Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz-Methodik im Kontext von Outsourcing

Version 2.2
Stand: 23.12.2019

Inhaltsverzeichnis

Bundesamt für Sicherheit in der Informationstechnik Postfach
20 03 63
53133 Bonn
Tel.: +49 22899 9582-6222
E-Mail: gs-zert@bsi.bund.de
Internet: https://www.bsi.bund.de

1 Einleitung

Beim Outsourcing lagern Institutionen Geschäftsprozesse und Dienstleistungen ganz oder teilweise zu externen Dienstleistern aus. Outsourcing kann die Nutzung und den Betrieb von Hard- und Software betreffen, wobei die Leistung in den Räumlichkeiten des Auftraggebers oder in einer externen Betriebsstätte des Outsourcing-Dienstleisters erbracht werden kann. Typische Beispiele sind der Betrieb eines Rechenzentrums, einer Applikation, einer Webseite oder des Wachdienstes. Outsourcing ist ein Oberbegriff, der oftmals durch weitere Begriffe ergänzt wird wie Hosting, Housing oder Colocation.

Die grundsätzliche Vorgehensweise zum IT-Grundschutz ist in den BSI-Standards, im IT-Grundschutz-Kompendium sowie in den gültigen Prüfgrundlagen für die Zertifizierung beschrieben.

Das vorliegende Dokument richtet sich vorrangig an Antragsteller und Auditoren im Rahmen eines IT-Grundschutz-Zertifizierungsverfahrens. Daneben ist es auch anwendbar, wenn eine Institution ihr Sicherheitskonzept gemäß IT-Grundschutz aufbauen und Outsourcing-Dienstleister einbinden möchte. In den folgenden Kapiteln finden sich Ergänzungen und Konkretisierungen, die zu berücksichtigen sind, wenn Outsourcing angewendet wird. Im Anschluss finden sich einige Beispiele.

In diesem Dokument ist mit “Kunde“ stets die Institution gemeint, die einen externen Dienstleister im Rahmen von Outsourcing einbindet. Kunde kann damit insbesondere der Antragsteller für ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz sein.

2 Sicherheitskonzeption nach IT-Grundschutz

Dieses Kapitel richtet sich an Kunden und Auditoren.

2.1 Strukturanalyse

Bei der Strukturanalyse ist zunächst der Informationsverbund vollständig darzustellen. Hierbei ist zu identifizieren, ob Outsourcing im Informationsverbund stattfindet, d. h. ob einzelne Zielobjekte im Verantwortungsbereich von Outsourcing-Dienstleistern liegen. Zunächst geht es bei dieser "Ist"-Aufnahme um die reine Darstellung des Sachverhaltes.

Wenn ein Zielobjekt von einem externen Dienstleister betreut wird, kann es sein, dass der Kunde dieses Zielobjekt (beim externen Dienstleister) nicht komplett beschreiben kann, etwa wenn der exakte Servername oder die Lokation des Rechenzentrums nicht bekannt ist. Dann ist ein entsprechender Hinweis aufzunehmen.

Eine Strukturanalyse unter Berücksichtigung von Outsourcing ist in Kapitel 4.1 in Tabelle 1 und Tabelle 2 angegeben.

2.2 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung erfolgt gemäß BSI-Standard 200-2.

2.3 Modellierung

Outsourcing-Baustein
Der Kunde muss für jeden externen Dienstleister, der für ein Zielobjekt verantwortlich ist, den Baustein *OPS.2.1 Outsourcing für Kunden* modellieren und umsetzen. Wenn der externe Dienstleister IT-Grundschutz nutzt, sollte der Kunde außerdem überprüfen, dass der externe Dienstleister den Baustein *OPS.3.1 Outsourcing für Dienstleister* vollständig umgesetzt hat.

