Richtlinie

Externe Anbieter von IT-Diensten und IT-nahen Dienstleistungen

Geltungsbereich:	BU tkAB
Prozesseigner:	ISO (Information Security Officer)
Ersteller:	Michael Müller / ISO
Version:	13.03.2024 (V1.1)
Informationsklasse:	Intern

thyssenkrupp

Revisionsverzeichnis:

Version	Änderung	Seite	Date	geändert von
1.0	Erstausgabe	1 - 8	17.03.2023	Michael Müller
1.1	Formale Fehlerkorrektur	3	13.03.2024	Rainer Pusch

Inhalt

1 Ziel dieser Richtlinie

Das Ziel dieser Richtlinie ist die sichere Dienstleitungserbringung externer IT-Dienste und IT naher Dienstleistungen. Dies beinhaltet auch Dienstleistungen die im Produktionsbereich (OT) erbracht werden

2 Beschreibung

Diese Sicherheitsrichtlinie ist verpflichtend für alle externen Anbieter von IT-Diensten, die für ein tkAB verbundenes Unternehmen tätig sind. Diese Vorgaben sind als Mindestanforderung für eine Dienstleistungserbringung innerhalb der tkAB IT zu verstehen.

Soweit diese Mindestanforderungen durch den externen Anbieter von IT-Diensten nicht erfüllt werden können, wird tkAB nicht mit diesem externen Anbieter von IT-Diensten zusammenarbeiten.

2.1 Verantwortlichkeiten

Der externe Anbieter von IT-Diensten hat dafür zu sorgen, dass die Dienstleistungserbringung der hier vorliegenden Richtlinie folgt.

Der beauftragte externe Anbieter von IT-Diensten hat jederzeit sicher zu stellen, dass sein Handeln und das Handeln seiner Beschäftigten nicht die Verfügbarkeit, Integrität oder Vertraulichkeit der IT-Systeme der tkAB Unternehmen beeinträchtigt.

Urheberrechtliche und patentrechtliche Bestimmungen sowie Lizenzvereinbarungen sind einzuhalten.

Die bereitgestellten Zugangsdaten dürfen nicht an Dritte weitergegeben werden.

2.2 Zugang zu Gebäuden und Produktionsstätten

Der externe Anbieter von IT-Diensten muss seine Beschäftigten darauf hinweisen, dass diese sich bei ihrem Ansprechpartner in einem tkAB verbundenen Unternehmen anzumelden haben. Der externe Anbieter von IT-Diensten wird seine Beschäftigten ebenso darauf hinweisen, dass diesen, ein Besucherausweis übergeben wird und dass sie diesen Ausweis deutlich sichtbar tragen müssen.

2.3 Nutzung von IT-Systemen und IT-Infrastrukturen

2.3.1 Nutzungsgrundlage und Nutzungsrechte

Innerhalb der Infrastruktur eingesetzte Hard- und Software darf die Sicherheit und Leistungsfähigkeit der Infrastruktur nicht beeinträchtigen. Daher darf der externe Anbieter von IT-Diensten nur vom Zentralbereich IT freigegebene Produkte und Geräte verwenden. Nutzung von Internet und Kommunikationsinfrastruktur.

Alle Zugriffe können vom Zentralbereich IT zu Diagnose- und Sicherheitszwecken protokolliert werden.

Der externe Anbieter von IT-Diensten hat seine Beschäftigten darauf hinzuweisen, dass, wenn der Zugriff auf Internetressourcen oder E-Mail-Accounts bereitgestellt wurde, die Nutzung von Internet und E- Mail ausschließlich für geschäftliche Zwecke erlaubt ist.

OT-Systeme im Produktionsumfeld dürfen keinen Internetzugriff, auch nicht bei Wartungsarbeiten, erhalten.

Es dürfen ausschließlich tkAB eigene Remote-Support-Lösungen verwendet werden.

Die Verwendung von „Cloud-Lösungen" bedarf immer einer gesonderten Freigabe durch die Abteilung Informationssicherheits-Management der tkAB.

2.3.2 Hard- und Softwaremanagement

Der externe Anbieter von IT-Diensten darf nur IT-Komponenten bereitstellen, installieren oder verbauen, wenn diese vor ihrem Anschluss an das tkAB-Netzwerk (LAN/WLAN/OT/IT) von der IT überprüft und freigegeben worden sind.

Zur Freigabe der Hard- bzw. Software muss eine schriftliche Dokumentation vorliegen. Diese Dokumentation muss mindestens folgende Punkte beinhalten:

- Konfiguration der Netzwerkkomponenten und Funktionen
- Funktion der Software-Schnittstellen
- Benötigte Berechtigungen
- Zugangsdaten

Die vom externen Anbieter von IT-Diensten eingesetzten IT-Komponenten müssen die vorgegebenen IT-Sicherheitslösungen unterstützen. Der externe Anbieter von IT-Diensten muss diese beim Zentralbereich IT anfordern.

