Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

IT-Sicherheitsdienstleister-Zertifizierung: Programm im Bereich IS-Penetrationstest

IS-Penetrationstest

Version 2.2 vom 01.11.2024

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 274 1000
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Änderungshistorie

Version	*Datum*	*Name/Org-Einheit*	*Beschreibung*
1.0	20.07.2015	Anerkennungsstelle S 25	Erstausgabe
2.0	11.01.2017	CK13	Revision in 2017
2.1	02.07.2018	QMB D	Revision in 2018
2.1.1	30.11.2021	Anerkennungsstelle SZ 12	Revision: • Austausch der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramme) • Aktualisierung von Links
2.2	01.11.2024	S 21	Revision: • Überarbeitung der Anforderungen an IT-Sicherheitsdienstleister für den Bereich IS-Penetrationstests • Ergänzungen der Regelungen zu Fernbegutachtungen • Umwandeln der Referenzen der VB-Stellen zu VB-IT-Sicherheitsdienstleister • Entfernen der Abbildung 1 Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm) in Kapitel 1.1 und entsprechende Anpassung im Kapitel • Redaktionelle und strukturelle Anpassungen

Tabelle: Änderungshistorie

Inhalt

1 Einleitung

Die Zertifizierung als IT-Sicherheitsdienstleister wird auf Veranlassung des Inhabers oder der Geschäftsleitung einer Stelle durchgeführt.

Zertifiziert werden Stellen, die von natürlichen oder juristischen Personen des Privatrechts betrieben werden. Hinsichtlich staatlicher Stellen gelten ggf. abweichende Regelungen.

1.1 Zielsetzung und Eingliederung in die Dokumentenstruktur

Dieses Dokument beinhaltet detaillierte Anforderungen und weitere Informationen als Ergänzung zur übergeordneten „Verfahrensbeschreibung zur Zertifizierung von IT-Sicherheitsdienstleistern“ [VB-IT-Sicherheitsdienstleister]. Es richtet sich insbesondere an die Antragsteller, die sich dafür entschieden haben, eine Zertifizierung im Bereich IS-Penetrationstest durchführen zu lassen.

Es werden die speziellen Anforderungen mit detaillierten Hinweisen zu Verfahrensabläufen benannt, die ein Antragsteller berücksichtigen muss. An den entsprechenden Stellen im Dokument wird z. B. auf Formulare oder weitere Hilfsmittel hingewiesen, die besonders bei einer Erstzertifizierung hilfreich sind.

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

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

2 Zertifizierungsprogramm

2.1 Einführung IS-Penetrationstest

Ein IS-Penetrationstest ist ein erprobtes und geeignetes Vorgehen, um das Angriffspotenzial auf ein IT-Netz, ein einzelnes IT-System oder eine (Web-)Anwendung festzustellen. Hierzu werden die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System eingeschätzt und daraus notwendige ergänzende Sicherheitsmaßnahmen abgeleitet beziehungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen überprüft.

IT-Sicherheitsdienstleister im Geltungsbereich „IS-Penetrationstest“ sollen folgende Aufgaben durchführen bzw. Dienstleistungen anbieten:

- Durchführung von Sicherheitsanalysen und Schwachstellenerkennungen sowie
- Durchführung von Penetrationstests [PEN].

Die beauftragten IT-Sicherheitsdienstleister müssen sich durch Zuverlässigkeit und Unabhängigkeit bzw. Unparteilichkeit sowie durch Fachkompetenz und Qualität der Dienstleistung auszeichnen. Ziel der Zertifizierung ist somit die Sicherstellung der Vertrauenswürdigkeit und Kompetenz der IT-Sicherheitsdienstleister, um Institutionen bei der Auswahl von IT-Sicherheitsdienstleistern zu unterstützen.

