EMPFEHLUNG: IT IN UNTERNEHMEN

Sichere Konfiguration von Microsoft Office

für den Einsatz auf dem Betriebssystem Microsoft Windows

Büroanwendungen gehören in vielen Organisationen zu den am häufigsten genutzten Anwendungsprogrammen. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen. Wegen ihrer großen Verbreitung und Angriffsfläche werden diese auch häufig als Angriffsweg genutzt, beispielsweise um mittels Makros in Office-Dokumenten Schadsoftware zu verbreiten und auf Zielsystemen auszuführen. Mit einer wohlüberlegten Konfiguration dieser Produkte kann das Risiko der Ausnutzung von Standardfunktionen oder Schwachstellen minimiert werden.

Ziel

Hauptaugenmerk dieser Empfehlung liegt auf dem Einsatz von Microsoft Office in mittelgroßen bis großen Organisationen, in denen die Endsysteme mit Gruppenrichtlinien in einer Active Directory-Umgebung verwaltet werden. Alternativ können diese auch als lokale Sicherheitsrichtlinien angewendet werden. **Die Empfehlungen beziehen sich auf die Versionen 2021 und 2024 von Microsoft Office.** Bei Einsatz einer anderen Version lassen sich die Empfehlungen grundsätzlich für Entscheidungen zu einer Konfiguration unter Berücksichtigung möglicher Abweichungen ebenfalls heranziehen und anwenden.

Bei den vorliegenden Computer- und Benutzerrichtlinien handelt es sich um Richtlinien von Microsoft Office, die sicherheitsrelevant sind. Weitere Einstellungen finden sich in den BSI-Veröffentlichungen:

- ✔ Sichere Konfiguration von Microsoft Access
- ✔ Sichere Konfiguration von Microsoft Excel
- ✔ Sichere Konfiguration von Microsoft Outlook
- ✔ Sichere Konfiguration von Microsoft PowerPoint
- ✔ Sichere Konfiguration von Microsoft Visio
- ✔ Sichere Konfiguration von Microsoft Word

Sicherheitsprinzipien

Bei vielen Anwendungsprodukten ist die Konfiguration häufig ein Kompromiss aus Sicherheit und Funktionalität. Je mehr die Sicherheit in den Fokus gerückt wird, desto mehr wird die Anwendungsfunktionalität damit eingeschränkt. Administrierende stehen immer vor der Herausforderung, hier die Balance zu finden und sollten die Konfiguration der Produkte und der benötigten Funktionalität

von dem benötigten Schutzbedarf der verarbeiteten Informationen abhängig machen.

Für die Bereitstellung einer sicheren Standardanwendungsfunktionalität ist es demnach nicht einfach, organisationsübergreifende Empfehlungen zur Verfügung zu stellen, die in unterschiedlichen Anwendungsszenarien zum Einsatz kommen, sowie unterschiedliche Schutzbedürfnisse haben. Die Empfehlungen wurden daher anhand einer Reihe von Grundannahmen entwickelt, die im Folgenden kurz dargestellt werden:

- Für Benutzende soll die Anzahl wichtiger Sicherheitsentscheidungen minimiert werden.
- Die benötigte Anwendungsfunktionalität soll nicht wesentlich beeinträchtigt werden.
- Nicht benötigte Funktionen sollen deaktiviert werden, um die Angriffsfläche zu verringern.
- Fokus auf Angriffsszenarien, die nach aktuellem Kenntnisstand auch ausgenutzt werden.
- Erhöhung des Datenschutzes, indem soweit wie möglich die Übertragungen von – für die Funktionalität nicht benötigte – Informationen an den Hersteller unterbunden wird.
- Erhöhung des Datenschutzes, indem externe Cloud-Dienste vermieden werden.

Voraussetzungen

Die Sicherheit aller Microsoft Office-Produkte stützt sich auf die Sicherheit der Einsatzumgebung. Es wird daher vorausgesetzt, dass bereits

- entsprechende Richtlinien und bewährte Methoden zum Schutz der Organisationsinfrastruktur entwickelt wurden,
- aktuell branchenübliche Sicherheitstechniken eingesetzt werden sowie
- die im BSI-Grundschutz enthaltenen Empfehlungen und bewährten Methoden implementiert wurden.

