ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
1.	MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure environments)		Disabled	M 4.245 Basiseinstellungen für Windows Group Policy Objects https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04245.html
2.	Remove Program Compatibility Property Page		Enabled	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
3.	Turn off Application Compatibility Engine		Not Configured	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
4.	Detect compatibility issues for applications and drivers		Enabled	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
5.	Turn off Program Compatibility Assistant		Not Configured	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
6.	Turn off SwitchBack Compatibility Engine		Not Configured	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
7.	Notify blocked drivers		Not Configured	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
8.	Detect application installers that need to be run as administrator		Enabled	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
		Scenario Execution Level	Detection, Troubleshooting and Resolution	
9.	Detect application install failures		Not Configured	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
10.	Detect application failures caused by deprecated Windows DLLs		Not Configured	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
		Scenario Execution Level		
11.	Detect applications unable to launch installers under UAC		Enabled	M 2.441 Kompatibilitätsprüfung von Software gegenüber

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Scenario Execution Level	Detection and Troubleshooting Only	Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
12.	Detect application failures caused by deprecated COM objects		Not Configured	M 2.441 Kompatibilitätsprüfung von Software gegenüber Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02441.html
		Scenario Execution Level		
13.	Accounts: Rename guest account		default-guest-renamed	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
14.	Accounts: Rename administrator account		default-administrator-renamded	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
15.	Interactive logon: Number of previous logons to cache (in case domain controller is not available)		2	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
16.	Interactive logon: Require Domain Controller authentication to unlock workstation		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
17.	Interactive logon: Do not require CTRL+ALT+DEL		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
18.	Recovery console: Allow automatic administrative logon		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
19.	MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
20.	Interactive logon: Prompt user to change password before expiration		14	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
21.	Interactive logon: Message text for users attempting to log on		Dieses System ist auf autorisierte Benutzer beschränkt. Der Versuch, nicht autorisierten Zugriff zu erlangen, wird strafrechtlich verfolgt.	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
22.	Interactive logon: Message title for users attempting to log on		SIE MACHEN SICH STRAFBAR, WENN SIE OHNE ERFORDERLICHE AUTORISIERUNG FORTFAHREN	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
23.	Interactive logon: Machine inactivity limit		900	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
24.	Interactive logon: Do not display last user name		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
25.	Interactive logon: Display user information when the session is locked		Do not display user information	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
26.	Shutdown: Allow system to be shut down without having to log on		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
27.	Devices: Allow undock without having to log on		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
28.	Allow log on through Remote Desktop Services		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
29.	Deny log on through Remote Desktop Services		Guests	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
30.	Deny log on locally		Guests	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
31.	Log on as a batch job		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
32.	Deny log on as a batch job		Guests	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
33.	Deny log on as a service		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
34.	Log on as a service		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
35.	Allow log on locally		Administrators, Users	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
36.	ASLR		Enabled	M 4.245 Basiseinstellungen für Windows Group Policy Objects https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04245.html
		ASLR Setting:	Application Opt In	

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
37.	Account lockout threshold		3	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
38.	Account lockout duration		60	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
39.	Reset account lockout counter after		30	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
40.	Minimum password length		8	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
41.	Enforce password history		6	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
42.	Password must meet complexity requirements		Enabled	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
43.	Store passwords using reversible encryption		Disabled	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
44.	Minimum password age		1	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
45.	Maximum password age		90	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
46.	Domain member: Maximum machine account password age		30	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
47.	Domain member: Disable machine account password changes		Disabled	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html M 4.48 Passwortschutz unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html
48.	Interactive logon: Machine account lockout threshold		10	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
49.	Accounts: Administrator account status		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
50.	Accounts: Block Microsoft accounts		Users can't add or log on with Microsoft accounts	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
51.	Accounts: Guest account status		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
52.	Enumerate administrator accounts on elevation		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
53.	Enable computer and user accounts to be trusted for delegation		No One	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
54.	Accounts: Limit local account use of blank passwords to console logon only		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
55.	User management of sharing user name, account picture, and		Enabled	M 4.244 Sichere Systemkonfiguration von

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
	domain information with apps (not desktop apps)	Action:	Always off	Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
56.	Validate smart card certificate usage rule compliance		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Object identifier:		
57.	Choose drive encryption method and cipher strength		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Select the encryption method:	AES 256-bit	
58.	Prevent memory overwrite on restart		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
59.	Choose default folder for recovery password		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Configure the default folder path:		
60.	Provide the unique identifiers for your organization		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Allowed BitLocker identification field:		
		BitLocker identification field:		
61.	Allow access to BitLocker-protected fixed data drives from earlier versions of Windows		Disabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Do not install BitLocker To Go Reader on FAT formatted fixed drives		
62.	Choose how BitLocker-protected fixed drives can be recovered		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Allow data recovery agent	WAHR	
		Configure storage of BitLocker recovery information to AD DS:	Backup recovery passwords and key packages	
		Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives	FALSCH	
		Omit recovery options from the BitLocker setup wizard	WAHR	
		Save BitLocker recovery information to AD DS for fixed data drives	FALSCH	
		Unnamed value	Allow 48-digit recovery password	

