Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

RWE Effizienz GmbH
Freistuhl 7
44137 Dortmund

für die Firewall- und Serverinstallation

SmartHome Backend und Webservices

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 und ist bis zum 31.03.2013 gültig.

Security SQ9540.11 TÜViT® 2011 Trusted Site
Voluntary Validation

Zertifikat-Registrier-Nr.:
TUVIT-SQ9540.11

Essen, 13.05.2011

Joachim Faulhaber
Stellv. 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-Zertifikate der Zertifizierungsstelle TÜV Informationstechnik GmbH“, Version 1.0 vom 18.05.2010, TÜViT GmbH

Prüfbericht

- „Auflagenprüfung SmartHome Backend und Webservices“, Version 1.1 vom 07.04.2011, TÜViT GmbH
- „Sicherheitstechnische Qualifizierung (SQ)® SmartHome Backend und Webservices“, Version 1.1 vom 02.03.2011, 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 die Firewall- und Serverinstallation „SmartHome Backend und Webservices“ der RWE Effizienz GmbH. Dieser ist im Prüfbericht detailliert beschrieben.

Der Prüfgegenstand SmartHome Backend und Webservices ist Teil der SmartHome-Lösung der RWE Effizienz GmbH.

- Smarthome Backend und Webservices: Das Backend beinhaltet die notwendigen Dienste und Webservices, um den Betrieb der SmartHome-Lösung zu unterstützen. Dazu gehören die Registrierung der Smart Home Controller

(SHC), die Zuordnung der SHC zu Benutzern, das Speichern der angelegten Profile, Device-Management sowie Softwareupdates.

Die Lösung besteht aus den folgenden weiteren drei Hauptkomponenten, die jedoch nicht Gegenstand der Zertifizierung sind:

- SmartHome Controller: Der SHC steuert direkt die angeschlossenen Devices. Zudem können die Devices über Regeln und Profile gesteuert werden, die auf dem SHC hinterlegt werden.
- SmartHome Devices: Die Devices bestehen in der jetzigen Ausbaustufe aus den Aktoren Heizkörperthermostat und Zwischenstecker sowie aus dem Sensor Wandsender. Die Aktoren können vom SHC entweder durch Einrichten eines Zeitprofils oder durch eine direkte Anwenderanfrage über einen Control/Configuration Node gesteuert werden. Zudem ist es möglich, dass Sensoren und Aktoren direkt verbunden werden.
- Control and Configuration Node: Der Control and Configuration Node ist die zentrale Anwenderschnittstelle, mit welcher der Endanwender die SmartHome-Lösung entsprechend seinen Vorstellungen einrichten kann. Mit dieser Anwenderschnittstelle (Silverlight-Applikation oder webbasierter Client) kann der SHC sowohl aus dem lokalen Netzwerk als auch über Remote Control/Configuration Nodes und mobile Geräte gesteuert werden.

Prüfergebnis

- Die anwendbaren Anforderungen für die Sicherheits-technische Qualifizierung sind erfüllt.

- Die systemspezifischen Sicherheitsanforderungen sind erfüllt.

Systemspezifische Sicherheitsanforderungen

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

1 Vertrauenswürdiger Pfad

- Die Kommunikation zwischen dem Control und Configuration Node und den Servern im Backend erfolgt über vertrauenswürdige Pfade, die die Integrität und Vertraulichkeit der übertragenen Daten schützen.
- Die Administration der Server im Backend erfolgt durch von RWE autorisierte Personen und wird über vertrauenswürdige Pfade durchgeführt, die die Integrität und Vertraulichkeit der übertragenen Daten schützen.

2 Authentisierung

- Das Backend verwendet Authentisierungsverfahren, die die Verbindung zwischen SHC und Backend schützen.
- Fehlerhafte Authentifizierungsversuche werden abgewiesen.

3 Zugriffskontrolle

- Konfigurations- und Profildaten, die im Backend gespeichert werden, sind gegen unautorisierte Zugriffe geschützt.
- Bei Nutzung der Webservices des Backends sind die Schalt- und Konfigurationsvorgänge vor Manipulationen geschützt.
- Die Komponenten im Backend weisen keine bekannten ausnutzbaren Schwachstellen auf.

4 Datenflusskontrolle

- Die Systeme im Backend werden durch eine mehrstufige Firewall-Installation gegen Angriffe aus dem Internet geschützt.
- Die Netzseparierung im Backend erlaubt keine direkte Verbindung aus dem unsicheren Netz in das zu schützende Netz und umgekehrt.
- Die Firewall-Installation des Backends erlaubt nur die für den Betrieb erforderlichen Kommunikations-verbindungen.
- Die interne Struktur des Backends wird verdeckt.

5 Protokollierung

- Sicherheitsrelevante Ereignisse werden bei den Firewallkomponenten des Backends auf einem zentralen Protokollierungsserver gespeichert und regelmäßig ausgewertet.
- Der Systemzustand der Komponenten im Backend wird hinsichtlich Prozesse, Kapazitäten und Auslastung überwacht.
- Spezielle, einstellbare Protokollmeldungen einzelner Systemkomponenten führen zu einer unverzüglichen Warnung der Verantwortlichen.

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. 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.