Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.18

Informationssicherheitsvorfalls- und Schwachstellenmanagement

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.1

Inhalt

I. Zweck

In dieser Regelung werden die Anforderungen an die IT Defense Organisation von Audi definiert, die im Folgenden als Audi-CERT bezeichnet wird. Eine erfolgreiche IT-Sicherheitsstrategie hängt davon ab, dass alle an Planung, Entwicklung und Betrieb von IT-Services Beteiligten entsprechende Beiträge leisten und kooperieren. Aus diesem Grund beschreibt diese Regelung auch die notwendigen Voraussetzungen, die von der IT-Organisation, System Eigentümern, Applikationsverantwortlichen und Service Nutzern erfüllt sein müssen, damit die Services von Audi-CERT realisiert und genutzt werden können.

In dieser Regelung werden ebenfalls Anforderungen an das Schwachstellenmanagement definiert. Die unterschiedlichen Rollen, Verantwortlichkeiten und Begriffe werden erläutert.

1. Allgemeine Begriffsbestimmungen im Zusammenhang mit dem IT-Security- Incident-Management

1.1. Ziel

In diesem Kapitel werden die allgemeinen Begriffe, Rollen und zugehörigen Zuständigkeiten und Anforderungen im Zusammenhang mit dem Incident Management für die IT-Sicherheit sowie Schemata zur Kategorisierung von IT-Sicherheitsvorfällen beschrieben.

1.2. Begriffsbestimmungen

1.2.1 Rollen und Funktionen

Rolle	Beschreibung
Audi-CERT	Audi-CERT ist die Organisation innerhalb der IT-Sicherheitsabteilung der AUDI Brand, die sich mit dem Thema IT Defense befasst. Seit dem 1. August 2019 heißt die Abteilung „IT Security Defense / Operations“.
Asset Eigentümer	Beim Asset Eigentümer handelt es sich um denjenigen Mitarbeiter oder diejenige Organisationseinheit, die für ein IT-Asset zuständig ist. (Normalerweise der Application Owner)
Incident Handler	Der diensthabende Incident Handler des Audi-CERTs bearbeitet die im Tagesgeschäft auftretenden Vorfälle werden unter Anwendung des Incident-Handling-Prozesses. Der Incident Handler muss die Sicherheitsvorfälle anhand des am ehesten zutreffenden Standardverfahrens (Playbook) bearbeiten.

1.2.2 Begriffe

Begriff	Beschreibung
Zuständigkeitsbereich Audi-CERT	Der Zuständigkeitsbereich bezeichnet den Teil der IT Umgebung, für den Audi-CERT zuständig ist. Innerhalb seines Zuständigkeitsbereichs ist Audi-CERT verpflichtet, eine aktive Überwachung und Verfolgung

	von potenziellen Bedrohungen durchzuführen, und ist damit beauftragt, Untersuchungen durchzuführen, um Bedrohungen zu erkennen, zu analysieren, einzudämmen und auszuschalten. Über den Zuständigkeitsbereich muss das Top-IT-Management bei Audi einschließlich der betreffenden Audi CISOs entscheiden. Anhand der Größe und Art des Zuständigkeitsbereichs ergeben sich die Größe der Audi-CERT Teams, die Schulungsanforderungen und die benötigte Ausstattung.
Einsatzregeln	Durch die Einsatzregeln werden die Maßnahmen, die Audi-CERT je nach Schwere eines Sicherheitsvorfalls und den möglichen geschäftlichen Auswirkungen des Sicherheitsvorfalls eigenständig ergreifen darf, sowie potenzielle Maßnahmen zur Bekämpfung des Angriffs festgelegt. Es muss eine allgemeine Festlegung der Einsatzregeln vorliegen, die von allen verantwortlichen Prozessbeteiligten auf der Entscheidungs-Ebene vereinbart und unterzeichnet worden ist. Sobald ein Sicherheitsvorfall formal registriert wurde, müssen die Prozessbeteiligten über die Einsatzregeln informiert werden und diesen zustimmen. Wenn keine Einigung möglich ist, müssen die Einsatzregeln so angepasst werden, dass sie für alle beteiligten Parteien akzeptabel sind. Ist weiterhin keine Einigung möglich, so muss Audi-CERT den Sicherheitsvorfall in der Befehlskette eskalieren (CISO & CIO von Audi BRUSSELS, CISO der Audi Marke, CIO der Audi Marke).
Sicherheitsvorfall	Ein Sicherheitsvorfall bezeichnet ein Ereignis, das mindestens einen der normalerweise vorhandenen Faktoren der IT-Sicherheit beeinträchtigt: Vertraulichkeit, Verfügbarkeit oder Integrität. Nicht alle Sicherheitsvorfälle werden von Audi-CERT bearbeitet. Es werden drei Arten von Sicherheitsvorfällen unterschieden: Informationsabfluss (Information leakage), zielgerichtete und nicht zielgerichtete Bedrohungen.
GRC-Verstoß	Wenn innerhalb des Zuständigkeitsbereichs von Audi-CERT ein Verstoß gegen die Informationssicherheitsregelungen oder andere innerhalb der Audi BRUSSELS festgestellt wird, wird der zuständige Governance-Verantwortliche informiert, das den Verstoß im Rahmen des anwendbaren Risikoakzeptanzprozesses bearbeiten wird. Audi-CERT wird durch die angebotenen Services entsprechende Unterstützung gewähren; dies gilt auch für den „Lessons Learned“ Teil des Prozesses.
Bedrohung	Eine Bedrohung besteht durch eine Einzelperson oder eine Gruppe, welche die Fähigkeit, Absicht und Gelegenheit hat, Audi zu schaden.
Zielgerichtete oder nicht zielgerichtete Bedrohung	Wenn ein Sicherheitsvorfall durch eine wie oben definierte Bedrohung verursacht wird, ist Audi-CERT verpflichtet, den Vorfall zu bearbeiten und den betroffenen Eigentümern der IT-Assets und Prozessbeteiligten mithilfe der angebotenen Services Unterstützung zu gewähren. Eine nicht zielgerichtete Bedrohung richtet sich nicht speziell gegen Audi als Organisation. Wenn z. B. ein typischer Cybercrime-Akteur Malware über

