TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der IT-Sicherheitsverband.

Prüfungs- und Zertifizierungsordnung zum "TeleTrusT Information Security Professional" (T.I.S.P.)

Stand: 2017-01

ANMERKUNG Zur besseren Lesbarkeit und ohne Diskriminierungsabsicht werden im folgenden Text nur männliche Formen benutzt. Zum Beispiel bezeichnet Kandidat, Experte, Inhaber oder Zertifikatsinhaber sowohl weibliche wie männliche Personen.

1 Ziel der Prüfung

Mit einer erfolgreich abgelegten Prüfung zum TeleTrusT Information Security Professional (T.I.S.P.) weist ein Kandidat seine umfassenden und ganzheitlichen Kenntnisse und Fähigkeiten im IT-Sicherheitsumfeld auf operativer, taktischer und strategischer Ebene nach. Der Schwerpunkt der Prüfung liegt auf dem Test eines ganzheitlich vorhandenen Denkansatzes für das IT-Sicherheitsmanagement unter Einbezug der spezifischen europäisch geprägten Sicherheitskultur und der einschlägigen gesetzlichen Normen und Standards.

2 Voraussetzungen

Eine erfolgreiche Ausbildung zum T.I.S.P. setzt ausreichende theoretische und praktische Kenntnisse und Fertigkeiten auf dem Gebiet des IT-Sicherheitsmanagements sowie der Techniken, Technologien und Produkte voraus. Auf Grund ihrer besonderen Verantwortung müssen IT-Sicherheitsexperten neben fundiertem Wissen über einen festen Charakter, einen gesunden Menschenverstand und ein gefestigtes Rechtsverständnis verfügen.

3 Zulassung zur Prüfung

Zu einer T.I.S.P.-Prüfung wird zugelassen, wer ausreichende theoretische Vorbildung sowie praktische Erfahrungen nachweist und eine 5-tägige T.I.S.P.-Schulung bei einem anerkannten Schulungsanbieter besucht hat, die nicht länger als 12 Monate zurückliegen sollte.

3.1 Antrag auf Zulassung

Der Kandidat stellt mit seiner Anmeldung zu einem T.I.S.P.-Prüfungstermin den Antrag zur Zulassung zur Prüfung. Die Anmeldung erfolgt direkt bei der Personenzertifizierungsstelle.

Folgende Unterlagen und Nachweise sind für den Antrag zur Zulassung vom Kandidaten vorzulegen:

1) Nachweise, die geeignet sind die theoretischen Vorkenntnisse des Kandidaten zu belegen. Als Nachweise werden anerkannt:
   a) Zeugnisse, Zertifikate oder Teilnahmebestätigungen über einschlägige Berufsausbildungen bzw. Bildungsmaßnahmen im Bereich der IT-Sicherheit;
   oder
   b) Projektreferenzen mit der Darlegung der inhaltlichen Schwerpunkte aus den letzen drei Jahren. Diese Nachweise sind vor allem notwendig bei selbständiger Tätigkeit.

2) Nachweis einer mindestens dreijährigen Berufstätigkeit im Bereich IT-Sicherheit mit aussagekräftiger Beschreibung der bearbeiteten Themenschwerpunkte (Arbeitszeugnisse, Zwischenzeugnisse oder ähnliche aussagekräftige Bestätigungen des Arbeitgebers).

3) Nachweis des Schulungsanbieters, dass der Kandidat an einer anerkannten T.I.S.P.-Schulung teilgenommen hat.

3.2 Zulassungsentscheidung

Die Personenzertifizierungsstelle entscheidet über die Zulassung zur Prüfung zum T.I.S.P. auf Basis der vom Kandidaten vorgelegten Nachweise. Sofern beim Zulassungsantrag noch kein Nachweis über den Besuch einer anerkannten Schulung vorliegt, muss mindestens die Anmeldung zu einer anerkannten T.I.S.P.-Schulung, welche vor dem Prüfungstermin stattfindet, nachgewiesen werden.

Bei positiver Prüfung der Zulassungsvoraussetzungen erhält der Kandidat eine Einladung zur Prüfung. Reichen die nachgewiesenen Zulassungsvoraussetzungen nicht aus, erhält der Kandidat eine begründete Absage. Er hat die Möglichkeit, durch das Nachreichen ergänzender Unterlagen eine erneute Überprüfung zu veranlassen.

Gegen die Nichtzulassung zur Prüfung kann der Kandidat Beschwerde bei der Schiedsstelle der Personenzertifizierungsstelle einlegen.

