Bundesamt für Sicherheit in der Informationstechnik

Lizenzierungschema für IT-Grundschutz-Auditoren

Stand: 14.02.2002

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik

Redaktion: mailto: gssiegel@bsi.bund.de

Änderungsverzeichnis

Datum	Name	Änderung
01.02.2002	Dr. Isselhorst, Dr. Niggemann	1. Version

Inhaltsverzeichnis

1 Grundsätzliches 4
2 Lizenzierungsverfahren 5
2.1 Antragstellung 5
2.2 Fachkundenachweis 5
2.3 Prüfung der eingereichten Fachkundenachweise 5
2.4 Schulung 5
2.5 Schriftliche Prüfung 6
2.6 Vertragsschluss 6
2.7 Lizenzerteilung 6
2.8 Erfahrungsaustausch 7
2.9 Lizenzverlängerung 7
2.10 Lizenzentzug 7
3 Fachkundenachweis 8

1 Grundsätzliches

Vor der Vergabe eines IT-Grundschutz-Zertifikats muss ein IT-Grundschutz-Audit des betrachteten IT-Verbunds gemäß dem aktuellen Prüfschema für Auditoren durchgeführt werden. Diese Audits werden von Auditoren durchgeführt, die als Person ihre Fachkenntnisse im Bereich IT-Sicherheit und IT-Grundschutz sowie ihre Befähigung zur Durchführung von IT-Grundschutz-Audits vorab nachgewiesen haben müssen.

Damit die IT-Grundschutz-Audits einheitlich und vergleichbar sind, müssen die Auditoren auf vergleichbare Erfahrungswerte und Fachkunde zurückgreifen können. Um dies sicherzustellen, müssen die Auditoren persönlich beim BSI lizenziert sein. Eine Lizenzierung von Stellen oder Institutionen wird nicht angestrebt. Rechtliche Grundlagen des Verfahrens sind das Errichtungsgesetz des Bundesamts für Sicherheit in der Informationstechnik sowie ein entsprechender Erlass des Bundesministeriums des Innern vom 06. Februar 2001.

Potenzielle Auditoren können eine Lizenz für die Durchführung von IT-Grundschutz-Audits erlangen, indem sie das vom BSI angebotene Lizenzierungsverfahren durchlaufen und eine ausreichende Qualifikation nachweisen.

Eine Lizenz ist für einen Zeitraum von 5 Jahren gültig. In diesem Zeitraum wird durch das BSI ein jährlicher Erfahrungsaustausch zwischen den IT-Grundschutz-Auditoren ermöglicht, um die Einheitlichkeit des Verfahrens und die Fortentwicklung des IT-Grundschutz-Zertifizierungsschemas sicherzustellen. Eine vom BSI erteilte Lizenz kann entzogen werden, wenn der Auditor mehrfach am Erfahrungsaustausch nicht teilnimmt oder nachweislich grob gegen das Prüfschema für Auditoren verstößt.

Das Lizenzierungsverfahren und die entsprechenden Modalitäten werden nachfolgend beschrieben.

2 Lizenzierungsverfahren

2.1 Antragstellung

Der Antrag auf Lizenzierung als IT-Grundschutz-Auditor beim BSI ist natürlichen Personen vorbehalten.

Die Teilnahme am Lizenzierungsverfahren ist gebührenpflichtig.

Der Antragsteller erklärt sich mit dem Antrag dazu bereit, die Lizenzierungsgebühr zu entrichten. Diese umfasst die Kosten für Bearbeitung und Prüfung des Antrags sowie Schulung und schriftliche Prüfung. Die Kosten sind auch für den Fall zu entrichten, dass die Lizenz wegen nicht bestandener Prüfung nicht erteilt wird.

Die Anträge werden in der Reihenfolge des Eingangs bearbeitet.

2.2 Fachkundenachweis

Dem Antrag sind Fachkundenachweise beizulegen, aus denen sich ergibt, dass der Antragsteller über genügend Fachkenntnisse im Bereich IT-Sicherheit und praktische Erfahrung in der Anwendung des IT-Grundschutzhandbuchs besitzt.

