Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheitsrichtlinie für das Outsourcing von IT-Leistungen

- Beispiel -

Stand: Dezember 2008

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn • Postfach 20 03 63, 53133 Bonn
Tel.: + 49 (0) 1888 9582-0 • Fax: + 49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

INHALTSVERZEICHNIS

1 Einleitung

Diese Sicherheitsrichtlinie umfasst Regelungen zur Sicherstellung der Informationssicherheit im Falle des Outsourcings von IT-Leistungen.

Diese Sicherheitsrichtlinie basiert auf den IT-Grundschutz-Katalogen des BSI. In der rechten Spalte befinden sich Verweise zu Hintergrundinformationen und zu Maßnahmenvorschlägen innerhalb der IT-Grundschutz-Kataloge. M x.xx

Hinweis:

Bemerkungen und Hinweise, an welchen Stellen sich eine individuelle Anpassung oder Ergänzung der Musterrichtlinie besonders empfiehlt, sind gelb hinterlegt. Beispielsweise wird in dieser Beispielrichtlinie für verschiedene Tätigkeiten eine verantwortliche Person benannt. Die Verantwortlichkeiten müssen natürlich an die eigene Organisationsstruktur angepasst werden.

2 Geltungsbereich

Diese Sicherheitsrichtlinie gilt für alle Betriebsteile und ist bei der Gestaltung von Outsourcing-Vorhaben zugrunde zu legen, wenn Dienstleistungen im Bereich Informationsverarbeitung betroffen sind.

Bereits vor jeder Outsourcing-Entscheidung sind Sicherheitsaspekte zu bedenken und bei einer Ausschreibung zu berücksichtigen. M 2.250, M 2.251

Die Richtlinie ist gegenüber dem Outsourcing-Dienstleister als Prüfungsgrundlage zu nutzen und den Verträgen mit Dienstleistern zugrunde zu legen.

Für die inhaltliche Bearbeitung sowie für die Pflege und Änderung der Texte ist der IT-Sicherheitsbeauftragte in Zusammenarbeit mit dem Leitungsstab zuständig und verantwortlich.

3 Auswahl eines Outsourcing-Dienstleisters

Es ist selten Erfolg versprechend, eine Geschäftsbeziehung lediglich auf Verträge und Regressansprüche zu begründen. Daher ist der Outsourcing-Dienstleister sorgfältig auszuwählen und eine vertrauensvolle und kooperative Zusammenarbeit anzustreben. M 2.252

Bei der Auswahl ist zu prüfen, ob der Auftragnehmer als makellos, unbescholten und unbestechlich einzuschätzen ist (Zuverlässigkeit) und ob ein ernsthaftes und fachkundiges Betreiben der Dienstleistung gewährleistet ist (Seriosität).

Zu diesem Zweck sind folgende Punkte zu hinterfragen:

- Referenzen — M 2.252
- Kompetenz und Verfügbarkeit des Ansprechpartners — M 2.26
- Vertrauenswürdigkeit der Mitarbeiter — M 3.33
- Notfallplanung — M 6.9, M 6.83
- Zertifizierungen — M 2.66, M 2.252
- garantierte Verfügbarkeit (maximale Ausfallzeit) — M 6.1
- Sicherheitskonzept und Sicherheitsrichtlinien. — M 2.192, M 2.195

Für die Beurteilung sollte bei größeren Vorhaben eine Besichtigung des Outsourcing-Dienstleisters erfolgen.

4 Vertragsspezifische Regelungen

Externen darf generell erst dann Zugang zu IT-Systemen und Anwendungen gewährt werden, wenn ein Vertrag unterschrieben wurde, der die Bedingungen für die Verbindung oder den Zugang definiert.

Im Vertrag ist schriftlich zu vereinbaren: M 2.253

- Weisungsgebundenheit des Outsourcing-Dienstleisters
- Einhaltung der einschlägigen Gesetze, Vorschriften und internen Regelungen — M 3.2, M 2.254
- Stillschweigen über alle bekannt werdenden Informationen — M 3.6
- technische und organisatorische Maßnahmen im Einflussbereich des Outsourcing-Dienstleisters und deren Kontrolle — M 2.182, M 2.251
- Melde- und Kommunikationswege — M 2.42
- Notfallvorsorgemaßnahmen — M 6.83
- Personaleinsatz durch den Outsourcing-Dienstleister
- Zutritts- und Zugangsrechte
- Regelungen für den Fall der Nicht- oder mangelhaften Erfüllung
- Verfügbarkeitsanforderungen — M 6.1
- Rechte und Pflichten des externen Personals — M 2.4, M 2.193
- Regelungen zur Haftung
- Verfahren bei Beendigung des Vertrags (siehe Kapitel 7.5).

5 Organisation

Es sind auf beiden Seiten Verantwortliche zu benennen. Es ist sicherzustellen, dass diese ausreichende Befugnisse besitzen.

