Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

SLA Software Logistik Artland GmbH
Friedrichstraße 30
49610 Quakenbrück

für das IT-System

Meat Integrity Solution (MIS)

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ)®, Version 10.0
Security Assurance Level SEAL-5

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

Die Anlage ist Bestandteil des Zertifikats und besteht aus 7 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht bis zum 28.02.2017.

Security SQ9546.15 TÜViT® 2015 Trusted Site

Voluntary Validation

Zertifikat-Registrier-Nr.:
TUVIT-SQ9546.15

Essen, 25.02.2015

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
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

- „Sicherheitstechnisch Qualifizierung Meat Integrity Solution (MIS) der SLA Software Logistik Artland GmbH“, Version 1.2 vom 30.01.2015, 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 „Meat Integrity Solution (MIS)“ der SLA Software Logistik Artland GmbH. SLA vertreibt dieses IT-System zur Erfassung und Aufbereitung von Messdaten, die in Schlachtbetrieben im Rahmen der Fleischverarbeitung erhoben werden. Die Messdaten werden dabei signiert abgespeichert und über ein Web-Portal aufbereitet zur Verfügung gestellt. Eine detaillierte Beschreibung des IT-Systems ist im Prüfbericht hinterlegt.

Prüfergebnis

Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung nach Security Assurance Level SEAL-5 für IT-Systeme sind erfüllt.

Der Prüfgegenstand erfüllt die systemspezifischen Sicherheitsanforderungen.

Die im Prüfbericht genannten Empfehlungen sind zu beachten.

Systemspezifische Sicherheitsanforderungen

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

1 Vertrauenswürdiger Pfad

- Die Kommunikation zwischen dem SLA MIS Connector sowie den angeschlossenen Komponenten erfolgt ausschließlich über vertrauenswürdige Pfade, welche die Integrität und Vertraulichkeit der übertragenen Daten schützen.
- Die Kommunikation zwischen dem SLA MIS Connector und der MIS Datenbank erfolgt ausschließlich über vertrauenswürdige Pfade, welche die Integrität und Vertraulichkeit der übertragenen Daten schützen.
- Die Kommunikation zwischen dem MIS System und der zentralen MIS Plattform erfolgt ausschließlich über vertrauenswürdige Pfade, welche die Integrität und Vertraulichkeit der übertragenen Daten schützen.
- Die aus dem Internet erreichbaren Systemkomponenten der Webanwendung enthalten keine zum Zeitpunkt der technischen Untersuchung bekannten, ausnutzbaren Schwachstellen.

- Administrative Tätigkeiten erfolgen über vertrauenswürdige Pfade, welche die Integrität und Vertraulichkeit der Daten schützen.

2 Authentifizierung

- Zum Schutz der Verbindungen innerhalb des MIS Systems werden ausschließlich sichere Authentisierungsverfahren eingesetzt.
- Die Webanwendung verwendet sichere Authentisierungsmerkmale.
- Die Authentisierungsmerkmale werden bei der Authentifizierung durch die Webanwendung auf sichere Weise geprüft.

3 Zugriffskontrolle

- Das MIS System ist nach erfolgreicher Inbetriebnahme gegenüber unautorisierte, lokale Schalt- und Konfigurationsvorgänge geschützt.
- Die innerhalb des MIS Systems gespeicherten Daten sind gegen unautorisierte Zugriffe und Veränderungen geschützt.
- Die Zertifikate und Schlüssel zur Authentisierung und Verschlüsselung werden geschützt gespeichert und sind gegen unberechtigte Zugriffe geschützt.
- Die unautorisierte Kopplung von Komponenten an den SLA MIS Connector wird verhindert.
- Die unautorisierte Änderung von bestehenden Zuordnungen zwischen den Komponenten und dem SLA MIS Connector wird verhindert.

- Das innerhalb der Webanwendung implementierte/genutzte Session Management ist geeignet, die Sitzungen der Benutzer sicher zu separieren.
- Es sind wirksame Zugriffskontrollen umgesetzt, die einen unautorisierten Zugriff auf URL, Geschäftsfunktionen, Daten, Services und Dateien verhindern.
- Die Sicherheitskonfiguration der Webanwendung wird vor unautorisierten Änderungen geschützt.

4 Änderungsmanagement

- Auf dem MIS System wird seitens SLA ausschließlich geprüfte und abgenommene Software eingespielt und installiert.

5 Datenflusskontrolle

- Das MIS System stellt ausgehend ausschließlich Verbindungen zu dem Schlachthof EDV System bzw. der zentralen MIS Plattform her.
- Innerhalb des MIS Systems stehen nur die betrieblich notwendigen Netzwerkdienste zur Verfügung.
- Der unautorisierte Zugriff auf die MIS Datenbank wird durch geeignete Maßnahmen verhindert.
- Die Kommunikation gegenüber der Webanwendung erfolgt ausschließlich über vertrauenswürdige Pfade.
- Die Webanwendung verarbeitet ausschließlich die definierten Daten.
- Die Webanwendung wird durch eine Firewall-Installation geschützt und erlaubt nur die für den Betrieb zwingend erforderlichen Kommunikationsverbindungen.

6 Protokollierung

- Sicherheitsrelevante Ereignisse innerhalb des MIS Systems werden erfasst und ausgewertet.
- Die Fehlerbehandlung sowie die Protokollierungsfunktionalitäten der Webanwendung sind geeignet, um sicherheitsrelevante Ereignisse (z. B. Angriffsversuche) zu identifizieren.
- Die Fehlerbehandlung gibt keine vertraulichen Informationen an unautorisierte Personen preis.
- Für die Betriebssysteme und Serverprozesse ist ein Protokollierungskonzept zur Erfassung und Auswertung von sicherheitsrelevanten Ereignissen umgesetzt.

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
Schwachstellenanalyse und Penetrationstests		X	X	X	X
Änderungsmanagement					X

Tabelle: Prüfkriterien und Security Assurance Level für IT-Systeme