Informationssicherheit

IT Systemkomponenten

Regelung Nr. 03.03.02

Clients

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Diese Regelung legt Sicherheitsanforderungen für Clients fest. Zusätzliche Anforderungen an die Sicherheit von Windows-Clients sowie von Unix- bzw. Linux-Clients werden definiert.

Im Sinne dieser Regelung bedeutet der Begriff „Informationssicherheit“ IT-Sicherheit als Bestandteil einer ganzheitlichen Informationssicherheit.

1. Client-Sicherheit

1.1. Ziel

Diese Regelung legt die notwendigen Informationssicherheitsanforderungen für den sicheren Betrieb von Clients fest.

Die folgenden Clients fallen in den Geltungsbereich dieses Dokuments:

- Windows-PCs (z. B. Produktion, Technik [CAD])
- Notebooks/Laptops
- Tablet-PCs
- Mobiltelefone/Smartphones/PDAs
- Unix-Workstations (einschließlich Linux)
- PCs in Testeinrichtungen oder Werken/Test-PCs
- Drucker (besonders multifunktionale)
- Mac-PCs

1.2. Prinzipien

Eine Standard-Clientkonfiguration[1] für jedes Betriebssystem (sowie ggf. für unterschiedliche Versionen eines Betriebssystems) muss von der für den Betrieb des betreffenden Clients zuständigen Stelle definiert werden.

1.2.1.1 Dokumentation

Alle für Standard-Clients zugelassenen Dienste und Anwendungen müssen dokumentiert werden.

1.2.1.2 Änderungsmanagement (Change Management)

Jegliche Änderungen an der Standard-Clientkonfiguration müssen dokumentiert werden. Änderungen müssen nachzuverfolgen sein.

Die zuständigen Stellen[2] müssen einen Änderungsmanagementprozess (Change Management Prozess) definieren[3].

[1] Siehe Anhang B.1.2

[2] Siehe Anhang B.1.3

[3] Siehe Anhang B.1.1

Das Change Management muss auch IT-Notfälle[4] abdecken, um ein sofortiges Handeln zu ermöglichen.

1.2.1.3 Testumgebung

Alle Funktionen der Sicherheitskonfiguration und diesbezüglichen Änderungen an Clients müssen vom Betreiber in einer Testumgebung getestet werden. Der Umfang dieser Tests muss vom Betreiber und von der Informationssicherheitsorganisation festgelegt werden. Softwareprodukte müssen vor der operativen Bereitstellung getestet werden.

1.2.1.4 Bereitstellung, Transport, Reparatur und Entsorgung

Für Bereitstellung, Transport, Reparatur und Entsorgung gelten die folgenden Mindestanforderungen:

- Vor einer Reparatur muss sichergestellt werden, dass keine Unbefugten auf Daten zugreifen können (z. B. durch Verschlüsselung, sichere Löschung[5] und/oder vergleichbare sichere Verfahren, mithilfe vertraglich mit der Entsorgungsfirma vereinbarter Spezialverfahren). Dies ist nicht notwendig, wenn die Reparatur vor Ort stattfindet und überwacht wird.
- Gespeicherte Anmeldedaten für die Authentifizierung im Netzwerk (z. B. WLAN-Kennwörter) müssen entfernt werden.
- Ein Austausch durch den Hersteller im Rahmen der Garantie ist nicht zulässig für Festplatten, auf denen vertrauliche, personenbezogene oder geheime Daten gespeichert sind. Die Festplatte muss physisch zerstört werden (z. B. mit einem Shredder).
- Im Fall der Entsorgung müssen alle Daten entfernt werden (z. B. physisch, durch sichere Löschung[6] oder ein vergleichbares sicheres Verfahren, mithilfe vertraglich mit der Entsorgungsfirma vereinbarter Spezialverfahren). Datenträger müssen sicher gelöscht oder zerstört werden. Es muss gewährleistet sein, dass die Daten mit hoher Wahrscheinlichkeit nicht rekonstruiert werden können[7].
- Nach einer Reparatur müssen die aktuelle Sicherheitskonfiguration und die Daten wiederhergestellt werden.
- Zusätzliche unternehmensspezifische Anforderungen, im Speziellen für den Transport, müssen beachtet werden[8].

1.2.1.5 Reaktionszeiten

Clients erfordern keine spezielle Verfügbarkeit. Da sich jeder Benutzer an jedem Client anmelden kann, ist keine Wiederherstellungszeit festgelegt.

Wenn eine spezielle Verfügbarkeit notwendig ist, muss dies mit dem Hersteller oder mit den für die betreffenden Clients zuständigen Stellen vereinbart werden.

---

[4] Siehe Anhang A.1.7

[5] Siehe Anhang A.1.3

[6] Siehe Anhang A.1.3

[7] Siehe Anhang A.1.3

[8] Siehe Anhang A.1.3

1.2.1.6 Ausnahmen

Ausnahmen von der Standard-Clientkonfiguration müssen von der zuständigen Stelle[9] freigegeben werden.

1.2.2 Authentifizierung/Autorisierung

1.2.2.1 Autorisierungskonzept

Unterschiedliche Benutzertypen müssen definiert werden.

Beispiele für Benutzertypen sind im Folgenden aufgeführt:

Nicht alle der folgenden Benutzertypen gelten für alle Betriebssysteme.

Bei Bedarf müssen spezielle Standards für Clients oder Berechtigungen für Softwareentwickler definiert werden.

- Beispiel: Endbenutzer

  Der Endbenutzer hat Zugriffsrechte für persönliche Dateien, mit denen er im Tagesgeschäft arbeitet. Der Benutzer darf keine Software installieren können. Der zuständige Client-Administrator kann dem Benutzer Zugriffsrechte für Netzlaufwerke auf Servern innerhalb der Domäne erteilen.

- Beispiel: Client-Administrator (Beispiel)

  Der Client-Administrator hat auf den Clients Administrationsrechte. Er darf nur freigegebene und lizenzierte Software installieren. Der Administrator kann Benutzer und Zugriffsrechte auf den Clients ändern oder löschen.

- Beispiel: Gruppenadministrator (z. B. lokaler Administrator/Key-User/NIS-Administrator)

  Der Gruppenadministrator verwaltet die Zuweisung, Änderung oder Löschung von Benutzern und Zugriffsrechten für Ressourcen innerhalb einer Administrationszone (z. B. Ressourcendomäne oder Organisationseinheit). Er darf nur freigegebene und lizenzierte Software installieren.

- Beispiel: Master-Administrator

  Der Master-Administrator ist für die Administration der Master-Domäne zuständig. Er verwaltet Benutzer und stellt Verbindungen zu den Master-Domänen der Konzerngesellschaften her. Der Master-Administrator verfügt über weiterreichende Berechtigungen als die Gruppenadministratoren. Er darf die Autorisierungen der Gruppenadministratoren installieren, ändern und löschen. Nur Master-Administratoren dürfen seine Autorisierungen klonen. Das „Vier-Augen-Prinzip“ muss angewendet werden (z. B. über ein geteiltes Kennwort).

1.2.2.2 Lokale Benutzerkonten

Lokale Benutzerkonten dürfen nur von Client- und Gruppenadministratoren für administrative Zwecke installiert und verwendet werden.

[9] Siehe Anhang B.1.3

Beim Zuweisen der Autorisierungen für einzelne lokale Benutzer auf dem Client muss das Prinzip minimaler Rechte beachtet werden.

1.2.2.3 Freigaben auf Clients

Auf dem Client dürfen nur die für administrative Zwecke verwendeten Verzeichnisse freigegeben werden. Der Zugriff auf Clients über das Netzwerk ist nur für administrative Zwecke zulässig.

