Informationssicherheit

IT Systemkomponenten

Regelung Nr. 03.03.01

Server

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Der Zweck dieser Regelung ist die Festlegung der Sicherheitsanforderungen an den Betrieb von Serversystemen.

Im Sinne dieser Regelung bezeichnet der Begriff Informationssicherheit die IT-Sicherheit als Bestandteil der ganzheitlichen Informationssicherheit.

1. Serversicherheit

1.1. Ziel

Das Ziel dieses Kapitels ist die Festlegung notwendiger Informationssicherheits-anforderungen für den Betrieb von Serversystemen. Durch Erfüllung dieser Anforderungen wird eine Basissicherheit erreicht.

Als Server gilt jedes Rechnersystem, das zentral einen oder mehrere Dienste und/ oder Applikationen für andere Rechner (Netzwerk-Clients) über das Netzwerk zur Verfügung stellt. Diese Definition beinhaltet keine Netzwerkkomponenten, Sicherheitsgateways oder Hypervisor Architekturen.

Server im Sinne dieser Regelung sind z.B.:

- Windows-Server
- Unix-Server
- Terminal-Server

1.2. Allgemeine Anforderungen

Serverbetreiber und Unternehmens-Organisationseinheiten, die vom Server zur Verfügung gestellte Services nutzen, müssen gemeinschaftlich die Datenklassifizierung des Servers angeben und dokumentieren[1]. Die Datenklassifizierung wird von den jeweils kritischsten Daten abgeleitet, die sich auf dem Server befinden. Neben den allgemeinen Sicherheitsanforderungen, die in anderen Teilen des Regelwerks für die jeweilige Klassifizierung definiert wurden, gelten für Server folgende Sonderpunkte:

- Server müssen sich in den dedizierten Räumen für IT-Systeme befinden[2], die zur Unterbringung von Servern zugelassen sind.
- Es dürfen nur Serverbetriebssysteme eingesetzt werden, die von der verantwortlichen Einheit[3] für die Serverinfrastruktur genehmigt wurden.

[1] Siehe Anhang A.1.2

[2] Siehe Anhang A.1.12, A.1.13, A.1.14

[3] Siehe Anhang B.1.3

- Weitere unternehmensspezifische Regelungen, die sich auf Serverhosting und -betrieb beziehen[4] müssen beachtet werden.
- Auf den Servern dürfen nur Aktivitäten ausgeführt werden, die unbedingt für den Betrieb oder die Administration der Server notwendig sind. Vorbereitende Aktivitäten müssen auf Clients ausgeführt werden[5].

1.2.1 Besondere Anforderungen für die Integrität

Basierend auf der Datenklassifizierung muss eine Analyse durchgeführt werden, um mögliche Konsequenzen im Falle der Kompromittierung eines Servers zu identifizieren, z. B. wenn ein Angreifer die administrative Kontrolle über einen Server erlangt. Die Analyse muss eine Bewertung des Einflusses und des Plans enthalten, wie die Integrität des Servers und der betroffenen Systeme sichergestellt werden kann.

1.2.2 Besondere Anforderungen für die Verfügbarkeit

Es muss für jeden Service bzw. jeden Server das erforderliche Servicelevel hinsichtlich der Verfügbarkeit (entsprechend der Verfügbarkeitsklassen) und der Wiederherstellungszeit definiert werden. Dieser muss von den SLAs der Services abgeleitet werden, die vom Server bereitgestellt werden.

Für jede Verfügbarkeitsklasse müssen den Verfügbarkeitsanforderungen entsprechende Eskalationsprozesse definiert werden, welche die folgenden Punkte enthalten müssen:

- Ereignisse, die Eskalationsprozesse auslösen (z. B. Erkennen von Ausfällen durch das Systemmanagement).
- Wiederherstellprozesse und tatsächliche Wiederherstellzeiten des Servers, inklusive der Dienste und Daten.
- Maximal zulässige Dauer für Diagnose oder Fehlerbehebung.
- Verantwortlichkeiten für jeden Prozessschritt.
- Verfügbarkeiten und Kontaktdaten des Verantwortlichen für jeden Prozessschritt.
- Die Eskalationskette muss dokumentiert sein.

In Abhängigkeit von den Verfügbarkeitsanforderungen müssen geeignete technische Maßnahmen umgesetzt werden.

Wartungsverträge für Server mit Dienstleistern müssen entsprechend der geforderten Service Level abgeschlossen werden.

Es dürfen nur Server-Betriebssysteme eingesetzt werden, die durch die für Server Infrastruktur zuständige Stelle freigegeben sind.

[4] Siehe Anhang B.1.4

[5] Dies beinhaltet z.B. das Herunterladen von Patches, Surfen im Internet, Lesen von Anleitungen und Tätigkeiten die Verwendung oder Installation von auf Servern unzulässiger Software wie Apple QuickTime, CA AV Engine, Adobe Reader, Mozilla, Firefox beinhaltet

Gesellschaftsspezifische Regelungen zum Betrieb und Hosting von Servern müssen berücksichtigt werden.

Alle physikalischen Server müssen mit mindestens zwei LAN-Schnittstellen betrieben werden.

Der Einsatz von SAN (Storage Area Network) zum Speichern aller Nutzdaten wird gewöhnlich empfohlen.

Die Speicherung und Übertragung von Daten muss gemäß ihrer Klassifizierung[6] erfolgen.

1.3. System-Realisation

1.3.1 Installation

Installation und Basiskonfiguration muss offline oder in einer sicheren Netzwerkumgebung (Installationsnetzwerk) durchgeführt werden, falls der Server in Verbindung mit dem Internet oder in nicht vertrauenswürdigen Netzen eingesetzt werden soll.

