SiM-08202
Client unter Windows 10

Sicherheitsmodul Richtlinie

BUNDESPOLIZEI

Dokumenteninformation

Name	SiM-08202 Client unter Windows 10
Dokumentverantwortlicher	Bundespolizeipräsidium, Referat 51
Erstellt am	13.09.2017
Zuletzt geändert	13.09.2017
Bearbeitungszustand	Aktiv
Dokumentablage	
Version	1.* (Version für BSI)

Änderungsnachweis

Dokument-Änderung					
Nr.	Datum	Version	Beschreibung der Änderung	Autor	Zustand
1	13.09.2017	1.* (Version für BSI)		Projektgruppe aGS	Final

Impressum:

Bundespolizeipräsidium
Referat 51, Informationssicherheit
Heinrich-Mann-Allee 103
14473 Potsdam

bpolp.ref51.is@polizei.bund.de

Inhaltsverzeichnis

1 Steckbrief

Name	SiM-08202 - Client unter Windows 10
Berücksichtigte BSI-Bausteine	SYS.02.02.03 Client unter Windows 10 SYS.02.01 Allgemeiner Client
Benutzerdef. Baustein / Maßnahmen	Nein, insgesamt 0 Maßnahme(n), davon 0 technische Aspekte 0 nichttechnische Aspekte
Technische Checks	391
Webfragen	379

Tabelle 3: ***Steckbrief***

2 Allgemeines

2.1 Geltungsbereich

Dieses Sicherheitsmodul gilt für den Einsatz von Windows 10 auf den Standard-Clients der Bundespolizei.

2.2 Mitgeltende Dokumente BPOL

Bei der Umsetzung dieser Richtlinie sind die Rahmenkonzeption Informationssicherheit, das Kryptokonzept, die gesetzlichen Vorgaben des Datenschutzes, die Dienstanweisung für Systemadministratoren der Bundespolizei, die Dienstanweisung für die Nutzung der Informations- und Kommunikationstechnik sowie das Datensicherungsrahmenkonzept für die Bundespolizei in der jeweils aktuellen Fassung zu beachten.

Es werden keine weiteren Dokumente referenziert.

2.3 Aktualisierung / Archivierung

Aktualisierungen bzw. die Archivierung dieser Richtlinie richten sich nach den entsprechenden Verfahrensanweisungen "SiM aktualisieren" bzw. "SiM archivieren" in der jeweils gültigen Fassung.

3 Standardbeschreibung

3.1 Rahmenbedingungen

Dieses Sicherheitsmodul gilt für den Einsatz von Windows 10 auf stationären und mobilen Clients sowie SINA-Gastsystemen innerhalb des BPOL-Net.

3.2 Webfragebögen

Nachfolgend werden alle im SiM enthaltenen Webfragen, einschließlich der zugeordneten Antwortmöglichkeiten und der für die automatisierte Auswertung hinterlegten Bewertungen dargestellt.

Frage	Fragestellung	Antwortoption
SYS.02.01.A001 (B) Benutzerauthentisierung		
08202-1000	Gibt es eine Sicherheitsrichtlinie für die Anforderungen und Vergabe von Passwörtern?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1001	Ist jedes Windows-System und jedes Benutzerkonto durch ein Passwort geschützt?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1002	Ist sichergestellt, dass Windows Benutzerkonten nur von einer dazu berechtigten Person verwendet werden können?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1003	Werden starke Passwörter für die Windows Benutzerkonten erzwungen?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1004	Wird das Kennwort für das Computer-Konto regelmäßig geändert?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
08202-1005	Wird die Option Benutzer muss Kennwort bei der nächsten Anmeldung ändern bei allen neuen Konten aktiviert?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1006	Wird nach der Rückkehr aus dem Standby-Modus, dem Ruhezustand oder dem hybriden Energiesparmodus ein Kennwort vom Benutzer verlangt?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A002 (B) Rollentrennung		
08202-1007	Gibt es ein Benutzer- und Administrationskonzept für Windows-Client-Betriebssysteme?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.

Frage	Fragestellung	Antwortoption
08202-1008	Ist festgelegt, dass nur Administratoren Administrationsrechte erhalten dürfen?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1009	Dürfen nur Administratoren Anwendungen installieren bzw. entfernen?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1010	Dürfen nur Administratoren die Systemkonfiguration ändern?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1011	Dürfen nur Administratoren Systemdateien modifizieren bzw. löschen?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1012	Ist der Zugriff auf alle Administrationswerkzeuge für Benutzer von Windows Client-Betriebssystemen unterbunden worden?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1013	Haben Nutzer nur lesenden Zugriff auf Systemdateien?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
SYS.02.01.A003 (B) Aktivieren von Autoupdate-Mechanismen		
08202-1014	Existiert einer Regelung für automatische Suche und Installation von Updates?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1015	Erfolgt keine regelmäßige Wartung oder ist kein zentrales Softwarevereteilungssystems für Updates im Einsatz müssen die automatischen Update-Mechanismen aktiviert werden.	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1016	Sollte ein Zeitinterval für den Auto-Update-Machanismus vorgegeben werden können, so muss dieses auf "tägliche" Suche eingestellt sein.	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1017	Werden Updates vor ihrer Installation getestet und freigegeben?	• Ja. • Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A004 (B) Regelmäßige Datensicherung		

Frage	Fragestellung	Antwortoption
08202-1018	Gibt es Richtlinien wann und wie oft eine Datensicherung durchgeführt werden soll?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1019	Entspricht das festgelegte Verfahren für die Datensicherungen den Verfügbarkeitsanforderungen?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
08202-1020	Bei vertraulichen Daten, gegebenenfalls auch bei Auslagerung der Backups: Werden die gesicherten Daten verschlüsselt gespeichert?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1021	Ist festgelegt, wie die Datensicherungen organisatorisch und technisch ablaufen?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1022	Sind die Benutzer über die Festlegungen zur Durchführung von Datensicherungen informiert?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1023	Werden bei der Wiederherstellung der Daten die Zugriffsrechte wieder hergestellt?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1024	Werden zumindest alle Daten, die nicht aus anderen Informationen abgeleitet werden können, regelmäßig gesichert?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1025	Wird bei der Durchführung der Sicherung eine Protokolldatei angelegt?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1026	Wird der Datensicherungsvorgang dokumentiert?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1027	Wird diese Protokolldatei nach Abschluss der Sicherung auf Fehler und Auffälligkeiten überprüft?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1028	Wird regelmäßig getestet, ob die gesicherten Daten problemlos zurückgespielt werden können?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1029	Wurden die Anforderungen für die Beschaffung einer Sicherungssoftware definiert?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A005 (B) Bildschirmsperre [Benutzer]		
08202-1030	Existiert eine Richtlinie, die neben anderen Sicherheitsmaßnahmen auch die Sperrung des Bildschirms bei Abwesenheit vom Arbeitsplatz regelt?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1031	Ist die manuelle Bildschirmsperre allen Mitarbeitern bekannt und wird diese auch eingesetzt?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1032	Ist ein Zeitraum für die automatische Bildschirmsperre definiert, der sowohl Nutzer- als auch Sicherheitsbelange berücksichtigt?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1033	Bei fehlender Unterstützung durch das Betriebssystem: Wird eine fehlende Bildschirmsperre durch andere Maßnahmen realisiert?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
SYS.02.01.A006 (B) Einsatz von Viren-Schutzprogrammen		
08202-1034	Bei Auffinden eines Schadprogrammes: Wird untersucht, ob das gefundene Schadprogramm vor seiner Entdeckung bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1035	Ist auch für verschlüsselte Daten ein ausreichender Schutz vor Schadprogrammen gewährleistet?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1036	Ist für die genutzten Internet-Dienste ein ausreichender Schutz vor Schadprogrammen gewährleistet?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1037	Ist sichergestellt, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Viren-Schutzprogramme vornehmen können?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1038	Sind die Nutzer mit dem Scanprogramm vertraut, insbesondere mit der Möglichkeit des "On-Demand-Scans"?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1039	Sind Viren-Schutzprogramme auf allen IT-Systemen installiert, auf denen dies laut Sicherheitskonzept vorgesehen ist?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1040	Wird bei Datenaustausch und Datenübertragung eine Suche nach Schadprogrammen durchgeführt?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1041	Wird das zentrale E-Mail-Gateway durch ein Viren-Schutzprogramm gesichert?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1042	Wird eine regelmäßige Untersuchung des gesamten Datenbestandes auf Schadprogramme durchgeführt?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1043	Wird sichergestellt, das sowohl Scanprogramm als auch Signaturen stets auf dem aktuellsten Stand sind?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
SYS.02.01.A007 (B) Protokollierung		
08202-1044	Wurde ein bedarfsgerechtes Überwachungskonzept für IT-Systeme entworfen und umgesetzt?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1045	Ist festgelegt, dass die Synchronisierung der Systemzeit mittels einer zuverlässigen Zeitquelle sichergestellt wird?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1046	Werden die in der Überwachungsrichtlinie festgelegten Sicherheitseinstellungen umgesetzt?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1047	Ist die Überwachung in den Gruppenrichtlinien bzw. den lokalen Einstellungen aktiviert worden?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1048	Existiert eine Regelung zur Protokollierung von Clientsystemen?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1049	Wird eine Protokollierung auf Clientseite sichergestellt?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
08202-1050	Wurden Überwachungseinstellungen für wichtige Systemdateien und Registry-Einträge konfiguriert?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1051	Werden die Protokolleinträge, die AppLocker bei versuchten Regelverstößen generiert, bei der Protokollauswertung der Systeme berücksichtigt?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1052	Werden wichtige Systemereignisse protokolliert?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1053	Werden die Protokolldateien bei Erreichen der Maximalgröße gesichert?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1054	Existiert eine Regelung das Protokolldateien regelmäßig überprüft werden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
SYS.02.01.A008 (A) Absicherung des Boot-Vorgangs		
08202-1055	Existieren Regelungen, um den Bootvorgang von Clients gegen Manipulationen zu sichern?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1056	Ist sichergestellt, dass nur Nutzer mit administrativen Rechten die Bootkonfigurationseinstellungen von Clients ändern können?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1057	Ist sichergestellt, dass nur Administratoren die Clients von Laufwerken oder externen Speichermedien booten können?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1058	Wurden die Benutzer über die Gefährdung informiert und sensibilisiert damit die Sicherheitsmaßnahmen akzeptiert und beachtet werden?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1059	Ist die Datei boot.ini im Wurzelverzeichnis der ersten Platte vor Veränderungen geschützt?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1060	Sind alle vorhandenen Festplattenpartitionen mit dem Dateisystem NTFS formatiert?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1061	Wurde darauf geachtet, dass die Benutzer Startskripte beim Start von Windows nicht verändern oder abbrechen können?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
SYS.02.01.A009 (A) Festlegung einer Sicherheitsrichtlinie für Clients		
08202-1062	Ist eine Client-Sicherheitsrichtlinie vorhanden, die das zu erreichende Sicherheitsniveau beschreibt?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1063	Orientiert sich die Sicherheitsrichtlinie zu Windows-Clients an den geltenden Sicherheitsrichtlinien des Unternehmens bzw. der Behörde?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1064	Berücksichtigt die Client-Sicherheitsrichtlinie mindestens die Aspekte Regelungen für die Arbeit der Benutzer der Clients, Regelungen für die Arbeit der Administratoren und Revisoren, Vorgaben für die Installation und Grundkonfiguration, Vorgaben für den sicheren Betrieb, Netzkommunikation und –dienste und Protokollierung?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1065	Wird die Client-Sicherheitsrichtlinie regelmäßig den aktuellen Erfordernissen angepasst?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A010 (A) Planung des Einsatzes von Clients		
08202-1066	Existieren ein Grob- bzw. die notwendigen Teilkonzepte zur Einsatzplanung von Client-Server-Netzen?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1067	Existieren Vorgaben für die Dokumentation von Änderungen und werden diese umgesetzt?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1068	Existieren Vorgaben zu den eingesetzten Netzdiensten und der Netzanbindung, die die Anforderungen der Einsatzprofile berücksichtigen?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1069	Existieren Vorgaben zur Authentisierung und Benutzerverwaltung?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1070	Existiert eine Liste mit allen nicht benötigten Anwendungen sowie und Komponenten und sind diese deaktiviert?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1071	Sind die Aufgaben der Clients und darauf aufbauend die benötigten Dienste definiert?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1072	Werden die Einsatzkonzepte regelmäßig den aktuellen Erfordernissen angepasst?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1073	Werden in den Konzepten Anforderungen bzgl. Monitoring und Protokollierung definiert, die sich mit den Anforderungen und Schutzzielen decken?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1074	Wird bei der Betriebssystemauswahl die Nutzung spezieller Hardware berücksichtigt?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1075	Wurde für jeden Client-Typ unterschiedliche Anforderungsprofile erstellt?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A011 (A) Beschaffung von Clients		
08202-1076	Existiert eine Anforderungsliste, anhand derer die am Markt erhältlichen Produkte vor einer Beschaffung bewertet werden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1077	Sind schlüssige und nachvollziehbare Bewertungskriterien für die einzelnen Anforderungen definiert?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.

Frage	Fragestellung	Antwortoption
08202-1078	Wird die Anfroderungsliste regelmäßig aktualisiert?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1079	Wurde mit dieser Anforderungsliste eine Bewertung der am Markt erhältlichen Produkte durchgeführt?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
SYS.02.01.A012 (S) Kompatibilitätsprüfung von Software		
08202-1080	Gibt es eine Strategie zum Umstieg auf sichere Anwendungen als Alternative zu Altanwendungen unter Windows-Client-Versionen ab Windows Vista?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1081	Wird vor einer beabsichtigten Beschaffung von Software deren Kompatibilität zum eingesetzten Betriebssystem geprüft?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1082	Wird vor einer beabsichtigter Hardwareänderung oder bei einer Betriebssystemmigration die Treibersoftware für alle betreffenden Komponenten auf Kompatibilität und Verfügbarkeit zur eingesetzten Windows-Version geprüft?	• Ja. • Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1083	Wrde die Kompatibilität in einer Testumgebung geprüft, wenn vom Hersteller der Software oder aus anderen Fachkreisen keine sichere Information zur Kompatibilität vorhanden ist?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
SYS.02.01.A013 (A) Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung		
08202-1084	Ist der Zugriff auf Ausführungsumgebungen reglementiert?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1085	Ist sichergestellt, dass der Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung nur für Benutzer mit administrativen Berechtigungen möglich ist?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
SYS.02.01.A014 (A) Updates und Patches für Firmware, Betriebssystem und Anwendungen		
08202-1086	Ist die Strategie für die Aktualisierung von Windows Client-Systemen festgelegt?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1087	Berücksichtigt die definierte Update-Strategie für Windows Client-Systeme auch anwendungsspezifische Updates, zum Beispiel von Drittherstellern?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1088	Ist die Vertrauenswürdigkeit der Update-Quellen für Windows Client-Systeme gewährleistet?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1089	Ist gewährleistet, dass nur getestete und freigegebene Updates auf Windows Client-Systemen installiert werden?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1090	Gibt es eine Strategie zur Wiederherstellung der Funktionsfähigkeit der Systeme bei Problemen oder Fehlern?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1091	Gibt es einen regelmäßigen Abgleich mit dem aktuellen Patch-Stand der Systeme und den von Microsoft verfügbaren Updates?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1092	Informieren sich die Administratoren regelmäßig über Schwachstellen und verfügbare Sicherheits-Updates?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1093	Ist sichergestellt, dass identifizierten Schwachstellen so schnell wie möglich behoben werden?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1094	Sofern noch keine entsprechenden Patches zur Verfügung stehen: Ist gewährleistet, dass abhängig von der Schwere der Schwachstellen andere geeignete Maßnahmen zum Schutz des IT-Systems getroffen werden?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
SYS.02.01.A015 (A) Sichere Installation und Konfiguration von Clients		
08202-1095	Wurde eine Bedarfsanalyse unter Windows bezüglich der erforderlichen Systemdienste durchgeführt?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1096	Ist sichergestellt, dass die erforderlichen Windows-Sicherheitseinstellungen nach der Installation auch tatsächlich konfiguriert werden (installierte Komponenten, angewandte Richtlinien, Berechtigungen im Dateisystem/ Registry, zugewiesene Benutzerrechte, erlaubte Systemdienste usw.)?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1097	Ist sichergestellt, dass Windows-Systeme erst nach der vollständigen Installation, Konfiguration und dem Einspielen aller Patches und Updates produktiv ins Netz gehen?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1098	Sind Kennwörter in Installationsskripten und Konfigurationsdateien geschützt und wurden diese nach der Installation vom System gelöscht?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1099	Werden alle Installations- und Konfigurationsschritte nachvollziehbar dokumentiert?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1100	Wird bei einer unbeaufsichtigten Installation von Windows ein Administrator-Kennwort vergeben?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1101	Wird die Installation und Konfiguration nur von autorisierten Personen (Administratoren oder vertraglich gebundene Dienstleister) nach einem definierten Prozess durchgeführt?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1102	Wird eine sichere Grundkonfiguration aller eingesetzten IT-Systeme entsprechend den Vorgaben der Sicherheitsrichtlinie vorgenommen?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1103	Wird gewährleistet, dass bei der Installation von Windows-Systemen nur die benötigten Systemkomponenten installiert werden?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1104	Sind die Vor- und Nachteile des Einsatzes eines TPM abgewogen und eine Entscheidung zur Verwendung im Betriebssystem getroffen worden?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1105	Werden alle sicherheitsrelevanten Einstellungen bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft ?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1106	Werden wegen der Migration erweiterte Zugriffsberechtigungen und gelockerte Sicherheitseinstellungen der Domäne nach Abschluss der Migration wieder auf das höchstmögliche Sicherheitsniveau gebracht?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1107	Werden zusätzliche Programme zur unwiederbringlichen Löschung, insbesondere bei vertraulichen Daten, eingesetzt?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
SYS.02.01.A016 (A) Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen		

Frage	Fragestellung	Antwortoption
08202-1108	Sind alle nicht benötigten Dienste deaktiviert?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1109	Sind alle nicht verwendeten Netzwerkkomponenten von existierenden Schnittstellen entfernt worden?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1110	Wurden nicht benötigte Benutzerkonten deaktiviert oder entfernt?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A017 (A) Einsatzfreigabe		
08202-1111	Ist geregelt, dass bevor ein Client im produktiven Betrieb eingesetzt und an ein produktives Netz angeschlossen wird, eine Einsatzfreigabe erforderlich ist?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
08202-1112	Erfolgt die Einsatzfreigabe durch eine in der Institution autorisierte Stelle?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.