2.2 Anforderungen an IT-Sicherheitsdienstleister für den Bereich IS-Penetrationstest

Der IT-Sicherheitsdienstleister muss über die erforderliche Fachkompetenz im Geltungsbereich verfügen sowie ein Informationssicherheitsmanagementsystem mit einem Sicherheitskonzept auf der Basis von IT-Grundschutz [IT-GS] nach der Vorgehensweise der Standard-Absicherung nachweisen.

Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess eines IT-Sicherheitsdienstleisters. Es dient der Umsetzung der Sicherheitsstrategie und beschreibt das Vorgehen, wie die gesetzten Sicherheitsziele der Institution erreicht werden. Durch die Vorlage eines Sicherheitskonzepts auf der Basis von IT-Grundschutz – mindestens für diesen Geltungsbereich – weist der IT-Sicherheitsdienstleister die erfolgreiche Anwendung von IT-Grundschutz für den betrachteten Informationsverbund nach. Für das Sicherheitskonzept auf der Basis von IT-Grundschutz muss die Vorgehensweise der Standard-Absicherung verwendet werden.

Damit zeigt der IT-Sicherheitsdienstleister, dass

1. ein funktionierendes IS-Management vorhanden ist,
2. ein definiertes Sicherheitsniveau erreicht wurde und
3. die IT-Grundschutz-Methodik im Zertifizierungsbereich angewandt wird.

Bei der Zertifizierung zum IT-Sicherheitsdienstleister kann die beantragende Stelle entweder eine IS-Kurzrevision durch das BSI durchführen lassen oder ein „ISO-27001-Zertifikat auf Basis von IT-Grundschutz“ nachweisen.

Bei der IS-Kurzrevision handelt es sich um eine Stichprobenprüfung der Dokumente und ggf. einer Inaugenscheinnahme (Vor-Ort-Prüfung), wobei die Umsetzung von IT-Grundschutz vom IS-Revisionsteam des BSI überprüft wird. Damit wird geprüft, ob der IT-Sicherheitsdienstleister die dokumentierten Sicherheitsprozesse umgesetzt und die erforderlichen Sicherheitsmaßnahmen auf der Basis von IT-Grundschutz realisiert hat. Auch bei Vorlage eines „ISO-27001-Zertifikat auf Basis von IT-Grundschutz“ kann die zur Verarbeitung von Verschlusssachen verwendete Technik vom BSI überprüft werden. Die IS-Kurzrevision wird in der Regel als Fernbegutachtung durchgeführt.

Die Einhaltung der Bestimmungen zum Umgang mit Verschlusssachen der „Verfahrensbeschreibung zur Zertifizierung von IT-Sicherheitsdienstleistern“ [VB-IT-Sicherheitsdienstleister] ist Voraussetzung für die

Zertifizierung des IT-Sicherheitsdienstleisters. Der Antragsteller muss in der Lage sein, Verschlusssachen bis zu VS-NfD zu bearbeiten.

Bei Beantragung der Zertifizierung als IT-Sicherheitsdienstleister muss mindestens die Bereitschaft (schriftliche Eigenerklärung) zur Aufnahme in die Geheimschutzbetreuung des Bundes seitens des IT-Sicherheitsdienstleisters sowie zur Durchführung einer Sicherheitsüberprüfung der benannten Experten beim BSI vorliegen. Zum Zeitpunkt der Übernahme einer Tätigkeit als IT-Sicherheitsdienstleister für den UP-Bund kann es erforderlich sein, dass der IT-Sicherheitsdienstleister in die Geheimschutzbetreuung des Bundes aufgenommen ist und die Sicherheitsüberprüfung der benannten Experten abgeschlossen ist.

Zertifiziert werden können IT-Sicherheitsdienstleister, die für den Geltungsbereich „IS-Penetrationstest“ mindestens zwei zertifizierte Penetrationstester beschäftigen. Eine Vertretungsregelung muss vorhanden sein.

Das Zertifizierungsverfahren für Penetrationstester ist in der Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen [VB-Personen] mit dem entsprechenden Anforderungsdokumenten beschrieben.