Die Authentizität und Integrität der Installationsquelle muss sichergestellt und aktuell gehalten werden (Image Maintenance).

Die Herstelleranweisungen zur Installation müssen berücksichtigt werden.

Falls systembezogene Nutzerkennungen[7] für Installationszwecke verwendet werden (z. B. für geteilte Zugriffe, Beitritt zur Domäne) dürfen die entsprechenden Passwörter nicht im Klartext in Antwortdateien (Skripte zur unbeaufsichtigten Installation, post-install scripts, etc.) bereitgestellt werden. Installations-Accounts sollten nur über minimale Rechte verfügen und müssen so konfiguriert sein, dass Missbrauch für andere Zwecke verhindert wird. Die Verwendung systembezogener Nutzerkennungen für Installationszwecke muss dem verantwortlichen Administrator zuzuordnen sein.

Prinzipiell dürfen nur Software-Komponenten oder Pakete installiert werden, die erforderlich sind um den Server zu betreiben und zu administrieren und um die eigentlichen Dienste bereitzustellen. Es dürfen auf produktiven Systemen keine Entwicklungswerkzeuge, Beispieldaten, Netzwerkanalyse-Werkzeuge oder ähnliches installiert sein, sofern dies nicht für den eigentlichen Zweck des Servers erforderlich ist.[8]

Nach der Installation muss das Betriebssystem überprüft werden und alle nicht benötigten Komponenten müssen deinstalliert werden.

Jeder Server sollte nur eine Rolle ausüben (einen spezifischen Dienst bereitstellen). Ausnahmen können in Einzelfällen sinnvoll sein, z.B. bei Infrastruktur-Diensten oder virtuellen Umgebungen. Wenn mehrere Services auf demselben Server implementiert

[6] Siehe Anhang A.1.1

[7] Wie definiert in A.1.2

[8] Die beinhaltet die Nutzung und Installation von Software wie Apple QuickTime, CA AV Engine, Adobe Reader, Mozilla Firefox

werden, müssen diese auf Kompatibilität, Einfluss potenzieller Gefährdungen und Datenklassifikation geprüft werden.

Das System muss vor dem produktiven Einsatz mit aktuellen Sicherheitspatches aktualisiert werden. Die Installation muss im Installationsnetzwerk oder in einem geschützten Netzwerk erfolgen. Die Grundinstallation zum Schutz vor Schadsoftware[9] muss im Installationsnetzwerk erfolgen und dort aktualisiert werden.

Es muss ein geeignetes Lizenzmodell ausgewählt werden. Die Beschaffung von Lizenzen muss dokumentiert und regelmäßig überprüft werden, damit Anzahl und Art der Lizenz den zugehörigen Lizenzprogrammen entsprechen.

Der Installationsprozess und der Basiskonfigurationsprozess müssen verständlich und klar dokumentiert sein.

1.3.2 Konfiguration und Systemhärtung

1.3.2.1 Allgemeine Anforderungen

Die Serverzeit muss regelmäßig über die AUDI NTP-Infrastruktur synchronisiert werden.

Der automatische Start von Wechselmedien (“Autorun”) muss deaktiviert werden.

Die automatische Sperrung von interaktiven Verbindungen auf Servern ist grundsätzlich zu implementieren. Die Verbindung muss bei Inaktivität nach einem definierten Zeitraum (höchstens 10 Minuten) gesperrt werden. Die Sperre darf nur nach einer angemessenen Benutzerauthentifizierung (z. B. Passwort, PKI-Karte, etc.) aufgehoben werden.

Alle nicht autorisierten Kommunikationsversuche durch das Betriebssystem müssen verhindert werden (z. B. müssen „Phone Home“-Funktionen deaktiviert werden).

In der Regel dürfen Server nicht über Internet kommunizieren, mit Ausnahme der Server, die für Internetservices dediziert sind.[10]

Wenn das Betriebssystem erweiterte Schutzfunktionen (z.B. ASLR, DEP, etc.) zur Verfügung stellt, muss eine Aktivierung abgewogen werden. Wenn die Abwägung zu einer negativen Entscheidung führt, müssen die Entscheidung und die Gründe dafür dokumentiert werden.

Jede Beschriftung oder Etiketten mit sensiblen Informationen (z.B. ILO Mgt. Informationen) dürfen nicht für unautorisierten Personen sichtbar sein und sind, falls erforderlich, zu entfernen.

Die Anforderungen der Regelung Systemschutz[11] (speziell Security Settings zur Systemhärtung) müssen beachtet werden.

---

[9] Siehe Kapitel 1.3.2.7

[10] Siehe Anhang A.1.12

[11] Siehe Anhang A 1.5

1.3.2.2 Netzwerk

Server dürfen nur nach Freigabe der zuständigen Stelle[12] an das Netzwerk angeschlossen werden.

Es dürfen nur freigegebene Netzwerkprotokolle eingesetzt werden[13].

Alle anderen Kommunikationsprotokolle müssen abgeschaltet werden[14].

Statische IP-Adressen müssen verwendet werden.

Es dürfen nur unbedingt erforderliche statische Routen (z.B. für administrative Zugriffe oder Zugriffe auf Datenbanken) vorhanden sein. Mit Ausnahme von Wartungs-, Administrations-, und Storage-Netzwerken dürfen Server nicht an Netze unterschiedlicher Sicherheitsniveaus angeschlossen werden. Routing-Funktionen müssen deaktiviert werden.

