konten-spezifisch vorgenommen werden.

 Computer Configuration/Administrative Templates/System/Disk Quotas

Gruppenrichtlinieneinstellung	Konfigurationsoptionen	Erläuterung
Apply policy to removable media	„Enabled“ oder „Disabled“	Wird die Einstellung als „Aktiviert“ konfiguriert, werden die Disk Quota Policies auch auf Wechseldatenträger angewendet. Diese wirkt sich nur auf NTFS-formatierte Partitionen aus.
Enable disk quotas	„Enabled“ oder „Disabled“	Das Disk Quota Management wird auf allen NTFS formatierten Partitionen des Clients aktiviert. Benutzende können die Einstellung über die Oberfläche nicht ändern. Neben der „Aktivierung“ der Einstellung muss noch ein Quota Limit festgesetzt werden.
Enforce disk quota limit	„Enabled“ oder „Disabled“	Durch die Einstellung wird das Quota Limit auf einen definierten Wert gesetzt. Benutzende können die Quota Limits nicht mehr verändern.

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
Specify default quota limit and warning level	<b>„Enabled“</b> oder <b>„Disabled“</b>  <b>Options:</b> Specify a quota limit and warning level applied to users when they first write to a quota-enabled volume. <ul style="list-style-type: none"> <li>• Default quota limit</li> <li>• Default warning level</li> </ul>	Die Einstellung bestimmt das Quota Limit, das jeweils pro Benutzenden gilt. Es wird außerdem festgelegt, ab wann dem Benutzenden eine Warnung angezeigt werden soll.
Log event when quota limit is exceeded	<b>„Enabled“</b> oder <b>„Disabled“</b>	Durch die Richtlinieneinstellung werden Ereignisse über das Erreichen der gesetzten Quota in das Windows Event-Log geschrieben. Die Ereignisse können aus dem Application-Log entnommen werden.
Log event when quota warning level is exceeded	<b>„Enabled“</b> oder <b>„Disabled“</b>	Durch die Richtlinieneinstellung werden Ereignisse über das Erreichen der gesetzten Quotawarnung in das Windows Event-Log geschrieben. Die Ereignisse können aus dem Application-Log entnommen werden.

### SYS.2.1.A45 Erweiterte Protokollierung (H)

Nachfolgend sollen einige Anregungen für Ereignisse von Aktivitäten des Clients gegeben werden, aus denen Verhalten, welches nicht direkt in Verbindung mit der Sicherheit steht, protokolliert werden kann:

- Aufrufe der Windows-Registry
- Prozesszeugung/-terminierung
- Betriebssystemstart und -shutdown
- Installation und Konfigurationsänderungen von Diensten
- Softwareinstallation/-deinstallation
- Verarbeitung der Gruppenrichtlinien
- Druckernutzung
- Nutzung externer Medien
- Änderungen und Zugriff auf Netzlaufwerke
- An- und Abmeldung von Konten (auch erfolgreiche Anmeldevorgänge)
- Auf- und Abbau von RDP-Verbindungen
- Weiterleitung von Ereignissen (Events)
- Windows Fehlerberichtserstattung (Error Reporting)
- Löschen des Event-Logs
- Beenden von interaktiven Sitzungen
- Änderung der Systemzeit



- Zugriff auf Schlüsselmaterial im Zertifikatsspeicher
- Überwachung der Änderungen im Task Scheduler
- Windows Update

Bei der Abwägung zwischen der Protokollierung von nicht direkt mit der Sicherheit in Verbindung stehenden Ereignissen sollten mögliche Auswirkungen auf die Systemperformance berücksichtigt werden.

## 5 Konfiguration: SYS.2.2.3 Clients unter Windows 10

### 5.1 Basis-Anforderungen

#### SYS.2.2.3.A1 Planung des Einsatzes von Cloud-Diensten unter Windows 10 (B)

Die in Windows 10 mitausgelieferten Komponenten, die Cloud-Dienste nutzen, werden im Hilfsmittel in der Anforderung [SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen](#) betrachtet.

#### SYS.2.2.3.A2 Auswahl und Beschaffung einer geeigneten Windows-10-Version (B)

Der Funktionsumfang von Windows 10 unterscheidet sich in den bereitgestellten Editionen: Windows 10 Home, Windows 10 Pro/Pro for Workstations und Windows 10 Enterprise/Education. Eine Übersicht der enthaltenen Funktionen und Gegenüberstellung der einzelnen Funktionen können auf den Webseiten des Herausgebenden abgerufen werden:

- <https://www.microsoft.com/en-us/windowsforbusiness/compare>

In der Übersicht kann geprüft werden, ob der zur Verfügung stehende Funktionsumfang der vorgesehenen Version von Windows 10 ausreichend ist, um die geforderten Anforderungen des Grundschutzes umzusetzen.

Beispiele:

- Eine starke Reduzierung der Telemetriedaten (siehe [SYS.2.2.3.A4 Telemetrie- und Datenschutzeinstellungen unter Windows](#)) durch Einstellung des Telemetrielevels „0 (Security)“ ist erst mit der Windows 10 Enterprise-Edition möglich. In der Pro-Edition kann die Telemetrie maximal mit Level „1 (Basic)“ beschränkt werden.
- Die Anforderung [SYS.2.1.A33 Einsatz von Ausführungskontrolle \(H\)](#) lässt sich mit dem ausgelieferten Funktionsumfang in der Pro-Edition mit den sog. „Software Restriction Policies (SRP)“ umsetzen. Erst mit der Windows 10 Edition Enterprise ließen sich stattdessen die Nachfolgerfunktionen Microsoft AppLocker bzw. Device Guard verwenden.

Zwischen den Windows 10 Editionen (Home/Pro/Enterprise/Education) sowie dem gewählten Wartungskanal (GAC/LTSC)<sup>137</sup> bestehen funktionale Unterschiede, die sich mit Veröffentlichung einer neuen Windows 10 Version verändern. Die im Hilfsmittel beschriebenen Konfigurationsempfehlungen sind in Windows 10 Version 20H2 verfügbar. Je nach eingesetzter Edition kann sich der Funktionsumfang und die Auswirkung einer Konfiguration jedoch unterscheiden. Bei den entsprechenden Konfigurationsempfehlungen wird hierauf hingewiesen.

#### SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen unter Windows 10 (B)

Mit den Gruppenrichtlinieneinstellungen kann die Erhebung und Übertragung von Telemetriedaten nicht vollständig deaktiviert werden. Um eine Übertragung von Telemetriedaten vollständig zu verhindern, ist die Installation und Konfiguration von Windows 10 in einer isolierten, vom Internet getrennten, Umgebung erforderlich, sodass das Betriebssystem vollständig vom Internet entkoppelt wird. In Kapitel 4 der Konfigurations- und Protokollierungsempfehlungen<sup>138</sup> des SiSyPHuS Win10 Projekts werden die verschiedenen Konfigurationsvarianten und deren Wirksamkeit gegenübergestellt. Die Auswahl der geeignetsten Maßnahme hängt von der betrieblichen Umgebung des Zielsystems ab.

<sup>137</sup> <https://learn.microsoft.com/en-us/windows/deployment/update/waas-overview>

<sup>138</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHuS/Analyse\\_Telemetriekomponente\\_1\\_2.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHuS/Analyse_Telemetriekomponente_1_2.pdf)



## Computer Configuration/Administrative Templates/Windows Components/Data Collection and Preview Builds

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Allow device name to be sent in Windows diagnostic data	<b>Disabled</b>	Personalisierte oder individuelle Informationen zum IT-System oder von Benutzenden sollten nicht an Microsoft übermittelt werden. Durch Konfigurieren dieser Richtlinie wird festgelegt, dass der Geräte name nicht an Microsoft übermittelt wird. Diese Konfiguration entspricht dem vordefinierten Verhalten.
Allow Telemetry	<b>Enabled</b>  <b>Options:</b> 0 – Security (nur Enterprise Edition) oder 1 – Basic (Pro Edition)	Diese Empfehlung deckt sich mit den Analyseergebnissen des Arbeitspaket 4 des SiSyPHuS-Projekts. Hinweis: In der Bedienoberfläche steht der Wert 0 (Security) nicht zur Auswahl und wird nach Konfiguration über die Gruppenrichtlinieneinstellung auch nicht angezeigt. Wird keine Enterprise- oder Education-Edition eingesetzt, ist der Wert „0 – Security“ nicht wirksam. In diesem Fall kann die Übermittlung von Telemetriedaten nur auf der Netzebene oder durch Deaktivierung des Telemetrie-Dienstes verhindert werden (siehe Empfehlung zur Anforderung <a href="#">SYS.2.2.3.A25 Umgang mit Fernzugriffsfunktionen der „Connected User Experience and Telemetry“</a> ).
Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service	<b>Enabled</b>  <b>Options:</b> • Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service: Disable Authenticated Proxy usage	Um zu verhindern, dass der Dienst „Connected User Experience and Telemetry“ automatisch einen authentifizierten Proxy verwendet, um Informationen an Microsoft zu versenden, sollte die Richtlinie konfiguriert werden.
Limit Enhanced diagnostic data to the minimum required by Windows Analytics	<b>Enabled</b>	Die Einstellung ist erst ab Telemetrielevel 2 („Enhanced“) wirksam.
Do not show feedback notifications	<b>Enabled</b>	Durch Feedbackbenachrichtigungen können Meinungen von Benutzenden durch Microsoft eingeholt werden. Benutzende sollten grundsätzlich kein Feedback an Dritte senden dürfen, um zu verhindern, dass möglicherweise sensible Informationen abfließen.


**SYS.2.2.3.A5 Schutz vor Schadsoftware unter Windows 10 (B)**

Die Anforderung kann durch Umsetzung der Anforderung [SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware \(B\)](#) realisiert werden. Wenn eine Anwendungsausführungskontrolle auf Basis einer Erlaubt-Liste z. B. mit AppLocker (siehe Anforderung [SYS.2.1.A33 Einsatz von Ausführungskontrolle](#)) als Alternative genutzt werden soll, muss geprüft werden, ob zusätzlich installierte Software (z.B. Office-Programme, Webbrowser, PDF-Betrachter) den Einsatz eines Schutzprogramms gegen Schadsoftware erforderlich macht. Hierbei sollte insbesondere betrachtet werden, wie hoch das Risiko von kritischen Schwachstellen oder Funktionalitäten, die Code-Ausführung ermöglichen, ist, da diese durch die Ausführungskontrolle nicht geblockt werden können.

**SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem [Benutzer] (B)**

 Computer Configuration/Administrative Templates/Windows Components/Microsoft account

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Block all consumer Microsoft account user authentication	<b>Enabled</b>	Mit der Einstellung wird verhindert, dass Microsoft-Konten zur Authentifizierung in Anwendungen oder Diensten verwendet werden können. Eine interaktive Anmeldung an Windows mit einem Microsoft-Konto ist jedoch weiterhin möglich. Solange noch Anmelde-Token zwischengespeichert sind, ist eine Anmeldung mit Microsoft Accounts in Anwendungen oder Diensten ebenfalls weiterhin möglich, obwohl die Einstellung aktiviert wurde. Deswegen ist es empfehlenswert, diese Einstellungen vor einer ersten Anmeldung an Anwendungen oder Diensten mit Microsoft-Konten vorzunehmen.

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Accounts: Block Microsoft accounts	Users can't add or log on with Microsoft accounts	Mit dieser Einstellung wird verhindert, dass lokale Konten mit Microsoft-Konten verbunden werden können und zur Anmeldung an Windows verwendet werden können.


 Computer Configuration/Administrative Templates/Windows Components/App runtime

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Allow Microsoft accounts to be optional	<b>Enabled</b>	Die Einstellung betrifft nur GAC-Versionen von Windows 10, da die LTSC-Version keinen Microsoft Store unterstützt. Wird die Richtlinie deaktiviert, müssen sich Benutzende mit einem Microsoft-Account anmelden.
Network Security: Allow PKU2U authentication requests to this computer to use online identities	<b>Disabled</b>	Durch die Richtlinieneinstellung wird verhindert, dass der Client Authentisierungsanfragen durch Verwendung von Online-

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		Konten annehmen kann. Auf Stand-alone Systemen können Online-Konten durch Konten der Gruppe „Users“ verknüpft werden. Auf domänenverwalteten Clients ist dies voreingestellt nicht möglich.


## 5.2 Standard-Anforderungen

### SYS.2.2.3.A9 Sichere zentrale Authentisierung in Windows-Netzen (S)

 Computer Configuration/Windows Settings/Security Settings/Account Policies/Kerberos Policy


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Enforce user logon restrictions	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Hiermit wird jede Anfrage für ein Service Ticket vom Key Distribution Center (KDC) anhand der Berechtigungen des Kontos evaluiert. Die Validierung jedes Session Tickets verhindert, dass ein Konto ein Kerberos Service Ticket für einen Dienst erhält, auf den es keinen Zugriff (mehr) hat.
Maximum lifetime for service ticket	600 minutes (10 hours)	Vordefinierter Wert für ein Kerberos Service Ticket, Die „minimale“ maximale Gültigkeitsdauer kann 10 Minuten betragen.
Maximum lifetime for user ticket	10 hours	Vordefinierter Wert für ein Kerberos Ticket Granting Ticket. Dieser Wert wird für Benutzende, deren Konto Mitglied der AD-Gruppe „Protected Users“ sind, vordefiniert auf 240 Minuten (4 Stunden) Gültigkeit verkürzt.
Maximum lifetime for user ticket renewal	7 days	Dies ist die Zeitspanne, in der ein Ticket Granting Ticket (TGT) erneuert werden kann. Die „Renewal“-Zeit ist die maximale kumulierte Zeit, auf die ein Ticket erweitert werden kann. Dieser Wert wird für Benutzende, deren Konto Mitglied der AD-Gruppe „Protected Users“ sind, vordefiniert auf 240 Minuten (4 Stunden) Gültigkeit verkürzt.
Maximum tolerance for computer clock synchronization	5 minutes	Dieser Wert gibt die maximale Zeitspanne, die zwischen der Client-Uhrzeit und der Uhrzeit auf dem Domänencontroller, der die Kerberos Authentisierung durchführt, liegen darf. Das Kerberos-Protokoll verwendet als Mitigation von Replay-Angriffen Zeitstempel.

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		<p>Damit diese Zeitstempel sinnvoll genutzt werden können, sollte die Uhrzeit des Clients und des Domänencontrollers möglichst synchron sein (siehe auch <a href="#">Synchronisation der Systemzeit mit Hilfe eines Zeitserver</a>).</p> <p>Ist die Differenz zwischen den Zeitstempeln von Client und Domänencontroller unterhalb des hier gesetzten Wertes, werden die verwendeten Zeitstempel als authentisch angesehen.</p>


 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Network security: Configure encryption types allowed for Kerberos	„AES128_HMAC_SHA1“ „AES256_HMAC_SHA1“ „Future encryption types“	<p>Windows 10 und Windows Server ab 2008 R2 haben die DES-Cipher Suites in den Voreinstellungen deaktiviert, weil stärkere Cipher Suites verfügbar sind.</p> <p>Für die Kerberos-Kompatibilität mit Nicht-Windows-Systemen kann es ggf. notwendig sein, diese zu aktivieren, hier ist eine Einzelfallprüfung erforderlich.</p> <p>Wenn diese Policy nicht konfiguriert ist, nutzen Windows 10 Clients und Windows Server ab 2008 R2 „RC4_HMAC_MD5“, „AES128_HMAC_SHA1“ und „AES256_HMAC_SHA1“.</p> <p>„RC4_HMAC_MD5“ sollte – wenn in der eigenen Infrastruktur möglich – deaktiviert werden. Eine genaue Analyse ist vorab notwendig:</p> <p>Hier kann eine Event-Log-Analyse helfen, um zu prüfen, wo und wann RC4 noch verwendet wird. Der folgende Eintrag im Event-Log kann hier hilfreich sein: Event-ID 4769 „A Kerberos service ticket was requested“ auf den Domänencontrollern, in diesem Event-Eintrag muss auf RC4 gefiltert werden, RC4-Tickets haben den Ticket Encryption Type 0x17.</p> <p>Im Anschluss an die Analyse sollten auch Child-Domain-Trust-Szenarien betrachtet werden, bei denen die Einstellung „the other domain supports Kerberos AES encryption“ noch nicht gesetzt ist.</p> <p>Wenn alle DCs mindestens das Domain Functional Level 2008R2 und Forest Functional Level 2008R2 haben, kann aus DC-Sicht „RC4_HMAC_MD5“ deaktiviert</p>

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
		werden. Dies sollte, wenn möglich, in einer Testumgebung getestet werden. Weiterführende Informationen <sup>139,140</sup> können bei der Planung der Deaktivierung von „RC4_HMAC_MD5“ ggfs. hilfreich sein.

 Computer Configuration/Administrative Templates/System/Kerberos

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Support device authentication using certificate	<b>Enabled</b>  <b>Options:</b> Device authentication behavior using certificate: <ul style="list-style-type: none"> <li>• Automatic</li> </ul>	Voreingestellt wird für die Authentifizierung des Clients am Domänencontroller (Geräte-Authentisierung) vorzugsweise das Clientzertifikat (Kerberos Public Key Cryptography für Initial Authentication, kurz: PKInit) verwendet. Ist eine Authentifizierung mittels Zertifikats nicht möglich, wird die Authentifizierung mittels Passwort des Computerkontos durchgeführt. Hinweis: Durch Auswahl der Option „Force“ wird die Authentifizierung mittels Zertifikat erzwungen, damit nur eine zertifikatsbasierte Anmeldung der Geräte in der Domäne zugelassen wird. Hierzu sollte vorab geprüft werden, ob dies von allen Geräten unterstützt wird. Die Richtlinieneinstellung sollte nicht deaktiviert werden, da ansonsten nur noch das Computerkontenpasswort für die Authentisierung an den Domänencontrollern verwendet wird.

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Network security: LAN Manager authentication level	Siehe Konfigurationsempfehlungen zur Anforderung <a href="#">SYS.2.1.A18 Einsatz von verschlüsselten Kommunikationsverbindungen</a> .	Siehe Konfigurationsempfehlungen zur Anforderung <a href="#">SYS.2.1.A18 Einsatz von verschlüsselten Kommunikationsverbindungen</a> .
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients		
Network security: Allow LocalSystem NULL session fallback	<b>Disabled</b>	Es handelt sich um das vordefinierte Verhalten. NULL-Sitzungen für LocalSystem sind unsicher, da diese nicht authentifiziert sind.