Gruppenrichtlinien

Im Folgenden werden die empfohlenen sicherheitsrelevanten Computerrichtlinien sowie Benutzerrichtlinien von Desktop- und Laptopcomputern aufgelistet. Diese können nur in Abhängigkeit von den Bedürfnissen innerhalb der Organisation umgesetzt werden. Wurde eine Active Directory-Umgebung innerhalb der gesamten Organisation bereitgestellt, auf denen die Office-Version ausgeführt wird, können diese über eine Gruppenrichtlinie zentral verwaltet werden. Da die Beschreibungen der jeweiligen Richtlinien im Editor für Gruppenrichtlinien zu finden sind, wird auf eine Darstellung im Dokument verzichtet.

Richtlinien sind von Microsoft standardmäßig auf „Nicht konfiguriert“ voreingestellt. Je nach Richtlinie kann das entweder einer aktivierten oder deaktivierten Einstellung entsprechen. In einigen wenigen Fällen hat eine nicht konfigurierte Einstellung eine eigene Bedeutung. Darüber hinaus kann „Nicht konfiguriert“ bedeuten, dass dem Nutzenden die Einstellung im Office-Programm selbst überlassen wird.

Da es prinzipiell möglich ist, dass sich durch Updates die Bedeutung von „Nicht konfiguriert“ ändert, sollten alle Richtlinien durch den Administrierenden immer auf „Aktiviert“ (☑) oder „Deaktiviert“ (☒) und nur im Ausnahmefall auf „Nicht konfiguriert“ (☐) gesetzt werden. Rot markierte Einstellungen kennzeichnen, dass die BSI-Empfehlungen von der durch Microsoft festgelegten Bedeutung von „Nicht konfiguriert“ abweichen. Sollte bei Aktivierung der Richtlinie eine Auswahl oder Eingabe notwendig sein, befindet sich diese im Falle einer konkreten Empfehlung in der Fußnote.

Computerrichtlinien

Aktualisierungen *Updates*

1.	**Automatische Updates aktivieren** *Enable Automatic Updates*	☑
2.	**Aktualisierungspfad** *Update Path*	☑[1]
3.	**Option zum Aktivieren oder Deaktivieren von Updates ausblenden** *Hide option to enable or disable updates*	☑
4.	**Upgrade von Office 2019 auf Microsoft 365 Apps for Enterprise** *Upgrade Office 2019 to Microsoft 365 Apps for enterprise*	☒

Sicherheitseinstellungen *Security Settings*		
5.	**Grafikfilterimport** *Graphics filter import*	☒
6.	**VBA für Office-Anwendungen deaktivieren** *Disable VBA for Office applications*	☑
7.	**Paketreparatur deaktivieren** *Disable Package Repair*	☒

Sicherheitseinstellungen\IE-Sicherheit *Security Settings\IE Security*		
8.	**ActiveX-Installation einschränken** *Restrict ActiveX Install*	☑
9.	**Dateidownload einschränken** *Restrict File Download*	☑
10.	**Add-On-Verwaltung** *Add-on Management*	☑
11.	**Sperrung der Zone des lokalen Computers** *Local Machine Zone Lockdown Security*	☑
12.	**Konsistente MIME-Verarbeitung** *Consistent Mime Handling*	☑
13.	**Sicherheitsfeature für MIME-Ermittlung** *Mime Sniffing Safety Feature*	☑
14.	**Objektzwischenspeicherungsschutz** *Object Caching Protection*	☑
15.	**Sicherheitseinschränkungen für Skriptfenster** *Skripted Window Security Restrictions*	☑
16.	**Schutz vor Zonenanhebung** *Protection from Zone Elevation*	☑
17.	**Informationsleiste** *Information Bar*	☑
18.	**Benutzername und Kennwort deaktivieren** *Disable user name and password*	☑
19.	**Binden an Objekt** *Bind to objekt*	☑
20.	**Gespeichert von URL** *Saved from URL*	☑

1 Pfad zum Speicherort

21.	**URL navigieren** *Navigate URL*	☑
22.	**Popups blockieren** *Block popups*	☒

Benutzerrichtlinien

Dokumentinformationsbereich *Document Information Panel*		
23.	**Dokumenteninformationsbereich für Signal übertragende Elemente der Benutzeroberfläche** *Document Information Panel Beaconing UI*	☑[2]
24.	**Dokumenteninformationsbereich deaktivieren** *Disable Document Information Panel*	☑