Nicht benötigte Netzwerkschnittstellen sind abzuschalten. An im Netzwerk betriebene Rechner dürfen keine Geräte angeschlossen werden, die Verbindungen in weitere Netze ermöglichen (Ausnahme: Konsolen unter entsprechenden Sicherheitsvorkehrungen). Werden (in zu genehmigenden Ausnahmen) solche Geräte betrieben, sind spezielle Sicherheitsvorkehrungen zu treffen.

Alle administrativen Verbindungen müssen verschlüsselt werden. Authentifizierungsdaten müssen verschlüsselt übertragen werden. Die Regelung Kryptographie[15] und die Datenklassifizierung[16] der übertragenen Daten muss bei der Auswahl geeigneter kryptographischer Maßnahmen berücksichtigt werden.

1.3.2.3 Dienste

Es dürfen nur die erforderlichen Dienste installiert und gestartet sein. Für diesen Zweck vorhandene Dienstbenutzer-Konten müssen mit so wenig Rechten wie nötig angelegt werden. Dienstbenutzer-Konten dürfen keine Rechte zur interaktiven Anmeldung am Server haben. Konten mit lokaler oder globaler administrativer Autorisierung (Root, Administrator, Domänenadmin-Konten usw.) dürfen nicht verwendet werden, um Anwendungen zu starten, oder Anwendungen müssen direkt nach dem Start Rechte abgeben, sodass sie als nicht privilegierte Konten ausgeführt werden. Falls es notwendig ist, solche Accounts dazu zu verwenden, müssen diese Ausnahmenutzungen dokumentiert und freigegeben werden. Genehmigte Ausnahmen sind in Anhang C aufgelistet. Spezielle Vorsichtsmaßnahmen müssen vorhanden seien.

Dienste, die eine Authentifizierung im Klartext erfordern, müssen durch sichere Dienste ersetzt werden.

---

[12] Siehe Anhang B.1.4

[13] Siehe Anhang A.1.12

[14] Ausnahme: Voice over IP, siehe Anhang A.1.4

[15] Siehe Anhang A.1.6

[16] Siehe Anhang A.1.1

Die benötigten Protokolle und Dienste auf einem Server sind von den zuständigen Stellen[17] zu definieren und genehmigen. Dabei sind grundsätzlich die jeweils sichersten Versionen der Protokolle und Dienste zu verwenden. Hierbei muss das Anwendungsgebiet und die Datenklassifizierung[18] beachtet werden.

Die Liste der erlaubten Dienste eines Servers muss in einer Positivliste klar und verständlich dokumentiert werden. Vor Inbetriebnahme und nach Installation aller Applikationen muss überprüft und sichergestellt sein, dass keine unerlaubten Dienste vorhanden oder aktiviert sind.

1.3.2.4 Dateisystem

Zugriffsrechte auf das Dateisystem müssen auf ein Mindestmaß begrenzt werden (Least Privilege und Need-to-Know Prinzip). Nur Administrator-, Patch Management Accounts, Recovery Operators und systembezogene Nutzerkennungen dürfen (falls erforderlich) Schreibrechte auf Dateien des Server-Betriebssystems erhalten.

Daten müssen strukturiert verwaltet werden. Systemdateien und Nutzdaten müssen auf unterschiedlichen Partitionen gespeichert werden.

Zugriffsberechtigungen müssen in regelmäßigen Abständen entsprechend der Regelung zum Access und Identity Management[19] überprüft werden.

1.3.2.5 Authentisierung[20]

Sofern technisch möglich, müssen administrative Anmeldungen über starke Authentifizierung (z.B. PKI mit PIN, SecurID) erfolgen. Authentisierungsinformationen müssen verschlüsselt übertragen werden.

Authentisierungsinformationen dürfen nicht zwischengespeichert werden.

Alle existierenden Standard-Benutzerkonten müssen gelöscht, deaktiviert oder gesichert (z.B. mit zufälligen Einmalpasswörtern in Password-Safes und nachvollziehbarem Zugriff). Lokale Konten müssen einem Benutzer zugeordnet sein (Ausnahme Notfallkonten). Die Anzahl lokaler Konten muss auf ein Minimum beschränkt werden. Passwörter für lokale Konten müssen auf jedem Server einzigartig sein[21]. Alle Benutzer müssen explizit authentisiert werden bevor sie Zugriff auf Informationen erhalten, die sich auf dem System befinden oder durch dieses bereitgestellt werden.

Informationen über den letzten angemeldeten Benutzer (z. B. Benutzer-ID) dürfen bei einer Anmeldeaufforderung nicht angezeigt werden.

---

[17] Siehe Anhang B.1.6

[18] Siehe Anhang A.1.1

[19] Siehe Anhang A.1.8

[20] Die Anforderungen der folgenden Regelungen im Anhang müssen beachtet werden: A.1.8 und A.1.1

[21] DB2: System Security Settings zu dieser Technologie beachten

1.3.2.6 Autorisierung

Die Benutzerrechte müssen gemäß der Rolle des Benutzers auf ein notwendiges Minimum beschränkt werden[22]. Insbesondere müssen technische Accounts betrachtet werden und deren Berechtigungen, mit den vom Betriebssystem zur Verfügung gestellten Optionen, eingeschränkt werden.

Von Benutzern und Applikationen benötigte Berechtigungen müssen Rollen zugewiesen werden. Accounts müssen diesen Rollen entsprechend zugeordnet werden. Das direkte Zuweisen von Berechtigungen an Accounts ist nicht zulässig. Für Rollen und Accounts müssen zentrale Verzeichnisdienste gegenüber lokalen Datenbanken bevorzugt werden.

1.3.2.7 Schutz gegen Schadsoftware

Ein Schutz vor Schadsoftware ist unter Einhaltung der Vorgaben der Systemschutzregelung[23] zu implementieren.