Wenn ein Administrator auf den Desktop oder Dateien eines Benutzers zugreifen möchte (z. B. für remote Support) muss er das Einverständnis des betreffenden Benutzers einholen. Tätigkeiten im Rahmen der regulären administrativen Aufgaben (eDiscovery, Patches, etc.) benötigen nicht diese Zustimmung.

1.2.3 Client-Härtung

1.2.3.1 Allgemeine Anforderungen

Im Netzwerk des Konzerns dürfen ausschließlich Clients verwendet werden, die von der zuständigen Stelle[10] freigegeben wurden.

Eine automatisierte interaktive Anmeldung ist für personalisierte Konten nicht zulässig.

Der automatische Start von Wechselmedien muss deaktiviert werden, damit Programme nicht automatisch ausgeführt werden können.

1.2.3.2 Diensteinschränkungen

Die zuständige Stelle[11] muss die für den Betrieb notwendigen Protokolle und Dienste festlegen. Sofern technisch möglich, muss die am stärksten gesicherte Version der Protokolle und Dienste verwendet werden. Beim Festlegen der Versionen von Protokollen und Diensten (z. B. Verschlüsselung von geheimen Daten zur Speicherung und Übertragung) müssen Netzwerkumgebung und Informationsklassifizierung[12] der verarbeiteten Daten berücksichtigt werden.

Nicht benötigte Protokolle und Dienste müssen deinstalliert oder deaktiviert werden.

Serverdienste (z. B. der DNS-Serverdienst) dürfen nicht auf Netzwerk-Clients installiert werden. Das heißt, auf dem Client dürfen keine aus dem Netzwerk erreichbaren Dienste laufen (z.B. DNS-Server, Webserver, Datenbankserver).

1.2.3.3 Zugriffsschutz

Clients müssen gegen unbefugten Zugriff geschützt werden.

Standard-Benutzerkonten und -Administratorkonten müssen deaktiviert werden. Es muss ein neues lokales Administratorkonto mit einem sicheren Kennwort gemäß der Kennwortrichtlinie erstellt werden. Falls die Deaktivierung der Standard-Konten aus technischen Gründen nicht möglich ist, müssen die Standard-Benutzerkonten und -Administratorkonten umbenannt und mit einem sicheren Kennwort gemäß den Kennwortrichtlinien versehen werden.

---

[10] Siehe Anhang B.1.3

[11] Siehe Anhang B.1.3

[12] Siehe Anhang A.1.3

Software zum Sperren von Desktop-Workstations muss auf jedem Client installiert werden. Die Sperre darf erst nach Authentifizierung des Benutzers (z. B. Kennwort, PKI-Karte usw.) entfernt werden. Die Sperre muss automatisch aktiviert werden, wenn der Benutzer für einen vordefinierten Zeitraum (max. 10 Minuten) inaktiv ist.

Die Kennwortrichtlinien[13] müssen nach Möglichkeit technisch durchgesetzt werden.

1.2.3.4 BIOS (Firmware)

BIOS-Startkennwörter dürfen nicht gesetzt werden, da sonst die Softwareverteilung (z. B. für Sicherheitsupdates mit „Wake-On-LAN“) nicht gewährleistet ist.

Nur die zuständigen Stellen[14] dürfen BIOS-Konfigurationen ändern. Die BIOS-Konfigurationen müssen durch ein Kennwort geschützt werden.

Folgende Einstellungen gelten ausschließlich für interne Geräte:

Einstellung	Voraussetzung	Hinweis/Regel zur Ausnahme
Startreihenfolge	Erstes Startgerät ist die Festplatte.	Systemstarts über Diskette, CD-ROM, externe Geräte (z. B. USB-Gerät, Netzwerk/PXE) usw. sind standardmäßig deaktiviert
Startgeräte-Auswahlmenü	Ist aktiviert	
Aktivierung über Modem	Ist deaktiviert.	
Wake-On-LAN	Darf aktiviert werden.	Zur Softwareverteilung.

Folgende Einstellungen gelten ausschließlich für mobile Geräte:

Einstellung	Voraussetzung	Hinweis/Regel zur Ausnahme
Startreihenfolge	Erstes und einziges Startgerät ist die Festplatte.	Systemstarts über Diskette, CD-ROM, externe Geräte (z. B. USB-Gerät, Netzwerk/PXE) usw. sind nicht zulässig.
Startgeräte-Auswahlmenü	Ist deaktiviert.	Das Startgeräte-Auswahlmenü muss deaktiviert werden.
Aktivierung über Modem	Ist deaktiviert.	
Wake-On-LAN	Darf aktiviert werden.	Zur Softwareverteilung.

[13] Siehe Anhang A.1.3

[14] Siehe Anhang B.1.6

1.2.3.5 Dateisystem

Datenspeichermedien müssen für ein vom Hersteller empfohlenes Dateisystem formatiert sein. Der Anwendungsbereich und insbesondere die Datenklassifizierung müssen berücksichtigt werden.

1.2.3.6 Anwendungen

Standard-Anwendungssoftware und Client-Betriebssysteme müssen von der zuständigen Stelle[15] zur Installation freigegeben werden. Nicht zur Standardausstattung gehörende Anwendungen dürfen nur mit Freigabe durch die zuständigen Stellen[16] installiert oder eingesetzt werden.

1.2.3.7 Sicherheits-Patches

Von den für die Planung zuständigen Stellen[17] freigegebene Sicherheits-Patches müssen unverzüglich installiert werden.

Die für den Betrieb zuständige Stelle[18] ist auch für das Installieren der notwendigen Sicherheits-Patches zuständig.

1.2.3.8 Netzwerkverbindung

Alle Clients müssen als IP-Endgeräte konfiguriert werden. Routing muss deaktiviert werden. Gleichzeitige Verbindungen zwischen dem Client und mehreren Netzwerken sind nicht zulässig.

Nur freigegebene Netzwerkprotokolle dürfen verwendet werden. Alle anderen Kommunikationsprotokolle müssen deaktiviert werden.

Nicht benötigte Netzwerkschnittstellen müssen deaktiviert werden. Geräte mit zusätzlichen Netzwerkverbindungen dürfen nicht an im Netzwerk betriebene Computer angeschlossen werden.

Modem/ISDN

Die Verwendung von Modems an Desktop-Workstations, die im Netzwerk eingebunden sind, ist nicht gestattet.

Laptops müssen so konfiguriert werden, dass die beiden Netzwerkverbindungen (Modem und Unternehmensnetzwerk) nicht gleichzeitig betrieben werden können.

Multifunktionsgeräte mit Modem- bzw. Faxfunktion (z. B. HP Office Jet)

IT-Geräte dürfen nicht in mehreren Netzwerken verwendet bzw. betrieben werden.

[15] Siehe Anhang B.1.7

[16] Siehe Anhang B.1.7

[17] Siehe Anhang B.1.8

[18] Siehe Anhang B.1.9

Ausnahme: Multifunktionsdrucker (Drucker mit Scan-, Fax- und Druckfunktion), die von der zuständigen Stelle[19] freigegeben wurden, dürfen mit mehreren Netzwerken gleichzeitig verbunden werden.

1.2.4 Schutz des Clients

1.2.4.1 Schutz vor Schadsoftware

Die Anforderungen der Regelung Systemschutz[20] müssen beachtet werden.

Benutzer dürfen nicht in der Lage sein, die Sicherheitsmaßnahmen oder Einstellungen der Sicherheitssoftware zu ändern oder zu deaktivieren. Jede Konfigurationsänderung oder Deaktivierung des Client-Schutzes muss automatisch der zuständigen Stelle[21] gemeldet werden.

1.2.4.2 Personal Firewall

Allgemeines

Eine dauerhaft aktive Personal Firewall muss installiert sein.