2.3 Prüfung der eingereichten Fachkundenachweise

Das BSI prüft, ob die vorgelegten Fachkundenachweise ausreichend sind. Sollten die Nachweise nicht ausreichend sein, wird der Antragsteller unterrichtet und aufgefordert, weitere Nachweise zu erbringen. Kann die Fachkunde nicht ausreichend nachgewiesen werden, wird der Antragsteller nicht für das Lizenzierungsverfahren zugelassen.

2.4 Schulung

Nach Zulassung zum Lizenzierungsverfahren wird der Antragsteller zur Teilnahme an einer obligatorischen Schulung eingeladen. Die 1,5-tägige Schulungsveranstaltung, die allgemeine Kenntnisse zur IT-Sicherheit voraussetzt, hat folgende Inhalte:

- Vorgehensweise zur Anwendung des IT-Grundschutzhandbuchs (ca. ein halber Tag) und
- Erläuterung und Diskussion des Prüfschemas für Auditoren (ca. ein Tag).

Die Anzahl der Teilnehmer je Schulung ist begrenzt, um eine intensive Stoffvermittlung und Diskussion offener Punkte zur ermöglichen.

Die Schulungsinhalte zum IT-Grundschutzhandbuch dienen der Wiederholung und Auffrischung der Kenntnisse. Projekterfahrung mit dem IT-Grundschutzhandbuch muss bereits im Vorfeld nachgewiesen werden.

2.5 Prüfung

Unmittelbar Anschluss an die 1,5-tätige Schulung findet eine Prüfung über die Anwendungsweise und Inhalte des IT-Grundschutzhandbuchs und insbesondere über das Prüfschema für IT-Grundschutz-Audits statt, die noch am selben Tag abgeschlossen sein wird. Die Auswertung erfolgt durch das BSI. Das Ergebnis wird unmittelbar mitgeteilt.

2.6 Vertragsschluss

Die Lizenz als IT-Grundschutz-Auditor setzt den Abschluss des Lizenzierungsvertrags mit dem BSI voraus. In diesem Vertrag sind die Rechte und Pflichten des Auditors geregelt.

Der Lizenznehmer verpflichtet sich, dass er bei der Durchführung von IT-Grundschutz-Audits die Vorgaben des BSI, insbesondere die im *Prüfschema für Auditoren* festgelegte Vorgehensweise, beachten und einhalten wird. Darüber hinaus erklärt er, die Vertraulichkeit der ihm in den Audits zur Kenntnis gelangten Informationen zu wahren sowie keine Audits durchzuführen, die die Unabhängigkeit der Auditergebnisse gefährden könnten.

2.7 Lizenzerteilung

Die Lizenz wird erteilt, wenn folgende Bedingungen erfüllt sind:

- die Fachkundenachweise sind ausreichend,
- die Schulungsveranstaltung wurde absolviert,
- die Prüfung wurde bestanden,
- der Lizenzierungsvertrag zwischen BSI und Auditor wurde unterzeichnet und
- die Kosten für die Lizenzerteilung wurden entrichtet.

Die Lizenzurkunde enthält folgende Informationen:

- vollständiger Name und Adresse des Lizenznehmers
- auf Wunsch Name und Adresse des Arbeitgebers
- Beginn der Gültigkeit
- Ende der Gültigkeit

Die Lizenzurkunde bestätigt, dass der Lizenznehmer für die Dauer der Gültigkeit befugt ist, IT-Grundschutz-Audits für die Erlangung von IT-Grundschutz-

Zertifikaten durchzuführen. Er darf außerdem IT-Grundschutz-Selbsterklärungen (Einstiegsstufe oder Aufbaustufe) durch ein Testat bestätigen.