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Unnamed value	Allow 256-bit recovery key	
63.	Configure use of hardware-based encryption for fixed data drives		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Restrict crypto algorithms or cipher suites to the following:	2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42	
		Restrict encryption algorithms and cipher suites allowed for hardware-based encryption	FALSCH	
		Use BitLocker software-based encryption when hardware encryption is not available	WAHR	
64.	Configure use of passwords for fixed data drives		Disabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Configure password complexity for fixed data drives:		
		Minimum password length for fixed data drive:		
		Require password for fixed data drive		
65.	Configure use of smart cards on fixed data drives		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Require use of smart cards on fixed data drives	WAHR	
66.	Deny write access to fixed drives not protected by BitLocker		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
67.	Enforce drive encryption type on fixed data drives		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Select the encryption type:		
68.	Require additional authentication at startup		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Allow BitLocker without a compatible TPM	FALSCH	
		Configure TPM startup key and PIN:	Do not allow startup key and PIN with TPM	
		Configure TPM startup key:	Do not allow startup key with TPM	
		Configure TPM startup PIN:	Require startup PIN with TPM	
		Configure TPM startup:	Do not allow TPM	

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
69.	Use enhanced Boot Configuration Data validation profile		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
70.	Configure TPM platform validation profile for native UEFI firmware configurations		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		PCR 0: Core System Firmware executable code		
		PCR 1: Core System Firmware data		
		PCR 10: Initialized to 0 with no Extends (reserved for future use)		
		PCR 11: BitLocker Access Control		
		PCR 12: Data events and highly volatile events		
		PCR 13: Boot Module Details		
		PCR 14: Boot Authorities		
		PCR 15: Reserved for Future Use		
		PCR 16: Reserved for Future Use		
		PCR 17: Reserved for Future Use		
		PCR 18: Reserved for Future Use		
		PCR 19: Reserved for Future Use		
		PCR 2: Extended or pluggable executable code		
		PCR 20: Reserved for Future Use		
		PCR 21: Reserved for Future Use		
		PCR 22: Reserved for Future Use		
		PCR 23: Reserved for Future Use		
		PCR 3: Extended or pluggable firmware data		
		PCR 4: Boot Manager		
		PCR 5: GPT / Partition Table		
		PCR 6: Resume from S4 and S5 Power State Events		

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		PCR 7: Secured Boot State		
		PCR 8: Initialized to 0 with no Extends (reserved for future use)		
		PCR 9: Initialized to 0 with no Extends (reserved for future use)		
71.	Allow enhanced PINs for startup		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
72.	Enable use of BitLocker authentication requiring preboot keyboard input on slates		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
73.	Choose how BitLocker-protected operating system drives can be recovered		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Allow data recovery agent	WAHR	
		Configure storage of BitLocker recovery information to AD DS:	Store recovery passwords and key packages	
		Do not enable BitLocker until recovery information is stored to AD DS for operating system drives	WAHR	
		Omit recovery options from the BitLocker setup wizard	WAHR	
		Save BitLocker recovery information to AD DS for operating system drives	WAHR	
		Unnamed value	Require 48-digit recovery password	
		Unnamed value	Allow 256-bit recovery key	
74.	Configure minimum PIN length for startup		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Minimum characters:	7	
75.	Allow Secure Boot for integrity validation		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
76.	Enforce drive encryption type on operating system drives		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Select the encryption type:	Full encryption	

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
77.	Configure use of hardware-based encryption for operating system drives		Enabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Restrict crypto algorithms or cipher suites to the following:	2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42	
		Restrict encryption algorithms and cipher suites allowed for hardware-based encryption	FALSCH	
		Use BitLocker software-based encryption when hardware encryption is not available	WAHR	
78.	Disallow standard users from changing the PIN or password		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
79.	Allow network unlock at startup		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
80.	Configure use of passwords for operating system drives		Disabled	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Configure password complexity for operating system drives:		
		Minimum password length for operating system drive:		
		Require ASCII-only passwords for removable OS drives		
81.	Reset platform validation data after BitLocker recovery		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
82.	Configure TPM platform validation profile for BIOS-based firmware configurations		Not Configured	M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		PCR 0: Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions		
		PCR 1: Platform and Motherboard Configuration and Data		
		PCR 10: Boot Manager		
		PCR 11: BitLocker Access Control		
		PCR 12: Reserved for Future Use		