Die Personal Firewall muss den Netzwerkdatenverkehr auf das erforderliche Minimum beschränken. Dies gilt sowohl für eingehenden als auch für ausgehenden Datenverkehr.

Die Einstellungen für den zulässigen Netzwerkdatenverkehr müssen dokumentiert werden.

IT-Notfall

Es muss möglich sein, die Einstellungen kurzfristig zentral zu ändern.

1.2.4.3 Host-based Intrusion Prevention System (HIPS)

Allgemeines

Wenn der Client außerhalb des Unternehmensnetzwerks eingesetzt wird bzw. wenn vertrauliche oder geheime Informationen auf dem Client gespeichert sind, muss auf dem Client ein Host-based Intrusion Prevention System installiert werden und ständig aktiv sein.

Aktionen, die durch die zentral verwalteten Rahmenregeln als Eindringversuche erkannt werden, müssen vom Host-based Intrusion Prevention System blockiert und sofort gemeldet werden. Wenn das System zu diesem Zeitpunkt nicht mit dem Unternehmensnetzwerk verbunden ist, muss ein Alarm gesendet werden, sobald das System wieder Zugang zum Unternehmensnetzwerk hat.

Aktualisierungen

Automatische und sofortige Aktualisierungen von sicherheitsrelevanten Komponenten (z. B. Signaturen) müssen nach einem definierten Prozess erfolgen.

[19] Siehe Anhang B.1.10

[20] Siehe Anhang A.1.4

[21] Siehe Anhang B.1.5

IT-Notfall

Folgendes muss zentral initiiert werden können:

- Sofortige Aktualisierung von Signaturdatenbank oder Scan-Engine
- Konfigurationsänderungen am HIPS

1.2.5 Schutz der Informationen

1.2.5.1 Informationsklassifizierung

Informationen müssen gemäß deren Klassifizierung geschützt werden (Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit)[22].

1.2.5.2 Schutz vor Verlust und unautorisiertem Zugriff

Auf jedem Client muss eine sichere Authentifizierung (basierend auf Kenntnis und Besitz) gewährleistet sein. Ausnahme: „Info-Terminals“ mit anonymem Zugriff auf definierte und eingeschränkte Intranet-Sites sowie „Stapelterminals“ bzw. MFDs.

Eine Verschlüsselung für Daten muss gewährleistet sein (z. B. wenn mehrere Benutzer einen Client gemeinsam nutzen). Die Verschlüsselung muss benutzerspezifisch umgesetzt werden. Ausnahmen sind über den Prozess von Ausnahmegenehmigungen zu beantragen.

Nicht mehr benötigte vertrauliche oder geheime Daten müssen zuverlässig gelöscht werden (z. B. durch Überschreiben oder ähnliche sichere Verfahren)[23].

Auslagerungs- und Cachedateien müssen beim Abmelden sicher gelöscht werden. Dies muss automatisch erfolgen und der Benutzer darf den Prozess nicht anhalten können. Cachedateien, die für die Offline-Arbeit benötigt werden (z. B. Dateien für den Outlook-Cachemodus), oder Dokumente, an denen lokal gearbeitet wird (z. B. aus dem DMS ausgecheckte Dokumente), dürfen nicht beim Abmelden gelöscht werden.

1.2.5.3 Schutz vor Manipulation

Die Möglichkeit, elektronische Signaturen zu verwenden und zu überprüfen, muss auf dem Client gegeben sein, damit relevante Daten vor Manipulation geschützt werden können.

1.2.5.4 Client-Inventar

Es muss gewährleistet sein, dass die folgenden Informationen zu den Clients jederzeit gesammelt werden können (Online-Betrieb: der aktuelle Status; Offline-Betrieb: letzte Version, mit der der Client online war):

- Betriebssystem, Version und Patch-Level
- Standardsoftware, Version und Patch-Level
- Sicherheitsprodukte (z. B. Virenschutz), Version, Patch-Level und Erkennungsdatenbank
- Installierte und aktive Dienste
- Benutzer- und Zugriffsautorisierung
- Zusätzliche installierte Software (nicht zur Standardausstattung gehörende Software, Hacker-Tools, Spyware usw.)

[22] Siehe Anhang A.1.3

[23] Siehe Anhang A.1.3

- Verfügbarer Speicherplatz auf der Festplatte (z. B. Ausreichend für Installation eines Sicherheitsupdates?)
- Kontaktdaten (z. B. Standort, IT-Ansprechpartner/Administrator)
- Konfiguration für Protokollierung und Auditing

1.2.5.5 Softwareverteilung und Verwaltungstools

Verwaltungstools und Softwareverteilungsmechanismen müssen die folgenden Funktionen bieten und die folgenden Anforderungen erfüllen:

- Modulare Struktur von Softwarepaketen (modulare Anwendungspakete)
- Softwarepakete müssen kryptografisch signiert sein
- Verteilung von Sicherheitssoftware
- Verteilung von Signaturdatenbanken (z.B. für Virus/Malware Schutz)
- Installation von Service Packs, Patches, Hotfixes usw.
- Verteilung von Richtlinien (Konfiguration bzw. Regeln) für Betriebssystem, Anwendungen und Sicherheitsprodukte
- Verteilungen müssen ohne Unterbrechung durch den Benutzer durchsetzbar sein
- Möglichkeit einer sofortigen „Push-Verteilung“, damit bei einem IT-Notfall Maßnahmen ergriffen werden können
- Benachrichtigung bei Fehlern
- Nicht erreichbare Clients müssen aktualisiert werden können, sobald sie sich wieder mit dem Netzwerk verbinden

Zentrale Verwaltung:

- Community Strings müssen gemäß der Kennwortrichtlinie zugewiesen werden, wenn SNMP (Simple Network Management Protocol) verwendet wird.
- SNMP-Dienst Version 1 muss deaktiviert werden.
- SNMP-Dienst Version 3 muss bevorzugt verwendet werden. Community Strings müssen verschlüsselt werden.

1.2.6 Berichterstattung

Es muss möglich sein, die folgenden Berichte regelmäßig (z. B. einmal pro Woche) und auf Anforderung zu erstellen:

- Inventar, Abweichungen zwischen Soll- und Istzustand
- Fertigstellung des Rollouts in Prozent (z. B. Hotfix XY zu 95 % verteilt)
- Auswertungsmöglichkeit bzw. Analyse von Vorfällen (z. B. Art und Anzahl der Angriffe)

2. Windows-Clients

2.1. Ziel

Dieses Kapitel beschreibt die notwendigen Einstellungen und Parameter für die Microsoft Windows-Client-Betriebssysteme. Es umfasst allgemeine Einstellungen und Parameter, die für alle aktuell genehmigten verwendeten Microsoft Windows Betriebssysteme gelten.

2.2. Beschränkung des Systems auf ein Minimum

Jede zusätzliche Windows-Komponente oder Anwendung eines Drittanbieters ist anfällig für Schwachstellen. Deshalb ist es notwendig, nur die für die Bereitstellung der Dienste des Clients erforderliche Software zu installieren. In Betriebssystemen vor Windows Vista müssen nicht notwendige Komponenten[24], wie von der zuständigen Stelle festgelegt, entfernt werden.

2.3. Beschränkung der Dienstkonfiguration auf ein Minimum

Nicht notwendige Dienste müssen deaktiviert werden. Soweit möglich, dürfen aktive Dienste nicht mit einem lokalen Systemkonto gestartet werden. Für diesen Zweck muss ein Konto mit möglichst wenig Rechten (Dienstkonto) erstellt und verwendet werden. Die Listen im Anhang[25] geben einen Überblick über die Standarddienste sowie über einige weitere gängige Dienste und die Einstellungen, die angewendet werden müssen.

