Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

thyssenkrupp Elevator Innovation GmbH
Thyssenkrupp Allee 1
45143 Essen

für das IT-Produkt

MaxBox HV02.00

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 6 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Prüfbericht.

Security TÜViT® 2019 Trusted Product

Certificate ID: 6135.19

Zertifikat ist gültig bis 30.04.2021

Essen, 10.04.2019

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

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 1.0 vom 24.08.2015, TÜV Informationstechnik GmbH

Prüfbericht

- Englisches Dokument: „Evaluation Report Security Qualification MaxBox HV02.00 der thyssenkrupp Elevator Innovation GmbH“, Version 1.0 vom 26.03.2019, TÜV Informationstechnik GmbH

Prüfanforderungen

- „Sicherheitstechnische Qualifizierung (SQ) der TÜV Informationstechnik GmbH“, Version 10.0 vom 21.03.2011, TÜV Informationstechnik GmbH, siehe aktuellen Anforderungskatalog: Trusted Site Security/Trusted Product Security, Sicherheitstechnische Qualifizierung (SQ) Anforderungskatalog für die Version 10.0, Dokumentationsversion 2.7 vom 07.01.2019, TÜV Informationstechnik GmbH
- Produktspezifische Sicherheitsanforderungen (siehe unten)

Die Prüfanforderungen sind am Ende zusammenfassend aufgeführt.

Prüfgegenstand

Gegenstand der Prüfung ist das IT-Produkt MaxBox HV02.00 der thyssenkrupp Elevator Innovation GmbH. Dieser ist im Prüfbericht detailliert beschrieben.

Prüfergebnis

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

Die MaxBox muss in einer sicheren Betriebsumgebung aufgestellt und betrieben werden, die den physischen Zugriffsschutz gewährleistet. Die Anforderungen an eine sichere Betriebsumgebung sind vom Hersteller in der Betriebsanleitung MAX (Version 04/2017 vom 13.04.2017, thyssenkrupp Elevator AG) sowie im MAX-Security Concept (Version 14 von 27.02.2019, thyssenkrupp Elevator AG) geregelt.

Die im Prüfbericht genannten Hinweise und Empfehlungen sind zu beachten.

Produktspezifische Sicherheitsanforderungen

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

1 Authentisierung und Authentifizierung

Die MaxBox verwendet sichere Authentifizierungstechniken, die die Kommunikationsteilnehmer eindeutig identifizieren. Von der MaxBox bereitgestellten Dienste können nur nach vorheriger erfolgreicher Authentifizierung genutzt werden.

2 Vertrauenswürdiger Pfad

Zum Schutz der Integrität und der Vertraulichkeit von übertragenen Daten wird die Kommunikation zwischen der MaxBox und dem Backend-Dienst über einen vertrauenswürdigen Pfad hergestellt.

3 Zugriffskontrolle

Die Daten, Dienste und Funktionen der MaxBox sind im provisionierten Zustand vor unauthentisierten Zugriff über die Netzwerkschnittstelle und das Mobilfunknetz geschützt.

4 Änderungsmanagement

Der MaxBox-Update-Mechanismus akzeptiert nur authentische und vertrauenswürdige Software-Updates vom Hersteller.

5 Systemhärtung

Die MaxBox stellt nur Dienste bereit, die für den vorgesehenen Betrieb erforderlich sind.

6 Protokollierung

Die MaxBox protokolliert sicherheitsrelevante Ereignisse.

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

1 Technische Sicherheitsanforderungen (ab SEAL-1)

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-Produkts angemessen sein und geltenden Sicherheitsansprüchen genügen.

2 Architektur und Design (ab SEAL-3)

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

3 Entwicklungsprozess (ab SEAL-3)

Die Entwicklung des IT-Produkts muss im Rahmen eines definierten Development Life Cycle erfolgen, der mindestens die Phasen Planung, Analyse, Design, Implementierung, Test, Deployment und Maintenance berücksichtigt. Die Maintenance Phase des Development Life Cycle muss Schwachstellen berücksichtigen und beseitigen, mit deren Hilfe sicherheitsrelevante Komponenten umgangen oder deaktiviert werden können. Im Rahmen der Test Phase des Development Life Cycles müssen Tests bezogen auf die Sicherheitsfunktionalität des IT-Produkts berücksichtigt werden.

4 Betriebsvorgaben (ab SEAL-4)

Die Dokumentation bestehend aus den sicherheitsrelevanten Vorgaben an die Betriebsumgebung des Produkts, den Handbüchern zur Installation und Administration sowie den Handbüchern für die Endbenutzer muss gut verständlich und nachvollziehbar sein. Sie muss den berechtigten Personen bekannt und jederzeit frei zugänglich sein.

5 Schwachstellenanalyse und Penetrationstests

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

6 Sourcecode-Analyse (ab SEAL-4)

Der Sourcecode darf keine Verwundbarkeiten, Fehler oder Inkonsistenzen enthalten, wie beispielsweise undokumentierte Befehle, Parameter oder Testfunktionen.

7 Änderungsmanagement (ab SEAL-5)

Das Patch-Management muss lückenlos dokumentiert und für das IT-Produkt geeignet sein. Das Vorgehen bei Änderungen am IT-Produkt muss klar definiert und geeignet sein. Die beteiligten Personen müssen damit vertraut und Verantwortlichkeiten müssen eindeutig geregelt sein. Änderungen an dem IT-Produkt dürfen nicht zu einer Reduzierung des erreichten Sicherheitsniveaus führen.

Security Assurance Level

Die folgende Tabelle zeigt die für den Security Assurance Level anwendbaren Prüfkriterien. Ein Zertifikat kann erteilt werden, wenn ein IT-Produkt die Prüfung erfolgreich durchlaufen und mindestens den Level SEAL-3 erreicht hat.

Security Assurance Level	SEAL-1	SEAL-2	SEAL-3	SEAL-4	SEAL-5
Technische Sicherheitsanforderungen	X	X	X	X	X
Architektur und Design			X	X	X
Entwicklungsprozess			X	X	X
Betriebsvorgaben				X	X
Schwachstellenanalyse und Penetrationstests		X	X	X	X
Sourcecode-Analyse				X	X
Änderungsmanagement					X

Tabelle: Prüfkriterien und Security Assurance Level für IT-Produkte