Frage	Fragestellung	Antwortoption
08202-1113	Ist die Kompatibilitätsprüfung in das Test- und Freigabeverfahren der Software integriert?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1114	Werden Änderungen an der Registry vorher auf einem Testsystem ausführlich getestet?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1115	Werden die AppLocker-Regeln vor dem Einsatz auf einem produktiven System zunächst auf einem Testsystem oder durch den Betrieb im Überwachungsmodus erprobt?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1116	Werden vor der Einführung neuer Applikationen auf Windows Client-Betriebssystemen Funktions- und Sicherheitstests durchgeführt?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
08202-1117	Wird vor der Einsatzfreigabe die Installations- und Konfigurationsdokumentation sowie die Funktionsfähigkeit der IT-Systeme in einem Test geprüft?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1118	Wird die Einsatzfreigabe dokumentiert?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
SYS.02.01.A018 (A) Nutzung von TLS [Benutzer]		
08202-1119	Ist sichergestellt, dass die eingesetzten Clients kryptographische Algorithmen und Schlüssellängen verwenden, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1120	Ist sichergestellt, dass die Validierung von Zertifikaten den Sicherheitsrichtlinien der Institution entspricht?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1121	Sind Session Renegotiation und TLS-Kompression deaktiviert?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1122	Unterstützen die eingesetzten Client-Produkte TLS in der Version 1.2?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1123	Wird auch bei der Nutzung von SSL/TLS ein ausreichender Schutz vor Schadprogrammen und unerlaubten aktiven Inhalten gewährleistet?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1124	Wird darauf geachtet, dass neue Zertifikate erst nach Überprüfung des "Fingerprints" aktiviert werden?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1125	Wird die Sicherheitsrichtlinie der jeweiligen Zertifizierungsstellen geprüft, bevor sicherheitskritische Informationen über eine SSL/TLS-geschützte Verbindung übertragen werden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1126	Werden alle Daten, die über den Sicheren Kanal übertragen werden, signiert und verschlüsselt?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
SYS.02.01.A019 (A) Restriktive Rechtevergabe		
08202-1127	Existiert eine Regelung für die Benutzerumgebung temporärer Benutzerkonten?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1128	Ist der Kreis der zugriffsberechtigten Administratoren möglichst klein gehalten?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1129	Sind Benutzerumgebung und Startprozedur für den jeweiligen Benutzer an seine Aufgaben angepasst?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1130	Sind die restriktiven Berechtigungen mit dem Patchmanagement und dem Netz- und Systemmanagement abgestimmt?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1131	Sind in System-Verzeichnissen nur die notwendigen Privilegien für die Benutzer zur Verfügung gestellt?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1132	Werden Freigabeberechtigungen nicht an integrierte Systemgruppen wie Authentifizierte Benutzer oder Jeder erteilt?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1133	Wird die Nutzung von Editor-Programmen oder Compilern verhindert, wenn diese nicht für die Aufgabenerfüllung des Benutzers erforderlich sind?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1134	Wird regelmäßig überprüft, ob die Berechtigungen, insbesondere für Systemverzeichnisse und -dateien, den Vorgaben der Sicherheitsrichtlinie entsprechen?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1135	Wurde der Sicherheitsgruppe "Jeder" das Schreibrecht innerhalb von Systemordnern entzogen?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1136	Wurde der Zugriff durch die Gruppe Jeder auf die Registry eingeschränkt?	• Nein. • Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
08202-1137	Wurde für Anwendungen unter Windows ein restriktives Berechtigungskonzept definiert und umgesetzt?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1138	Wurden alle Berechtigungen restriktiv nach den so genannten Need-to-know- oder Least-Privilege-Strategien vergeben?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1139	Werden die Zugriffsrechte und Installationsmöglichkeiten für normale Benutzer unter Windows restriktiv vergeben?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
SYS.02.01.A020 (A) Schutz der Administrationsschnittstellen		
08202-1140	Werden bei der Remote-Administration bzw. bei Nutzung eines Managementsystems ausschließlich sichere Protokolle verwendet?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1141	Werden die zur Administration von Clients verwendeten Methoden in der Sicherheitsrichtlinie beschrieben?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
SYS.02.01.A021 (A) Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras		
08202-1142	Keine betriebliche Notwendigkeit zur Nutzung des Mikrofons: Existiert eine Regelung zur Abschaltung oder physikalischen Trennung des Rechnermikrofons?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1143	Bei internem Mikrofon bzw. betrieblicher Notwendigkeit: Existieren eindeutige Regelungen zur Rechtevergabe für die Nutzung des Mikrofons?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
SYS.02.01.A022 (A) Abmelden nach Aufgabenerfüllung [Benutzer]		
08202-1144	Erfolgt eine Verpflichtung aller Benutzer, sich nach Aufgabenerfüllung entsprechend vom IT-System oder von der Anwendung abzumelden?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1145	Sind technische Verfahren (z. B. automatisches Aktivieren der Bildschirmsperre) etabliert, um unerwünschte Benutzerwechsel unter ein und derselben Benutzerkennung bei kurzen Unterbrechungen der Arbeit am IT-System zu verhindern?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1146	Existiert eine Richtlinie für die Nutzung der Heimnetzgruppen-Funktionalität?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
SYS.02.01.A023 (A) Nutzung von Client-Server-Diensten		
08202-1147	Existiert eine Richtlinie, die den Einsatz von Peer-to-Peer-Diensten regelt?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1148	Werden Maßnahmen ergriffen um den unautorisierten Einsatz (Personen, Informationen, Dienste) von Peer-to-Peer-Diensten zu verhindern?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1149	Wurde der Einsatz von Peer-to-Peer-Diensten von der Geschäftsleitung genehmigt und die Restrisiken dokumentiert und angenommen?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1150	Wurde die Gruppenrichtlinie Beitritt des Computers zu einer Heimnetzgruppe verhindern entsprechend der Richtlinie konfiguriert?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1151	Wurden die Benutzer im Umgang mit den Freigaben der Heimnetzgruppe geschult?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1152	Ist dokumentiert, welche Peer-to-Peer-Dienste von wem genutzt werden, und welche Informationen dabei ausgetauscht werden?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A024 (A) Umgang mit Wechseldatenträgern im laufenden System		

Frage	Fragestellung	Antwortoption
08202-1153	Existiert eine Richtlinie, die den Umgang mit Wechselmedien und externen Datenspeichern regelt?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1154	Sind die Nutzer über alle Regelungen zum Umgang mit Laufwerken für Wechselmedien und externe Datenspeicher informiert?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1155	Wird der Anschluss von USB-Geräten protokolliert und werden diese Protokolle regelmäßig ausgewertet?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1156	Wird verhindert, dass Inhalte von eingelegten Wechseldatenträgern automatisch ausgeführt werden?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1157	Wurde die Korrektheit der technischen Umsetzung getestet?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1158	Wurden Vorgaben zur Nutzung von Wechselmedien definiert und umgesetzt?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1159	Sind die Benutzer über die sie betreffenden Vorgaben zur Nutzung von Wechselmedien informiert?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1160	Werden technische Maßnahmen ergriffen, um den Missbrauch von Wechselmedien zu verhindern?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
SYS.02.01.A025 (A) Richtlinie zur sicheren IT-Nutzung [Benutzer]		
08202-1161	Gibt es Regelungen zur Überwachung, ob die festgelegten Sicherheitsrichtlinien eingehalten werden?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1162	Ist die Kenntnisnahme der PC-Richtlinie durch den Benutzer vor erstmaliger Nutzung eines organisationseigenen IT-Systems verpflichtend?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.

Frage	Fragestellung	Antwortoption
08202-1163	Ist sichergestellt, dass die PC-Richtlinie allen relevanten Parteien zur Verfügung steht?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1164	Sind alle Benutzer darüber informiert, dass über den Papierkorb gelöschte Dateien nicht zuverlässig gelöscht sind?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1165	Wird die PC-Richtlinie regelmäßig, spätestens nach 2 Jahren, aktualisiert?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
SYS.02.01.A026 (S) Schutz von Anwendungen		
08202-1166	Wird der Systemzustand und die Funktionsfähigkeit der Clients laufend überwacht?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
SYS.02.01.A027 (A) Geregelte Außerbetriebnahme eines Clients		
08202-1167	Existiert ein dokumentiertes Verfahren zur Außerbetriebnahme von Clients?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1168	Wird sichergestellt, dass alle evtl. noch auf dem Client vorhandenen Daten gesichert und anschließend vom Client sicher gelöscht werden?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
SYS.02.01.A028 (A) Verschlüsselung der Clients (C)		
08202-1169	Ist geregelt, dass verschlüsselte Dateien, Partitionen oder Datenträger auch regelmäßig gesichert werden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1170	Ist geregelt, dass wenn vertrauliche Informationen auf den Clients gespeichert werden, die schutzbedürftigen Dateien, ausgewählte Dateisystembereiche oder besser die gesamte Festplatte verschlüsselt werden?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
SYS.02.01.A029 (A) Systemüberwachung (A)		
08202-1171	Existiert ein bedarfsgerechtes Systemüberwachungs- und Monitoringkonzept?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1172	Sind Stärke und Genauigkeit der Systemüberwachung von Windows Client-Betriebssystemen der Gefährdungslage angepasst?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1173	Werden Fehlerzustände sowie die Überschreitung definierter Grenzwerte an das Betriebspersonal gemeldet?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1174	Wird die Überwachungseinstellungen gemeinsam mit den Serverkomponenten von DirectAccess sorgfältig auf die Anforderungen des Informationsverbunds abgestimmt?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
SYS.02.01.A030 (A) Einrichten einer Referenzinstallation für Clients (C, I, A)		
08202-1175	Existieren Checklisten für Testfälle?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1176	Existiert eine dokumentierte Referenzinstallation für Clients?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1177	Bei hohen Schutzbedarfen: Besteht für jeden Clienttyp eine eigene Referenzinstallation, mit der Wechselwirkungen von Programmen/ Updates ausgeschlossen werden können?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
SYS.02.01.A031 (A) Einrichtung lokaler Paketfilter (C, I, A)		

Frage	Fragestellung	Antwortoption
08202-1178	Ist die Sicherheitsstrategie der lokalen Firewall gemäß dem Whitelist-Verfahren restriktiv?	• Nein. • Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
08202-1179	Ist für die Konfiguration eines lokalen Paketfilters eine Grundkonfiguration vorgesehen?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1180	Werden auf IT-Systemen lokale Zugriffsbeschränkungen auf Netz- und Anwendungsebene umgesetzt?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1181	Werden Maßnahmen zur lokalen ICMP-Filterung eingesetzt?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1182	Wird das lokale Firewall-Regelwerk regelmäßig überprüft?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1183	Wird die Richtlinie zum Einsatz einer lokalen Firewall regelmäßig aktualisiert?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.
SYS.02.01.A032 (A) Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits (C, I, A)		
08202-1184	Bei höheren Sicherheitsanforderungen an ein IT-System: Ist der Einsatz zusätzlicher Sicherheitsprodukte geprüft worden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1185	Werden organisatorische Maßnahmen ergriffen, falls ein geeignetes Sicherheitsprodukt kurzfristig nicht beschafft werden kann?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
SYS.02.01.A033 (A) Application Whitelisting (C, I, A)		
08202-1186	Ist alternativ einzelnen Anwendungen explizit die Ausführung gestattet worden?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1187	Sind vollständige Pfade bzw. Verzeichnisse festgelegt, aus denen Programme gestartet werden dürfen?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1188	Wird per Application Whitelisting sichergestellt, dass nur erlaubte Programme ausgeführt werden können?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A034 (A) Einsatz von Anwendungsisolation (C, I, A)		
08202-1189	Werden Anwendungen, mit denen externe Daten bearbeitet werden, ausschließlich in einer vom Betriebssystem isolierten Ablaufumgebung betrieben?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A035 (A) Aktive Verwaltung der Wurzelzertifikate (C, I)		
08202-1190	Sind auf dem Client lediglich die für den Betrieb notwendigen und vorab dokumentierten Wurzelzertifikate enthalten?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1191	Werden alle auf dem IT-System vorhandenen Zertifikatsspeicher in die Prüfung einbezogen werden (z.B. Zertifikatsspeicher von Web-Browsern, etc.)?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1192	Wird im Zuge der Beschaffung und Installation des Clients dokumentiert welche Wurzelzertifkate für den Betrieb des Clients notwendig sind?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1193	Wird regelmäßig überprüft, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der Institution entsprechen?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
SYS.02.01.A036 (E) Selbstverwalteter Einsatz von SecureBoot und TPM		
08202-1194	Ist der Boot-Vorgang bei UEFI-basierten mobilen IT-Systemen mit Secure Boot abgesichert?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1195	Werden auf UEFI-kompatiblen Systemen der Bootloader, Kernel sowie alle benötigten Firmware-Komponenten durch selbstkontrolliertes Schlüsselmaterial signiert ?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1196	Wird nicht benötigtes Schlüsselmaterial entfernt?	• Nein. • Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
SYS.02.01.A037 (E) Schutz vor unbefugten Anmeldungen (C, I, A)		
08202-1197	Werden anonyme Zugänge über das Netzwerk verhindert?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1198	Wird zur Verhinderung des Zugangs zum System durch kompromittierte Anmeldeinformationen eine Mehrfaktorauthentisierung verwendet?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.
SYS.02.01.A038 (A) Einbindung in die Notfallplanung (A)		
08202-1199	Enthalten die Notfall-Bootmedien alle erforderlichen Programme, Treiber und Daten?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1200	Entsprechen das gewählte Datensicherungsverfahren und die dafür verwendete Hard- und Software den Anforderungen an eine Wiederherstellung innerhalb der geforderten Wiederherstellungszeit?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1201	Existiert ein Notfallplan, und ist er Bestandteil des Notfallkonzeptes der Institution?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1202	Haben die Personen, die für die Wiederherstellung verantwortlich sind, bei einem Ausfall des IT-Systems Zugriff auf alle notwendigen Informationen wie Konfigurationsdaten, Lizenzschlüssel, administrative Benutzerkonten und Kennwörter?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1203	Ist die Aktualität des Notfallplans auch nach Konfigurationsänderungen sichergestellt?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1204	Ist die vollständige Wiederherstellung von rollenspezifischen Systemkomponenten gewährleistet, und sind die mit den Rollen verbundenen Einstellungen dokumentiert?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1205	Ist eine aktuelle Dokumentation der Datensicherung vorhanden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1206	Ist eine begründete Entscheidung zum Einsatz des TPM getroffen worden, und bestehen adäquate Konzepte für den Verlust dort gespeicherter kryptographischer Informationen?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1207	Ist sichergestellt, dass nur die hierzu berechtigten Personen auf die Notfall-Bootmedien zugreifen können?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1208	Sind die für eine Neuinstallation notwendigen Installationsdatenträger und Produktschlüssel vorhanden?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1209	Sind die notwendigen Dokumentationen und Handlungsanweisungen vor unbefugtem Zugriff geschützt?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1210	Sind im Notfallplan die notwendigen Voraussetzungen zur Wiederherstellung durch Neuinstallation festgehalten?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1211	Sind kryptographische Schlüssel und Zertifikate, insbesondere bei der Speicherung im TPM und beim Einsatz einer Festplattenverschlüsselung, in der Notfallplanung geeignet berücksichtigt?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1212	Stehen Notfall-Bootmedien zur Verfügung, mit denen die IT-Systeme gestartet und in einen kontrollierten Zustand versetzt werden können?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1213	Werden alle Programme und Bibliotheken ausschließlich vom Bootmedium geladen?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1214	Werden Bootmedien nach dem Erstellen getestet?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
08202-1215	Werden die Notfall-Bootmedien auf einem aktuellen Stand gehalten?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1216	Werden die Notfall-Bootmedien zumindest bei Erstellung und Änderung auf Schadprogramme überprüft?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1217	Werden Inhalte für Bootmedien aus sicheren Quellen bezogen?	• Ja. • Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1218	Wird für die Systemwiederherstellung das vorhandene Bereitstellungs- bzw. Installationskonzept berücksichtigt?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
SYS.02.01.A039 (A) Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] (A)		
08202-1219	Bei der Verwendung von Ausweichsystemen: Ist die Kapazität der Gesamtheit der Systeme bei einer möglichen Übernahme von Rollen und Funktionen ausreichend, um die ausgefallenen Systeme abzudecken?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1220	Bei erhöhten Anforderungen an die Verfügbarkeit von stationären Clients: Ist an Client und USV ein Überspannungsschutz vorhanden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1221	Bei erhöhten Anforderungen an die Verfügbarkeit von stationären Clients: Ist der Client an eine USV angeschlossen?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1222	Bei erhöhten Anforderungen an die Verfügbarkeit von stationären Clients: Ist die Leistung und die Stützzeit der USV ausreichend dimensioniert?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1223	Bei erhöhten Anforderungen an die Verfügbarkeit von stationären Clients: Wird bei Änderungen am Verbraucher erneut die Dimensionierung von Leistung und Stützzeit der USV geprüft?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1224	Bei erhöhten Anforderungen an die Verfügbarkeit von stationären Clients: Wird die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV regelmäßig getestet?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1225	Bei erhöhten Anforderungen an die Verfügbarkeit von stationären Clients: Wird die USV regelmäßig gewartet?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
SYS.02.01.A040 (A) Betriebsdokumentation		
08202-1226	Wird die Durchführung betrieblicher Aufgaben einschließlich Konfigurationsänderungen an Clients nachvollziehbar dokumentiert (Wer? Was? Wann?)?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1227	Sind aus der Dokumentation, insbesondere Konfigurationsänderungen nachvollziehbar?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1228	Werden auch sicherheitsrelevante Aufgaben (wer ist z. B. befugt, neue Festplatten einzubauen) dokumentiert?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1229	Wird die Dokumentation gegen unbefugten Zugriff und Verlust geschützt?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1230	Ist vorgesehen, automatische Dokumentationsmöglichkeiten zu nutzen?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
SYS.02.01.A041 (E) Verhinderung der Überlastung der lokalen Festplatte		
08202-1231	Sind Quotas eingerichtet worden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1232	Werden die Nutzer vor dem Erreichen der Quotas informiert?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
SYS.02.02.03.A001 (B) Planung des Einsatzes von Cloud-Diensten		

Frage	Fragestellung	Antwortoption
08202-1233	Ist bei Verwendung von Windows 10-basierten Geräten eine strategische Festlegung erfolgt, welche enthaltenen Cloud-Services in welchem Umfang genutzt werden sollen bzw. dürfen?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1234	Ist die Nutzung von Cloud-Diensten wie z. B. OneDrive in der Sicherheitsrichtlinie für Client-Systeme geregelt, und in der Einführungsplanung berücksichtigt?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
SYS.02.02.03.A002 (B) Geeignete Auswahl einer Windows 10-Version und Beschaffung		
08202-1235	Erfüllen die zum Einsatz kommenden Hardware-Plattformen die Anforderungen der Windows Hardware Certification Requirements?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1236	Ist speziell für die KMS-Reaktivierung sichergestellt, dass der KMS bei Clients von insgesamt mindestens 25 Windows-Systemen und bei Servern von mindestens 5 Windows-Systemen aktiv genutzt wird?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1237	Ist speziell für die KMS-Reaktivierung sichergestellt, dass die Windows-Systeme innerhalb von 210 Tagen nach der letzten Aktivierung mit dem KMS kommunizieren können?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1238	Ist speziell für die KMS-Reaktivierung sichergestellt, dass ein KMS im Zeitraum einer angestrebten Reaktivierung verfügbar ist?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1239	Ist unter Berücksichtigung des ermittelten Schutzbedürfnisses und des Einsatzzwecks sowie der Umsetzbarkeit der erforderlichen Absicherungsmaßnahmen die Auswahl des entsprechenden Lizenzmodells und Releasepfades (CB, CBB oder LTSB) erfolgt?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1240	Sind die technischen Voraussetzungen für die Aktivierung erfüllt?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1241	Stehen angemessene Verfahren für die Lizensierung, Aktivierung oder Re-Aktivierung der Systeme zur Verfügung?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1242	Werden in Abstimmung mit der Hardware- und Softwareplanung bevorzugt 64-Bit-Versionen eingesetzt?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1243	Wird basierend auf dem Ergebnis der Überprüfung der etablierte Beschaffungsprozess um die Auswahl des entsprechenden Lizenzmodells und Releasepfades (CB, CBB oder LTSB) erweitert?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1244	Wurde der Funktionsumfang und die Versorgung mit funktionalen Änderungen einer Windows 10-Version unter Berücksichtigung des ermittelten Schutzbedürfnisses und des Einsatzzwecks ausgewählt und die Umsetzbarkeit der erforderlichen Absicherungsmaßnahmen geprüft?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1245	Wurde die Auswahl der geeigneten Windows Version begründet und dokumentiert?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1246	Wurde geprüft, ob die Anwendungen die unter einer 64-Bit-Variante von Windows laufen sollen, 64-Bit fähig sind?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1247	Wurde vor der Beschaffung des Windows 10 Systems geprüft welche Editionen für den Einsatzzweck notwendig sind?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
SYS.02.02.03.A003 (B) Geeignetes Patch- und Änderungsmanagement		

Frage	Fragestellung	Antwortoption
08202-1248	Sind alle Windows 10 Systeme einem Patch- und Änderungsmanagement unterstellt?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1249	Sind für komplexe Patches oder Änderungen ein Umsetzungsplan, Tests, Kontroll- und Abbruchpunkte sowie Prioritäten für die Verteilung definiert?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1250	Werden die Gruppenrichtlinien getestet, bevor sie in einer Produktivumgebung eingesetzt werden?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1251	Wird bei jedem funktionalen Update überprüft, ob alle Anforderungen aus dem IT-Grundschutz auch nach dem Einspielen des Updates weiterhin erfüllt sind?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1252	Wird nach funktionalen Updates des Betriebssystems überprüft, ob alle Anforderungen aus dem IT-Grundschutz und den internen Vorgaben weiterhin erfüllt werden?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
SYS.02.02.03.A004 (B) Telemetrie und Datenschutzeinstellungen		