<sup>139</sup> <https://techcommunity.microsoft.com/t5/itops-talk-blog/tough-questions-answered-can-i-disable-rc4-type-for-kerberos-on/ba-p/382718>

<sup>140</sup> <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/decrypting-the-selection-of-supported-kerberos-encryption-types/ba-p/1628797> (Abschnitt: „Do’s and Don’ts of RC4 disablement for Kerberos Encryption Types“)

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Network security: Do not store LAN Manager hash value on next password change	<b>Enabled</b>	Hashes des LAN Managers werden voreingestellt nicht gespeichert, wenn Passwörter geändert werden.



Computer Configuration/Administrative Templates/System/Remote Procedure Call

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Enable RPC Endpoint Mapper Client Authentication	<b>Enabled</b>	Die Richtlinieneinstellung legt fest, dass RPC-Clients sich am RPC Endpoint Mapper authentisieren müssen.
Restrict Unauthenticated RPC clients	<b>Enabled</b> <b>Options:</b> <ul style="list-style-type: none"> <li>• RPC Runtime Unauthenticated Client Restriction to Apply: Authenticated</li> </ul>	In der Voreinstellung verhält sich die RPC-Serverlaufzeit so, als wenn der Wert „Authenticated“ für Windows Clients und der Wert „none“ für Server-Versionen aktiviert wurde.

### SYS.2.2.3.A12 Datei- und Freigabeberechtigungen unter Windows 10 (S)

In Windows 10 können Freigaben über die Computerverwaltung (CompMgmt.msc) unterhalb der Systemwerkzeuge („System Tools“) aufgelistet werden. Alternativ kann eine Auflistung auch mittels des Kommandozeilenbefehls „net share“ erfolgen. Voreingestellt existieren nachfolgende aktive administrative Freigaben in Windows 10:

Freigabebezeichner	Beschreibung
DriveLetter\$ (z. B. C\$, D\$, ...)	Es handelt sich um eine administrative Freigabe für einen Zugriff auf das Systemlaufwerk. Sind weitere Laufwerke oder Partitionen mit Laufwerksbuchstaben verbunden, so wird eine eigenständige administrative Freigabe angelegt. (Hinweis: Der Laufwerksbuchstabe kann abweichen, je nachdem wie dieser gewählt wurde.)
IPC\$	Freigabe von Named Pipes zur Interprozesskommunikation (Die Ressource kann nicht gelöscht werden).
ADMIN\$	Freigabe, die während der Remoteverwaltung eines Clients verwendet wird.

#### Local Account Token Filter Policy


Voreingestellt können in nicht-domänenverwalteten Umgebungen Remotezugriffe auf die administrativen Freigaben in Windows 10 nur mit dem Built-In Administrator des lokalen Systems durchgeführt werden. Das Built-In Administratorkonto ist voreingestellt deaktiviert. Sofern es manuell aktiviert wurde, sollte sichergestellt werden, dass sich die Kennwörter der Built-In Administrationskonten auf allen Systemen voneinander unterscheiden. Weitere lokale Konten, die Mitglied der lokalen Administratorgruppe sind, können vordefiniert keinen Remotezugriff auf die administrativen Freigaben durchführen. Durch die Konfiguration der „Benutzerkontensteuerung“ erhalten solche Konten beim Remotezugriff einen erhöhten Zugriffstoken (engl.: *Elevated Token*), um die Aktion durchzuführen.

Durch Erstellen des Registrierungsschlüssels „LocalAccountTokenFilterPolicy“ mit dem Schlüsselwert 0 lässt sich dieses voreingestellte Verhalten explizit konfigurieren, so dass ein Remotezugriff auf die administrativen Freigaben nur durch das Built-In Administrationskonto („Administrator“) möglich ist. Hierbei




handelt es sich um eine Defense-in-Depth Maßnahme, um u. a. Pass-the-Hash Angriffen entgegen zu wirken.

```
C:\ reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
"LocalAccountTokenFilterPolicy" /t REG_DWORD /d 0 /f
```

 Computer Configuration/Administrative Templates/MS Security Guide


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Apply UAC restrictions to local accounts on network logons	Siehe Konfigurationsempfehlungen zur Anforderung <a href="#">SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten</a> .	Siehe Konfigurationsempfehlungen zur Anforderung <a href="#">SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten</a> .

Um einen Remotezugriff auf die administrativen Freigaben auch durch das Built-In Administrationskonto zu unterbinden, muss der sog. „Admin Approval Mode“ für das Built-In Administrationskonto aktiviert werden:

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
User Account Control: Admin Approval Mode for the Built-in Administrator account	<b>Enabled</b>	Obwohl das Built-In Administrationskonto deaktiviert werden muss, sollte die Richtlinie trotzdem aktiviert werden, um im Falle einer versehentlichen Aktivierung des Kontos noch einen zusätzlichen Schutz durch den sog. „Admin Approval Mode“ zu bieten.

In domänenverwalteten Umgebungen erfolgt der Remotezugriff durch Domänenkonten, die Mitglied der lokalen Administrationsgruppe („Administrators“) sind, auf die administrativen Freigaben mit einem vollwertigen administrativen Zugriffstoken ohne Beteiligung der „Benutzerkontensteuerung“.

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Network access: Allow anonymous SID/Name translation	<b>Disabled</b>	Es handelt sich um die vordefinierte Einstellung. Anonym sollten keine SID-Attribute für andere Konten anfragen werden dürfen.
Network access: Do not allow anonymous enumeration of SAM accounts	<b>Enabled</b>	Es handelt sich um die vordefinierte Einstellung. Über anonyme Zugriffe sollten keine SAM Accounts aufgelistet werden dürfen.
Network access: Do not allow anonymous enumeration of SAM accounts and shares	<b>Enabled</b>	In der Voreinstellung darf keine anonyme Auflistung der SAM Accounts und Freigaben erfolgen. Um zu verhindern, dass anonym Domänenanmeldungen und Netzfreigabenamen aufgelistet werden, sollte die Richtlinie konfiguriert werden.
Network access: Let Everyone permissions apply to anonymous users	<b>Disabled</b>	Vordefiniert enthält der Token, der bei einer anonymen Verbindung erstellt wird, nicht die „EVERYONE“-SID. Daher werden

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		alle Zugriffsrechte, die der „EVERYONE“-Gruppe zugeordnet sind, nicht gültig für anonyme Benutzende. Anonym kann nur auf solche Ressourcen zugegriffen werden, für die über die Built-In Gruppe „ANONYMOUS LOGON“ explizit Rechte zugewiesen wurden.
Network access: Named Pipes that can be accessed anonymously	Die Liste sollte leer sein.	Der anonyme Zugriff auf Named Pipes sollte nicht ermöglicht werden.
Network access: Restrict anonymous access to Named Pipes and Shares	<b>Enabled</b>	Bei aktivierter Einstellung (Voreinstellung) wird ein anonymer Zugriff auf solche Freigaben und Pipes beschränkt, die in den Richtlinieneinstellungen „Network access: Named pipes that can be accessed anonymously“ und „Network access: Shares that can be accessed anonymously“ angegeben wurden.
Network access: Restrict clients allowed to make remote calls to SAM	Auswahl der Built-In Administrationsgruppe über „Edit Security...“ oder Eintrag: O:BAG:BAD:(A;RC;;;BA)	Mitgliedern der lokalen Built-In Administrationsgruppe wird ein Remotezugriff über SAMRPC ermöglicht. Durch Auswahl der Berechtigungen wird der Security Descriptor automatisch in die Richtlinie übertragen.
Network access: Shares that can be accessed anonymously	Die Liste sollte leer sein.	Auf Netzfreigaben sollte nicht anonym zugegriffen werden können.
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	Die Richtlinieneinstellung bezieht sich auf Netzanmeldungen, welche lokale Konten zur Authentifizierung verwenden. Mit dem klassischen Modell können die Zugriffsrechte auf Ressourcen feingranular zugewiesen werden. Beim „Guest only“-Modell werden alle lokalen Konten automatisch dem Gastkonto zugeordnet. Die Richtlinieneinstellung hat keine Auswirkung auf eine netzbasierte Anmeldung mit Domänenkonten <sup>141</sup> .

## UNC-Pfade

Um die Sicherheitsanfälligkeit in Gruppenrichtlinien, die das Ausführen von Remotecode ermöglichen, zu beheben, können gehärtete UNC-Pfade festgelegt werden. Die nachfolgenden Tabellen beschreiben, wie Pfade definiert werden und welche Härtungsmöglichkeiten zur Auswahl stehen:

<b>Angabe</b>	<b>Beschreibung</b>
\\*\<Share>	Die Konfiguration wirkt auf jeden Server (*), welcher den angegebenen <Share> konfiguriert hat.
\\<Server>\*	Die Konfiguration wirkt auf den angegebenen <Server> auf alle existierenden Shares (*).

<sup>141</sup> [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj852218\(v=ws.11\)#best-practices](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj852218(v=ws.11)#best-practices)

<b>Angabe</b>	<b>Beschreibung</b>
\\<Server>	Identisch zu \\<Server>\*
\\<Server>\<Share>	Die Konfiguration wirkt auf den angegebenen <Server> mit dem expliziten <Share>, wenn es auf dem Server konfiguriert ist.



Computer Configuration/Administrative Templates/Network/Network Provider

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Hardened UNC Paths	<b>Enabled</b>  <b>Options:</b> \\*\NETLOGON, RequireMutualAuthentication=1, RequireIntegrity=1  \\*\SYSVOL, RequireMutualAuthentication=1, RequireIntegrity=1	Die Richtlinieneinstellung konfiguriert den gehärteten Zugriff auf UNC-Pfade.



Computer Configuration/Administrative Templates/Network/Lanman Workstation

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Enable insecure guest logons	<b>Disabled</b>	Die Richtlinieneinstellung sollte deaktiviert werden, um zu verhindern, dass über den SMB Client mit nicht authentisierten Konten auf freigegebene Ressourcen zugegriffen wird.

### SYS.2.2.3.A13 Einsatz der SmartScreen-Funktion (S)



Computer Configuration/Administrative Templates/Windows Components/Windows Defender SmartScreen/Explorer

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Configure Windows Defender SmartScreen	<b>Disabled</b>	Bei der Nutzung von SmartScreen werden ggfs. vertrauliche Daten an externe Dienste gesendet. Dem gegenüber steht eine verbesserte Schutzwirkung von SmartScreen. Daher muss die Nutzung von SmartScreen unter Abwägung der Schutzziele getroffen werden.

### SYS.2.2.3.A14 Einsatz des Sprachassistenten Cortana [Benutzer] (S)

Bereits während der Installation (siehe [SYS.2.1.A15 Sichere Installation und Konfiguration von Clients](#)) kann der Nutzung von Cortana widersprochen werden. Die Deinstallation/Deaktivierung der zugehörigen App „Cortana“ sowie die Anpassung des Autostarts von Cortana wird über die Konfigurationsempfehlung zur Anforderung [SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen](#) beschrieben.



Computer Configuration/Administrative Templates/Windows Components/Search

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow Cortana	<b>Disabled</b>	Bei Nicht-Konfiguration der Richtlinien-einstellung ist die Nutzung von Cortana möglich. Mit der Einstellung wird die Verwendung von Cortana für Benutzende unterbunden.
Allow Cortana above the lock screen	<b>Disabled</b>	Interaktionen auf dem Sperrbildschirm sollten bei aktivierter Cortana nicht ohne Authentisierung ermöglicht werden. Bei Nicht-Konfiguration der Richtlinien-einstellung ist eine Interaktion auf dem Sperrbildschirm mit Cortana möglich.
Allow search and Cortana to use location	<b>Disabled</b>	Standortinformationen sollten durch die Windows Suche und Cortana nicht verwendet werden dürfen.

### SYS.2.2.3.A15 Einsatz der Synchronisationsmechanismen unter Windows 10 (S)

Die von Microsoft integrierten Synchronisationsmechanismen in Windows 10 bedürfen einer vorherigen Authentisierung am Azure Active Directory. Dies können individuelle Microsoft-Konten oder organisationsspezifische Tenants innerhalb des Azure Active Directory sein. Da gemäß [SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem](#) bereits die Integration von Online-Konten ausgeschaltet ist, ist die Umsetzung der entsprechenden Konfigurationen eine weitere Absicherungsmaßnahme im Sinne einer Defense-in-Depth-Strategie.



Computer Configuration/Administrative Templates/Windows Components/Sync your settings

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Do not sync	<b>Enabled</b>	Im vordefinierten Verhalten wird Benutzenden mit Microsoft-Konto die Entscheidung überlassen, ob Einstellungen und Apps des PCs mit Microsofts Cloud-Diensten synchronisiert werden. Durch Aktivierung der Einstellung wird verhindert, dass kontenspezifische Einstellungen mit externen Diensten synchronisiert werden.
Do not sync app settings	<b>Enabled</b>	
Do not sync Apps	<b>Enabled</b>	
Do not sync browser settings	<b>Enabled</b>	
Do not sync desktop personalization	<b>Enabled</b>	
Do not sync on metered connections	<b>Enabled</b>	
Do not sync other Windows settings	<b>Enabled</b>	
Do not sync passwords	<b>Enabled</b>	
Do not sync personalize	<b>Enabled</b>	
Do not sync start settings	<b>Enabled</b>	

### Synchronisation von kontenspezifischen Daten



Computer Configuration/Administrative Templates/Windows/System/OS Policies

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow Clipboard synchronization across devices	<b>Disabled</b>	Die Zwischenablage lässt sich zwischen mehreren Geräten teilen, an dem sich dasselbe Microsoft-Konto/Azure AD-Konto angemeldet hat.


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		Um zu verhindern, dass möglicherweise sensible Informationen abfließen, sollte diese Funktion deaktiviert werden.
Allow upload of User Activities	<b>Disabled</b>	Da die Aktivitäten des Benutzenden grundsätzlich sensible oder persönliche Informationen beinhalten können, sollte die Möglichkeit, diese hochzuladen, über die Gruppenrichtlinie deaktiviert werden.
Allow publishing of User Activities	<b>Disabled</b>	Da die Aktivitäten des Benutzenden grundsätzlich sensible oder persönliche Informationen beinhalten können, sollte die Möglichkeit, diese zu veröffentlichen, über die Gruppenrichtlinie deaktiviert werden.
Enables Activity Feed	<b>Disabled</b>	Es handelt sich um eine Historie über durchgeführte Aktivitäten innerhalb eines Kontos in Form eines Feeds, der für den Benutzenden angelegt wird und über mehrere Geräte hinweg synchronisiert werden kann. Damit solche Aktivitäten, die möglicherweise sensible Informationen beinhalten, nicht veröffentlicht werden können oder über die Cloud synchronisiert werden, sollte die Funktion deaktiviert werden.

### Datensynchronisation von Windows Apps (nur lokales System)

 Computer Configuration/Administrative Templates/Windows Components/App Package Deployment

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Allow a Windows app to share application data between users	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Windows Apps können auf einem System lokal zwischen verschiedenen Konten keine Daten untereinander austauschen.

### Datensynchronisation zum OneDrive-Dienst

 Computer Configuration/Administrative Templates/Windows Components/OneDrive

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Prevent the usage of OneDrive for file storage	<b>Enabled</b>	Vordefiniert dürfen Apps und Features Dateien auch vom Cloudspeicherdienst OneDrive abrufen und darauf abspeichern.
Prevent OneDrive from generating network traffic until the user signs in to OneDrive	<b>Enabled</b>	Der OneDrive Synchronisierungsdienst startet nach einer interaktiven Anmeldung an Windows automatisch und erzeugt Netzverkehr (z. B. um Updates abzurufen). Um dieses Verhalten zu verhindern und einen Netzverkehr erst nach Anmeldung mit einem Microsoft-

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
		Konto an OneDrive zu erlauben, ist die Richtlinie zu aktivieren.
Save documents to OneDrive by default	<b>Disabled</b>	Sofern ein OneDrive-Konto einem Konto in Windows zugeordnet worden ist, werden Dateien und Dokumente von Apps bei Nicht-Konfiguration der Richtlinieneinstellung im Cloudspeicherdienst OneDrive gespeichert. Um dies zu verhindern und Dateien vorzugsweise lokal zu speichern, sollte die Richtlinie deaktiviert werden.

### Synchronisation der Systemzeit mit Hilfe eines Zeitservers (NTP)



Computer Configuration/Administrative Templates/Windows/System/Windows Time Service/Time Providers

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Configure Windows NTP Client <sup>142</sup>	Die Richtlinie sollte konfiguriert und in den Optionen ein NTP-Server festgelegt werden, welcher durch den Client zur Synchronisierung der Systemzeit verwendet werden soll.	Bei nicht-domänenverwalteten Windows 10 Clients wird die Systemzeit voreingestellt mit einem Zeitserver über das Network Time Protocol (NTP) synchronisiert. Der NTP-Server wird voreingestellt von Microsoft (time.windows.com) bereitgestellt. Über die Bedienoberfläche, aber auch über die Gruppenrichtlinieneinstellung, kann der zu verwendende Zeitserver individuell für Windows 10 angegeben werden. In domänenverwalteten Umgebungen wird die Systemzeit mit den Domänencontrollern synchronisiert.
Enable Windows NTP Client	<b>Enabled</b>	Nach Konfiguration des NTP Clients über die vorgenannte Richtlinie „Configure Windows NTP Client“ muss dieser noch über diese Richtlinieneinstellung aktiviert werden.
Enable Windows NTP Server	<b>Disabled</b>	Serverdienste, wie ein NTP-Server, sollten nicht auf Clients ausgeführt werden und als Zeitgeber für andere Clients agieren.

### SYS.2.2.3.A16 Anbindung von Windows 10 an den Microsoft-Store (S)

Für domänenverwaltete oder Stand-alone Clients wird in dieser Empfehlung kein hybrides Szenario betrachtet, daraus folgt auch keine Nutzung des Windows-Stores.