	Spam-E-Mails verbreitet, so handelt es sich um eine nicht zielgerichtete Bedrohung. Eine zielgerichtete Bedrohung richtet sich speziell gegen Audi, mit der Absicht, der Organisation zu schaden. Beispiele hierfür sind Akteure aus dem Umfeld des organisierten Verbrechens, die IT-Systeme angreifen, um Geld oder wertvolle Informationen oder Produkte zu stehlen (d. h. Diebstahl von Fahrzeugen und Services) oder Personen, die im Auftrag von Unternehmen oder Nationalstaaten Betriebsspionage oder Sabotage betreiben.
IT-Asset	Ein IT-Asset bezeichnet einen beliebigen Host (z. B. Client-System, Server, virtuelle Maschine usw.), eine Anwendung, eine Komponente der Infrastruktur (z. B. Switch, Router, Firewall usw.) oder eine andere Computer-Vorrichtung (z. B. computergestützte Fertigungswerkzeuge im Produktionsbereich), die Teil der IT-Infrastruktur von Audi ist.
IT Defense	IT Defense ist der Begriff, mit dem bei Audi das Konzept der aktiven Überwachung der IT-Umgebung auf potenzielle Bedrohungen und ungewöhnliches Verhalten, das Reagieren auf IT-Sicherheitsvorfälle, das Sammeln von Informationen und Erkenntnissen zu potenziellen Bedrohungen für die IT-Umgebung von Audi, die Unterstützung bei der Eindämmung, der Abmilderung der Folgen und der Ausschaltung jeglicher erkannter Bedrohungen sowie schließlich die Schlussfolgerungen aus dem Sicherheitsvorfall und die Verbesserung des Sicherheitsverhaltens innerhalb der Organisation („Lessons Learned“).
Informationsabfluss (Information leakage)	Eine absichtliche oder unabsichtliche Preisgabe von personenbeziehbaren Informationen, die AUDI BRUSSELS gehören, werden von dem Datenschutzbeauftragten bearbeitet. Andere nicht personenbeziehbare Informationsabflüsse werden von der Unternehmenssicherheit behandelt. Audi-CERT unterstützt die Bearbeitung dieser Vorfälle durch seine Erkennungs- und Analyseressourcen, aber die Bearbeitung der Vorfälle selbst und insbesondere die Berichterstattung an die Prozessbeteiligten und Behörden obliegt den Datenschutzbeauftragten.
Incident response Team	Ein Sicherheitsvorfall, der nicht anhand eines der Standardverfahren bearbeitet werden kann, muss an das Incident Response Team eskaliert werden. Ein speziell zugewiesenes Incident Response Team, das zumindest aus einem Lead Incident Responder und einem oder mehreren Incident Analysten von Audi-CERT oder zur Unterstützung eingesetzten externen Incident Response-Teams und zusätzlichen Fachleuten besteht, bearbeitet den Sicherheitsvorfall im Rahmen des Incident Response-Prozesses.
PoC (Point of Contact)	Die Kontaktperson (PoC) dient als Bindeglied zwischen einem Audi BRUSSELS bzw. einem bestimmten Teil der IT-Infrastruktur (z. B. dem Produktionsbereich in Brüssel) und Audi-CERT. Der PoC muss die lokalen Kommunikations- und Eskalationspfade kennen.

2. IT Defense und Incident Response

2.1. Kontakt Audi-CERT & Meldung von Sicherheitsvorfällen

Audi-CERT muss sicherstellen, dass es interne und externe Kontaktinformationen gemäß des RFC3250 Richtlinien bereitstellt.

Die Meldung von Sicherheitsvorfällen hat gemäß dem Prozess-Standard „Information Security Incident“ über den lokalen Helpdesk von AUDI BRUSSELS zu erfolgen: **HelpDesk [EHD – 2406 / UHD 2223].**

2.2. IT-Defense Service

Um eine effektive IT Defense durchzuführen, muss Audi-CERT in der Lage sein, wenigstens drei Kern-Services bereitzustellen, die eine aktive Gefahrenabwehr ermöglichen: Threat Intelligence, Continuous Security Monitoring und Incident Response. Audi-CERT entscheidet nach eigenem Ermessen, ob diese Services vollständig durch internes Personal oder mit zusätzlicher Unterstützung durch externe Unternehmen abgedeckt werden. Für jeden dieser Services muss jedoch wenigstens ein speziell zugewiesener interner Mitarbeiter zuständig sein. Alle Prozesse der einzelnen Services müssen vollständig dokumentiert und vom Personal von Audi-CERT sowie externem Support-Personal befolgt werden.