1.3.2.8 Host Intrusion Detection System (HIDS)/ Lokale Firewall

Server, die sich in Netzwerken mit erweitertem Schutzbedarf (Hochsicherheitsumgebungen) befinden, müssen mit installierten HIDS Sensoren versehen werden. Auf diesen Servern sind unsichere Dienste, die nicht abgeschaltet oder durch sichere Dienste ersetzt werden können, durch HIDS besonders zu überwachen.

Bei hohem Schutzbedarf muss eine lokale Firewall verwendet werden.

1.3.2.9 Protokollierung

Die Protokollierung muss auf allen Servern entsprechend der Vorgaben der Regelung zur Protokollierung[24] umgesetzt sein.

1.3.3 Kryptographie

Die Vorgaben der Kryptographie-Regelung[25] müssen eingehalten werden. Server-Betriebssysteme werden mit vorinstallierten Zertifikaten zum Überprüfen der Authentizität und Integrität von Dateien des Betriebssystems, der Authentizität von Remotesystemen für Updates oder ähnlichen Zwecke ausgeliefert. Diese vorinstallierten Zertifikate müssen überprüft werden. Werden diese nicht benötigt müssen sie entfernt werden.

1.3.4 Test und Freigabe

Server dürfen in produktiven Umgebungen nur nach erfolgreichem Test gegen den Anforderungskatalog[26] betrieben werden.

---

[22] Siehe Anhang B.1.1

[23] Siehe Anhang A.1.5

[24] Siehe Anhang A.1.7

[25] Siehe Anhang A.1.6

[26] Siehe Anhang A.1.5

Alle Sicherheitskonfigurationen und Änderungen am Server müssen vom Betreiber angemessen in einer Testumgebung getestet werden. Software-Produkte müssen vor der Produktivsetzung und während des Lebenszyklus getestet werden.

Server dürfen nur nach Freigabe durch die zuständige Stelle[27] an das Netzwerk angeschlossen werden.

1.3.5 Dokumentation

Der Standard-Server ist vom Betreiber der Server in separaten Dokumenten zu definieren und zu beschreiben.

Alle Maßnahmen, die den Standard-Server verändern, müssen dokumentiert werden.

Die Dokumentation sollte u. a. folgende Punkte beinhalten:

- Im Netzwerk angebotene Services, einschließlich benötigter Netzwerkprotokolle und-Ports
- Installierte Software, einschließlich Versionen
- Lokale Benutzer, deren Zweck und verantwortliche Person
- Verantwortliche Personen für den Server
- Laufende Prozesse
- Tasks (inklusive geplante Tasks für lokale Konten)

1.4. Betrieb

Es muss ein Administrationskonzept vorliegen. Dieses Konzept muss mindestens folgende Aspekte umfassen:

- Die bestehenden Typen der administrativen Rollen
- Wie diese Rollen technisch implementiert werden (z. B. innerhalb von AD)
- Welche Rolle auf welche Komponenten zugreifen kann
- Einschränkungen und Zugriffsarten, mit denen Administratoren auf die zu verwaltenden Server zugreifen (Fernzugriff, lokal, Authentifizierung)
- Zugelassene Administrationstools
- Workflows für administrative Aufgaben (z. B.: Wird sichergestellt, dass alle administrativen Aufgaben mit denselben Standards ausgeführt werden?)
- Stellen Sie sicher, dass eine Gefährdung eines nicht administrativen Benutzerkontos nicht das Administratorkonto desselben Benutzers beeinflusst.
- Aufgaben für die Verwendung lokaler Tools
- Aufgaben für die Verwendung zentraler Lösungen

[27] Siehe Anhang B.1.7

- Konten, die zum Dokumentieren von Änderungen verwendet werden
- Benötigtes Wissen/benötigte Qualifikation zum Ausführen administrativer Aufgaben
- Der Prozess zum Bereitstellen und Ablehnen administrativer Rechte (Unterschied zwischen internen und externen Mitarbeitern)
- Steuern und Überwachen administrativer Aktionen (wer und wie)
- Spezielle Protokollierung für Administratoren

1.4.1 Administrative Zugriffe

Nur entsprechend ausgebildete und auf den Datenschutz verpflichtete Mitarbeiterinnen und Mitarbeiter dürfen Server administrieren. Die Administratoren müssen entsprechend gesellschaftsspezifischer Prozesse geschult werden.

Um die Nachweisbarkeit sicherzustellen, müssen personalisierte Accounts zur Administration von Servern verwendet werden. Die Administratoren dürfen keine normalen Benutzertätigkeiten mit administrativen Berechtigungen ausführen.

Um administrative Zugriffe abzusichern, müssen mindestens die folgenden Punkte implementiert werden:

- Sofern technisch möglich, müssen administrative Dienste und Protokolle (SSH, RDP, SMB) auf produktiven Netzwerkinterfaces deaktiviert werden und nur auf administrativen Netzwerkinterfaces zur Verfügung stehen (Management-Netzwerk).
- Administrative Schnittstellen (Terminals, Konsolen, etc.) müssen exklusiv auf administrative Gruppen beschränkt werden.
- Der Zugriff muss durch Netzwerkzonierung beschränkt werden (Zugriff auf Management-Netzwerke muss auf Administratoren beschränkt sein).
- Administration muss über Management-Netzwerke erfolgen.
- Soweit technisch möglich, muss über verschlüsselte Verbindungen administriert werden.
- Nach Beendigung administrativer Tätigkeiten müssen alle interaktiven Verbindungen beendet werden.

1.4.2 Überwachung

Server-Hardware und Software muss durch geeignete Maßnahmen überwacht werden, um Auswirkungen auf die Verfügbarkeit, Integrität, Vertraulichkeit und Nachweisbarkeit zu verhindern oder zu minimieren.