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		PCR 13: Reserved for Future Use		
		PCR 14: Reserved for Future Use		
		PCR 15: Reserved for Future Use		
		PCR 16: Reserved for Future Use		
		PCR 17: Reserved for Future Use		
		PCR 18: Reserved for Future Use		
		PCR 19: Reserved for Future Use		
		PCR 2: Option ROM Code		
		PCR 20: Reserved for Future Use		
		PCR 21: Reserved for Future Use		
		PCR 22: Reserved for Future Use		
		PCR 23: Reserved for Future Use		
		PCR 3: Option ROM Configuration and Data		
		PCR 4: Master Boot Record (MBR) Code		
		PCR 5: Master Boot Record (MBR) Partition Table		
		PCR 6: State Transition and Wake Events		
		PCR 7: Computer Manufacturer-Specific		
		PCR 8: NTFS Boot Sector		
		PCR 9: NTFS Boot Block		
83.	Enforce drive encryption type on removable data drives		Enabled	M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html
		Select the encryption type:	Full encryption	
84.	Configure use of passwords for removable data drives		Enabled	M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04
		Configure password complexity for removable data drives:	Allow password complexity	

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Minimum password length for removable data drive:	8	/m04339.html
		Require password for removable data drive	FALSCH	
85.	Configure use of smart cards on removable data drives		Enabled	M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html
		Require use of smart cards on removable data drives	FALSCH	
86.	Configure use of hardware-based encryption for removable data drives		Enabled	M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html
		Restrict crypto algorithms or cipher suites to the following:	2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42	
		Restrict encryption algorithms and cipher suites allowed for hardware-based encryption	FALSCH	
		Use BitLocker software-based encryption when hardware encryption is not available	WAHR	
87.	Deny write access to removable drives not protected by BitLocker		Enabled	M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Do not allow write access to devices configured in another organization	WAHR	
88.	Control use of BitLocker on removable drives		Enabled	M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Allow users to apply BitLocker protection on removable data drives	WAHR	
		Allow users to suspend and decrypt BitLocker protection on removable data drives	WAHR	
89.	Choose how BitLocker-protected removable drives can be recovered		Enabled	M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista und Windows 7
		Allow data recovery agent	WAHR	