Add-Ins Microsoft „Speichern als PDF“ und „Speichern als XPS“ *Microsoft Save As PDF and XPS add-ins*		
25.	**Einschließen von Dokumenteigenschaften in PDF- und XPS-Ausgabe deaktivieren** *Disable inclusion of document properties in PDF and XPS output*	☑

Eingeschränkte Berechtigungen verwalten *Manage Restricted Permissions*		
26.	**Benutzer können Berechtigungen für Inhalte, deren Rechte verwaltet werden, nicht ändern** *Prevent users from changing permissions on rights managed content*	☒
27.	**Benutzer mit früheren Versionen von Office können mit Browsern lesen...** *Allow users with earlier versions of Office to read with browsers...*	☒
28.	**Benutzer müssen zum Überprüfen der Berechtigung immer eine Verbindung herstellen** *Always require users to connect to verify permission*	☒
29.	**Gruppen in Office immer erweitern, wenn die Berechtigung für Dokumente eingeschränkt wird** *Always expand groups in Office when restricting permission for documents*	☑
30.	**Benutzer können nie Gruppen angeben, wenn die Berechtigung für Dokumente eingeschränkt wird** *Never allow users to specify groups when restricting permission for documents*	☑
31.	**Berechtigungsrichtlinien-Standardserver für Symbolleiste für den Schnellzugriff angeben** *Specify Permission Policy Default Server for Quick Access Toolbar*	☑[3]

Telemetriedashboard *Telemetry Dashboard*		
32.	**Telemetrie-Datensammlung aktivieren** *Turn on telemetry data collection*	☒
33.	**Datenschutzeinstellungen im Office-Telemetrie-Agent aktivieren** *Turn on privacy settings in Office Telemetry Agent*	☑
34.	**Hochladen von Daten für den Office-Telemetrie-Agent** *Turn on data uploading for Office Telemetry Agent*	☒

2 Benutzeroberfläche immer anzeigen
3 Lokale IP-Adresse, z.B. 127.0.0.1

Smart Document's (Word, Excel) *Smart Documents (Word, Excel)*		
35.	**Manifestverwendung durch Smart Document's deaktivieren** *Disable Smart Document's use of manifests*	☑

Signieren *Signing*		
36.	**Office-Signaturanbieter unterdrücken** *Suppress Office Signing Providers*	☑[4]
37.	**Menüelement für externe Signaturdienste unterdrücken** *Suppress external signatures services menu item*	☑
38.	**Vorversions-Formatsignaturen** *Legacy format signatures*	☒
39.	**EKU-Filterung** *EKU filtering*	☒

Servereinstellungen *Server Settings*		
40.	**Abrufen veröffentlichter Hyperlinks von SharePoint Server durch den Office-Client deaktivieren** *Disable the Office client from polling the SharePoint Server for published links*	☑

Verschiedenes *Miscellaneous*		
41.	**OneDrive-Anmeldung anzeigen** *Show OneDrive Sign In*	☒
42.	**Screenshots nicht automatisch mit einem Link versehen** *Do not automatically hyperlink screenshots*	☑
43.	**Anmeldung bei Office blockieren** *Block signing into Office*	☑[5]
44.	**Steuerelementbloggen** *Control Blogging*	☑[6]
45.	**Cloudbasierte Microsoft-Dateispeicherorte in der Backstage-Ansicht ausblenden** *Hide Microsoft cloud-based file locations in the Backstage view*	☑[7]

Globale Optionen\Benutzerdefiniert *Global Options\Customize*		
46.	**Alle Benutzeranpassungen deaktivieren** *Turn off all user customizations*	☑
47.	**Benutzeroberflächenerweiterung von Dokumenten und Vorlagen deaktivieren** *Disable UI extending from documents and templates*	☑

4 Westlich und Ostasiatisch aktivieren
5 Keine zulässig
6 Deaktiviert
7 3

Online präsentieren *Present Online*		
48.	**Office-Präsentationsdienst aus der Liste der Onlinepräsentationsdienste in PowerPoint und Word entfernen** *Remove Office Presentation Service from the list of online presentation services in PowerPoint and Word*	☑
49.	**Einschränken des programmgesteuerten Zugriffs für das Erstellen von Onlinepräsentationen in PowerPoint und Word** *Restrict programmatic access for creating online presentations in PowerPoint and Word*	☑
50.	**Verhindern, dass Benutzer Onlinepräsentationsdienste in PowerPoint und Word hinzufügen können** *Prevent users from adding online presentation services in PowerPoint and Word*	☑

