Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

KDVZ Citkomm
Griesenbraucker Straße 4
58640 Iserlohn

für das VPN-Gateway

iWAN-Gateway, Version 2

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 30.04.2013 gültig.

Security PQ6119.11 TÜViT® 2011 Trusted Product
Voluntary Validation

Zertifikat-Registrier-Nr.:
TUVIT-PQ6119.11

Essen, 05.04.2011

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 der 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

- „Prüfbericht Sicherheitstechnische Qualifizierung (Nachprüfung) des iWAN-Gateways, Version 2, der KDVZ Citkomm“, Version 1.0 vom 10.03.2011, TÜViT GmbH

Prüfanforderungen

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

  Hieraus sind für Produkte die Anforderungen unter Punkt 8. „IT-Systeme: Operationelle Umgebung“ nicht anwendbar.

- Produktspezifische Sicherheitsanforderungen (siehe unten)

Prüfgegenstand

Der Prüfgegenstand, das iWAN-Gateway, Version 2, ist ein VPN-Gateway mit Firewall-Funktionalität und besteht aus den Komponenten

- iWAN-baseGate, Releasestand 2,
  zur Anbindung eines einzelnen Kunden-LANs an ein Virtuelles Privates Netzwerk (VPN)

- iWAN-easyGate, Releasestand 2,
  zur Anbindung weiterer verteilter IT-Komponenten des Kunden-LANs

jeweils mit Netzwerkschnittstellen für LAN- und Internet-Verbindungen und einer ISDN-Backup Schnittstelle.

Das Produkt „iWAN-Home“ ist nicht Teil des Prüfgegenstands.

Prüfergebnis

- Der Prüfgegenstand erfüllt die anwendbaren Anforderungen der Kriterien „Sicherheitstechnische Qualifizierung (SQ)®“.
- Der Prüfgegenstand erfüllt die produktspezifischen Sicherheitsanforderungen.

Produktspezifische Sicherheitsanforderungen

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

1 Identifizierung & Authentifizierung

- Die eindeutige Identifikation und Authentifizierung für Benutzer sowie die Verwaltung der iWAN-Gateways selbst durch die Administratoren der KDVZ erfolgt über einen vertrauenswürdigen Pfad, der die Integrität und Vertraulichkeit der übertragenen Daten schützt.
- Dem Aufbau eines VPN zwischen den iWAN-Gateways liegt eine eindeutige und erfolgreiche Identifizierung und Authentifizierung der beteiligten iWAN-Gateways als Terminierungsendpunkte zu Grunde.
- Fehlversuche bei der Authentifizierung gegenüber den iWAN-Gateways insbesondere für den administrativen Bereich werden als Protokollierungsinformationen gespeichert.

2 Zugriffskontrolle

- Das iWAN-Gateway schützt sich selbst vor den zum

Zeitpunkt der Prüfung bekannten Angriffen

- aus dem Internet,
- aus dem aufgebauten VPN und
- aus weiteren an das iWAN-Gateway angeschlossenen lokalen Netzwerken.

- Auf dem eingesetzten iWAN-Gateway sind nur zum Betrieb unbedingt erforderliche Software und Dienste vorhanden.

3 Datenflusskontrolle

- Für den Schutz der lokalen Netzwerkstruktur ist eine Mehrstufigkeit der Firewall-Architektur des iWAN-Gateway umgesetzt. Eine direkte Verbindung aus dem Internet in das zu schützende Netzwerk und umgekehrt ist dabei nicht möglich.
- Das Standard-Regelwerk des iWAN-Gateway stellt sicher, dass
  - alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden (White-List) und
  - die Filterregeln logisch widerspruchsfrei und in der Reihenfolge zur Abarbeitung konsistent festgelegt sind.
- Der Paketfilter mit Stateful Packet Inspection unterstützt mindestens eine getrennte Filterung eingehender und abgehender Pakete an jeder Netzwerkschnittstelle durch Weiterleiten oder Verwerfen von Paketen anhand:
  - der Quell-IP- und Ziel-IP-Adresse einzelner Rechner oder Teilnetze,
  - des Quell- und Zielports für TCP- und UDP-Pakete,

- des ICMP-Subtypes,
- der TCP-Flags (URG, ACK, PSH, RST, SYN, FIN),
- des Verbindungsstatus bei verbindungsorientierten Protokollen (z. B. TCP).

- Es werden mindestens folgende Aktionen für jede Filterregel unterstützt:
  - Weiterleiten des Pakets („Allow“),
  - Verwerfen des Pakets („Deny & Drop“),
  - Verwerfen des Pakets und Meldung an den Absender („Deny & Reject“).

4 Übertragungssicherheit

- Die Vertraulichkeit des Datenverkehrs innerhalb des VPN zwischen den iWAN-Gateways wird durch geeignete Kryptoverfahren sichergestellt.

5 Protokollierung

- Für jede aufgebaute oder abgewiesene VPN-Verbindung des iWAN-Gateways ist eine Protokollierung von:
  - IP-Adresse (Gegenstelle/User),
  - Portnummer (Dienst),
  - Uhrzeit und Datum für jedes Paket,

  des Quell- und Zielsystems möglich.
- Das iWAN-Gateway bietet die Möglichkeit, alle Protokollierungsinformationen über einen vertrauenswürdigen Pfad, der die Integrität und Vertraulichkeit der übertragenen Daten schützt, an eine konfigurierbare zentrale Stelle bei der KDVZ zu schicken.
- Bei Ausfall einer Protokollierungskomponente bietet das

iWAN-Gateway die Möglichkeit, eine Warnung an die Administratoren der KDVZ auszugeben.

- Die Aktivitäten der Administratoren auf den iWAN-Gateways werden technisch als Protokollierungs-informationen manipulationssicher aufgezeichnet.

6 Änderungsmanagement

- Die Integrität der Softwarepakete, Konfigurationsdateien und Update-Pakete (z. B. Sicherheitsupdates) wird von KDVZ durch geeignete Mechanismen vor dem Updateprozess der iWAN-Gateways sichergestellt. Es wird durch KDVZ sichergestellt, dass nur überprüfte Pakete installiert werden.

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.