Folgenden Punkte müssen abgedeckt werden:

- Hardware (Prozessor, RAM, Massenspeicher)
- Betriebssystem (kritische Dienste, Ressourcen-Verbrauch, Sicherheitsrelevante Ereignisse)
- Dienste/Applikationen (Latenz, Last, Verfügbarkeit)

- Server Health (Temperatur, Komponenten)

1.4.3 Reporting

Es müssen Maßnahmen getroffen werden um die folgenden Berichte sowohl auf Anfrage als auch regelmäßig (z. B. wöchentlich) generieren zu können:

- Inventory, Differenzen SOLL/IST
- Patchlevel
- Prozentual erfolgter Rollout (z. B. Hotfix-Verteilung).
- Vorfälle (z. B. Art/Anzahl von Angriffen).

1.4.4 Überprüfungen der Sicherheit

Server müssen regelmäßigen Überprüfungen der Sicherheit unterzogen werden. Im Vorfeld muss sich der Betreiber eine Übersicht über aktuelle Sicherheitslücken des Serversystems verschaffen.

Die Überprüfung der Sicherheit muss mindestens die folgenden Punkte abdecken. Wenn möglich, sollten regelmäßige Prüfungen auf Basis von automatisierten Berichten erfolgen:

- Sind die erforderlichen und geplanten Schutzmaßnahmen aktiv und effektiv?
- Sind Accounts für Benutzer aktiv, die keinen Zugriff mehr benötigen? Identifizierte Accounts müssen bereinigt werden.
- Welche Accounts haben administrative Privilegien?
- Sind Accounts vorhanden, die über nicht benötigte Privilegien verfügen? Identifizierte nicht benötigte Privilegien müssen entfernt werden.
- Wer außer den Administratoren kann auf Dateien auf Betriebssystem-Ebene zugreifen?
- Welche Accounts können Daten auf dem Server verändern?
- Verfügt der Server über ausreichend Ressourcen zum Erbringen des vereinbarten Service Level zur Verfügbarkeit, Vertraulichkeit, Integrität und Nachweisbarkeit?
- Ist der Server / das System frei von Schadsoftware?
- Sind der Zustand und die Ausstattung der Hardware zufriedenstellend?
- Ist das System auf einem aktuellen Stand (sind alle empfohlenen Patches installiert)?
- Befinden sich auf dem Server Daten die gemäß des Betriebs- und/oder Sicherheitskonzepts unzulässig sind? Identifizierte Daten müssen entfernt werden.
- Existiert ein angemessener Wartungsplan?
- Sind die erforderlichen Garantie- und Wartungsvereinbarungen noch gültig und entsprechen den aktuellen Service Level, rechtlichen und vertraglichen Anforderungen?
- Welche auf dem System laufenden Dienste sind über das Netzwerk erreichbar? Sind diese entsprechend dieser Regelung konfiguriert?
- Entsprechen die Sicherheitsattribute (ACLs) von

- Systemprogramme und Systemkonfigurationen,
- Applikationsprogramme und -Daten,
- Benutzerverzeichnissen und -Daten

dieser Regelung?

- Sind Systemprogramme und Systemkonfigurationen unverändert und konsistent[28]?

1.4.5 Änderungsverwaltung[29]

1.4.5.1 Softwareverteilung

Managementtools und Software-Verteilungsmechanismen müssen die folgenden Funktionalitäten haben und die folgenden Voraussetzungen erfüllen:

- Modularer Aufbau der Softwarepakete (nur einzelne Applikationen, nicht das komplette System-Image)
- Verteilung von Sicherheitssoftware
- Verteilung von Malware Signaturen/Definitionen
- Einspielen von Service-Packs, Patches, Hotfixes, etc.
- Verteilen von Policies (Konfiguration/Regeln) für Betriebssystem, Anwendungen, Management- und Monitoring-Tools und Sicherheitsprodukte.
- Verteilungen/Installationen müssen erzwungen werden können ohne Abbruchmöglichkeit des Benutzers.
- Für Server die im laufenden Betrieb kein Reboot durchgeführt werden dürfen, muss ein spezielles Verfahren festgelegt werden.
- Möglichkeit eines sofortigen „Pushens“, damit im IT-Notfall sofort Gegenmaßnahmen ergriffen werden können
- Rückmeldungen bei erfolgten und fehlgeschlagenen Ereignissen.
- Nicht erreichbare Server müssen umgehend nachgezogen werden können, sobald sie wieder am Netz sind.
- Integrität verteilter Software muss für jeden Bereitstellungsendpunkt verifiziert werden
- Rollen und Rechtekonzept (und, falls erforderlich, Mandantenfähigkeit)
- Mechanismen müssen sicherstellen, dass nur autorisiertes Personal das Rollout für Softwareaktualisierungen durchführen darf

Zentrales Management:

- Bei Einsatz von Simple Network Management Protocol (SNMP) sind die Community-Strings entsprechend der Anforderungen für Passwörter[30] konfiguriert werden.
- Der Dienst SNMP Version 1 muss grundsätzlich abgeschaltet sein.

[28] Die Dokumentation der Ergebnisse ist erforderlich.

[29] Siehe Anhang A.1.10

[30] Siehe Anhang A.1.2

- Der Einsatz von SNMP Version 3 muss bevorzugt werden. Die Community-Strings sind zu verschlüsseln.