2.3. Threat Intelligence (TI)

Der Service „Threat Intelligence“ hat die Aufgabe zu bestimmen, welche Bedrohungen und Bedrohungsgruppen die größte Gefahr für die IT-Systeme innerhalb des Zuständigkeitsbereichs von Audi-CERT darstellen, die Prozessbeteiligten mit einem Überblick über die Bedrohungslandschaft zu versorgen sowie dem CSM Personal (Continuous Service Monitoring) von Audi-CERT die Informationen zu liefern, die es benötigt, um Bedrohungen innerhalb der IT-Umgebung erfolgreich aufzuspüren.

Der TI-Service umfasst die Generierung von Informationen über Bedrohungen, Nutzung der von Drittanbietern gelieferten Erkenntnisse zu Bedrohungen intern bei Audi-CERT sowie ihre Weitergabe an andere Parteien innerhalb seines Zuständigkeitsbereichs. Audi-CERT muss gemäß den Statuten, die vom GISSC des Volkswagen Konzerns festgelegt wurden, an der Weitergabe von TI mitwirken. Audi-CERT muss die TI-Services für die AUDI BRUSSELS bereitstellen.

2.3.1 Anforderungen an Audi CERT

Audi-CERT muss sicherstellen, dass potenzielle Bedrohungen, die sich gegen IT-Assets von AUDI BRUSSELS richten, so verfolgt werden, dass

- Prozessbeteiligte fundierte strategische Entscheidungen zur Minimierung von Risiken treffen können, die durch die für die Bedrohung verantwortlichen Akteure verursacht werden;
- die Bemühungen der Services Continuous Security Monitoring und Incident Response, die Entdeckungsmöglichkeiten zu optimieren und das Auftreten von False Positives zu minimieren, unterstützt werden.

Außerdem sollte der Threat Intelligence-Service anstreben, andere IT Defense Teams innerhalb des Audi Konzerns, des Volkswagen Konzerns und des Kreises, in dem TI zu teilen ist, an den von ihnen gewonnenen Erkenntnissen teilhaben zu lassen. Das Teilen von wesentlichen Informationen mit gleichgeordneten Stellen hilft allen Beteiligten. Ohne das Teilen solcher Informationen kann kein Threat Intelligence-Service erfolgreich arbeiten. Alles

Teilen von Informationen muss einer definierten und abgesegneten Informationsaustausch Vorgabe (Information Sharing Policy) folgen.

2.3.2 Anforderungen an die Nutzer des Service

Nutzer des Threat Intelligence-Service von Audi-CERT müssen eine Kontaktperson abstellen, die zeitnah auf Erkenntnisse bezüglich einer Bedrohung reagieren muss. Zeitnah bedeutet im Allgemeinen am nächsten Arbeitstag. Falls jedoch zeitkritische Informationen über bevorstehende Bedrohungen geschäftskritischer Assets vorliegen, die sich im Zuständigkeitsbereich des Nutzers des Service befinden, ist eine Reaktion innerhalb von Stunden anzustreben. Dies ist vom jeweiligem Management von AUDI BRUSSELS festzulegen, der den Threat Intelligence-Service von Audi-CERT nutzt.

2.4. Continuous Security Monitoring (CSM)

Der CSM-Service soll die zeitnahe und effektive Erkennung potenzieller Bedrohungen der IT-Infrastruktur innerhalb des Zuständigkeitsbereichs von Audi-CERT sowie die Ersteinschätzung und Bestimmung der Schwere jeglicher potenziellen Bedrohungen, die erkannt werden, sicherstellen.

Dieser Service dient zur Erfassung aller Datenquellen, die zur Erkennung von Bedrohungen der IT-Umgebung innerhalb des Zuständigkeitsbereichs von Audi-CERT. Die Erkennung von Bedrohungen in diesen Daten erfolgt mithilfe von Referenzwerten und Threat Intelligence. Die identifizierten Ereignisse benötigen Analyse mit dem Ziel der Bestimmung, ob es sich bei einem Ereignis um einen tatsächlichen Sicherheitsvorfall oder um eine False-Positive-Meldung handelt. Falls festgestellt wird, dass ein Ereignis auf einen Sicherheitsvorfall hindeutet, nimmt das CSM-Team eine Ersteinschätzung vor, um die Art und Schwere der Bedrohung zu bestimmen. Aus dem Ergebnis der Ersteinschätzung ergeben sich die nächsten Schritte, die zum Umgang mit dem Sicherheitsvorfall durchgeführt werden müssen.