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Configure storage of BitLocker recovery information to AD DS:	Backup recovery passwords and key packages	https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Do not enable BitLocker until recovery information is stored to AD DS for removable data drives	FALSCH	
		Omit recovery options from the BitLocker setup wizard	WAHR	
		Save BitLocker recovery information to AD DS for removable data drives	FALSCH	
		Unnamed value	Do not allow 48-digit recovery password	
		Unnamed value	Do not allow 256-bit recovery key	
90.	Allow access to BitLocker-protected removable data drives from earlier versions of Windows		Enabled	M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html M 4.337 Einsatz von BitLocker Drive Encryption https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04337.html
		Do not install BitLocker To Go Reader on FAT formatted removable drives	WAHR	
91.	Prevent installation of devices using drivers that match these device setup classes		Enabled	M 4.339 Verhindern unautorisierter Nutzung von Wechselmedien unter Windows Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html
		Also apply to matching devices that are already installed.	WAHR	
		Prevent installation of devices using drivers for these device setup classes:		
92.	Allow Standby States (S1-S3) When Sleeping (On Battery)		Disabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
93.	Allow Standby States (S1-S3) When Sleeping (Plugged In)		Disabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
94.	Turn off Automatic Root Certificates Update		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
95.	Turn off Search Companion content file updates		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
96.	MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
97.	System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
98.	Configure registry policy processing		Enabled	M 4.75 Schutz der Registry unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04075.html
		Do not apply during periodic background processing	FALSCH	
		Process even if the Group Policy objects have not changed	WAHR	
99.	Require trusted path for credential entry		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
100.	Turn off Data Execution Prevention for Explorer		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
101.	Boot-Start Driver Initialization Policy		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
		Choose the boot-start drivers that can be initialized:	Good, unknown and bad but critical	
102.	Always install with elevated privileges		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
103.	Allow deployment operations in special profiles		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
104.	MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
105.	Point and Print Restrictions		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
		Enter fully qualified server names separated by semicolons		
		Users can only point and print to machines in their forest		
		Users can only point and print to these servers:		
		When installing drivers for a new connection:		
		When updating drivers for an existing connection:		
106.	Configure Windows SmartScreen		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
		Pick one of the following settings	Require approval from an administrator before running downloaded unknown software	
107.	Specify settings for optional component installation and component repair		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
		Alternate source file path		
		Contact Windows Update directly to download repair content instead of Windows Server Update Services (WSUS)		
		Never attempt to download payload from Windows Update		
108.	Do not enumerate connected users on domain-joined computers		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
109.	Turn off the "Publish to Web" task for files and folders		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
110.	System settings: Optional subsystems		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
111.	Turn off the Windows Messenger Customer Experience Improvement Program		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
112.	Configure Solicited Remote Assistance		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
		Maximum ticket time (units):		
		Maximum ticket time (value):		
		Method for sending email invitations:		
		Permit remote control of this computer:		
113.	Turn Off the Display (Plugged In)		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
		Turn Off the Display (seconds):		
114.	DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
115.	MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
116.	DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
117.	System objects: Require case insensitivity for non-Windows subsystems		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
118.	Turn off app notifications on the lock screen		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
119.	Do not display the password reveal button		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
120.	Turn off Event Viewer "Events.asp" links		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
121.	Turn Off the Display (On Battery)		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
		Turn Off the Display (seconds):		
122.	Do not allow drive redirection		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
123.	Allow Remote Shell Access		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
124.	Turn off Internet download for Web publishing and online ordering wizards		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
125.	Recovery console: Allow floppy copy and access to all drives and all folders		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
126.	Turn off location		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
127.	Devices: Allowed to format and eject removable media		Administrators and Interactive Users	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
128.	Prevent the computer from joining a homegroup		Enabled	M 4.423 Verwendung der Heimnetzgruppen-Funktion unter Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04423.html
129.	Enumerate local users on domain-joined computers		Disabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
130.	Turn off Windows Location Provider		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
131.	Turn off printing over HTTP		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
132.	Create a pagefile		Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
133.	Create permanent shared objects		No One	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
134.	Increase scheduling priority		Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
135.	Create global objects		Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
136.	Profile single process		Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
137.	Take ownership of files or other objects		Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
138.	Create symbolic links		Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
139.	Act as part of the operating system		No One	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
140.	Modify firmware environment values		Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
141.	Back up files and directories		Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
142.	Profile system performance		NT SERVICE\WdiServiceHost,Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
143.	Restore files and directories		Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
144.	Perform volume maintenance tasks		Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
145.	Adjust memory quotas for a process		Administrators, Local Service, Network Service	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
146.	Bypass traverse checking		Users, NETWORK SERVICE, LOCAL SERVICE, Administrators	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
147.	Increase a process working set		Administrators, Local Service	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
148.	Lock pages in memory		No One	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
149.	Remove computer from docking station		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
150.	Replace a process level token		Local Service, Network Service	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
151.	Create a token object		No One	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
152.	Modify an object label		No one	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
153.	MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
154.	Disallow Digest authentication		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
155.	Allow the use of biometrics		Not Configured	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
156.	Allow Basic authentication		Disabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
157.	Allow Basic authentication		Disabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
158.	Turn on PIN sign-in		Disabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
159.	Devices: Restrict floppy access to locally logged-on user only		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
160.	Devices: Restrict CD-ROM access to locally logged-on user only		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
161.	System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
162.	Domain member: Digitally sign secure channel data (when possible)		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
163.	Access Credential Manager as a trusted caller		No One	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
164.	Impersonate a client after authentication		Administrators, SERVICE, Local Service, Network Service	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
165.	Always prompt for password upon connection		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
166.	Require a Password When a Computer Wakes (Plugged In)		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
167.	Do not allow passwords to be saved		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
168.	Require a Password When a Computer Wakes (On Battery)		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
169.	System cryptography: Force strong key protection for user keys stored on the computer		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
170.	Domain member: Require strong (Windows 2000 or later) session key		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
171.	Allow unencrypted traffic		Disabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
172.	Set client connection encryption level		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
		Encryption Level	High Level	

