



TUVIT

Zertifikat

Die Zertifizierungsstelle der
TÜV Informationstechnik GmbH bescheinigt hiermit
der

Deutsche Bank AG

Alfred-Herrhausen-Allee 16-24
65755 Eschborn

die

Sicherheitstechnische Qualifizierung

für die

Firewall-Installation (Internet-Portal)

Der Umfang der in der Qualifizierung einbezogenen System-Teile und die mit der Installation verfolgten Sicherheitsziele sind im Dokument *SQ Deutsche Bank, Version 1.0a* spezifiziert. Die Qualifizierung wurde auf der Grundlage der Anforderungen der Spezifikation SQ, Version 8.3 von der TÜV Informationstechnik GmbH durchgeführt.

Dieses Zertifikat gilt nur in Verbindung mit dem Qualifizierungsbericht *SQ Deutsche Bank, Version 1.0a* vom 02.12.2002 sofern die Maßgaben für die Installation eingehalten werden.

Dieses Zertifikat berechtigt zur Nutzung des Prüfzeichens



Voluntary Validation

© 2002 TÜVIT GmbH - ein Unternehmen der RWTÜV-Gruppe -

Zertifikat-Registrier-Nr.: TUVIT-SQ9520.02

Essen, den 6.12.2002 **gez. Dr. Gruschwitz**

Zertifizierungsstelle

Zusammenfassung der Anforderungen für die Sicherheitstechnische Qualifizierung (SQ), Version 8.3

1 Technische Sicherheitsanforderungen und Vorgaben

Es liegen technische Sicherheitsanforderungen vor, die den „geltenden Sicherheitsansprüchen“ genügen. Sie weisen keine inhaltlichen Widersprüche auf.

2 Dokumentation der IT-Installation

In der Dokumentation sind die einzelnen Elemente und Beziehungen der IT-Installation erkennbar und verständlich dargelegt. Die Dokumentation beschreibt die Zerlegung in grundlegende Subsysteme und ermöglicht die Nutzungsbeziehungen und Datenflüsse zwischen den identifizierten Subsystemen nachzuvollziehen.

3 Benutzer-, Administrations- und sonstige Betriebsdokumente

Handbücher zur IT-Installation sowie zu den sicherheitsspezifischen und kritischen Subsystemen liegen vor.

4 Sicherheit der verwendeten Komponenten

Für alle Komponenten und Subsysteme, 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

Geeignete Konfigurationswerkzeuge der sicherheitsspezifischen Komponenten sind vorhanden und ein Monitoring dieser Komponenten ist möglich. Alle administrativen Tools sind in der gleichen Güte gesichert, wie die sicherheitsspezifischen Subsysteme selbst.

6 Tests und Inspektionen

Mittels Netzwerkttests und Konfigurationsanalysen wurde festgestellt, dass keine bekannten und direkt ausnutzbaren Schwachstellen auf der untersuchten IT-Installation existieren.

7 Änderungsmanagement

Für die Planung und Durchführung von Änderungen existiert ein Konzept, um die Konsequenzen für die Sicherheit adäquat bewerten zu können. Dieses legt dar, in welcher Weise Änderungen stattfinden dürfen und wie die Dokumentation der IT-Installation angepasst wird.

8 Operationelle Anforderungen

Geeignete operationelle Bedingungen, die eine einwandfreie Funktionsweise des zu untersuchenden Systems unterstützen, liegen vor. Die personellen Verantwortlichkeiten und die räumlichen Gegebenheiten genügen dem Sicherheitsanspruch der IT-Installation.

9 Sicherheitsanalysen

Die Prüfer haben ihre Sicherheitsanalysen in einem Prüfbericht dokumentiert. Das Ergebnis ist, dass sämtliche Sicherheitsanforderungen erfüllt und die resultierenden Restrisiken in Absprache mit dem Auftraggeber tragbar sind.