Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.20

Informationssicherheit in Produktionsumgebungen

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 Definition erforderlicher Sicherheitsanforderungen an Produktions-IT-Umgebungen.

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

1. Sichere Produktions-IT-Umgebungen

1.1. Ziel

Das Ziel dieses Kapitels besteht in der Definition von Sicherheitsanforderungen an Produktions-IT-Netzwerke und Produktions-IT-Systeme. Produktionsnetzwerke und Produktions-IT-Systeme erfordern spezifische Sicherheitsmaßnahmen, die von den Anforderungen im Konzernnetzwerk abweichen können.

Insbesondere folgende Ziele müssen erreicht werden:

- Vermeidung unbefugter/unbemerkter Netzwerkverbindungen und Anmeldeversuche bei IT-Systemen in der Produktionsausrüstung über das Internet, Audi-Intranet und/oder andere Produktions-IT-Netzwerke (über Einwählverbindungen oder direktes Anmelden)
- Sicherstellen der Funktionalität sowie Integrität, Verfügbarkeit, Vertraulichkeit und Nachvollziehbarkeit der Daten und Programme in der verbundenen Produktions-IT-Ausrüstung.

1.2. Allgemeine Anforderungen

- Alle Anforderungen an IT-Systeme, die in den Regelungen für Clients[1] und Server[2] definiert sind, müssen eingehalten werden und gelten auch in Produktionsumgebungen.
- Zur Verwendung von Clients in Produktionsumgebungen sind die in Kapitel 2 definierten Abweichungen zulässig.
- Die zentralen Kennwortregelungen[3] müssen befolgt werden.
- Administrative Rollen müssen implementiert und von Benutzerrollen getrennt werden.
- Vor der Implementierung eines Sicherheitsgateway muss die zuständige Stelle[4] eine IT-Risikoanalyse (mit Zweck und Standort der Implementierung) durchführen. Abhängig von den Ergebnissen der IT-Risikoanalyse müssen die Anforderungen

[1] Siehe Anhang A.1.6

[2] Siehe Anhang A.1.5

[3] Siehe Anhang A.1.10

[4] Siehe Anhang B.1.2

aus Kapitel 1.3 implementiert werden. Das Ergebnis muss von der zuständigen Stelle [5] genehmigt werden. Der Ausnahmeprozess[6] ist einzuhalten.

- Falls geforderte Sicherheitsmaßnahmen für spezifische Systeme nicht implementiert werden können, muss die zuständige Stelle[7] eine IT-Risikoanalyse (mit Zweck und Standort der Implementierung) durchführen. Das Ergebnis muss von der zuständigen Stelle [8] genehmigt werden. Der Ausnahmeprozess[9] ist einzuhalten.
- Sicherungs- und Wiederherstellungskonzepte müssen implementiert werden.
- IT-Systeme dürfen erst nach Genehmigung durch die zuständige Stelle[10] mit dem Produktionsnetzwerk verbunden werden. Das Inventar der IT-Systeme und Infrastruktur muss auf dem neuesten Stand gehalten werden[11].

1.3. Zusätzliche technische Anforderungen

Folgende Anforderungen müssen implementiert werden:

- Verkehr darf nicht direkt zwischen Büronetzwerken des Konzerns und Produktions-IT-Netzwerken weitergeleitet werden. Verbindungen zum Unternehmensnetzwerk oder anderen Produktions-IT-Netzwerken (z. B. anderen Konzerngesellschaften) müssen durch ein Sicherheitsgateway geschützt sein (mindestens eine Firewall, Intrusion Detection- und Intrusion Prevention-Systeme verbessern die Sicherheit). Die zuständige Stelle[12] ist für regelkonforme Implementierung und regelkonformen Betrieb des Sicherheitsgateways verantwortlich.
- DMZ-Infrastrukturen (oder sicherere Maßnahmen, wie das Secure Zone Konzept) müssen zwischen Büro- und Produktions-IT-Netzwerken implementiert werden.
- Abgesehen vom Sicherheitsgateway sind keine doppelt vernetzten Hosts (dual homed) und Geräte erlaubt. Dies ist lediglich zulässig, wenn beide Netzwerksegmente die gleiche Sicherheitsklassifizierung besitzen, keine hohen Risiken im Rahmen einer Risikoanalyse identifiziert worden sind und falls notwendig ein erweitertes Monitoring umgesetzt wurde. Dies schränkt nicht die Nutzung eines zweiten Interfaces zur Nutzung von administrativen Netzwerken ein.
- Das Sicherheitsgateway muss den zulässigen Datenverkehr auf das erforderliche Mindestmaß reduzieren.
- VPN-Verbindungen von Produktions-IT-Netzwerken zu Büronetzwerken des Konzerns sind nicht zulässig.