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
173.	Allow unencrypted traffic		Disabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
174.	Domain member: Digitally encrypt or sign secure channel data (always)		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
175.	Domain member: Digitally encrypt secure channel data (when possible)		Enabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
176.	Do not process the run once list		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
177.	Do not process the legacy run list		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
178.	Disallow WinRM from storing RunAs credentials		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
179.	Shutdown: Clear virtual memory pagefile		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
180.	Shut down the system		Administrators, Users	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
181.	System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing		Enabled	M 4.147 Sichere Nutzung von EFS unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04147.html
182.	Change the time zone		LOCAL SERVICE, Administrators, Users	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
183.	Change the system time		LOCAL SERVICE, Administrators	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
184.	Debug programs		Administrators	M 4.245 Basiseinstellungen für Windows Group Policy Objects https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04245.html
185.	Devices: Prevent users from installing printer drivers		Not Defined	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
186.	Load and unload device drivers		Administrators	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
187.	DEP		Enabled	M 4.245 Basiseinstellungen für Windows Group Policy Objects https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04245.html
		DEP Setting:	Application Opt Out	
188.	Turn off Data Execution Prevention for HTML Help Executible		Disabled	M 4.245 Basiseinstellungen für Windows Group Policy Objects https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04245.html
189.	Configure EFS recovery policy processing		Enabled	M 4.147 Sichere Nutzung von EFS unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04147.html
		Allow processing across a slow network connection	FALSCH	
		Do not apply during periodic background processing	WAHR	
		Process even if the Group Policy objects have not changed	FALSCH	
190.	Default Protections for Internet Explorer		Enabled	M 4.245 Basiseinstellungen für Windows Group Policy Objects https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04245.html
191.	Default Protections for Microsoft Works, Microsoft Office, Adobe Acrobat and Adobe Acrobat Reader products		Enabled	M 4.245 Basiseinstellungen für Windows Group Policy Objects https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04245.html
192.	Default Protections for other popular software		Enabled	M 4.245 Basiseinstellungen für Windows Group Policy Objects https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04245.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
193.	Windows Firewall: Domain: Display a notification		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
194.	Windows Firewall: Domain: Logging: Size limit (KB)		16384	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
195.	Windows Firewall: Domain: Logging: Name		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
196.	Windows Firewall: Domain: Apply local firewall rules		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
197.	Windows Firewall: Domain: Apply local connection security rules		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
198.	Windows Firewall: Domain: Allow unicast response		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
199.	Windows Firewall: Domain: Outbound connections		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
200.	Windows Firewall: Domain: Logging: Log dropped packets		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
201.	Windows Firewall: Domain: Logging: Log successful connections		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
202.	Windows Firewall: Domain: Inbound connections		Not Configured	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
		Inbound connections		
203.	Windows Firewall: Domain: Firewall state		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
204.	Windows Firewall: Public: Outbound connections		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
205.	Windows Firewall: Public: Apply local firewall rules		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
206.	Windows Firewall: Public: Apply local connection security rules		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
207.	Windows Firewall: Public: Logging: Log dropped packets		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
208.	Windows Firewall: Public: Display a notification		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
209.	Windows Firewall: Public: Allow unicast response		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
210.	Windows Firewall: Public: Logging: Name		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
211.	Windows Firewall: Public: Logging: Log successful connections		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
212.	Windows Firewall: Public: Logging: Size limit (KB)		16384	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/aM 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.htmlm04/m04146.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
213.	Windows Firewall: Public: Firewall state		On (recommended)	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
214.	Windows Firewall: Public: Inbound connections		Not Configured	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
		Inbound connections		
215.	Windows Firewall: Private: Firewall state		On (recommended)	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
216.	Windows Firewall: Private: Outbound connections		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
217.	Windows Firewall: Private: Apply local firewall rules		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
218.	Windows Firewall: Private: Logging: Size limit (KB)		16384	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
219.	Windows Firewall: Private: Apply local connection security rules		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_contenaM 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.htmlt/m/m04/m04146.html
220.	Windows Firewall: Private: Display a notification		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
221.	Windows Firewall: Private: Inbound connections		Not Configured	M 4.146 Sicherer Betrieb von Windows Client-