Bausteine für Zielobjekte, die der externe Dienstleister verantwortet
Der Kunde muss sicherstellen, dass bezogen auf seine Zielobjekte die Modellierung vollständig ist, das heißt die Modellierung muss auch die Baustein-Zielobjekt-Zuordnungen enthalten, für die der externe Dienstleister verantwortlich ist. Hilfreich ist in diesem Kontext eine separate Auflistung der Baustein-Zielobjekt-Zuordnungen, die für den externen Dienstleister relevant sind. Zu berücksichtigen sind die relevanten Bausteine aus den Schichten OPS, APP, SYS, NET und INF.

Eine Modellierung unter Berücksichtigung von Outsourcing ist in Kapitel 4.1 in Tabelle 4 angegeben.

2.4 IT-Grundschutz-Check

Der Kunde muss alle Anforderungen aus allen Bausteinen bearbeiten, die sich durch die Modellierung ergeben haben. Dies gilt auch dann, wenn der Kunde einen externen Dienstleister mit einer Tätigkeit beauftragt und damit die Umsetzung von Anforderungen delegiert hat. In diesem Fall erfolgt die Umsetzung der Anforderungen häufig über die vertraglichen Regelungen, die der Kunde mit dem externen Dienstleister abgeschlossen hat.

Damit bleibt der Kunde für die Umsetzung von Anforderungen verantwortlich, hat dies aber an den externen Dienstleister delegiert und dies vertraglich fixiert. So kann im Rahmen des IT-Grundschutz-Checks des Kunden geprüft werden, ob alle Anforderungen durch die vertraglichen Regelungen abgedeckt sind.

Dass der Kunde die Dienstleistersteuerung umsetzt und seine Dienstleister ausreichend kontrolliert, prüft der Auditor im Rahmen der Auditierung der Outsourcing-Bausteine. Ferner gelten die Anforderungen aus Kapitel 3.

Einen IT-Grundschutz-Check unter Berücksichtigung von Outsourcing ist in Kapitel 4.1 in Tabelle 5 angegeben.

2.5 Risikoanalyse

Die Risikoanalyse erfolgt gemäß der verwendeten Methodik, z.B. BSI-Standard 200-3.

3 Auditierung beim Dienstleister

Dieses Kapitel richtet sich an Auditoren.

Ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz ist ausgerichtet auf den Informationsverbund des Antragstellers. Die in diesen Informationsverbund eingebundenen externen Dienstleister, die für ein Zielobjekt verantwortlich sind, bekommen über diese Zertifizierung kein eigenständiges Zertifikat, sondern werden nur in den Zertifizierungsprozess involviert und wie folgt geprüft:

Wenn der Dienstleister ein gültiges **ISO 27001-Zertifikat auf der Basis IT-Grundschutz** vorweist und der Geltungsbereich dieses Zertifikates die Zielobjekte des Kunden samt Schutzbedarf vollständig und korrekt umfasst, dann kann dieses Zertifikat im Rahmen der Zertifizierung des Kunden-Informationsverbunds herangezogen werden. In diesem Fall ist kein zusätzliches Audit beim Dienstleister vor Ort notwendig.

Wenn der Dienstleister ein gültiges **ISO/IEC 27001-Zertifikat** einer akkreditierten Zertifizierungsstelle vorweist und der Geltungsbereich dieses Zertifikates die Zielobjekte des Kunden samt Schutzbedarf vollständig und korrekt umfasst, ist kein zusätzliches Audit beim Dienstleister vor Ort notwendig. Im Rahmen der Auditierung der Outsourcing-Bausteine prüft der Auditor, ob sinnvolle Sicherheitsanforderungen festgelegt sind und der Outsourcing-Dienstleister auf die Einhaltung von IT-Grundschutz oder einem vergleichbaren Schutzniveau verpflichtet ist (OPS.2.1.A1 Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben), der Outsourcing-Kunde regelmäßig die Anforderungen, insbesondere die Sicherheitsanforderungen, überprüft, also seine Kontroll- und Prüfungsrechte wahrnimmt (OPS.2.1.A4 Vertragsgestaltung mit dem Outsourcing-Dienstleister) und das ein Sicherheitskonzept für das Outsourcing-Vorhaben vorliegt und seine Wirksamkeit durch den Outsourcing-Kunden überprüft wird (OPS.2.1.A6 Erstellung eines Sicherheitskonzepts für das Outsourcing-Vorhaben). Der Auditor muss sich davon überzeugen und sicherstellen, dass der Outsourcing-Kunde seine Dienstleister-Steuerung angemessen nachkommt und der Outsourcing-Dienstleister ein dem IT-Grundschutz vergleichbares Schutzniveau einhält.