Online präsentieren\Präsentationsdienste *Present Online\Presentation Services*		
51.	**Präsentationsdienst in PowerPoint und Word konfigurieren #1 bis #10** *Configure presentation service in PowerPoint and Word #1 to #10*	☒

Datenschutz\Trust Center *Privacy\Trust Center*		
52.	**Bestätigungs-Assistenten bei der ersten Ausführung deaktivieren** *Disable Opt-in Wizard on first run*	☑
53.	**Automatisches Empfangen kleiner Updates zur Verbesserung der Zuverlässigkeit** *Automatically receive small updates to improve reliability*	☒
54.	**Programm zur Verbesserung der Benutzerfreundlichkeit aktivieren** *Enable Customer Experience Improvement Program*	☒
55.	**Die Verwendung verbundener Erfahrungen in Office zulassen** *Allow the use of connected experiences in Office*	☒
56.	**Die Verwendung verbundener Erfahrungen, die Inhalt analysieren, in Office zulassen** *Allow the use of connected experiences in Office that analyze content*	☒
57.	**Die Verwendung verbundener Erfahrungen, die Onlineinhalte herunterladen, in Office zulassen** *Allow the use of connected experiences in Office that download online content*	☒
58.	**Die Verwendung zusätzlicher optionaler verbundener Erfahrungen in Office zulassen** *Allow the use of additional optional connected experiences in Office*	☒
59.	**Stufe der von Office an Microsoft gesendeten Clientsoftware-Diagnosedaten konfigurieren** *Configure the level of client software diagnostic data sent by Office to Microsoft*	☑[8]
60.	**Persönliche Informationen senden** *Send personal information*	☒

Dienste *Services*		
61.	**Office-Roamingbenutzereinstellungen deaktivieren** *Disable Roaming Office User Settings*	☑

8 Weder noch

Dienste\Fax *Services\Fax*		
62.	**Internetfaxfeature deaktivieren** *Disable Internet Fax feature*	☑

Extras|Optionen|Allgemein|Dienstoptionen\Onlineinhalte *Tools | Options | General | Service Options...\Online Content*		
63.	**Onlineinhalteoptionen** *Online Content Options*	☑[9]

Extras|Optionen|Allgemein|Weboptionen\Dateien *Tools | Options | General | Web Options...\Files*		
64.	**Office-Dokumente beim Browsen mit Lese-/Schreibzugriff senden** *Open Office documents as read/write while browsing*	☒

Extras|Optionen|Rechtschreibung\Rechtschreibprüfung für Datensammlung *Tools | Options | Spelling\Proofing Data Collection*		
65.	**Korrekturhilfen verbessern** *Improve Proofing Tools*	☒

Sicherheitseinstellungen *Security Settings*		
66.	**Benutzeroberfläche für PDF-Verschlüsselungseinstellung deaktivieren** *Turn off PDF encryption setting UI*	☒
67.	**OLE-Objekte überprüfen** *Check OLE objects*	☑[10]
68.	**Excel-RTD-Server überprüfen** *Check Excel RTD servers*	☒
69.	**Verschlüsselungstyp für kennwortgeschützte Office Open XML-Dateien** *Encryption type for password protected Office Open XML files*	☑[11]
70.	**Mindestlänge für Kennwort festlegen** *Set minimum password length*	☑
71.	**Automatisierungssicherheit** *Automation Security*	☑[12]
72.	**Alle ActiveX-Steuerelemente deaktivieren** *Disable all ActiveX*	☑
73.	**Kennwort zum Öffnen der Benutzeroberfläche deaktivieren** *Disable password to open UI*	☒
74.	**Dokumentmetadaten für kennwortgeschützte Dateien schützen** *Protect document metadata for password protected files*	☑
75.	**OWC-Datenquellenanbieter überprüfen** *Check OWC data source providers*	☑

9 Für Office keine Internetverbindungen zulassen
10 IE-Killbitliste außer Kraft setzen
11 Microsoft Enhanced RSA und AES Cryptographic Provider, AES-256, 256-Bit
12 Makros standardmäßig deaktivieren