1.4.5.2 Konfigurations-Management

Die folgenden Server-Informationen müssen ad hoc (wenn online der aktuelle Stand, wenn offline der Stand vom letzten online) eingeholt werden können:

- Betriebssystem, Version und Patch Level
- Standard-Software-Programme, Version und Patch Level
- Sicherheitsprodukte (z. B. Virenschutz), Version, Patch Level und Erkennungsdatenbank
- Installierte sowie aktivierte Dienste
- zusätzlich installierte Nicht-Standardprogramme
- Freier und verfügbarer Festplattenplatz
- Kontaktdaten wie Standort, Ansprechpartner/Administrator, etc.
- Protokoll- und Auditing-Konfiguration[31]

1.4.5.3 Patch Management

Es müssen geeignete Verfahren umgesetzt werden, um Server regelmäßig und sofort bei kritischen Aktualisierungen, mit Updates zu versehen[32]. Hierzu muss der Administrator zu anderen Quellen (z. B. Sicherheitsempfehlungen von VW CERT[33]) auch Ressourcen des Herstellers nutzen und regelmäßig einen Überblick über bekannte Verwundbarkeiten des Systems haben.

Bevor Patches und Updates installiert werden muss eine Sicherung durchgeführt und überprüft werden, um eine Rücksicherung auf den aktuellen Stand zu ermöglichen.

Produktive Systeme dürfen nur nach erfolgten Test und erfolgter Freigabe in einer Entwicklungs-/Test-/Integrationsumgebung aktualisiert werden. Zu diesem Zweck muss eine Testumgebung, die der produktiven Umgebung weitest möglich entspricht, verfügbar gemacht werden.

Alle Änderungen müssen in einer klaren und verständlichen Form (dem Change Management entsprechend) dokumentiert werden, um einen fehlerfreien Betrieb zu gewährleisten. Der Change-Management-Prozess[34] muss von der zuständigen Stelle[35] festgelegt sein.

---

[31] Siehe Anhang A.1.7

[32] Die Anforderungen des Anhangs A.1.10 müssen beachtet werden.

[33] https://cert.vw.vwg/cms/en/security-advisories

[34] Siehe Anhang B.1.2

[35] Siehe Anhang B.1.8

1.4.5.4 User Administration

Alle lokalen und Domänen-Accounts[36] müssen entweder auf dem System vom Administrator angelegt und gelöscht werden oder durch ein zentrales Access und Identity Management System, welches von der zuständigen Stelle freigegeben wurde.

Automatisches Anlegen, Löschen, Aktivieren oder Deaktivieren lokaler Accounts ist nicht zulässig. Abweichungen von dieser Regelung sind nur in Ausnahmefällen zulässig (z.B. Installationsroutinen, die Nutzer anlegen) und müssen dokumentiert werden. Der Systemadministrator muss festlegen, welche Accounts angelegt sein dürfen und angelegt oder gelöscht werden sollen.

Das Anlegen von lokalen oder Domänen-Accounts muss dokumentiert werden. Diese Dokumentation muss regelmäßig überprüft und aktuell gehalten werden.

Alle nicht verwendeten lokalen Benutzeraccounts müssen im Rahmen von regelmäßigen Wartungsmaßnahmen oder Überprüfungen der Sicherheit, entfernt werden. Die Anforderungen zur Erstellung von Passwörtern[37] müssen beachtet werden.

1.4.5.5 Reparatur

Die folgenden Minimalanforderungen an die Prozesse für Reparatur, Entsorgung, Auslieferung müssen erfüllt sein:

- Vor der Reparatur muss sichergestellt werden, dass auf Daten nicht durch unautorisierte Personen zugegriffen werden kann (z. B. durch Verschlüsselung, sicheres Löschen[38] und/oder vergleichbare sichere Verfahren, oder durch spezielle vertragliche Vereinbarungen mit der Reparaturfirma). Dies ist nicht notwendig, wenn die Reparatur vor Ort erfolgt und beaufsichtigt wird.
- Bei der Entsorgung sind die Anforderungen aus Kapitel 1.5.1 zu beachten.
- Nach Reparatur ist wieder der aktuelle Sicherheits- und Datenstand herzustellen.

Gesellschaftsspezifische Regelungen müssen beachtet werden.

1.4.5.6 Aktualisieren der Dokumentation

Die Systemdokumentation muss im Rahmen des Change Managements[39] dem aktuellen Stand gehalten werden.

1.4.6 Backup und Widerherstellung von Daten

Backup und Wiederherstellung von Servern muss entsprechend der Regelungen zum Backup und Archivierung[40] umgesetzt und regelmäßig überprüft werden.

---

[36] Beim Erstellen von Benutzeraccounts müssen die Anforderungen des Anhangs A.1.8 beachtet werden.

[37] Siehe Anhang A.1.2

[38] Siehe Kapitel 1.5.1

[39] Siehe Anhang A.1.10

[40] Siehe Anhang A.1.9

Dies gilt sowohl für das komplette Systemabbild als auch für wichtige Systemeinstellungen und Systemkomponenten. Die Art, Häufigkeit, Vorhaltezeit, Speicherort und Zustand des Backups sowie weiterer Backup-Parameter muss dem mit den Dienstnutzern vereinbarten Service-Level und dem durch die Datenklassifikation geforderten Sicherheitsniveau entsprechen.

Die Fachabteilungen müssen die Möglichkeit haben, die Fehlerfreiheit der Wiederherstellung zu prüfen.

Wiederherstellprozeduren müssen das System auf den mit den Dienstnutzern vereinbarten Stand (RPO: Restore Point Objective) innerhalb der vereinbarten Wiederherstellzeit (RTO: Restore Time Objective) wiederherstellen.

Der gesamte Prozess muss dokumentiert, regelmäßig getestet und falls nötig verbessert werden. Dienstnutzer müssen in die Wiederherstelltests eingebunden werden, wenn der Wiederherstellungserfolg beurteilt werden muss.