Frage	Fragestellung	Antwortoption
08202-1253	Sind die notwendigen Kommunikationsbeziehungen und übermittelten Daten der Anwendungen bekannt und dokumentiert? Wurden die Anwendungen so konfiguriert, dass nur ein notwendiges Minimum an Daten übertragen wird?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1254	Wird durch geeignete Maßnahmen, etwa auf Netzebene, sichergestellt, dass keine Diagnose- und Nutzungsdaten an Microsoft übertragen werden?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1255	Wird sichergestellt, dass Datenübertragungen an den Hersteller nur in einem Umfang erfolgen, der für den Betrieb unbedingt notwendig ist?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1256	Wurde bei der Auswahl von Anwendungen und Apps die Minimierung der Datenübertragung an Dritte als Kriterium berücksichtigt?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1257	Wurde unter Windows ab Version 7 die Einstellung für "Computerwartung" aktiviert?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1258	Wurden die Einstellungen für "Neueste Problembehandlungen vom Windows-Onlinedienst für Problembehandlung abrufen", "Problemberichte senden", "Regelmäßig Daten über Computerkonfiguration an Microsoft senden", "Windows-Sicherung", "Programm zur Benutzerfreundlichkeit" und "Problembehandlung - andere Einstellungen" unter Windows ab Version 7 deaktiviert?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1259	Wurden die Einstellungen zu den an den Hersteller Microsoft übertragenen Telemetriedaten sowie anderer Daten zur „Verbesserung der Benutzerfreundlichkeit" durch das Betriebssystem auf Konformität mit den organisationsinternen Vorgaben überprüft und Datenübertragungen restriktiv konfiguriert?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.
SYS.02.02.03.A005 (B) Schutz vor Schadsoftware		
08202-1260	Wird der Einsatz einer spezialisierten Komponente zum Schutz vor Schadsoftware auf Windows 10-Clients umgesetzt, sofern nicht gleich- oder höherwertige andere Maßnahmen (z.B. eine Anwendungskontrolle in Verbindung mit Anwendungsisolation sowie Maßnahmen zur Exploit-Mitigation) zum Schutz des IT-Systems vor Infektion mit Schadsoftware getroffen wurden?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.02.03.A006 (B) Integration von Online-Konten in das Betriebssystem [Benutzer]		
08202-1261	Erfolgt die Anmeldung am Windows-System über ein lokales oder Active-Directory-basiertes Konto und nicht mit einem Microsoft-Konto?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1262	Ist die Anmeldung am System und der Domäne nur mit dem Konto eines selbst betriebenen Verzeichnisdienstes möglich?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1263	Ist die Anmeldung über Online-Konten (z.B. MS-Konto) deaktiviert?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
08202-1264	Ist die Anmeldungen mit lokalen Konten nur Administratoren vorbehalten?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.
08202-1265	Wird die Synchronisierung von Nutzerdaten mit Microsoft Cloud-Diensten und das Sharing von WLAN-Passwörtern vollständig deaktiviert?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1266	Wurden Microsoft-Konten für die Nutzer nicht oder nur mit den unbedingt erforderlichen Angaben zu den Personen angelegt?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
SYS.02.02.03.A007 (A) Lokale Sicherheitsrichtlinien		
08202-1267	Ist die Autostart-Funktionalität für alle Laufwerke deaktiviert worden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.

Frage	Fragestellung	Antwortoption
08202-1268	Ist eine für die Windows-Clients bedarfsgerechte Arbeitsumgebung für die Benutzer eingerichtet worden?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1269	Ist sichergestellt, dass Standardbenutzer den Geschützten Modus für die drei Sicherheitszonen Internet, Lokales Intranet und Eingeschränkte Sites nicht deaktivieren können?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1270	Setzen Sie lokale Sicherheitsrichtlinien ein?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1271	Sind alle nicht benötigten Anwendungen und Komponenten mittels Gruppenrichtlinien oder durch die Nutzung einer Software zur Anwendungskontrolle deaktiviert worden?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1272	Sind die automatische Benutzeranmeldung und der automatische Login in der Wiederherstellungskonsole deaktiviert worden?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1273	Sind die Firewalleinstellungen restriktiv konfiguriert ?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1274	Werden Abweichungen dokumentiert und begründet?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1275	Werden alle nicht benötigten Anwendungen und Komponenten deaktiviert?	• Ja. • Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
08202-1276	Werden bei einem Einsatz in einer Active Directory Umgebung die Rechte zum Hinzufügen von Arbeitsstationen zur Domäne eingeschränkt?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1277	Werden die Einstellungen der Gruppenrichtlinien für Systeme, die einer Domäne angeschlossen sind, über das Active Directory verteilt und durchgesetzt?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1278	Werden die lokalen Sicherheitseinstellungen dokumentiert?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1279	Werden die Sicherheitsrichtlinien gemäß den Empfehlungen des Betriebssystem Herstellers und dem voreingestellten Standardverhalten konfiguriert, sofern das Standardverhalten nicht anderen Anforderungen aus dem Grundschutz oder der Organisation widerspricht?	• Ja. • Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
08202-1280	Werden die Standardstarteinstellungen der Windows-Dienste DPS, WDiSvcHost, und WerSvc genutzt?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1281	Werden die Verwaltungswerkzeuge der Windows Client-Betriebssysteme entsprechend den Anforderungen eingesetzt?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1282	Werden sicherheitsrelevante Einstellungen bedarfsgerecht konfguriert, getestet und regelmäßig überprüft?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.

Frage	Fragestellung	Antwortoption
08202-1283	Wird der Geschützte Modus für die gewünschten Zonen in den Internetsicherheitseinstellungen erzwungen?	• Nein. • Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
08202-1284	Wird die Erlaubnis oder das Verbot der Speicherung von Zugangsdaten mit Hilfe der Anmeldeinformationsverwaltung in einer Richtlinie festgelegt?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1285	Wird die selbstständige Kommunikation von Windows Diensten und Anwendungen unterbunden?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1286	Wird ein Verbot der Speicherung von Zugangsdaten mit Hilfe der Anmeldeinformationsverwaltung technisch durchgesetzt?	• Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1287	Wird verhindert, dass Windows Clients Anwendungen, Windows Apps oder Dienste im Netz zur Verfügung stellen?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.

Frage	Fragestellung	Antwortoption
08202-1288	Wurde bei Clientsystemen ab Windows Vista für den Built-In Administrator ein Kennwort angelegt?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1289	Wurde darauf geachtet, dass nur die unbedingt notwendigen Konten unter Windows vorhanden sind?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1290	Wurde das Gastkonto mit einem komplexen Kennwort versehen?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1291	Wurde der Systemzugang auf autorisierte Personen beschränkt?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1292	Wurde eine entsprechende Warnmeldung für Benutzer konfiguriert, die sich lokal anzumelden versuchen?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1293	Wurden alle sicherheitsrelevanten Einstellungen in den Gruppenrichtlinien konfiguriert?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1294	Wurden die Basiseinstellungen für die Windows Group Policy Objects an eigene Anforderungen angepasst?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1295	Wurden die Konfigurationsempfehlungen des Herstellers zur Absicherung der Systeme herangezogen?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1296	Wurden mögliche sicherheitsrelevante Auswirkungen untersucht, die sich aus dem Abschwächen der Basiseinstellungen der Windows Group Policy Objects ergeben?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
SYS.02.02.03.A008 (A) Zentrale Verwaltung der Sicherheitsrichtlinien von Clients		
08202-1297	Erfolgt eine geeignete Verteilung der Sicherheitseinstellungen auf mehrere Gruppenrichtlinienobjekt (GPO)?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1298	Ist sichergestellt, dass auf allen Rechnern die richtigen Gruppenrichtlinienobjekte für die jeweils eingesetzte Windows-Version angewandt werden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1299	Liegen der Planung der Sicherheitsrichtlinien die unterschiedlichen Einsatzszenarien der Windows-Clients zugrunde?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1300	Sind alle technisch nicht umsetzbaren Konfigurationsparameter dokumentiert, begründet und mit dem Sicherheitsmanagement abgestimmt?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1301	Sind die Gruppenrichtlinien (Gruppen, anwendungsspezifische, benutzerspezifische) bedarfsgerecht konfiguriert?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1302	Werden alle Einstellungen des Windows 10 Clients durch ein zentrales Management verwaltet?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.

Frage	Fragestellung	Antwortoption
08202-1303	Werden in der Sicherheitsrichtlinie auch Anforderungen an die Sicherheit bei der Datenübertragung geregelt?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1304	Werden Werkzeuge eingesetzt, welche eine zentrale und einheitliche Konfiguration der Sicherheitseinstellungen ermöglichen?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
SYS.02.02.03.A009 (A) Sichere zentrale Authentisierung der Windows-Clients		
08202-1305	Setzen Sie eine zentrale Authentisierung ausschließlich mittels Kerberos ein?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1306	Sind abweichende Einstellungen begründet sowie mit dem Sicherheitsmanagement abgestimmt?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1307	Sind die eingesetzten kryptografischen Mechanismen entsprechend dem ermittelten Schutzbedarf und basierend auf den internen Richtlinien konfiguriert, dokumentiert?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein. • Ja.

Frage	Fragestellung	Antwortoption
08202-1308	Verhindert eine GPO die Verwendung älterer Protokolle?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1309	Verhindert eine Gruppenrichtlinie die Verwendung älterer Protokolle (nicht älter alsNTLMv2)?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1310	Wird die Speicherung der LAN Manager-Hashwerte bei Kennwortänderungen per Gruppenrichtlinie deaktiviert?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1311	Wird in reinen Windows-Netzen (mit Client- und Server-Betriebssystemen ab Windows 2000) zur zentralen Authentisierung für SSO ausschließlich Kerberos eingesetzt?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1312	Wird Kerberos als Authentisierungsverfahren oder mindestens NTLMv2-Authentisierung genutzt sowie die 128-Bit-Verschlüsselung aktiviert, wenn auf allen Rechnern Client-Betriebssysteme ab Windows XP bzw. Server-Betriebssysteme ab Windows Server 2003 mit aktivierter 128-Bit-Verschlüsselung ausgeführt werden?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1313	Wurde anonymen Zugängen über das Netz die Berechtigung "Jeder" entzogen?	• Nein. • Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
08202-1314	Wurde gewährleistet, dass auch ältere Clients das NTLMv2 Verfahren zur Authentisierung verwenden (z. B. durch das Einspielen entsprechender Service Packs oder zusätzlicher Software)?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
SYS.02.02.03.A010 (A) Konfiguration zum Schutz von Anwendungen in Windows 10		
08202-1315	Ist die Datenausführungsverhinderung (DEP) für alle Programme und Dienste (Opt-Out Modus) aktiviert worden?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1316	Werden unter AppLocker bevorzugt Regeln auf der Grundlage von Anwendungssignaturen definierter Herausgeber eingesetzt?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1317	Wird AppLocker zur Verhinderung der unautorisierten Installation und Ausführung von Software und Windows-Apps (ab Windows 8) auf den Clients genutzt?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1318	Wird bei der Nutzung von AppLocker der Ansatz der Positivliste ("Es ist alles verboten, was nicht explizit erlaubt ist") genutzt?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
SYS.02.02.03.A011 (A) Schutz der Anmeldeinformationen in Windows 10		
08202-1319	Sofern VSM und CG nicht möglich sind, wird für den Betrieb des für die Verwaltung der Anmeldeinformationen zuständigen LSAS-Dienstes der geschützte Modus (PPL - Protected Process Light) aktiviert?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1320	Wird der "Virtual Secure Mode (VSM)" für die Speicherung lokaler Passwörter genutzt, sofern Windows 10 in der Enterprise-Version auf einem physikalischen System installiert ist?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1321	Wird die Netzwerkanmeldung von lokalen Konten unterbunden?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
SYS.02.02.03.A012 (A) Datei- und Freigabeberechtigungen		
08202-1322	Gibt es für Windows Versionen ein Konzept zur Datenablage, Datensicherung und Verschlüsselung der Benutzerdaten?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1323	Sind die Berechtigungen aller Verzeichnisse und Dateien auf allen, von einem älteren Windows-Betriebssystem aktualisierten, Rechnern überprüft worden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1324	Sind die eingestellten Datei- und Verzeichnisberechtigungen von freigegebenen Verzeichnissen für den Netzzugriff geeignet? Wurden die Freigaben so restriktiv wie möglich vergeben?	• Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1325	Werden die Schreibrechte für Nutzer auf einen definierten Bereich im Dateisystem beschränkt?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
08202-1326	Wird der Zugriff auf Dateien und Ordner auf dem lokalen System sowie auf Netzwerkfreigaben gemäß einem Berechtigungs- und Zugriffskonzept konfiguriert (dies umfasst im Speziellen auch die standardmäßig vorhandenen administrativen Freigaben auf dem System)?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1327	Wird sichergestellt, dass Clients keine Dateifreigaben anbieten?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1328	Wird sichergestellt, dass Nutzer keine Schreibrechte in Ordner des Betriebssystems oder von installierten Programmen erhalten?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1329	Wurde ein bedarfsgerechtes Berechtigungs- und Zugriffskonzept für Windows erstellt?	• Nein. • Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
SYS.02.02.03.A013 (A) Einsatz der SmartScreen-Funktionen		
08202-1330	Ist die SmartScreen-Funktion, die aus dem Internet heruntergeladene Dateien und Webinhalte auf mögliche Schadsoftware untersucht und dazu unter Umständen personenbezogene Daten an Microsoft überträgt, deaktiviert?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)
08202-1331	Wurde die Verträglichkeit der SmartScreen Funktion zu internen oder externen Datenschutzvorgaben überprüft und bewertet?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.02.03.A014 (A) Einsatz des Sprachassistenten Cortana [Benutzer]		
08202-1332	Sind in Ihrer Institution Regelungen zur Deaktivierung von Cortana getroffen?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.

Frage	Fragestellung	Antwortoption
08202-1333	Wurde der Sprachassistent CORTANA deaktiviert?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)
SYS.02.02.03.A015 (A) Einsatz der Synchronisationsmechanismen in Windows 10		
08202-1334	Ist die Synchronisierung von Nutzerdaten mit Microsoft Cloud-Diensten und das Sharing von WLAN-Passwörtern auf Windows 10-Clients vollständig deaktiviert?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
SYS.02.02.03.A016 (A) Anbindung von Windows 10 an den Windows Store		
08202-1335	Gibt es Vorgaben für die Installation von Apps aus dem Windows-Store und deren Nutzung? Sind die Vorgaben und Anforderungen entsprechend in der Planung berücksichtigt?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1336	Wird der Einsatz von Apps aus dem Windows Store auf Clients ab Windows 8 berücksichtigt?	• Ja. • Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
08202-1337	Wird die Anbindung an einen AppStore, sofern sie nicht unbedingt benötigt wird, deaktiviert?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
SYS.02.02.03.A017 (A) Verwendung der automatischen Anmeldung		
08202-1338	Ist die automatische Anmeldung deaktiviert?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1339	Wird die Speicherung von Kennwörtern, Zertifkaten und anderen Anmeldeinformationen zur automatischen Anmeldung auf Webseiten und IT-Systemen verhindert?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
SYS.02.02.03.A018 (A) Einsatz der Windows-Remoteunterstützung (nicht RDP)		
08202-1340	Ist die Gruppe der berechtigten Benutzer für den Remote-Desktopzugriff über die Zuweisung entsprechender Benutzerrechte oder in den Richtlinien festgelegt worden?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1341	Kann eine Remote-Unterstützung nur nach einer expliziten Einladung über EasyConnect oder eine Einladungsdatei erfolgen?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1342	Wird bei der Speicherung einer Einladung in einer Datei ein Kennwort auf die Datei vergeben?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.

Frage	Fragestellung	Antwortoption
08202-1343	Sind die Gruppenrichtlinien sicher und bedarfsgerecht konfiguriert worden?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1344	Werden die Auswirkungen auf die Konfiguration der Firewall bei der Planung der Remote-Unterstützung berücksichtigt?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1345	Wurden die Fernsteuerungsmechanismen vollständig deaktiviert, wenn deren Einsatz nicht vorgesehen ist?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
SYS.02.02.03.A019 (A) Verwendung des Fernzugriffs über RDP [Benutzer]		
08202-1346	Muss der aktuell angemeldete Benutzer dem Aufbau einer Sitzung immer explizit zustimmen?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
08202-1347	Stellt eine Prüfung sicher, ob Umleitungen der Zwischenablage, Drucker, Dateiablagen und Smartcard-Anschlüssen notwendig sind, und werden diese andernfalls deaktiviert?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.

Frage	Fragestellung	Antwortoption
08202-1348	Wird vorgeschreiben, dass bei RDP-Verbindungen immer die bestmögliche Verschlüsselungsstufe verwendet werden soll?	• Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Ja. • Nein.
SYS.02.02.03.A020 (A) Einsatz der Benutzerkontensteuerung für privilegierte Konten		
08202-1349	Ist der Einsatz der User Account Control (UAC) im Berechtigungskonzept geregelt?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1350	Ist die Benutzerkontensteuerung (UAC, User Account Control) aktiviert?	• Teilweise (Verweis oder Erläuterung) • Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1351	Ist für Administratoren die GPO-Richtlinie Benutzerkontensteuerung: Verhalten der Benutzeraufforderung mit erhöhten Rechten für Administratoren im Administratorbestätigungsmodus gemäß einer Abwägung von Bedienbarkeit und Sicherheitsniveau konfiguriert und diese Entscheidung dokumentiert?	• Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja.
08202-1352	Sind alle Konten mit Administratorrechten dokumentiert?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1353	Sind vorhandene Sicherheitsmaßnahmen und -merkmale des eingesetzten IT-/ Betriebssystems wie die Benutzerkontensteuerung (UAC) aktiv, um die Einschränkung der Benutzerumgebung durchzusetzen?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung) • Ja.
08202-1354	Werden vergebene Administratorrechte regelmäßig auf ihre Notwendigkeit überprüft, entsprechend angepasst und gegebenenfalls wieder entzogen?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1355	Wurde definiert, welche Sicherheitsmechanismen für den Integritätsschutz ab Windows Vista/Server 2008 umgesetzt werden sollen?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein. • Teilweise (Verweis oder Erläuterung)
08202-1356	Wurden die Benutzer für den Umgang mit dem Geschützten Modus geschult, so dass sie nicht ohne hinreichende Prüfung herunter geladene Dateien bzw. Programme autorisieren?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
SYS.02.02.03.A021 (A) Einsatz des Encrypting File Systems EFS (C, I)		
08202-1357	Existieren von allen privaten Schlüsseln Datensicherungen?	• Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1358	Ist den Benutzern bekannt, wie sie sich bei Verlust eines Authentisierungsmittels zu verhalten haben?	• Ja. • Nein. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
08202-1359	Ist der Einsatz von EFS ausreichend zur Erfüllung der betrieblichen Anforderungen an die Vertraulichkeit?	• Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1360	Ist eine geeignete Form der Authentisierung des Benutzers gegenüber BitLocker beim Systemstart ausgewählt worden?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1361	Ist sichergestellt, dass nur Befugte Zugriff auf das Wiederherstellungskennwort oder den Wiederherstellungsschlüssel von Windows BitLocker To Go haben?	• Nein. • Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)
08202-1362	Sind alle Windows Benutzer im korrekten Umgang mit EFS geschult?	• Nein. • Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1363	Sind mit EFS verschlüsselte Dateien zusätzlich durch restriktive Zugriffsrechte geschützt?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1364	Verwenden Benutzer unter Windows ein geeignetes Verschlüsselungskennwort oder -zertifikat?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein. • Ja.
08202-1365	Werden alle Schlüssel und Kennwörter vernichtet, wenn Datenträger verloren gehen oder ausgesondert werden?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1366	Wird die Registry-Verschlüsselung mit Passwort mittels des Tools syskey verwendet, wenn EFS mit lokalen Konten eingesetzt wird?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)
08202-1367	Wird verhindert, dass die Windows Boot-Datei autoexec.bat verschlüsselt werden kann?	• Nein. • Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1368	Wurde ein dediziertes Konto für den Wiederherstellungsagenten erzeugt und dessen privater Schlüssel gesichert und aus dem System entfernt?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
08202-1369	Wurden der Ruhezustand (Hibernation Modus) und der hybride Standbymodus bei Verwendung von EFS und Nutzung von Windows Versionen vor Windows Vista und Windows Server 2008 deaktiviert?	• Ja. • Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Nein.
SYS.02.02.03.A022 (A) Windows PowerShell (WPS) (C, I, A)		
08202-1370	Ist die Ausführung von Windows PowerShell-Skripten mit dem Befehl Set-ExecutionPolicy AllSigned oder durch eine Gruppenrichtlinie eingeschränkt worden?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1371	Ist eine Protokollierung von Schreib- und Lesezugriffen auf das Windows PowerShell-Profil eingerichtet, und werden die Protokolle regelmäßig ausgewertet?	• Nein. • Ja. • Entbehrlich (Verweis oder Erläuterung) • Teilweise (Verweis oder Erläuterung)
08202-1372	Ist in der Windows PowerShell die Ausführbarkeit der Dateien von WPS auf Dateiebene den Gruppen der Administratoren, lokal und Domäne vorbehalten?	• Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung) • Nein.
SYS.02.02.03.A023 (A) Erweiterter Schutz der Anmeldeinformationen in Windows 10 (C, I)		

