Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Deutsche Telekom AG
Products & Innovation
T-Online-Allee 1
64295 Darmstadt

für das IT-System

Developer Garden App Monitor

die Erfüllung aller Anforderungen der Kriterien

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

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

Die Anlage ist Bestandteil des Zertifikats und besteht aus 5 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht bis zum 31.10.2015.

Security SQ9545.13 TÜViT® 2013 Trusted Site

Voluntary Validation

© TÜViT - Member of TÜV NORD GROUP

Zertifikat-Registrier-Nr.:
TUVIT-SQ9545.13

Essen, 17.10.2013

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
Member of TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de

Zertifizierungssystem

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

- „Zertifizierungsschema für TÜViT Trusted-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, Version 1.0 vom 18.05.2010, TÜV Informationstechnik GmbH

Prüfbericht

- „Sicherheitstechnische Qualifizierung Developer Garden App Monitor der Deutsche Telekom AG“, Version 1.1 vom 07.10.2013, TÜV Informationstechnik GmbH

Prüfanforderungen

- „Sicherheitstechnische Qualifizierung (SQ)® der TÜV Informationstechnik GmbH“, Version 10.0 vom 21.03.2011, TÜV Informationstechnik GmbH
- Systemspezifische Sicherheitsanforderungen (siehe unten)

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

- Gegenstand der Prüfung ist das IT-System „Developer Garden App Monitor“ der Deutsche Telekom AG. Dieses ist im Prüfbericht detailliert beschrieben.

Prüfergebnis

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

- Der Prüfgegenstand erfüllt die systemspezifischen Sicherheitsanforderungen.

Die im Prüfbericht genannten Anmerkungen sind zu beachten.

Systemspezifische Sicherheitsanforderungen

Die folgenden systemspezifischen Sicherheitsanforderungen lagen der Zertifizierung zugrunde und wurden überprüft.

1 Vertrauenswürdiger Pfad

- Die Übertragung der durch das IT-System gesammelten Daten sowie der Zugriff auf die Web-Schnittstelle zum Abruf der Daten (Dashboard) erfolgt über vertrauenswürdige Pfade, welche die Integrität und Vertraulichkeit der übertragenen Daten schützen.
- Die Administration der Server im Backend erfolgt durch autorisierte Personen und wird über vertrauenswürdige Pfade durchgeführt, welche die Integrität und Vertraulichkeit der übertragenen Daten schützen.

2 Authentisierung und Zugriffskontrolle

- Die Web-Schnittstelle zum Abruf der Daten (Dashboard) wird vor unauthentisierten Zugriffen geschützt.
- Die Web-Schnittstelle zum Abruf der Daten (Dashboard) schützt die durch das IT-System aufbereiteten und aggregierten Daten vor unautorisierten Zugriffen.
- Der Zugriff auf die durch das IT-System gesammelten unaufbereiteten Daten (Rohdaten) ist weder durch die Web-Schnittstelle zum Abruf der Daten (Dashboard) noch über den Web-Service möglich.
- Die Komponenten im Backend weisen keine bekannten ausnutzbaren Schwachstellen auf.

3 Datenflusskontrolle

- Die Systeme im Backend werden durch eine mehrstufige Firewall-Installation gegen Angriffe aus dem Internet geschützt.
- Die Netzseparierung im Backend erlaubt keine direkte Verbindung aus unsicheren Netzen in das zu schützende Netz und umgekehrt.
- Die Firewall-Installation des Backends erlaubt nur die für den Betrieb zwingend erforderlichen Kommunikationsverbindungen.
- Sowohl der Web-Service zur Erfassung der Daten, als auch die Web-Schnittstelle zum Abruf der Daten (Dashboard) validieren die Eingabedaten und setzen eine Ausgabekodierung um. Der Web-Service verarbeitet ausschließlich die definierten Daten.

4 Protokollierung

- Im Rahmen der Protokollierung werden sicherheitsrelevante Ereignisse erfasst und ausgewertet.

Zusammenfassung der Anforderungen 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 / Prüfkriterien	SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Technische Sicherheits-anforderungen	X	X	X	X	X
Architektur und Design			X	X	X
Installation und Betrieb			X	X	X
Schwachstellenanalyse und Penetrationstests		X	X	X	X
Änderungsmanagement					X

Tabelle: Prüfkriterien und Security Assurance Level für IT-Systeme