2.4.1 Anforderungen an Audi-CERT

Audi-CERT hat sicherzustellen, dass die am weitesten verbreiteten, grundlegenden Angriffstechniken, wie sie in der Mitre ATT&CK Matrix definiert sind, sowie die Techniken, die von den für Audi wichtigsten Bedrohungsakteuren verwendet werden, erkannt werden können. Wenn Logdateien für diese Erkennungen fehlen, müssen diese an das IT Security Operations-Team gemeldet werden und im Eingliederungsprozess für den Log-Aggregator Priorität erhalten. Audi-CERT muss über die Abdeckung aller relevanten Angriffstechniken berichten. Das Verstehen von relevanten Angriffstechniken basiert auf Audi's aktueller Bedrohungslage basierend auf Audi's aktueller Bedrohungslandkarte, welche im Kontext des TI services entwickelt wird. Unterstützung bei der Entwicklung anwendungsspezifischer Angriffserkennungsregeln ist nur möglich, wenn Service Nutzer die Anforderungen, welche im Abschnitt 2.3.2. aufgelistet sind, erfüllen.

Es ist Audi-CERT's Verantwortung Threat Intelligence in den CSM-Service zu integrieren und eine Erstbewertung von Ereignissen zu potentiellen Sicherheitsvorfällen durchzuführen. Das Ziel einer Integration von Threat Intelligence in den CSM service ist es, verdächtiges Verhalten basierend auf der aktuellen Gefahrenlage, wie sie im TI service beschrieben wird, zu analyisieren.

Der Zeitraum, in dem der CSM-Service betrieben wird (z. B. rund um die Uhr oder nur von 8 bis 17 Uhr an Arbeitstagen) muss von den zuständigen Managern und Prozessbeteiligten festgelegt werden. Diese Festlegungen werden sich auf die Größe der Teams von Audi-CERT und IT Security Operations sowie auf deren Dienstzeiten/Schichtpläne auswirken.

Die von Audi-CERT zur Durchführung einer kontinuierlichen Sicherheitsüberwachung eingesetzten Technologien und Services müssen so bereitgestellt werden, dass die erwarteten Anforderungen an die Services erfüllt werden. Dies bedeutet: Wenn der CSM-Service für AUDI BRUSSELS innerhalb des Zuständigkeitsbereichs von Audi-CERT eine Überwachung im Zeitraum von 9 bis 17 Uhr (Geschäftsstunden an Wochentagen) erfordert, müssen die Überwachungs-Tools eine angemessene Verfügbarkeit in diesem Zeitraum garantieren.

2.4.2 Anforderungen an die Nutzer des Service

Alle Nutzer des CSM-Service müssen Audi-CERT eine Liste der zu überwachenden IT-Assets zur Verfügung stellen. Für jedes Asset müssen

- System Identifikation (z.B. Systemname oder IP Addresse)
- Funktion,
- Netzwerk Topologiekarte,
- PoC (Kontakt),
- relevante Geschäftsprozesse, und
- Geschäftskritikaliätseinschätzung

vollständig durch den jeweiligen Applikationsverantwortlichen bereitgestellt werden.

Die Nutzer des CSM Service müssen für jede von Audi-CERT zu überwachende IT-Umgebung Kontaktpersonen zur Verfügung stellen und sollten für hoch kritische Assets direkte Kontaktpersonen benennen, wenn eine schnellstmögliche Alarmierung erwartet wird. Service Nutzer müssen die Ereignisanalyse zur Verifikation, ob es sich dabei um einen tatsächlichen Sicherheitsvorfall handelt unterstützen.

Jeder Applikationsverantwortlicher bzw. Systemverantwortliche muss sicherstellen, dass alle Log Quellen in ein zentrales Log-aggregationssystem[1] fließen. Sollten dabei Daten fehlen oder in einem ungeeigneten Format vorliegen, so muss der Applikationsverantwortliche sich um die Verbesserung kümmern.

2.5. Incident Response (IR)

Der Zweck des Incident Response-Service besteht darin, zeitnahe, effiziente Ressourcen zum Einordnen, Eindämmen, Abmildern und Ausschalten von Bedrohungen jeglicher IT-Systeme innerhalb des Zuständigkeitsbereichs von Audi-CERT zur Verfügung zu stellen.

Der Incident Response-Service umfasst die Bearbeitung von Sicherheitsvorfällen im Rahmen des Incident Response-Prozesses. Hierzu gehört bei Bedarf auch das Entsenden eines speziellen Incident Response Teams an AUDI BRUSSELS. Audi-CERT muss immer einen Lead Incident Responder bereitstellen, der für die Kommunikation zwischen den Analysten und der Kontaktperson von AUDI BRUSSELS, bei dem der Sicherheitsvorfall aufgetreten ist, und den Analysten zuständig ist, die für die Erfassung forensischer Spuren, die Analyse des Sicherheitsvorfalls, das Erstellen von Statusberichten und für die Weitergabe von Handlungsempfehlungen, wie die Bedrohung eingedämmt, abgemildert und ausgeschaltet werden kann, an die Asset Eigentümer zuständig sind. Der Incident Response-Prozess ist im Kapitel „Incident Response-Prozess“ beschrieben.

[1] Bei Audi wird hierfür die Splunk Infrastruktur eingesetzt

2.5.1 Anforderungen an Audi-CERT

Audi-CERT hat sicherzustellen, dass entsprechend geschultes Personal verfügbar ist, um bei Bedarf innerhalb von 48 Stunden vor Ort auf den Sicherheitsvorfall zu reagieren. Incident Responder müssen den Audi-CERT Incident Response-Prozess und alle anwendbaren Playbooks (Incident Responce Prozesse) befolgen. Sie müssen sicherstellen, dass die vereinbarten Einsatzregeln eingehalten werden und dass die Betriebssicherheit und -zuverlässigkeit für die geschäfts- und insbesondere produktions-/fertigungskritischen Systeme zu allen Zeitpunkten gewährleistet sind.