Computer Configuration/Administrative Templates/Windows Components/Store

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off the Store application	<b>Enabled</b>	Um zu verhindern, dass Benutzende eigenständig (öffentlich verfügbare) Apps in Windows 10 installieren können, wird mit

<sup>142</sup> <https://learn.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings>

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
		der Richtlinieneinstellung der Zugriff auf den Windows Store für Benutzende deaktiviert.
Disable all apps from Microsoft Store	<b>Disabled</b>	Die Richtlinieneinstellung verhindert die Ausführung von vorinstallierten Apps sowie weiteren Apps, die über den Microsoft Store bezogen wurden. Hinweis: Die Richtlinieneinstellung wird nur in der Windows 10 Enterprise bzw. Education Edition umgesetzt.

 Computer Configuration/Administrative Templates/System/Internet Communication Management

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off access to the Store	<b>Enabled</b>	Durch Deaktivierung über die Richtlinieneinstellung wird verhindert, dass der „Öffnen mit“-Dialog die Option anbietet, eine App über den Store zu suchen.

### SYS.2.2.3.A17 Keine Speicherung von Daten zur automatischen Anmeldung (S)


In der Windows-Anmeldeinformationsverwaltung (engl.: *Windows Credential Manager*) werden Anmeldeinformationen von Konten für Websites, Anwendungen und Netze (zwischen-)gespeichert. Es wird unterschieden zwischen Webanmeldeinformationen und Windows-Anmeldeinformationen. Die Anmeldeinformationen werden verschlüsselt in folgenden Pfaden als Datei (.vcred) gespeichert:

```
%systemdrive%\Users\[Username]\AppData\Local\Microsoft\Vault\  
%systemdrive%\Users\[Username]\AppData\Local\Microsoft\Credentials\  

```

Der zugehörige Schlüssel befindet sich in einer Datei (Policy.vpol), die üblicherweise im selben Verzeichnis wie die verschlüsselten Anmeldeinformationen abgelegt sind.


Mögliche Angreiferinnen und Angreifer stehen verschiedene Mechanismen und Funktionen<sup>143</sup> zur Verfügung, um gespeicherte Anmeldeinformationen aufzulisten und auszulesen.

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options/

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Network access: Do not allow storage of passwords and credentials for network authentication	<b>Enabled</b>	Voreingestellt speichert der Credential Manager Passwörter sowie andere Anmeldeinformationen auf dem Client für eine mögliche Authentifizierung an der Domäne zu einem späteren Zeitpunkt. Anmeldeinformationen sollten nicht zwischengespeichert werden. Um zu verhindern, dass Anmeldeinformationen für eine Netzauthentifizierung gespeichert werden, sollte die Richtlinie konfiguriert werden. Durch die Anmeldeinformationsverwaltung (Credential Manager) werden

<sup>143</sup> MITRE ATT&CK Technique T1555.004 (Credentials from Password Stores: Windows Credential Manager)  
<https://attack.mitre.org/techniques/T1555/004/>


Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
		mit aktivierter Richtlinieneinstellung keine Passwörter und Zugangsdaten lokal auf dem Client zur (automatischen) Anmeldung an Diensten und Ressourcen im Netz gespeichert.

 Computer Configuration/Administrative Templates/MSS (Legacy)

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
MSS: (DisableSavePassword) Prevent the dial-up password from being saved	<b>Enabled</b>	Damit Anmeldeinformationen von Einwahl- und VPN-Verbindungen nicht gespeichert werden, sollte die Richtlinieneinstellung aktiviert werden.

### SYS.2.2.3.A18 Einsatz der Windows-Remoteunterstützung (S)

Die Windows Remoteunterstützung kann über die Gruppenrichtlinie konfiguriert werden:

 Computer Configuration/Administrative Templates/System/Remote Assistance

Gruppenrichtlinieneinstellung	Konfigurationsoptionen	Erläuterung
Configure Offer Remote Assistance	„Enabled“ oder „Disabled“	Damit Benutzende über die Systemsteuerung die „Angeforderte Remoteunterstützung“ nicht eigenständig aktivieren oder deaktivieren können, sollte die Einstellung über die Gruppenrichtlinie vorgegeben werden. Wird die Remoteunterstützung nicht verwendet, sollte sie deaktiviert werden. In der Windows Firewall existiert im vordefinierten Verhalten eine eingehende Verbindungsfreigabe für die Remoteunterstützung (Private und Domain Profile). Es wird ein dynamisch festgelegter Port aus dem Bereich 1024-65535 gewählt. Dieser wird erst geöffnet, sobald die Remoteunterstützung („msra.exe“) gestartet wird und die Einladung erstellt wurde.
Configure Solicited Remote Assistance	„Enabled“ oder „Disabled“ (je nachdem, ob die Remote Assistance verwendet wird)  <b>Options:</b> Permit remote control of this computer: <ul style="list-style-type: none"> <li>• Allow helpers to remotely control the computer</li> <li>• Allow helpers to only view the computer</li> </ul> Maximum ticket time (value): <ul style="list-style-type: none"> <li>• 1-99</li> </ul> Maximum ticket time (units): <ul style="list-style-type: none"> <li>• Hours, Minutes, Days</li> </ul> Method for sending email invitations: <ul style="list-style-type: none"> <li>• Mailto oder Simple MAPI</li> </ul>	

In der lokalen Windows-Firewall sind vordefiniert für die Profile Domain und Private folgenden eingehenden Regeln aktiviert, die bei einer restriktiven Firewallkonfiguration für die Funktion Remoteunterstützung des Clients nicht gelöscht werden dürfen (Siehe Empfehlungen zum Umgang mit den Firewall-Regeln zur Anforderung [SYS.2.1.A31 Einrichtung lokaler Paketfilter](#)):

- Remote Assistance (DCOM-In) (nur Domain)
- Remote Assistance (PNRP-In)
- Remote Assistance (SSDP TCP-In)




- Remote Assistance (SSDP UDP-In)
- Remote Assistance (TCP-In)

### SYS.2.2.3.A19 Sicherheit beim Fernzugriff über RDP [Benutzer] (S)

Fernzugriffe auf Clients werden häufig für die Verwaltung von Endgeräten beispielsweise durch eine zentrale Administration genutzt. Darüber hinaus kann hierüber aber auch eine normale Nutzung von Client-Funktionalitäten erfolgen. Die allgemeinen Anforderungen hierzu finden sich im Baustein OPS.1.2.5. Die spezifischen Anforderungen in Windows 10 sind Gegenstand im SYS.2.2.3.A9. Für den Fernzugriff mit Remote Desktop wird vordefiniert der Port 3389 durch den RDP-Listener verwendet. Eine Änderung des Ports für den Listener ist über die Windows-Registry möglich, wird von Microsoft jedoch nicht empfohlen.

Es können zwei Szenarien betrachtet werden, in denen der Windows 10 Client als RDP-Server oder als RDP-Client fungiert.

#### Szenario 1: Windows 10 Client als RDP Server, auf den zugegriffen wird

 Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections

Gruppenrichtlinieneinstellung	Konfigurationsoptionen	,Erläuterung
Allow users to connect remotely by using Remote Desktop Services	„Enabled“ oder „Disabled“	Im vordefinierten Verhalten ist kein Remotezugriff möglich, was der Einstellung „Disabled“ entspricht. Sofern der Remotezugriff verwendet werden soll, ist die Einstellung auf „Enabled“ zu setzen.

 Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignment/

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users	Über die Richtlinie wird festgelegt, welche Gruppen für den Remote-Desktopzugriff berechtigt sind. Bei den empfohlenen Gruppen handelt es sich um die vordefinierte Konfiguration. In diesem Fall sollte überprüft werden, dass die Gruppe „Remote Desktop Users“ nur solche Konten enthält, die einen Remotezugriff auf den Client benötigen.
Deny log on through Remote Desktop Services	Guests, NT AUTHORITY\Local Account	Die „Deny“-Einstellung hat eine höhere Priorität als die „Allow“-Einstellung. In domänenverwalteten Clients sollten lokale Konten nicht für das Anmelden über die Remote Desktop Dienste verwendet werden. In nicht-domänenverwalteten Umgebungen führt der Ausschluss der lokalen Konten zur Anmeldung über Remote Desktop dazu, dass keine Anmeldung über RDP mehr möglich ist.



Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Require user authentication for remote connections by using Network Level Authentication	<b>Enabled</b>	Durch Network Level Authentication erfolgt vor dem Aufbau einer Remote Desktop Verbindung vordefiniert eine Authentisierung. Dies kann helfen, den Client als RDP-Server vor entfernten Angreiferinnen und Angreifern und schädlicher Software zu schützen, da es u. a. das Risiko von erfolgreichen Denial-of-Service Angriffen verringert.
Set client connection encryption level	High Level	Die Netzkommunikation zwischen RDP-Client und -Server wird verschlüsselt (128-Bit).
Require use of specific security layer for remote (RDP) connections	<b>Enabled</b> <b>Options:</b> SSL	Die Voreinstellung sieht vor, dass der Security Layer zwischen Client und Server ausgehandelt wird (SSL oder RDP). Bei einer nicht explizit konfigurierten Gruppenrichtlinieneinstellung kann der voreingestellte Wert aus der Windows Registry entnommen werden: „HKLM\SYSTEM\Current ControlSet\Control\Terminal Server\WinStations\RDP-Tcp“ Durch die Empfehlung wird TLS vorausgesetzt. Es wird TLS 1.2 verwendet, wenn die Konfiguration zum Einsatz von TLS 1.2 gem. den Empfehlungen zu <a href="#">SYS.2.1.A18 Nutzung von verschlüsselten Kommunikationsverbindungen</a> vorgenommen wurde. Abweichend zur Beschreibung der Gruppenrichtlinieneinstellung wird mit Auswahl der Option „SSL“ auch TLS 1.2 unterstützt.
Server authentication certificate template	Pfadangabe zur Zertifikatsvorlage (sofern PKI vorhanden)	In der voreingestellten Konfiguration wird ein selbstsigniertes Zertifikat für die RDP-Sitzung verwendet. Bei Nutzung einer Public-Key-Infrastruktur sollte ein durch die PKI ausgestelltes Zertifikat gegenüber dem selbstsignierten Zertifikat vorgezogen und der Pfad zur Zertifikatsvorlage angegeben werden.
Always prompt for password upon connection	<b>Enabled</b>	Im vordefinierten Verhalten dürfen Anmeldeinformationen auf dem Client gespeichert werden, um eine automatische Anmeldung auf den RDP-Server durchführen zu können (entspricht „Disabled“). Mit der Einstellung kann der RDP-Server

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		verhindern, dass sich Clients mit gespeicherten Anmeldeinformationen anmelden dürfen. Nach Ändern der Einstellung müssen die RDP-Dienste auf dem RDP-Server neu gestartet werden. Anmerkung: Gespeicherte Anmeldeinformationen auf dem RDP-Client werden im Credential Manager von Windows 10 hinterlegt.
Require secure RPC communication	<b>Enabled</b>	Im vordefinierten Verhalten versucht der RDP-Server vom RDP-Client eine authentifizierte und verschlüsselte RPC-Verbindung auszuhandeln (entspricht „Disabled“). Wird dies vom Client nicht unterstützt oder akzeptiert, wird auch eine ungesicherte RPC-Verbindung hergestellt. Durch Aktivierung der Einstellung lassen sich nur gesicherte RPC-Verbindungen zwischen RDP-Server und RDP-Client herstellen.



Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Session Time Limits


<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Set time limit for active but idle Remote Desktop Services sessions	<b>Enabled</b> <b>Options:</b> 15 Minuten oder weniger	Im vordefinierten Verhalten werden Remote-Desktopsitzungen zeitlich unbeschränkt aufrechterhalten. Ähnlich wie die automatische Sperre bei Konteninaktivität sollte auch eine nicht verwendete RDP-Sitzung nach Inaktivität sicherheitshalber gesperrt werden.
Set time limit for disconnected sessions	<b>Enabled</b> <b>Options:</b> <ul style="list-style-type: none"> <li>• End a disconnected session: Auswahl einer Zeitangabe (verschiedene Abstände möglich)</li> </ul> Der Wert sollte nicht, wie im vordefinierten Verhalten festgelegt, zeitlich unbeschränkt („Never“) sein, sondern es sollte ein realistischer Wert (z. B. 15 Minuten) gewählt werden.	Im vordefinierten Verhalten werden Remote-Desktop-Sitzungen zeitlich unbeschränkt aufrechterhalten. Hiermit lässt sich vermeiden, dass in Vergessenheit geratene Sitzungen weiterhin aufrechterhalten werden und Anwendungen weiter ausgeführt werden.



Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Services/Device and Resource Redirection

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung/ Konfigurationsoption</b>	<b>Erläuterung</b>
Allow audio and video playback redirection	„Enabled“ oder „Disabled“	Bei einer nicht explizit konfigurierten Gruppenrichtlinieneinstellung kann das vordefinierte Verhalten aus der Windows-Registry entnommen werden: „HKLM\SYSTEM\ ControlSet001HKLM\ SYSTEM\ControlSet001\ Control\Terminal Server\ fDisableCam“
Allow audio recording redirection	„Enabled“ oder „Disabled“	Der Remote Server kann das Audio Input Device (z. B. das Mikrofon) mitschneiden, sofern im RDP-Client die Audioaufzeichnung für die RDP-Sitzung im Reiter „Local Resources“ unter „Remote Audio“ ausgewählt wird. Vordefiniert ist Remoteaudio in den Einstellungen des RDP-Clients ausgewählt. Es sollte für den jeweiligen Anwendungsfall geprüft werden, ob die Funktion benötigt wird. Anderenfalls sollte die Funktion deaktiviert werden („Disabled“). Hierdurch ist es nicht mehr möglich, dass Audioaufnahmen des verbundenen Benutzenden, ohne dessen Kenntnis auf dem Remote Server aufgezeichnet werden.
Allow time zone redirection	„Enabled“ oder „Disabled“	Durch die Einstellung wird die Zeitzone des Clients in die RDP-Sitzung übertragen.
Do not allow Clipboard redirection	„Enabled“ oder „Disabled“	Durch die Richtlinieneinstellung kann die Verwendung der Zwischenablage gesteuert werden. Dabei ist zu berücksichtigen, dass der RDP-Server dann alle Einträge der Zwischenablage mitlesen kann.
Do not allow COM port redirection	<b>Enabled</b>	Es handelt sich um die Kommunikation über die serielle Schnittstelle. Sofern es hierfür keinen Anwendungsfall gibt, sollte eine Umleitung von COM-Geräten an den RDP-Server verhindert werden.
Do not allow drive redirection	<b>Enabled</b>	Mit der Einstellung wird verhindert, dass Laufwerke des Clients als Netzlaufwerke in der RDP-Sitzung verbunden werden. Sofern es hierfür keinen Anwendungsfall gibt, sollte eine Umleitung von lokalen Laufwerken des RDP-Clients an den RDP-Server verhindert werden. Schadsoftware könnte bei einer Umleitung der lokal angeschlossenen Laufwerke

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung/ Konfigurationsoption</b>	<b>Erläuterung</b>
		des RDP-Clients ohne die Interaktion von Benutzenden ausgeführt werden.
Do not allow LPT port redirection	<b>Enabled</b>	Es handelt sich um die Weiterleitung von über LPT-Ports angeschlossenen Geräten, wie z. B. Drucker. Sofern es hierfür keinen Anwendungsfall gibt, sollte eine Umleitung von Geräten, die über den LPT-Port am RDP-Client angeschlossen sind, an den RDP-Server verhindert werden.
Do not allow smart card device redirection	<b>Enabled</b>	Sofern eine Anmeldung für mittels Smart Card am RDP-Server nicht benötigt wird, sollte die Umleitung der Smart Card deaktiviert werden.
Do not allow supported Plug and Play device redirection	<b>Enabled</b>	Empfehlung entspricht dem vordefinierten Verhalten. Sofern es keinen Anwendungsfall für die Umleitung von Plug-and-Play-Geräten gibt, sollte eine Umleitung an den RDP-Server verhindert werden. Die Einstellung bezieht sich auch RemoteFX-Geräte.
Do not allow video capture redirection	<b>„Enabled“ oder „Disabled“</b>	Der Remote-Server kann das Video Input Device (z. B. eine Webcam) mitschneiden, sofern Benutzende im RDP-Client die Videoaufzeichnung für die RDP-Sitzung im Reiter „Local Resources“ unter „Local devices and resources → More → Video capture devices“ auswählen.

 *Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Services/Printer Redirection*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Do not allow client printer redirection	<b>Disabled</b>	Durch die Richtlinieneinstellung kann festgelegt werden, ob über den RDP-Server auf am RDP-Client angeschlossen Drucker zugegriffen werden darf. In diesem Fall werden die Drucker auf dem RDP-Server verbunden. Die Umleitung von lokal am Client angeschlossenen Druckern sollte nur bei einem konkreten Anwendungsfall aktiviert werden.



Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Connection Client/RemoteFX USB Device Redirection

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow RDP redirection of other supported RemoteFX USB devices from this computer	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Sofern kein konkreter Anwendungsfall besteht, in dem unterstützte RemoteFX USB-Geräte verwendet werden, sollte die Umleitung deaktiviert werden.

### RemoteFX im Vergleich zur RDP High-Level Device Redirection

Tabelle 23: RemoteFX im Vergleich zur RDP High-Level Device Redirection

RemoteFX USB Redirection	RDP High-Level Device Redirection
Auf dem Client werden Gerätetreiber nicht erfordert.	Gerätetreiber müssen auf dem Client installiert werden.
Gerätetreiber müssen serverseitig installiert sein.	Grundsätzlich werden keine Gerätetreiber auf dem Server benötigt.
Mittels einer Umleitung können viele unterschiedliche Gerätetypen verwendet werden. Beispiel: Scanner, Multifunktionsdrucker, Webcams, die mit der RDP High-Level Device Redirection nicht unterstützt werden.	Es wird eine spezifische Methode entsprechend für jeden Gerätetyp verwendet.
Ein Gerät kann nur exklusiv von einer Remote-Desktopsitzung verwendet werden. Der lokale Client kann das Gerät während einer RDP-Sitzung nicht nutzen.	Der Zugriff auf ein Gerät kann aus mehreren RDP-Sitzungen (und vom lokalen Client) gleichzeitig erfolgen.