4 Prüfung

4.1 Prüfungsinhalte

Die Prüfungsinhalte sind durch den Lehrplan T.I.S.P. festgelegt. Es werden zu den 18 Themenfeldern insgesamt 180 Multiple-Choice Fragen gestellt. Die Verteilung der Fragen auf die einzelnen Blöcke orientiert sich an der Gewichtung der Themen im Lehrplan. Folgende Themenblöcke sind Inhalt der Prüfung:

- Allgemeine Grundlagen
  - Netzwerksicherheit
  - Firewalls
  - Intrusion Detection
  - Hackermethoden, wichtige Angriffsszenarien
  - VPN
  - Sicherheit im WWW und E-Commerce
  - Sicherheit in mobilen Netzen
- Kryptographie
  - Grundlagen
  - Symmetrische / asymmetrische Verschlüsselung
  - PKI
- Sicherheitsmanagement
  - Information Security Management
  - Authentisierung
  - Autorisierung
  - Berechtigungsmanagement
  - BCM
  - Notfallmanagement
  - Security Awareness
  - Physische Sicherheit
  - Betriebswirtschaftliche Aspekte der IT-Sicherheit
- Rechtliche Grundlagen
- Systemsicherheit
  - Computer-Viren und Content Security
  - Betriebssystemsicherheit (Windows, Unix / Linux)

Hilfsmittel sind in der Prüfung nicht zugelassen.

4.2 Prüfungsdauer
Für die Beantwortung der Prüfungsfragen stehen den Kandidaten vier Stunden zur Verfügung.

4.3 Bestehen der Prüfung
Die Prüfung zum T.I.S.P. ist bestanden, wenn der Kandidat mindestens 70 % der gestellten Aufgaben richtig gelöst hat. Die Auswertung der Prüfung ist im T.I.S.P.-Bewertungsschema festgelegt (siehe http://www.teletrust.de/tisp/).

4.4 Prüfungswiederholung
Die Prüfung kann einmal ohne weitere Auflagen wiederholt werden. Für eine weitere Wiederholung ist die erneute Teilnahme an einer anerkannten T.I.S.P.-Schulung Zulassungsvoraussetzung.

5 Zertifizierung

5.1 Erstzertifizierung
Die Personenzertifizierungsstelle stellt das T.I.S.P.-Zertifikat aus, wenn der Kandidat die Prüfung zum T.I.S.P. erfolgreich bestanden hat, alle Zulassungsvoraussetzungen erfüllt sind und die Prüfungskosten bezahlt wurden.

Über die Zertifizierung wird ein T.I.S.P.-Zertifikat ausgestellt, in dem das Jahr und der Monat der Zertifizierung angegeben ist. Das Zertifikat wird von Personenzertifizierungsstelle und TeleTrusT unterschrieben.

Seit dem 01.01.2009 sind die Zertifikate auf 36 Monate ab Prüfungsdatum befristet. Die Gültigkeitsdauer wird ebenfalls im Zertifikat dokumentiert.

Zertifikate, die vor dem 01.01.2009 ausgestellt wurden, haben unbefristete Gültigkeit.

5.2 Re-Zertifizierung
Aufgrund der schnell aufeinander folgenden technologischen Änderungen im Umfeld der modernen Informations- und Kommunikationstechnik ist eine nachhaltige Beschäftigung mit den Methoden und Technologien der IT-Sicherheit für einen IT-Sicherheitsexperten unumgänglich. Aus diesem Grund wird eine Re-Zertifizierung von erfolgten T.I.S.P.-Zertifizierungen angeboten.

Die Re-Zertifizierung muss bis spätestens zum Ablauf des vierten Jahres nach der letzten Zertifizierung erfolgen. Danach ist keine Re-Zertifizierung mehr möglich. Das Zertifikat wird, ausgehend vom Datum des Erlöschens der Gültigkeit, um drei Jahre verlängert.

Für die Re-Zertifizierung muss der Antragssteller keine Prüfung absolvieren. Der T.I.S.P.-Inhaber muss seine Weiterbildung und kontinuierliche Beschäftigung im Themenumfeld IT-Sicherheit geeignet nachweisen und entsprechende Nachweise dem Antrag beifügen.

Erforderlich sind:

a) Tätigkeitsbeschreibung des Arbeitgebers oder bei Selbstständigen eine aussagekräftige Projektliste. Dabei ist der Umfang der praktischen Tätigkeit zu quantifizieren (in % des persönlichen Arbeitsvolumens).
b) Besuch mindestens eines T.I.S.P. Community Meetings innerhalb der letzen drei Jahre.
c) Nachweise zu Fortbildungen/ Weiterentwicklung aus dem Bereich IT-Sicherheit/ Informationssicherheit im Volumen von durchschnittlich 20 Stunden pro Jahr. Anerkannt werden:
   - Teilnahme an geeigneten betrieblichen und/oder externen Weiterbildungsangeboten, Seminaren, Workshops oder Tagungen/Konferenzen (8h pro Tag);
   - Teilnahme an weiteren T.I.S.P. Community Meetings (8h pro Meeting);
   - Anerkannte Publikationen über eigene Forschungs- und Entwicklungstätigkeiten zu aktuellen Themen der Informationssicherheit (max. 20 h);
   - Nachweis über die persönliche Konzeption von Weiterbildungsangeboten zu aktuellen Themen der Informationssicherheit, die geeignet sind das persönliche Wissen weiter zu entwickeln. (max. 20 h);
   - Dokumentation von Projekten zu aktuellen Themen der Informationssicherheit, die geeignet sind das persönliche Wissen weiter zu entwickeln (persönliche Beteiligung am Arbeitsvolumens des Projektes von mind. 50 % (max. 20h).

