Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.04

Sicherheitsprotokollierung und -monitoring

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Diese Regelung definiert Grundsätze und Anforderungen zur Protokollierung, Auswertung und Monitoring sicherheitsrelevanter Ereignisse.

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

1. Protokollierung sicherheitsrelevanter Ereignisse[1]

1.1. Ziel

Die Informationssicherheit Handlungsleitlinien für Systembetreiber und Administratoren[2] beinhalten allgemeine Protokollierungsvorgaben. Weitere Vorgaben zur Protokollierung von Sicherheitsereignissen[3], die sich auf das Sicherheitsniveau der AUDI BURSSELS und des Konzerns auswirken können, sind in den folgenden Kapiteln dieser Regelung definiert.

Diese Ereignisse werden protokolliert um Sicherheitsvorfälle in Systemen und Prozessen, zu erkennen und zu untersuchen.

Weitere Gründe zur Protokollierung sind nicht Bestandteil dieser Regelung.

1.2. Allgemeine Anforderungen

- Zur Erfassung unberechtigter Aktivitäten in der Informationsverarbeitung müssen Netzwerkkomponenten, Betriebssysteme, Datenbanken, Middleware, und Anwendungen Log-Meldungen erstellen.
- Für festgelegte Systeme sind technologiespezifische Protokollierungsanforderungen[4] definiert und müssen eingehalten werden.
- Log-Daten müssen vor unberechtigten Zugriff geschützt werden[5].
- Die Systemzeit aller Informationsverarbeitungssysteme, die Log-Meldungen erzeugen oder verarbeiten müssen mit einer festgelegten und genauen Zeitquelle synchronisiert werden.
- Log-Daten dürfen während der festgelegten Aufbewahrungszeiten (hängt von gesetzlichen und Systemspezifischen Anforderungen ab) nur aus den Quelldaten

[1] Definitionen in A.4

[2] Siehe Anhang A.1.3

[3] Definition: Siehe Anhang A.4. Beispiele sind in Kapitel 1.4 zu finden

[4] Siehe Anhang A.3.2

[5] Siehe Anhang A.1.3

gelöscht oder überschrieben werden, wenn diese bereits ausgewertet oder an eine zentrale Stelle zur Auswertung übertragen wurden.

- Länderspezifische Rechts-und Datenschutzanforderungen sind zu beachten.

1.3. Klassifizierung von Log-Meldungen

Log-Meldungen müssen gemäß den Anforderungen der Informationssicherheit Handlungsleitlinien[6] klassifiziert werden.

Die für die Log-Quelle verantwortliche Stelle ist auch für die Klassifizierung der Log-Meldungen verantwortlich. Die Eigentümer der durch die Protokollquellen verarbeiteten Informationen müssen bei der Klassifizierung beteiligt werden.

1.4. Protokollierung von Log-Meldungen[7]

Es ist zwischen Protokollierung und Auswertung klar zu trennen. Die unten aufgeführten Ereignisse können komplett oder teilweise für die Analyse von Vorfällen sehr wichtig sein. Es wird an dieser Stelle darauf hingewiesen, dass im Rahmen von Auswertungen nicht alle Ereignisse herangezogen werden und auch ggf. nicht ohne entsprechende Freigabe (durch Betriebsrat, Gewerkschaften, Personalwesen und Datenschutz) dürfen (z.B. bezüglich Leistungskontrolle).

1.4.1 Audit Protokollierung

Log-Quellen müssen so konfiguriert werden, dass Log-Meldungen, wenn technisch möglich, mindestens für die folgenden sicherheitsrelevanten Ereignisse erstellt werden:

- Erfolgreiche und abgelehnte Anmeldeversuche sowie Abmeldungen
- Erstellen, Ändern, Sperren, Entsperren und Löschen von Konten und Rollen in Anwendungen
- Passwortänderungen und/oder Zertifikatsänderungen
- Berechtigungsänderungen (z. B. Benutzerrechte, Objektberechtigungen, Gruppenmitgliedschaften)
- Starten und Beenden von Prozessen (z. B. das Starten und Beenden von Diensten, Aktivieren und Deaktivieren von Schutzsytemen wie Virenscanner und Firewalls)
- Änderungen am Zeitdienst
- Änderungen an den Protokollierungs-Einstellungen (speziell das Deaktivieren der Protokollierung)

