Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

TRIADE InformationSystems GmbH
Stresemannallee 6
41460 Neuss

für den Archivierungsserver

TRIADE TriCSS-Appliance, V1.0.0

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnische Qualifizierung (SQ)®, Version 9.0

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, V1.1 vom 27.08.2007.

Dieses Zertifikat ist bis zum 31.08.2009 gültig.

Security PQ6106.07 TÜViT® 2007 Trusted Product
Voluntary Validation

09

Zertifikat-Registrier-Nr.:
TUVIT-PQ6106.07

Essen, 04.09.2007 gez. Dr. Sutter
Zertifizierungsstelle

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Langemarckstraße 20
45141 Essen
www.certuvit.de

TÜV®

Prüfbericht

„Sicherheitstechnische Qualifizierung (SQ)® des Produktes TriCSS-Appliance 1.0.0 der TRIADE InformationsSystems GmbH“, Version 1.1 vom 27.08.2007, TÜV Informationstechnik GmbH

Prüfvorgehen

Die Anforderungen für die Sicherheitstechnische Qualifizierung (SQ)® des Produktes wurden aus einer Teilmenge der Prüfkriterien für Dokumentenmanagement-Lösungen (PK-DML)[1] hergeleitet. Im Folgenden sind die PK-DML relevanten Anforderungen zusammen mit den abgeleiteten produktspezifischen Sicherheitsanforderungen sowie den funktionalen und qualitativen Anforderungen aufgelistet.

PK-DML – Relevante Anforderungen

Folgende für Archivierungssysteme relevante Anforderungen der PK-DML liegen der Zertifizierung zugrunde.

3.x Dokumentation von Systemkomponenten, Funktionalität und Schnittstellen

4.5 Benutzerverwaltung und Berechtigungskonzept

4.6 Konsistenzsicherung + Transaktionssicherung

4.7 / 6.17 Protokollierung

4.8 Ausfallsicherheit

4.9 Zugriff

5.10 Überwachung des ordnungsgemäßen Betriebs

5.12 Aktualisierung SW

5.14 Recovery

6.12 Bearbeitungsvermerke

6.16 Unveränderbarkeit

[1] Prüfkriterien für Dokumentenmanagement-Lösungen (PK-DML), Ausgabe März 2004, herausgegeben vom Verband für Organisations- und Informationssysteme, e. V. (VOI). Die Listennummerierung ist dem Kriterienwerk entnommen.

Produktspezifische Sicherheitsanforderungen

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

Identifizierung & Authentisierung

1. Das IT-Produkt muss Benutzer eindeutig identifizieren und authentifizieren.
2. Die Authentisierungsdaten müssen hinreichend stark sein, um gängigen Angriffen ausreichend lange standzuhalten.
3. Fehlversuche bei der Authentisierung gegenüber dem IT-Produkt insbesondere für den administrativen Bereich müssen erkennbar sein.

Zugriffskontrolle

4. Das IT-Produkt muss Funktionen bereitstellen, die es ermöglichen, Zugriffsrechte der Benutzer einzuschränken.
5. Einem Benutzer darf es mit vertretbarem Aufwand nicht möglich sein, seine Rechte unbefugt zu erweitern.
6. Die von dem IT-Produkt zur Verfügung gestellten Dienste müssen auf die betrieblich notwendigen Dienste beschränkt sein. Die Zugangsmöglichkeit auf Konsolenebene muss deaktivierbar sein.
7. Die Authentisierung gegenüber den Netzwerkfreigaben soll sowohl auf Benutzer- als auch auf IP-Ebene möglich sein.

Transportverschlüsselung

8. Die Kommunikation über unsichere Netze muss über einen vertrauenswürdigen Pfad erfolgen, der die Vertraulichkeit der übertragenen Daten sicherstellt. Dieses betrifft im Speziellen die Kommunikation bei administrativen Arbeiten an der TriCSS Appliance.

Logging

9. Eine zuverlässige und nachvollziehbare Protokollierung von verschiedenen Ereignissen muss gegeben sein. Dies umfasst neben dem Logging von Anmeldungen am System ebenso die Ausgabe von System- und Applikationsrelevanten Ereignissen.

Funktionale und qualitative Anforderungen

Die folgenden produktspezifischen funktionalen und qualitativen Anforderungen liegen der Zertifizierung zugrunde und wurden überprüft.