Die Listen sind nicht vollständig, weil zusätzliche installierte Software zusätzliche Dienste erfordern kann. Zusätzliche unternehmensspezifische Einstellungen[26] müssen beachtet werden.

Benutzer dürfen keine deaktivierten Dienste manuell starten können.

2.4. Benutzerkonten

2.4.1 Lokale Benutzerkonten

Auf jedem Windows-Client dürfen nur die zwei in der folgenden Tabelle beschriebenen lokalen Konten vorhanden sein.

Konto	Voraussetzung	Hinweis/Regel zur Ausnahme
Gast	• Ein sicheres Kennwort ist vergeben. • Das Konto ist deaktiviert.	
Administrator 1)	• Es muss ein neues Administratorkonto 1) mit sicherem Kennwort erstellt werden • Das Default Administrator Konto muss deaktiviert werden 2)	1) Der Name darf nicht offensichtlich sein. Das Umbenennen des Kontos von „Administrator“ in „Admin“ reicht nicht aus. 2) Ausnahme: Kann diese Anforderung aus technischen Gründen nicht umgesetzt werden, muss das Default Administrator Konto umbenannt werden, wobei Namen wie „Admin“ nicht ausreichen 1). Das Default Administrator Konto muss mit einem sicheren Kennwort geschützt werden.

[24] Beispiele für nicht erforderliche Komponenten: Spiele, Windows Messenger, Outlook Express usw.

[25] Siehe Anhang C.1

[26] Siehe Anhang B.2.1

In höheren Windows-Versionen als NT 4.0 (2000, Vista, 7 usw.) kann das Deaktivieren und Umbenennen der Konten per Gruppenrichtlinienobjekt erfolgen. Verwenden Sie daher Folgendes:

Computerkonfiguration \ Windows-Einstellungen \ Lokale Richtlinien \ Sicherheitsoptionen

- *Konto: Gastkontenstatus bzw. Administratorkontostatus*
- *Konto: Gast- bzw. Administratorkonto umbenennen*

Alle Kennwörter müssen den Richtlinien für systembezogene Benutzerkonten[27] entsprechen.

Für deaktivierte Standardkonten ist es nicht notwendig, das Kennwort regelmäßig zu ändern.

2.4.2 Domänenbenutzerkonten

Domänenbenutzerkonten für die Client-Anmeldung gehören nicht zum Umfang dieses Dokuments[28].

2.5. Benutzerrechte

Es wird empfohlen, Rechte den Benutzergruppen zuzuweisen. Nur in Ausnahmefällen sollten Rechte einzelnen Konten gewährt werden. Eine Liste unterschiedlicher Benutzerrechte ist im Anhang[29] enthalten.

2.6. Protokollierung

Die maximale Größe des Ereignisprotokolls muss angemessen sein.

2.6.1 Basiskonfiguration

Die Einstellungen[30] für die Basiskonfiguration können mithilfe eines Richtlinienobjekts verwaltet werden:

Computerkonfiguration \ Richtlinien \ Windows-Einstellungen \ Sicherheitseinstellungen \ Lokale Richtlinien \ Überwachungsrichtlinie

2.6.2 Erweiterte Überwachungseinstellungen

Windows Vista und höher bieten die Möglichkeit einer feingranularen Protokollierung. Dafür muss die folgende Anweisung eingestellt werden (**Computerkonfiguration \ Richtlinien \ Windows-Einstellungen \ Sicherheitseinstellungen \ Lokale Richtlinien \ Sicherheitsoptionen**). Bei Verwendung dieser Einstellung sollten die Einstellungen aus Kapitel 2.6.1 auf „*Nicht definiert*“ gesetzt werden.

Einstellung	Wert
Überwachung: Unterkategorieeinstellungen der Überwachungsrichtlinie erzwingen (Windows Vista oder höher), um Kategorieeinstellungen der Überwachungsrichtlinie außer Kraft zu setzen	Aktiviert

[27] Siehe Anhang A.1.1

[28] Siehe Anhang A.1.6

[29] Siehe Anhang C.2

[30] Siehe Anhang C.3.1

Beachten Sie, dass eine Konfiguration von feingranularen Überwachungseinstellungen über eine Gruppenrichtlinie nur unter Windows Server 2008 R2 oder neuer möglich ist. Das bedeutet, dass zumindest der Domänencontroller über die Version2008 R2 oder neuer verfügen muss.

Die empfohlenen Einstellungen für eine feingranulare Überwachung sind im Anhang[31] aufgeführt.

2.7. Netzwerk

2.7.1 Deaktivieren von NetBIOS über TCP/IP

NetBIOS über TCP/IP muss deaktiviert werden, falls nicht benötigt.

2.7.2 Konfiguration des Netzwerktyps

Wenn eine neue Netzwerkverbindung unter Windows Vista oder höher konfiguriert wird, muss sie einem Netzwerktyp zugewiesen werden. Die folgenden Typen können ausgewählt werden:

- Heimnetzwerk
- Firmennetzwerk
- Öffentliches Netzwerk

Je nach ausgewähltem Netzwerktyp ändert Windows die Datei-und Druckerfreigabe im System. Um maximale Sicherheit zu gewährleisten, muss die Option „Öffentliches Netzwerk“ ausgewählt werden. Windows deaktiviert dann die Datei- und Druckerfreigabe und ändert die Sichtbarkeit des Systems im Netzwerk zu „Unsichtbar“ (was zu einem späteren Zeitpunkt geändert werden kann).

Alle Netzwerke muss der Netzwerk- oder Standorttyp auf „Öffentlich“ gesetzt werden.

2.8. Patch-Management

Um die Systeme auf dem aktuellen Stand zu halten, muss ein Patch-Managementprozess[32] eingesetzt werden.

Eine Nichtzulassung von Patches oder Service Packs benötigt die Freigabe durch die zuständige Stelle[33].

2.9. Datenausführungsverhinderung (DEP)

Datenausführungsverhinderung (DEP) ist eine Sicherheitsfunktion von Windows 7 und höher. Sie trägt dazu bei, Beschädigungen des Systems durch Viren oder andere sicherheitsrelevante Vorfälle zu vermeiden. DEP überwacht laufende Programme, um sicherzustellen, dass sie nur den Speicherplatz nutzen, der ihnen vom System zugeteilt wurde. Wenn DEP feststellt, dass ein Programm in „fremde“ Speicherbereiche schreibt, schließt es das Programm und benachrichtigt den Benutzer.

---

[31] Siehe Anhang C.3.2

[32] Weitere Informationen finden Sie in Anhang A.1.5

[33] Siehe Anhang B.2.2

Die Verwendung von EMET (Enhanced Mitigation Experience Toolkit) wird empfohlen. EMET ist ein Sicherheitstool von Microsoft, das alle laufenden Anwendungen im System mithilfe der Schutzmechanismen DEP und ASLR (zufällige Anordnung des Layouts des Adressraums) erfasst. Es beseitigt zwar nicht die Sicherheitslücken, aber es verhindert, dass sie ausgenutzt werden. Der Quellcode der verwendeten Anwendungen darf nicht geändert werden. Konfiguration, Verwaltung und Überwachung von EMET können per Gruppenrichtlinie erfolgen.

2.10. Gruppenrichtlinien und Registrierungseinträge

Direkte Änderungen an Registrierungsschlüsseln müssen vermieden werden. Gruppenrichtlinien werden von Windows-Versionen unterstützt, die neuer sind als Windows NT. Das manuelle Einstellen der Registrierungseinträge ist daher nur unter Windows NT zulässig.

Die Einstellungen für die verschiedenen Versionen von Windows sind im Anhang[34] aufgeführt.