Modifikationen an der Hardware oder Software eines Endgerätes (wie z.B. Einbau von Festplatten, Speichererweiterung, WLAN-Karten) müssen mit dem Bereich ITM (tkAB) koordiniert werden.

IT-Komponenten werden ausschließlich in Abstimmung mit dem Bereich ITM (tkAB) vernichtet.

Bei der Nutzung von externen Speichermedien (z.B. USB-Stick, externe Festplatte, USB-Geräte) ist darauf zu achten, dass lediglich von tkAB Bereich ITM freigegebene Medien (siehe Richtlinie „Umgang mit mobilem IT-Equipment“) genutzt werden dürfen.

2.3.3 Netzwerk

Die unternehmenseigene Netzwerkinfrastruktur wird ausschließlich von den dafür autorisierten Stellen betrieben. Jegliche nicht von der IT autorisierte Modifikation ist untersagt.

Ein uneingeschränkter Netzwerkzugriff ist nur für eigene bzw. freigegebene und durch die IT administrierte Endgeräte erlaubt.

Die Verwendung und der Betrieb von WLAN-Komponenten dürfen nur nach Rücksprache mit der IT erfolgen.

2.4 Sicherheitstechnische Mindestanforderungen

Der externe Anbieter von IT-Diensten muss sicherstellen, dass auf der von ihm verwendeten und bereitgestellten Hardware die aktuelle Version des bei tkAB genutzten Virenschutzsystems mit einer aktualisierten Virensignatur-Datenbank installiert ist.

Die aktuellen Updates für Betriebssystem und verwendete Software müssen installiert und mindestens einmal pro Vierteljahr auf Aktualität geprüft werden.

Alle Systeme des Dienstleisters, die zur Erstellung und Konfiguration verwendet werden, müssen ebenso über einen aktuellen Virenschutz verfügen sowie alle sicherheitsrelevanten Systemupdates und Patches müssen installiert sein.

Weiterhin muss der externe Anbieter von IT-Diensten sicherstellen, dass seine Beschäftigten eine Unterweisung hinsichtlich IT-Sicherheit erhalten haben. Sollte zur Erbringung der Dienstleistung die Verarbeitung von personenbezogenen Daten notwendig sein bzw. wenn der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, muss der externe Anbieter von IT-Diensten sicherstellen, dass seine Beschäftigten nach § 5 BDSG unterwiesen und verpflichtet sind.

Die Übertragung von Daten der tkAB an Dritte ist nicht zulässig, sofern keine gesonderte schriftliche Genehmigung vorliegt.

Sämtlicher E-Mail-Verkehr zwischen tkAB und dem externen Anbieter von IT-Diensten ist vertraulich zu behandeln.

Das Speichern von Daten der tkAB in unverschlüsselter Form ist auf mobilen Datenträgern (z.B. USB-Sticks) unzulässig. Ausnahmen erfordern eine gesonderte Genehmigung durch die IT Security.

Daten aller Art, die im Rahmen der Abarbeitung des Auftrags für tkAB generiert werden, befinden sich im Eigentum der tkAB.

Nach Abschluss der Arbeiten sind bereitgestellte Daten aller Art an die beauftragende Gesellschaft zurückzugeben, wobei keine Kopien, Auszüge oder sonstige vollständige oder teilweise Reproduktionen einbehalten werden dürfen.

2.5 Umgang mit technischen Störungen

Der externe Anbieter von IT-Diensten hat seinen Beschäftigten darauf hinzuweisen, dass wenn während des Betriebs Störungen auftreten oder ein IT-Sicherheitsvorfall bekannt wird, umgehend der jeweilige tkAB Ansprechpartner informiert werden muss.

2.6 Regelung bereitgestellte Benutzerkonten

Die erteilten Zugriffsberechtigungen und die Verwendung personenbezogener oder anderer betrieblichen Daten dienen ausschließlich der Erfüllung des Vertragsgegenstandes.

Der externe Anbieter von IT-Diensten hat dafür zu sorgen, dass sich jeder der eingesetzten Beschäftigten mit der für ihn beantragten Benutzerkennung anmelden kann. Die Benutzerkennung und das Passwort dürfen nicht an Dritte weitergegeben werden.

Bei Beendigung des Dienstleistungsvertrages muss der externe Anbieter von IT-Diensten veranlassen, dass alle Ausweise und ausgehändigten Datenträger durch seine Beschäftigten an tkAB zurückgeben werden. Nicht mehr benötigte Benutzerkonten von Beschäftigten des externen Anbieters von IT-Diensten müssen der IT zwecks Deaktivierung unverzüglich gemeldet werden.