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Inbound connections		BetriebssystemenaM 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
222.	Windows Firewall: Private: Logging: Name		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
223.	Windows Firewall: Private: Allow unicast response		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
224.	Windows Firewall: Private: Logging: Log successful connections		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
225.	Windows Firewall: Private: Logging: Log dropped packets		Not Defined	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
226.	Windows Firewall: Block IP protocol number 41		41	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
227.	Windows Firewall: Block UDP port 3544		3544	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html M 2.76 (A) Auswahl und Einrichtung geeigneter Filterregeln https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02076.html
228.	Turn off heap termination on corruption		Disabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
229.	Manage auditing and security log		Administrators	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
230.	Generate security audits		Local Service, Network Service	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
231.	Audit: Shut down system immediately if unable to log security audits		Disabled	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
232.	Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings		Enabled	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
233.	Audit: Audit the use of Backup and Restore privilege		Not Defined	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
234.	Audit Policy: Detailed Tracking: RPC Events		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
235.	Audit Policy: Detailed Tracking: Process Termination		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
236.	Audit Policy: Detailed Tracking: DPAPI Activity		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
237.	Audit: Audit the access of global system objects		Not Defined	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
238.	Audit Policy: Detailed Tracking: Process Creation		Success	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
239.	Audit Policy: Account Logon: Credential Validation		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
240.	Audit Policy: Account Logon: Kerberos Authentication Service		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
241.	Audit Policy: Account Logon: Kerberos Service Ticket Operations		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
242.	Audit Policy: Account Logon: Other Account Logon Events		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
243.	Audit Policy: Logon-Logoff: Account Lockout		Success	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
244.	Audit Policy: Logon-Logoff: IPsec Extended Mode		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
245.	Audit Policy: Logon-Logoff: IPsec Main Mode		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
246.	Audit Policy: Logon-Logoff: IPsec Quick Mode		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
247.	Audit Policy: Logon-Logoff: Logoff		Success	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
248.	Audit Policy: Logon-Logoff: Logon		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
249.	Audit Policy: Logon-Logoff: Network Policy Server		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
250.	Audit Policy: Logon-Logoff: Other Logon/Logoff Events		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
251.	Audit Policy: Logon-Logoff: Special Logon		Success	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
252.	Audit Policy: Account Management: Application Group Management		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
253.	Audit Policy: Account Management: Computer Account Management		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
254.	Audit Policy: Account Management: Distribution Group Management		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
255.	Audit Policy: Account Management: Other Account Management Events		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
256.	Audit Policy: Account Management: Security Group Management		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
257.	Audit Policy: Account Management: User Account Management		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
258.	Audit Policy: Object Access: Application Generated		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
259.	Audit Policy: Object Access: Central Access Policy Staging		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
260.	Audit Policy: Object Access: Certification Services		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
261.	Audit Policy: Object Access: Detailed File Share		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
262.	Audit Policy: Object Access: File Share		Success	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
263.	Audit Policy: Object Access: File System		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
264.	Audit Policy: Object Access: Filtering Platform Connection		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
265.	Audit Policy: Object Access: Filtering Platform Packet Drop		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
266.	Audit Policy: Object Access: Handle Manipulation		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
267.	Audit Policy: Object Access: Kernel Object		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
268.	Audit Policy: Object Access: Other Object Access Events		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
269.	Audit Policy: Object Access: Registry		Success and Failure	M 4.75 Schutz der Registry unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04075.html M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
270.	Audit Policy: Object Access: Removable Storage		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
271.	Audit Policy: Object Access: SAM		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
272.	Audit Policy: Policy Change: Audit Policy Change		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
273.	Audit Policy: Policy Change: Authentication Policy Change		Success	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
274.	Audit Policy: Policy Change: Authorization Policy Change		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
275.	Audit Policy: Policy Change: Filtering Platform Policy Change		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
276.	Audit Policy: Policy Change: MPSSVC Rule-Level Policy Change		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
277.	Audit Policy: Policy Change: Other Policy Change Events		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
278.	Audit Policy: Privilege Use: Non Sensitive Privilege Use		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
279.	Audit Policy: Privilege Use: Other Privilege Use Events		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
280.	Audit Policy: Privilege Use: Sensitive Privilege Use		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
281.	Audit Policy: DS Access: Detailed Directory Service Replication		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
282.	Audit Policy: DS Access: Directory Service Access		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
283.	Audit Policy: DS Access: Directory Service Changes		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
284.	Audit Policy: DS Access: Directory Service Replication		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
285.	Audit Policy: System: IPsec Driver		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
286.	Audit Policy: System: Other System Events		No Auditing	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
287.	Audit Policy: System: Security State Change		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
288.	Audit Policy: System: Security System Extension		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
289.	Audit Policy: System: System Integrity		Success and Failure	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