[6] Siehe Anhang A.1.2

[7] Weitere Informationen: siehe Anhang A.1.3

- Alle anderen Ereignisse die von den für die Log-Quelle verantwortlichen Personen als sicherheitsrelevant erachtet werden. Diese beinhalten[8] z. B.:

- Erfolgreiche oder abgelehnte Zugriffe auf Daten oder andere Ressourcen
- Änderungen an der Systemkonfiguration
- Verwenden von Berechtigungen
- Verwenden von Systemwerkzeugen und -Anwendungen
- Dateizugriffe und Art des Zugriffs
- Warnungen von Zugriffskontrollsystemen (z. B. unerlaubte Versuche auf geschützte Verzeichnisse zuzugreifen)

- Die Tätigkeiten der Systembetreiber an IT-Systemen mit vertraulichen und/oder geheimen Informationen sind zu protokollieren.

Betreiber von Log-Quellen müssen dokumentieren, welche sicherheitsrelevanten Ereignisse von der Protokollquelle protokolliert werden.

1.4.2 Operative Protokollierung

Neben sicherheitsrelevanten Ereignissen muss die eigentliche Funktion der Log-Quelle protokolliert werden. Zum Beispiel:

- Firewall: erlaubte oder verweigerte Kommunikation zwischen Netzwerkzonen
- Intrusion Prevention System (IPS): Identifizierte Malware in der Netzwerkkommunikation
- Authentifizierungsdienste: Erfolgreiche und abgelehnte Logins

1.5. Aufbau von Log-Meldungen

Log-Meldungen müssen folgende Angaben zu Ereignissen enthalten:

- Zeitstempel, der das Datum und die Uhrzeit des Ereignisses enthält
- Identifizierungsmerkmale: so viele wie nötig, um die Protokollquelle eindeutig zu identifizieren - zum Beispiel:

- Erforderlich: Netzwerkadresse (IPv4 oder IPv6)
- Pseudonym
- Protokoll / Dienst (z.B. HTTP, HTTPS, …)
- SessionID (oft in Anwendungen verwendet)
- Name der Protokollquelle (z. B. Datenbankinstanz, Web-Server-Instanz, Anwendungsname)

[8] Siehe Anhang A.1.2

- Beschreibung des sicherheitsrelevanten Ereignisses

Zusätzlich sollten die folgenden Ereignisse (falls vorhanden) enthalten sein:

- Schweregrad des Ereignisses
- Kategorie (z. B. Authentifizierung, Autorisierung, ...)

Log-Meldungen dürfen keine Passwörter, deren Hashes oder jegliche Form der Benutzerauthentifizierung (z. B. öffentlichen Schlüssel, ...) enthalten.

1.6. Auswertung von Protokolldaten

Die für ein System oder eine Applikation verantwortliche Stelle muss sicher stellen, dass im Rahmen der Betriebsübergabe das System oder die Applikation an einen zentralen Logdatenkollektor[9] angebunden wird.

Die Logdaten müssen permanent, zentral auf Informationssicherheitsprobleme hin ausgewertet[10] werden. Bei Bedarf muss eine zeitnahe direkte Auswertung[11] von Logdaten erfolgen.

Die Auswertung der Logdaten zur technischen Fehleranalyse erfolgt durch die jeweiligen Administratoren des Systems.

Gesellschaftsspezifische und rechtliche Vorschriften[12] (z. B. Aufbewahrungsfristen und Löschungspflichten) müssen bei der Auswertung von Protokolldaten beachtet werden.

Die Auswertung darf nicht durch den Initiator der Log-Meldungen durchgeführt werden (Segregation of Duty).

[9] Splunk Infrastruktur

[10] Dies erfolgt durch CSIRT / BISL

[11] Siehe Anhang B.1.1

[12] Siehe Anhang B.1.2

2. Monitoring sicherheitsrelevanter Ereignisse

2.1. Ziele

Das Ziel dieses Kapitels ist die Definition von erforderlichen Anforderungen an das Monitoring sicherheitsrelevanter Ereignisse in IT-Systemen, IT-Diensten und Prozessen bezüglich der Informationssicherheit.