2.11. Temporäre Dateien

Dateien, die von Outlook oder anderen Office-Programmen geöffnet wurden, bleiben auch nach dem Schließen der jeweiligen Anwendung im temporären Verzeichnis. Dies bedeutet ein Sicherheitsrisiko, weil es sich um vertrauliche Dokumente handeln könnte. Es muss gewährleistet sein, dass temporäre Verzeichnisse regelmäßig mit einer sicheren Methode bereinigt werden.

Funktion	Voraussetzung	Hinweis/Regel zur Ausnahme
Papierkorb	Dateien, die sich seit mehr als einer Woche im Papierkorb befinden, werden so gelöscht, dass sie nicht wiederhergestellt werden können.	Da hierfür ein geeignetes Tool notwendig ist, muss die Aufgabenplanung aktiviert werden.
Temporäre Verzeichnisse	Werden regelmäßig bereinigt (jeden Werktag).	

2.12. Systemsperre

Eine Systemsperre muss auf allen Geräten sichergestellt sein. Wenn ein Benutzer (Ausnahme: Gruppenuser) für eine vordefinierte Zeit (max. 10 Minuten) inaktiv ist, muss sich die Sperre automatisch aktivieren. Die Sperre darf nur durch die erfolgreiche Authentisierung eines Benutzers (z.B. mittels Passwort, PKI-Karte, etc.) aufgehoben werden. Authentisierung und Aktivierungszeit müssen unabhängig von Benutzereinstellungen gewährleistet sein.

Ausnahmen sind über den Prozess von Ausnahmegenehmigungen[35] zu beantragen.

[34] Siehe Anhang C.4

[35] Siehe Anhang A.1.2

3. Unix- bzw. Linux-Clients

3.1. Ziel

Ziel dieses Kapitels ist die Festlegung der Sicherheitsanforderungen für Unix- bzw. Linux-Clients.

3.2. Sicherheitskonfiguration

Die beschriebenen Voraussetzungen müssen konfiguriert werden. Ausnahmen müssen von der zuständigen Stelle[36] freigegeben werden.

3.2.1 Benutzer-IDs und Kennwörter

3.2.1.1 Lokale Konten

Konto	Voraussetzung
Gast	Eine Anmeldung als Gast ist nicht zulässig.
Root	Ein sicheres Kennwort ist festgelegt.
Benutzer mit lokalen Administrationsrechten	Ein sicheres Kennwort ist festgelegt. Der Benutzername muss dem Standard-Namensschema entsprechen. Superuser-Befehle dürfen nur mit „sudo“ ausgegeben werden.
Normales Benutzerkonto	Ein sicheres Kennwort ist festgelegt. Der Benutzername muss dem Standard-Namensschema entsprechen. Nach Möglichkeit sollte eine zentrale Authentifizierung (Kerberos, Active Directory) eingesetzt werden.

Kennwörter müssen den Richtlinien für systembezogene Benutzerkonten[37/38] entsprechen.

3.2.2 Betriebssystem

Die folgenden Sicherheitseinstellungen müssen für alle Unix- bzw. Linux-Betriebssysteme beachtet werden. Je nach Betriebssystem kann es sein, dass einige Einstellungen nicht vorhanden sind.

3.2.2.1 Paketverwaltung

Es dürfen nur Pakete installiert werden, die für die Zwecke des betreffenden Clients erforderlich sind. Insbesondere sind Dienste, die Netzwerk-Listener bereitstellen, nicht zulässig. Dazu gehören beispielsweise folgende:

- NFS-Server
- FTP-Server
- TFTP-Server
- Telnet-Server
- SAMBA-Server
- SSH-Server
- Mail-Server

[36] Siehe Anhang B.3.1

[37] Siehe Anhang A.1.1

[38] Siehe Anhang A.1.3

- DNS-Server

3.2.2.2 Paket-Repository

Je nach verwendetem Betriebssystem muss ein zentrales Softwareverteilungssystem eingesetzt werden, in dem nur freigegebene Softwarepakete zugänglich sind. Öffentliche Repositorys dürfen nicht verwendet werden.

3.2.2.3 Dateisystem

Das Dateisystem muss nach File System Hierarchy Standard (FHS)[39] strukturiert werden.

Der Zugriff auf **Systemdateien** muss beschränkt werden. Die folgende Tabelle kann dabei als Leitfaden dienen.

/etc/*	Root	Root	-rw-r----- (0640)
/var/spool/cron/crontabs/*	<Besitzer>	Crontab|sys	-r-------- (0400)
/etc/cron.d/*	Root	Root	-rwxr-x--- (0750)
/etc/cron.[hourly|daily|weekly]/*	Root	Root	-rwxr-x--- (0750)
/var/log/*	Root	Root	-rw-r----- xr-x (0640)
/var/log/<systemlogdaten>	Root	Root	-rw-r----- (0640)
/var/log/<dienste != user root>	Je nach Dienstanforderung	Je nach Dienstanforderung	Je nach Dienstanforderung
/var/log/wtmp	Root	Root	-rw-r----- (0640)
/var/run/utmp	Root	Root	-rw-r----- (0640)

Dateien und/oder Verzeichnisse, die **für alle lesbar** und besonders **für alle beschreibbar** sind, sollten vermieden werden, sofern technisch möglich.

```
find / -perm -2 ! -type l -ls
```

SID- und **GID-**Dateien sollten vermieden werden.

```
find / -type f \( -perm -004000 -o -perm -002000 \) -exec ls -lg {} \;
```

Besondere Dateien

Parameter	Wert
/etc/hosts.equiv	Als leere Datei erstellen
/etc/hosts.lpd	Als leere Datei erstellen
$HOME/.rhosts	Regelmäßig suchen und löschen find / -name '.rhosts' -exec /bin/cat {} \; -print
.exrc	Regelmäßig suchen und löschen bash# find / -name '.exrc' -exec /bin/cat {} \; -print

[39] Siehe Anhang A.3

Parameter	Wert
.forward	Regelmäßig suchen und löschen bash# find / -name '.forward' -exec /bin/cat {} \; -print
Besondere Dateien (Zeichen- und Sperrvorrichtungen)	Dürfen nur in /dev gespeichert werden bash# find / \(-type b -o -type c \) -print | grep -v '^/dev/'
Verwaiste Dateien	Regelmäßig suchen und löschen find / \(-nouser -o -nogroup \) -print

Mounting-Einstellungen

Die folgenden Mounting-Optionen müssen verwendet werden:

Parameter	Wert
$HOME	nosuid, noexec, nodev
/var	nosuid, noexec, nodev
/tmp	nosuid, noexec, nodev
Externe Dateisysteme	nosuid, noexec, nodev

- nosuid: SID- und GID-Bit werden deaktiviert.
- nodev: Besondere Dateien werden nicht interpretiert.
- noexec: Das execute-Bit wird deaktiviert.

3.2.2.4 Grenzwerte

Sofern durch das Betriebssystem unterstützt, muss Folgendes definiert und implementiert werden.

- Quoten sollten festgelegt werden
- Maxlogin-Werte für nicht personalisierte Benutzer
- Maximale Größe für Kerndateien
- Anzahl der Prozesse für jeden Benutzer

3.2.2.5 Benutzereinstellungen

Folgende Einstellungen müssen für Benutzerkonten festgelegt werden:

Variable	Beschreibung
EXINIT	=" (leer)
PATH	Reihenfolge beibehalten: Systemverzeichnisse (/usr/bin /bin /usr/local/bin …) Zusätzliche Software (/opt/…) Insbesondere darf das lokale Verzeichnis „.“ nicht einbezogen werden.
umask	022 oder 027

3.2.2.6 Dienste

Nur an „localhost“ gebundene Netzwerk-Listener sind zulässig.