2.7 Fernwartung / Fernzugriff

Der lokale Zugriff auf das Netzwerk ist einem Fernzugriff immer zu vorzuziehen. Ein Fernzugriff ist nur nach Rücksprache mit der IT und den nachfolgend aufgeführten Regelungen möglich.

Der Remote Zugriff zur Fernwartung wird nur über tkAB eigene Systeme bereitgestellt, jegliche anderen Möglichkeiten werden nicht unterstützt.

Der externe Anbieter von IT-Diensten muss sicherstellen, dass das eigene Netzwerk seines Beschäftigten keinen unkontrollierten Zugriff Dritter auf das tkAB Netzwerk ermöglicht.

Es dürfen nur durch die tkAB IT freigegebene Verbindungen bzw. Software zur Fernwartung genutzt werden.

Kein IT-System darf eigenständig eine VPN-Verbindung aufbauen.

Der externe Anbieter von IT-Diensten ist verpflichtet, während der Laufzeit der Beauftragung die Funktionalität des Fernzugriffs mindestens einmal pro Vierteljahr zu prüfen.

2.8 Leistungserbringung

2.8.1 Software

Es ist sicherzustellen, dass für entwickelte Softwareprodukte der Quellcode zugänglich ist.

Bei der Softwareentwicklung ist die aktuell gültige Fassung der „tkAB Coding-Guideline for Software Development“ zu beachten.

Bei jeglicher Entwicklungsarbeit in SAP-Systemen ist die aktuelle Entwicklungsrichtlinie für SAP-Entwicklungen der tkAB in der jeweils aktuellen Fassung anzuwenden.

Folgende Aktivitäten sind dem externen IT-Dienstleister grundsätzlich untersagt:

- Modifikationen von SAP-Standard-Objekten
- Anpassungen von Berechtigungsrollen mit externen IT-Diensten
- Änderungen an den Systemeinstellungen (Mandanten-/Systemöffnungen)
- Einplanen periodischer Batch-Jobs sowie Event-gesteuerter Batch-Jobs
- Änderungen an SICF-Dienst-Einstellungen
- Änderungen am Switch-Framework

Vor dem Import in produktiven SAP-Systemen muss eine vollständige Dokumentation aller durchgeführten Entwicklungen vorliegen.

Geltungsgrundlage hierbei ist das gültige Vorgehensmodell für Software-Changes gemäß V-Modell zwecks Einhaltung der IT-Governance für Änderungen an produktiven Systemen der tkAB.

2.8.2 Hardware

Die durch den externen IT-Dienstleister eingebrachte Hardware ist in Absprache mit dem Ansprechpartner bei tkAB den internen Richtlinien entsprechend auszulegen.

Dies beinhaltet auch die Hardware für einen möglichen Remote-Support.

3 Anmerkungen

3.1 Kennzahlen/Indikatoren/Messgrößen

Für die Überwachung und Bewertung dieser Anweisung/Richtlinie bedarf es keiner speziellen Kennzahl.

Die Überwachung und Bewertung erfolgen über die regelmäßig stattfindenden Audits.

3.2 Begriffe

Begriff	Beschreibung
OT	Operational Technology
tkAB	Thyssenkrupp Automotive Body Solutions GmbH
N5	Webbasiertes Dokumentenmanagementsystem für prozessorientierte Integrierte Management Systeme

Weitere Begriffe sind im Prozessportal unter Auskünfte in der „Übersicht der thyssenkrupp Automotive Body Solutions Begriffe“ beschrieben.

3.3 Lenkung und Archivierung

Dieses Dokument wird gemäß dem Vier-Augen-Prinzip über N5 gelenkt und ist ohne Unterschrift gültig.

Die Archivierung erfolgt gemäß „Lenkung von dokumentierten Informationen - Dokumente“ unter Management Prozesse / Integriertes Management System.

3.4 Hinweise

Die Überprüfung und Anpassung der Vorgaben erfolgt in regelmäßig stattfindenden Bewertungs-, Planungs- und Korrekturgesprächen unter Anwendung des PDCA-Zyklus.

3.5 Mitgeltende Unterlagen

Die nachfolgend gelisteten Richtlinien im Umgang mit der Erbringung von IT-Dienstleistungen oder Softwareänderungen sind für externe Lieferanten ergänzend und verpflichtend zu befolgen:

- Entwicklungsrichtlinie für SAP-Entwicklungen der tkAB
- tkAB Coding-Guideline for Software Development
- Umgang mit mobilem IT-Equipment