Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

T-Systems Business Services GmbH
Godesberger Allee 117
53175 Bonn

für den IP-basierten Telefonie- und Internet-Anschluss

Business Access IP (BAIP), Rel. 3

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, V1.2 vom 29.04.2008.

Dieses Zertifikat ist bis zum 31.05.2010 gültig.

Security PQ6112.08 TÜViT® 2008 Trusted Product
Voluntary Validation

Zertifikat-Registrier-Nr.:
TUVIT-PQ6112.08

Essen, 19.05.2008 gez. Dr. Sutter

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

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

Prüfbericht

- „Sicherheitstechnische Qualifizierung (SQ)® des Business Access IP (BAIP), Releasestand 3 der T-Systems Business Services GmbH“, Version 1.2 vom 29.04.2008, TÜV Informationstechnik GmbH

Prüfanforderungen

- Produktspezifische Sicherheitsanforderungen (siehe unten)
- Sicherheitstechnische Qualifizierung (SQ)®, Version 9.0, TÜV Informationstechnik GmbH

  Hinweis:
  Hierbei sind für ein Produkt die SQ-Anforderungen unter Punkt 8. „IT-Systeme: Operationelle Umgebung“ nicht anwendbar.

Prüfobjekt

Das Prüfobjekt „Business Access IP (BAIP), Releasestand 3“, besteht aus den beiden Komponenten:

- Integrated Access Device (IAD), Releasestand 10 (ONEOS5-VOIP_SIP-V3.7R10E10_BAI_10D), mit den folgenden lokalen Anschlüssen:
  - für TK-Endgeräte,
  - für IP-Endgeräte (LAN und DMZ),
  - zum Provider Edge mit Administrations-, Voice- und Internetkanal und
  - für die serielle Konsole zur Installation des IAD.
- Provider Edge (PE), Releasestand 8.1.R4.3, einschließlich der Administrations-, Voice- und Internet-Schnittstelle zu den Integrated Access Devices (IAD) und der Schnittstelle des PE zum Internet.

Die IAD werden beim Kunden aufgestellt und das PE wird zentral von T-Systems betrieben.

Produktspezifische Sicherheitsanforderungen

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

Vertrauenswürdiger Pfad

- Der Internetverkehr wird vom PE bis zur Internetschnittstelle ausschließlich in Netzwerken der Deutsche Telekom AG übertragen.
- Die IP-Telefonie wird vom PE bis zum öffentlichen Telefonnetz ausschließlich in Netzwerken der Deutsche Telekom AG übertragen.
- Die Inbetriebnahme des IAD (auch Autokonfiguration genannt) erfolgt über einen vertrauenswürdigen Pfad innerhalb des Netzwerks der Deutsche Telekom AG.
- Die Authentisierung des IAD im laufenden Betrieb erfolgt über einen vertrauenswürdigen Pfad innerhalb des Netzwerks der Deutsche Telekom AG.
- Zentrale Komponenten, die zum Betrieb des BAIP benötigt werden, sind in Serverräumen positioniert.

Zugriffskontrolle

- Eine unautorisierte Person kann nicht über das IAD eines Kunden telefonieren und kann das IAD nicht administrieren.
- Der IAD schützt sich selbst gegen bekannte Angriffe aus dem Internet.
- Die Administration des IAD während der Inbetriebnahme und im laufenden Betrieb erfolgt ausschließlich durch von T-Systems autorisierte Personen und Systeme.

- Am IAD werden drei separate logische Kanäle, sogenannte Permanent Virtual Circuits (PVC), für Voice, Internet und Administration verwendet. Diese werden am PE konfiguriert. Ein Zugriff vom Internet auf die Voice- und Administrations-Daten ist nicht möglich.
- Nach erfolgter Inbetriebnahme ist das IAD vor unberechtigter Administration und Konfiguration über die serielle Schnittstelle geschützt.

Änderungsmanagement

- Es wird nur von T-Systems geprüfte und abgenommene, vertrauenswürdige Software in das IAD eingespielt und installiert.

Datenflusskontrolle

- Das IAD beinhaltet Basis-Sicherheitsfunktionen (Firewall) mit folgenden Eigenschaften:
  - Ein direkter Verbindungsaufbau aus dem Internet in das Kundennetzwerk (LAN) über das IAD ist nicht möglich.
  - Ein Verbindungsaufbau aus der DMZ zum LAN ist nicht möglich.
- Es ist sichergestellt, dass von dem IAD eines Kunden kein Zugriff auf die Voice- und Administrationsdaten des IAD eines anderen Kunden möglich ist.

Verfügbarkeit

- Das BAIP erlaubt eine hochwertige Sprachqualität durch Konfiguration einer reservierten Bandbreite des Voice Kanals von 256 / 512 kbit bei 2,3 / 4,6 Mbit Gesamtbandbreite.
- Im Rahmen des Vertrages mit dem Kunden garantiert T-Systems eine Verfügbarkeit des VoIP-Dienstes von 97%.

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.