3.2.2.7 Protokollierung

Alle Log-Meldungen müssen lokal gespeichert werden. Besondere Ereignisse, wie von der zuständigen Stelle[40] definiert, müssen an einen zentralen Protokolldienst gesendet werden. Für das Betriebssystem und den zentralen Protokolldienst muss jeweils das am besten gesicherte der bereitgestellten Log-Protokolle verwendet werden.

3.2.2.8 Benutzerkonten

Nicht verwendete Konten müssen gesperrt oder gelöscht werden.

3.2.2.9 Netzwerk

Folgende Netzwerkeinstellungen müssen implementiert werden:

Parameter	Wert
IPv6	Sollte deaktiviert werden, wenn IPv6 nicht verwendet wird.
IP-Forwarding	Muss deaktiviert werden.
IP-Spoofing	Maßnahmen gegen Spoofing sollten ergriffen werden.
ARP cache thrashing	Der ARP-Cache sollte geschützt werden.
Directed Broadcasts	Muss deaktiviert werden.
Source Routed	Muss deaktiviert werden.
Random TCP ISNs	Sollte aktiviert werden.
SYN-flooding	SYN-Flooding-Schutz sollte aktiviert werden.
ICMP	Ein Client sollte nur auf direkte Echoanforderungen reagieren.
Stack Execution	Sollte deaktiviert werden.

[40] Siehe Anhang B.3.1

4. Mobile Arbeitsumgebung

4.1. Ziel

Dieses Kapitel legt die notwendigen Sicherheitsanforderungen für mobile Arbeitsumgebungen fest.

Mobile Arbeitsumgebungen sind Arbeitsumgebungen ohne den physischen Schutz von Arbeitsstätten innerhalb des Geländes einer Konzerngesellschaft. Ein mobiles Arbeitsumfeld kann beispielsweise auch ein Konferenzraum sein, wenn dieser nicht wie der übliche Arbeitsplatz eines Arbeitnehmers geschützt ist.

Die Verwendung des Begriffs „mobile Geräte“ in diesem Kapitel umfasst folgende Geräte:

- Laptops
- Mobiltelefone, Smartphones, Tablets
- PDAs
- Token zu Authentisierung (z.B. RSA, PKI-Karte)

4.2. Allgemeine Anforderungen

Beim Arbeiten in Bereichen, zu denen Dritte Zugang haben (z. B. Bahnhöfe oder Flughäfen), müssen unternehmenskritische Daten geschützt werden. Dies gilt für Dokumente und insbesondere für mobile Geräte. Daten können beispielsweise durch Einsehen oder Fotografieren des Bildschirms, Abfangen von Daten während der Übermittlung oder Stehlen von Geräten eingesehen werden.

Daher müssen die folgenden Anforderungen erfüllt sein:

- Daten, die als „vertraulich“ oder höher eingestuft werden, dürfen nur verarbeitet werden, wenn unautorisierte Personen keine Sicht auf den Bildschirm haben.
- Für mobiles Arbeiten mit mobilen Geräten muss ein Sichtschutzfilter verwendet werden.
- Dokumente (digital und gedruckt) müssen gegen Diebstahl oder Zugriff durch unautorisierte Personen geschützt werden.
- Es dürfen nur so wenige Daten wie möglich lokal auf mobilen Geräten gespeichert werden.
- Mobile Geräte dürfen nicht unbeaufsichtigt liegen gelassen werden, wenn unautorisierte Personen den Raum betreten können.
- Vor Verlassen des Arbeitsplatzes muss der Bildschirm durch den Benutzer gesperrt werden. Nach 10-minütiger Inaktivität muss sich der Bildschirm automatisch sperren.
- Unternehmenskritische Daten dürfen nur auf mobilen Geräten gespeichert werden, sofern dies zur Erfüllung von unternehmenswichtigen Aufgaben notwendig ist.
- Wenn einige Kommunikationsschnittstellen (z. B. Bluetooth, WLAN) nicht benötigt werden, müssen diese durch den Benutzer auf dem Gerät deaktiviert werden.
- Mobile Geräte und Datenspeicher müssen sicher transportiert werden (z. B. Notebook-Tasche).
- Authentifizierungsmedien (z. B. PKI-Karte) dürfen nicht in der gleichen Tasche aufbewahrt werden wie das zugehörige Gerät.

- Der Verlust oder Diebstahl eines mobilen Geräts oder von Daten (z. B. Dokumenten) muss unverzüglich an die zuständige Stelle[41] übermittelt werden.
- Sofern dies technisch möglich ist, muss auf allen mobilen Geräten eine Antivirus-Anwendung installiert und aktiviert sein. Aktualisierungen müssen regelmäßig durchgeführt werden.
- Mobile Geräte müssen regelmäßig an das Unternehmensnetzwerk angeschlossen werden, um die neuesten Aktualisierungen für das Betriebssystem und Antivirus-Anwendungen zu erhalten. Mobiltelefone, Smartphones und Tablets müssen regelmäßig gegen das Regelwerk des Mobile Device Managements geprüft werden.
- Mobile Geräte müssen durch eine Firewall geschützt werden, sofern dies technisch möglich ist.
- Alle Geräte müssen registriert sein und einem Benutzer mit einer eindeutigen Identifikationsnummer zuzuordnen sein (Geräte-ID).
- Mobile Geräte dürfen nur durch die zuständige Stelle[42] zur Verfügung gestellt und eingerichtet werden.
- Falls die Geräte repariert oder verschrottet werden müssen, muss die zuständige Stelle[43] sicherstellen, dass die Informationssicherheitsaspekte eingehalten werden (z. B. sicheres Löschen von Daten).
- Es muss möglich sein, das Gerät im Diebstahl- oder Verlustfall zu sperren oder Daten per Fernzugriff zu löschen.

4.3. Physischer Schutz

- Mobile Geräte müssen gegen Diebstahl gesichert werden.
- Mobile Geräte müssen sicher aufbewahrt werden (z. B. Tresor oder abgeschlossener Schrank). Falls dies nicht möglich ist, muss ein Sicherheitsschloss für Laptops und Tablets verwendet werden (z. B. in Konferenzräumen während der Mittagspause).

4.4. Zugriffsschutz für Geräte

4.4.1 Authentifizierung

- Systemzugriffe (Anmelden oder Entsperren) müssen durch Benutzerauthentifizierung geschützt werden. Vorzugsweise muss der sicherste technische Authentifizierungsmechanismus verwendet werden, der praktikabel ist.
- Die Authentifizierungsabfrage (Anmeldungsaufforderung) muss während des Einschaltens ausgeführt werden.
- Es gibt zwei Möglichkeiten für einen sicheren Anmeldevorgang. Eine der folgenden Methoden muss implementiert werden.

[41] Siehe Anhang B.4.1

[42] Siehe Anhang B.4.2

[43] Siehe Anhang B.4.3

Benutzerzertifikate

- Benutzerzertifikate gespeichert auf einer Smartcard, die die Anforderungen der entsprechenden Informationssicherheitsregelung[44] erfüllt und durch eine PIN geschützt ist.

Benutzerkennwörter

- Bei Benutzerkennwörtern zur Authentifizierung müssen die Anforderungen für Passwörter eingehalten werden[45].

4.4.2 Verschlüsselung

Um den Zugriff von unautorisierten Personen auf Daten und Anwendungen zu verhindern, müssen zusätzlich zur geschützten Anmeldung alle Dateien, Datenbanken und Anwendungen verschlüsselt werden.