76.	**Verschlüsselungstyp für kennwortgeschützte Office 97-2003-Dateien** *Encryption type for password protected Office 97-2003 files*	☑[13]
77.	**Linkwarnungen unterdrücken** *Suppress hyperlink warnings*	☒
78.	**ActiveX-Objekte überprüfen** *Check ActiveX objects*	☑[14]
79.	**Fehlerberichterstattung für Dateien mit Dateiüberprüfungsfehlern deaktivieren** *Turn off error reporting for files that fail file validation*	☑
80.	**Dokumenteigenschaften verschlüsseln** *Encrypt document properties*	☑
81.	**Dokumentmetadaten für Office Open XML-Dateien, deren Rechte verwaltet werden, schützen** *Protect document metadata for rights managed Office Open XML Files*	☑
82.	**VBA für Office-Anwendungen deaktivieren** *Disable VBA for Office applications*	☑
83.	**Steuerelemente in Forms3 laden** *Load Controls in Forms3*	☑[15]
84.	**In Word und Excel können keine verwalteten Codeerweiterungen geladen werden** *Prevent Word and Excel from loading managed code extensions*	☑
85.	**Regelstufe für Kennwort festlegen** *Set password rules level*	☑[16]
86.	**ActiveX-Steuerelementinitialisierung** *ActiveX Control Initialization*	☑[17]
87.	**Kennworthashformat als ISO-kompatibel festlegen** *Set password hash format as ISO-compliant*	☑
88.	**Domänentimeout für Kennwortregeln festlegen** *Set password rules domain timeout*	☑[18]
89.	**Alle Benachrichtigungen für Vertrauensstellungsleiste aus Sicherheitsgründen deaktivieren** *Disable all Trust Bar notifications for security issues*	☒
90.	**Zulassen, dass VBA Typbibliotheksverweise über Pfade von nicht vertrauenswürdigen Intranet-Speicherorten lädt** *Allow VBA to load typelib references by path from untrusted intranet locations*	☒
91.	**Zusätzliche Sicherheitsüberprüfungen von VBA-Bibliotheksverweisen deaktivieren, die möglicherweise auf unsichere Speicherorte auf dem lokalen Computer verweisen** *Disable additional security checks on VBA library references that may refer to unsafe locations on the local machine*	☒
92.	**Anpassungen von VSTO 2003 und 2005 auf Dokumentebene deaktivieren** *Disable VSTO 2003 and 2005 document-level customizations*	☒
93.	**Minimierung des Ungültigmachens von digitalen VBA-Projektsignaturen aktivieren** *Enable Minimizing VBA Project Digital Signature Invalidation*	☒
94.	**Liste mit 3D -Modelldateiformaten deaktivieren** *Disable 3D Model File Format List*	☒

13 Microsoft Enhanced RSA und AES Cryptographic Provider, AES-256, 256-Bit
14 IE-Killbitliste außer Kraft setzen
15 1
16 Prüfung der lokalen Länge und lokalen Komplexität und Domänenrichtlinienprüfungen
17 4
18 4.000

Sicherheitseinstellungen\Digitale Signaturen *Security Settings\Digital Signatures*		
95.	**OCSP zum Signaturgenerierungs-Zeitpunkt anfordern** *Require OCSP at signature generation time*	☑
96.	**XadES-Mindesstufe für digitale Signaturgenerierung angeben** *Specify minimum XadES level for digital signature generation*	☑[19]
97.	**XadES-Teile einer digitalen Signatur überprüfen** *Check the XadES portions of a digital signature*	☑
98.	**Beim Überprüfen von Signaturen keine abgelaufenen Zertifikate zulassen** *Do not allow expired certificates when validating signatures*	☑
99.	**Hashalgorithmus für digitale Signatur auswählen** *Select digital signature hashing algorithm*	☑[20]
100.	**Zeitstempel-Hashalgorithmus konfigurieren** *Configure time stamping hashing algorithm*	☑[21]
101.	**Vorversions-Hashalgorithmus konfigurieren** *Configure legacy hashing algorithm*	☑[22]
102.	**Ungültigen Hashalgorithmus konfigurieren** *Configure invalid hashing algorithm*	☑[23]
103.	**Mindestgröße für öffentlichen RSA-Schlüssel konfigurieren** *Configure minimum RSA public key size*	☑[24]
104.	**Größe für öffentlichen RSA-Vorversionsschlüssel konfigurieren** *Configure legacy RSA public key size*	☑[25]
105.	**Größe für ungültigen öffentlichen RSA-Schlüssel konfigurieren** *Configure invalid RSA public key size*	☑[26]
106.	**Mindestgröße für öffentlichen DSA-Schlüssel konfigurieren** *Configure minimum DSA public key size*	☑[27]
107.	**Größe für öffentlichen DSA-Vorversionsschlüssel konfigurieren** *Configure legacy DSA public key size*	☑[28]
108.	**Größe für ungültigen öffentlichen DSA-Schlüssel konfigurieren** *Configure invalid DSA public key size*	☑[29]
109.	**Zertifikatausstellerfilter angeben** *Specify filtering for certificate issuers*	☑
110.	**Namen des Zeitstempelservers angeben** *Specify timestamp server name*	☑
111.	**Timeout für Zeitstempelserver angeben** *Set timestamp server timeout*	☑[30]
112.	**Signaturüberprüfungsstufe festlegen** *Set signature verification level*	☑[31]

