Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Personenzertifizierung: Programm IS-Penetrationstester

IS-Penetrationstester

Version 2.0 vom 01.11.2024

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 247-1000
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Änderungshistorie

Version	*Datum*	*Name/Org.-Einheit*	*Beschreibung*
1.0	17.05.2019	Personenzertifizierungsstelle Referat SZ 12	Neuausgabe aufgrund Dokumentenumstrukturierung und der Umstellung auf ein Antrag-Bescheidverfahren
1.1	05.08.2020	Personenzertifizierungsstelle Referat SZ 12	Revision: • Ergänzung der fehlenden Anforderung „Anstellung bei einem zertifizierten IT-Sicherheitsdienstleister“ in Kapitel 2.1.2.2, • Ergänzung der Nebenbestimmungen in Kapitel 5.1 „Pflichten des IS-Penetrationstesters“ und • weitere editorische und sprachliche Korrekturen in diversen Kapiteln.
1.2	19.04.2021	Personenzertifizierungsstelle Referat SZ 12	Revision: • Ergänzung/Änderung der Anforderungen an IS-Penetrationstester in Kapitel 2.1 • Ergänzung/Änderung des Verfahrens in den Kapiteln 3.1 und 3.2 • Ergänzung/Änderung zur Aufrechterhaltung der Zertifizierung in den Kapiteln 4.1 und 4.3 • weitere editorische und sprachliche Korrekturen in diversen Kapiteln
2.0	01.11.2024	Personenzertifizierungsstelle S21	Revision: • Umstrukturierung des Dokumentes • Entfernen der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm) in Kapitel 1.1 und entsprechende Anpassung im Kapitel. • Überarbeitung der Literaturangaben und der Zitate der Rechtsnormen. • 2.1.2.1 Zweiten Satz in Praxiserfahrung (2.1.2.2) überführt • 2.2. Zweiten Satz mit aktueller AG-Bescheinigung ergänzt • 2.2.6. Sperrfrist eingefügt

Tabelle 1: Änderungshistorie

Inhalt

1 Einleitung 5
1.1 Zielsetzung und Eingliederung des Programms IS-Penetrationstester 5
2 Zertifizierungsprogramm IS-Penetrationstester 6
2.1 Anforderungen an den IS-Penetrationstester 6
2.1.1 Die persönlichen Eigenschaften eines IS-Penetrationstesters 6
2.2 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren 7
2.2.1 Anstellung bei einem zertifizierten IT-Sicherheitsdienstleister 7
2.2.2 Berufserfahrung 7
2.2.3 Praxiserfahrung 8
2.2.4 Anforderung an die Fachkompetenz 8
2.2.5 Optionale Qualifizierungsmaßnahme 9
2.2.6 Bewertung der nachzuweisenden Fachkompetenz durch eine Prüfung 9
2.3 Aufrechterhaltung der Zertifizierung 9
2.3.1 Anforderungen an die Tätigkeiten des IS-Penetrationstesters 9
2.3.2 Kompetenzüberwachung 9
2.3.3 Anforderungen zur Rezertifizierung 9
3 Spezielle Rahmenbedingungen 10
3.1 Pflichten des IS-Penetrationstesters 10
4 Referenzen und Glossar [Verzeichnisse] 11

1 Einleitung

Das vorliegende Dokument beschreibt die Anforderungen für die Kompetenzfeststellung und Zertifizierung von Personen im Programm IS-Penetrationstester.

Ein IS-Penetrationstester kann nur im Rahmen seiner Anstellung bei einem vom BSI zertifizierten IT-Sicherheitsdienstleister im Programm IS-Penetrationstester (siehe [VB-Stellen]) die Personenzertifizierung erlangen.

Bei Erstzertifizierung erfolgt die Zertifizierung der Person und die des IT-Sicherheitsdienstleisters zeitgleich. Als Nachweise sind vorzulegen:

- Bei in Zertifizierung befindlichem IT-Sicherheitsdienstleister:
  Kopie des Antrags auf Zertifizierung als IT-Sicherheitsdienstleister.
- Bei bereits zertifiziertem IT-Sicherheitsdienstleister:
  Kopie des Zertifikats des IT-Sicherheitsdienstleisters.