### Szenario 2: Windows 10 Client als RDP-Client, mit dem auf einen RDP-Server zugegriffen wird


Entsprechend den unter Szenario 1 beschriebenen serverseitigen Einstellungen ist es möglich, den RDP-Client zum Zugriff auf einen RDP-Server individuell zu konfigurieren.



Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Connection Client

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Configure server authentication for client	<b>Enabled</b>  <b>Options:</b> Authentication setting: <ul style="list-style-type: none"> <li>• Warn me if authentication fails</li> </ul> oder <ul style="list-style-type: none"> <li>• Do not connect if authentication fails</li> </ul>	Im vordefinierten Verhalten werden Benutzende nur informiert, dass der RDP-Server sich mit einem nicht vertrauenswürdigen Zertifikat authentisiert. Eine Verbindung kann nach Bestätigung des Benutzenden dennoch aufgebaut werden. Um nur Verbindungen zu RDP-Servern, die sich mit vertrauenswürdigen Zertifikaten authentisieren, zuzulassen, kann die Einstellung zu „Do not connect if authentication fails“ konfiguriert werden. Bei Verwendung von selbstsignierten Zertifikaten muss das Serverzertifikat des RDP-Servers dazu unterhalb der vertrauenswürdigen Root-Zertifizierungsstellen auf dem RDP-Client installiert sein.

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Do not allow passwords to be saved	<b>Enabled</b>	Mit aktivierter Einstellung wird es nicht mehr Benutzenden des RDP-Clients überlassen, ob sie ihr Passwort für zukünftige Verbindungen dauerhaft hinterlegen möchten.

 Computer Configuration/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Connection Client/RemoteFX USB Device Redirection

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Allow RDP redirection of other supported RemoteFX USB devices from this computer	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Sofern kein konkreter Anwendungsfall besteht, in dem unterstützte RemoteFX USB Geräte verwendet werden, sollte die Umleitung deaktiviert werden.

### Microsoft Terminal Server Client (MSTSC)

 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Terminal Server\

Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)	Registry-Key	ValueName	Value (DWORD)	Begründung
Disable Clipboard in MSTSC	Terminal Server Client	DisableClipboardRedirection	0x00000000 oder 0x00000001	Die Einstellungen betreffen das Umleiten von Geräten und
Disable Drive Redirection in MSTSC	Terminal Server Client	DisableDriveRedirection	0x00000000 oder 0x00000001	Funktionen vom RDP-Client zu einem RDP-Server.
Disable Printer Redirection in MSTSC	Terminal Server Client	DisablePrinterRedirection	0x00000000 oder 0x00000001	Im Falle einer Kompromittierung des RDP-Servers können hierdurch auch Risiken für den RDP-Client bestehen.

### SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten (S)


Zur Konfiguration des Verhaltens der „Benutzerkontensteuerung“ (engl.: *User Account Control*) können in den zugehörigen Richtlinieneinstellungen (s. u.) aus nachfolgenden Verhaltensweisen ausgewählt werden<sup>144</sup>:

- Elevate without prompting
- Prompt for credentials
- Prompt for credentials on the secure desktop
- Prompt for consent
- Prompt for consent on the secure desktop

<sup>144</sup> <https://learn.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-group-policy-and-registry-key-settings>

- Prompt for consent for non-Windows-binaries

### Konfigurationseinstellungen zur „Benutzerkontensteuerung für privilegierte Konten“

 Computer Configuration/Windows Settings/Security Settings/Local Policies/Security Options

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
User Account Control: Admin Approval Mode for the Built-in Administrator account	<b>Enabled</b>	Obwohl das Built-In Administrationskonto deaktiviert werden muss, sollte die Richtlinie trotzdem aktiviert werden, um im Falle einer versehentlichen Aktivierung des Kontos noch einen zusätzlichen Schutz durch den sog. „Admin Approval Mode“ zu bieten.
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Grundsätzlich sollte für die Eingabeaufforderung für erhöhte Rechte zum sog. „Secure Desktop“ gewechselt werden. Durch die Richtlinieneinstellung kann hiervon eine Ausnahme für Anwendungen, die eine barrierefreie Bedienung des Clients ermöglichen (sog. „User Interface Accessibility“, kurz: UIA oder UIAccess), getroffen werden.
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for credentials on the secure desktop	Mit der Einstellung werden Benutzende dazu aufgefordert, einen Anmeldenamen und das Passwort eines privilegierten Kontos innerhalb des Secure Desktops einzugeben, um eine Aktion mit erhöhten Privilegien auszuführen.
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop	Diese Einstellung ist relevant für administrative Verwaltung des Clients. Administrierende, die lokal oder aus der Ferne Unterstützung leisten, können sich in der Umgebung des Benutzenden höhere Rechte anfordern. Dies bietet den Vorteil, dass Benutzende den Administrationsvorgang mitverfolgen können.
User Account Control: Detect application installations and prompt for elevation	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Bei der Ausführung von Installationspaketen von Anwendungen kann mit der Richtlinieneinstellung festgelegt werden, ob eine Aufforderung zur Eingabe von Anmeldeinformationen eines höher berechtigten Kontos angezeigt werden soll.
User Account Control: Only elevate executables that are signed and validated	<b>Disabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Microsoft bietet mit der Richtlinieneinstellung die Möglichkeit, die UAC-Aufrufe hinsichtlich der ausführbaren Dateien noch besser abzusichern. Bei Aktivierung




<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		der Richtlinie werden alle ausführbaren Dateien einer Signaturprüfung unterzogen.
User Account Control: Only elevate UIAccess applications that are installed in secure locations	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Durch die Richtlinieneinstellung wird geprüft, ob die UIAccess-Anwendung aus einem der in der Richtlinienbeschreibung genannten Verzeichnisse ausgeführt wird, welche grundsätzlich als sicher gelten, da diese bspw. vor nicht-administrativen Schreibzugriffen geschützt ist. Unabhängig von dieser Einstellung wird die digitale Signatur der ausführbaren Datei geprüft.
User Account Control: Run all administrators in Admin Approval Mode	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Durch die Richtlinieneinstellung wird der Admin Approval Mode für alle Administrationskonten verwendet.
User Account Control: Switch to the secure desktop when prompting for elevation	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Diese Richtlinieneinstellung überschreibt alle möglicherweise abweichend gesetzten Einstellungen der anderen Richtlinien zur „Benutzerkontensteuerung“ (in Bezug auf die Nutzung des sicheren Desktops).
User Account Control: Virtualize file and registry write failures to per-user locations	<b>Enabled</b>	Die Empfehlung entspricht dem vordefinierten Verhalten. Die Richtlinieneinstellung betrifft ältere Anwendungen, die nicht mindestens für Windows Vista ausgelegt wurden und deshalb in Verzeichnisse schreiben, die administrative Berechtigungen erfordern. Mit der aktivierten Richtlinieneinstellung erfolgt eine automatische Umlenkung in geschützte Verzeichnisse.



Computer Configuration/Administrative Templates/MS Security Guide

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Apply UAC restrictions to local accounts on network logons	<b>Enabled</b>	Sollte aufgrund eines Konfigurationsfehlers, entgegen den Empfehlungen zur Anforderung <a href="#">SYS.2.1.A20 Schutz der Administrationsverfahren bei Clients</a> , dieselben Anmeldedaten für administrative Konten auf mehreren Systemen genutzt werden, so verhindert diese Einstellung, dass mögliche Angreiferinnen und Angreifer sich mit abgeleiteten Anmeldeinformationen auf dem anderen

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		System anmelden können. Durch die UAC wird erzwungen, dass eine Eingabe der Anmeldeinformationen für das administrative Konto erfolgen muss.

 *Computer Configuration/Administrative Templates/Windows Components/Credential User Interface*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Do not display the password reveal button	<b>Enabled</b>	Bei erhöhtem Schutzbedarf und im Falle von aktivierter Remoteunterstützung sollte die Möglichkeit zur Einblendung des Passwortes deaktiviert werden, um ein versehentliches Aufdecken des Passwortes eines administrativen Kontos zu verbergen.
Enumerate administrator accounts on elevation	<b>Disabled</b>	Bei erhöhtem Schutzbedarf kann die Auflistung auf dem System vorhandener administrativer Konten in der Oberfläche zur Eingabe der Anmeldeinformationen deaktiviert werden.
Require trusted path for credential entry	<b>Enabled</b>	Der sichere Kanal schützt eingegebene Anmeldeinformationen vor unbefugten abgreifen durch Malware, wie beispielsweise einen (Software-)Keylogger.

## 5.3 Anforderungen bei erhöhtem Schutzbedarf

### SYS.2.2.3.A21 Einsatz des Encrypting File Systems (H)

Das Encrypting File System (EFS) ist ein in Windows 10 mitgeliefertes Verschlüsselungssystem von Microsoft, mit welchem sich Dateien und Verzeichnisse eines NTFS-Dateisystems verschlüsseln lassen. Mit Windows 10 Version 1607 und Server 2016 wurde EFS um eine Unterstützung für das FAT32-Dateisystem erweitert. EFS ist in Windows 10 in der Voreinstellung aktiviert und lässt sich über die Gruppenrichtlinieneinstellungen über folgenden Pfad verwalten:

 *Computer Configuration/Windows Settings/Security Settings/Public Key Policies/Encrypting File System*

Um die Richtlinieneinstellungen bearbeiten zu können, muss zunächst ein Wiederherstellungsagent neu erstellt oder hinzugefügt werden<sup>145</sup>. Hierfür sollte ein dediziertes Konto verwendet werden. Außerdem müssen alle Konten über entsprechende EFS-Zertifikate verfügen, um Daten mit EFS ver- und entschlüsseln zu können.

Der private Schlüssel, der zur Verschlüsselung der Daten durch EFS verwendet wird, wird durch das Kontenpasswort geschützt. Dieses Passwort sollte sich an den Empfehlungen zur Anforderung [SYS.2.1.A1 Sichere Benutzerauthentisierung](#) orientieren und entsprechend sicher gewählt werden.

Zur Einrichtung und Konfiguration in domänenverwalteten Umgebungen wird über die Dokumentation von Microsoft eine umfangreiche Anleitung mit weiterführenden Hinweisen zur Verfügung gestellt:

<sup>145</sup> <https://learn.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-and-verify-an-efs-dra-certificate>

- **Protecting Data by Using EFS to Encrypt Hard Drives**

[https://learn.microsoft.com/en-us/previous-versions/tn-archive/cc875821\(v=technet.10\)#EJAA](https://learn.microsoft.com/en-us/previous-versions/tn-archive/cc875821(v=technet.10)#EJAA)

### SYS.2.2.3.A22 Verwendung der Windows PowerShell (H)

#### Einschränkung der Ausführung der PowerShell und von PowerShell-Skripten

Damit Windows PowerShell (WPS)-Dateien (Skripte) nur von administrativen Konten ausgeführt werden dürfen, können spezifische Gruppenrichtlinieneinstellungen für die „Benutzerkonfiguration“ vorgenommen werden:



User Configuration/Administrative Templates/Windows Components/Windows PowerShell

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn on Script Execution	<b>Disabled</b>	Die Richtlinieneinstellung verhindert, dass PowerShell-Skripte durch Benutzende ausgeführt werden können, für die diese Gruppenrichtlinie angewendet wird. Sollen administrative Konten weiterhin PowerShell-Skripte ausführen dürfen, ist für diesen Benutzendenkreis keine Richtlinieneinstellung vorzunehmen, bzw. die Gruppenrichtlinie nicht anzuwenden.

Es kann auch restriktiver die Ausführung von PowerShell-Skripten auf dem gesamten Client verhindert werden (Benutzende und Administrierende), indem die Richtlinieneinstellung über die „Computerkonfiguration“ vorgenommen wird:



Computer Configuration/Administrative Templates/Windows Components/Windows PowerShell

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn on Script Execution	<b>Disabled</b>	Die Richtlinieneinstellung legt fest, dass PowerShell-Skripte auf dem gesamten Client nicht mehr ausgeführt werden können. Anmerkung: Diese Einstellung wird vorrangig angewendet, falls ebenfalls die Richtlinie über die „Benutzerkonfiguration“ gesetzt wird.

Sofern eine Skriptausführung über die PowerShell für einzelne Benutzende, Administrierende oder bestimmte Clients benötigt wird, sollte die Ausführung über die Ausführungsrichtlinie (engl.: *Execution Policy*) eingeschränkt werden, sodass nur noch signierte PowerShell-Skripte ausgeführt werden können<sup>146</sup>:



Computer Configuration/Administrative Templates/Windows Components/Windows PowerShell



User Configuration/Administrative Templates/Windows Components/Windows PowerShell

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn on Script Execution	<b>Enabled</b> <b>Options:</b>	Die Richtlinieneinstellung führt dazu, dass nur noch signierte PowerShell-Skripte ausgeführt werden.

<sup>146</sup> MITRE ATT&CK Technique T1059.001 (Command and Scripting Interpreter: PowerShell)

<https://attack.mitre.org/techniques/T1059/001/>

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
	<ul style="list-style-type: none"> <li>Execution Policy: Allow only signed scripts.</li> </ul>	<p>Anmerkung: Diese Einstellung setzt ein Zertifikatsmanagement bzw. einen sorgfältigen Umgang mit selbstsignierten Zertifikaten voraus. Es sollte nur vertrauenswürdigen Herausgebern vertraut werden.</p> <p>Weitere Informationen zur Ausführung signierter PowerShell-Skripte sind in der Dokumentation einsehbar<sup>147</sup>.</p>

Damit zusätzlich die Nutzung der PowerShell für Benutzende eingeschränkt wird, ist eine Ausführungskontrolle (siehe [SYS.2.1.A33 Einsatz von Ausführungskontrolle](#)) einzusetzen, welche eine Ausführung der PowerShell nur für Administrationskonten gestattet. Neben der PowerShell sollte auch die Einschränkung der Windows PowerShell Integrated Scripting Environment (ISE) berücksichtigt werden. Diese lässt sich als optionales Windows Feature, wie die ältere PowerShell Version 2.0, deaktivieren (siehe [SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen](#)).

Weiterführende Informationen zur Nutzungsbeschränkung der PowerShell und des Windows Script Hosts können aus dem Kapitel 5.5 der Konfigurationsempfehlungen zur Härtung von Windows 10 des SiSyPHuS Win10 Projekts<sup>148</sup> entnommen werden.

### Protokollierung der PowerShell

Für die Protokollierung der PowerShell wird in Kapitel 4.3.4 des Arbeitspaketes 10 des SiSyPHuS Win10 Projekts<sup>149</sup> die Konfiguration der folgenden Gruppenrichtlinien empfohlen, die auch unter Windows 10 20H2 angewendet werden können:

- Abschnitt 4.3.4.1: Aktivierung der Modulprotokollierung
- Abschnitt 4.3.4.2: Protokollierung von PowerShell-Skriptblöcken
- Abschnitt 4.3.4.2: PowerShell-Aufzeichnung

Die detaillierten Beschreibungen zu den empfohlenen Einstellungen und deren mögliche Auswirkungen können in AP 10 nachgeschlagen werden. Ebenfalls werden dort allgemeine Indikatoren für böswillige PowerShell-Aktivitäten aufgelistet, die in den Protokolldaten beobachtet werden können.

 Computer Configuration/Administrative Templates/Windows Components/Windows PowerShell

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn on Module Logging	<p><b>Enabled</b></p> <p><b>Options:</b></p> <ul style="list-style-type: none"> <li>Module Names: *</li> </ul>	<p>Im vordefinierten Verhalten wird die Verwendung von PowerShell-Modulen nicht protokolliert. Durch die Einstellung wird die Protokollierung von zu spezifizierenden PowerShell-Modulen aktiviert. Eine Eingrenzung der überwachten Module kann durch die Option „Module Names“ eingegrenzt werden, um die</p>

<sup>147</sup> [https://learn.microsoft.com/de-de/powershell/module/microsoft.powershell.core/about/about\\_signing?view=powershell-7.1](https://learn.microsoft.com/de-de/powershell/module/microsoft.powershell.core/about/about_signing?view=powershell-7.1)

<sup>148</sup> [https://www.bsi.bund.de/EN2021/Topics/Cyber-Security/Recommendations/SiSyPHuS\\_Win10/AP11/SiSyPHuS\\_AP11\\_node.html](https://www.bsi.bund.de/EN2021/Topics/Cyber-Security/Recommendations/SiSyPHuS_Win10/AP11/SiSyPHuS_AP11_node.html)

<sup>149</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Cyber-Security/SiSyPHuS/AP10/Logging\\_Configuration\\_Guideline.pdf?blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Cyber-Security/SiSyPHuS/AP10/Logging_Configuration_Guideline.pdf?blob=publicationFile&v=5)

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		aufgezeichneten Protokolldaten zu reduzieren.
Turn on PowerShell Script Block Logging	<b>Enabled</b>  <b>Options:</b> Log script block invocation start / stop events: Disabled	Im vordefinierten Verhalten werden PowerShell-Skriptblöcke nicht protokolliert. Diese Einstellung konfiguriert die Protokollierung des Inhalts von ausgeführten PowerShell-Skripten. Mit der Einstellung wird die Verarbeitung von Befehlen, Skriptblöcken, Funktionen und Skripts protokolliert. Die Protokolle können z. B. über den Event Viewer (Applications and Services Log → Microsoft → PowerShell → Operational) abgerufen werden. Die Option „Log script block invocation start / stop events: Disabled“ sollte nicht aktiviert werden, da diese Konfiguration zu einem hohen Ereignisaufkommen mit hohen Datenmengen führt.
Turn on PowerShell Transcription	<b>Enabled</b>  <b>Options:</b> Transcript output directory: [Angabe eines Pfades, auf das Benutzende keine Schreibrechte haben]. <input checked="" type="checkbox"/> Include invocation headers	Im vordefinierten Verhalten werden PowerShell-Sitzungen nicht aufgezeichnet. Mit dieser Einstellung werden alle PowerShell-Eingaben und -Ausgaben in der Aufzeichnungsdatei „PowerShell_transcript“ gespeichert. Diese kann auch sensitive Informationen wie z. B. Passwörter umfassen, wenn diese im Klartext eingegeben wurden. Wird kein Pfad angegeben, werden alle Aufzeichnungen als Textdateien im Verzeichnis „Dokumente“ des jeweiligen ausführenden Kontos gespeichert. Um die Aufzeichnungen vor unautorisierter Modifikation zu schützen, sollte ein Pfad gewählt werden, auf den Benutzende keine Schreibrechte haben. Für eine zentrale Speicherung der Aufzeichnungen kann ein Pfad im Netz gewählt werden.