---

[5] Siehe Anhang B.1.3

[6] Siehe Anhang A.1.2

[7] Siehe Anhang B.1.2

[8] Siehe Anhang B.1.3

[9] Siehe Anhang A.1.2

[10] Siehe Anhang B.1.6

[11] Siehe Anhang A.1.10

[12] Siehe Anhang B.1.4

- Die Verbindung zwischen Büro- und Produktionsnetzwerken muss durch angemessene Maßnahmen[13] gesichert sein, die Netzwerkbedrohungen wie schädlichen Code, Viren usw. minimieren. Produktions-IT-Netzwerke sollten Konzernnetzwerke als schädlich behandeln, da Konzernnetzwerke über das öffentliche Internet zugänglich sind und daher einen physischeren Zugriff ermöglichen als Produktionsnetzwerke. Der Datenverkehr muss überwacht und untersucht werden. (Minimum bis einschließlich Layer 4).
- Die Regelungen für den Remote-Zugriff[14] müssen befolgt werden.

1.4. Organisatorische Anforderungen

- Alle Betriebsstellen von IT-Systemen in Produktions-IT-Umgebungen sind für die Verfügbarkeit und Sicherheit dieser Systeme verantwortlich. Dazu zählt die Bereitstellung qualifizierter Mitarbeiter.
- Es müssen klare Verantwortlichkeiten für IT-Systeme und Informationssicherheit im Produktionsumfeld definiert sein.
- Der Betreiber muss Dokumentation verfügbar halten, um die Einhaltung der Informationssicherheitsanforderungen und -konzepte auf Anfrage nachzuweisen. Bei neuen oder aktualisierten Produktionskomponenten muss eine detaillierte Beschreibung der Maßnahmen und Implementierungsstatus der Informationssicherheitsmaßnahmen angegeben und dokumentiert werden. Dies umfasst die Dokumentation der verwendeten IT-Komponenten.
- In Zusammenarbeit mit der Planungsorganisationseinheit muss der Planer in einer Freigabe vor Bereitstellung der Komponente die Einhaltung der Informationssicherheitsregelungen und -konzepte nachweisen.
- Kaufbedingungen der Einkaufsorganisationseinheit müssen die Sicherheitsanforderungen referenzieren, die Geräte für Produktionsumgebungen erfüllen müssen. Zumindest die Anforderungen der Regelungen für Clients[15] und Server[16] müssen eingehalten werden.
- Geräte, die mit dem Netzwerk oder Netzwerkgeräten von Lieferanten (z. B. zu Service-/Supportzwecken von Systemen mit spezieller Software) verbunden sind, müssen die Anforderungen der Regelung für Clients[17] erfüllen. Insbesondere müssen Lieferanten schriftlich bestätigen, dass Geräte aktuelle Antiviren-Patterns enthalten und aktuelle Sicherheitspatches installiert sind. Während der Servicebereitstellung gesammelte Daten müssen nach Beendigung sicher gelöscht werden.
- Bei neuen und aktualisierten Produktionsmaschinen/-standorten muss die detaillierte Spezifikation der erforderlichen Informationssicherheitsmaßnahmen von der Planungsorganisationseinheit im Lastenheft beschrieben werden.

---

[13] z.B.: IPS/IDS, application layer gateways, next-generation firewalls

[14] Siehe Anhang A.1.4

[15] Siehe Anhang A.1.6

[16] Siehe Anhang A.1.5

[17] Siehe Anhang A.1.6

- Die Umgebungen müssen durch die zuständigen Stellen[18] regelmäßig auf Schwachstellen überprüft werden (mindestens einmal pro Jahr). Die Ergebnisse sind zu dokumentieren.
- Regelmäßige interne Sicherheitsprüfungen müssen durch die zuständige Stelle ausgeführt werden. Die Ergebnisse sind zu dokumentieren und dem CERT zur Verfügung zu stellen.
- Firewall-Ereignisse, Verbindungsereignisse, Anmeldeversuche und Protokolle von Sicherheitssystemen und Betriebssystemen müssen entsprechend der Regelung zur Überwachung und Protokollierung[19] überwacht werden.