Die Wiederherstellprozeduren (Disaster Recovery) müssen dokumentiert und regelmäßig getestet werden. Die Tests müssen dokumentiert werden.

1.4.7 Archivierung

Gesellschaftsspezifische Regelungen[41] müssen beachtet werden.

1.4.8 Datenübertragung

Es gelten die Regelungen der “Informationssicherheit Handlungsleitlinien für Mitarbeiterinnen und Mitarbeiter”[42].

1.5. Außerdienststellung

Im Falle der Außerdienststellung müssen die folgenden Punkte berücksichtigt werden:

- Backups von Daten, die noch benötigt werden
- Bereitstellung von angemessenen Ersatzsystemen (falls nötig)
- Benachrichtigung der Dienstnutzer (wer ist betroffen?)
- Entfernen von Referenzen in anderen Systemen (z.B. DNS, DHCP, directory services, PKI)
- Sichere Entsorgung von Daten
- Sichere Entsorgung von Backup-Datenträgern
- Entfernen weiterer Informationen (z.B. Beschriftungen an der Hardware)
- Sperren von Systemzertifikaten
- Löschen von zugehörigen Management-Accounts des Systems

[41] Siehe Anhang A.1.1

[42] Siehe Anhang A.1.1

- Aktualisierung der Dokumentation für Notfall- und Disaster Recovery Prozeduren

1.5.1 Sicheres Löschen von Datenträgern

Bei der Entsorgung müssen alle Daten unwiederbringlich zerstört werden (z. B. physikalische Zerstörung der Datenträger, sicheres Löschen[43] oder vergleichbar sichere Verfahren, durch spezielle vertragliche Regelungen, die mit der Entsorgungsfirma festgelegt werden müssen).

Datenträger müssen sicher gelöscht oder zerstört werden. Es muss sichergestellt sein, dass die Daten mit hoher Wahrscheinlichkeit nicht wiederhergestellt werden können[44].

Datenträger können beispielsweise durch einen Schredder mechanisch zerstört werden.

Das angewendete Verfahren und die Auswahl einer angemessenen Entsorgungsfirma muss durch die verantwortliche Stelle genehmigt werden.

1.5.2 Entsorgung von Hardware

Vor der Entsorgung von Systemhardware müssen alle Daten entfernt werden.

Alle zusätzlichen Informationen (z.B. Beschriftungen) müssen entsprechend der Datenklassifikation entfernt werden.

1.6. Notfall

1.6.1 Notfallplanung

Es gelten die Anforderungen der Regelung IT Service Continuity[45].

Es muss ein Notfallplan für den Ausfall eines Servers muss erstellt werden. Dieser Plan muss mindestens die folgenden Punkte beinhalten:

- Backup der Daten
- Technische Dokumentation
  - BIOS und Firmware Versionen
  - Hardwareausstattung
  - Installierte Komponenten / Pakete
  - Installierte Software
  - Netzwerkkonfiguration
  - Dienste
  - Partitionierung von Massenspeichern
  - Benutzeraccounts und Gruppen mit Autorisierungen
  - Freigaben und Freigabeberechtigungen, Dateisystem-Berechtigungen

[43] Siehe Anhang A.1.1

[44] Siehe Anhang A.1.1

[45] Siehe Anhang A.1.11

  - Sicherheitseinstellungen
- Redundanz oder alternativer Betrieb
- Anweisungen zum Neustart
- Test eines Notfallplans
- Wiederherstellung

Zu Wiederherstellzwecken müssen Notfalldatenträger zum Booten verfügbar sein und ein definiertes Verfahren zur Wiederherstellung muss für den Server dokumentiert sein.

Wiederherstellungsverfahren müssen dokumentiert sein und regelmäßig getestet werden. Die Tests müssen dokumentiert werden.

II. Verantwortlichkeiten

II.I Kapitel 1: Serversicherheit

Diese Regelung ist von allen Betreibern von IT-Systemen anzuwenden und 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 Mitarbeiterinnen und Mitarbeiter

A.1.2 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

A.1.3 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.4 Informationssicherheit Regelung Nr. 03.02.03 Internet-Telefonie/Video-Telefonie

A.1.5 Informationssicherheit Regelung Nr. 03.01.01 Anti Malware & Systemschutz

A.1.6 Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

A.1.7 Informationssicherheit Regelung Nr. 03.01.04 Sicherheitsprotokollierung und -monitoring

A.1.8 Informationssicherheit Regelung Nr. 03.01.05 Authentifizierung und IAM

A.1.9 Informationssicherheit Regelung Nr. 03.01.06 Backup und Archivierung

A.1.10 Informationssicherheit Regelung Nr. 03.01.08 Change- und Patch-Management

A.1.11 Informationssicherheit Regelung Nr. 03.01.14 IT Service Continuity Management

A.1.12 Informationssicherheit Regelung Nr. 03.01.19 Virtualisierung

A.1.13 Informationssicherheit Regelung Nr. 03.05.01 Physischer Schutz

A.1.14 Informationssicherheit Regelung Nr. 03.01.16 Dienstleistungserbringung durch Dritte

A.2 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zu den Standards ISO/IEC 27001:2013, ISO/IEC 27001:2005 und VDA.

Thema	Kapitel	ISO 27001:2013	ISO 27001:2005	VDA

Documented operating procedures	1.3.4	A.12.1.1	A.10.1.1	-
Installation of software on operational systems	1.3.1	A.12.5.1	-	-

A.3 Anlagen

A.3.1 Anlage 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.4 Abkürzungen und Definitionen

In diesem Abschnitt werden ausschließlich Begriffe und Abkürzungen aus dem Informationssicherheitsbereich definiert. Begriffe und Abkürzungen aus anderen Bereichen werden durch die dafür verantwortlichen Stellen definiert.