Externe Mitarbeiter sind vor Beginn ihrer Tätigkeit einzuweisen und über hausinterne Regelungen und Vorschriften zur Informationssicherheit sowie die organisationsweite Leitlinie zur Informationssicherheits zu unterrichten. M 3.11, M 3.2, M 3.5, M 2.254

Externe Mitarbeiter, die (eventuell) Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen und zur Verschwiegenheit zu verpflichten. M 3.2, M 3.6

Der Outsourcing-Dienstleister hat die Weisungen des Auftragnehmers zu

befolgen. Dies ist regelmäßig zu überprüfen. M 2.182

Aufträge an Subunternehmer durch den Outsourcing-Dienstleister bedürfen einer Genehmigung. Subunternehmer unterliegen den gleichen Anforderungen wie der Hauptauftragnehmer.

6 Zutritts-, Zugangs- und Zugriffsrechte externer Mitarbeiter

Externe müssen sich ausweisen. M 2.16

Sofern ein Zutritt zu Sicherheitszonen zwingend erforderlich ist, sind externe Mitarbeiter zu beaufsichtigen. Kurzfristig oder einmalig zum Einsatz kommendes Fremdpersonal ist wie Besucher zu begleiten oder zu beaufsichtigen. M 2.16

Der Zugriff auf Daten durch Externe ist soweit wie möglich zu vermeiden. Externen kann, sofern dies zwingend erforderlich ist, ein zeitlich begrenzter Zugang gewährt werden, wenn entsprechende Sicherheitsmaßnahmen eingerichtet worden sind. M 4.16 M 2.220

Sofern ein dauerhafter Zugang notwendig ist, sind einer namentlich benannten Person restriktive Zugangsrechte zu gewähren. M 2.220, M 4.16

Es ist sicherzustellen, dass die externen Mitarbeiter keinen Zugriff auf Systeme außerhalb ihres Tätigkeitsbereiches erhalten. M 2.32

„Regelungen zum Ende der Tätigkeiten“ (siehe Kapitel 7.5) sind zu beachten.

7 Sicherheitsmaßnahmen

7.1 Allgemeine Regelungen

Für umfangreiche oder komplexe Outsourcing-Vorhaben muss ein eigenes Sicherheitskonzept erstellt werden. M 2.254

Es ist seitens des externen Outsourcing-Dienstleisters ein Sicherheitsprozess zu etablieren, der zu kontrollieren ist. M 2.182, M 2.256

Die durchgeführten Arbeiten sind zu dokumentieren (Umfang, Ergebnisse, Zeitpunkt, evtl. Name des externen Mitarbeiters). M 2.34

Eine Fehlerbeseitigung im Betriebssystem und in systemnaher Software darf durch das externe Personal nur nach Genehmigung erfolgen. M 2.215

Es sind Regelungen zur Kommunikation und dem Datenaustausch zwischen Auftraggeber und dem Dienstleister zu schaffen. Hierbei ist auch die "Sicherheitsrichtlinie für die Internetnutzung" (siehe Musterdokument des BSI) zu beachten. M 5.88

In Sicherheitszonen kann das Mitbringen tragbarer IT-Systeme, Mobiltelefone, Kameras etc. vom IT-Sicherheitsbeauftragten verboten werden. M 2.17

7.2 Arbeiten durch externes Personal im Hause

Arbeiten, die von Externen innerhalb der Räumlichkeiten des Auftragnehmers stattfinden, sind in separaten Räumlichkeiten durchzuführen.

Bei Arbeiten an sensitiven Systemen bzw. Systemen mit sensitiven Daten hat eine fachkundige Kraft die Arbeiten zu beaufsichtigen. M 2.16

7.3 Arbeiten durch externe Dienstleister außerhalb des Hauses

Wird Hardware zur Wartung oder Reparatur außer Haus gegeben, sind alle sensitiven Daten, die sich auf Datenträgern befinden, vorher sicher zu löschen. M 2.218 Der Transport von Datenträgern hat sicher zu erfolgen. M 2.167, M 2.3

7.4 Externe Arbeiten über Fernzugriff

Generell ist der „Zugriff vor Ort“ dem „Fernzugriff“ vorzuziehen. M 2.102

Die sichere Anbindung an das interne Netz ist zu regeln. M 5.87

Es ist die "Sicherheitsrichtlinie zur IT-Nutzung" (Musterdokument des BSI) zu beachten.

7.5 Regelungen zum Ende der Tätigkeiten

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen. M 2.4

Es ist die ordnungsgemäße Funktion von gewarteten IT-Systemen zu überprüfen. Bei entsprechend gefährdeten IT-Systemen ist eine Virenüberprüfung durchzuführen. M 2.62 M 2.160

Es sind außerdem sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Außerdem sind ausscheidende Mitarbeiter explizit darauf hinzuweisen, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt. M 4.17 M 3.2, M 3.6

Daten, die im Rahmen des Outsourcings extern gespeichert wurden, sind nach Abschluss des Auftrags vollständig und sicher zu löschen. Dies ist zu kontrollieren. M 2.167 M 2.256