### SYS.2.2.3.A23 Erweiterter Schutz der Anmeldeinformationen unter Windows 10 (H)

Auf UEFI-basierten Systemen wird SecureBoot über die Firmware aktiviert. Der Status des geschützten Modus für den Local Credential Store LSA wird im Windows Event-Log protokolliert und kann über die Ereignisanzeige im System-Log eingesehen werden:

Event Viewer → Windows Logs → System → WinInit-Ereignis suchen:

12: LSASS.exe was started as a protected process with level: 4

## Verwendung des Restricted Admin Mode



Computer Configuration/Administrative Templates/System/Credentials Delegation

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Restrict delegation of credentials to remote servers	<b>Enabled</b>	Der eingeschränkte Admin-Modus und Microsoft Defender Remote Credential Guard werden unterstützt. Anmeldeinformationen werden nicht an den Zielhost übergeben <sup>150</sup> .
Encryption Oracle Remediation	<b>Enabled</b>  <b>Options:</b> Force Updated Clients	Die Richtlinieneinstellung wirkt sich auf Anwendungen aus, die CredSSP verwenden (z. B. Remote Desktop) und wurde aus Kompatibilitätsgründen eingeführt. Mit der Option „Force Updated Clients“ wird verhindert, dass Client-Anwendungen, die CredSSP verwenden, Verbindungen zu Clients aufbauen, die veraltete Versionen und Dienste von CredSSP verwenden.
Remote host allows delegation of non-exportable credentials	<b>Enabled</b>	Damit der Restricted Admin Mode unterstützt wird, muss diese Richtlinieneinstellung aktiviert werden.

Sofern der Windows 10 Client das Zielsystem ist, muss nachfolgender Registry-Key gesetzt werden, damit der Restricted Admin Mode verwendet wird:



HKLM\SYSTEM\CurrentControlSet\Control\Lsa

Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)	Registry-Key	ValueName	Value
Disable RestricedAdmin	Lsa	DisableRestrictedAdmin	0x00000000

**Hinweis:** Wert 0x00000000 steht für „Deaktiviert“

### SYS.2.2.3.A24 Aktivierung des Last-Access-Zeitstempels (H)

Der Last-Access-Zeitstempel ist in Windows 10 in der Voreinstellung aktiviert. Der Zeitstempel gibt Auskunft darüber, wann eine Datei zuletzt geöffnet oder geschrieben wurde.

Mit dem Kommandozeilenwerkzeug „fsutil“ lässt sich der Status des Last-Access-Zeitstempels überprüfen:

```
C:\> fsutil behavior query disableLastAccess
DisableLastAccess = 2 (System Managed, Disabled)
```

### SYS.2.2.3.A25 Umgang mit Fernzugriffsfunktionen der „Connected User Experience and Telemetry“ (H)

Der Windows-Dienst „Benutzererfahrung und Telemetrie im verbundenen Modus“ („Connected User Experience and Telemetry“) ist fester Bestandteil von Windows 10 und dient u. a. der Übertragung von Telemetriedaten. Im Rahmen der systembasierten Maßnahmen (Kap. 3.1.2) der Konfigurations- und Protokollierungsempfehlungen zur Analyse der Telemetriekomponente in Windows 10 der SiSyPHus-

<sup>150</sup> <https://learn.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard>

Studie des BSI<sup>151</sup> wird empfohlen, den Dienst zu deaktivieren. Zusätzlich ist im 2. Schritt die ETW-Session „DiagTrack-Listener“ zu deaktivieren. Außerdem ist zu prüfen, ob die Sitzung bereits Daten auf die Festplatte ausgelagert hat.

### Deaktivierung des Dienstes „Connected User Experience and Telemetry“



Computer Configuration/Windows Settings/Security Settings/System Services

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Connected User Experience and Telemetry	<b>Enabled</b>  <b>Options:</b> <ul style="list-style-type: none"> <li>Select service startup mode: Disabled</li> </ul>	Der Windows-Dienst „Benutzererfahrung und Telemetrie im verbundenen Modus (Connected User Experience and Telemetry) wird mit dieser Einstellung deaktiviert. Die Initiierung der „DiagTrack-Listener“ ETW-Sitzung wird hierdurch verhindert.

### Deaktivierung der Trace Session des Diagtrack-Listener

Performance Monitor → Data Collector Sets → Startup Event Trace Session → Diagtrack-Listener

1. Properties (im Kontextmenü der Diagtrack-Listener Sitzung)
2. Reiter: Trace Session
3. Haken bei „Enabled“ entfernen

**Hinweis:** Zur Durchführung der Schritte sind Administrationsrechte notwendig. Beim Schließen der Eigenschaften der Sitzung erscheint eine Fehlermeldung, dass die Berechtigung nicht ausreichend ist. Die Sitzung wird durch Schließen mit „Cancel“ dennoch deaktiviert. Alternativ zum Performance Monitor kann die ETW-Sitzung über Konfiguration des Registry-Wertes vorgenommen werden:



HKLM\SYSTEM\CurrentControlSet\Control\WMI\Autologger

Empfehlung für den Anzeigenamen der Gruppenrichtlinieneinstellung (ADML)	Registry-Key	ValueName	Value
Disable Diagtrack-Listener Session	Diagtrack-Listener	Start	0x00000000

### Löschen der möglicherweise bereits angelegten Even Trace Logdatei (ETL)

Die zugehörige(n) „Diagtrack-Listener.etl<id>“-Datei(en) wird/werden in der Voreinstellung in das Verzeichnis:

%windir%\System32\LogFiles\WMI\

gespeichert. Sofern diese Datei(en) bereits angelegt worden ist/sind, sollte(n) sie entfernt werden, da hierin bereits aufgezeichnete Telemetriedaten enthalten sein könnten.

### Durchführen eines Neustarts

Anschließend muss der Client neu gestartet werden.

<sup>151</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/E20172000\\_BSI\\_Win10\\_AFUNKT\\_TELE\\_DEAKTIVIEREN\\_v1\\_0.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/E20172000_BSI_Win10_AFUNKT_TELE_DEAKTIVIEREN_v1_0.html)

## 6 Konfigurationen zu weiteren Bausteinen

### 6.1 Basisanforderungen

#### 6.1.1 SYS.3.1 Laptops

##### SYS.3.1.A3 Einsatz von Personal Firewalls (B)

Windows 10 enthält mit der Windows-Firewall bereits eine „Personal Firewall“. Empfehlungen zur restriktiven Konfiguration werden unter [SYS.2.1.A31 Einrichtung lokaler Paketfilter \(H\)](#) beschrieben.

### 6.1.2 DER.1 Detektion von sicherheitsrelevanten Ereignissen

#### DER.1.A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion [Fachverantwortliche] (B)

Das Windows Event-Log kann mit Hilfe des Event Viewers ausgewertet werden. Insbesondere sollten hierbei die Windows-Protokolle zur Sicherheit (Security) berücksichtigt werden.

Empfehlungen zur Konfiguration der Protokollierung in Windows 10 werden in der SiSyPHuS Win 10 Studie bereitgestellt:

- [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Empfehlung\\_zur\\_Konfiguration\\_der\\_Protokollierung\\_Win\\_10.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Empfehlung_zur_Konfiguration_der_Protokollierung_Win_10.html)

### 6.1.3 OPS.1.1.4 Schutz vor Schadprogrammen

#### OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes (B)

Der Microsoft Defender beinhaltet Funktionen, die auf Cloud-Dienste zurückgreifen, welche die Detektionsrate deutlich verbessern können<sup>152</sup>. Daher sollte geprüft werden, ob die Cloud-Funktionen wegen der höheren Detektionsrate genutzt werden sollen (siehe [SYS.2.1.A42](#)). Neben der Detektionsrate sollten generell weitere Auswahlkriterien geprüft werden, wie bspw. Hersteller-Support, Funktionen zum Exploit Schutz (siehe Empfehlungen zu [Attack Surface Reduction](#)), Nutzung der AMSI-Schnittstelle, Berücksichtigung von Anforderungen anderer IT-Systeme (z.B. Server-Systeme) sowie Möglichkeiten zum zentralen Monitoring und Reporting. Vor der Nutzung der Cloud-Dienste muss zudem sichergestellt werden, dass gesetzlich einzuhaltende Anforderungen erfüllt werden (z. B. für den Datenschutz bezüglich der Übertragung von Beispieldateien). Dies kann u.a. den Abschluss eines Auftragsdatenverarbeitungsvertrages (ADV) erfordern. Zusätzlich müssen auch die Anforderungen des Geheimnisses berücksichtigt werden.

#### Microsoft Defender Antivirus: Microsoft Active Protection Service (MAPS)



Computer Configuration/Administrative Templates/Windows Components/Microsoft Defender Antivirus/MAPS

Gruppenrichtlinieneinstellung	Konfigurationsoptionen	Erläuterung
Join Microsoft MAPS	Abhängig von der Entscheidung zur Nutzung, d. h. entweder „Enabled“ oder „Disabled“  Mögliche Werte sind:	Beim Microsoft Active Protection Service (MAPS) handelt es sich um ein Programm von Microsoft, bei dem Unternehmen und Organisationen beitreten können, damit Informationen über potenzielle Schad-

<sup>152</sup> <https://www.av-comparatives.org/tests/malware-protection-test-march-2022/>



<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
	<ul style="list-style-type: none"> <li>• (0x0) Disabled (default)</li> <li>• (0x1) Basic membership</li> <li>• (0x2) Advanced membership</li> </ul>	software an Microsoft zur Analyse bereitgestellt werden können. <sup>153</sup> Das Aktivieren ist notwendig, damit Cloudabfragen erfolgen können (auch ohne Beispielübermittlung). Anmerkung: Die Gruppenrichtlinie zum Beitritt von MAPS hat Vorrang.
Configure local setting override for reporting to Microsoft MAPS	„Enabled“ oder „Disabled“	Durch die Einstellung kann konfiguriert werden, ob die lokale Konfiguration durch die Gruppenrichtlinie überschrieben werden soll. Wird die Einstellung nicht konfiguriert oder deaktiviert, ist eine abweichende lokale Konfiguration nicht möglich.
Configure the 'Block at First Sight' Feature	„Enabled“ oder „Disabled“	Mit der Einstellung kann konfiguriert werden, dass eine Ausführung oder Zugriff auf Inhalte erst nach einer Prüfung durch MAPS erfolgt. Diese Funktion kann nicht genutzt werden, wenn die Übertragung von Beispielen („Send file samples when further analysis is required“) mit Wert 0x2 („Never send“) konfiguriert ist.
Send file samples when further analysis is required	<p>Mögliche Werte sind:</p> <ul style="list-style-type: none"> <li>• (0x0) Always prompt</li> <li>• (0x1) Send safe samples automatically</li> <li>• (0x2) Never send</li> <li>• (0x3) Send all samples automatically</li> </ul>	Die Einstellung bezieht sich auf eine automatische Beispielübermittlung. Sofern MAPS und „Bei erster Anzeige blockieren“ („Block at First Sight“) genutzt werden, sollte hier festgelegt werden, wie das Einreichen von Dateien behandelt werden soll. Wird der Wert 0x2 (Never send) gewählt, kann die Funktion „Block at first sight“ nicht genutzt werden.

### Microsoft Defender Antivirus: MpEngine



Computer Configuration/Administrative Templates/Windows Components/Windows Defender Antivirus/MpEngine

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
Configure extended cloud check	<p>Abhängig von der Entscheidung zur Nutzung von MAPS, d. h. entweder „Enabled“ oder „Disabled“</p> <p><b>Options:</b></p> <ul style="list-style-type: none"> <li>• Specify the extended cloud check:</li> </ul>	Wird MAPS, „Bei erster Anzeige blockieren“ sowie „Dateibeispiele senden“ genutzt, kann über die Richtlinieneinstellung der Zeitwert um max. 50 Sek. erhöht werden, der festlegt, wie lange eine verdächtige Datei durch Microsoft Defender blockiert werden soll. Wird kein Wert festgelegt beträgt die Wartezeit 10 Sekunden.

<sup>153</sup> <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-cloud-protection-microsoft-defender-antivirus?view=o365-worldwide>

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
	Angabe eines Zeitwertes in Sekunden (Bereich: 0-50)	
Select cloud protection level	<p>Abhängig von der Entscheidung zur Nutzung von MAPS, d. h. entweder „<b>Enabled</b>“ oder „<b>Disabled</b>“</p> <p><b>Options:</b></p> <ul style="list-style-type: none"> <li>• Select cloud protection level:</li> <li>• Default blocking level</li> <li>• Moderate blocking level</li> <li>• High blocking level</li> <li>• High+ blocking level</li> <li>• Zero tolerance blocking level</li> </ul>	Bei Nutzung von MAPS kann das Scan- und Blockier-Verhalten des Microsoft Defenders zu verdächtigen Dateien festgelegt werden. Microsoft empfiehlt über die Security Baselines die Auswahl des „High blocking level“ (0x2)
Enable file hash computation feature	Abhängig von der Entscheidung zur Nutzung des Dienstes „Microsoft Defender Advanced Threat Protection (MDATP)“, d. h. entweder „ <b>Enabled</b> “ oder „ <b>Disabled</b> “	Im vordefinierten Verhalten werden durch Microsoft Defender keine Prüfsummen über gescannte Dateien berechnet. Die Funktion kann das Block-Verhalten bei Nutzung des Dienstes „Microsoft Defender Advanced Threat Protection (MDATP)“ verbessern. Anderenfalls bietet diese Funktion jedoch keine Vorteile und sollte deaktiviert bleiben.

 Computer Configuration/Administrative Templates/Windows Components/Windows Defender SmartScreen/Explorer

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
Configure Windows Defender SmartScreen	Abhängig von der Entscheidung zur Nutzung entweder „ <b>Enabled</b> “ oder „ <b>Disabled</b> “	Bei der Nutzung von SmartScreen werden ggfs. vertrauliche Daten an externe Dienste gesendet. Dem gegenüber steht eine verbesserte Schutzwirkung durch SmartScreen. Daher muss die Nutzung von SmartScreen unter Abwägung der Schutzziele getroffen werden.
Configure App Install Control	<p>Abhängig von der Entscheidung zur Nutzung entweder „<b>Enabled</b>“ oder „<b>Disabled</b>“</p> <p>Optionen bei „<b>Enabled</b>“:</p> <ul style="list-style-type: none"> <li>• Turn off app recommendations</li> <li>• Show me app recommendations</li> </ul>	Mit App Install Control von Microsoft Windows Defender SmartScreen kann vorgegeben werden, dass durch einen Benutzenden ausschließlich Apps aus dem Store bezogen werden können. Hinweis: Die Einstellung wird nur umgesetzt, wenn SmartScreen aktiviert ist.

<b>Gruppenrichtlinieneinstellung</b>	<b>Konfigurationsoptionen</b>	<b>Erläuterung</b>
	<ul style="list-style-type: none"> <li>Warn me before installing apps from outside the Store</li> <li>Allow apps from Store only</li> </ul>	

## 6.1.4 ORP.4 Identitäts- und Berechtigungsmanagement

### ORP.4.A2 Einrichtung, Änderung und Entzug von Berechtigungen [IT-Betrieb] (B)

Berechtigungen und Privilegien für Konten, beispielsweise von Benutzenden, können in Windows 10 an verschiedenen Stellen konfiguriert werden:

#### Installationsberechtigungen

 *Computer Configuration/Administrative Templates/Windows Components/Windows Installer*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Allow user control over installs	<b>Disabled</b>	Der empfohlene Wert entspricht dem vordefinierten Verhalten. Benutzende werden daran gehindert, Installationsoptionen zu verändern, die grundsätzlich nur durch Administrierende erfolgen sollten. Dies umfasst beispielsweise die Angabe von Installationsverzeichnissen. Zu beachten ist, dass es neben dem Windows Installer weitere Installer u. a. von Drittanbietern gibt, die mit dieser Gruppenrichtlinieneinstellungen nicht adressiert werden.

 *Computer Configuration/Administrative Templates/Windows Components/Windows Installer*

 *User Configuration/Administrative Templates/Windows Components/Windows Installer*

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
Always install with elevated privileges	<b>Disabled</b>	Durch die Deaktivierung der Gruppenrichtlinieneinstellung sollte konfiguriert werden, dass Installationen mit SYSTEM-Berechtigungen ausgeführt werden. Dies entspricht dem vordefinierten Verhalten bei Nicht-Konfiguration der Richtlinieneinstellung. Eine aktivierte Richtlinieneinstellung („Enabled“) führt hingegen zu einem Sicherheitsrisiko, da grundsätzliche eine Privilegienerweiterung für weniger privilegierte Konten von Benutzenden ermöglicht werden kann.