Abkürzung/Begriff	Erklärung
ACL	Access Control List, Zugriffssteuerungsliste – Software-Technik, mit der Betriebssysteme und Anwendungsprogramme Zugriff auf Daten und Funktionen eingrenzen können.
ASLR	Computer Security Technik zur Verhinderung von Buffer Overflow Attacken durch eine zufällige Anordnung der Address Space Positionen der Key data areas eines Prozesses

Authentisierung	Überprüfung, ob ein Kommunikationspartner (Person oder System) wirklich der ist, für den er sich ausgibt.
Autorisierung	Zuweisung und Überprüfung von Benutzerrechten für den Zugriff auf Daten oder Diensten. Autorisierung geschieht oft nach einer erfolgreichen Authentisierung.
DEP	Datenausführungsverhinderung – Sicherheitsfunktion von Windows 7, die dazu beiträgt Beschädigungen des Systems durch Viren oder andere sicherheitsrelevante Vorfälle zu vermeiden.
Disaster Recovery	Wiederherstellungsprozedur nach einem Vorfall in der IT (z.B. Datenwiederherstellung, Ersatz von nicht mehr benutzbarer Infrastruktur)
Firewall	Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
HIDS	Host Intrusion Detection System - Host-basierte IDS: System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen (HIDS) und so die Sicherheit von Netzwerken erhöhen.
PKI	Public-Key-Infrastructure – Ein System, das digitale Zertifikate ausstellt, verteilt und prüft. Es dient zur Absicherung rechnergestützter Kommunikation.
Positivliste	Auch Whitelist oder weiße Liste. Umfasst in der IT – im Gegensatz zu einer Schwarzen Liste – die Quellen und Ressourcen, welche nach Meinung der Verfasser der Liste vertrauenswürdig und unschädlich sind.
SecurID	Mechanismus, um eine 2-Faktor Authentifizierung eines Benutzers gegenüber einer Netzwerk-Ressource durchzuführen. Ist auch bekannt als RSA SecurID.
Sicherheitsgateway	Ein Sicherheitsgateway ist ein System aus Software- und Hardwarekomponenten zur sicheren Verbindung von IT-Netzwerken (z. B. einige IT-Systeme mit verschiedenen Aufgaben wie Paketfilterung, Virenschutz oder Überwachung von Netzwerkverkehr).
SSH	Secure Shell – Netzwerkprotokoll zum Herstellen einer verschlüsselten Netzwerkverbindung mit einem entfernten Gerät
VDA	Verband der Automobilindustrie

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[46].

A.6 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht

[46] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Serversicherheit

B.1.1 Benutzertypen:

- Gruppen-Administrator (z. B. Lokaler Administrator/KeyUser/NIS-Administrator) Der Gruppen-Administrator verwaltet innerhalb einer Administrationszone (z.B. Ressourcen-Domain/Organisational-Unit) Zugriffsrechte auf Ressourcen.
- Master-Administrator
  Dem Master-Administrator obliegt die Verwaltung der Master-Domain, er richtet Benutzer ein und baut Verbindungen zu Master-Domains der Konzerntöchter auf. Er hat weitergehende Rechte als der Gruppen-Administrator. Er darf die Berechtigungen der Gruppen-Administratoren einrichten, ändern und löschen.
- Lokale Benutzerkonten:
  Lokale Benutzerkonten werden nur von Gruppenadministratoren für administrative Zwecke angelegt und verwendet.

B.1.2 In diesem Fall: Änderungen am Standard Server durch das Change Management.

B.1.3 IT-Services

B.1.4 Definiert durch IT-Services

B.1.5 Keine weiteren Details

B.1.6 Ist durch den Projekt/Server-Verantwortlichen zu bestimmen. Abhängig vom Protokoll und Service kann eine Freigabe von IT Sicherheit notwendig sein.

B.1.7 Der Server Verantwortliche muss die Einhaltung der Informationssicherheitsregelungen sicherstellen. Ausnahmen müssen von IT Sicherheit freigegeben werden. Die Verbindung zum Konzernnetzwerk der AUDI AG wird von IT Communications Services hergestellt.

B.1.8 IT-Services

C. Freigegebene Root-Dienste

C.1 Liste mit freigegebenen Diensten für Unix mit privilegierten Konten

Die folgende Software kann mit privilegierten Konten ausgeführt werden, wenn die Restriktionen der Systemsicherheitseinstellungen erfüllt sind. Insbesondere gilt dies für die folgenden Klassen von Software:

- **Administrative Tools**

  Folgende Software wird für Systemadministration, Betrieb und Fehlerbehebung verwendet:

  - Editors
  - network-traffic analysis tools (rechtliche Anforderungen sind zu beachten)
  - logfile analysis tools(im Einklang mit rechtlichen und betrieblichen Anforderungen)
  - archive-tools
  - sudo
  - rsync
  - IBM Platform LSF

- **Sicherung**

  Folgende Software wird für Sicherung von Daten oder Komplettsystem verwendet:

  - Tivoli Storage Agent
  - Tivoli Storage Manager

- **Überwachung**

  Folgende Software wird für Überwachung des Systemzustands verwendet:

  - Tivoli Endpoint
  - CA Systemedge
  - GANGLIA

- **Cluster-Software**

  Folgende Software wird verwendet, um eine zuverlässige und stabile Service Kontinuität zwischen zwei oder mehreren Hardwarekomponenten zu unterstützten:

  - Oracle Cluster Software (Solaris)
  - HACMP (AIX)
  - HP Serviceguard (HP-UX, Linux)
  - Red Hat Cluster Suite (Linux)