Wenn der Dienstleister **kein gültiges Zertifikat** vorweist, muss der Auditor ein Vor-Ort-Audit bei diesem Dienstleister vornehmen und inhaltlich Maßnahmen aus der Modellierung des Kunden beim Dienstleister prüfen. Den Umfang der Auditierung muss der Auditor im Rahmen der Auditplanung vor der Durchführung des Vor-Ort-Audits mit dem BSI abstimmen.

4 Beispiele

4.1 Hosting

Ein externes Rechenzentrum wird beauftragt, die Server des Kunden inklusive Betriebssystem zu betreiben. Das externe Rechenzentrum weist ein gültiges ISO/IEC 27001-Zertifikat auf.

Eine mögliche Strukturanalyse für IT-Systeme könnte wie folgt aussehen:

Bezeichnung	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Administratoren
S1	Server für Personalverwaltung	Windows Server 2012 R2	1	RZ1	In Betrieb	RZ ABC GmbH als externer Dienstleister

Tabelle *1*: Beispiel Strukturanalyse Server im Hosting

Eine mögliche Strukturanalyse für Räume und Gebäude könnte wie folgt aussehen:

Bezeichnung	Beschreibung	Lokation	Zugeordnet
R1	Raum in Rechenzentrum	Beauftragt: Externes Rechenzentrum: RZ ABC GmbH, Rechenzentrumstr. 1, 53111 Bonn	Systeme: S1
RZ1	RZ-Gebäude	Beauftragt: Externes Rechenzentrum: RZ ABC GmbH, Rechenzentrumstr. 1, 53111 Bonn	Räume: R1

Tabelle *2*: Beispiel Strukturanalyse Räume und Gebäude

Eine mögliche Übersicht der externen Dienstleister könnte wie folgt aussehen:

Bezeichnung	Beschreibung	Dienstleister
DL1	Betreiber des Rechenzentrums	RZ ABC GmbH, Rechenzentrumsstr. 1, 53111 Bonn
DL2	Wartung der Server	Fernwartungs GmbH, Hausstr. 2, 53112 Bonn
DL3	Betreiber der Anwendung A1	App-Host GmbH, Hauptstr. 3, 12345 Berlin

Tabelle *3*: Beispiel Übersicht externe Dienstleister

Die Modellierung enthält dann die folgende Zuordnung:

Schicht	Baustein	Zielobjekt	Erläuterung
OPS.2 Betrieb von Dritten	*OPS.2.1 Outsourcing für Kunden*	DL1	Externes Rechenzentrum: RZ ABC GmbH
INF Infrastruktur	*INF.1 Allgemeines Gebäude*	RZ1	Beauftragt: Externes Rechenzentrum: RZ ABC GmbH
INF Infrastruktur	*INF.2 Rechenzentrum sowie Serverraum*	R1	Beauftragt: Externes Rechenzentrum: RZ ABC GmbH
SYS.1 Server	*SYS.1.1 Allgemeiner Server*	S1	Beauftragt: Externes Rechenzentrum: RZ ABC GmbH
SYS.1 Server	*SYS.1.2.2 Windows Server 2012*	S1	Beauftragt: Externes Rechenzentrum: RZ ABC GmbH

Tabelle *4*: Beispiel Modellierung Hosting (Auswahl)