Reporting nach dem Sicherheitsvorfall und Beiträge zum Prozess des „Lessons Learned[2]“ sind ein wichtiger Aspekt der Reaktion auf Sicherheitsvorfälle, der von Audi-CERT unterstützt werden muss. Audi-CERT ist allerdings nicht dafür zuständig, die Implementierung der Erkenntnisse außerhalb der Audi-CERT Organisation zu verfolgen.

2.5.2 Anforderungen an die Nutzer des Service

Nutzer des Service müssen lokale Kontaktpersonen für alle von einem Sicherheitsvorfall betroffenen Systeme bereitstellen. Die Kontaktpersonen müssen entweder Audi-CERT Incident Responder mit direkten Zugang zu den betroffenen Systemen zur Verfügung stellen oder dafür sorgen, dass Personal verfügbar ist, das von den Incident Respondern im Hinblick auf das Erfassen von forensischen Daten informiert werden und jegliche benötigten forensischen Daten zeitnah zur Verfügung stellen kann. Wenn die zeitnahe Bereitstellung forensischer Daten durch die Nutzer des Service nicht sichergestellt werden kann, gelten die Standard-Reaktionszeiten nicht und können von den Nutzern des Service auch nicht eingefordert werden.

Wenn ein Incident Response-Team vor Ort entsandt werden muss, hat der Nutzer des Service dafür zu sorgen, dass angemessene Büroräumlichkeiten für das Incident Response-Team verfügbar sind. Dazu gehören ein Kontrollraum/Besprechungsraum, ein verschließbarer Lagerraum für gesicherte Spuren bzw. Beweise und die gesamte notwendige Büro-Infrastruktur (Schreibtische, Stühle, Netzwerk-/Internet-Zugang, Strom, usw.).

2.5.3 Berichtskanäle KPIs (Leistungskennzahlen) für die Services von Audi-CERT

Audi-CERT muss KPIs für jeden Service und jeden zugehörigen Prozess definieren, mit denen die Effektivität der einzelnen Services und Prozesse gemessen werden kann. Da es manchmal Abhängigkeiten von Services geben wird, die außerhalb des Einflussbereiches von Audi-CERT liegen, sollten die KPIs so definiert werden, dass diese externen Abhängigkeiten nicht als Faktoren eingerechnet sind. Wenn dies nicht möglich ist, sollte es beim Reporting entsprechend vermerkt werden, wenn eine Abweichung von den KPIs durch eine Abhängigkeit von externen Gegebenheiten verursacht wurde.

2.6. Zuständigkeitsbereich von Audi-CERT

Audi-CERT ist für die Durchführung aller Services zuständig, welche für die IT-Umgebung (inklusive Cloud) und für die Produktionsbereichsumgebung der AUDI BRUSSELS angeboten werden. AUDI BRUSSEL, müssen eine schriftliche Vereinbarung mit Audi-CERT über seinen speziellen Zuständigkeitsbereich innerhalb BRUSSELS und die für jede Umgebung geltenden

[2] Siehe Anhang B.2.2

Einsatzregeln erstellen. AUDI BRUSSELS muss wenigstens eine Kontaktperson für jede in der Zuständigkeitsbereichsvereinbarung beschriebene IT-Umgebung benennen

2.6.1 Rechte und Pflichten von AUDI BRUSSELS bei Nutzung der Services von Audi-CERT

Audi-CERT muss die maximalen Reaktionszeiten einhalten, die in der Prozessbeschreibung der angebotenen Services genannt sind. Falls die maximale Reaktionszeit nicht eingehalten werden kann, muss der zuständige Teamleiter (z. B. Lead CSM Analyst, Lead Incident Responder) AUDI BRUSSELS möglichst umgehend informieren und den Sicherheitsvorfall bei Bedarf an das eigene Management eskalieren, damit die zum Erbringen der Services gemäß den vereinbarten Reaktionszeiten erforderlichen Ressourcen zur Verfügung gestellt werden können.

AUDI BRUSSELS muss alle Daten, Systemzugänge und lokalen Ressourcen zur Verfügung stellen, die Audi-CERT zur Erbringung eines Service entsprechend den Angaben in den Prozessbeschreibungen benötigt. Das bevorzugte Verfahren, um Zugriff auf diese Daten zu ermöglichen, ist die Nutzung etablierter Tools[3]. Wenn diese Voraussetzungen nicht erfüllbar sind, muss die jeweilige Kontaktperson von AUDI BRUSSELS das Audi-CERT und die betroffenen Prozessbeteiligten möglichst umgehend informieren. In diesem Fall gelten die maximalen Reaktionszeiten für die von Audi-CERT angebotenen Services ggf. nicht.