[18] Siehe Anhang B.1.5

[19] Siehe Anhang A.1.7

2. Clients in Produktionsumgebungen (Ausnahmen zur Client-Regelung 03.02.02)

Aufgrund abweichender Anforderungen in Produktionsumgebungen sind Änderungen an der Client-Regelung (mit Fokus auf Büronetzwerke) erforderlich und in diesem Kapitel definiert.

2.1. Allgemeine Anforderungen

- Die Regelung für Clients[20] muss befolgt werden. Die Definition für „Client“ aus dieser Regelung findet Anwendung.
- Nur die in dieser Regelung (Clients in Produktionsumgebungen) in den Kapiteln 2.2 und 2.3 definierten Änderungen sind für die Verwendung von Clients in Produktionsumgebungen (Produktions-Clients) zulässig.
- Diese Produktions-Clients dürfen nur in Produktionsnetzwerken verwendet werden. Ein Produktionsnetzwerk ist ein gemäß der Definition in Kapitel 1 getrenntes Netzwerk.
- Produktions-Clients dürfen nur für Aufgaben und Prozesse verwendet werden, die direkt mit der Produktion verbunden sind. Andere Verwendungen (insbesondere Surfen im Internet, Benutzer-E-Mails und alle typischen Verwendungen von Büro-Clients) sind nicht erlaubt.
- Produktions-Clients dürfen nur von der zuständigen Stelle[21] als Softwarepaket bereitgestellt werden.
- Für jede weitere Änderung an Produktions-Clients oder jede andere Verwendung von Produktions-Clients ist die Freigabe durch die zuständige Stelle[22] erforderlich.
- Der Betrieb von Produktions-Clients darf nur von der zuständigen Stelle[23] ausgeführt werden.

2.2. Zusätzliche Anforderungen an Clients in Produktionsumgebungen

- Die Benutzerbestätigung für die Annahme der Informationssicherheitsrichtlinien kann deaktiviert werden, um den Start ohne Benutzeraktion zu ermöglichen.
- Die Microsoft Scripting Engine (wscript.exe, wsh-script, PowerShell und c-script) kann bei Bedarf aktiviert werden.

[20] Siehe Anhang A.1.6

[21] Siehe Kapitel B.2.2

[22] IT-Sicherheit

[23] Siehe Kapitel B.2.3

2.3. Spezifische Regelungen für Clients in Produktionsumgebungen

Die folgenden Änderungen an der Regelung Nr. 03.03.02 – Clients sind für Produktions-Clients zulässig:

2.3.1 Change Management

- Die zuständige Stelle muss einen Change Management-Prozess[24] definieren.
- Alle Tests der zentralen Sicherheitskonfiguration und Änderungen am Produktions-Client selbst sind von dieser Stelle auszuführen.
- Lokale Änderungen am Produktions-Client müssen einem festgelegten Change Management-Prozess folgen (wie durch die Regelung zum Change Management[25] definiert).

2.3.2 Reaktionszeiten

Clients in Produktionsumgebungen können eine spezielle Verfügbarkeit erfordern. Wenn eine spezielle Verfügbarkeit erforderlich ist, muss dies mit den Stellen, die diese Clients unterstützen, abgestimmt werden.

Die Wiederherstellungszeit wird von der lokalen Betriebseinheit in Zusammenarbeit mit den anfordernden Organisationseinheiten definiert.

Support muss von der lokalen Betriebsorganisation entsprechend der erforderlichen Verfügbarkeit sichergestellt werden.

2.3.3 Lokale Benutzerkonten

Integration in zentrale Benutzerverwaltung wird bevorzugt.

Lokale Benutzerkonten auf Produktions-Clients sind nur erlaubt, wenn zentrale Benutzerverwaltung (z. B. Active Directory) nicht verfügbar ist und lokale Konten für Verwaltung und Betrieb des Clients erforderlich sind. Die Kennwortrichtlinie[26] muss befolgt werden.