Frage	Fragestellung	Antwortoption
08202-1373	Sind die vorhandenen Schlüssel für UEFI Secure Boot kontrolliert und hinsichtlich Vertrauenswürdigkeit bewertet worden?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1374	Wird der Start des Betriebssystems bei UEFI-basierten Geräten mittels UEFI Secure Boot abgesichert?	• Teilweise (Verweis oder Erläuterung) • Ja. • Nein. • Entbehrlich (Verweis oder Erläuterung)
08202-1375	Wird der Status von Secure Boot bei UEFI-basierten Systemen für LSASS bei Systemstart überwacht?	• Teilweise (Verweis oder Erläuterung) • Entbehrlich (Verweis oder Erläuterung) • Ja. • Nein.
08202-1376	Wird von der Option "RestrictedAdmin" gebrauch gemacht, wenn eine Fernwartung der Client-Systeme mittels RDP vorgesehen ist?	• Entbehrlich (Verweis oder Erläuterung) • Ja. • Teilweise (Verweis oder Erläuterung) • Nein.
SYS.02.02.03.A024 (A) Aktivierung des Last-Access-Zeitstempels (A)		
08202-1377	Wurde bei der Erstellung des Sicherheitskonzeptes für Systeme mit Windows 10 geprüft, ob man auf den Last-Access-Zeitstempel verzichten kann?	• Nein. • Teilweise (Verweis oder Erläuterung) • Ja. • Entbehrlich (Verweis oder Erläuterung)

Frage	Fragestellung	Antwortoption
08202-1378	Wurden bei dieser Prüfung auch Performanceaspekte von Windows 10 in die Bewertungen einbezogen?	• Ja. • Teilweise (Verweis oder Erläuterung) • Nein. • Entbehrlich (Verweis oder Erläuterung)

Tabelle 4: ***Webfragebögen***

3.3 Technische Prüfungen

Dieses Kapitel enthält eine Übersicht über alle in diesem SiM grundsätzlich verwendbaren technischen Checks. Bei einigen Checks werden sehr vom jeweiligen Einsatzzweck abhängige Parameter abgefragt. Mit Blick auf einen möglichst breiten Geltungsbereich des SiM ist bei diesen Checks für die erste Erhebung doch das Format der Webfrage gewählt worden. Die entsprechenden Checks sind mit dem Vermerk "Als Webfrage" in der Spalte Bewertung gekennzeichnet.

Check	Prüfaspekt	Prüfparameter	Bewertung
SYS.02.01.A001 (B) Benutzerauthentisierung			
08202-0001	Is 'Maximum password age' set to greater or equal 1 and less or equal 42 (days) or never expires?		This check passes if the value set for 'Maximum password age' is between 1 and 42.
08202-0002	Is 'Password must meet complexity requirements' set to 'Enabled'?		This check passes if 'Passwords must meet complexity requirements' is set to Enabled.
SYS.02.01.A003 (B) Aktivieren von Autoupdate-Mechanismen			
08202-0003	Is 'Configure Automatic Updates' set to 'Enabled: 4 - Auto download and schedule the install'?		This check passes if 'Configure Automatic Updates' is set to 'Enabled (4- Auto download and schedule the install)'.
08202-0004	Is 'Configure Automatic Updates: Scheduled install day' set to '0 - Every day'?		This check passes if 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'.
SYS.02.01.A007 (B) Protokollierung			
08202-0005	Is 'Application: Control Event Log behavior when the log file reaches its maximum size' set to 'Disabled'?		This check passes if Application: Control Event Log behavior when the log file reaches its maximum size is set to Disabled.
08202-0006	Is 'Specify the maximum log file size (KB) (Application Log)' set to 'Enabled: 32768' or greater?		This check passes if maximum application log size is 32768 KB or more.
08202-0007	Is 'Audit Account Lockout' set to 'Success'?		This check passes if 'Audit Account Lockout' is set to 'Success'
08202-0008	Is 'Audit Application Group Management' set to 'Success and Failure'?		This check passes if 'Audit Policy: Account Management: Computer Account Management' is set to Success and Failure.
08202-0009	Is 'Audit Policy: Account Logon: Credential Validation' set to 'Success and Failure'?		This check passes if 'Audit Policy: Account Logon: Credential Validation' is set to Success and Failure.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0010	Is 'Audit Policy: Account Management: Computer Account Management' set to 'Success and Failure'?		This check passes if 'Audit Policy: Account Management: Computer Account Management' is set to Success and Failure.
08202-0011	Is 'Audit Policy: Account Management: Other Account Management Events' set to 'Success and Failure'?		This check passes if 'Audit Policy: Account Management: Other Account Management Events' is set to Success and Failure.
08202-0012	Is 'Audit Policy: Account Management: Security Group Management' set to 'Success and Failure'?		This check passes if 'Audit Policy: Account Management: Security Group Management' is set to Success and Failure.
08202-0013	Is 'Audit Policy: Account Management: User Account Management' set to 'Success and Failure'?		This check passes if 'Audit Policy: Account Management: User Account Management' is set to Success.
08202-0014	Is 'Audit Policy: Detailed Tracking: PNP Activity' set to 'Success'?		This check passes if 'Audit Policy: Detailed Tracking: PNP Activity' is set to 'Success'.
08202-0015	Is 'Audit Policy: Detailed Tracking: Process Creation' set to 'Success'?		This check passes if 'Audit Policy: Detailed Tracking: Process Creation' is set to Success.
08202-0016	Is 'Audit Policy: Logon/Logoff: Other Logon/Logoff Events' set to 'Success and Failure'?		This check passes, if the state for this setting is: Success and Failure.This subcategory reports other logon/logoff-related events such as: * Terminal Services session disconnects and reconnects * Using RunAs to run processes under a different account * Locking and unlocking a workstation.
08202-0017	Is 'Audit Policy: Logon-Logoff: Account Lockout' set to 'Success'?		This check passes if 'Audit Account Lockout' is set to 'Success'
08202-0018	Is 'Audit Policy: Logon-Logoff: Logoff' set to 'Success'?		This check passes if 'Audit Policy: Logon-Logoff: Logoff' is set to Success.
08202-0019	Is 'Audit Policy: Logon-Logoff: Logon' set to 'Success and Failure'?		This check passes if 'Audit Policy: Logon-Logoff: Logon' is set to Success and Failure.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0020	Is 'Audit Policy: Logon-Logoff: Special Logon' set to 'Success and Failure'?		This check passes if 'Audit Policy: Logon-Logoff: Special Logon' is set to Success and Failure.
08202-0021	Is 'Audit Policy: Object Access: Removable Storage' set to 'Success and Failure'?		This check passes if "Audit Removable Storage' is set to 'Success and Failure'
08202-0022	Is 'Audit Policy: Policy Change: Audit Policy Change" set to 'Success and Failure'?		This check passes if 'Audit Policy: Policy Change: Audit Policy Change' is set to Success and Failure.
08202-0023	Is 'Audit Policy: Policy Change: Authentication Policy Change' set to 'Success and Failure'?		This check passes if 'Audit Policy: Policy Change: Authentication Policy Change' is set to Success and Failure.
08202-0024	Is 'Audit Policy: Privilege Use: Sensitive Privilege Use' set to 'Success and Failure'?		
08202-0025	Is 'Audit Policy: System: IPsec Driver' set to 'Success and Failure'?		This check passes if 'Audit Policy: System: IPsec Driver' is set to Success and Failure.
08202-0026	Is 'Audit Policy: System: Other System Events' set to 'Success and Failure'?		This check passes if 'Audit Policy: System: Other System Events is set to Succes and Failure.
08202-0027	Is 'Audit Policy: System: Security State Change' set to audit 'Success and Failure'?		This check passes if 'Audit Policy: System: Security State Change' is set to Success and Failure.
08202-0028	Is 'Audit Policy: System: Security System Extension' set to 'Success and Failure'?		This check passes if 'Audit Policy: System: Security System Extension' is set to Success and Failure.
08202-0029	Is 'Audit Policy: System: System Integrity' set to 'Success and Failure'?		This check passes if 'Audit Policy: System: System Integrity' is set to Success and Failure.
08202-0030	Is 'Security: Control Event Log behavior when the log file reaches its maximum size' set to 'Disabled'?		This check passes if Security: Control Event Log behavior when the log file reaches its maximum size is set to Disabled.
08202-0031	Is 'Setup: Control Event Log behavior when the log file reaches its maximum size' set to 'Disabled'?		This check passes if Setup: Control Event Log behavior when the log file reaches its maximum size is set to Disabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0032	Is 'Setup: Specify the maximum log file size (KB)' set to 'Enabled: 32,768' or greater?		This check passes if Setup: Maximum Log Size (KB) is 32768 KB or more.
08202-0034	Is 'Specify the maximum log file size (KB) (Security Log)' set to 'Enabled: 196,608' or greater?		This check passes if 'Security: Maximum Log Size (KB)' is set to 196,608 KB or more.
08202-0035	Is 'Specify the maximum log file size (KB) (System Log)' set to 'Enabled: 32768' or greater?		This check passes if System: Maximum Log Size (KB) is 32768 KB or more.
08202-0036	Is 'System: Control Event Log behavior when the log file reaches its maximum size' set to 'Disabled'?		This check passes if System: Control Event Log behavior when the log file reaches its maximum size is set to Disabled.
SYS.02.01.A008 (A) Absicherung des Boot-Vorgangs			
08202-0037	Is 'Allow enhanced PINs for startup' set to 'Enabled'?		This check passes if 'Allow enhanced PINs for startup' is set to 'Enabled'.
08202-0038	Is 'Allow Secure Boot for integrity validation' set to 'Enabled'?		This check passes if 'Allow Secure Boot for integrity validation' is set to 'Enabled'.
SYS.02.01.A014 (A) Updates und Patches für Firmware, Betriebssystem und Anwendungen			
08202-0039	Is 'Defer Upgrades and Updates' set to 'Enabled: 1 months, 0 weeks'?		This check passes if 'Defer Upgrades and Updates' is set to 'Enabled: 1 months, 0 weeks'?.
08202-0040	Is 'No auto-restart with logged on users for scheduled automatic updates installations' set to 'Disabled?		This check passes if 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled.
SYS.02.01.A015 (A) Sichere Installation und Konfiguration von Clients			
08202-0041	Is 'Allow user control over installs' set to 'Disabled'?		This check passes if 'Allow user control over installs' is set to 'Disabled'.
08202-0042	Is 'Configure Cookies' set to 'Enabled: Block only 3rd-party cookies'?		This check passes if 'Configure Cookies' is set to 'Enabled: Block only 3rd-party cookies.' or higher.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0043	Wird die Synchronisierung der Systemzeit mittels einer zuverlässigen Zeitquelle sichergestellt?		This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You might want to disable this service if you decide to use a third-party time provider.The recommended state for this setting is: Enabled.
SYS.02.01.A019 (A) Restriktive Rechtevergabe			
08202-0044	Is 'Access credential Manager as a trusted caller' set to 'No One'?		This check passes if 'Access Credential Manager as a trusted caller' is set to None.
08202-0045	Is 'Access this computer from the network' set to 'Administrators'?		This check passes if 'Access this computer from the network' is set to Administrators, Users.
08202-0046	Is 'Act as part of the operating system' set to 'No One'?		This check passes if 'Act as part of the operating system' is set to No One.
08202-0047	Is 'Adjust memory quotas for a process' set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'?		This check passes if "Adjust memory quotas for a process" is set to authorized users.
08202-0048	Is 'Allow log on locally' set to 'Administrators, Users'?		This check passes if 'Allow log on locally' is set to Administrators, Users.
08202-0049	Is 'Back up files and directories' set to 'Administrators'?		This check passes if right to back up files and directories is set to Administrators.
08202-0050	Is 'Change the system time' set to 'Administrators, LOCAL SERVICE'?		This check passes if 'Change the system time' is set to Local Service, Administrators.
08202-0051	Is 'Change the time zone' set to 'Administrators, LOCAL SERVICE'?		This check passes if Change the time zone is set to Local Service, Administrators.
08202-0052	Is 'Create a pagefile' set to 'Administrators'?		This check passes if 'Create a pagefile' is set to Administrators.
08202-0053	Is 'Create a token object' set to 'No One'?		This check passes if 'Create a token object' is set to None.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0054	Is 'Create global objects' set to 'Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE'?		Check passes if Create global objects is set to Administrators, SERVICE, LOCAL SERVICE, NETWORK SERVICE.
08202-0055	Is 'Create permanent shared objects' set to 'No One'?		This check passes if 'Create permanent shared objects' permits none.
08202-0056	Is 'Create symbolic links' set to 'Administrators'?		The check passes if 'Create symbolic links' is set to Administrators. Fails if: Otherwise.
08202-0057	Is 'Debug programs' set to 'Administrators'?		This check passes if 'Debug programs' is set to Administrators.
08202-0058	Is 'Domain member: Digitally encrypt or sign secure channel data (always)' set to 'Enabled'?		This check passes if 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to Enabled.
08202-0059	Is 'Domain member: Digitally encrypt secure channel data (when possible)' set to 'Enabled'?		This check passes if 'Domain member: Digitally encrypt secure channel data (when possible)' is set to Enabled.
08202-0060	Is 'Domain member: Digitally sign secure channel data (when possible)' set to 'Enabled'?		This check passes if 'Domain member: Digitally sign secure channel data (when possible)' is set to Enabled.
08202-0061	Is 'Domain member: Disable machine account password changes' set to 'Disabled'?		This check passes if 'Domain member: Disable machine account password changes' is set to Disabled.
08202-0062	Is 'Domain member: Maximum machine account password age' set to greater or equal 1 and less or equal 42 (days)?		This check passes if 'Domain member: Maximum machine account password age' is set to 42.
08202-0063	Is 'Domain member: Require strong (Windows 2000 or later) session key' set to 'Enabled'?		The check passes if 'Domain member: Require strong (Windows 2000 or later) session key' is enabled. (This check is not applicable to standalone or workgroup machines.)
08202-0064	Is 'Enable computer and user accounts to be trusted for delegation' set to 'No One'?		This check passes if 'Enable computer and user accounts to be trusted for delegation' is assigned to no one.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0065	Is 'Enumerate administrator accounts on elevation' set to 'Disabled'?		This check passes if 'Enumerate administrator accounts on elevation' is set to 'Disabled'.
08202-0066	Is 'Force shutdown from a remote system' set to 'Administrators'?		The check passes if 'Force shutdown from a remote system' is set to Administrators. Fails if: Otherwise.
08202-0067	Is 'Generate security audits' set to 'LOCAL SERVICE, NETWORK SERVICE'?		This check passes if 'Generate security audits' is set to Local Service, Network Service.
08202-0068	Is 'Impersonate a client after authentication' set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' ?		This check passes if 'Impersonate a client after authentication' is set for Administrators, Service, Local Service, and Network Service.
08202-0069	Is 'Increase scheduling priority' set to 'Administrators'?		The check passes if 'Increase scheduling priority' is set to Administrators. Fails if: Otherwise.
08202-0070	Is 'Interactive logon: Do not display last user name' set to 'Enabled'?		This check passes if 'Interactive logon: Do not display last user name' is set to Enabled.
08202-0071	Is 'Interactive logon: Do not require CTRL+ALT+DEL' set to 'Disabled'?		This check passes if "Interactive logon: Do not require CTRL+ALT+DEL" is set to Disabled.
08202-0072	Is 'Interactive logon: Machine account lockout threshold' set to greater or equal 4 and less or equal 10 (invalid logon attempts)?		This check passes if 'Interactive logon: Machine account lockout threshold' is set to greater or equal 4 and less or equal 10 invalid logon attempts.
08202-0073	Is 'Interactive logon: Machine inactivity limit' set to less or equal 900 (seconds)?		Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session. The configured state for this setting is: less or equal 900 (seconds).

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0074	Is 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' set to '0' (logon(s))?		This check passes if 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to 0 Logons. Note:-This checks affects the workstations joined to a domain.
08202-0075	Is 'Interactive logon: Prompt user to change password before expiration' set greater and less or equal 10 (days)?		This check passes if 'Interactive logon: Prompt user to change password before expiration' is set between 5 and 10 Days.
08202-0076	Is 'Interactive logon: Smart card removal behavior' set to 'Lock Workstation' or higher?		This check passes if 'Interactive logon: Smart card removal behavior' is set to Lock Workstation or Force Logoff, or Disconnect if a remote Terminal Services session.
08202-0077	Is 'Microsoft network client: Digitally sign communications (always)' set to 'Enabled'?		This check passes if 'Microsoft network client: Digitally sign communications (always)' is set to Enabled.
08202-0078	Is 'Microsoft network client: Digitally sign communications (if server agrees)' set to 'Enabled'?		This check passes if 'Microsoft network client: Digitally sign communications (if server agrees)' is set to Enabled.
08202-0079	Is 'Microsoft network client: Send unencrypted password to third-party SMB servers' set to 'Disabled'.		This check passes if 'Microsoft network client: Send unencrypted password to connect to third-party SMB servers' is set to Disabled.
08202-0080	Is 'Microsoft network server: Amount of idle time required before suspending session' set to greater or equal 1 and less or equal 15 (minutes)?		This check passes if 'Microsoft network server: Amount of idle time required before suspending session' is set to 15 minutes or less.
08202-0081	Is 'Microsoft network server: Digitally sign communications (always)' set to 'Enabled'?		This check passes if 'Microsoft network server: Digitally sign communications (always)' is set to Enabled.
08202-0082	Is 'Microsoft network server: Digitally sign communications (if client agrees)' set to 'Enabled'?		This check passes if 'Microsoft network server: Digitally sign communications (if client agrees)' is set to Enabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0083	Is 'Microsoft network server: Disconnect clients when logon hours expire' set to 'Enabled'?		This check passes if 'Microsoft network server: Disconnect clients when logon hours expire' is set to Enabled.
08202-0084	Is 'Microsoft network server: Server SPN target name validation level' set to 'Required from client'?		This policy setting controls the level of validation a computer with shared folders orprinters (the server) performs on the service principal name (SPN) that is provided by theclient computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis for file and printsharing and other networking operations, such as remote Windows administration. TheSMB protocol supports validating the SMB server service principal name (SPN) within theauthentication blob provided by a SMB client to prevent a class of attacks against SMBservers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. Thissecurity setting determines the level of validation a SMB server performs on the serviceprincipal name (SPN) provided by the SMB client when trying to establish a session to anSMB server.
08202-0085	Is 'Modify an object label' set to 'No One'?		The check passes if 'Modify an object label' is set to None. Fails if: Otherwise.
08202-0086	Is 'Modify firmware environment values' set to 'Administrators'?		This check passes if 'Modify firmware environment values' is set to Administrators.
08202-0087	Is 'Perform volume maintenance tasks' set to 'Administrators'?		The check passes if 'Perform volume maintenance tasks' is set to Administrators Fails if: Otherwise.
08202-0088	Is 'Profile single process' set to 'Administrators'?		This check passes if Profile single process is set to Administrators.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0089	Is 'Profile system performance' set to 'Administrators, NT SERVICE\WdiServic eHost'?		This check passes if 'Profile system performance' is set to Administrators, NT SERVICE\WdiServiceHost.
08202-0090	Is 'Restore files and directories' set to 'Administrators'?		This check passes if Restore files and directories is set to Administrators.
08202-0091	Is 'Shut down the system' set to 'Administrators, Users'?		This check passes if 'Shut down the system' is set to Administrators, Users.
08202-0092	Is 'System objects: Require case insensitivity for non-Windows subsystems' set to 'Enabled'?		This check passes if "System objects: Require case insensitivity for non-Windows subsystems" is set to Enabled.
08202-0093	Is 'System objects: Strengthen default permissions of internal system objects(e.g. Symbolic Links)' set to 'Enabled'?		This check passes if 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to Enabled.
08202-0094	Is 'Take ownership of files or other objects' set to 'Administrators'?		This check passes if 'Take ownership of files or other objects' is set to Administrators.
SYS.02.01.A026 (S) Schutz von Anwendungen			
08202-0095	(Delivery Optimization) Is 'Download Mode' set to 'Disabled'?		Set this policy to configure the use of Windows Update Delivery Optimization in downloads of Windows Apps and Updates. Available mode are: 0=disable 1=peers on same NAT only 2=Local Network / Private Peering (PCs in the same domain by default) 3= Internet Peering The defined state for this setting is: Disabled.
08202-0096	(EMET Setting) 'Default Action and Mitigation Settings' / Is 'Anti Detours' = '1' and 'Banned Functions' = '1' and 'Deep Hooks' = '1' and 'Exploit Action' = '2'?		This setting configures the default action after detection and advanced ROP mitigation. The recommended state for this setting is: Default Action and Mitigation Settings - Enabled Deep Hooks - Enabled Anti Detours - EnabledBanned Functions - Enabled Exploit Action - User Configured