2.7. Priorisierung von Sicherheitsvorfällen

2.7.1 Ersteinschätzung des Sicherheitsvorfalls

Die Ersteinschätzung wird in durch das Audi-CERT CSM Team vorgenommen. Dies erfolgt mit folgendem Verfahren, welches bei Bedarf durch AUDI-CERT angepasst wird:

1. Zielgerichtet oder nicht zielgerichtet?
   Im ersten Schritt der Priorisierung eines Sicherheitsvorfalls wird mithilfe von Threat Intelligence bestimmt, ob es sich um eine zielgerichtete Bedrohung handelt oder nicht. Wenn ein Analyst zumindest anfänglich eine zielgerichtete Bedrohung nicht ausschließen kann, ist zur weiteren Bearbeitung des Sicherheitsvorfalls der Incident Response-Prozess einzuleiten. In diesem Fall wird die Priorität des Sicherheitsvorfalls auf „Hoch“ gesetzt.
2. Wenn eine zielgerichtete Bedrohung nicht bestätigt werden kann oder der Analyst, der die Ersteinschätzung vornimmt, feststellt, dass es sich um eine nicht zielgerichtete Bedrohung handelt, muss die Schwere des Sicherheitsvorfalls anhand der folgenden Metriken eingeordnet werden:
   a. Sind Systeme der Risikoklasse 1 (ITSCM) betroffen?
   b. Sind mehr als 50 Systeme betroffen?
   c. Sind eventuell Daten betroffen, die unter die Bestimmungen von GDPR fallen? (wenn bekannt / offensichtlich)
   d. Besteht eine unmittelbare Gefahr für geschäftskritische oder produktions-/fertigungskritische Prozesse?
   e. Besteht das Risiko, dass sich die Bedrohung in weitere Assets verbreitet (z. B. ein Wurm)?

[3] Bei Audi der Log-Aggregator (Splunk) und die zentrale EDR-Lösung (FireEye HX)

f. Sind Daten der Kategorien „Vertraulich“ oder „Geheim“ betroffen?

Wenn weniger als 3 der obigen Fragen mit „Ja“ beantwortet werden können, ist die Priorität des Sicherheitsvorfalls auf „Mittel“ zu setzen.
Wenn 3 oder mehr der Fragen mit „Ja“ beantwortet werden können, ist die Priorität des Sicherheitsvorfalls auf „Hoch“ zu setzen.
Wenn keine der Fragen mit „Ja“ beantwortet werden kann, ist die Priorität des Sicherheitsvorfalls auf „Niedrig“ zu setzen.

2.7.2 Reaktionszeiten bei Sicherheitsvorfällen

Hinweis: Die Reaktionszeiten gelten nur, wenn den Analysten alle für die Ersteinschätzung notwendigen Daten zur Verfügung stehen. Die Zeit zwischen der Anforderung der Daten durch die Audi-CERT Analysten und der Bereitstellung der Daten durch die zuständigen Asset-Eigentümer darf nicht in die für Audi-CERT geltenden Reaktionszeit eingerechnet werden.

- Die Ersteinschätzung sollte innerhalb von 30 Minuten erfolgen sobald security-relevante Logs verfügbar sind und darf nicht länger als 60 Minuten dauern. Da das Ziel der Ersteinschätzung eine grobe Einordnung der Art der Bedrohung und die Entscheidung für einen angemessenen Bearbeitungsprozess ist, muss damit gerechnet werden, dass der Bericht unvollständig ist, was nicht notwendigerweise ein Problem darstellt.
- Wenn eine mittlere oder hohe Priorität festgestellt wird, müssen die Analysten innerhalb von vier Stunden nach der offiziellen Bekanntgabe des Sicherheitsvorfalls und/oder der Verfügbarkeit aller für eine weitere Ersteinschätzung notwendigen Daten einen ersten Einordnungsbericht vorlegen. Bei einem Sicherheitsvorfall mit mittlerer Priorität sollte der Einordnungsbericht genügend Informationen liefern, anhand derer Audi-CERT und die Prozessbeteiligten entscheiden können, ob der Sicherheitsvorfall über den Incident Handling- oder den Incident Response-Prozess bearbeitet werden soll. Bei einem Sicherheitsvorfall mit hoher Priorität sollte der Einordnungsbericht die Prozessbeteiligten über die nächsten Schritte informieren, z. B. ob eine Reaktion vor Ort notwendig ist und ob externes Personal benötigt wird. In diesem Fall ist der Incident Response-Prozess obligatorisch.

Nach der Ersteinschätzung und -einordnung ist das weitere Meldeverfahren während des Sicherheitsvorfalls zwischen den betroffenen Prozessbeteiligten und dem Lead Incident Responder zu vereinbaren. Allgemein sollte bei Sicherheitsvorfällen mit hoher Priorität, die über den Incident Response-Prozess bearbeitet werden, zunächst am Ende jedes Arbeitstages ein Bericht vorgelegt werden, bei Sicherheitsvorfällen mit mittlerer Priorität ein Bericht pro Woche. Bei Sicherheitsvorfällen mit niedriger Priorität ist während des Vorfalls keine Berichterstellung notwendig, es sei denn, die Prozessbeteiligten fordern einen entsprechenden Bericht an.

Nach Abschluss des Sicherheitsvorfalls ist innerhalb einer Woche ein Abschlussbericht[4] zu erstellen.

[4] Siehe Anhang B.2.1

2.8. KPIs für Audi-CERT Services

Audi-CERT muss für jeden Service und verbunden Prozess KPIs definieren, welche die Effektivität jedes Services und Prozesses messen. Da gelegentlich Service Abhängigkeiten von Services ausserhalb der Verantwortung des Audi-CERTs existieren, sollten KPIs so definiert werden, dass sie diese externen Abhängigkeiten nicht abdecken. Sollte das nicht möglich sein, sollte eine Abweichung in den KPIs, welche von den externen Abhängigkeiten verursacht wurde, bei Reports als solche dargestellt werden.