19 Keine Mindeststufe
20 SHA512
21 SHA512
22 SHA1
23 SHA1
24 1024
25 512
26 512
27 1024
28 1024
29 512
30 5
31 Office 2013-Regeln

113.	**Erforderliche XadES-Stufe für Signaturgenerierung** *Requested XadES level for signature generation*	☑[32]
114.	**Alternative Zertifikatsanbieter anzeigen** *Display alternative certificate providers*	☒

Sicherheitseinstellungen\Hinterlegte Zertifikate *Security Settings\Escrow Certificates*		
115.	**Hinterlegter Schlüssel #1 bis #20** *Escrow Key #1 to #20*	☒

Sicherheitseinstellungen\Trust Center *Security Settings\Trust Center*		
116.	**Vertrauenswürdiger Speicherort #1 bis #20** *Trusted Locations #1 to #20*	☒
117.	**Mischung aus Richtlinien- und Benutzerspeicherorten zulassen** *Allow mix of policy and user locations*	☒
118.	**Das mindestens erforderliche Betriebssystem für die Überprüfung von agilen VBA-Signaturen festlegen** *Set the minimum operating system for verifying agile VBA signatures*	☑[33]
119.	**Nur VBA-Makros vertrauen, die V3-Signaturen verwenden** *Only trust VBA macros that use V3 signatures*	☑
120.	**VBA-Legacysignaturen vertrauen** *Trust legacy VBA signatures*	☑

Sicherheitseinstellungen\Trust Center\Geschützte Ansicht *Security Settings\Trust Center\Protected View*		
121.	**Unsicherer Speicherort #1 bis #20** *Unsafe Location #1 to #20*	☒

Sicherheitseinstellungen\Trust Center\Vertrauenswürdige Kataloge *Security Settings\Trust Center\Trusted Catalogs*		
122.	**Vertrauenswürdiger Katalog-Speicherort #1 bis #10** *Trusted Catalog Location #1 to #10*	☒
123.	**Unsichere Web-Add-Ins und Kataloge zulassen** *Allow Unsecure web add-ins and Catalogs*	☒
124.	**Web-Add-Ins blockieren** *Block Web-Add-ins*	☑
125.	**Office Store blockieren** *Block the Office Store*	☑
126.	**Standardspeicherort für SharePoint-Katalog** *Default SharePoint Catalog Location*	☒
127.	**Standardspeicherort für freigegebene Ordner** *Default Shared Folder Location*	☒

32 XadES-X-L
33 Windows 8

128.	**Benutzer*innen die Kontrolle über die vertrauenswürdigen freigegeben Ordnerkataloge gestatten** *Allow users to control the Trusted Shared Folder Catalogs*	☒

Restrisiken

Die Konfiguration der Gruppenrichtlinien hilft nur dabei, die Angriffsfläche auf Anwendungen von Microsoft Office zu verringern bzw. die Sicherheit zu erhöhen. So existieren beispielsweise Verhaltensweisen, die nicht mittels Gruppenrichtlinien konfigurierbar sind. So können beispielsweise durch die Telemetrie auch sensible Daten an Microsoft übertragen werden.