- Mobile Geräte müssen verschlüsselt werden, wenn sie außerhalb des Betriebsgeländes getragen werden oder vertrauliche, geheime oder personenbezogene Daten auf dem Gerät enthalten sind. Geräte, die nicht verschlüsselt werden können, sollten nicht in Umlauf gebracht werden. Für Laptops ist eine Verschlüsselung verpflichtend[46].
- Die Verschlüsselung muss automatisch durchgeführt werden (ohne Benutzerinteraktion), während eine Datei gespeichert wird oder ein Programm/eine Anwendung geschlossen wird. Die Authentifizierungsanforderungen[47] müssen eingehalten werden.

4.5. Ausstattung und Konfiguration

Jedes Gerät muss mit einer Standardkonfiguration konfiguriert werden, wenn das Gerät dem Endbenutzer übergeben wird. Die Standardkonfiguration muss folgende Aspekte abdecken (sofern vom Gerät unterstützt):

4.5.1 Sichere Konfiguration

- Standardbenutzerprofile müssen Folgendes enthalten:

- Lokale Sicherheitseinstellungen (z. B. Authentifizierungstyp, Verschlüsselungsalgorithmen)
- Anwendungsprofil (für jede Benutzergruppe)
- Zusätzliche benötigte Sicherheitssoftware (z. B. VPN-Clients, Plug-Ins zur Authentifizierung)
- Erlaubte Kommunikationsschnittstellen
- Intervalle für Datensicherungen

---

[44] Siehe Anhang A.1.8

[45] Siehe Anhang A.1.3

[46] In manchen Ländern ist eine Verschlüsselung gesetzlich nicht zulässig. In diesen Fällen dürfen nur so wenig wichtige Daten wie möglich auf Laptops gespeichert werden. Die Speicherung von als „vertraulich“ oder höher eingestuften Daten muss vom Eigentümer dieser Daten freigegeben werden.

[47] Siehe Anhang A.1.9

- Firewall-Konfiguration
- Browser-Konfiguration (Proxy)
- Funktionelle Restriktionen (z. B. Deaktivierung nicht benötigter Funktionen)

- Die Konfiguration von Benutzerprofilen muss automatisch während der Synchronisierung mit dem Unternehmensnetzwerk überprüft werden.
- Die mobilen Geräte müssen während der Verbindung mit dem Unternehmensnetzwerk automatisch nach Aktualisierungen für das Betriebssystem und Antivirus-Software suchen und diese installieren. Mobiltelefone, Smartphones und Tablets müssen regelmäßig gegen das Regelwerk des Mobile Device Managements geprüft werden.

4.5.2 Softwareverteilung

- Die Verteilung von Softwarepaketen muss zentral verwaltet werden.
- Regelmäßige Berichte über die Softwareversion müssen erstellt werden. Dies muss von der Software unterstützt werden.
- Für Mobiltelefone, Smartphones und Tablets muss sichergestellt werden, dass Anwendungen von Drittanbieter-Appstores (z. B. Apple iTunes, Google Playstore) nur nach Freigabe durch die zuständige Stelle[48] installiert werden können. Dies muss mittels Whitelist oder Blacklist forciert werden. Ebenfalls muss sichergestellt werden, dass Anwendungen von Drittanbietern keinen Zugriff auf Mails, Kontakte oder Kalender haben.

4.5.3 Sicherung und Wiederherstellung

- Datensicherungen von mobilen Geräten müssen regelmäßig durchgeführt werden.
- Es muss sichergestellt werden, dass alle Datensicherungen von Systemen zentral auf dem Server gespeichert werden.
- Die Wiederherstellung darf nur durch autorisierte Stellen oder Benutzer möglich sein.

4.6. Datenaustausch

4.6.1 Sicheres Übertragungsprotokoll

Alle Übertragungen von oder auf mobile Geräte müssen verschlüsselt erfolgen. Die Verbindung zwischen dem Gerät und dem IT-Systemnetzwerk der Konzerngesellschaft muss stets verschlüsselt sein. Dies gilt für folgende Schnittstellen:

- Wireless LAN/IEEE 802.11
- Bluetooth
- UMTS/LTE
- USB-Sticks
- SD-Karten

[48] Siehe Anhang B.4.4

4.6.2 Verschlüsselung

- Der Datenaustausch zwischen mobilen Geräten und einem IT-System über ein Konzernnetzwerk mit Funkschnittstellen (Wireless LAN/IEEE 802.11, Bluetooth, UMTS, LTE usw.) muss verschlüsselt stattfinden.
- Zugriffe von externen Netzwerken auf Ressourcen innerhalb des Konzernnetzwerks sind nur über eine VPN-Verbindung zwischen dem mobilen Gerät (VPN-Client) und dem VPN-Gateway erlaubt. Weitere Anforderungen[49] müssen eingehalten werden.
- Bei Versenden von vertraulichen, geheimen oder persönlichen Daten per E-Mail ohne Verwendung einer VPN-Verbindung muss sichergestellt werden, dass PGP oder S/MIME mit X.509-Zertifikaten verwendet wird. Die privaten PGP-Schlüssel von Benutzern müssen in einem verschlüsselten lokalen Schlüsselspeicher auf dem Gerät gespeichert werden. Bei S/MIME müssen die zugewiesenen Schlüssel möglichst auf Smartcards gespeichert werden.

4.6.3 Zugriffsbeschränkungen für Anwendungen

- Es muss sichergestellt werden, dass alle Anwendungen sichere Protokolle für die Kommunikation mit dem Unternehmensnetzwerk verwenden.
- Anwendungen auf Smartphones oder Laptops dürfen ausschließlich anonyme Daten an den Hersteller versenden.

[49] Siehe Anhang A.1.10

5. Client-Anwendungen und Standardsoftware

5.1. Ziel

Dieses Kapitel beschreibt die notwendigen Einstellungen und Parameter für genehmigte Microsoft Office Produkte

5.2. Microsoft Office

Microsoft Office unterstützt die Verwaltung über Gruppenrichtlinienobjekte. Um dies zu nutzen, müssen Sie zunächst die entsprechenden Vorlagen von der Microsoft-Website herunterladen und installieren: https://www.microsoft.com/en-us/download

5.2.1 Allgemeine Office-Einstellungen

Dieses Kapitel enthält allgemeine Vorgaben für Microsoft Office.

5.2.1.1 Programm zur Verbesserung der Benutzerfreundlichkeit

Das Programm zur Verbesserung der Benutzerfreundlichkeit von Microsoft muss deaktiviert werden.

5.2.1.2 Begrüßungsassistent

Der Begrüßungsassistent muss beim erstmaligen Ausführen eines Office-Programms deaktiviert werden. Fehlerberichterstattung

Die Fehlerberichterstattung an Microsoft in Office muss deaktiviert werden.

5.2.1.3 Interneteinstellungen

Die Office-Updates werden über WSUS empfangen. Deshalb muss der Zugriff auf Updates, Add-Ins und Patches auf Office.com deaktiviert werden sowie. der Zugriff auf Online-Inhalte muss beschränkt werden. Office-Diagnose

Die Datenträgerdiagnose ist Teil der Office-Diagnose und ermittelt, ob auf der Festplatte des Computers Fehler auftreten oder ob sie Probleme für Office-Anwendungen verursacht. Es kann beispielsweise sein, dass sich eine für die Ausführung von Office-Anwendungen notwendige Datei auf einem fehlerhaften Sektor der Festplatte befindet.

Die Kompatibilitätsdiagnose ist Teil der Office-Diagnose und ermittelt, ob zwischen mehreren auf dem Computer installierten Versionen von Microsoft Office Konflikte bestehen.

5.2.1.4 Vertrauenswürdiger Speicherort

Für Office muss ein vertrauenswürdiger Speicherort etabliert werden. Dieser Speicherort wird als vertrauenswürdige Quelle für das Öffnen von Dateien in Word verwendet. Makros und Code in diesen Dateien werden ohne Warnung an den Benutzer ausgeführt. Wenn Sie diesen Speicherort ändern oder einen weiteren hinzufügen, achten Sie darauf, dass der neue Speicherort gesichert ist und nur die für das Hinzufügen von Dokumenten bzw. Dateien benötigten Benutzer-berechtigungen bestehen.

