TÜVIT

Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH
bescheinigt hiermit dem Unternehmen

Telekom Deutschland GmbH
Landgrabenweg 151
53227 Bonn

Zertifikatsgültigkeit:
25.11.2022 – 25.11.2024

für das IT-System

Kundencenter

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ)
Version 10.0
Security Assurance Level SEAL-3

der TÜV Informationstechnik GmbH. Die Anforderungen sind in der Anlage zum Zertifikat zusammenfassend aufgelistet.

Die Anlage ist Bestandteil des Zertifikats mit der ID 9560.22 und besteht aus 4 Seiten.

Essen, 25.11.2022

Dr. Christoph Sutter, Leiter Zertifizierungsstelle

Zum Zertifikat

TÜV Informationstechnik GmbH
Am TÜV 1 ▪ 45307 Essen
tuvit.de

TÜVNORDGROUP

Zertifizierungsprogramm

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Zertifizierungsprogramms durch:

- „Zertifizierungsprogramm (nicht akkreditierter Bereich) der Zertifizierungsstelle der TÜV Informationstechnik GmbH“, Version 1.1 vom 01.03.2020, TÜV Informationstechnik GmbH

Evaluierungsbericht

- „Evaluierungsbericht – Sicherheitstechnische Qualifizierung, Kundencenter”, Version 1.1 vom 02.11.2022, TÜV Informationstechnik GmbH

Evaluierungsanforderungen

- „Trusted Site Security / Trusted Product Security, Sicherheitstechnische Qualifizierung (SQ) Anforderungskatalog für die Version 10.0, Dokumentenversion 2.8 vom 16.03.2020, TÜV Informationstechnik GmbH
- Systemspezifische Sicherheitsanforderungen (siehe unten)

Die Evaluierungsanforderungen sind am Ende zusammenfassend aufgeführt.

Evaluierungsgegenstand

Evaluierungsgegenstand ist das IT-System „Kundencenter“ der Telekom Deutschland GmbH. Dieses wird im Evaluierungsbericht detailliert beschrieben.

Evaluierungsergebnis

Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-3 für IT-Systeme sind erfüllt.

Die system-spezifischen Sicherheitsanforderungen sind erfüllt.

Die im Prüfbericht genannten Empfehlungen sind zu beachten.

Systemspezifische Sicherheitsanforderungen

Die folgenden systemspezifische Sicherheitsanforderungen lagen der Zertifizierung zugrunde und wurden überprüft:

1 Identifizierung und Authentifizierung

Das Kundencenter identifiziert und authentifiziert Endkunden eindeutig und hinreichend stark, um gängigen Angriffen standzuhalten.

2 Zugriffskontrolle und Session Management

Schützenswerte Daten, Dienste und Funktionen werden vom Kundencenter vor unbefugten Zugriffen geschützt.

Die vom Kundencenter verwendeten Sitzungsdaten werden sicher generiert, verwaltet und gelöscht, so dass die Vertraulichkeit gewährleistet wird.

3 Datensicherheit und Transportsicherheit

Vom Kundencenter werden keine vertraulichen Informationen über die interne Netzwerkstruktur preisgegeben.

Die Kommunikation sowie der Zugriff auf das Kundencenter erfolgt über gesicherte Verbindungen, welche die Integrität und Vertraulichkeit der übertragenen Daten nach dem aktuellen Stand der Technik (BSI TR-02102-2) schützen.

Die Zugangsdaten werden vom Kundencenter sicher gespeichert, so dass ihre Vertraulichkeit und Integrität gewährleistet sind.

4 Privacy by Design und Privacy by Default

Das Kundencenter speichert nur erforderliche personenbezogenen Daten, die für die Prozesse der Endkunden erforderlich sind. Nicht mehr erforderliche personenbezogene Daten werden gelöscht.

