Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

D-TRUST GmbH
Kommandantenstraße 15
10969 Berlin

für den Bereich

Netzwerkinfrastruktur des Trustcenters der D-TRUST GmbH

die Erfüllung aller Anforderungen der Kriterien

Sicherheitstechnischen 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, V1.0 vom 30.11.2007.

Dieses Zertifikat ist bis zum 31.01.2010 gültig.

Security SQ9534.08 TÜViT® 2008 Trusted Site Voluntary Validation

Zertifikat-Registrier-Nr.:
TUVIT-SQ9534.08

10

Essen, 15.01.2008 gez. Faulhaber
Zertifizierungsstelle

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

Prüfbericht

- „Sicherheitstechnische Qualifizierung (SQ)® der Netzwerkinfrastruktur des Trustcenters der D-TRUST GmbH“, Version 1.0 vom 30.11.2007, TÜV Informationstechnik GmbH

Prüfanforderungen

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

Prüfobjekt

- Netzwerkinfrastruktur des Trustcenters des Zertifizierungsdiensteanbieters nach Signaturgesetz D-TRUST GmbH.

Weitere Netze der D-TRUST GmbH, die nicht zum Trustcenter gehören, sind nicht Gegenstand der Zertifizierung.

Unternehmensspezifische Sicherheitsanforderungen

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

Allgemeine Anforderungen

- Die Identifikation und Authentisierung für Administratoren sowie die Verwaltung von Komponenten der Firewall-Installation erfolgt über einen vertrauenswürdigen Pfad.
- Die einzelnen Komponenten der Firewall-Installation halten Standardangriffen gegen den TCP/IP-Stack stand.
- Die Struktur des zu schützenden Netzwerkes ist verdeckt. Es werden beispielsweise keine internen Header oder Adressen in das unsichere Netzwerk übermittelt.
- Source-Routing Informationen werden ignoriert. Es wird statisches Routing innerhalb der Firewall-Installation verwendet.

- Die Firewall-Installation implementiert mindestens eine logische Mehrstufigkeit, die eine DMZ umfasst. Es werden zwei getrennte Filter verwendet, die hintereinander angeordnet sind und mindestens eine DMZ umfassen.
- Eine direkte Verbindung aus dem unsicheren Netz in das zu schützende Netz und umgekehrt ist nicht erlaubt.
- Auf den Komponenten der Firewall-Installation existieren keine ausnutzbaren Schwachstellen, die direkten Zugriff auf die Systeme ermöglichen.
- Auf den Komponenten der Firewall-Installation werden lediglich die zum Betrieb benötigten Dienste angeboten. Unbenötigte Dienste sind deaktiviert.

Protokollierung

- Für jede aufgebaute oder abgewiesene Verbindung auf der Anwendungsschicht kann eine Protokollierung der Benutzer-Identifikation, IP-Adresse, des Quell- und Zielrechners, Portnummer, Zeit und Datum durchgeführt werden.
- Auf allen Komponenten der Firewall-Installation wird die Systemzeit mindestens täglich synchronisiert.
- Spezielle, einstellbare Protokollmeldungen einzelner Komponenten führen zu einer unverzüglichen Warnung der Verantwortlichen.
- Die Protokollinformationen aller Firewall-Komponenten werden über einen vertrauenswürdigen Pfad an eine zentrale Stelle geschickt.
- Eine maschinell unterstützte Auswertung der Protokolldaten ist möglich.
- Bei Ausfall der Protokollierungskomponente wird eine Warnung ausgegeben, die ein unverzügliches Eingreifen des Administrators ermöglicht.

Paketfilter

- Der Netzwerkverkehr kann in Abhängigkeit von
  - Quell- und Ziel-IP (einzelne Hosts oder Teilnetze/IP-Bereiche)
  - Quell- und Zielport (für TCP und UDP) bzw. ICMP-Subtypes
  - TCP-Flags (Unterscheidungsmöglichkeit für bestehende oder neue Verbindungen)

  gefiltert werden.
- Folgende Aktionen werden für jede Filterregel unterstützt:
  - Weiterleiten des Paketes (Allow)
  - Verwerfen des Paketes (Deny & Drop)
  - Verwerfen mit Benachrichtigung (Deny & Reject)
- Es ist möglich, die Filterregeln für die Netzwerkschnittstellen getrennt einzustellen.
- Die Einstellung der Filterregeln gewährleistet, dass alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden.
- Die Filterregeln der Filterkomponenten der Firewall-Installation sind widerspruchsfrei.

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.