## Zuordnung von Privilegien und Rechten in Windows 10 („User Rights Assignments“)

 Computer Configuration/Windows Settings/Security Settings/Local Policies/User Rights Assignments

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
<a href="#">Access Credential Manager as a trusted caller</a>	Die Liste in der Richtlinieneinstellung sollte keine Konten oder Gruppen enthalten.	Privileg: <i>SeTrustedCredManAccessPrivilege</i> Das Privileg wird durch den Credential Manager während Datensicherung und -wiederherstellung benötigt. Wird das Recht missbräuchlich verwendet, können gespeicherte Anmeldeinformationen von Konten ausgespäht werden. Aus diesem Grund sollte dieses Privileg nicht an Konten oder Gruppen vergeben werden.
<a href="#">Access this computer from the network</a>	Siehe Empfehlungen unter Anforderung SYS.2.2.3.A11.	Privileg: <i>SeNetworkLogonRight</i> Siehe Empfehlungen unter Anforderung <a href="#">SYS.2.2.3.A11 Schutz der Anmeldeinformationen unter Windows 10</a> .
<a href="#">Act as part of the operating system</a>	Die Liste in der Richtlinieneinstellung sollte keine Konten oder Gruppen enthalten.	Privileg: <i>SeTcbPrivilege</i> Das Privileg ermöglicht einem Prozess, die Identität eines beliebigen Kontos anzunehmen und dadurch Zugriff auf Ressourcen zu erhalten, die mit dessen Berechtigungen abrufbar sind.
<a href="#">Add workstations to domain</a>	Die Liste der Konten und Gruppen enthält in Windows 10 voreingestellt keine Einträge. Es sollte in einer übergeordneten Richtlinie auf Domänencontrollerebene festgelegt werden, welche Konten Rechner in die Domäne aufnehmen dürfen. Voreingestellt wird in der Richtlinie „Domain Controllers“ die Gruppe „Authenticated Users“ aufgelistet. In verwalteten Umgebungen sollten „Standardbenutzer“ keine Rechte erhalten, um Rechner zur Domäne hinzuzufügen.	Privileg: <i>SeMachineAccountPrivilege</i> Mit dem Privileg dürfen je Konto bis zu 10 Clients zu einer Domäne hinzugefügt werden. Innerhalb einer Windows-Domäne verfügen voreingestellt alle Konten, die Mitglied der Gruppe „Authenticated Users“ sind, über dieses Privileg.
<a href="#">Adjust memory quotas for a process</a>	Grundsätzlich sollten nur Konten dieses Privileg erhalten, sofern diese es benötigen.	Privileg: <i>SeIncreaseQuotaPrivilege</i> Das Privileg ermöglicht eine Anpassung des maximal in Anspruch nehmenden Speichers für einen Prozess. Das Privileg lässt sich für Denial-of-Service-Angriffe missbrauchen, indem die Speicherquota eines Prozesses zu niedrig angesetzt wird und dieser hierdurch nicht mehr voll funktionsfähig ist.

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
<a href="#">Allow log on locally</a>	Siehe Empfehlungen zur Anforderung <a href="#">SYS.2.1.A1 Sichere Benutzerauthentifizierung</a> .	Recht: <i>SeInteractiveLogonRight</i>
<a href="#">Allow log on through Remote Desktop Services</a>	Siehe Empfehlungen zur Anforderung <a href="#">SYS.2.2.3.A19 Sicherheit beim Fernzugriff über RDP</a> .	Recht: <i>SeRemoteInteractiveLogonRight</i>
<a href="#">Back up files and directories</a>	Siehe Empfehlungen zur Anforderung <a href="#">SYS.2.1.A27 Geregelte Außerbetriebnahme eines Clients</a> .	Privileg: <i>SeBackupPrivilege</i>
<a href="#">Bypass traverse checking</a>	Microsoft empfiehlt bei erhöhtem Schutzbedarf, eine zugriffsbasierte Auflistung (Access-based Enumeration) vorzunehmen und anderenfalls die bereits in der Liste enthaltenen Gruppen und Benutzende nicht zu verändern. Sollte die Liste verändert werden, sollten die Auswirkungen in Tests beobachtet werden.	Privileg: <i>SeChangeNotifyPrivilege</i> Das Privileg ermöglicht es Konten, einen Zugriff auf tiefere Datei- und Verzeichnisebenen im NTFS-Dateisystem oder der Registry zu erhalten, um auf Dateien oder Unterordner zuzugreifen, auf die die Konten berechtigt sind.
<a href="#">Change the system time</a>	Um zu verhindern, dass die Systemzeit missbräuchlich verfälscht wird, sollten keine weiteren Konten in die Liste aufgenommen werden.	Privileg: <i>SeSystemtimePrivilege</i> Mit dem Privileg dürfen Konten die interne Systemzeit ändern. Wird dieses Privileg missbräuchlich verwendet, können Zeitstempel von Eventlog-Einträgen, Dateien und Verzeichnissen verfälscht werden. Voreingestellt verfügen Konten der Gruppe „Administrators“ und das Konto „LOCAL SERVICE“ über das Privileg, die interne Systemzeit ändern zu dürfen. In einer verwalteten Umgebung mit Domäne kann es bei Abweichungen der Systemzeit von der Domäne zu Anmeldeproblemen kommen.
<a href="#">Change the time zone</a>	Da sich die Änderung der Zeitzone nicht auf die interne Systemzeit auswirkt, ist die Vergabe dieses Privilegs aus Sicherheitssicht unproblematisch.	Privileg: <i>SeTimeZonePrivilege</i> Dieses Privileg ermöglicht es Konten, die Zeitzone des Geräts zu verändern.
<a href="#">Create a pagefile</a>	Administrators	Privileg: <i>SeCreatePagefilePrivilege</i> Dieses Privileg ermöglicht Konten, eine Auslagerungsdatei anzulegen und ihre maximale Größe festzulegen.

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
		Eine missbräuchliche Anpassung der Auslagerungsdatei kann zu Denial-of-Service-Angriffen führen, in dem diese zu klein gewählt wird.
<a href="#">Create a token object</a>	Die Liste in der Richtlinien-einstellung sollte keine Kon-ten oder Gruppen enthalten.	Privileg: <i>SeCreateTokenPrivilege</i> Ein Konto, das über dieses Privileg verfügt, kann beliebige Zugriffstoken erstellen und hat somit vollständige Kontrolle über das System. Das Privileg wird nur betriebs-systemintern verwendet.
<a href="#">Create global objects</a>	Voreingestellt sind folgende Konten in der Liste aufgelistet: Administrators; LOCAL SERVICE; NETWORK SERVICE; SERVICE. Es sollten keine weiteren Konten oder Gruppen der Liste hinzugefügt werden.	Privileg: <i>SeCreateGlobalPrivilege</i> Das Privileg erlaubt es Konten, globale Objekte anzulegen. Dies erfolgt beispielsweise bei Einsatz von Remote-Desktop-Diensten. Deshalb verfügt auch die Gruppe „Remote Desktop Users“ über dieses Privileg, auch wenn diese nicht explizit in der Liste aufgeführt wurde.
<a href="#">Create permanent shared objects</a>	Die Liste enthält vorein-gestellt keine Einträge. Es sollten keine Konten oder Gruppen der Liste hinzuge-fügt werden.	Privileg: <i>SeCreatePermanentPrivilege</i> Konten mit diesem Privileg können permanent freigegebene Objekte erzeugen (bspw. Semaphoren oder Mutexe). Prozesse, die dieses Privileg benötigen, sollten das SYSTEM-Konto verwenden.
<a href="#">Create symbolic links</a>	Die Liste sollte nur Konten von Administrierenden beinhalten.	Privileg: <i>SeCreateSymbolicLinkPrivilege</i> Das Privileg ermöglicht Konten die Erstellung von symbolischen Links auf Dateisystemobjekten (Dateien oder Verzeichnisse im NTFS-Dateisystem). Durch symbolische Verlinkungen können Angriffe auf das Dateisystem vorgenom-men werden, um beispielsweise Berechti-gungen von Dateien zu verändern, Daten zu manipulieren oder zu löschen.
<a href="#">Debug programs</a>	Siehe Empfehlungen zur Anforderung <a href="#">SYS.2.1.A16 Deaktivierung und Deinstal-lation nicht benötigter Komponenten und Kennungen</a> .	Privileg: <i>SeDebugPrivilege</i>
<a href="#">Deny Access to this computer from the network</a>	Siehe Empfehlungen zur Anforderung <a href="#">SYS.2.1.A1 Sichere Benutzerauthenti-sierung</a> (bei Einsatz von LAPS) und <a href="#">SYS.2.2.3.A11 Schutz der Anmeldeinforma-tionen unter Windows 10</a> .	Recht: <i>SeDenyNetworkLogonRight</i>
<a href="#">Deny log on as a batch job</a>	ANONYMOUS LOGON, Guests	Recht: <i>SeDenyBatchLogonRight</i>

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
		Durch Hinzufügen von „ANONYMOUS LOGON, Guests“ zu der Liste soll verhindert werden, dass sich diese Konten als Batchaufträge anmelden können.
<a href="#">Deny log on as a service</a>	ANONYMOUS LOGON, Guests	Recht: <i>SeDenyServiceLogonRight</i> Durch Hinzufügen von „ANONYMOUS LOGON, Guests“ zu der Liste soll verhindert werden, dass diese Konten Prozesse als Dienst registrieren können.
<a href="#">Deny log on locally</a>	Siehe Empfehlungen zur Anforderung <a href="#">SYS.2.1.A1 Sichere Benutzerauthentifizierung</a> .	Recht: <i>SeDenyInteractiveLogonRight</i>
<a href="#">Deny log on through Remote Desktop Services</a>	Siehe Empfehlungen zur Anforderung <a href="#">SYS.2.1.A1 Sichere Benutzerauthentifizierung</a> .	Recht: <i>SeDenyRemoteInteractiveLogonRight</i>
<a href="#">Enable computer and user accounts to be trusted for delegation</a>	Es sollten keine Konten oder Gruppen der Liste hinzugefügt werden.	Privileg: <i>SeEnableDelegationPrivilege</i> Durch die Delegation können Anmeldeinformationen von einem an ein weiteres IT-System durchgereicht werden (bspw. von einem Webserver an einen Datenbankdienst). In einer domänenverwalteten Umgebung ist diese Einstellung auf den Clients ohne Relevanz. Die Liste enthält voreingestellt keine Einträge.
<a href="#">Force shutdown from a remote system</a>	Es sollten keine Konten oder Gruppen der Liste hinzugefügt werden.	Privileg: <i>SeRemoteShutdownPrivilege</i> Konten mit diesem Privileg dürfen den Client aus der Ferne über das Netz zum Herunterfahren zwingen. Voreingestellt ist die Gruppe „Administrators“ in der Liste enthalten. Durch das unkontrollierte und unberechtigte Herunterfahren des Clients aus der Ferne können Denial of Service Angriffe durchgeführt werden.
<a href="#">Generate security audits</a>	Es verfügen voreingestellt nur „LOCAL SERVICE“ und „NETWORK SERVICE“ über dieses Privileg. Grundsätzlich sollten keine Konten oder Gruppen der Liste hinzugefügt werden, sofern es keinen Anwendungsfall hierzu gibt.	Privileg: <i>SeAuditPrivilege</i> Das Privileg wird benötigt, um Events über die ReportEvent API in das Security-Event-Log zu schreiben. Das Audit-Log kann bei Kompromittierung eines Kontos ein potenzieller Angriffsvektor sein.
<a href="#">Impersonate a client after authentication</a>	Voreingestellt sind in der Liste die Gruppen und Konten „Administrators,	Privileg: <i>SeImpersonatePrivilege</i>

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
	SERVICE, Local Service, Network Service“ enthalten. Es sollten keine weiteren Konten oder Gruppen der Liste hinzugefügt werden.	Dieses Privileg wird benötigt, wenn ein Thread einen Token für eine Imper-sonierung verwenden möchte.
<a href="#">Increase a process working set</a>	Es sollten keine zusätzlichen Konten oder Gruppen der Liste hinzugefügt werden.	Privileg: <i>SeIncreaseWorkingSetPrivilege</i> Mit dem Privileg können Konten die Anzahl der Speicherseiten, die von Prozessen verwendet werden, reduzieren oder erhöhen. Wird das Working Set für einen Prozess vergrößert, reduziert sich der verbleibende physische Arbeitsspeicher für das System.
<a href="#">Increase scheduling priority</a>	Voreingestellt sind die Gruppen „Administrators“ sowie „Window Manager\Window Manager Group“ enthalten. Es sollten keine weiteren Mitglieder in die Liste aufgenommen werden.	Privileg: <i>SeIncreaseBasePriorityPrivilege</i> Das Privileg ermöglicht Konten, die Priorisierung von Prozessen herauf zu stufen. Hierdurch können jedoch kritische Prozesse in der Priorisierung herabgesetzt werden, sodass ihnen weniger Verarbeitungszeit zur Verfügung steht und es zu Denial-of-Service Situationen kommen kann.
<a href="#">Load and unload device drivers</a>	Voreingestellt ist die Gruppe „Administrators“ in der Liste. Es sollten keine weiteren Mitglieder in die Liste aufgenommen werden.	Privileg: <i>SeLoadDriverPrivilege</i> Mit diesem Privileg können dynamisch Gerätetreiber in den Kernel hinein oder heraus geladen werden. Treiber werden i. d. R. mit hohen Privilegien ausgeführt, sodass das Installieren von Treibern nur administrativen Konten vorbehalten sein sollte.
<a href="#">Lock pages in memory</a>	Die Liste enthält voreingestellt keine Einträge. Es sollten keine Konten oder Gruppen der Liste hinzugefügt werden, sofern es keinen konkreten Anwendungsfall gibt.	Privileg: <i>SeLockMemoryPrivilege</i> Durch das Privileg können Konten festlegen, dass Daten eines Prozesses im physischen Arbeitsspeicher gehalten werden und keine Auslagerung auf die Festplatte erfolgen soll (Pagefile). Durch Sperren der Auslagerungsmöglichkeit können Denial-of-Service Szenarien auftreten, da ggfs. der physische Speicher voll ausgelastet wird.
<a href="#">Log on as a batch job</a>	Voreingestellt sind die Gruppen „Administrators, Backup Operators, Performance Log Users“ enthalten. Es sollten keine weiteren Konten oder Gruppen der Liste hinzugefügt werden, sofern es keinen konkreten Anwendungsfall gibt.	Recht: <i>SeBatchLogonRight</i> Konten mit diesem Recht können beispielsweise in geplanten Aufgaben im Task Scheduler angegeben werden, damit sie mit den Rechten des Benutzenden ausgeführt werden. Es sollten nur Konten mit dem Recht ausgestattet werden, die dieses explizit für diese Aufgabe benötigen.



<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
<a href="#">Log on as a service</a>	Voreingestellt befindet sich in der Liste ein virtuelles Dienstkonto: „NT SERVICE\ALL SERVICES“. Es sollten keine weiteren Konten oder Gruppen der Liste hinzugefügt werden, sofern es keinen konkreten Anwendungsfall gibt.	Recht: <i>SeServiceLogonRight</i> Konten mit diesem Recht können Dienste und Netzdienste starten, die durchgehend laufen (im Hintergrund, auch wenn kein Konto interaktiv am Client angemeldet ist).
<a href="#">Manage auditing and security log</a>	Voreingestellt ist die Gruppe „Administrators“ in der Liste enthalten. Es sollten keine weiteren Konten oder Gruppen der Liste hinzugefügt werden, sofern es keinen konkreten Anwendungsfall gibt.	Privileg: <i>SeSecurityPrivilege</i> Konten mit diesem Privileg dürfen die Überwachung von Objektzugriffen auf Dateien, AD-Objekte und Registry-Keys verwalten. Darüber hinaus dürfen sie das Security-Log in der Ereignisanzeige lesen und löschen. Die Berechtigung sollte nur administrativen Konten vorbehalten sein, um zu verhindern, dass wichtige Sicherheitsereignisse durch Benutzende gelöscht werden.
<a href="#">Modify an object label</a>	Die Liste enthält voreingestellt keine Einträge. Es sollten keine Konten oder Gruppen der Liste hinzugefügt werden.	Privileg: <i>SeRelabelPrivilege</i> Konten mit diesem Privileg dürfen die Integritätsbezeichner von Objekten modifizieren. Die Integritätsbezeichner kommen im Rahmen von Windows Integrity Controls (WIC) zum Einsatz und sorgen dafür, dass Prozesse mit niedrigerer Integrität Prozesse mit höherer Integrität nicht modifizieren können. Ein Konto, welches dieses Privileg besitzt, könnte bspw. Prozesse mit hoher Integrität missbräuchlich so weit herunterstufen, dass sie von Prozessen mit niedrigerer Integrität gelöscht werden können.
<a href="#">Modify firmware environment values</a>	Siehe Empfehlungen zur Anforderung <a href="#">SYS.2.1.A36 Selbstverwalteter Einsatz von SecureBoot und TPM</a> .	Privileg: <i>SeSystemEnvironmentPrivilege</i>
Obtain an impersonation token for another user in the same session <sup>154</sup>	Die Liste enthält voreingestellt die Gruppe „Administrators“. Es sollten keine Konten oder Gruppen der Liste hinzugefügt werden.	Privileg: <i>SeDelegateSessionUserImpersonatePrivilege</i> Das Privileg ermöglicht Programmen, die im Kontext des Kontos mit diesem Privileg laufen, sich als Client auszugeben.
<a href="#">Perform volume maintenance tasks</a>	Voreingestellt ist die Gruppe „Administrators“ in der Liste enthalten.	Privileg: <i>SeManageVolumePrivilege</i> Mit dem Privileg dürfen Konten administrative Tätigkeiten vornehmen,

<sup>154</sup> Es konnte kein Verweis auf die Microsoft Dokumentation angegeben werden.

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
		die sich auf eine Laufwerks- und Partitionsverwaltung beziehen. Dies umfasst beispielsweise das Erstellen oder Entfernen von Partitionen oder das Ausführen der Datenträgerbereinigung. Administrative Tätigkeiten sollten nur von Administrierenden mit separaten administrativen Konten vorgenommen werden. Daher sollten der Liste keine Konten von Benutzenden hinzugefügt werden.
<a href="#">Profile single process</a>	Voreingestellt ist die Gruppe „Administrators“ in der Liste enthalten.	Privileg: <i>SeProfileSingleProcessPrivilege</i> Konten mit diesem Privileg dürfen sich Leistungsprofile über Anwendungsprozesse anzeigen. In der Regel wird dieses Privileg nicht von Benutzenden benötigt, da die im Betriebssystem enthaltenen Leistungsberichte verwendet werden können.
<a href="#">Profile system performance</a>	Voreingestellt sind die Gruppen „Administrators“ und das Servicekonto „NT SERVICE\WdiServiceHost“ in der Liste enthalten.	Privileg: <i>SeSystemProfilePrivilege</i> Das Privileg ermöglicht Konten die Verwendung der Performance Monitoring Werkzeuge in Windows, um die Leistung von Systemprozessen zu überwachen. Systemprozesse sollten nur von Administrierenden überwacht werden. Mögliche Angreiferinnen und Angreifer könnten die Leistung des Clients überwachen, um kritische Prozesse zu identifizieren und diese gezielt anzugreifen.
<a href="#">Remove computer from docking station</a>	Voreingestellt ist die Gruppe „Administrators“ in der Liste enthalten. Es sollten keine Konten oder Gruppen der Liste hinzugefügt werden. Auch sollten administrative Konten nicht über das Privileg verfügen, sodass der zugehörige Eintrag zu löschen ist.	Privileg: <i>SeUndockPrivilege</i> Konten, denen dieses Privileg zugewiesen wurde, dürfen das Notebook aus einer Dockingstation entfernen, ohne dass der Sperrbildschirm ausgelöst wird und sie sich am System authentisieren müssen.
<a href="#">Replace a process level token</a>	Voreingestellt sind die Konten „Network Service, Local Service“ in der Liste enthalten. Es sollten keine Konten oder Gruppen der Liste hinzugefügt werden.	Privileg: <i>SeAssignPrimaryTokenPrivilege</i> Konten, die über das Privileg verfügen, können Prozesse unter einem anderen Konto ausführen („CreateProcessAsUser“), sofern sie die Anmeldeinformationen des anderen Kontos kennen.