Die Verarbeitung personenbezogener Daten erfolgt in einer für den Betroffenen fairen und transparenten Weise mit datenschutzfreundlichen Voreinstellungen unter Zugrundelegung einer verständlichen sowie nachvollziehbaren Informationsbasis über die Datenverarbeitung.

5 Systemhärtung

Die aus dem Internet erreichbaren Komponenten und Schnittstellen weisen keine bekannten, ausnutzbaren Schwachstellen auf.

6 Protokollierung

Im Rahmen der Protokollierung werden sicherheitsrelevante Ereignisse erfasst und ausgewertet.

Zusammenfassung der Evaluierungsanforderungen für die Sicherheitstechnische Qualifizierung (SQ), Version 10.0

1 Technische Sicherheitsanforderungen

Die technischen Sicherheitsanforderungen müssen dokumentiert, widerspruchsfrei und überprüfbar sein. Die Spezifikation muss in Anlehnung an ISO/IEC 17007 erfolgen. Des Weiteren müssen die technischen Sicherheitsanforderungen im Rahmen einer individuellen Bedrohungs- und Risikoanalyse hergeleitet sein, sie müssen aus bereits definierten Schutzprofilen hergeleitet sein, oder sie müssen konform zu veröffentlichten Sicherheitsanforderungen anerkannter Autoritäten oder Gremien der IT-Sicherheit sein. Weiterhin müssen sie für den Einsatzzweck des IT-Systems angemessen sein und geltenden Sicherheitsansprüchen genügen.

2 Architektur und Design

Das IT-System muss sinnvoll und verständlich strukturiert sein. Seine Komplexität darf keinen Einfluss auf die Sicherheit haben. Die Härtungs- und Schutzmaßnahmen müssen angemessen und wirkungsvoll sein. Es darf keine konzeptionellen Schwachstellen enthalten, mit deren Hilfe sicherheitsrelevante Komponenten umgangen oder deaktiviert werden können.

3 Installation und Betrieb (ab SEAL-4)

Die vorhandenen Überwachungsmaßnahmen müssen wirkungsvoll sein. Die überwachten Ereignisse müssen geeignet sein, Sicherheitsvorfälle zuverlässig und zeitnah zu erkennen. Die Administration erfolgt über einen vertrauenswürdigen Pfad hinsichtlich Vertraulichkeit und Integrität. Die Dokumentation muss verständlich und nachvollziehbar sein. Sie muss den berechtigten Personen bekannt und jederzeit frei zugänglich sein.

4 Schwachstellenanalyse und Penetrationstests

Die Sicherheitsmaßnahmen des IT-Systems müssen einer Überprüfung durch Penetrationstests standhalten. Es darf nicht möglich sein, Sicherheitsmaßnahmen zu brechen oder zu umgehen. Das IT-System muss sicher konfiguriert sein, darf keine ausnutzbaren Schwachstellen haben und muss alle definierten technischen Sicherheitsanforderungen erfüllen.

5 Änderungsmanagement (ab SEAL-5)

Das Patch-Management muss dokumentiert und für das IT-System geeignet sein. Das Vorgehen bei Änderungen am IT-System muss klar definiert und geeignet sein. Die beteiligten Personen

müssen damit vertraut sein. Verantwortlichkeiten müssen eindeutig geregelt sein. Änderungen dürfen nicht zu einer Reduzierung des erreichten Sicherheitsniveaus führen.

Security Assurance Level

Die folgende Tabelle zeigt die für den Security Assurance Level anwendbaren Prüfkriterien für IT-Systeme. Eine Zertifizierung eines IT-Systems ist möglich ab Level SEAL-3.

		Security Assurance Level				
		SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Evaluierungskriterien	Technische Sicherheits-anforderungen	X	X	X	X	X
	Architektur und Design			X	X	X
	Installation und Betrieb				X	X
	Schwachstellenanalyse und Penetrationstests		X	X	X	X
	Änderungsmanagement					X

Tabelle: Evaluierungskriterien und Security Assurance Level für IT-Systeme