Im IT-Grundschutz-Check des Kunden werden die Anforderungen wie folgt dokumentiert:

Baustein-Zielobjekt-Zuordnung	Anforderung	Status	Erläuterung
INF.1 / RZ1	*INF.1.A2 Angepasste Aufteilung der Stromkreise*	Ja	Vertrag vom 01.03.2010 verpflichtet externen Dienstleister zur Einhaltung der IT-Grundschutz-Bausteine. Dies wurde im Rahmen des Dienstleisteraudits am 11.10.2017 verifiziert.
	INF.1.A14 Blitzschutzeinrichtungen	Ja	Vertrag vom 01.03.2010 verpflichtet externen Dienstleister zur Einhaltung der IT-Grundschutz-Bausteine. Dies wurde im Rahmen des Dienstleisteraudits am 11.10.2017 verifiziert.
	…		
INF.2 / R1	*INF.2.A2 Bildung von Brandabschnitten*	Ja	Vertrag vom 01.03.2010 verpflichtet externen Dienstleister zur Einhaltung der IT-Grundschutz-Bausteine. Dies wurde im Rahmen des Dienstleisteraudits am 11.10.2017 verifiziert.
	…		
SYS.1.1 / S1	*SYS.1.1.A3 Restriktive Rechtevergabe*	Ja	Vertrag vom 01.03.2010 verpflichtet externen Dienstleister zur Einhaltung der IT-Grundschutz-Bausteine. Dies wurde im Rahmen des Dienstleisteraudits am 11.10.2017 verifiziert.
	…		

Tabelle 5: Beispiel IT-Grundschutz-Check Hosting (Auswahl)

Sofern für den Dienstleister kein gültiges ISO 27001-Zertifikat auf der Basis von IT-Grundschutz oder ISO/IEC 27001-Zertifikat einer akkreditierten Zertifizierungsstelle vorliegt, prüft der Auditor diesen Dienstleister durch ein Vor-Ort-Audit.

4.2 Housing

Ein externes Rechenzentrum stellt Rechenzentrumsfläche zur Verfügung, in dem die IT-Systeme des Kunden durch den Kunden selber betrieben werden. Das externe Rechenzentrum verfügt über ein gültiges ISO 27001-Zertifikat auf der Basis von IT-Grundschutz. Das externe Rechenzentrum erhält keinen Zugriff auf die IT-Systeme. Eine mögliche Strukturanalyse wäre identisch zum Beispiel in Kapitel 4.1, Tabelle 1 und Tabelle 2.

Im Gegensatz zum Beispiel in Kapitel 4.1, Tabelle 4 ändert sich die Modellierung nur dahingehend, dass der Server S1 in der Verantwortung des Kunden betrieben wird:

Schicht	Baustein	Zielobjekt	Erläuterung
OPS.2 Betrieb von Dritten	*OPS.2.1 Outsourcing für Kunden*	DL1	Externes Rechenzentrum: RZ ABC GmbH
INF Infrastruktur	*INF.1 Allgemeines Gebäude*	RZ1	Beauftragt: Externes Rechenzentrum: RZ ABC GmbH
INF Infrastruktur	*INF.2 Rechenzentrum sowie Serverraum*	R1	Beauftragt: Externes Rechenzentrum: RZ ABC GmbH
SYS.1 Server	*SYS.1.1 Allgemeiner Server*	S1	Umsetzung durch IT-Abteilung
SYS.1 Server	*SYS.1.2.2 Windows Server 2012*	S1	Umsetzung durch IT-Abteilung

Tabelle 6: Modellierung Beispiel Housing (Auswahl)

Der IT-Grundschutz-Check ist ähnlich wie der IT-Grundschutz-Check in Beispiel in Kapitel 4.1, Tabelle 5, mit dem Unterschied, dass der Kunde die Bausteine der Schicht SYS.1 Server selber bearbeitet und nicht an den externen Dienstleister überträgt.