5.2.2 Gemeinsame Makroeinstellungen

Die Office Applikationen müssen eine Anzeige für die Vertrauenswürdigkeit aller Makros anzeigen, egal ob signiert oder unsigniert.

Alle unsignierten Makros müssen in Outlook generell blockiert werden. Es sind nur Makros zulässig, die von einem vertrauenswürdigen Anbieter signiert sind.

Ebenfalls müssen die Zugriffseinstellungen für Visual Basic-Projekte so angepasst werden, dass den Zugriffen auf Visual Basic-Projekten nicht vertraut wird.

5.2.3 Access-Einstellungen

Die Eingabeaufforderung zur Konvertierung älterer Datenbanken muss deaktiviert werden.

5.2.4 Outlook-Einstellungen

Dieses Kapitel enthält die Einstellungen für Outlook

5.2.4.1 HTML

Benutzer können ein anderes als das Standardformat wählen, wenn sie Nachrichten verfassen.

5.2.4.2 PST-Einstellungen

Das Standardverzeichnis von PST und OST-Dateien muss dem Pfad %userprofile%\ Lokale Einstellungen\Anwendungsdaten\Microsoft\Outlook entsprechen

5.2.4.3 Kalenderoptionen

Die Outlook-Kalenderoptionen müssen den folgenden Anforderungen entsprechen:

- Die Internet Frei/Gebucht-Optionen müssen deaktiviert werden
- Das Roaming von Internetkalendern muss deaktiviert werden.
- Die Internetkalenderintegration muss deaktiviert werden.

5.2.4.4 Outlook als Standard-E-Mail-Client

Outlook muss als Standard-E-Mail-Client forciert werden. Benutzer dürfen nicht in der Lage sein diese Einstellung zu verändern.

5.2.4.5 RSS

Die Standardeinstellungen von Outlook für RSS-Feeds müssen wie folgt angepasst werden:

- Aktivieren der RSS-Funktion
- Aktivieren des außer Kraft setzen des veröffentlichen Synchronisierungsintervalls
- Deaktivieren der Synchronisation des Outlook-RSS-Feeds mit der gemeinsamen Feedliste.

5.2.4.6 Suchoptionen

Die Eingabeaufforderung zur Installation der Windows Desktopsuche in Outlook, sollte die Komponente nicht vorhanden sein, muss deaktiviert werden.

II. Verantwortlichkeiten

II.I Kapitel 1: Client-Sicherheit

Diese Regelung muss von allen Bereichen einzuhalten, die Clients bereitstellen oder verwenden.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.II Kapitel 2: Windows-Clients

Diese Regelung ist von allen Betreibern und Administratoren von Windows-Systemen einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.III Kapitel 3: Unix- bzw. Linux-Clients

Diese Regelung ist von allen Betreibern und Administratoren von Unix- bzw. Linux-Systemen einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.IV Kapitel 4: Mobile Arbeitsumgebung

Diese Regelung muss von allen mobil arbeitenden Mitarbeitern angewandt und eingehalten werden.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.V Kapitel 5: Client-Anwendungen und Standardsoftware

Diese Regelung ist von allen Betreibern und Administratoren von Client-Anwendungen und Standardsoftware einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

A.1.2 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.3 Informationssicherheitshandlungsleitlinien für Mitarbeiter und Mitarbeiterinnen

A.1.4 Informationssicherheit Regelung Nr. 03.01.01 Anti Malware & Systemschutz

A.1.5 Informationssicherheit Regelung Nr. 03.01.08 Change- und Patch-Management

A.1.6 Informationssicherheit Regelung Nr. 03.04.06 Active Directory

A.1.7 Informationssicherheit Regelung Nr. 03.01.14 IT Service Continuity

A.1.8 Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

A.1.9 Informationssicherheitshandlungsleitlinien für Systementwickler

A.1.10 Informationssicherheit Regelung Nr. 03.02.04 Netzwerkzugänge

A.2 Anlagen

A.2.1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

A.3 Quellen und Referenzen

- http://www.pathname.com/fhs/

A.4 Abkürzungen und Definitionen

IT-Notfall	Ein IT-Notfall ist ein IT-Sicherheitsvorfall, der sofortiges Handeln erfordert.
IT-Sicherheitsvorfall	Ein IT-Sicherheitsvorfall ist jedes Ereignis bezogen auf IT-Sicherheit, dass an eine zentrale CERT-Hotline oder an ein CERT gemeldet wurde und Dort weiter verfolgt/protokolliert wird.

A.5 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen.

Nächster Überprüfungstermin: 06.08.2021

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[50].

A.6 Dokumentenhistorie

Version	Name	Org. Unit	Date	Comment
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht

[50] Siehe Anhang A.2.1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Client-Sicherheit

B.1.1 In diesem Zusammenhang ist mit Change-Management der Prozess zur Änderung des Standard Clients gemeint.

B.1.2 In diesem Zusammenhang ist der "Standard Client" definiert als: Basisinstallation des Betriebssystems, welche Programme und Tools für alle Benutzer beinhalten kann.

B.1.3 IT-Services; Bei Sicherheitsrelevanten Einstellungen ist die IT-Sicherheit mit einzubeziehen.

B.1.4 Informationssicherheitshandlungsleitlinie für Mitarbeiter

B.1.5 IT-Sicherheit

B.1.6 IT-Services

B.1.7 Die Freigabe erfolgt durch den jeweils verantwortlichen Lifecycle-Verantwortlichen

B.1.8 Freigabe von Sicherheitspatches:

Der jeweilige Lifecycle-Verantwortliche muss Informationen zu Patches einholen und diese validieren. Die Freigabe erfolgt dann anhand des Prozesses zum Change- und Patch-Management (siehe A.1.5)

B.1.9 IT-Services, bei Produktionsendgeräte die jeweiligen Instandhaltungen und Planungen

B.1.10 IT-Sicherheit

B.2 Kapitel 2: Windows Clients

B.2.1 Keine zusätzlichen Anforderungen

B.2.2 Die Nichtzulassung eines Patches erfolgt anhand der Risikobewertung innerhalb des Change und Patch-Management Prozesses (siehe A.1.5) durch die beteiligten Parteien.

B.2.3 Keine weiteren Details

B.2.4 Keine weiteren Details

B.2.5 Keine weiteren Details

B.3 Kapitel 3: Unix- bzw. Linux-Clients

B.3.1 IT-Sicherheit

B.3.2 IT-Sicherheit

B.4 Mobile Arbeitsumgebung

B.4.1 Unternehmenssicherheit mit Information an den DPO

B.4.2 Beschaffung, IT bzw. bei Produktionsendgeräte die jeweiligen Instandhaltungen und Planungen

B.4.3 IT bzw. bei Produktionsendgeräte die jeweiligen Instandhaltungen und Planungen

B.4.4 Zuständigkeit: Audi AppCenter

B.5 Client-Anwendungen und Standardsoftware

-

C. Settings für Windows Clients

C.1 Minimal Service Configuration

Siehe “Security Settings for Clients” (Anhang zu A.1.4).

C.2 User Rights

Siehe “Security Settings for Clients” (Anhang zu A.1.4).

C.3 Logging

Siehe “Security Settings for Clients” (Anhang zu A.1.4).

C.3.1 Base Configuration

C.3.2 Extended Audit Settings

C.4 Group Policies / Registry Entries

Siehe “Security Settings for Clients” (Anhang zu A.1.4).