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0097	(EMET Setting) Is 'Address Space Layout Randomization (ASLR)' set to 'Enabled: Application Opt-In'?		This setting determines how applications become enrolled in address space layout randomization (ASLR). The recommended state for this setting is: Enabled: Application Opt-In.
08202-0098	(EMET Setting) Is 'Data Execution Prevention (DEP)' set to 'Enabled: Application Opt-Out'?		This setting determines how applications become enrolled in data execution protection (DEP). The recommended state for this setting is: Enabled: Application Opt-Out.
08202-0099	(EMET Setting) Is 'Structured Exception Handler Overwrite Protection (SEHOP)' set to 'Enabled: Application Opt-Out'?		When a software component suffers from a memory corruption vulnerability, an exploit may be able to overwrite memory that contains data structures that control how the software handles exceptions. By corrupting these structures in a controlled manner, an exploit may be able to execute arbitrary code. SEHOP verifies the integrity of those structures before they are used to handle exceptions, which reduces the reliability of exploits that leverage structured exception handler overwrites.
SYS.02.01.A037 (E) Schutz vor unbefugten Anmeldungen (C, I, A)			
08202-0100	Is "Reset account lockout counter after" set greater or equal 15 (minute(s))?		This check passes if the value for 'Reset account lockout counter after' is set to 15 minutes or more.
08202-0101	Is "Restrict unauthenticated RPC clients' set to 'Enabled'?		The check passes if 'Restrictions for Unauthenticated RPC clients' is set to Enabled:Authenticated. Fails if: Otherwise.
08202-0102	Is 'Account lockout duration' set greater or equal 15 (minute(s))?		This check passes if the value for 'Account lockout duration' is set to 15 minutes or more.
08202-0103	Is 'Account lockout threshold' set greater or equal 1 and less or equal 10 (invalid logon attempt(s))?		• This check passes if the value for 'Account lockout threshold' is set to 10 or fewer.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0104	Is 'Deny access to this computer from the network' set to 'Local account, Guests'?		This check passes if 'Deny access to this computer from the network' is set to at least Guests'and Local Account. Note: Do not deny access to Administrators.
08202-0105	Is 'Deny log on as a batch job' set to "Guests'?		This check passes if Deny Log on as a batch job is set to Guests.
08202-0106	Is 'Deny log on as a service' set to 'Guests'?		This check passes if Deny Log on as a service is set to Guests.
08202-0107	Is 'Deny log on Locally' set to 'Guests'?		This check passes if 'Deny log on Locally' is set to at least Guests, but not Administrators.
08202-0108	Is 'Deny logon through Remote Desktop Services' set to 'Local account, Guests'?		The check passes if Deny logon through Remote Desktop Services is set to Guests, Local Account
SYS.02.02.03.A004 (B) Telemetrie und Datenschutzeinstellungen			
08202-0109	Is 'Allow Telemetry' set to 'Enabled: 0 - Security [Enterprise Only]'?		This check passes if 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]'.
08202-0110	Is 'Do not show feedback notifications' set to 'Enabled'?		This check passes if 'Do not show feedback notifications' is set to 'Enabled'.
08202-0111	Is 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' set to 'Disabled'?		This check passes if 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to'Disabled'.
08202-0112	Is 'Toggle user control over Insider builds' set to 'Disabled'?		This check passes if 'Toggle user control over Insider builds' is set to 'Disabled'.
08202-0113	Is 'Turn off app notifications on the lock screen' set to 'Enabled'?		This check passes if 'Turn off app notifications on the lock screen' is set to 'Enabled'.
08202-0114	Is 'Turn off location' set to 'Enabled'?		This check passes if 'Turn off location' is set to 'Enabled'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0115	Is 'Turn off Microsoft consumer experiences' set to 'Enabled'?		This policy setting turns off experiences that help consumers make the most of their devices and Microsoft account. The recommended state for this setting is: Enabled.
08202-0116	Is 'Turn off the Windows Messenger Customer Experience Improvement Program' set to 'Enabled'?		This check passes if 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to Enabled.
08202-0117	Is 'Turn off Windows Customer Experience Improvement Program' set to 'Enabled'?		This check passes if 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'.
08202-0118	Is 'Turn off Windows Error Reporting' set to 'Enabled'?		This check passes when 'Turn off Windows Error Reporting is set to Enabled.
08202-0119	Is 'Windows Game Recording and Broadcasting' set to 'Disabled'?		This check passes if 'Windows Game Recording and Broadcasting' is set to 'Disabled'.
SYS.02.02.03.A006 (B) Integration von Online-Konten in das Betriebssystem [Benutzer]			

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0120	Is 'Accounts: Block Microsoft accounts' set to 'Enabled: Users can't add or log on with Mocrosoft accounts'?		This policy setting prevents users from adding new Microsoft accounts on this computer.If you select the "Users can't add Microsoft accounts" option, users will not be able to create new Microsoft accounts on this computer, switch a local account to a Microsoft account, or connect a domain account to a Microsoft account. This is the preferred option if you need to limit the use of Microsoft accounts in your enterprise.If you select the "Users can't add or log on with Microsoft accounts" option, existing Microsoft account users will not be able to log on to Windows. Selecting this option might make it impossible for an existing administrator on this computer to log on and manage the system.If you disable or do not configure this policy (recommended), users will be able to use Microsoft accounts with Windows.The recommended state for this setting is: Users can't add or log on with Microsoft accounts.
08202-0121	Is 'Allow Microsoft accounts to be optional' set to 'Enabled'?		This check passes if 'Allow Microsoft accounts to be optional' is set to 'Enabled'.
08202-0122	Is 'Prevent the usage of OneDrive for file storage' set to 'Enabled'?		This check passes if 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'.
08202-0123	Is 'Prevent using Localhost IP address for WebRTC' set to 'Enabled'?		This check passes if 'Don't allow WebRTC to share the LocalHost IP address' is set to 'Enabled'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0124	Was the Client Side Extension for LAPS installed?		In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.
SYS.02.02.03.A007 (A) Lokale Sicherheitsrichtlinien			

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0125	Disable IPv6 / Is Registry-DWORD 'HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\DisabledComponents' set to '0x11 (17)'?		Internet Protocol version 6 (IPv6) is a set of protocols that computers use to exchange information over the Internet and over home and business networks. IPv6 allows for many more IP addresses to be assigned than IPv4 did. Older networking, hosts and operating systems may not support IPv6 natively. The recommended state for this setting is: DisabledComponents - 0xff (255)
08202-0126	Is 'Accounts: Administrator account status' set to 'Disabled'?		This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings. The recommended state for this setting is: Disabled.
08202-0127	Is 'Accounts: Guest account status' set to'Disabled'?		This check passes if 'Accounts: Guest account status' is set to Disabled.
08202-0127	Is 'Accounts: Rename guest account' - 'Value must be not equal to' set to 'Guest, Gast'?		This check passes if the Guest account has been renamed with any value that does not have the term 'Guest' or 'Gast'.
08202-0128	Is 'Accounts: Limit local account use of blank passwords to console logon only' set to 'Enabled'?		This check passes if 'Accounts: Limit local account use of blank passwords to console logon only' is set to Enabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0129	Is 'Accounts: Rename administrator account' - 'Value must not be equal to' set to 'Admin'?		This check passes if the Administrator account has been renamed to a value that does not contain terms 'Administrator' or 'Admin'.
08202-0130	Is 'Accounts: Rename guest account' - 'Value must be not equal to' set to 'Guest, Gast'?		This check passes if the Guest account has been renamed with any value that does not have the term 'Guest' or 'Gast'.
08202-0131	Is 'Allow a Windows app to share application data between users' set to 'Disabled'?		This check passes if 'Allow a Windows app to share application data between users' is set to 'Disabled'.
08202-0132	Is 'Allow indexing of encrypted files' set to 'Disabled'?		This check passes if 'Allow indexing of encrypted files' is set to 'Disabled'.
08202-0133	Is 'Allow InPrivate browsing' set to 'Disabled'?		This check passes if 'Turn off InPrivate browsing' is set to 'Disabled'.
08202-0134	Is 'Allow Input Personalization' set to 'Disabled'?		This check passes if 'Allow Input Personalization' is set to 'Disabled'.
08202-0135	Is 'Allow standby states (S1-S3) when sleeping (on battery)' set to 'Disabled'?		Dictates whether or not Windows is allowed to use standby states when sleeping thecomputer. When this policy is enabled, Windows may use standby states to sleep thecomputer. If this policy is disabled, the only sleep state a computer may enter is hibernate.
08202-0136	Is 'Allow standby states (S1-S3) when sleeping (plugged in)' set to 'Disabled'?		Dictates whether or not Windows is allowed to use standby states when sleeping thecomputer. When this policy is enabled, Windows may use standby states to sleep thecomputer. If this policy is disabled, the only sleep state a computer may enter is hibernate.
08202-0137	Is 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' set to 'Disabled'?		This check passes if 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disabled'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0138	Is 'Always install with elevated privileges' set to 'Disabled'?		This check passes if 'Always install with elevated privileges' is set to 'Disabled'.
08202-0139	Is 'Always prompt for password upon connection' set to 'Enabled'?		This check passes if 'Always prompt for password upon connection' is set to 'Enabled'.
08202-0140	Is 'Boot-Start Driver Initialization Policy' set to 'Enabled: Good only'?		This check passes if 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good only'.
08202-0141	Is 'Configuration of wireless settings using Windows Connect Now' set to 'Disabled'?		This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP) over In-band 802.11 Wi-Fi through the Windows Portable Device API (WPD) and via USB Flash drives. Additional options are available to allow discovery and configuration over a specific medium. The recommended state for this setting is: Disabled.
08202-0142	Is 'Configure offer remote assistance' set to 'Disabled'?		This control defines whether Windows will allow unsolicited offers to provide remoteassistance to the local user. Remote assistance provides the remote party with the abilityto view or control the local system.
08202-0143	Is 'Configure Password Manager' set to 'Disabled'?		This check passes if 'Turn off Password Manager' is set to 'Disabled'.
08202-0144	s 'Configure Pop-up Blocker' set to 'Enabled'?		This check passes if 'Configure Pop-up Blocker' is set to 'Enabled'.
08202-0145	Is 'Configure registry policy processing' set to 'Enabled' and the first additional value = 'Do not apply during periodic background processing' unchecked (False)'?		This check passes if "Registry Policy Processing: Do not apply during periodic background processing" is set to Enabled: FALSE (unchecked)

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0146	Is 'Configure registry policy processing' set to 'Enabled' and the second additional value = 'Process even if the Group Policy objects have not changed' checked (True)?		This check passes if "Registry Policy Processing: Process even if the Group Policy objects have not changed" is set to Enabled: TRUE (checked)
08202-0147	Is 'Configure solicited remote assistance' set to 'Disabled'?		This control defines whether Windows will allow the local user to request a remote partyto view or control their system.
08202-0148	Is 'Disallow Autoplay for non-volume devices' set to 'Enabled'?		This check passes if 'Disallow Autoplay for non-volume devices' is set to 'Enabled'.
08202-0149	Is 'Disallow copying of user input methods to the system account for sign-in' set to 'Enabled'?		This check passes if 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0150	Is 'Do not allow password expiration time longer than required by policy' set to 'Enabled'?		In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled.
08202-0151	Is 'Do not allow passwords to be saved' set to 'Enabled'?		This check passes if 'Do not allow passwords to be saved' is set to 'Enabled'.
08202-0152	Is 'Do not allow supported Plug and Play device redirection' set to 'Enabled'?		This check passes if 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'.
08202-0153	Is 'Do not delete temp folders upon exit' set to 'Disabled'?		This check passes if 'Do not delete temp folders upon exit' is set to 'Disabled'.
08202-0154	Is 'Do not display network selection UI' set to 'Enabled'?		This check passes if 'Do not display network selection UI' is set to 'Enabled'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0155	Is 'Do not enumerate connected users on domainjoined computers' set to 'Enabled'?		This check passes if 'Do not enumerate connected users on domainjoined computers' is set to 'Enabled'.
08202-0156	Is 'Enable insecure guest logons' set to 'Disabled'?		This check passes if 'Enable insecure guest logons' is set to 'Disabled'.
08202-0157	Is 'Enable local admin password management' set to 'Enabled'?		In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled.
08202-0158	Is 'Enable RPC endpoint mapper client authentication' set to 'Enabled'?		If you enable this policy setting, client computers that communicate with this computer areforced to provide authentication before RPC communication can be established. By default,RPC clients do not use authentication to communicate with the RPC Server EndpointMapper Service when they request the endpoint of a server.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0159	Is 'Enable screen saver' set to 'Enabled'?		
08202-0160	Is 'Enable Windows NTP Server' set to 'Disabled'?		This check passes if 'Enable Windows NTP Server' is set to 'Disabled'.
08202-0161	Is 'Enable/Disable PerfTrack' set to 'Disabled'?		This check passes if 'Enable/Disable PerfTrack' is set to 'Disabled'.
08202-0162	Is 'Enforce password history' set greater or equal 24 (password(s))?		This check passes if the value for 'Enforce password history' is set as 24 or more.
08202-0163	Is 'Enumerate local users on domain-joined computers' set to 'Disabled'?		This check passes if 'Enumerate local users on domain-joined computers' is set to 'Disabled'.
08202-0164	Is 'Include command line in process creation events' set to 'Disabled'?		This check passes if 'Include command line in process creation events' is set to 'Disabled'.
08202-0165	Is 'Let Windows apps access account information' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access account information' is set to 'Enabled: Force Deny'.
08202-0166	Is 'Let Windows apps access call history' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access call history' is set to 'Enabled: Force Deny'.
08202-0167	Is 'Let Windows apps access contacts' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access contacts' is set to 'Enabled: Force Deny'.
08202-0168	Is 'Let Windows apps access email' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access email' is set to 'Enabled: Force Deny'.
08202-0169	Is 'Let Windows apps access location' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access location' is set to 'Enabled: Force Deny'?
08202-0170	Is 'Let Windows apps access messaging' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access messaging' is set to 'Enabled: Force Deny'.
08202-0171	Is 'Let Windows apps access motion' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access motion' is set to 'Enabled: Force Deny'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0172	Is 'Let Windows apps access notifications' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access notifications' is set to 'Enabled: Force Deny'.
08202-0173	Is 'Let Windows apps access the calendar' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access the calendar' is set to 'Enabled: Force Deny'.
08202-0174	Is 'Let Windows apps access the camera' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access the camera' is set to 'Enabled: Force Deny'.
08202-0175	Is 'Let Windows apps access the microphone' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access the microphone' is set to 'Enabled: Force Deny'.
08202-0176	Is 'Let Windows apps access trusted devices' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps access trusted devices' set to 'Enabled: Force Deny'.
08202-0177	Is 'Let Windows apps control radios' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps control radios' is set to 'Enabled: Force Deny'.
08202-0178	Is 'Let Windows apps make pone calls' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps make phone calls' is set to 'Enabled: Force Deny'.
08202-0179	Is 'Let Windows apps sync with devices' set to 'Enabled: Force Deny'?		This check passes if 'Let Windows apps sync with devices' is set to 'Enabled: Force Deny'.
08202-0180	Is 'Load and unload device drivers' set to 'Administrators'?		This check passes if 'Load and unload device drivers' is set to Administrators.
08202-0181	Is 'Lock pages in memory' set to 'No One'?		The check passes if 'Lock pages in memory' is set to None. Fails if: Otherwise.
08202-0182	Is 'Log on as a batch job' set to 'Administrators'?		The check passes if Log on as a batch job is set to Administrator

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0183	Is 'Log on as a service' set to 'No One'?		This policy setting allows accounts to launch network services or to register a process as aservice running on the system. This user right should be restricted on any computer in ahigh security environment, but because many applications may require this privilege, itshould be carefully evaluated and tested before configuring it in an enterpriseenvironment. On Windows Vista-based computers, no users or groups have this privilegeby default.When configuring a user right in the SCM enter a comma delimited list of accounts.Accounts can be either local or located in Active Directory, they can be groups, users, orcomputers.The recommended state for this setting is: No One.
08202-0184	Is 'Manage auditing and security log' set to 'Administrators'?		This check passes if 'Manage auditing and security log' is set to Administrator.
08202-0185	Is 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' set to 'Enabled'?		This check passes if 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled'.
08202-0186	Is 'Minimum password age' set greater or equal 1 (day(s))?		This check passes if 'Minimum password age' is set to one or more days.
08202-0187	Is 'Minimum password length' set greater or equal 14 (characters)?		This check passes if the value for 'Minimum password length' is set to 14 or more characters.
08202-0188	Is 'Network access: Allow anonymous SID/Name translation' set to 'Disabled'?		The check passes if 'Network access: Allow anonymous SID/Name translation' is set to Disabled.
08202-0189	Is 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' set to 'Enabled'?		This check passes if 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to Enabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0190	Is 'Network access: Do not allow anonymous enumeration of SAM accounts' set to 'Enabled'?		This check passes if 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to Enabled.
08202-0191	Is 'Network access: Do not allow storage of passwords and credentials for network authentication' set to 'Enabled'?		This policy setting determines whether the Stored User Names and Passwords feature maysave passwords or credentials for later use when it gains domain authentication. If youenable this policy setting, the Stored User Names and Passwords feature of Windows doesnot store passwords and credentials.
08202-0192	Is 'Network access: Let Everyone permissions apply to anonymous users' set to 'Disabled'?		This check passes if 'Network access: Let Everyone permissions apply to anonymous users' is set to Disabled.
08202-0193	Is 'Network access: Named Pipes that can be accessed anonymously' set to None (leave field empty)?		This policy setting determines which communication sessions, or pipes, will have attributesand permissions that allow anonymous access. Note: When you configure this setting youspecify a list of one or more objects. The delimiter used when entering the list is a line feedor carriage return, that is, type the first object on the list, press the Enter button, type thenext object, press Enter again, etc. The setting value is stored as a comma-delimited list ingroup policy security templates. It is also rendered as a comma-delimited list in GroupPolicy Editor's display pane and the Resultant Set of Policy console. It is recorded in theregistry as a line-feed delimited list in a REG_MULTI_SZ value