3. Schwachstellenmanagement

3.1. Ziel

In diesem Kapitel werden die allgemeinen Begriffe, Rollen und zugehörigen Zuständigkeiten und Anforderungen im Zusammenhang mit dem Schwachstellenmanagement (Vulnerability Management) für die Informationssicherheit sowie Schemata zur Kategorisierung von IT-Sicherheitsvorfällen beschrieben.

3.2. Definition einer Schwachstelle

Innerhalb der Informationssicherheit wird eine Schwachstelle als eine Schwäche angesehen, die es einem Angreifer erlaubt, die Einhaltung eines oder mehrerer Sicherheitsziele für ein Informationsobjekt negativ zu beeinflussen. Schwachstellen können aus mehreren Gründen auftreten: Aufgrund eines Fehlers in einem (Geschäfts-) Prozesses, dem Fehlen eines Sicherheitsaspekts in einem (Geschäfts-) Prozess, jedoch höchstwahrscheinlich von einem IT-System.

3.3. Lebenszyklus des Schwachstellenmanagement

AUDI BRUSSELS muss bei der Implementierung eines wiederkehrenden (Geschäfts-) Prozesses die folgenden Fragen adressieren Probleme:

- Identifizierung von Sicherheitslücken,
- Bewertung der Sicherheitslücken,
- Beheben/Minderung von Sicherheitslücken,
- oder (falls eine Behebung nicht möglich ist) dokumentieren der Schwachstelle durch das Informationssicherheit Risikomanagement.

Die Maßnahmen zum Beheben oder Mindern der Schwachstelle oder die Risikoakzeptanz müssen in die Schwachstellenidentifizierung/den Management Prozess zurückgeführt werden.

Diese zirkulären und regelmäßig durchgeführten Aktivitäten stellen den Lebenszyklus des Schwachstellenmanagements dar.

Bei der Umsetzung der oben genannten Prozesse sind folgende Besonderheiten zu berücksichtigen:

3.3.1 Identifizierung von Schwachstellen

AUDI BRUSSELS muss einen Identifizierungsprozess implementieren, der mindestens die folgenden Punkte abdeckt:

- AUDI BRUSSELS muss die Sicherheitsbewertung durchführen, um die Reife der Informationssicherheit in seinen Prozessen zu identifizieren. Es wird empfohlen diese Bewertung mindestens einmal jährlich durchzuführen.
- Informationen über Schwachstellen (z.B. aus Advisories herausgenommen) müssen mit den Informationen über die IT-Infrastruktur bzw. den Appliaktionen aus dem Konfigurationsmanagementsystem verglichen werden. Es empfiehlt sich, diesen Abgleich in Intervallen von nicht mehr als einem Tag durchzuführen. Für die gängigsten Softwarekomponenten bietet CERT-VW einen

Sicherheitsberatungsdienst an. Dies liegt in der Verantwortung des jeweiligen Applikationsverantwortlichen und IT-Service (B/FP-1).

- AUDI BRUSSELS muss netzwerkbasierte Schwachstellenprüfungen gegen Listen bekannter Schwachstellen durchführen um eine unabhängige Sicht auf die Schwachstellen innerhalb der IT-Systeme zu erhalten. Es sollte sichergestellt sein, dass die gesamte Infrastruktur des Unternehmens mindestens alle vier Wochen gescannt wird.
  Hierfür stellt die IT-Sicherheit die Standarlösung „Nessus“ bereit. Es liegt in der Verantwortung des jeweiligen Applikationsverantwortlichen und IT-Service (B/FP-1), dass die Systeme überprüft werden und die Schwachstellen gepatched oder anderweitig mitigiert werden
- AUDI BRUSSELS muss regelmäßig einen Penetrationstest auf die IT-Infrastruktur, speziell auf die Perimeter, durchführen. Penetrationstests der Perimeter sollten in Abständen von nicht mehr als sechs Monate durchgeführt werden..

3.3.2 Bewertung von Schwachstellen

Schwachstellen innerhalb von IT-Systemen treten in der Regel in hohen Mengen und systematischer Ähnlichkeit auf. Daher ist ein standardisiertes Bewertungsverfahren erforderlich.

Schwachstellen in IT-Systemen (sei es durch fehlerhafte Konfiguration oder unsichere Software) muss mit dem Common Vulnerability Scoring System (CVSS)[5], Version 3. bewertet werden. Eine Bewertung wird durchgeführt, um die Priorisierung von Maßnahmen zur Behebung oder Minderung der Schwachstelle zu erleichtern.

Der CVSS bietet drei Arten von Scores zur Bewertung von Informationssicherheits-Schwachstellen:

1. Der *Base Score* stellt einen Rohwert einer Schwachstelle dar und basiert auf Informationen über den möglichen Angriffsvektor, die Angriffskomplexität, falls der Angreifer den angegriffenen Bereich verlassen kann und falls Privilegien und / oder Benutzerinteraktion erforderlich sind oder nicht. Darüber hinaus werden die Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Datenbeständen berücksichtigt.
2. Der *Temporal Score* berücksichtigt zusätzlich zeitliche Vektoren: Wahrscheinlichkeit eines Angriffs, Einfachheit der Behebung der Schwachstelle (z.B. Verfügbarkeit von Patches) und ob die Schwachstelle bestätigt oder unbestätigt ist.
3. Der *Environmental Score* berücksichtigt die tatsächliche lokale Umgebung und basiert auf dem *Base Score*.