Wenn die Integration in zentrale Benutzerverwaltung nicht möglich ist, sind nur folgende Kontotypen zulässig:

- Benutzerkonto (z. B. VWUSER) für die Verwendung installierter Anwendungen und den automatischen Anmeldungsprozess
- Administratorkonto (z. B. SPMAdmin) für die Verwendung durch Dienstleister zur Verwaltung des Clients in Servicezeiten. Dieser Account muss deaktiviert sein und darf nur während des Services aktiviert werden.

[24] Change Management Prozess von Audi AG

[25] Siehe Anhang A.1.8

[26] Siehe Anhang A.1.10

- Administratorkonto (z. B. localadmin) für die Verwendung der Betriebseinheit zur Unterstützung des Clients

Es ist zu protokollieren bzw. zu dokumentieren, wer welches nicht personalisierte Konto zu welchem Zeitpunkt und auf welchem System verwendet hat.

2.3.4 Freigaben auf Clients

Lokale Netzwerkfreigaben sind zulässig, wenn die folgenden Bedingungen erfüllt werden:

- Sie sind notwendig, damit die Produktionsumgebung funktioniert.
- Zugriffe auf Freigaben müssen mit Einschränkungen für Benutzergruppen und/oder Einschränkungen für Quell-IPs gesichert sein. Freigaben, die für jeden zugänglich sind, sind nicht erlaubt.
- Ihre Verwendung wird dokumentiert und der lokalen Stelle zur Ausnahmenbehandlung[27] gemeldet.
- Ihre Verwendung wird durch die lokale Stelle zur Ausnahmenbehandlung genehmigt.

2.3.5 Zugriffsschutz

Zugriff auf den Desktop muss durch Kennwortschutz gesichert werden, sodass alle Anwendungen im Vollbildmodus (Kiosk-Modus) ausgeführt werden.

Die Funktionen „Bildschirmschoner“ und „Sperrbildschirm“ können deaktiviert werden, wenn die folgenden Bedingungen erfüllt werden:

- Physischer Zugriff auf den Client ist geschützt (Computer ist in einen Schrank eingeschlossen).
- Domänensystemkonten oder lokale Benutzerkonten für automatische Anmeldung werden verwendet und sind erforderlich, damit der Client funktioniert.

Für das Benutzerkonto (z. B. VWUSER) ist die Funktion „Automatische Anmeldung“[28] erlaubt.

2.3.6 BIOS

Die lokale Betriebseinheit[29] darf die BIOS-Konfiguration ändern. Das BIOS muss jedoch durch ein Kennwort gesichert sein.

[27] Siehe Anhang A.1.2

[28] Anforderungen für Autologon oder in Informationssicherheit Regelung Nr. 03.03.02 Clients definiert

[29] Siehe Anhang B.2.1

2.3.7 Anwendungen

Die lokale Betriebseinheit ist verantwortlich für die Freigabe und Dokumentation von Anwendungen auf Produktions-Clients und für den sicheren Betrieb des Clients. Sicherer Betrieb umfasst insbesondere Patch-Management und Anti-Malware.

Alle Anwendungen müssen vollständig betriebsfähig sein mit Benutzerberechtigungen und Benutzerzugriffsrechten.

2.3.8 Netzwerkverbindung

Eine gleichzeitige Netzwerkverbindung von Produktions-Clients (im Produktionsnetzwerk) ist nur für Maschinennetzwerke bzw. Netzwerke einer Produktionseinrichtung zulässig. Andere Netzwerke (mit Ausnahme administrativer Netze) dürfen nicht mit Produktions-Clients verbunden werden.

2.3.9 Benutzerrechte

Die folgenden Berechtigungen können Administratoren zugewiesen werden:

- Dauerhaft freigegebene Objekte erstellen
- Herunterfahren des Systems von einem Remote-System erzwingen
- Clients zu einer Domäne hinzufügen
- Lokal anmelden

Die folgenden Berechtigungen können Benutzerkonten zugewiesen werden:

- Lokal anmelden

2.3.10 Gruppenrichtlinien/Registrierungseinträge

Winreg – Schreibzugriff über das Netzwerk muss möglich sein

> Support für Produktions-IT-Client erfolgt häufig remote (z. B. über eine Administrator-Station, vorzugsweise über ein administratives Netzwerk). Remote-Support muss in der Lage sein, lokale Registrierungseinstellung remote zu ändern.