4.3 IT-Support mit externem Zugriff

Im Gegensatz zum IT-Support ohne externen Zugriff, siehe Beispiel in Kapitel 4.4, wartet der externe Dienstleister die IT-Systeme des Kunden von außen, das heißt, es liegt ein Fernwartungsvertrag vor.

In der Strukturanalyse wird der externe Dienstleister bei der Administration des Servers erfasst:

Bezeichnung	Beschreibung	Plattform	Anzahl	Aufstellungsort	Status	Administratoren
S1	Server für Personalverwaltung	Windows Server 2012 R2	1	RZ1	In Betrieb	Fernwartungs GmbH als externer Dienstleister

Tabelle 7: Beispiel Strukturanalyse Server für IT Support mit externem Zugriff

Ferner ist die externe Verbindung im Netzstrukturplan zu erfassen. Eine mögliche Modellierung kann dann wie folgt aussehen:

Schicht	Baustein	Zielobjekt	Erläuterung
OPS.2 Betrieb von Dritten	*OPS.2.1 Outsourcing für Kunden*	DL2	Externer Dienstleister: Fernwartungs GmbH
OPS.1 Eigener Betrieb	*OPS.1.2.5 Fernwartung*	DL2	Externer Dienstleister: Fernwartungs GmbH

Tabelle 8: Beispiel Modellierung für IT-Support mit externem Zugriff

In den meisten Fällen sind neben dem Baustein *OPS.1.2.5 Fernwartung* keine weiteren Bausteine relevant. Ebenso besteht in diesem Szenario keine Notwendigkeit eines Vor-Ort-Audits durch den Auditor.

4.4 Sonstige Dienstleister

Oft werden externe Dienstleister von einem Kunden beauftragt, um Aufgaben in seinem Namen wahrzunehmen, ohne jedoch die Verantwortung für ein Zielobjekt zu übernehmen. Da ein Dienstleister dennoch Zugang zu Zielobjekten haben kann, muss der Dienstleister in die Sicherheitskonzeption nach IT-Grundschutz eingebunden werden. Der Baustein OPS.2.1 Outsourcing für Kunden ist nicht anzuwenden, die Einbindung erfolgt auf Anforderungsebene wie im Folgenden beschrieben:

Grundsätzlich muss der Kunde bei sonstigen Dienstleistern die Anforderung ORP.2.A4 *Regelungen für den Einsatz von Fremdpersonal* umsetzen. Abhängig von der Art des gewählten Dienstleisters, müssen noch weitere Anforderungen betrachtet werden. Die folgende, nicht abschließende Aufstellung zeigt einige Beispiele für Dienstleister und die relevanten Anforderungen:

- **Sicherheitsdienste**
  - *INF.1.A26 Pförtner- oder Sicherheitsdienst*

- **Reinigungskräfte**
  - *INF.1.A30 Organisatorische Vorgaben für die Gebäudereinigung*

- **Wartungsdienste für Infrastruktur (USV, Klimaanlagen)**
  - *ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonal*
  - *INF.1.A5 Handfeuerlöscher*

- **IT-Support ohne externen Zugriff**
  - *ORP.1.A3 Beaufsichtigung oder Begleitung von Fremdpersonal*
  - *OPS.1.1.2.A2 Vertretungsregelungen und Notfallvorsorge*

- **IT-Support mit externem Zugriff**
  Der Zugriff erfolgt nur bei Bedarf und ohne Regelmäßigkeit, z. B. wenn bei einem Problem der Hersteller eines Produktes über Fernwartung unterstützt.
  - *OPS.1.2.5.A19 Fernwartung durch Dritte*

Dienstleister, wie z.B. Internet-Provider, die eine Anbindung an das Internet als Schnittstelle bereitstellen und keine IT-Sicherheitsmanagement-Tätigkeiten im engeren Sinne übernehmen, werden im Rahmen von Outsourcing nicht weiter betrachtet.