1.1 Zielsetzung und Eingliederung des Programms IS-Penetrationstester

Dieses Dokument beinhaltet detaillierte Hinweise als Ergänzung zum übergeordneten Dokument „Verfahrensbeschreibung zur Zertifizierung von Personen“ [VB-Personen] für die Situation, in der sich der Antragsteller entschieden hat, eine Zertifizierung als IS-Penetrationstester durchführen zu lassen.

Es werden konkret die Anforderungen und Aufgaben benannt, die ein Antragsteller berücksichtigen muss, um den Regelungen des Programms gerecht zu werden. An den entsprechenden Stellen im Dokument wird z. B. auf Formulare oder andere Hilfsmittel hingewiesen, die besonders bei einer Erstzertifizierung hilfreich sind.

Die Beschreibung der verschiedenen Dokumentenkategorien befindet sich in der übergeordneten [VB-Personen].

Das Dokument „Verzeichnisse“ [Verzeichnisse] gibt einen Überblick über alle benötigten Hilfs- und Informationsquellen (Literaturverzeichnis) und enthält ein Stichwort- und Abkürzungsverzeichnis (Glossar).

2 Zertifizierungsprogramm IS-Penetrationstester

Um Bundesbehörden bei der Auswahl von IT-Sicherheitsdienstleistern zu unterstützen, hat das BSI als neutrale staatliche Stelle ein Zertifizierungsverfahren für IT-Sicherheitsdienstleister das Programm „IS-Penetrationstests“ entwickelt. Insbesondere bei Bundesbehörden mit sicherheitssensiblen Bereichen müssen sich die beauftragten IT-Sicherheitsdienstleister durch Unabhängigkeit, Fachkompetenz und Qualität der Dienstleistung auszeichnen. Ziel der Zertifizierung des IT-Sicherheitsdienstleisters ist somit die Sicherstellung der Vertrauenswürdigkeit und Kompetenz.

Die Grundlage jeder Dienstleistung in diesem Programm sind qualifizierte und kompetente Mitarbeiter.

Penetrationstests sind auf die individuelle Situation der Behörde abzustimmen und somit nur in begrenztem Umfang standardisierbar. Bei einem Penetrationstest kann deshalb nur bis zu einem gewissen Grad nach einem starren Muster vorgegangen werden. Deshalb sollte die Durchführung von Penetrationstests von Experten vorgenommen werden, die über möglichst umfassende, praktische Erfahrungen in den Gebieten IT-Betrieb sowie IT-Sicherheit verfügen.

2.1 Anforderungen an den IS-Penetrationstester

2.1.1 Die persönlichen Eigenschaften eines IS-Penetrationstesters

Im Folgenden sind die persönlichen Eigenschaften eines IS-Penetrationstesters dargestellt, die für die Tätigkeiten im Programm notwendig sind, jedoch als „Soft Skills" nur eingeschränkt im Rahmen eines Zertifizierungsverfahrens bewertet werden können.

2.1.1.1 Kommunikationsfähigkeiten

- Umfassende und sachliche Berichterstattung
- Didaktische Fähigkeiten
- sehr gute schriftliche und mündliche Ausdrucksfähigkeit
- Führung von Beratungsgesprächen
- fachkundige Ergebnispräsentation
- Verständnis für die behördliche Arbeitsweise

2.1.1.2 Soziale Kompetenz

- Analytische Fähigkeiten
- Wille zur Weiterentwicklung von Fähigkeiten
- Verantwortungsbewusstes Handeln
- Teamfähigkeit
- Konfliktmanagement
- Kreativität
- Beharrlichkeit
- Konstruktive Grundhaltung
- offener und transparenter Umgang mit den Grenzen des eigenen Wissens

2.1.1.3 Unabhängigkeit

- Fachliche und sachliche Unabhängigkeit
- Unbeeinflussbarkeit und Unvoreingenommenheit
- Verschwiegenheit und Unbestechlichkeit

2.2 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise überprüft (siehe [VB-Personen]).

Ein Lebenslauf (Ausbildungs-und Arbeitshistorie) und ggf. Bescheinigungen der Teilnahme an relevanten Fortbildungen, sowie eine aktuelle Arbeitgeberbescheinigung mit Angabe der Art und des Umfanges (Voll- oder Teilzeit in %) der Beschäftigung sind vorzulegen.