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0194	Is 'Network access: Remotely accessible registry paths and sub-paths' set to (see description)?		This Check passes if : Network access: Remotely accessible registry paths and sub-paths is 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
08202-0195	Is 'Network access: Remotely accessible registry paths' set to 'System\CurrentControlSet\Control\ ProductOptions, System\CurrentControlSet\Control\S erver Applications, Software\Microsoft\Windows NT\CurrentVersion '?		This Check passes if : 'Network access: Remotely accessible registry paths' is set to System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0196	Is 'Network access: Restrict anonymous access to Named Pipes and Shares' set to 'Enabled'?		When enabled, this policy setting restricts anonymous access to only those shares andpipes that are named in the Network access: Named pipes that can be accessedanonymously and Network access: Shares that can be accessed anonymously settings. Thispolicy setting controls null session access to shares on your computers by addingRestrictNullSessAccess with the value 1 in the HKLM\System\CurrentControlSet\Services\LanMar registry key. This registry valuetoggles null session shares on or off to control whether the server service restrictsunauthenticated clients' access to named resources. Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in yourenvironment.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0197	Is 'Network access: Shares that can be accessed anonymously' set to None (leave field empty)?		This policy setting determines which network shares can be accessed by anonymous users.The default configuration for this policy setting has little effect because all users have to beauthenticated before they can access shared resources on the server. Note: It can be verydangerous to add other shares to this Group Policy setting. Any network user can accessany shares that are listed, which could exposure or corrupt sensitive data. Note: When youconfigure this setting you specify a list of one or more objects. The delimiter used whenentering the list is a line feed or carriage return, that is, type the first object on the list,press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as acomma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policyconsole. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value.
08202-0198	Is 'Network access: Sharing and security model for local accounts' set to 'Classic - local users authenticate as themselves'?		This check passes if 'Network access: Sharing and security model for local accounts' is set to "Classic - local users authenticate as themselves."
08202-0199	Is 'Network security: Allow Local System to use computer identity for NTLM' set to 'Enabled'?		This policy setting allows Local System services that use Negotiate to use the computeridentity when reverting to NTLM authentication. This policy is supported on at leastWindows 7 or Windows Server 2008 R2.
08202-0200	Is 'Network security: Allow LocalSystem NULL session fallback' set to 'Disabled'?		This check passes if "'Network security: Allow LocalSystem NULL session fallback' set to Disabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0201	Is 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' set to 'Disabled'?		This check passes if 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to Disabled.
08202-0202	Is 'Network Security: Configure encryption types allowed for Kerberos' set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'?		This policy setting allows you to set the encryption types that Kerberos is allowed to use.This policy is supported on at least Windows 7 or Windows Server 2008 R2.
08202-0203	Is 'Network security: Do not store LAN Manager hash value on next password change' set to 'Enabled'?		This check passes if 'Network security: Do not store LAN Manager hash value on next password change' is set to Enabled.
08202-0204	Is 'Network security: Force logoff when logon hours expire' set to 'Enabled'?		This check passes if 'Network security: Force logoff when logon hours expire' is set to 'Enabled'.
08202-0205	Is 'Network security: LAN Manager authentication level' set to 'Send NTLMv2 response only. Refuse LM & NTLM'?		This check passes if 'Network security: LAN Manager authentication level' is set to Send NTLMv2 response only\refuse LM &NTLM.
08202-0206	Is 'Network security: LDAP client signing requirements' set to 'Negotiate signing'?		This check passes if 'Network security: LDAP client signing requirements' is set to "Negotiate signing" or "Require Signing".
08202-0207	Is 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' set to 'Require NTLMv2 session security, Require 128-bit encryption'?		This check passes if 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to Require NTLMv2 session security, Require 128-bit encryption.
08202-0208	Is 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' set to 'Require NTLMv2 session security, Require 128-bit encryption'?		This check passes if 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to Require NTLMv2 session security and Require 128-bit encryption.
08202-0209	Is 'Prevent downloading of enclosures' set to 'Enabled'?		This check passes if 'Prevent downloading of enclosures' is set to 'Enabled'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0210	Is 'Prevent enabling lock screen camera' set to 'Enabled'?		This check passes if 'Prevent enabling lock screen camera' is set to 'Enabled'.
08202-0211	Is 'Prevent enabling lock screen slide show' set to 'Enabled'?		This check passes if 'Prevent enabling lock screen slide show' is set to 'Enabled'.
08202-0212	Is 'Prevent installation of devices that match any of these device IDs' set to 'Enabled'?		This check passes if 'Prevent installation of devices that match any of these device IDs' is set to 'Enabled'.
08202-0213	Is 'Prevent installation of devices using drivers that match these device setup classes' set to 'Enabled'?		This check passes if 'Prevent installation of devices using drivers that match these device setup classes' is set to 'Enabled'-
08202-0214	Is 'Prevent Internet Explorer security prompt for Windows Installer scripts' set to 'Disabled'?		This check passes if 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'.
08202-0215	Is 'Prevent the computer from joining a homegroup' set to 'Enabled'?		This check passes if 'Prevent the computer from joining a homegroup' is set to 'Enabled'.
08202-0216	Is 'Prohibit access of the Windows Connect Now wizards' set to 'Enabled'?		This check passes if 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'.
08202-0217	Is 'Prohibit connection to non-domain networks when connected to domain authenticated network' set to 'Enabled'?		This check passes if 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled'.
08202-0218	Is 'Prohibit installation and configuration of Network Bridge on your DNS domain network' set to 'Enabled'?		This check passes if 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'.
08202-0219	Is 'Replace a process level token' set to 'Local Service, Network Service'?		This check passes if 'Replace a process level token' is set to Local Service, Network Service.
08202-0220	Is 'Require a password when a computer wakes (on battery)' set to 'Enabled'?		This check passes if 'Require a Password When a Computer Wakes (On Battery)' is set to Enabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0221	Is 'Require a password when a computer wakes (plugged in)' set to 'Enabled'?		This check passes if 'Require a Password When a Computer Wakes (Plugged In)' is set to Enabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0222	Is 'Require additional authentication at startup' (for operating system drives) set to 'Enabled'?		This policy setting allows you to configure whether BitLocker requires additionalauthentication each time the computer starts and whether you are using BitLocker with orwithout a Trusted Platform Module (TPM). This policy setting is applied when you turn onBitLocker. Note: Only one of the additional authentication options can be required atstartup, otherwise a policy error occurs. If you want to use BitLocker on a computerwithout a TPM, select the Allow BitLocker without a compatible TPM check box. In thismode a USB drive is required for start-up and the key information used to encrypt the driveis stored on the USB drive, creating a USB key. When the USB key is inserted the access tothe drive is authenticated and the drive is accessible. If the USB key is lost or unavailableyou will need to use one of the BitLocker recovery options to access the drive. On acomputer with a compatible TPM, four types of authentication methods can be used atstartup to provide added protection for encrypted data. When the computer starts, it canuse only the TPM for authentication, or it can also require insertion of a USB flash drive containing a startup key, the entry of a 4-digit to 20-digit personal identification number(PIN), or both. If you enable this policy setting, users can configure advanced startupoptions in the BitLocker setup wizard. If you disable or do not configure this policy setting,users can configure only basic options on computers with a TPM. Note: If you want torequire the use of a startup PIN and a USB flash drive, you must configure BitLockersettings using the commandline tool manage-bde instead of the
		112 / 156	BitLocker DriveEncryption setup wizard.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0223	Is 'Require domain users to elevate when setting a network's location' set to 'Enabled'?		This check passes if 'Require domain users to elevate when setting a network's location' is set to 'Enabled'.
08202-0224	Is 'Set the default behavior for AutoRun' set to 'Enabled: Do not execute any autorun commands'?		This check passes if 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'.
08202-0225	Is 'Sign-in last interactive user automatically after a system-initiated restart' set to 'Disabled'?		This check passes if 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled'.
08202-0226	Is 'Store password using reversible encryption' set to 'Disabled'?		This check passes if 'Store password using reversible encryption' is set to Disabled.
08202-0227	Is 'System cryptography: Force strong key protection for user keys stored on the computer' set to 'User is prompted when the key is first used' or 'User must enter a password each time they use a key'?		This check passes if 'System cryptography: Force strong key protection for user keys stored on the computer' is set to "User is prompted when the key is first used" or "User must enter a password each time they use a key".
08202-0229	Is 'Turn off background refresh of Group Policy' set to 'Disabled'?		This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users and domain controllers. The recommended state for this setting is: Disabled.
08202-0230	Is 'Turn off Data Execution Prevention for Explorer' set to 'Disabled'?		Disabling data execution prevention can allow certain legacy plug-in applications to function without terminating Explorer. The recommended state for this setting is: Disabled.
08202-0231	Is 'Turn off downloading of print drivers over HTTP' set to 'Enabled'?		This check passes if 'Turn off downloading of print drivers over HTTP' is set to Enabled.The values prescribed in this section represent the minimum recommended level.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0232	Is 'Turn off handwriting personalization data sharing' set to 'Enabled'?		This check passes if 'Turn off handwriting personalization data sharing' set to 'Enabled'.
08202-0233	Is 'Turn off handwriting recognition error reporting' set to 'Enabled'?		This check passes if 'Turn off handwriting recognition error reporting' is set to 'Enabled'.
08202-0234	Is 'Turn off heap termination on corruption' set to 'Disabled'?		Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this. The recommended state for this setting is: Disabled.
08202-0235	Is 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' set to 'Enabled'?		This check passes if 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'.
08202-0236	Is 'Turn off Internet download for Web publishing and online ordering wizards' set to 'Enabled'?		This check passes if 'Turn off Internet download for Web publishing and online ordering wizards' is set to Enabled.
08202-0237	Is 'Turn off Microsoft Peer-to-Peer Networking Services' set to 'Enabled'?		This check passes if 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'.
08202-0238	Is 'Turn off picture password sign-in' set to 'Enabled'?		This check passes if 'Turn off picture password sign-in' is set to Enabled.
08202-0239	Is 'Turn off printing over HTTP' set to 'Enabled'?		This check passes if 'Turn off printing over HTTP' is set to Enabled.
08202-0240	Is 'Turn off Registration if URL connection is referring to Microsoft.com' set to 'Enabled'?		This check passes if 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled'.
08202-0241	Is 'Turn off Search Companion content file updates' set to 'Enabled'?		This check passes if 'Turn off Search Companion content file updates' is set to Enabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0242	Is 'Turn off shell protocol protected mode' set to 'Disabled'?		This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows. The recommended state for this setting is: Disabled.
08202-0243	Is 'Turn off the 'Order Prints' picture task' set to 'Enabled'?		This check passes if 'Turn off the Order Prints picture task' set to 'Enabled'.
08202-0244	Is 'Turn off the 'Publish to Web' task for files and folders' set to 'Enabled'?		This check passes if "Turn off the 'Publish to Web' task for files and folders" is set to Enabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0245	Is 'Turn on convenience PIN sign-in' set to 'Disabled'?		This policy setting allows you to control whether a domain user can sign in using a convenience PIN. In Windows 10, convenience PIN was replaced with Passport, which has stronger security properties. To configure Passport for domain users, use the policies under Computer configuration\Administrative Templates\Windows Components\Microsoft Passport for Work.If you enable this policy setting, a domain user can set up and sign in with a convenience PIN.If you disable or don't configure this policy setting, a domain user can't set up and use a convenience PIN.Note that the user's domain password will be cached in the system vault when using this feature.The recommended state for this setting is: Disabled.
08202-0246	Is 'Turn on Mapper I/O (LLTDIO) driver' set to 'Disabled'?		This check passes if 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'.
08202-0247	Is 'Turn on Responder (RSPNDR) driver' set to 'Disabled'?		This check passes if 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'.
08202-0248	Is 'Turn on Virtualization Based Security' set to Enabled?		This check passes if 'Turn on Virtualization Based Security' is set to Enabled: Secure Boot and DMA Protectors, Enable Virtualization Based Protection of Code Integrity without Lock and Enable Credential Guard without Lock.
08202-0249	Is 'Untrusted font blocking' set to 'Enabled: Block untrusted fonts and log events'?		This check passes if 'Untrusted Font Blocking' is set to 'Enabled: Block untrusted fonts and log events'.
08202-0250	Is 'Use enhanced anti-spoofing when available' set to 'Enabled'?		This policy setting determines whether enhanced anti-spoofing is configured for devices which support it. The recommended state for this setting is: Enabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0251	Is 'WDigest Authentication' set to 'Enabled'?		This check passes if 'WDigest Authentication' is set to 'Enabled'.
08202-0252	Is 'Windows Firewall: Domain: Apply local connection security rules' set to 'No'?		This check passes if "Windows Firewall: Domain: Apply local connection security rules" is set to No.
08202-0253	Is 'Windows Firewall: Domain: Apply local firewall rules' set to 'No'?		This check passes if"Windows Firewall: Domain: Apply local firewall rules" is set to No.
08202-0254	Is 'Windows Firewall: Domain: Display a notification' set to 'No'?		This check passes if "Windows Firewall: Domain: Display a notification" is set to No.
08202-0255	Is 'Windows Firewall: Domain: Firewall state' set to' On'?		This check passes if 'Windows Firewall: Domain: Firewall state' is set to On.
08202-0256	Is 'Windows Firewall: Domain: Inbound connections' set to 'Enabled: Block'?		This check passes if 'Windows Firewall: Domain: Inbound connections' is set to Block.
08202-0257	Is 'Windows Firewall: Domain: Logging: Log dropped packets' set to 'Yes'?		Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes.
08202-0258	Is 'Windows Firewall: Domain: Logging: Log successful connections' set to 'Yes'?		Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes.
08202-0259	Is 'Windows Firewall: Domain: Logging: Name' set to '%SYSTEMROOT%\Sys tem32\logfiles\firewall\domainfw.l og'?		Use this option to specify the path and name of the file in which Windows Firewall will write its log information.The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0260	Is 'Windows Firewall: Domain: Logging: Size limit (KB)' set to '16,384'?		Use this option to specify the size limit of the file in which Windows Firewall will write its log information.The recommended state for this setting is: 16,384 KB.
08202-0261	Is 'Windows Firewall: Domain: Outbound connections' set to 'Allow'?		This check passes if "Windows Firewall: Domain: Outbound connections" is set to Allow.
08202-0262	Is 'Windows Firewall: Private: Apply local connection security rules' to 'No'?		This check passes when "Windows Firewall: Private: Apply local connection security rules" is set to No.
08202-0263	Is 'Windows Firewall: Private: Apply local firewall rules' set to 'No'?		This check passes if "Windows Firewall: Private: Apply local firewall rules" is set to No.
08202-0264	Is 'Windows Firewall: Private: Display a notification' set to 'No'?		This check passes when "Windows Firewall: Private: Display a notification" is set to No.
08202-0265	Is 'Windows Firewall: Private: Firewall state' set to 'On'?		This check passes if 'Windows Firewall: Private: Firewall state' is set to On.
08202-0266	Is 'Windows Firewall: Private: Inbound connections' set to 'Enabled: Block'?		This check passes if 'Windows Firewall: Private: Inbound connections' is set to Block.
08202-0267	Is 'Windows Firewall: Private: Logging: Log dropped packets' set to 'Yes'?		Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes.
08202-0268	Is 'Windows Firewall: Private: Logging: Log successful connections' set to 'Yes'?		Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0269	Is 'Windows Firewall: Private: Logging: Name' set to '%SYSTEMROOT%\System32\logfiles\fi rewall\privatefw.log'?		Use this option to specify the path and name of the file in which Windows Firewall will write its log information.The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log.
08202-0270	Is 'Windows Firewall: Private: Logging: Size limit (KB)' set to '16,384 KB'?		Use this option to specify the size limit of the file in which Windows Firewall will write its log information.The recommended state for this setting is: 16,384 KB.
08202-0271	Is 'Windows Firewall: Private: Outbound connections' set to 'Allow'?		This check passes if "Windows Firewall: Private: Outbound connections" is set to Allow (default).
08202-0272	Is 'Windows Firewall: Public: Apply local connection security rules' set to 'No'?		This check passes if 'Windows Firewall: Public: Apply local connection security rules' is set to No.
08202-0273	Is 'Windows Firewall: Public: Apply local firewall rules' set to 'No'?		This check passes if 'Windows Firewall: Public: Apply local firewall rules' is set to No.
08202-0274	Is 'Windows Firewall: Public: Display a notification' set to 'Yes'?		This check passes if 'Windows Firewall: Public: Display a notification' is set to Yes.
08202-0275	Is 'Windows Firewall: Public: Firewall state' set to 'On'?		This check passes if 'Windows Firewall: Public: Firewall state' is set to On.
08202-0276	Is 'Windows Firewall: Public: Inbound connections' set to 'Block'?		This check passes if 'Windows Firewall: Public: Inbound connections' is set to Block.
08202-0277	Is 'Windows Firewall: Public: Logging: Log dropped packets' set to 'Yes'?		Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0278	Is 'Windows Firewall: Public: Logging: Log successful connections' set to 'Yes'?		Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes.
08202-0279	Is 'Windows Firewall: Public: Logging: Name' set to '%SYSTEMROOT%\System32\logfiles\fi rewall\publicfw.log'?		Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log.
08202-0280	Is 'Windows Firewall: Public: Logging: Size limit (KB)' set to '16,384'?		Use this option to specify the size limit of the file in which Windows Firewall will write its log information.The recommended state for this setting is: 16,384 KB.
08202-0281	Is 'Windows Firewall: Public: Outbound connections' set to 'Allow'?		This check passes if "Windows Firewall: Public: Outbound connections" is set to Allow.
08202-0282	Is 'Block launching Windows Store apps with Windows Runtime API access from hosted content.' set to 'Enabled'?		This check passes if 'Block launching Windows Store apps with Windows Runtime API access from hosted content.' is set to 'Enabled'.
SYS.02.02.03.A010 (A) Konfiguration zum Schutz von Anwendungen in Windows 10			
08202-0283	Is 'Turn off KMS Client Online AVS Validation' set to 'Enabled'?		This check passes if 'Turn off KMS Client Online AVS Validation' is set to 'Enabled'.
SYS.02.02.03.A011 (A) Schutz der Anmeldeinformationen in Windows 10			
08202-0284	Is 'Do not display the password reveal button' set to 'Enabled'?		This check passes if 'Do not display the password reveal button' is set to 'Enabled'.
08202-0285	Is 'Join Microsoft MAPS' set to 'Enabled: Disabled'?		This check passes if 'Join Microsoft MAPS' is set to 'Enabled: Disabled'.
SYS.02.02.03.A013 (A) Einsatz der SmartScreen-Funktionen			

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0286	Is 'Configure search suggestions in Address bar' set to 'Disabled'?		This check passes if 'Turn off address bar search suggestions' is set to 'Enabled'.
08202-0287	Is 'Configure Windows SmartScreen' set to 'Enabled: Require approval from an administrator before running downloaded unknown software'?		This policy setting allows you to manage the behavior of Windows SmartScreen. Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled. The recommended state for this setting is: Enabled: Require approval from an administrator before running downloaded unknown software.
08202-0288	Is 'Don't allow SmartScreen Filter warning overrides for unverified files' set to 'Enabled'?		This check passes if 'Don't allow SmartScreen Filter warning overrides for unverified files' is set to 'Enabled'.
08202-0289	Is 'Don't allow SmartScreen Filter warning overrides' set to 'Enabled'?		This check passes if 'Don't allow SmartScreen Filter warning overrides' is set to 'Enabled'.
08202-0290	Is 'Prevent managing SmartScreen Filter' (Internet Explorer) set to 'Enabled: On'?		This check passes if 'Prevent managing SmartScreen Filter' (Internet Explorer) is set to 'Enabled: On'.
08202-0291	Is 'Prevent managing SmartScreen Filter' (Microsoft Edge) set to 'Enabled: On'?		This check passes if 'Prevent managing SmartScreen Filter' (Microsoft Edge) is set to 'Enabled: On'.
08202-0292	Is 'Turn on SmartScreen Filter scan' set to 'Enabled'?		This check passes if 'Turn on SmartScreen Filter scan' is set to 'Enabled: Enable'.
SYS.02.02.03.A014 (A) Einsatz des Sprachassistenten Cortana [Benutzer]			
08202-0293	Is 'Allow Cortana' set to 'Disabled'?		This check passes if 'Allow Cortana' is set to 'Disabled'.
08202-0294	Is 'Allow search and Cortana to use location' set to 'Disabled'?		This check passes if 'Allow search and Cortana to use location' is set to 'Disabled'.
SYS.02.02.03.A016 (A) Anbindung von Windows 10 an den Windows Store			