<b>Gruppenrichtlinieneinstellung</b>	<b>Empfehlung</b>	<b>Erläuterung</b>
<a href="#">Restore files and directories</a>	Siehe Empfehlungen zur Anforderung <a href="#">SYS.2.1.A27</a> <a href="#">Geregelte Außerbetriebnahme eines Clients</a> .	Privileg: <i>SeRestorePrivilege</i>
<a href="#">Shut down the system</a>	Voreingestellt dürfen die Gruppen „Backup Operators“ und „Users“ den Windows 10 Client herunterfahren. Die Liste sollte entsprechend der Voreinstellung belassen werden.	Privileg: <i>SeShutdownPrivilege</i> Das Privileg gestattet Konten das Herunterfahren von Windows 10. Primär betrifft eine Begrenzung dieses Privilegs Serversysteme. Ohne das Privileg können Konten zudem keine Einstellungen der Energiesparoptionen vornehmen oder ein geplantes Herunterfahren abbrechen. Sofern Konten von Benutzenden das Recht entzogen wird, kann der Client nicht mehr heruntergefahren werden.
<a href="#">Synchronize directory service data</a>	Die Liste enthält voreingestellt keine Einträge. Es sollten keine Konten oder Gruppen der Liste hinzugefügt werden.	Privileg: <i>SeSyncAgentPrivilege</i> Das Privileg ermöglicht Konten die Synchronisierung jeglicher Verzeichnisservicedaten (Directory Service Data), und zwar unabhängig von den Schutzmechanismen der Objekte oder ihrer Eigenschaften. Dieses Privileg wird von Konten auf Windows 10 Clients nicht benötigt und sollte daher nicht vergeben werden.
<a href="#">Take ownership of files or other objects</a>	Voreingestellt enthält die Liste die Gruppe „Administrators“. Es sollten keine weiteren Konten oder Gruppen der Liste hinzugefügt werden.	Privileg: <i>SeTakeOwnershipPrivilege</i> Voreingestellt ist der Ersteller eines Objektes (auf NTFS oder innerhalb der AD-Datenbank) der Eigentümer (Owner). Die Eigentümer dürfen daher auch die Objektberechtigungen ändern, selbst dann, wenn ihnen jeglicher Zugriff auf das Objekt verwehrt werden sollte. Konten mit diesem Privileg dürfen das Eigentum an einem Objekt übernehmen (Take Ownership). Dies kann ein Sicherheitsrisiko darstellen, da diese hierdurch das Eigentum an jeglichen Objekten innerhalb des Systems übernehmen können.

## 6.1.5 CON.3 Datensicherungskonzept

### CON.3.A5 Regelmäßige Datensicherung [IT-Betrieb] (B)


Zur Umsetzung des Datensicherungskonzeptes (siehe Umsetzungshinweis zu CON.3.M5 Regelmäßige Datensicherung) für Windows 10 Clients bietet Windows 10 die folgenden Funktionen:

## Sichern und Wiederherstellen („Backup and Restore“)

Bei dieser Funktion handelt es sich um die bereits in Windows 7 integrierte Datensicherung und Wiederherstellung. Microsoft hat diese Funktion in Windows 10 (wieder) integriert, um die in früheren Windows-Versionen erstellten Sicherungen auch in Windows 10 weiterhin verfügbar zu machen<sup>155</sup>. Der Funktionsumfang dieses Features besteht in Windows 10 unverändert fort, sodass es hiermit ebenfalls möglich ist, auch Daten unter Windows 10 zu sichern oder ein vollständiges Systemabbild zu erstellen. Von Microsoft wird diese Funktion allerdings nicht näher beworben. Auch kann zum jetzigen Zeitpunkt keine Auskunft darüber gegeben werden, wie Microsoft in zukünftigen Windows 10 Versionen mit diesem Feature verbleibt. Irreführenderweise trägt die Funktion unter Windows 10 im Bezeichner „(Windows 7)“.

### Einrichten einer Datensicherung in Windows 10

Hinweis: Zur Durchführung der Schritte zur Einrichtung der Datensicherung werden administrative Rechte benötigt.

 *Windows Settings* → *Update & Security* → *Backup* → *Go to Backup and Restore (Windows 7)*

Alternativer Aufruf über die Systemsteuerung (Control Panel):

 *Control Panel* → *All Control Panel Items* → *Backup and Restore (Windows 7)*

#### 1. Datensicherung anlegen („Set up backup“)

Backup → Set up backup

#### 2. Speicherort wählen („Select where you want to save your backup“)

Es muss ein Ziellaufwerk ausgewählt werden, das zur Datensicherung verwendet wird. Hierbei sollte es sich idealerweise um einen Wechseldatenträger oder alternativ ein Netzlaufwerk handeln. In beiden Fällen sollte sichergestellt werden, dass dieses nicht permanent mit dem Client verbunden und nach Durchführung einer Datensicherung wieder getrennt wird. Hierdurch kann dem Risiko eines vollständigen Datenverlusts im Fall einer Kompromittierung durch Schadsoftware entgegengewirkt werden.

#### 3. Auswahl der zu sichernden Daten („What do you want to back up?“)

In diesem Schritt bietet Windows 10 zwei Optionen an:

- **Let Windows choose (recommended)**

Bei der Auswahl durch Windows werden alle Kontenprofilverzeichnisse, Inhalte der Bibliotheken (Dokumente, Bilder, Musik, Videos, etc.) sowie ein Systemabbild gesichert.

- **Let me choose**

Bei der von Benutzenden selbst festzulegenden Auswahl können individuell Verzeichnisse in die Datensicherung miteingeschlossen werden, um diese durch Windows zu sichern.

Die Option „Include a system image of drives: System reserved, (C), Windows Recovery Environment“ ist bereits vorausgewählt.

#### 4. Sicherungseinstellungen überprüfen („Review your backup settings“)

Im letzten Schritt werden die Einstellungen über die Datensicherungskonfiguration zusammengefasst und ein Zeitplan (Schedule) zur Durchführung der automatischen Datensicherung festgelegt. Die Datensicherung kann jederzeit auch manuell gestartet werden. Hierzu ist die Schaltfläche „Back up now“ unter „Backup and Restore (Windows 7)“ in der Systemsteuerung zu wählen.

---


<sup>155</sup> <https://support.microsoft.com/de-de/help/4027408/windows-10-backup-and-restore>


## 5. Überprüfen des Status der Datensicherung

Die korrekte Ausführung der Datensicherung sollte in der Systemsteuerung überprüft werden. Bei auftretenden Fehlern, sollten diese näher analysiert und gegebenenfalls die Datensicherungseinstellungen überprüft werden.

### Wiederherstellen von Dateien aus einer Datensicherung in Windows 10

Vorhandene Datensicherungen, die mit Windows erstellt worden sind, können hinsichtlich wiederherzustellender Dateien und Ordner durchsucht und wiederhergestellt werden. Hierfür sind im Gegensatz zur Erstellung von Datensicherungen keine administrativen Rechte erforderlich:

 *Windows Settings* → *Update & Security* → *Backup* → *Go to Backup and Restore (Windows 7)* → *Restore my files*

 *Control Panel* → *All Control Panel Items* → *Backup and Restore (Windows 7)* → *Restore my files*

#### 1. Durchsuchen der Datensicherung und Auswahl der wiederherzustellenden Dateien und Ordner („Browse or search your backup for files and folders to restore“)

Mittels Suchbegriff kann ein Datei- oder Ordnername ganz oder teilweise eingegeben werden, nach dem in der Datensicherung gesucht wird. Durch die Auswahlbox können diese zur Wiederherstellung vorge-merkt werden.

#### 2. Auswahl eines Wiederherstellungsortes („Where do you want to restore your files?“)

Dateien und Ordner können entweder an ihren ursprünglichen Pfad (engl.: *In the original location*) im Dateisystem wiederhergestellt werden, in denen sie sich zum Zeitpunkt der Datensicherung befunden haben oder unter Angabe eines neuen Pfades (engl.: *In the following location:*) wiederhergestellt werden.


#### 3. Wiederherstellen („Restore“)

Im letzten Schritt werden die Dateien durch Bestätigung der Schaltfläche „Restore“ aus der Datensicherung wiederhergestellt. Sofern am Zielort Dateien mit gleichem Dateinamen existieren, werden Benutzende für jeden einzelnen Fall dazu aufgefordert, auszuwählen, ob die Datei aus der Datensicherung an den Zielort kopiert und ersetzt, nicht kopiert oder kopiert, aber beide Dateien behalten werden sollen. In letztem Fall wird dem Dateinamen eine „(2)“ hinzugefügt.

Nach Abschluss der Datenwiederherstellung sollte eine entsprechende Meldung im Assistenten angezeigt werden („Your files have been restored“).

### Systemabbild („System Image“) erstellen

Um im Falle eines Defekts (z. B. bei Ausfall der Festplatte) das Systemlaufwerk, auf dem sich die Windows-Installation befindet, wiederherstellen zu können, muss zuvor ein Systemabbild und ein Systemreparaturdatenträger erstellt worden sein. Hierzu liefert Windows 10 ein Tool mit, das den gesamten Inhalt jeder Festplatte jeweils in einer eigenen Virtual Hard Disk-Datei sichert:

 *Windows Settings* → *Update & Security* → *Backup* → *Go to Backup and Restore (Windows 7)* → *Create a system image*

 *Control Panel* → *All Control Panel Items* → *Backup and Restore (Windows 7)* → *Create a system image*

#### 1. Auswahl eines Speicherortes für das Systemabbild („Where do you want to save the backup?“)

Mögliche Zielorte sind lokale Laufwerke, Wechseldatenträger oder ein Netzspeicherort. Bei der Auswahl sollte einerseits beachtet werden, dass der verfügbare Speicherplatz ausreichend zur Verfügung steht und andererseits nicht dauerhaft mit dem Client verbunden ist.

#### 2. Zusammenfassung und Bestätigung der Datensicherungseinstellungen („Confirm you backup settings“)


In einem Systemabbild werden in der Voreinstellung folgende Laufwerke gesichert:

- System Reserved (System)
- (C:) (System)
- Windows Recovery Environment (System)

Diese können nicht für die Erstellung eines Systemabbildes ausgewählt werden. Es können jedoch in der Liste weitere Laufwerke bzw. Partitionen ausgewählt werden, die mit in das zu erzeugende Systemabbild aufgenommen werden sollen.

### 3. Starten des Sicherungsvorgangs („Start backup“)


#### Wiederherstellen eines Systemabbilds


 *Windows Settings* → *Update & Security* → *Recovery* → *Advanced startup* → *Restart now*

1. („Reset PC and Advanced options“)
2. **Advanced options**
3. **System Image Recovery**

#### Systemreparaturdatenträger („System repair disk“) erstellen

Im Gegensatz zu einem Wiederherstellungslaufwerk („Repair Disk“) beinhaltet ein Wiederherstellungsmedium nur Werkzeuge („Tools“), die im Problemfall zur Systemreparatur eingesetzt werden können. Darüber hinaus kann mittels des Systemreparaturdatenträgers ein vorab erstelltes Systemabbild wiederhergestellt werden. Weitere Informationen zur Windows Wiederherstellungsumgebung (s. u).

 *Windows Settings* → *Update & Security* → *Backup* → *Go to Backup and Restore (Windows 7)* → *Create a system repair disk*

 *Control Panel* → *All Control Panel Items* → *Backup and Restore (Windows 7)* → *Create a system repair disk*

1. **Auswahl eines CD/DVD-Laufwerkes („Create a system repair disk“)**  
Hinweis: Damit ein Systemreparaturdatenträger erstellt werden kann, muss ein CD/DVD-Brenner vorhanden sein oder angeschlossen werden.
2. **Datenträger erstellen („Create disc“)**  
Sofern ein CD/DVD-Brenner erkannt worden ist und ein Rohling eingelegt wurde, kann der Systemreparaturdatenträger erstellt werden.
3. **Abschluss des Datenträgers**  
Sobald der Vorgang abgeschlossen ist, sollte der Datenträger entsprechend beschriftet werden und idealerweise zu vorhandenen Datensicherungslaufwerken abgelegt werden.

#### Wiederherstellungslaufwerk (Recovery Drive)<sup>156</sup>

Durch Anlegen eines Wiederherstellungslaufwerkes kann Windows 10 im Problemfall zügig wiederhergestellt bzw. neu installiert werden. Auf diesem Laufwerk, bei dem es sich um ein USB-Wechselmedium (USB-Stick oder USB-Festplatte) handelt, wird der aktuelle Stand der Systemdateien gesichert. Nicht Bestandteil des Wiederherstellungslaufwerkes ist die Sicherung von persönlichen Dateien, Programmen oder Apps. Im Wiederherstellungsfall kann vom Recovery Drive gebootet werden und Windows 10 neu installiert und eingerichtet werden.

<sup>156</sup> <https://support.microsoft.com/en-us/windows/create-a-recovery-drive-abb4691b-5324-6d4a-8766-73fab304c246>

 Control Panel → All Control Panel Items → Recovery → Create a recovery drive

1. Erstellen eines Wiederherstellungslaufwerks („Create a recovery drive“)
2. Auswahl der Sicherung von Systemdateien („Back up system files to the recovery drive“)
3. Es muss ein USB-Wechseldatenträger ausgewählt werden.  
Achtung: Der Datenträger wird formatiert.

Alternativ kann das Wiederherstellungslaufwerk mit flexibleren Parametern auch über die Kommandozeile erstellt werden. Hierzu stellt Microsoft folgende weiterführende Dokumentation zur Verfügung:

- <https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/customize-windows-re?view=windows-10>

Wiederherstellungslaufwerke können dazu genutzt werden, um ein System neu zu installieren oder zu reparieren, wenn ein System nicht mehr gestartet werden kann. Das System wird dann zum Stand der Erstellung des Wiederherstellungslaufwerks wiederhergestellt. Daher können auch Aktualisierungen des Wiederherstellungslaufwerks regelmäßig durchgeführt werden, sodass sich dieses immer auf einem möglichst aktuellen Stand befindet. Dieses kann durch Integration der Windows Updates<sup>157</sup> oder aber einer vollständigen Neuerstellung des Wiederherstellungslaufwerks erfolgen. Bei der Auswahl eines geeigneten Wiederherstellungslaufwerks sollte sowohl berücksichtigt werden, inwiefern dieses von möglichen Hardwaredefekten betroffen sein kann, bspw. bei Festplatten, als auch die Möglichkeit, dieses aktuell zu halten.

In vielen Fällen liefern Geräteherstellende ihre vorinstallierten Windows-Versionen mit konfigurierten Wiederherstellungsoptionen aus. Diese sollten getestet werden, ob sie den eigenen Anforderungen genügen.

Bei der Verteilung von Windows 10 mittels individuell angepasster Installationsabbilder können die Systempartitionen individuell auf die eigenen Bedürfnisse angepasst und konfiguriert werden. Hierzu stellt Microsoft eine weiterführende Dokumentation zur Verfügung:

- <https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/capture-and-apply-windows-system-and-recovery-partitions>

#### Dateiversionsverlauf<sup>158</sup>

Der Dateiversionsverlauf sichert in regelmäßigen Abständen (Voreingestellt bei aktivierten Dateiversionsverlauf ist stündlich) den Stand von Dateien auf ein festzulegendes Laufwerk. Das festzulegende Laufwerk sollte dabei nicht dem Laufwerk entsprechen, von dem gesichert wird. Es werden nur die persönlichen Dateien des zurzeit angemeldeten Kontos gesichert. Gesichert werden Ordner aus dem Kontenprofil, wie z. B. Bilder, Dokumente Kontakte, Favoriten und der persönliche Desktop. Gegebenenfalls sollten weitere Verzeichnisse mit in die Dateiversionierung aufgenommen werden, wenn auch diese mit gesichert werden sollen.

Der Begriff „Verlauf“ suggeriert, dass Dateien fortlaufend gesichert werden. In festgelegten Zeitintervallen werden automatisch Kopien der geänderten Dateien erstellt. Das gewählte Sicherungslaufwerk muss hierzu zur Verfügung stehen (permanent angeschlossen).

<sup>157</sup> <https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/add-update-to-winre?view=windows-10>

<sup>158</sup> <https://support.microsoft.com/en-us/windows/file-history-in-windows-5de0e203-ebae-05ab-db85-d5aa0a199255>

⚙️ *Windows Settings* → *Update & Security* → *Backup* → *Backup using File History*

🖥️ *Control Panel* → *All Control Panel Items* → *File History*

Jedes Konto kann spezifisch festlegen, welches (externes) Laufwerk für die Datensicherung verwendet werden soll.

Ein permanent mit dem Client verbundenes Laufwerk zur Sicherung des Dateiversionsverlaufs kann im Falle einer, beispielsweise durch einen Verschlüsselungstrojaner, ebenfalls von einer Kompromittierung betroffen sein, sodass die gesicherten Daten unwiderruflich zerstört werden können. Wenn das Laufwerk nicht direkt verbunden ist, besteht die Herausforderung den Dateiversionsverlauf ausreichend aktuell zu halten. Der Dateiversionsverlauf wird weiterhin angelegt und im Verzeichnis

```
%APPDATA%\Local\Microsoft\Windows\FileHistory
```

des jeweiligen Benutzenden gespeichert. Regelmäßig sollte das Sicherungslaufwerk angeschlossen oder verbunden werden und manuell über die Schaltfläche „Run now“ in einem der o.g. Konfigurationspfade angestoßen werden.

### Wiederherstellungspunkt (Systemwiederherstellungspunkt)

Die Systemwiederherstellung ist keine echte Datensicherung. Deshalb soll diese Methode nur als ergänzende – gleichwohl sinnvolle – Maßnahme zu einer tatsächlichen Datensicherung gesehen werden.