Die Lizenzurkunde trägt eine BSI-Registriernummer, die sich wie folgt zusammensetzt:

BSI-GSL-0001-2002

mit der Bedeutung:

BSI = Lizenzverleihende Stelle

GSL = IT-Grundschutz-Lizenz

0001 = laufende Vorgangsnummer

2002 = Jahr der Lizenzvergabe

2.8 Erfahrungsaustausch

Um einen Erfahrungsaustausch zwischen den lizenzierten IT-Grundschutz-Auditoren zu ermöglichen, lädt das BSI zu einem jährlichen Auditoren-Treffen ein. Die Teilnahme an mindestens 3 Terminen im Gültigkeitszeitraum ist Pflicht.

2.9 Lizenzverlängerung

Falls der Auditor im Zeitraum der Gültigkeit seiner Lizenz dem BSI mindestens drei Audit-Berichte gemäß Prüfschema für IT-Grundschutz-Audits vorgelegt hat und in ausreichendem Maße am Erfahrungsaustausch teilgenommen hat, wird die Lizenz nach Ablauf der Gültigkeit verlängert. Erfüllt der Auditor diese Voraussetzung nicht, muss eine neue Lizenzierung beantragt werden.

2.10 Lizenzentzug

Eine vom BSI erteilte Lizenz kann entzogen werden, wenn der Auditor mehrfach am Erfahrungsaustausch nicht teilnimmt oder schwerwiegend gegen das Prüfschema für Auditoren oder die vereinbarte Vertraulichkeit der Ergebnisse verstößt.

3 Fachkundenachweis

Das Lizenzierungsverfahren zum IT-Grundschutz-Auditor beinhaltet keine Schulungen zu Grundlagen der IT-Sicherheit oder des IT-Grundschutzes, solche grundlegenden Kenntnisse werden bei potenziellen Auditoren vorausgesetzt. Daher gelten für die Teilnahme am Lizenzierungsverfahren zum IT-Grundschutz-Auditor folgende Zulassungsvoraussetzungen:

- Der Antragsteller muss ausreichende Kenntnisse im Bereich der IT-Sicherheit besitzen und diese auch praktisch angewendet haben. Daher muss er nachweisen, dass er in den zurückliegenden zwei Jahren im Umfeld der IT-Sicherheit tätig gewesen ist. Beispiele für entsprechende Tätigkeitsfelder sind IT-Sicherheitsbeauftragte oder Berater für IT-Sicherheit.

  Insbesondere sollte er im Bereich IT-Sicherheitsmanagement Aufgaben wie die folgenden wahrgenommen haben:

  - Entwicklung von IT-Sicherheitszielen, -strategien sowie IT-Sicherheitsleitlinien,
  - Umsetzung bzw. Überprüfung von IT-Sicherheitsleitlinien,
  - Initiierung, Steuerung und Kontrolle des IT-Sicherheitsprozesses,
  - Erstellung des IT-Sicherheitskonzepts,
  - Überprüfung von IT-Sicherheitsmaßnahmen,
  - Aufbau und Durchführung von Schulungs- und Sensibilisierungsprogrammen,
  - Beratung in übergreifenden IT-Sicherheitsfragen.
- Der Antragsteller muss in den zurückliegenden fünf Jahren mindestens drei Projekte durchgeführt haben, in denen die Anwendung des IT-Grundschutzhandbuchs wesentlicher Bestandteil war. Hierzu zählen sowohl interne Projekte innerhalb einer Organisation als auch externe Projekte, z. B. Beratungsdienstleistungen. Beispiele für geeignete Projektinhalte sind IT-Sicherheitskonzeptionen oder IT-Sicherheitsrevisionen gemäß dem IT-Grundschutzhandbuch.

Als Nachweise sind beispielsweise geeignet:

- Zeugnisse oder Bestätigungen des Arbeitgebers,
- Bestätigungen von Auftraggebern oder Kunden,
- Veröffentlichungen,
- Gewerbenachweise.

Für den Nachweis der drei Referenzprojekte ist außerdem jeweils ein kurzer Projektbericht erforderlich, in dem die wesentlichen Ziele, Gegenstand und Vorgehensweise dargestellt werden. Angaben über Projekte mit Dritten können auch anonymisiert erfolgen. Das BSI behält sich vor, die gemachten Angaben zu überprüfen.