3 Verfahren zur Zertifizierung

3.1 Zusätzlich notwendige Unterlagen zur Beantragung

Notwendige Unterlagen zur Beantragung der Zertifizierung sind in der Verfahrensbeschreibung [VB-IT-Sicherheitsdienstleister] beschrieben.

Folgende zusätzliche Unterlagen müssen dem Zertifizierungsantrag des IT-Sicherheitsdienstleisters für den Bereich IS-Penetrationstest beigefügt werden:

- Systemdokumentation Qualitätsmanagement bei Variante A, siehe VB-IT-Sicherheitsdienstleister:
  - Prüfberichtsvorlagen für die Durchführung von IS-Penetrationstests
- Informationssicherheitsmanagement, hier alternativ:
  - Sicherheitskonzept auf der Basis von IT-Grundschutz (nach der Vorgehensweise der Standard-Absicherung) einschließlich eines Netzplans für den Informationsverbund zur Durchführung einer IS-Kurzrevision oder
  - ISO 27001-Zertifikat auf der Basis von IT-Grundschutz und zusätzlich Dokumentation der zur Verarbeitung von Verschlusssachen verwendeten Technik durch das BSI
- Benennung der Personen, die den Personenzertifizierungsprozess durchlaufen werden oder ggf. bereits zertifiziert sind. Bei Beantragung der Erstzertifizierung als IT-Sicherheitsdienstleister müssen mindestens die Anträge auf Personenzertifizierung beim BSI vorliegen. Die Zertifizierung der Stelle als IT-Sicherheitsdienstleister erfolgt zeitgleich mit der Personenzertifizierung.
- Bereitschaft zur Aufnahme in die Geheimschutzbetreuung und zur erweiterten Sicherheitsüberprüfung der Experten.

3.2 Spezielle Informationen zur Systembegutachtung

3.2.1 Durchführung der Fachbegutachtung

In der Systembegutachtung muss neben der Anforderungen an das Qualitätsmanagement der Nachweis der Erfüllung der Anforderungen an das Informationssicherheitsmanagement (ISMS) erfolgen. Dies geschieht in diesem Geltungsbereich durch eine IS-Kurzrevision oder alternativ durch die Vorlage eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz sowie der Überprüfung der zur Verarbeitung von Verschlusssachen verwendeten Technik durch das BSI.

3.2.2 Durchführung einer IS-Kurzrevision

Die IS-Kurzrevision ist ein Verfahren zur Einschätzung des Informationssicherheitsstatus und -prozesses in einer Institution. Ziel der IS-Kurzrevision ist es, der Leitungsebene mit wenig Aufwand einen Überblick über den Sicherheitsstatus und die bestehenden sicherheitskritischen Themenbereiche in der eigenen Institution zu verschaffen. Bei einer IS-Kurzrevision werden Anforderungen aus dem IT-Grundschutz betrachtet, die eine wesentliche Grundlage für Informationssicherheit bilden und sich darüber hinaus aufgrund von Erfahrungswerten als problembehaftet erwiesen haben. Die Prüfungstätigkeit zielt darauf ab, die Informationssicherheit zu verbessern.

Hierzu hat das BSI mit dem „Leitfaden für die IS-Revision auf Basis von IT-Grundschutz“ [IS-Kurzrevision] ein Verfahren entwickelt, das sowohl die Bundesverwaltung, als auch andere Behörden, die freie Wirtschaft und Dienstleister nutzen können, um den Status der Informationssicherheit in einer Institution festzustellen und Schwachstellen identifizieren zu können.

Die „Prüfthemen für die IS-Kurzrevision“ [Prüfthemenliste] beschreibt die bei der Durchführung einer IS-Kurzrevision zu überprüfenden Prüfthemen und gibt Beispiele für mögliche Stichproben zum jeweiligen Prüfthema. Sie ist für die Durchführung von IS-Kurzrevision verbindlich anzuwenden.