Durch Setzen eines Systemwiederherstellungspunktes werden installierte Software, Treiber, Updates, Einstellungen und Programmdateien gesichert. Funktioniert zum Beispiel nach der Installation eines Treibers Windows nicht mehr, kann über die Systemwiederherstellung zu einem Zeitpunkt zurückgekehrt werden, zu dem das System noch stabil agierte. Windows ist dann wieder auf dem Stand, an welchem der Wiederherstellungspunkt gesetzt wurde.

Windows bietet an, einen Wiederherstellungspunkt zu setzen, wenn es der Annahme ist, dass ein tieferer Eingriff in das System vorgenommen wird. Das kann der Fall sein, wenn ein neuer Treiber oder eine Aktualisierung von Windows installiert wird. Unabhängig davon können manuelle Wiederherstellungspunkte gesetzt werden.

**Wichtig:** Einen neuen Wiederherstellungspunkt zu setzen bedeutet keinen Schutz persönlicher Dateien. Vielmehr soll eine Neuinstallation von Windows sowie der verwendeten Programme und etwaiger Anpassungen vermieden werden.

🖥️ *Computer Configuration/Administrative Templates/Windows Components/Windows Defender Antivirus/Scan*

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Create a system restore point	<b>Enabled</b>	Voreingestellt wird einmal wöchentlich bzw. vor einer Software-/Treiberinstallation mit aus Sicht von Windows möglichen Auswirkungen auf die Systemstabilität ein Systemwiederherstellungspunkt durch das System erzeugt. Voraussetzung hierfür ist, dass die Systempartition mindestens eine Größe von 128 GB aufweist <sup>159</sup> . Durch das Aktivieren der Richtlinie wird täglich ein Systemwiederherstellungspunkt angelegt.

<sup>159</sup> <https://learn.microsoft.com/en-us/troubleshoot/windows-client/deployment/system-restore-points-disabled>





Computer Configuration/Administrative Templates/System/System Restore

Gruppenrichtlinieneinstellung	Empfehlung	Erläuterung
Turn off System Restore	Disabled	Die Systemwiederherstellung sollte nicht deaktiviert werden, damit Administrierende bei Bedarf eine Wiederherstellung durchführen können.

### Aktivieren der Systemwiederherstellung über die grafische Bedienschnittstelle



Control Panel → All Control Panel Items → Recovery → Configure System Restore

1. Auswahl „Configure“
2. Auswahl „Turn on system protection“
3. Auswahl des maximal beanspruchbaren Speicherplatzes für die Wiederherstellungspunkte

### Anpassung des zur Verfügung stehenden Speicherkontingents für Systemwiederherstellungspunkte

Eine Anpassung der maximalen Speichermenge für die Systemwiederherstellungspunkte kann über die Kommandozeile (CMD) vorgenommen werden<sup>160</sup>:

```
C:\> vssadmin resize shadowstorage /for=<ForVolumeSpec> /on=<OnVolumeSpec>
[/maxsize=<MaxSizeSpec>]
```

Alternativ kann die Größe des zur Verfügung stehenden Speicherplatzes für die Wiederherstellungspunkte auch über die grafische Oberfläche konfiguriert werden:



Control Panel → All Control Panel Items → Recovery → Configure System Restore → System Restore → Configure → Disk Space Usage

Hier können ebenfalls bereits alle angelegten Systemwiederherstellungspunkte gelöscht werden.

### Wiederherstellung von Wiederherstellungspunkten

Die Systemwiederherstellung zu einem vorherigen Systemwiederherstellungspunkt kann aus Windows 10 heraus oder über die Windows-Wiederherstellungsumgebung erfolgen:

### Systemwiederherstellung über die Systemsteuerung



Control Panel → All Control Panel Items → Recovery → Configure System Restore → System Restore

Hinweis: Ist die Schaltfläche ausgegraut, ist die Systemwiederherstellung nicht konfiguriert worden. Die Schutzeinstellungen für die verfügbaren Laufwerke können aus der Spalte „Schutz“ (Protection) entnommen werden.

Anschließend sollte der zuletzt aufgezeichnete Wiederherstellungspunkt ausgewählt werden, um den Zustand von Windows zum Zeitpunkt der Aufzeichnung zurückzusetzen. Sollte das Problem nach der Systemwiederherstellung nicht behoben worden sein, sollte mit dem vorherigen Systemwiederherstellungspunkt fortgefahren werden.

<sup>160</sup> <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/vssadmin-resize-shadowstorage>

## Systemwiederherstellung über die Windows-Wiederherstellungsumgebung

### 1. Windows Settings

Windows Settings → Update & Security → Recovery → Advanced Startup: „**Restart now**“ auswählen.

### 2. Start-Menü

Im Start-Menü lässt sich nach Anklicken des Ein/Aus-Buttons mit gehaltener Umschalttaste „**Restart**“ auswählen.

### 3. Anmelde-/Sperrbildschirm

Auf dem Anmelde-/Sperrbildschirm lässt sich nach Anklicken des Ein/Aus-Buttons mit gehaltener Umschalttaste „**Restart**“ auswählen.

Unabhängig der gewählten Möglichkeit wird anschließend ein Auswahlmenü angezeigt, bei dem folgende Optionen ausgewählt werden müssen:

#### 1. Troubleshoot („Reset your PC or see advanced options“)

#### 2. Advanced options

#### 3. System Restore („Use a restore point recorded on your PC to restore Windows.“)

Anschließend sollte der zuletzt aufgezeichnete Wiederherstellungspunkt ausgewählt werden, um den Zustand von Windows zum Zeitpunkt der Aufzeichnung zurückzusetzen. Sollte das Problem nach der Systemwiederherstellung nicht behoben worden sein, sollte mit dem vorherigen Systemwiederherstellungspunkt fortgefahren werden.

## Windows-Wiederherstellungsumgebung (Windows Recovery Environment, kurz: Windows RE)

Die Windows-Wiederherstellungsumgebung basiert auf der Windows Preinstallation Environment (Windows PE) und stellt Werkzeuge sowie Funktionen zur Behebung allgemeiner Probleme mit dem Betriebssystem zur Verfügung, wenn es beispielsweise nicht mehr ordnungsgemäß gestartet werden kann. Die Umgebung wird auf einer versteckten Partition während der Betriebssysteminstallation installiert und bereitgestellt, die den Bezeichner „Recovery“ trägt. Alternativ kann auch ein Wiederherstellungsmedium erstellt werden, das die Werkzeuge und Tools von Windows RE beinhaltet und im Problemfall gebootet werden kann.

Mit Hilfe der Werkzeuge von Windows RE werden folgende Möglichkeiten zur Verfügung gestellt:

- Automatische Reparatur und Tools für die Problembehandlung
  - Automatische Reparatur (Startup Repair)  
Durch die automatische Reparatur sollen Fehler und Probleme behoben werden, die den Startvorgang des Betriebssystems verhindern.
  - Änderung von Startoptionen
  - Deinstallation von Updates (Windows Qualitäts- und/oder Feature-Updates)
  - Eingabeaufforderung (mit Zugriff auf diverse Systemwerkzeuge)
- Wiederherstellung eines Systemwiederherstellungspunktes
- Wiederherstellung mittels eines Systemabbilds (Laufwerksabbild), sofern dieses vorab erstellt worden ist
- Zurücksetzen des „Computers“
  - unter Beibehalten der persönlichen Daten oder
  - mit einfachem Löschen der persönlichen Daten.

Eine umfassende Erläuterung zu Windows RE werden in einem TechNet-Bertrag zusammengefasst:

- <https://techcommunity.microsoft.com/t5/windows-it-pro-blog/windows-recovery-environment-explained/ba-p/2273533>

## 6.2 Standardanforderungen

### 6.2.1 DER.1 Detektion von sicherheitsrelevanten Ereignissen

#### **DER.1.A11 Nutzung einer zentralen Protokollierungsinfrastruktur für die Auswertung sicherheitsrelevanter Ereignisse [Fachverantwortliche] (S)**

Microsoft stellt über die Dokumentation eine Hilfestellung zur Verfügung, wie Ereignisse zur Detektion an eine zentrale Protokollierungsinfrastruktur weitergeleitet werden können:

- <https://learn.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection>

### 6.2.2 OPS.1.1.4 Schutz vor Schadprogrammen

#### **OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen [Benutzer] (S)**

Microsoft Defender protokolliert Schadsoftwarefunde und Angriffsversuche im Windows Event Log. Wenn keine zentrale Sammlung und Auswertung der Protokolle erfolgt, muss regelmäßig das lokale Event Log kontrolliert werden. Zusätzlich sollten die Benutzenden sensibilisiert werden, auf entsprechende Benachrichtigungen zu reagieren.

## 7 Überprüfung von angewendeten Gruppenrichtlinien

### 7.1 Resultant Set of Policy (RSoP)

Durch ein Resultant Set of Policy (RSoP) lässt sich die Anwendung von Gruppenrichtlinien auf Clients und Servern sowie Konten serverseitig durch eine Abfrage ermitteln.

Mit dem Resultant Set of Policy Assistenten in den Active Directory Verwaltungskonsolen lassen sich RSoP-Abfragen erstellen:

Microsoft Management Console → Active Directory Users and Computers

oder

Microsoft Management Console → Active Directory Users and Computers → Active Directory Sites and Services

Im Assistenten wird ein Zielcomputer und -konto ausgewählt, für den ein Richtlinienergebnis ermittelt werden soll. Nach Abschluss des Assistenten werden die angewendeten und abgelehnten Gruppenrichtlinienobjekte ermittelt. Darüber hinaus können in der Zusammenfassung die tatsächlich angewendeten Einstellungen überprüft und kontrolliert werden.

- Weitere Informationen und Anleitung zur Verwendung von RSoP:  
[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn265978\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn265978(v=ws.11))  
<https://learn.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-resultant-set-of-policy-logging>

RSoP kann auch dazu verwendet werden, um die Anwendung von Gruppenrichtlinieneinstellungen auf Computer und Konten zu simulieren (sog. „Group Policy Modeling“).

### 7.2 Berichtserstellung (GPResult)

Mit *GPResult* als Kommandozeilenwerkzeug lassen sich analog zu RSoP Gruppenrichtlinienergebnissätze über lokale oder entfernte Clients erzeugen, aus denen hervorgeht, welche Gruppenrichtlinienobjekte und -einstellungen angewendet oder abgelehnt wurden.

- **Syntax von GPResult**  
<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult>

## 8 Weiterführende Informationen und Hinweise

### 8.1 Problem- und Fehleranalyse

Das BSI kann keine individuelle Unterstützung für Anwendende anbieten. Hierzu zählen individuelle Fragen zur Einstellung bestimmter Konfigurationen und zu den Auswirkungen auf die IT-Infrastruktur.

Die im Hilfsmittel bereitgestellten Empfehlungen zur Konfiguration für Windows 10 20H2 sollten vor Einsatz in einer Produktivumgebung in einer Referenzinstanz/-installation in einer Testumgebung ausreichend hinsichtlich möglicher Auswirkungen und Beeinträchtigungen getestet werden.

Bei auftretendem unerwünschtem Verhalten ist es ratsam, thematisch zuordenbare Konfigurationsparameter (Gruppenrichtlinieneinstellungen, Registrierungsschlüssel und -werte) sukzessive in den Ursprungszustand zurück zu überführen, bis dieses Verhalten nicht mehr auftritt. Identifizierte Einstellungen, die zum Verhalten geführt haben, sollten unter Angabe der Ursache mit der Lösung entsprechend dokumentiert werden.

**Hinweis:** Einige Gruppenrichtlinieneinstellungen, die nach ihrer Aktivierung wieder deaktiviert werden, bleiben möglicherweise weiterhin aktiv. In diesem Fall muss der Wert innerhalb der Richtlinieneinstellung explizit abgeändert und gesetzt werden. Einige Gruppenrichtlinieneinstellungen können außerdem einen Neustart des Systems oder des betroffenen Dienstes erforderlich machen, bevor sie angewendet werden.

### 8.2 Unterstützung durch Microsoft

- **Microsoft Windows 10 – Produktsupport**  
<https://support.microsoft.com/de-de/windows?ui=de-DE&rs=de-DE&ad=DE>
- **Microsoft Windows 10 – TechNet Foren**  
<https://social.technet.microsoft.com/Forums/de-DE/home?forum=win10itprogeneralDE>
- **Microsoft globaler Kundendienst-Telefonnummern**  
<https://support.microsoft.com/de-de/topic/globale-kundendienst-telefonnummern-c0389ade-5640-e588-8b0e-28de8afeb3f2>
- **Microsoft-Support**  
<https://support.microsoft.com/de-de/contactus>
- **Technische Dokumentation zu Windows**  
<https://learn.microsoft.com/de-de/windows/resources/>

### 8.3 Vorschläge und Anregungen

Bestimmte Konfigurationen können sich in individualisierten IT-Infrastrukturen und Umgebungen anders auswirken, als dies pauschal und generell für alle denkbaren Szenarien vorhersehbar wäre. Das BSI ist deshalb interessiert an Erfahrungen aus der Praxis mit den Empfehlungen zur Konfiguration aus dem Hilfsmittel und freut sich über Rückmeldungen sowie Vorschläge und Anregungen zur Verbesserung des Hilfsmittels zur Umsetzung von Anforderungen des IT-Grundschutzes für Windows 10 an:

[grundschutz@bsi.bund.de](mailto:grundschutz@bsi.bund.de)

## 9 Verzeichnisse und Anhänge

Tabelle 1: Änderungshistorie.....	2
Tabelle 2: Verzeichnisstruktur und Inhalt der Microsoft Security Baselines („Windows 10 Version 20H2 and Windows Server Version 20H2 Security Baseline.zip“).....	9
Tabelle 3: Authentifizierungsmethoden in Windows 10.....	22
Tabelle 4: Updatekategorien in Windows.....	28
Tabelle 5: Verbindungskommunikationsendpunkte für Windows Update - Dienste.....	32
Tabelle 6: Verbindungskommunikationsendpunkte für Windows Defender Definition Updates.....	42
Tabelle 7: Verbindungskommunikationsendpunkt für den Abruf von Treibermetainformationen.....	52
Tabelle 8: Übersicht der Konten in Windows 10.....	57
Tabelle 9: Übersicht der Gruppen in Windows 10.....	57
Tabelle 10: Starttypen der Windows-Dienste.....	62
Tabelle 11: Exemplarischer Aufbau der Bezeichnung von Cipher Suites.....	81
Tabelle 12: Übersicht der vorinstallierten (Verwaltungs-)Werkzeuge.....	87
Tabelle 13: Protokolle und Schnittstellen von Desired State Configuration (DSC) und PowerShell Remoting.....	91
Tabelle 14: Protokolle und Schnittstellen von Windows Script Host Remoting und Windows Remote WMI.....	92
Tabelle 15: Voreinstellungen des Exploit-Schutzes (Systemeinstellungen).....	105
Tabelle 16: Möglichkeiten zur Konfiguration der systemweiten Mitigationen in den Systemeinstellungen.....	107
Tabelle 17: Unterschiede der Konfigurationsoptionen im Hinblick auf ASLR, DEP und SEHOP.....	107
Tabelle 18: Voreinstellungen des Exploit-Schutzes (Programmeinstellungen).....	107
Tabelle 19: Voreingestellte Speicherorte in Windows 10 für Konten-spezifische Daten.....	111
Tabelle 20: Auswirkungen der Firewallregeln (Matrix) auf ausgehende Verbindungen.....	119
Tabelle 21: Auswirkungen von Allow-/ Block-Regeln (Matrix) auf eingehende Verbindungen.....	119
Tabelle 22: Unterstützte Anmeldeinformationsanbieter in Windows 10.....	133
Tabelle 23: RemoteFX im Vergleich zur RDP High-Level Device Redirection.....	158

# Literaturverzeichnis

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021.** Einstellungen Härtungsempfehlungen (Version 1.1). [Online] 2021. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage11\\_Einstellungen\\_Haertungsempfehlung\\_V1\\_1.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage11_Einstellungen_Haertungsempfehlung_V1_1.html).

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2022.** IT-Grundschutz-Kompendium (Edition 2022). [Online] 1.. Februar 2022. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT\\_Grundschutz\\_Kompendium\\_Edition2022.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.html).

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021.** Konfigurationsempfehlungen zur Härtung von Windows 10 mit Bordmitteln. [Online] BSI, 2021. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen\\_zur\\_Haertung\\_von\\_Windows\\_10.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen_zur_Haertung_von_Windows_10.html).

**Bundesamt für Sicherheit in der Informationstechnik (BSI).** Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10 (SiSyPHuS Win10). [Online] [https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS\\_Win10/SiSyPHuS\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/SiSyPHuS_node.html).

**Bundesamt für Sicherheit in der Informationstechnik (BSI). 2019.** Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019. [Online] 04. 02 2019. [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise\\_Kompendium\\_CD\\_2019.html](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.html).

**Center for Internet Security (CIS).** CIS Microsoft Windows 10 Enterprise (Release 20H2 or older) Benchmark. [Online] [https://www.cisecurity.org/cis-benchmarks/#microsoft\\_windows\\_desktop](https://www.cisecurity.org/cis-benchmarks/#microsoft_windows_desktop).

**Microsoft Corp. 2021.** Finale Security Baselines für Windows 10 und Windows Server (Version 20H2). [Online] 07. 01 2021. <https://www.microsoft.com/de-de/techwiese/news/finale-security-baselines-fuer-windows-10-und-windows-server-version-20h2.aspx>.

**Pavel Yosifovich, Mark E. Russinovich, Alex Ionescu, David A. Solomon. 2017.** *Windows Internals, Part 1: System architecture, processes, threads, memory management, and more, 7th Edition*. Redmond, Washington : Microsoft Press, 2017.

**Unified Compliance. 2021.** Windows 10 Security Technical Implementation Guide (STIG). [Online] 10. März 2021. [https://www.stigviewer.com/stig/windows\\_10/](https://www.stigviewer.com/stig/windows_10/).

**Voges, Holger und Dausch, Martin. 2019.** *Gruppenrichtlinien in Windows Server und Windows 10*. München : Carl Hanser Verlag, 2019. ISBN 978-3-446-45549-8.