Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

e-netz Südhessen GmbH & Co. KG
Dornheimer Weg 24
64293 Darmstadt

für das IT System

Querverbundleitstelle Darmstadt

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 30.06.2016.

Security SQ9550.14 TÜViT® 2014 Trusted Site

Voluntary Validation

© TÜViT - Member of TÜV NORD GROUP

Zertifikat-Registrier-Nr.:
TUVIT-SQ9550.14

Essen, 17.07.2014

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 Basis des folgenden Produkt-Zertifizierungssystems durch:

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

Prüfbericht

- „Querverbundleitstelle Darmstadt der e-netz Südhessen GmbH & Co. KG“, Version 1.2 vom 10.07.2014, 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 „Querverbundleitstelle (QVL) Darmstadt“ des Betreibers „e-netz Südhessen 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® nach Security Assurance Level SEAL-5 für IT-Systeme 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 sicherheitsrelevanter Systemkomponenten und Implementationsspezifikationen
- 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 lediglich für Produktprüfungen relevant. Sie sind nicht Gegenstand der Zertifizierung.

TÜV®

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