290.	Control Event Log behavior when the log file reaches its maximum size		Disabled	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
291.	Control Event Log behavior when the log file reaches its maximum size		Disabled	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
292.	Control Event Log behavior when the log file reaches its maximum size		Disabled	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
293.	Control Event Log behavior when the log file reaches its maximum size		Disabled	M 4.344 Überwachung von Windows Vista-, Windows 7 und Windows Server 2008-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
294.	Network security: Do not store LAN Manager hash value on next password change		Enabled	M 2.11 Regelung des Passwortgebrauchs https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html
295.	Network security: Minimum session security for NTLM SSP based (including secure RPC) servers		Require message integrity,Require NTLMv2 session security,Require 128-bit encryption	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
296.	Network security: Allow Local System to use computer identity for NTLM		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
297.	Network Security: Restrict NTLM: Add server exceptions in this domain		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
298.	Network Security: Restrict NTLM: NTLM authentication in this domain		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
299.	Network security: Allow LocalSystem NULL session fallback		Disabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
300.	Network security: Minimum session security for NTLM SSP based (including secure RPC) clients		Require message integrity,Require NTLMv2 session security,Require 128-bit encryption	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
301.	Network Security: Restrict NTLM: Audit Incoming NTLM Traffic		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
302.	Network Security: Restrict NTLM: Add remote server exceptions for NTLM authentication		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
303.	Network security: LAN Manager authentication level		Send NTLMv2 response only. Refuse LM & NTLM	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
304.	Network Security: Allow PKU2U authentication requests to this computer to use online identities		Disabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
305.	Network Security: Restrict NTLM: Incoming NTLM traffic		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
306.	Network Security: Restrict NTLM: Audit NTLM authentication in this domain		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
307.	Network Security: Configure encryption types allowed for Kerberos		RC4\AES128\AES256\Future types	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html M 2.46 Geeignetes Schlüsselmanagement https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02046.html
308.	Network security: Force logoff when logon hours expire		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
309.	Network security: LDAP client signing requirements		Negotiate signing	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
310.	Network access: Let Everyone permissions apply to anonymous users		Disabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
311.	Network access: Allow anonymous SID/Name translation		Disabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
312.	Network access: Do not allow anonymous enumeration of SAM accounts and shares		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
313.	Network access: Remotely accessible registry paths		System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html M 4.75 Schutz der Registry unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04075.html
314.	Network access: Remotely accessible registry paths and sub-paths		System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html M 4.75 Schutz der Registry unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04075.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
315.	Network access: Shares that can be accessed anonymously		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
316.	Network access: Do not allow anonymous enumeration of SAM accounts		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
317.	Network access: Sharing and security model for local accounts		Classic - local users authenticate as themselves	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
318.	Network access: Restrict anonymous access to Named Pipes and Shares		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
319.	Network access: Named Pipes that can be accessed anonymously		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
320.	Network access: Do not allow storage of passwords and credentials for network authentication		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
321.	Enable RPC Endpoint Mapper Client Authentication		Disabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
322.	Restrict Unauthenticated RPC clients	 RPC Runtime Unauthenticated Client Restriction to Apply:	Enabled Authenticated	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
323.	MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)		3	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
324.	MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes		Disabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
325.	MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
326.	MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)		Highest protection, source routing is completely disabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
327.	MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)		Highest protection, source routing is completely disabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
328.	MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds		300000 or 5 minutes (recommended)	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
329.	Minimize the number of simultaneous connections to the Internet or a Windows Domain		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
330.	MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
331.	Set IP Stateless Autoconfiguration Limits State		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
332.	MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)		3	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
333.	Access this computer from the network		Users, Administrators	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
334.	Deny access to this computer from the network		Guests	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
335.	Microsoft network client: Digitally sign communications (always)		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
336.	Microsoft network client: Digitally sign communications (if server agrees)		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
337.	Microsoft network client: Send unencrypted password to third-party SMB servers		Disabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
338.	Microsoft network server: Amount of idle time required before suspending session		15	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
339.	Microsoft network server: Disconnect clients when logon hours expire		Enabled	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
340.	Microsoft network server: Server SPN target name validation level		Accept if provided by client	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
341.	MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic.		Not Defined	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
342.	Prohibit connection to non-domain networks when connected to domain authenticated network		Not Configured	M 5.123 Absicherung der Netzkommunikation unter Windows https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
343.	Intranet proxy servers for apps	 Type a proxy server IP address for the intranet	Disabled	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
344.	Proxy definitions are authoritative		Not Configured	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
345.	Internet proxy servers for apps		Not Configured	M 4.146 Sicherer Betrieb von Windows Client-