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0295	Is 'Disable all apps from Windows Store' set to 'Enabled'?		This check passes if 'Disable all apps from Windows Store' is set to 'Enabled'.
08202-0296	Is 'Disable pre-release features or settings' set to 'Disabled'?		This check passes if 'Disable pre-release features or settings' is set to 'Disabled'.
08202-0297	Is 'Turn off access to the Store' set to 'Enabled'?		This check passes if 'Turn off access to the Store' is set to 'Enabled'.
08202-0298	Is 'Turn off Automatic Download and Install of updates' set to 'Enabled'?		This check passes if 'Turn off Automatic Download and Install of updates' is set to 'Ensabled'.
08202-0299	Is 'Turn off the offer to update to the latest version of Windows' set to 'Enabled'?		This check passes if 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'.
08202-0300	Is 'Turn off the Store application' set to 'Enabled'?		This check passes if 'Turn off the Store application' is set to 'Enabled'.
SYS.02.02.03.A019 (A) Verwendung des Fernzugriffs über RDP [Benutzer]			
08202-0301	Is 'Allow Basic authentication (Client)' set to 'Disabled'?		This check passes if 'Allow Basic authentication (Client)' is set to 'Disabled'.
08202-0302	Is 'Allow unencrypted traffic (Client)'set to 'Disabled'?		This check passes if 'Allow unencrypted traffic (Client)' is set to 'Disabled'.
08202-0303	Is 'Allow log on through Remote Desktop Services' set to 'Remote Desktop Users'?		The check passes if Allow logon through Terminal Services is set to Remote Desktop Users (S-1-5-32-555)
08202-0304	Is 'Allow Remote Shell Access' set to 'Disabled'?		This check passes if 'Allow Remote Shell Access' set to 'Disabled'.
08202-0305	Is 'Allow unencrypted traffic (Client)'set to 'Disabled'?		This check passes if 'Allow unencrypted traffic (Client)' is set to 'Disabled'.
08202-0306	Is 'Allow users to connect remotely by using Remote Desktop Services' set to 'Disabled'?		This check passes if 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled'.
08202-0307	Is 'Disallow Digest authentication (Client)'set to 'Enabled'?		This check passes if 'Disallow Digest authentication (Client)' is set to 'Enabled'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0308	Is 'Allow Basic authentication (Server)'set to 'Disabled'?		This check passes if 'Allow Basic authentication (Server)' is set to 'Disabled'.
08202-0308	Is 'Disallow WinRM from storing RunAs credentials (Server)' set to 'Enabled'?		This check passes if 'Disallow WinRM from storing RunAs credentials (Server)' is set to 'Enabled'.
08202-0309	Is 'Do not allow COM port redirection' set to 'Enabled'?		This check passes if 'Do not allow COM port redirection' is set to 'Enabled'.
08202-0310	Is 'Do not allow drive redirection' set to 'Enabled'?		This control defines whether a user is allowed to share the local drives on their clientcomputers to Terminal Servers that they access
08202-0311	Is 'Do not allow LPT port redirection' set to 'Enabled'?		This check passes if 'Do not allow LPT port redirection' is set to 'Enabled'.
08202-0312	Is 'Do not use temporary folders per session' set to 'Disabled'?		This check passes if 'Do not use temporary folders per session' is set to 'Disabled'.
SYS.02.02.03.A020 (A) Einsatz der Benutzerkontensteuerung für privilegierte Konten			
08202-0313	Is 'Apply UAC restrictions to local accounts on network logons' set to 'Enabled'?		This check passes if 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'.
08202-0314	Is 'User Account Control: Admin Approval Mode for the Built-in Administrator account' set to 'Enabled'?		This check passes if 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to Enabled.
08202-0315	Is 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' set to 'Disabled'?		This check passes if 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to Disabled.
08202-0316	Is 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'?		This check passes if 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to "Prompt for consent on the secure desktop"'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0317	Is 'User Account Control: Behavior of the elevation prompt for standard users' set to 'Automatically deny elevation requests'?		This check passes if 'User Account Control: Behavior of the elevation prompt for standard users' is set to "Automatically deny elevation requests".
08202-0318	Is 'User Account Control: Detect application installations and prompt for elevation' set to 'Enabled'?		This check passes if 'User Account Control: Detect application installations and prompt for elevation' is set to Enabled.
08202-0319	Is 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' set to 'Enabled'?		This check passes if 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to Enabled.
08202-0320	Is 'User Account Control: Run all administrators in Admin Approval Mode' set to 'Enabled'?		This check passes if 'User Account Control: Run all administrators in Admin Approval Mode' is set to Enabled.
08202-0321	Is 'User Account Control: Switch to the secure desktop when prompting for elevation' set to 'Enabled'?		This check passes if 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to Enabled.
08202-0322	Is 'User Account Control: Virtualize file and registry write failures to per-user locations' set to 'Enabled'?		This check passes if 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to Enabled.
SYS.02.02.03.A021 (A) Einsatz des Encrypting File Systems EFS (C, I)			

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0323	Is 'Allow access to BitLocker-protect ed fixed data drives from earlier versions of Windows' set to 'Disabled'?		This policy setting configures whether or not fixed data drives formatted with the FAT filesystem can be unlocked and viewed on computers running Windows Server 2008,Windows Vista, Windows XP with Service Pack 3 (SP3), or Windows XP with Service Pack 2(SP2) operating systems. If this policy setting is enabled or not configured, fixed data drivesformatted with the FAT file system can be unlocked on computers running Windows Server2008, Windows Vista, Windows XP with SP3, or Windows XP with SP2, and their contentcan be viewed. These operating systems have read-only access to BitLocker-protecteddrives. When this policy setting is enabled, select the Do not install BitLocker To Go Readeron FAT formatted fixed drives check box to help prevent users from running BitLocker ToGo Reader from their fixed drives. If BitLocker To Go Reader (bitlockertogo.exe) is presenton a drive that does not have an identification field specified, or if the drive has the sameidentification field as specified in the Provide unique identifiers for your organizationpolicy setting, the user will be prompted to update BitLocker and BitLocker To Go Readerwill be deleted from the drive. In this situation, for the fixed drive to be unlocked oncomputers running Windows Server 2008, Windows Vista, Windows XP with SP3, orWindows XP with SP2, BitLocker To Go Reader must be installed on the computer. If thischeck box is not selected, BitLocker To Go Reader will be installed on the fixed drive toenable users to unlock the drive on computers running Windows Server 2008, WindowsVista, Windows XP with SP3, or Windows XP with SP2
		125 / 156	that do not have BitLocker To Go-Reader installed. If this policy set-

Check	Prüfaspekt	Prüfparameter	Bewertung

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0324	Is 'Allow access to BitLocker-protect ed removable data drives from earlier versions of Windows' set to 'Disabled'?		This policy setting configures whether or not removable data drives formatted with theFAT file system can be unlocked and viewed on computers running Windows Server 2008,Windows Vista, Windows XP with Service Pack 3 (SP3), or Windows XP with Service Pack 2(SP2) operating systems. If this policy setting is enabled or not configured, removable datadrives formatted with the FAT file system can be unlocked on computers running WindowsServer 2008, Windows Vista, Windows XP with SP3, or Windows XP with SP2, and theircontent can be viewed. These operating systems have read-only access to BitLockerprotecteddrives. When this policy setting is enabled, select the Do not install BitLocker ToGo Reader on FAT formatted removable drives check box to help prevent users from running BitLocker To Go Reader from their removable drives. If BitLocker To Go Reader(bitlockertogo.exe) is present on a drive that does not have an identification field specified,or if the drive has the same identification field as specified in the Provide unique identifiersfor your organization policy setting, the user will be prompted to update BitLocker andBitLocker To Go Reader will be deleted from the drive. In this situation, for the removabledrive to be unlocked on computers running Windows Server 2008, Windows Vista,Windows XP with SP3, or Windows XP with SP2, BitLocker To Go Reader must be installedon the computer. If this check box is not selected, BitLocker To Go Reader will be installedon the removable drive to enable users to unlock the drive on computers running WindowsServer 2008, Windows Vista, Windows
		127 / 156	XP with SP3, or Windows XP with SP2 that do nothave BitLocker To

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0325	Is 'Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)' for fixed data drives set to 'Enabled: XTS-AES 256-bit'?		This policy setting allows you to configure the algorithm and cipher strength used by BitLocker Drive Encryption. This policy setting is applied when you turn on BitLocker. Changing the encryption method has no effect if the drive is already encrypted or if encryption is in progress. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about the encryption methods available. The recommended state for this setting is Enabled:XTS-AES 256-bit (for operating system drives) XTS-AES 256-bit (for fixed data drives) AES-CBC 256-bit (for removable data drives)
08202-0326	Is 'Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)' for operating system drives set to 'Enabled: XTS-AES 256-bit'?		This policy setting allows you to configure the algorithm and cipher strength used by BitLocker Drive Encryption. This policy setting is applied when you turn on BitLocker. Changing the encryption method has no effect if the drive is already encrypted or if encryption is in progress. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about the encryption methods available. The recommended state for this setting is Enabled:XTS-AES 256-bit (for operating system drives) XTS-AES 256-bit (for fixed data drives) AES-CBC 256-bit (for removable data drives)

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0327	Is 'Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)' for removable data drives set to 'Enabled: XTS-AES 256-bit'?		This policy setting allows you to configure the algorithm and cipher strength used by BitLocker Drive Encryption. This policy setting is applied when you turn on BitLocker. Changing the encryption method has no effect if the drive is already encrypted or if encryption is in progress. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about the encryption methods available. The recommended state for this setting is Enabled:XTS-AES 256-bit (for operating system drives) XTS-AES 256-bit (for fixed data drives) AES-CBC 256-bit (for removable data drives)
08202-0328	Is 'Choose how BitLocker-protect ed fixed drives can be recovered' set to'Enabled'?		This check passes if the setting "Choose how BitLocker-protected fixed drives can be recovered" is enabled.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0329	Is 'Choose how BitLocker-protect ed operating system drives can be recovered' set to 'Enabled'?		This policy setting allows you to control how BitLocker-protected operating system drivesare recovered in the absence of the required startup key information. This policy setting isapplied when you turn on BitLocker. The Allow certificate-based data recovery agent checkbox is used to specify whether a data recovery agent can be used with BitLocker-protectedoperating system drives. Before a data recovery agent can be used it must be added fromthe Public Key Policies item in either the Group Policy Management Console or the LocalGroup Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide onMicrosoft TechNet for more information about adding data recovery agents. In Configureuser storage of BitLocker recovery information select whether users are allowed, required,or not allowed to generate a 48-digit recovery password or a 256-bit recovery key. SelectOmit recovery options from the BitLocker setup wizard to prevent users from specifyingrecovery options when they enable BitLocker on a drive. This means that you will not beable to specify which recovery option to use when you enable BitLocker, instead BitLockerrecovery options for the drive are determined by the policy setting. In Save BitLockerrecovery information to Active Directory Domain Services, choose which BitLockerrecovery information to store in AD DS for operating system drives. If you select Backuprecovery password and key package, both the BitLocker recovery password and keypackage are stored in AD DS. Storing the key package supports recovering
		130 / 156	data from a drivethat has been physically corrupted. If you select

Check	Prüfaspekt	Prüfparameter	Bewertung

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0330	Is 'Choose how BitLocker-protect ed removable drives can be recovered' set to 'Enabled'?		This policy setting allows you to control how BitLocker-protected removable data drivesare recovered in the absence of the required credentials. This policy setting is applied whenyou turn on BitLocker. The Allow data recovery agent check box is used to specify whethera data recovery agent can be used with BitLocker-protected removable data drives. Beforea data recovery agent can be used it must be added from the Public Key Policies item ineither the Group Policy Management Console or the Local Group Policy Editor. Consult theBitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more informationabout adding data recovery agents. In Configure user storage of BitLocker recoveryinformation select whether users are allowed, required, or not allowed to generate a 48-digit recovery password or a 256-bit recovery key. Select Omit recovery options from theBitLocker setup wizard to prevent users from specifying recovery options when theyenable BitLocker on a drive. This means that you will not be able to specify which recoveryoption to use when you enable BitLocker, instead BitLocker recovery options for the driveare determined by the policy setting. In Save BitLocker recovery information to ActiveDirectory Domain Services choose which BitLocker recovery information to store in AD DSfor removable data drives. If you select Backup recovery password and key package, boththe BitLocker recovery password and key package are stored in AD DS. If you select Backuprecovery password only the recovery password is stored in AD DS. Select the Do not enableBit-
		132 / 156	Locker until recovery information is stored in AD DS for removable data

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0331	Is 'Configure minimum PIN length for startup' (for Operating System Drives) set to 'Enabled' and 'Minimum characters' to'10'?		This policy setting allows you to configure a minimum length for a Trusted PlatformModule (TPM) startup PIN. This policy setting is applied when you turn on BitLocker. Thestartup PIN must have a minimum length of 4 digits and can have a maximum length of 20digits. If you enable this policy setting, you can require a minimum number of digits to beused when setting the startup PIN. If you disable or do not configure this policy setting,users can configure a startup PIN of any length between 4 and 20 digits.
08202-0332	Is 'Configure use of hardware-based encryption for fixed data drives' set to 'Enabled'?		This check passes if 'Configure use of hardware-based encryption for fixed data drives' is set to 'Enabled'.
08202-0333	Is 'Configure use of hardware-based encryption for operating system drives' set to 'Enabled'?		This check passes if 'Configure use of hardware-based encryption for operating system drives' is set to 'Enabled'.
08202-0334	Is 'Configure use of hardware-based encryption for removable data drives' set to 'Enabled'?		This check passes if 'Configure use of hardware-based encryption for removable data drives' is set to 'Enabled'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0335	Is 'Configure use of passwords for fixed data drives' set to 'Disabled'?		This policy setting specifies whether a password is required to unlock BitLocker-protectedfixed data drives. If you choose to permit the use of a password, you can require that apassword be used, enforce complexity requirements on the password, and configure aminimum length for the password. For the complexity requirement setting to be effectivethe Group Policy setting Password must meet complexity requirements located inComputer Configuration\Windows Settings\Security Settings\Account Policies\PasswordPolicy\ must be also enabled. Note: These settings are enforced when turning on BitLocker,not when unlocking a volume. BitLocker will allow unlocking a drive with any of theprotectors available on the drive. If you enable this policy setting, users can configure apassword that meets the requirements you define. To require the use of a password, selectRequire password for fixed data drive. To enforce complexity requirements on thepassword, select Require complexity. When set to Require complexity a connection to adomain controller is necessary when BitLocker is enabled to validate the complexity thepassword. When set to Allow complexity a connection to a domain controller will beattempted to validate the complexity adheres to the rules set by the policy, but if no domaincontrollers are found the password will still be accepted regardless of actual passwordcomplexity and the drive will be encrypted using that password as a protector. When set to Do not allow complexity, no password complexity validation will be done. Passwords mustbe at least
		134 / 156	8 characters. To configure a greater minimum length for the password,

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0336	Is 'Configure use of passwords for operating system drives' set to 'Disabled'?		This check passes if 'Configure use of passwords for operating system drives' is set to 'Disabled'.
08202-0337	Is 'Configure use of passwords for removable data drives' set to 'Disabled'?		This policy setting allows you to specify whether smart cards can be used to authenticateuser access to BitLocker-protected removable data drives on a computer. If you enable thispolicy setting smart cards can be used to authenticate user access to the drive. You canrequire a smart card authentication by selecting the Require use of smart cards onremovable data drives check box. Note: These settings are enforced when turning onBitLocker, not when unlocking a drive. BitLocker will allow unlocking a drive with any ofthe protectors available on the drive. If you disable this policy setting, users are not allowedto use smart cards to authenticate their access to BitLocker-protected removable datadrives. If you do not configure this policy setting, smart cards are available to authenticateuser access to a BitLocker-protected removable data drive.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0338	Is 'Configure use of smart cards on fixed data drives' set to 'Enabled'?		This policy setting allows you to specify whether smart cards can be used to authenticateuser access to the BitLocker-protected fixed data drives on a computer. If you enable thispolicy setting smart cards can be used to authenticate user access to the drive. You canrequire a smart card authentication by selecting the Require use of smart cards on fixed-data drives check box. Note: These settings are enforced when turning on BitLocker, notwhen unlocking a drive. BitLocker will allow unlocking a drive with any of the protectorsavailable on the drive. If you disable this policy setting, users are not allowed to use smartcards to authenticate their access to BitLocker-protected fixed data drives. If you do not configure this policy setting, smart cards can be used to authenticate user access to aBitLocker-protected drive.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0339	Is 'Configure use of smart cards on removable data drives' set to 'Enabled'?		This policy setting specifies whether a password is required to unlock BitLocker-protectedremovable data drives. If you choose to allow use of a password, you can require apassword to be used, enforce complexity requirements, and configure a minimum length.For the complexity requirement setting to be effective the Group Policy setting Password-must meet complexity requirements located in Computer Configuration\WindowsSettings\Security Settings\Account Policies\Password Policy\ must be also enabled. Note:These settings are enforced when turning on BitLocker, not when unlocking a volume.BitLocker will allow unlocking a drive with any of the protectors available on the drive. Ifyou enable this policy setting, users can configure a password that meets the requirementsthat you define. To require the use of a password, select Require password for removabledata drive. To enforce complexity requirements on the password, select Require-complexity. When set to Require complexity a connection to a domain controller isnecessary when BitLocker is enabled to validate the complexity the password. When set toAllow complexity a connection to a domain controller will be attempted to validate thecomplexity adheres to the rules set by the policy, but if no domain controllers are found thepassword will still be accepted regardless of actual password complexity and the drive willbe encrypted using that password as a protector. When set to Do not allow complexity, nopassword complexity validation will be done. Passwords must be at least 8 characters. Toconfigure a greater minimum
		137 / 156	length for the password, enter the desired number ofcharacters in