Die IS-Kurzrevision wird durch zwei Mitarbeiter des BSI durchgeführt und kann sich zeitlich an eine Systembegutachtung anschließen oder an einem separaten Termin durchgeführt werden.

4 Aufrechterhaltung der Zertifizierung

4.1 Anforderungen an den Ablauf des Penetrationstests

Mit Hilfe von Penetrationstests soll die Wirksamkeit der umgesetzten IT-Sicherheitsmaßnahmen zur Abwehr von Angriffen gegen IT-Systeme und Netze geprüft werden. Hierbei wird der Weg, den ein potenzieller Angreifer gehen würde, nachvollzogen, um eventuell noch vorhandene Schwächen in den IT-Systemen und Netzen aufzuspüren.

Potenzielle Angreifer kennen herkömmliche IT-Sicherheitsmaßnahmen und typische Defizite gut. Sie suchen daher gezielt nach Schwachstellen in den IT-Systemen und Netzen, also beispielsweise nach aktuellen Sicherheitslücken, die bislang noch nicht behoben worden sind, aber auch nach schon länger bekannten Lücken, für die noch keine Sicherheitspatches eingespielt wurden, oder nach konzeptionellen Schwächen in der gewählten IT-Architektur.

Das BSI bietet für die Durchführung von Penetrationstests weitere Informationen auf der folgenden Webseite an:

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/Pen_Test_und_IS_Webcheck/pent-tests-und-is-webcheck_node.html

4.2 Rezertifizierung

Fünf Monate vor Ablauf der Zertifizierung muss ein erneuter Antrag auf Rezertifizierung gestellt werden, damit gewährleistet ist, dass die Zertifizierung lückenlos fortgeführt werden kann.

Im Rahmen der Rezertifizierung kann die beantragende Stelle entweder eine erneute IS-Kurzrevision durch das BSI durchführen lassen oder ein „ISO-27001-Zertifikat auf Basis von IT-Grundschutz“ nachweisen.

5 Spezielle Rahmenbedingungen

5.1 Arbeitstreffen mit den IT-Sicherheitsdienstleistern

Das BSI kann maximal zwei eintägige Treffen bzw. Workshops pro Jahr, insbesondere zur Klärung schwieriger Grundsatz- oder Kriterienfragen, veranstalten, zu denen der IT-Sicherheitsdienstleister rechtzeitig eingeladen wird. Der Antragsteller lässt hieran mindestens einen fachkompetenten Mitarbeiter teilnehmen. Die Teilnahme ist zur Aufrechterhaltung der Zertifizierung als IT-Sicherheitsdienstleister zwingend erforderlich. Auf Vorschlag des BSI oder des IT-Sicherheitsdienstleisters werden Arbeitssitzungen zu spezifischen Fragestellungen durchgeführt. Hierunter fallen z.B.

- Diskussionen zu den fachlichen Anforderungen,
- Änderungen des Zertifizierungsverfahrens,
- Schulung hinsichtlich spezieller Methoden und Werkzeuge,
- Informationsaustausch zum Stand der Technik und zu Angriffsmethoden und Analysen,
- Spezifische Treffen z.B. zu Kryptothemen,
- Erfahrungsaustausch zum Qualitätsmanagement.

Die Anzahl solcher Arbeitssitzungen wird nach Dringlichkeit und fachlichen Erfordernissen festgelegt.

5.2 Verfahren bei Mängeln bei der Durchführung von IT-Sicherheitsdienstleistungen

Sollten bei den im Rahmen dieser Zertifizierung durchgeführten Tätigkeiten des IT-Sicherheitsdienstleisters (Qualitäts-)Mängel festgestellt werden, so wird zunächst versucht, diese zwischen der Anerkennungsstelle und dem zertifizierten IT-Sicherheitsdienstleister zu klären. Für den Fall, dass keine zufriedenstellende Klärung möglich ist, wird ein Mahn- und Aussetzungsverfahren in Anlehnung an das Verwaltungsverfahrensgesetz [VwVfG] durchgeführt.

6 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.