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Domain Proxies		Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
346.	Specify KDC proxy servers for Kerberos clients		Not Configured	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
		Define KDC proxy servers settings:		
347.	Disable revocation checking for the SSL certificate of KDC proxy servers		Not Configured	M 4.146 Sicherer Betrieb von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04146.html
348.	Allow users to connect remotely by using Remote Desktop Services		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
349.	Configure Offer Remote Assistance		Disabled	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
		Permit remote control of this computer:		
		Helpers:		
350.	Force shutdown from a remote system		Administrators	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
351.	Disable remote Desktop Sharing		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
352.	Restrict Remote Desktop Services users to a single Remote Desktop Services session		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
353.	Set rules for remote control of Remote Desktop Services user sessions		Enabled	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
		Options:	No remote control allowed	
354.	Use the specified Remote Desktop license servers		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
		License servers to use:		
355.	Set the Remote Desktop licensing mode		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP,

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Specify the licensing mode for the RD Session Host server.		Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
356.	Use Remote Desktop Easy Print printer driver first		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
357.	Set path for Remote Desktop Services Roaming User Profile		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
		Profile path		
358.	Set Remote Desktop Services User Home Directory		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
		Drive Letter		
		Home Dir Root Path:		
		Location:		
359.	Enforce Removal of Remote Desktop Wallpaper		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
360.	Set time limit for active Remote Desktop Services sessions		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
		Active session limit :		
361.	Set time limit for active but idle Remote Desktop Services sessions		Not Configured	M 2.327 Sicherheit beim Fernzugriff unter Windows XP, Vista und Windows 7 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02327.html
		Idle session limit:		
362.	SEHOP		Enabled	M 4.245 Basiseinstellungen für Windows Group Policy Objects https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04245.html
		SEHOP Setting:	Application Opt Out	
363.	Notify user of successful smart card driver installation		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
364.	Turn on root certificate propagation from smart card		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
365.	Turn on Smart Card Plug and Play service		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
366.	Turn on certificate propagation from smart card		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
367.	Display string when smart card is blocked		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
		Display string when smart card is blocked		
368.	Force the reading of all certificates from the smart card		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
369.	Interactive logon: Smart card removal behavior		Lock Workstation	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
370.	Interactive logon: Require smart card		Not Defined	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
371.	SSL Cipher Suite Order		Not Configured	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html M 2.46 Geeignetes Schlüsselmanagement https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02046.html
		SSL Cipher Suites		
372.	Do not sync personalize		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
		Allow users to turn "personalize" syncing on.		
373.	Do not sync other Windows settings		Not Configured	M 2.32 Einrichtung einer eingeschränkten

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
		Allow users to turn "other Windows settings" syncing on.		Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
374.	Do not sync		Enabled	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
		Allow users to turn syncing on.	FALSCH	
375.	Do not sync desktop personalization		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
		Allow users to turn "desktop personalization" syncing on.		
376.	Do not sync browser settings		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
		Allow users to turn "browser" syncing on.		
377.	Do not sync passwords		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
		Allow users to turn "passwords" syncing on.		
378.	Do not sync app settings		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
		Allow users to turn "app settings" syncing on.		
379.	Do not sync on metered connections		Not Configured	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
380.	Enable Persistent Time Stamp		Enabled	M 4.244 Sichere Systemkonfiguration von Windows Client-Betriebssystemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html
		Seconds:	60	
381.	User Account Control: Behavior of the elevation prompt for standard users		Prompt for credentials	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
382.	User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode		Elevate without prompting	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
383.	User Account Control: Only elevate UIAccess applications that are installed in secure locations		Enabled	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
384.	User Account Control: Virtualize file and registry write failures to per-user locations		Enabled	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html M 4.75 Schutz der Registry unter Windows-Systemen https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04075.html
385.	User Account Control: Only elevate executables that are signed and validated		Disabled	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
386.	User Account Control: Switch to the secure desktop when prompting for elevation		Disabled	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
387.	User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop		Disabled	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
388.	User Account Control: Run all administrators in Admin Approval Mode		Disabled	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
389.	User Account Control: Admin Approval Mode for the Built-in Administrator account		Disabled	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
390.	User Account Control: Detect application installations and prompt for elevation		Enabled	M 4.340 Einsatz der Windows-Benutzerkontensteuerung UAC ab Windows Vista https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
391.	Turn off access to the Store		Enabled	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html

ID	Einstellungsname	Optionen	Empfohlene Einstellung	BSI referenzierte Maßnahme
392.	Allow all trusted apps to install		Enabled	M 2.32 Einrichtung einer eingeschränkten Benutzerumgebung https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02032.html
393.	Configure Automatic Updates		Enabled	M 4.249 Windows Client-Systeme aktuell halten https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04249.html
		Configure automatic updating:	3 - Auto download and notify for install	
		Scheduled install day:	0 - Every day	
		Scheduled install time:	03:00	
394.	Turn off Automatic Download of updates		Not Configured	M 4.249 Windows Client-Systeme aktuell halten https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04249.html
395.	Reschedule Automatic Updates scheduled installations		Enabled	M 4.249 Windows Client-Systeme aktuell halten https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04249.html
		startup (minutes):	1	
396.	Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box		Disabled	M 4.249 Windows Client-Systeme aktuell halten https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04249.html
397.	Specify intranet Microsoft update service location		Enabled	M 4.249 Windows Client-Systeme aktuell halten https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04249.html
		Set the intranet statistics server:	http://wsus.your.com	
		Set the intranet update service for detecting updates:	http://wsus.your.com	
398.	No auto-restart with logged on users for scheduled automatic updates installations		Disabled	M 4.249 Windows Client-Systeme aktuell halten https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04249.html
399.	Specify the search server for device driver updates		Enabled	M 4.249 Windows Client-Systeme aktuell halten https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04249.html
		Select update server:	Search Managed Server	
400.	Turn off Windows Update device driver searching		Enabled	M 4.249 Windows Client-Systeme aktuell halten https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04249.html
401.	Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box		Disabled	M 4.249 Windows Client-Systeme aktuell halten https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04249.html