2.2.1 Anstellung bei einem zertifizierten IT-Sicherheitsdienstleister

Anforderung

Ein IS-Penetrationstester kann nur im Rahmen seiner Anstellung bei einem vom BSI zertifizierten IT-Sicherheitsdienstleister im Geltungsbereich Penetrationstests (s. [VB-Stellen]) die Personenzertifizierung erlangen.[1]

Nachweis

- Bei Anstellung bei einem in Zertifizierung befindlichen IT-Sicherheitsdienstleister:
  Kopie des Antrags auf Zertifizierung als IT-Sicherheitsdienstleister.
- Bei Anstellung bei einem bereits zertifizierten IT-Sicherheitsdienstleister:
  Kopie des Zertifikats des IT-Sicherheitsdienstleisters.

2.2.2 Berufserfahrung

Anforderung

Der Antragssteller muss fachspezifische, mindestens zweijährige Berufserfahrung in dem Gebiet von technischen Sicherheitsanalysen und Penetrationstests nachweisen.

Die Berufserfahrung kann auch einjährig durch Fortbildungen anerkannt werden, sofern

- diese erfolgreich innerhalb der letzten 2 Jahre
  von einer rechtlich vollständig getrennten Organisation als der beschäftigenden Organisation und mit einem Mindestumfang von 5 Tagen durchgeführt wurden,
- die Dauer der Fortbildungen in Summe mindestens 20 volle Werktage erreicht und
- diese als Kerninhalt Techniken, Methoden oder Kompetenzen im Bereich des Pentestings vermitteln

[1] Bei Erstzertifizierung erfolgt die Zertifizierung der Person und des IT-Sicherheitsdienstleisters zeitgleich.

Nachweis

Es muss ein Zeugnis oder eine Bestätigung eines unabhängigen Dritten (z.B. Arbeitgeber) über die mindestens zweijährige Berufserfahrung als Penetrationstester bzw. über relevante Fortbildungen für Penetrationstester vorgelegt werden.

Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung.

2.2.3 Praxiserfahrung

Anforderung

Es sind mindestens 100 Projekttage in leitender Funktion innerhalb der letzten 2 Jahre nachzuweisen, die mit einem Mindestumfang von 5 Tagen in Penetrationstest-Projekten abgeleistet wurden.

Nachweis

Vom jeweiligen Auftraggeber oder Arbeitgeber sind bestätigte Kurzberichte über die Durchführung von Penetrationstests vorzulegen.

Anzugeben sind hierbei:

- die Rollenverteilung im Projekt, insbesondere die Position/Verantwortung des Antragstellers,
- der Zeitraum und Umfang (Personentage) des Projektes.

Falls mehrere Personen an dem Auftrag beteiligt waren oder der Antragsteller neben dem Penetrationstest noch andere Tätigkeiten vorgenommen hat (beispielsweise Schulung oder Beratung) so ist nur die Anzahl der Personentage anzugeben, die vom Antragsteller für den Penetrationstestteil aufgewendet wurde.

Die Angaben im Kurzbericht können auch anonymisiert erfolgen.

2.2.4 Anforderung an die Fachkompetenz

2.2.4.1 Basiskenntnisse

Als IS-Penetrationstester werden folgende grundlegende Kenntnisse vorausgesetzt:

- Fähigkeit zur Systemadministration von Windows- und Linux-Systemen
- Verständnis der wesentlichen Netzwerkprotokolle, sowie Funktionsweise und Anwendung
- Beherrschung mindestens einer Programmier- oder Skriptsprache
- Kenntnisse über IT-Sicherheitsprodukte (Firewalls, WAFs, ALGs, Intrusion-Detection-Systemen, etc.)
- Kenntnisse üblicher Schwachstellenklassen in unterschiedlichen Domänen (Webapplikationen, Applikationen, Betriebssysteme, Netzwerke, Virtualisierung, Container)
- Kenntnisse über IT-Sicherheitsprozesse: Configurationmanagement, Patchmanagement, Backup, Changemanagement, ISMS

2.2.4.2 Erweiterte Fachkenntnisse

Als IS-Penetrationstester werden folgende Fachkenntnisse vorausgesetzt:

- Überblick über Ziele, Methodik, Vorgehen und Grenzen von Sicherheitsuntersuchungen
- Rechtliche Rahmenbedingungen von IT-Sicherheitsuntersuchungen

- Kenntnis der Verschlusssachenanweisung des Bundes
- Befähigung zur selbstständigen Vorbereitung und Durchführung von IT-Sicherheitstests, sowie zur Anleitung von Kollegen
- Geübter Umgang und Analysefähigkeit von IT-Dokumentationen, Konzepten, Richtlinien und Plänen
- Abschätzung von Schadenspotentialen und Risiken im Rahmen einer nachvollziehbaren Einstufung der Kritikalität identifizierter Mängel

2.2.5 Optionale Qualifizierungsmaßnahme

Das BSI bietet keine optionalen Qualifizierungsmaßnahmen für IS-Penetrationstester an.

