Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

Verteilnetzbetreiber (VNB) Rhein-Main-Neckar GmbH & Co. KG
Frankfurter Straße 100
64293 Darmstadt

für das IT-System

Querverbundleitstelle Darmstadt

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 7 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem zugehörigen Prüfbericht bis zum 30.06.2014.

Security SQ9544.12 TÜViT® 2012 Trusted Site
Voluntary Validation
© TÜViT - Member of TÜV NORD Group

Zertifikat-Registrier-Nr.:
TUVIT-SQ9544.12

Essen, 11.06.2012

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

Zertifizierungssystem

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH führt Zertifizierungen auf Basis des folgenden Produkt-Zertifizierungssystems durch:

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

Prüfbericht

- „Querverbundleitstelle Darmstadt des Verteilnetzbetreiber (VNB) Rhein-Main-Neckar GmbH & Co. KG“, Version 1.1 vom 29.05.2012, TÜViT GmbH

Prüfanforderungen

- „Sicherheitstechnische Qualifizierung (SQ)® der TÜV Informationstechnik GmbH“, Version 9.0 vom 01.10.2006, TÜViT GmbH
- Systemspezifische Sicherheitsanforderungen (siehe unten)

Prüfgegenstand

Gegenstand der Prüfung ist das IT-System Querverbundleitstelle (QVL) Darmstadt des Betreibers Verteilnetzbetreiber (VNB) Rhein-Main-Neckar GmbH & Co. KG. Die Querverbundleitstelle besteht aus 2 Leitstellen in Darmstadt und die für die Anbindung des Standorts Aschaffenburg notwendigen Systeme des Verbundleitsystems der Aschaffenburger Versorgungs-GmbH (AVG).

Untersucht wurden ausschließlich die unten aufgeführten systemspezifischen Sicherheitsanforderungen auf Basis der Sicherheitstechnischen Qualifizierung SQ®. Weitere Eigenschaften des IT Systems sind nicht Gegenstand der Zertifizierung.

Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheitstechnische Qualifizierung SQ® sind erfüllt.
- Die systemspezifischen Sicherheitsanforderungen sind erfüllt.
- Die im Prüfbericht genannten Empfehlungen sind zu beachten.

Systemspezifische Sicherheitsanforderungen

Die folgenden systemspezifischen Sicherheitsanforderungen des Dokuments:

- „Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“, Version 1.0 vom 10.06.2008, Bundesverband der Energie- und Wasserwirtschaft e. V.

liegen der Zertifizierung zugrunde und wurden überprüft.

1 Allgemeines/ Organisation

Der Bereich Allgemeines/ Organisation ist aufgeteilt in den Unterbereich Allgemeines mit den Unterpunkten:

- Sichere Systemarchitektur
- Ansprechpartner
- Patchfähigkeit, Patchmanagement
- Bereitstellung von Sicherheitspatches für alle Systemkomponenten

- Support für eingesetzte Systemkomponenten
- Verschlüsselung sensibler Daten bei Speicherung und Übertragung
- Verschlüsselungsstandards
- Interne/externe Sicherheits- und Anforderungstests und zugehörige Dokumentation
- Sichere Standard-Konfiguration und Erstinstallation bzw. (Wieder-) Inbetriebnahme
- Integritäts-Prüfung

und den Unterbereich Dokumentation mit den Unterpunkten:

- Design-Dokumentation, Beschreibung sicherheits-relevanter Systemkomponenten und Implementations-Spezifikationen
- Administrator- und Benutzer-Dokumentation
- Dokumentation sicherheitsrelevanter Einstellungen und Systemmeldungen
- Dokumentation der Voraussetzungen und Umgebungs-Anforderungen für den sicheren System-Betrieb

2 Basissystem

Der Bereich Basissystem ist aufgeteilt in die Unterbereiche:

- Grundsicherung und Systemhärtung
- Antiviren-Software
- Autonome Benutzerauthentifizierung

3 Netze/ Kommunikation

Der Bereich Netze/ Kommunikation ist aufgeteilt in den Unterbereich Sichere Netzwerkkonzeption und Kommunikationsverfahren mit den Unterpunkten:

- Eingesetzte Protokolle und Technologien
- Sichere Netzwerkstruktur
- Dokumentation der Netzwerkstruktur und –konfiguration

und den Unterbereich Sichere Wartungsprozesse und RAS-Zugänge mit den Unterpunkten

- Sichere Fern-Zugänge
- Anforderungen an die Wartungsprozesse
- Funktechnologien: Bedarf und Sicherheitsanforderungen

4 Datensicherung/ -wiederherstellung und Notfallplanung

Der Bereich Datensicherung/ -wiederherstellung und Notfallplanung ist aufgeteilt in die Unterbereiche

- Backup: Konzept, Verfahren, Dokumentation, Tests und
- Notfallkonzeption und Wiederanlaufplanung

Die darüber hinaus im Whitepaper enthaltenen Sicherheitsanforderungen der Bereiche „Anwendung“ sowie „Entwicklung, Test und Rollout“ sind für Systemprüfungen nicht relevant. Sie sind nicht Gegenstand der Zertifizierung.

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. Die bei den Tests und Analysen ermittelten Schwachstellen sind 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.