Die fünf Möglichkeiten unter c) des Nachweises der persönlichen Weiterbildung und Qualifikationsleistung sind als alternative Leistungen zu verstehen. Entscheidend ist es, dass die geforderte durchschnittliche Jahresleistung erreicht wird.

Für alle anzuerkennenden Leistungen sind überprüfbare schriftlich Nachweise vorzulegen wie z.B. Teilnahmebescheinigungen, Zertifikate, Dokumentationen oder Bestätigungen vom Arbeitgeber bzw. vom Auftraggeber. Die Prüfung des Antrags auf Re-Zertifizierung erfolgt durch die Personenzertifizierungsstelle. Sie stellt ein erneuertes Zertifikat aus wenn alle erforderlichen Nachweise erbracht wurden.

6 Schiedsstelle

Die Personenzertifizierungsstelle verfügt über eine Schiedsstelle an die sich Prüfungsteilnehmer mit Einsprüchen gegen Ablauf und/oder Ergebnis von Prüfungen wenden können.

TeleTrusT wird über alle Einspruchsverfahren und deren Verlauf von der Schiedsstelle aktuell unterrichtet. In Fällen in denen die Meinungsverschiedenheiten zwischen Kandidaten und Personenzertifizierungsstelle trotz Behandlung durch die Schiedsstelle von der Personenzertifizierungsstelle nicht behoben werden können, kann TeleTrusT als übergeordnete Schiedsstelle fungieren.

6.1 Einsprüche bei der Schiedsstelle

Betroffene Personen können Einsprüche gegen die Entscheidungen der Personenzertifizierungsstelle einlegen. Gründe, für Einsprüche können sein:

1) Die Verweigerung zur Zulassung zur Prüfung;
2) Die Verweigerung einer Zertifizierung oder Re-Zertifizierung zum T.I.S.P.

Die Anrufung der Schiedsstelle ist mit Kosten verbunden, die rückerstattet werden, wenn zugunsten der betroffenen Person entschieden wird.

6.2 Schiedsspruch

Die Schiedsstelle entscheidet abschließend über den eingereichten Einspruch. Sie hat sich ein umfassendes Bild von den konkreten Umständen des Einzelfalls zu verschaffen und ihre Entscheidung auf objektiv nachprüfbaren Tatsachen zu begründen. Erkennt die Schiedsstelle den Einspruch an, fungiert sie als Vermittler zwischen Antragsteller und Personenzertifizierungsstelle.

7 Kosten

Für die Prüfung und Zertifizierung zum T.I.S.P. fallen Kosten an, die sich nach der jeweils geltenden T.I.S.P.-Kostenordnung richten (siehe http://www.teletrust.de/tisp/).

8 Instanzen der T.I.S.P.-Zertifizierung

Folgende Institutionen sind für die Entwicklung und Vergabe des T.I.S.P. verantwortlich. Ihre Aufgaben werden wie folgt definiert:

8.1 TeleTrusT – Bundesverband IT-Sicherheit e.V.

- ist Namensgeber, Markenrechteinhaber und verantwortliche Institution für den T.I.S.P.;
- ist verantwortlich für das inhaltliche Konzept des T.I.S.P.-Zertifikatssystems und dessen Weiterentwicklung;
- publiziert die Zertifikate der Absolventen, sofern die Zustimmung vorliegt;
- ist Auftraggeber für die unabhängige Personenzertifizierungsstelle.

8.2 Die unabhängige Personenzertifizierungsstelle

- bestimmt über die Zulassung zur T.I.S.P.-Zertifikatsprüfung;
- führt die T.I.S.P.-Zertifikatsprüfung durch;
- wertet die Prüfungsergebnisse aus und spricht Zertifizierungen zum T.I.S.P. aus;
- prüft Anträge auf Re-Zertifizierung und entscheidet darüber;
- verifiziert T.I.S.P.-Zertifikate von Personen;
- überprüft und anerkennt die T.I.S.P.-Schulungsanbieter.

8.3 Die anerkannten Schulungsanbieter

- führen T.I.S.P.-Schulungen nach dem Konzept von TeleTrusT durch;
- verwalten die Anmeldungen zur T.I.S.P.-Schulung;
- stellen TeleTrusT Ressourcen für die inhaltliche Weiterentwicklung des T.I.S.P. zur Verfügung.

9 Datenschutz

Bewerber geben mit der Anmeldung zur T.I.S.P.-Schulung und Prüfung ihr Einverständnis zur Speicherung, Bearbeitung, Weiterverarbeitung ihrer persönlichen und personenbezogenen Daten. Es werden nur Daten erhoben, die zur eindeutigen Identifikation des Bewerbers im Rahmen der Zertifizierung und Re-Zertifizierung notwendig sind. Die anerkannten Schulungsanbieter, die Personenzertifizierungsstelle und TeleTrusT dürfen die persönlichen und personenbezogenen Daten nicht untereinander austauschen. Jede beteiligte Instanz erhebt selbst die Daten, die sie von den Bewerbern für die Durchführung ihrer Aufgabe benötigt. Näheres wird von der T.I.S.P.-Datenschutzerklärung geregelt.