2.2.6 Bewertung der nachzuweisenden Fachkompetenz durch eine Prüfung

Im Rahmen eines Projekttages im BSI werden die praktische Fachkompetenz und die persönlichen Voraussetzungen des IS-Penetrationstesters geprüft. Hierbei wird Grundwissen der Informationstechnik, Spezialwissen im Bereich von Penetrationstests, die Handhabung von Tools und Schwachstellen-Scannern, die Fähigkeit von technischen Analysen von Systemen, sowie die Vorgehensweise bei der Durchführung von Penetrationstests überprüft. Anhand eines kurzen Beispielprojekts weist der IS-Penetrationstester seine Qualifikation in Vorbereitung, Durchführung und Ergebnispräsentation nach, wobei der Fokus auf unterschiedliche Arten von Schwachstellensuche gelegt wird.

Sollte die Prüfung nicht bestanden werden, ist eine einmalige Wiederholungsprüfung möglich. Sollte auch diese nicht bestanden werden, so ist eine erneute Antragstellung erst nach Ablauf eines Jahres möglich.

2.3 Aufrechterhaltung der Zertifizierung

2.3.1 Anforderungen an die Tätigkeiten des IS-Penetrationstesters

Die Anforderungen an die Durchführung von Projekten sind dem “Leitfaden für die Informationssicherheitsrevision auf Basis von IT-Grundschutz” [REV] zu entnehmen.

2.3.2 Kompetenzüberwachung

Nach jedem durchgeführten Penetrationstest werden von den beauftragten Bundesbehörden Bewertungsbögen eingefordert. Anhand dessen wird die Durchführung der Dienstleistung bewertet.

2.3.3 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Penetrationstester nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, so muss er die von ihm in den letzten 3 Jahren durchgeführten Penetrationstests geeignet nachweisen (bspw. in Form von vom Auftraggeber oder Arbeitgeber bestätigten Kurzberichten über die Durchführung der Penetrationstests).

Dabei muss er mindestens 50 Personentage pro Jahr mit der Durchführung von Penetrationstests beschäftigt gewesen sein. Die Nachweise können auch außerhalb des UP Bund, d.h. bei privaten Auftraggebern erbracht werden.

Sollte ein Nachweis (z.B. mangels Aufträgen) nicht erbracht werden, muss eine erneute Zertifizierung (s. Kapitel 3.2) – auch mit dem Risiko des Nicht-Bestehens – durchlaufen werden.

3 Spezielle Rahmenbedingungen

3.1 Pflichten des IS-Penetrationstesters

Der IS-Penetrationstester stellt sicher, dass er

- alle Tätigkeiten objektiv und unabhängig sowie entsprechend den geltenden Vorgaben (Richtlinien und Verfahrensbeschreibungen) durchführt,
- die Vorgaben des BSI sowie die in den betreffenden Verfahrensbeschreibungen und Technischen Richtlinien festgelegten Vorgehensweisen beachtet und einhält,
- eventuelle Nebenbestimmungen sowie Auflagen erfüllt und Abweichungen umgehend behebt,
- bei signifikanten Änderungen, die sich auf das Programm oder die Arbeitsweise auswirken, die Personenzertifizierungsstelle unverzüglich unterrichtet.

4 Referenzen und Glossar [Verzeichnisse]

Das Dokument Verzeichnisse als Nachschlagewerk für Interessenten und Beteiligte an Zertifizierungs- und Anerkennungsverfahren [Verzeichnisse] gibt einen Überblick über alle benötigten Anforderungen, Quellen und Hilfsmittel mit einem Glossar- und Abkürzungsverzeichnis.

Die Listen im Bereich der Anforderungen, Quellen und Hilfsmittel sind als Stammliste zu verstehen und decken für sämtliche Anforderungen und Dokumente die Information über aktuelle Quellenhinweise ab.