Die Konzerngesellschaften können den CVSS *Environmental Score* ändern, wenn dies durch Maßnahmen zur Behebung oder Minderung von Schwachstellen gerechtfertigt ist. Jede Neubewertung muss für jedes System / jede Schwachstelle dokumentiert werden.

[5] http://www.first.org/cvss

3.3.3 Maßnahmen zur Behebung / Minderung von Schwachstellen

Innerhalb von IT-Systemen bedeutet die Behebung von Schwachstellen im Allgemeinen Patchen und / oder Neukonfiguration eines IT-Assets.

Verfügbare Patches / Updates müssen wie in der Patch-Management Regelung definiert installiert werden.

Wenn derzeit keine Patches zur Behebung der Schwachstelle verfügbar sind, müssen andere Maßnahmen zur Schadensminderung ergriffen werden (z.B. Netzwerktrennung, Firewall / IP Regel, Systemänderungen, Beenden des Dienstes, …)

Prozesse, die zur Behebung / Minderung von Schwachstellen dienen, müssen eine SLA bereitstellen, d.h. sie müssen innerhalb einer vorgegebenen maximalen Zeitdauer die Schwachstelle beheben / mindern.

Dieses SLA muss mit an die reale Welt der Hacker-Aktivitäten und der Angriffsfläche des Konzerns ausgerichtet werden.

Eine SLA von einer Woche zur Maßnahmen zur Behebung von Schwachstellen darf nicht überschritten werden.

Die Applikationsverantwortlichen und IT-Service (B/FP-1) sind verantwortlich für die Durchführung dieser Maßnahmen.

II. Verantwortlichkeiten

II.I Kapitel 1: Allgemeine Begriffsbestimmungen im Zusammenhang mit dem IT-Security- Incident-Management

Diese Regelung ist von allen CERTs und CISOs zu befolgen.

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: Verwaltung von IT-Sicherheitsvorfällen

Diese Regelung ist von allen CERTs, alle Verantwortlichen für IT-Systeme / Applikationen, IT-Service (B/FP-1) und alle CISOs zu befolgen.

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: Schwachstellenmanagement

Diese Regelung ist von allen CERTs, LISOs, CISOs und alle Verantwortlichen für IT-Systeme / Applikationen sowie IT-Service (B/FP-1) 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 Good Practice Guide for Incident Management: ENISA – Europäische Agentur für Netz- und Informationssicherheit (www.enisa.europa.eu)

A.1.3 Prozesshandbuch Incident Management

A.1.4 Methodikhandbuch zum GRC Regelprozess (siehe VW Wiki)

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

A.1.6 Informationssicherheit Regelung Nr. 03.03.01 Server

A.1.7 Informationssicherheit Regelung Nr. 03.03.02 Clients

A.1.8 Informationssicherheit Regelung Nr. 03.03.04 Multifunktions- und Peripheriegeräte

A.1.9 Informationssicherheit Regelung Nr. 03.04.02 Bereitstellen sicherer Applikationen

A.2 Anlagen

A.2.1 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 Quellen und Referenzen

-

A.4 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.

Nächstes Inspektionsdatum: 01.10.2023

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[6].

A.5 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht
1.1	Andreas Walter	B/FP	01.10.2020	Adaption für Nutzung AUDI-CERT

[6] Siehe Anhang A.2.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Allgemeine Begriffsbestimmungen im Zusammenhang mit dem IT-Security- Incident-Management

-

B.2 Kapitel 2: IT Defense und Incident Response

B.2.1 Der Kommunikationsweg bei Abschlussberichten für Sicherheitsvorfälle gestaltet sich wie folgt:

1. Der Abschlussbericht wird von einem Audi-CERT Mitglied erstellt.
2. Der Review der Sicherheitsvorfallberichte erfolgt durch ein anderes Teammitglied des Audi-CERTs. Identifizierte Punkte werden von dem Berichtersteller behoben.
3. Der Leiter des CERTs nimmt die Abschlussberichte ab und signiert diese.
4. Der Abschlussbericht wird an den CISO der AUDI BRUSSELS weitergeleitet.
5. Die Managementkontrolle wird durch den CIO der AUDI BRUSSELS
6. Zusätzlich berichtet der Leiter der zentralen IT Sicherheit die abgeschlossenen Sicherheitsvorfälle in die BT-L.

B.2.2 Für alle Sicherheitsvorfälle bei Audi findet CERT intern eine Lessons Learned Session zum Wissens Austausch statt. Darüber hinaus wird für alle Security Incident mit Priorität hoch oder mittel ein Lessons Learned mit der IT-Sicherheit und den betroffenen Fachbereichen durchgeführt. Die IT-Sicherheit übernimmt das Nachverfolgen der identifizierten offenen Punkte und prüft eine Übernahme in Security Awareness Schulungen.

B.3 Kapitel 3: Schwachstellenmanagement

-