2.3.11 Temporäre Dateien

Automatische Löschung des Papierkorbs und Browser-Cache kann deaktiviert werden.

II. Verantwortlichkeiten

II.I Kapitel 1: Sichere IT Produktionsumgebungen

Diese Regelung ist von allen Betreibern von IT-Systemen in der Produktion 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.

II.II Kapitel 2: Clients in Produktionsumgebungen

Diese Regelung ist von allen Betreibern von IT-Systemen in der Produktion 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 Informationssicherheit Regelung Nr. 03.01.01 Anti Malware & Systemschutz

A.1.2 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.3 Informationssicherheit Regelung Nr. 03.02.01 Funknetzwerke

A.1.4 Informationssicherheit Regelung Nr. 03.02.04 Netzwerkzugänge

A.1.5 Informationssicherheit Regelung Nr. 03.03.01 Server

A.1.6 Informationssicherheit Regelung Nr. 03.03.02 Clients

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

A.1.8 Informationssicherheit Regelung Nr. 03.01.08 Change- und Patch-Management

A.1.9 Nicht referenziert

A.1.10 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

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
Management of technical vulnerabilities	1.3	A.12.6.1	A.12.6.1	12.7
Segregation in networks	1.2, 2.1	A.13.1.3	A.11.4.5	13.3

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 Quellen und Referenzen

- **Standard ISO/IEC 27005:2011 Risikomanagement in der Informationssicherheit**

A.5 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**
CERT	Critical Emergency Response Teams
Dual Homed	Geräte die gleichzeitig mit unterschiedlichen Netzwerksegmenten verbunden sind. Hier besteht das Risiko einer Verbindung zweier unterschiedlicher Segmente mit unterschiedlichem Schutzbedarf.
Firewall	Sicherungssystem, das ein Netzwerksegment oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Die Zugriff werden anhand von Regelungen auf definierte Ports/Protokolle beschränkt.
Integrität	Bezeichnet die Korrektheit (Unversehrtheit) von Daten bzw. die Verhinderung unberechtigter Veränderung von Daten
IDS	Intrusion Detection-System zur Erkennung von Angriffen, die gegen ein Computersystem oder eine Rechnernetz gerichtet sind.
IPS	Intrusion Prevention System, ist ein System das über die Identifizierung von potentiellen Angriffen (IDS) hinaus

	Funktionen zur Abwehr von identifizierten Angriffen bereit stellt.
IT-Risikoanalyse	Risikoanalyse mit dem Fokus auf Informationstechnologien.
Risikoanalyse	Prozessschritt des Risikomanagements, zur Identifikation und Bewertung der identifizierten Gefahren hinsichtlich ihrer Eintrittswahrscheinlichkeiten und möglichen Auswirkungen betrachtet. (ISO 31000:2009)
Schwachstelle / Vulnerability	Eine Schwachstelle ist die ausnutzbare Bedrohung eines oder mehrerer Assets. Eine fehlende Maßnahme ist ebenfalls eine Schwachstelle.
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).
Threat	Potenzielle Ursache eines Informationssicherheitsvorfalls oder Bedrohung für ein IT-System, die möglicherweise zu einem Schaden des Systems oder der Organisation führt.
Verfügbarkeit	Bezeichnet die Gewährleistung der Verfügbarkeit von Daten/Systemen innerhalb eines vereinbarten Zeitrahmens.
Vertraulichkeit	Bezeichnet die Gewährleistung, dass Daten sowohl beim Zugriff als auch während der Übertragung lediglich von befugten Personen gelesen werden können.

A.6 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[30].

A.7 Dokumentenhistorie

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

[30] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Sichere Produktionsumgebung

B.1.1 IT-Services

B.1.2 IT-Services & IT-Sicherheit

B.1.3 IT-Sicherheit

B.1.4 IT-Services

B.1.5 IT-Sicherheit

B.1.6 IT-Sicherheit

B.2 Kapitel 2: Clients in Produktionsumgebungen

B.2.1 IT ggf. die jeweiligen Instandhaltungen und Planungen

B.2.2 IT

B.2.3 IT ggf. die jeweiligen Instandhaltungen und Planungen