Statusüberwachung

10. Eine Systemszustandsüberwachung hinsichtlich der Prozesse, Kapazitäten und Auslastungen muss implementiert sein.

Software-Update

11. Für die Erweiterung des IT-Produktes und Ausbesserung von Softwarefehlern müssen im administrativen Bereich Updates eingespielt werden können.

Ausfallsicherheit

12. Eine Prüfung der übertragenen Daten auf Vollständigkeit muss erfolgen. Dies verhindert im Falle einer temporären Störung die Speicherung unvollständiger und damit fehlerhafter Dateien.
13. Der Ausfall eines Festplattensystems darf nicht zum Ausfall des Systems führen. Die Daten müssen weiter zugreifbar sein.
14. Datenbank-Inkonsistenzen müssen korrigierbar sein.

Dokumentation

15. Die Dokumentation der TriCSS Appliance soll die allgemeine Funktionsweise und Systemwartung beschreiben und darüber hinaus eine seitens des Herstellers empfohlene Konfiguration im Detail beinhalten.

TÜV®

Zusammenfassung der Anforderungen für die Sicherheitstechnische Qualifizierung (SQ)®, Version 9.0

1. Technische Sicherheitsanforderungen

Basierend auf anerkannten Kriterien, Spezifikationen oder Normen sind Sicherheitsanforderungen definiert. Diese weisen keine inhaltlichen Widersprüche auf und genügen geltenden Sicherheitsansprüchen.

2. Dokumentation der Architektur

Für die Qualifizierung des IT-Produkts und seiner Einsatzumgebung bzw. des IT-Systems liegen für die Untersuchung angemessene Beschreibungen aller notwendigen Komponenten vor. Aus diesen sind die gegenseitigen Nutzungsbeziehungen und Datenflüsse sowie die Erfüllung der Sicherheitsanforderungen erkennbar.

3. Benutzer-, Administrations- und sonstige Betriebsdokumente

Geeignete Handbücher zur Installation, Administration und Benutzung liegen vor. Diese enthalten insbesondere Hinweise zur Konfiguration der notwendigen System- bzw. Produktkomponenten sowie zu den räumlichen Maßnahmen und zu personellen Verantwortlichkeiten, die den Sicherheitsanforderungen genügen.

4. Sicherheit der verwendeten Komponenten

Für alle Teilkomponenten, die Sicherheitsfunktionalitäten realisieren, konnte anhand von bereits durchgeführten formalen Evaluationen und/oder öffentlich zugänglichen Informationen nachvollzogen werden, dass sie als vertrauenswürdig eingestuft werden können.

5. Mittel des Systemmanagement

Es existieren geeignete Konfigurationsmöglichkeiten sowie ein angemessenes Monitoring und Logging, die den sicheren Betriebszustand gewährleisten. Dafür eingesetzte Werkzeuge unterliegen denselben Sicherheitsanforderungen, wie das IT-Produkt / das IT-System selbst.

6. Tests und Inspektionen

Umfangreiche Penetrationstests und technische Schwachstellenanalysen sind bei der Prüfung durchgeführt worden. Sofern bei den Tests und Analysen Schwachstellen ermittelt wurden, sind sie entsprechend ihres Risikograde bewertet worden.

7. Änderungsmanagement

Für die Planung und Durchführung von Neukonfigurationen sowie das Einspielen von Updates liegt ein Konzept vor, um Risiken und deren Auswirkungen adäquat bewerten zu können sowie die Erhaltung des angestrebten Schutzniveaus zu gewährleisten. Dieses legt dar, in welcher Weise Änderungen stattfinden dürfen und wie ggf. die Dokumentation angepasst wird.

8. IT-Systeme: Operationelle Umgebung

Es liegen geeignete operationelle Bedingungen vor. Die personellen Verantwortlichkeiten und räumlichen Gegebenheiten genügen dem Sicherheitsanspruch des IT-Systems.

9. Sicherheitsanalysen

Die Ergebnisse der vorher genannten Bewertungsaspekte sind im Rahmen einer abschließenden Analyse den Sicherheitsanforderungen gegenübergestellt und in einem Prüfbericht dokumentiert. Das Ergebnis ist, dass sämtliche Sicherheitsanforderungen erfüllt und die resultierenden Restrisiken tragbar sind.