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0340	Is 'Deny write access to removable drives not protected by BitLocker' set to 'Enabled'?		This policy setting configures whether BitLocker protection is required for a computer tobe able to write data to a removable data drive. If you enable this policy setting, allremovable data drives that are not BitLocker-protected will be mounted as read-only. If thedrive is protected by BitLocker, it will be mounted with read and write access. If the Denywrite access to devices configured in another organization option is selected, only driveswith identification fields matching the computer's identification fields will be given writeaccess. When a removable data drive is accessed it will be checked for valid identificationfield and allowed identification fields. These fields are defined by the Provide the uniqueidentifiers for your organization policy setting. If you disable or do not configure this policysetting, all removable data drives on the computer will be mounted with read and writeaccess.
08202-0341	Is the Enhanced Mitigation Experience Toolkit (EMET) V5.5 or higher installed?		The Enhanced Mitigation Experience Toolkit (EMET) is free, supported, software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0342	Is the fifth additional value of 'Choose how BitLocker-protected fixed drives can be recovered' = 'Save BitLocker recovery information to AD DSS for fixed data drives' unchecked (False)?		In Save BitLocker recovery information to Active Directory Doman Services choose whichBitLocker recovery information to store in AD DS for fixed data drives. If you select Backuprecovery password and key package, both the BitLocker recovery password and keypackage are stored in AD DS. Storing the key package supports recovering data from a drivethat has been physically corrupted. If you select Backup recovery password only, only therecovery password is stored in AD DS.
08202-0343	Is the fifth additional value of 'Choose how BitLocker-protected operating system drives can be recovered' = 'Save BitLocker recovery information to AD DS for operating system drives' checked (Enabled)?		In Save BitLocker recovery information to Active Directory Domain Services, choose whichBitLocker recovery information to store in AD DS for operating system drives. If you selectBackup recovery password and key package, both the BitLocker recovery password andkey package are stored in AD DS. Storing the key package supports recovering data from adrive that has been physically corrupted. If you select Backup recovery password only, onlythe recovery password is stored in AD DS.
08202-0344	Is the ffifth additional value of 'Choose how BitLocker-protected removable drives can be recovered' = 'Save BitLocker recovery information to AD DS for removable data drives' unchecked (False)?		In Save BitLocker recovery information to Active Directory Domain Services choose whichBitLocker recovery information to store in AD DS for removable data drives. If you selectBackup recovery password and key package, both the BitLocker recovery password andkey package are stored in AD DS. If you select Backup recovery password only the recoverypassword is stored in AD DS.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0345	Is the fifth additional value of 'Require additional authentication at startup' = 'Configure TPM startup key and PIN:' set to 'Do not allow startup key and PIN with TPM'?		On a computer with a compatible TPM, four types of authentication methods can be used atstartup to provide added protection for encrypted data. When the computer starts, it canuse only the TPM for authentication, or it can also require insertion of a USB flash drivecontaining a startup key, the entry of a 4-digit to 20-digit personal identification number(PIN), or both.
08202-0346	Is the first additional value of 'Choose how BitLocker-protected fixed drives can be recovered' = 'Allow data recovery agent' checked (True)?		This policy setting allows you to control how BitLocker-protected fixed data drives are recovered in the absence of the required credentials. This policy setting is applied when you turn on BitLocker.The "Allow data recovery agent" check box is used to specify whether a data recovery agent can be used with BitLocker-protected fixed data drives. Before a data recovery agent can be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more information about adding data recovery agents.
08202-0347	Is the first additional value of 'Choose how BitLocker-protected operating system drives' = 'Allow data recovery agent' unchecked (False)?		The Allow certificate-based data recovery agent check box is used to specify whether a datarecovery agent can be used with BitLocker-protected operating system drives. Before adata recovery agent can be used it must be added from the Public Key Policies item ineither the Group Policy Management Console or the Local Group Policy Editor. Consult theBitLocker Drive Encryption Deployment Guide on Microsoft TechNet for more informationabout adding data recovery agents.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0348	Is the first additional value of 'Choose how BitLocker-protected removable drives can be recovered' = 'Allow data recovery agent' checked (True)?		The Allow data recovery agent check box is used to specify whether a data recovery agentcan be used with BitLocker-protected removable data drives. Before a data recovery agentcan be used it must be added from the Public Key Policies item in either the Group Policy Management Console or the Local Group Policy Editor. Consult the BitLocker DriveEncryption Deployment Guide on Microsoft TechNet for more information about addingdata recovery agents.
08202-0349	Is the first additional value of 'Configure use of hardware-based encryption for fixed data drives' = 'Use BitLocker software-based encryption when hardware encryption is not available' checked (True)?		This check passes if 'Configure use of hardware-based encryption for fixed data drives: Use BitLocker software-based encryption when hardware encryption is not available' is set to 'Enabled: True'.
08202-0350	Is the first additional value of 'Configure use of hardware-based encryption for operating system drives' = 'Use BitLocker software-based encryption when hardware encryption is not available' checked (True)?		This check passes if 'Configure use of hardware-based encryption for operating system drives: Use BitLocker software-based encryption when hardware encryption is not available' is set to 'Enabled: True'.
08202-0351	Is the first additional value of 'Configure use of hardware-based encryption for removable data drives' = 'Use BitLocker software-based encryption when hardware encryption is not available' checked (True)?		This check passes if 'Configure use of hardware-based encryption for removable data drives: Use BitLocker software-based encryption when hardware encryption is not available' is set to 'Enabled: True'.
08202-0352	Is the first additional value of 'Configure use of smart cards on fixed data drives' = 'Require use of smart cards on fixed data drives' checked (True)?		This check passes if 'Configure use of smart cards on fixed data drives: Require use of smart cards on fixed data drives' is set to 'Enabled: True'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0353	Is the first additional value of 'Configure use of smart cards on removable data drives' ='Require use of smart cards on removable data drives' checked (True)?		This check passes if 'Configure use of smart cards on fixed data drives: Require use of smart cards on fixed data drives' is set to 'Enabled: True'.
08202-0354	Is the first additional value of 'Deny write access to removable drives not protected by BitLocker' = 'Do not allow write access to devices configured in another organization' checked (True)?		This policy setting configures whether BitLocker protection is required for a computer to be able to write data to a removable data drive. If you enable this policy setting, all removable data drives that are not BitLocker-protected will be mounted as read-only. If the drive is protected by BitLocker, it will be mounted with read and write access. If the "Deny write access to devices configured in another organization" option is selected, only drives with identification fields matching the computer's identification fields will be given write access. When a removable data drive is accessed it will be checked for valid identification field and allowed identification fields. These fields are defined by the "Provide the unique identifiers for your organization" policy setting. If you disable or do not configure this policy setting, all removable data drives on the computer will be mounted with read and write access. The recommended state for this setting is: Enabled: False (unchecked).

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0355	Is the first additional value of 'Password Settings' = 'Password Complexity' set to 'Large letters + small letters + numbers + specials'?		In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: Large letters + small letters + numbers + special characters.
08202-0356	Is the first additional value of 'Prevent installation of devices that match any of these device IDs' set to 'PCI\CC_0C0A'?		This check passes if 'Prevent installation of devices that match any of these device IDs: Prevent installation of devices that match any of these device IDs' is set to 'PCI\CC_0C0A'.
08202-0357	Is 'the first additional value of 'Prevent installation of devices using drivers that match these device setup classes' set to '\d48179be-ec20-1 1d1-b6b8-00c04fa3 72a7\'?		This check passes if 'Prevent installation of devices using drivers that match these device setup classes: Prevent installation of devices using drivers for these device setup' is set to '\d48179be-ec20-11d1-b6b8-00c04fa372a7\'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0358	Is the first additional value of 'Require additional authentication at startup' = 'Allow BitLocker without a compatible TPM' unchecked (False)?		This check passes if 'Require additional authentication at startup: Allow BitLocker without a compatible TPM' is set to 'Enabled: False'.
08202-0359	Is the fourth additional value of 'Choose how BitLocker-protected fixed drives can be recovered' ='Omit recovery options from the BitLocker setup wizard' checked (True)?		Select Omit recovery options from the BitLocker setup wizard to prevent users fromspecifying recovery options when they enable BitLocker on a drive. This means that youwill not be able to specify which recovery option to use when you enable BitLocker, insteadBitLocker recovery options for the drive are determined by the policy setting.
08202-0360	Is the fourth additional value of 'Choose how BitLocker-protected operating system drives can be recovered' = 'Omit recovery options from the BitLocker setup wizard' checked (True)?		Select Omit recovery options from the BitLocker setup wizard to prevent users fromspecifying recovery options when they enable BitLocker on a drive. This means that youwill not be able to specify which recovery option to use when you enable BitLocker, insteadBitLocker recovery options for the drive are determined by the policy setting.
08202-0361	Is the fourth additional value of 'Choose how BitLocker-protected removable drives can be recovered' = 'Omit recovery options from the BitLocker setup wizard' checked (True)?		Select Omit recovery options from the BitLocker setup wizard to prevent users fromspecifying recovery options when they enable BitLocker on a drive. This means that youwill not be able to specify which recovery option to use when you enable BitLocker, insteadBitLocker recovery options for the drive are determined by the policy setting.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0362	Is the fourth additional value of 'Require additional authentication at startup' = 'Configure TPM startup key:' set to 'Do not allow startup key with TPM'?		On a computer with a compatible TPM, four types of authentication methods can be used atstartup to provide added protection for encrypted data. When the computer starts, it canuse only the TPM for authentication, or it can also require insertion of a USB flash drivecontaining a startup key, the entry of a 4-digit to 20-digit personal identification number(PIN), or both.
08202-0363	Is the second additional value of 'Choose how BitLocker-protected fixed drives can be recovered' = 'Recovery password' set to 'Allow 48-digit recovery password'?		In Configure user storage of BitLocker recovery information select whether users areallowed, required, or not allowed to generate a 48-digit recovery password or a 256-bitrecovery key
08202-0364	Is the second additional value of 'Choose how BitLocker-protected operating system drives' = 'Configure user storage of BitLocker recovery information / Unnamed value 1' set to 'Require 48-digit recovery password'?		In Configure user storage of BitLocker recovery information select whether users areallowed, required, or not allowed to generate a 48-digit recovery password or a 256-bitrecovery key.
08202-0365	Is the second additional value of 'Choose how BitLocker-protected removable drives can be recovered' = 'Recovery password' set to 'Do not allow 48-digit recovery password'?		In Configure user storage of BitLocker recovery information select whether users areallowed, required, or not allowed to generate a 48-digit recovery password or a 256-bitrecovery key
08202-0366	Is the second additional value of 'Configure use of hardware-based encryption for fixed data drives' = Restrict encryption algorithms and cipher suites allowed for hardware-based encryption' unchecked (False)?		This check passes if 'Configure use of hardware-based encryption for fixed data drives: Restrict encryption algorithms and cipher suites allowed for hardware-based encryption' is set to 'Disabled: False'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0367	Is the second additional value of 'Configure use of hardware-based encryption for operating system drives' = 'Restrict encryption algorithms and cipher suites allowed for hardware-based encryption' unchecked (False)?		This check passes if 'Configure use of hardware-based encryption for operating system drives: Restrict encryption algorithms and cipher suites allowed for hardware-based encryption' is set to 'Enabled: False'.
08202-0368	Is the second additional value of 'Configure use of hardware-based encryption for removable data drives' = 'Restrict encryption algorithms and cipher suites allowed for hardware-based encryption' unchecked (False)?		This check passes if 'Configure use of hardware-based encryption for removable data drives: Restrict encryption algorithms and cipher suites allowed for hardware-based encryption' is set to 'Enabled: False'.
08202-0369	Is the second additional value of 'Password Settings' = 'Password Length' set to greater or equal 15 (characters)?		This check passes if 'Password Settings: Password Length' is set to Enabled:15 or more.
08202-0370	Is the second additional value of 'Prevent installation of devices that match any of these device IDs' = 'Also apply to matching devices that are already installed.' checked (True)?		This policy setting allows you to specify a list of Plug and Play hardware IDs and compatible IDs for devices that Windows is prevented from installing. This policy setting takes precedence over any other policy setting that allows Windows to install a device. If you enable this policy setting, Windows is prevented from installing a device whose hardware ID or compatible ID appears in the list you create. If you enable this policy setting on a remote desktop server, the policy setting affects redirection of the specified devices from a remote desktop client to the remote desktop server. If you disable or do not configure this policy setting, devices can be installed and updated as allowed or prevented by other policy settings. The recommended state for this setting is: True (checked).

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0371	Is the second additional value of 'Prevent installation of devices using drivers that match these device setup classes' = 'Also apply to matching devices that are already installed.' checked (True)?		This check passes if 'Prevent installation of devices using drivers that match these device setup classes: Also apply to matching devices that are already installed.' is set to 'True' (checked).
08202-0372	Is the second additional value of 'Require additional authentication at startup:' = 'Configure TPM startup' set to 'Do not allow TPM'?		On a computer with a compatible TPM, four types of authentication methods can be used atstartup to provide added protection for encrypted data. When the computer starts, it canuse only the TPM for authentication, or it can also require insertion of a USB flash drivecontaining a startup key, the entry of a 4-digit to 20-digit personal identification number(PIN), or both.
08202-0373	Is the seven additional value of 'Choose how BitLocker-protected removable drives can be recovered' = 'Do not enable BitLocker until recovery information is stored to AD DS for removable data drives' unchecked (False)?		Select the Do not enable BitLocker until recovery information is stored in AD DS for removable data drives check box if you want to prevent users from enabling BitLockerunless the computer is connected to the domain and the backup of BitLocker recoveryinformation to AD DS succeeds.
08202-0374	Is the seventh additional value of 'Choose how BitLocker-protected operating system drives can be recovered' = 'Do not enable BitLocker until recovery information is stored to AD DS for operating system drives' checked (Enabled)?		Select the Do not enable BitLocker until recovery information is stored in AD DS foroperating system drives check box if you want to prevent users from enabling BitLockerunless the computer is connected to the domain and the backup of BitLocker recoveryinformation to AD DS succeeds.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0375	Is the sixth additional value of 'Choose how BitLocker-protected drives can be recovered' = 'Configure storage of BitLocker recovery information to AD DS:' set to 'Backup recovery passwords and key packages'?		In Save BitLocker recovery information to Active Directory Doman Services choose whichBitLocker recovery information to store in AD DS for fixed data drives. If you select Backuprecovery password and key package, both the BitLocker recovery password and keypackage are stored in AD DS. Storing the key package supports recovering data from a drivethat has been physically corrupted. If you select Backup recovery password only, only therecovery password is stored in AD DS.
08202-0376	Is the sixth additional value of 'Choose how BitLocker-protected operating system drives can be recovered' = 'Configure storage of BitLocker recovery information to AD DS:' set to 'Store recovery passwords and key packages'?		In Save BitLocker recovery information to Active Directory Domain Services, choose whichBitLocker recovery information to store in AD DS for operating system drives. If you selectBackup recovery password and key package, both the BitLocker recovery password andkey package are stored in AD DS. Storing the key package supports recovering data from adrive that has been physically corrupted. If you select Backup recovery password only, onlythe recovery password is stored in AD DS.
08202-0377	Is the sixth additional value of 'Choose how BitLocker-protected removable drives can be recovered' = 'Configure storage of BitLocker recovery information to AD DS' set to 'Backup recovery passwords and key packages'?		In Save BitLocker recovery information to Active Directory Domain Services choose whichBitLocker recovery information to store in AD DS for removable data drives. If you selectBackup recovery password and key package, both the BitLocker recovery password andkey package are stored in AD DS. If you select Backup recovery password only the recoverypassword is stored in AD DS.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0378	Is the third additional value of 'Choose how BitLocker-protected drives can be recovered' = 'Recovery key' set to 'Allow 256-bit recovery key'?		In Configure user storage of BitLocker recovery information select whether users areallowed, required, or not allowed to generate a 48-digit recovery password or a 256-bitrecovery key.
08202-0379	Is the third additional value of 'Choose how BitLocker-protected operating system drives' = 'Configure user storage of BitLocker recovery information / Unnamed value 2' set to 'Do not allow 256-bit recovery key'?		In Configure user storage of BitLocker recovery information select whether users areallowed, required, or not allowed to generate a 48-digit recovery password or a 256-bitrecovery key.
08202-0380	Is the third additional value of 'Choose how BitLocker-protected removable drives can be recovered' = 'Recovery key' set to 'Do not allow 256-bit recovery key'?		In Configure user storage of BitLocker recovery information select whether users areallowed, required, or not allowed to generate a 48-digit recovery password or a 256-bitrecovery key.
08202-0381	Is the third additional value of 'Configure use of hardware-based encryption for fixed data drives' = 'Restrict crypto algorithms or cipher suites to the following' set to '2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42'?		This check passes if 'Configure use of hardware-based encryption for fixed data drives: Restrict crypto algorithms or cipher suites to the following:' is set to '2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42'.
08202-0382	Is the third additional value of 'Configure use of hardware-based encryption for operating system drives' = 'Restrict crypto algorithms or cipher suites to the following:' set to '2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42'?		This check passes if 'Configure use of hardware-based encryption for operating system drives: Restrict crypto algorithms or cipher suites to the following:' is set to '2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42'.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0383	Is the third additional value of 'Configure use of hardware-based encryption for removable data drives' = 'Restrict crypto algorithms or cipher suites to the following' set to '2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42'?		This check passes if 'Configure use of hardware-based encryption for removable data drives: Restrict crypto algorithms or cipher suites to the following:' is set to '2.16.840.1.101.3.4.1.2;2.16.840.1.101.3.4.1.42'.
08202-0384	Is the third additional value of 'Password Settings' = 'Password Age (Days)' set to less or equal 42?		In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The defined state for this setting is: Enabled: 42 or fewer.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0385	Is the third additional value of 'Require additional authentication at startup' = 'Configure TPM startup PIN:' set to 'Require startup PIN with TPM'?		On a computer with a compatible TPM, four types of authentication methods can be used atstartup to provide added protection for encrypted data. When the computer starts, it canuse only the TPM for authentication, or it can also require insertion of a USB flash drivecontaining a startup key, the entry of a 4-digit to 20-digit personal identification number(PIN), or both.
SYS.02.02.03.A022 (A) Windows PowerShell (WPS) (C, I, A)			
08202-0386	Is 'Turn on PowerShell Transcription' set to 'Disabled'?		This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.The recommended state for this setting is: Disabled.
08202-0387	Is 'Turn on PowerShell Script Block Logging' set to 'Enabled'?		This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log.
SYS.02.02.03.A023 (A) Erweiterter Schutz der Anmeldeinformationen in Windows 10 (C, I)			
08202-0388	Is 'Require secure RPC communication' set to 'Enabled'?		This check passes if 'Require secure RPC communication' is set to 'Enabled'.
08202-0389	Is 'Set client connection encryption level' set to 'Enabled: High Level'?		This check passes if 'Set client connection encryption level' is set to Enabled - High Level. This check is applicable only if the following prerequisites are satisfied: * If the 'Allow users to connect remotely using Terminal Services' policy is not disabled. * If Remote Desktop is allowed on the computer.

Check	Prüfaspekt	Prüfparameter	Bewertung
08202-0390	Is 'Set time limit for active but idle Remote Desktop Services sessions' set to 'Enabled: 5 minutes'?		This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected.
08202-0391	Is 'Set time limit for disconnected sessions' set to 'Enabled: 1 minute'?		This check passes if 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' .

Tabelle 5: ***Technische Prüfungen***

4 Risikoanalyse und -behandlung

Der folgende Abschnitt enthält eine generische Risikoanalyse und -behandlung für das SiM "Client unter Windows 10". Es umfasst die Betrachtung für normalen und hohen Schutzbedarf in den drei Schutzzielen Verfügbarkeit, Vertraulichkeit und Integrität. Die Risikoanalyse wurde dabei im Wesentlichen nach den Vorgaben des BSI-Standards 100-3, abstrahiert für die gesamte Klasse der durch das SiM modellierbaren Zielobjekte, durchgeführt.

Für die Erstellung dieses Abschnittes wurden die elementaren Gefährdungen des BSI-Gefährdungskataloges G 0 auf ihre Anwendbarkeit für die durch das SiM modellierbare Zielobjekte hin untersucht. Wie vom BSI empfohlen, wird eine elementare Gefährdung genau dann als anwendbar betrachtet, wenn sie durch eine direkte Einwirkung auf das Zielobjekt prinzipiell zu einem nennenswerten Schaden führen können. Das Ergebnis dieser Prüfung ist in der im Abschnitt 4.1 enthaltenen Kreuzreferenztabelle dokumentiert. Lichtblau unterlegte Spalten, kennzeichnen Maßnahmen, die erst ab einem hohen Schutzbedarf umzusetzen sind.

Aufbauend auf diese Prüfung erfolgte die eigentliche Risikobewertung und -behandlung. Die Tabelle in Abschnitt 4.2 dokumentiert die Ergebnisse dieser Arbeit. Sie enthält nur die anzuwendenden Gefährdungen. In den folgenden drei Spalten ist markiert, für welches der drei Schutzziele (Grundwerte) die Gefährdung relevant ist (entsprechend der Bewertung des BSI). Spalte 6 bezeichnet die Schutzbedarfskategorien, bei der die Gefährdung relevant ist. Der Wertebereich dieser Spalte umfasst die Werte "normal", "hoch" sowie "normal + hoch".

Die Spalte Bewertung enthält die Gefährdungsbewertungen im Kontext der Grundschutz-Maßnahmen. Spalte 8 beschreibt mit den Werten "ja" oder "nein" kurz, ob die angeführten Maßnahmen grundsätzlich eine angemessene Risikobehandlung darstellen. Soweit dies verneint wird, kennzeichnet Spalte 9 eine von vier Risikobehandlungsvarianten ("A" = "Risiko-Reduktion", "B" = "Risikovermeidung", "C" = "Risikoübernahme" und "D" = "Risiko-Transfer"). In Spalte 10 (Erläuterung Behandlung) wird die angegebene Risikobehandlungsvariante erläutert; insbesondere wird im Fall der Risikoreduktion (Variante „A“) an dieser Stelle dargelegt, wie das Risiko durch Z-Maßnahmen und benutzerdefinierte Maßnahmen auf ein akzeptables Niveau gemindert werden.

Die Spalte 11 erläutert die Konsolidierung der zur Risikoreduktion verwendeten Sicherheitsmaßnahmen mit den Grundschutzmaßnahmen anhand der im BSI-Standard 100-3 empfohlenen Kriterien "Eignung", "Zusammenwirken mit anderen Maßnahmen", "Benutzerfreundlichkeit" und "Angemessenheit". Das Konsolidierungsergebnis bzgl. dieser Aspekte ist in den letzten 4 Spalten noch einmal aus Übersichtlichkeitsgründen zusammengefasst.

4.1 Kreuzreferenztabelle

Es sind keine Einzelrisiken definiert.

4.2 Risikobetrachtung und -behandlung

Dieses Sicherheitsmodul besitzt noch keine Risikobetrachtungen.

Tabellenverzeichnis