2.2. Allgemeine Anforderungen

- Für jedes IT-System muss festgelegt und dokumentiert werden, ob – zusätzlich zur Protokollierung[13]– weitere Überwachungsmaßnahmen (Monitoring) implementiert werden müssen. Dafür muss die Sicherheitsklassifikation[14] der vom IT-System verarbeiteten Informationen berücksichtigt werden.
- Sollen zusätzliche Überwachungsmaßnahmen implementiert werden, muss ein Monitoring-Konzept entwickelt und dokumentiert werden[15]. Das Konzept muss zumindest folgende Aspekte umfassen:

- Art der Überwachungsmaßnahme (z. B. Schwachstellen-Scanner, Verwendung einer speziellen Überwachungssoftware)
- Prozess für die Auswertung, Berichterstattung und Eskalation in Abhängigkeit von der Überwachungsmaßnahme, einschließlich Klassifikation und Priorisierung sicherheitsrelevanter Ereignisse und einer Schnittstelle zum Security Incident Management
- Verantwortlichkeit für die Implementierung des Monitorings
- Verantwortlichkeit für die Durchführung des Monitorings

- Es müssen geeignete Maßnahmen etabliert sein, um eine Gefährdung der Monitoring-Informationen zu vermeiden (z. B. Funktionstrennung, 4-Augen-Prinzip, geteilte Schlüssel/Passwörter). Die Verantwortung für die Überwachung sollte bei einer Einheit liegen, die nicht in operative Aufgaben des zu überwachenden Systems involviert ist.

[13] Siehe Kapitel 1

[14] Siehe Anhang A.1.2

[15] Z. B. bei der IT-Planung

II. Verantwortlichkeiten

II.I Kapitel 1: Protokollierung sicherheitsrelevanter Ereignisse

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.

II.II Kapitel 2: Monitoring sicherheitsrelevanter Ereignisse

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 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.2 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.3 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

A.1.4 Nicht Referenziert

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(2014)
Event logging	1.4, 1.4.1, 1.4.2, 1.5	A.12.4.1	A.10.10.1, A.10.10.2, A.10.10.5	12.5
Protection of log information	1.2, 1.3	A.12.4.2	A.10.10.3	12.5
Administrator and operator logs	1.2, 1.4.1	A.12.4.3	A.10.10.4	
Clock synchronisation	1.2	A.12.4.4	A.10.10.6	

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.3.2 Audit Settings

Die Einstellungen sind im Anhang der Informationssicherheitsregelung 03.01.01 Anti Malware & Systemschutz mit enthalten: „Anhänge zur Regelung Anti Malware & Sytemschutz“ (volkswagen-security-settings.zip - Rubrik: Parameter Settings for Logging):

A.4 Abkürzungen und Definitionen

Begriff	**Definition**
Sicherheitsrelevantes Ereignis	Ein sicherheitsrelevantes Ereignis ist ein Ereignis auf einem System, einer Anwendung oder einer IT-Komponente, welches für sich allein oder durch Interaktion mit anderen Ereignissen Auswirkungen auf das Sicherheitsniveau des Konzerns haben kann.
Log-Meldung	Eine Log-Meldung ist eine einzelne Information mit Details zu einem sicherheitsrelevanten Ereignis.
Log-Quelle	Log-Quellen sind Systeme, Anwendungen oder IT-Komponenten, die Log-Meldungen erstellen.
Protokolldaten	Protokolldaten sind ein oder mehrere Log-Meldungen.
Log-Datei	Eine Log-Datei ist eine Datei mit Log-Daten.
Protokollierung	Protokollierung ist die Erstellung und Speicherung von Log-Meldungen. Log-Meldungen werden beispielsweise in Form von Log-Dateien gespeichert.
GDPR / DSGVO	Datenschutzgesetz
BISL	Brand Information Security Leitstand

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[16].

A.6 Dokumentenhistorie

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

[16] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Protokollierung sicherheitsrelevanter Ereignisse

B.1.1 Eine genaue manuelle Auswertung von Logdateien erfolgt bei Bedarf durch das CSIRT / BISL

B.1.2 z.B. GDPR / DSGVO

Beim Einsatz einer personenbezogenen Protokollierung ist dies mit dem DPO abzustimmen.

B.2 Kapitel 2: Monitoring sicherheitsrelevanter Ereignisse

-