Ergänzung zum Zertifizierungsschema Nr. 1	
Titel	IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten
Status	Version 1.0
Datum	08.03.2004

IT-Grundschutz-Zertifizierung von ausgelagerten Komponenten

Diese Ergänzung zum Zertifizierungsschema gibt verbindliche Hinweise, was ein Auditor beachten muss, wenn Komponenten des Untersuchungsgegenstandes teilweise oder komplett ausgelagert sind. Sie soll u. a. die folgenden Fragen klären:

- Welche Bausteine des IT-Grundschutzhandbuchs sind auch auf den Dienstleister anzuwenden?
- Wann ist der Baustein Outsourcing im Rahmen der Zertifizierung anzuwenden?
- Welche Outsourcing-Dienstleistungen sind überhaupt zertifizierungsrelevant?

Begriffsbestimmung

Der Antragsteller, der einen Geschäftsprozess, eine Organisationseinheit oder eine Fachaufgabe zertifizieren lassen möchte, wird im weiteren Verlauf als **Auftraggeber** bezeichnet, der Outsourcing-Partner als **Dienstleister**. "IT-Verbund" bezieht sich im Folgenden nicht auf den gesamten IT-Verbund des Antragstellers, sondern immer auf den Untersuchungsgegenstand des Zertifizierungsvorhabens. Ein Teil des IT-Verbundes kann sich dabei unter Kontrolle des Auftraggebers befinden, ein anderer im Einflussbereich des Dienstleisters.

Relevanz von Outsourcing-Dienstleistungen

Eine Auslagerung von Tätigkeiten oder Aufgaben ist nur dann für eine IT-Grundschutz-Zertifizierung relevant, wenn die folgenden Bedingungen alle erfüllt sind:

- Die Bindung an den Dienstleister erfolgt auf längere Zeit **und**
- durch die Dienstleistung kann die IT-Sicherheit des Auftraggebers beeinflusst werden **und**
- im Rahmen der Dienstleistung erbringt der Dienstleister auch regelmäßig nennenswerte IT-Sicherheitsmanagement-Tätigkeiten.

Beipiel: Der Auftraggeber mietet eine Standleitung zur Anbindung einer Außenstelle an die Firmenzentrale von einem TK-Anbieter. Über die Standleitung werden auch schutzbedürftige Daten übertragen. Die Dienstleistung besteht nur in der Bereitstellung der Leitung. In diesem Fall übernimmt der TK-Anbieter keine IT-Sicherheitsmanagement-Tätigkeiten im engeren Sinn, daher ist dieser Dienstleistungsvertrag für eine IT-Grundschutz-Zertifizierung **nicht** relevant.

Wenn der Auftraggeber hohe Anforderungen an die Verfügbarkeit der Leitung hat, ist der Baustein Notfallvorsorge zu bearbeiten (und ggf. eine redundante oder alternative Anbindung der Außenstelle zu planen).

Wenn der Auftraggeber hohe Anforderungen an die Vertraulichkeit der Datenübertragung hat, muss er den Baustein Kryptokonzept anwenden (und ggf. eine Verschlüsselung der Datenübertragung sicherstellen).

Beispiel: Der Auftraggeber mietet eine Standleitung zur Anbindung einer Außenstelle an die Firmenzentrale von einem TK-Anbieter. Über die Standleitung werden auch schutzbedürftige Daten übertragen. Die Dienstleistung geht über die Bereitstellung der Leitung hinaus. Der Dienstleister ist zusätzlich dafür verantwortlich, die Anbindung hochverfügbar bereitzustellen und kryptographisch zu sichern. In diesem Fall handelt es ich sich um "gemanagete" IT-Sicherheit, so dass die Dienstleistung für eine IT-Grundschutz-Zertifizierung relevant ist.

Beispiel: Der Auftraggeber mietet IT-Systeme (z. B. zur Datensicherung) von einem Dienstleister. Der Dienstleister wartet die IT-Systeme regelmäßig und sorgt dafür, dass sie funktionstüchtig sind und fehlerhafte Komponenten ausgetauscht werden. In diesem Fall übernimmt der Dienstleister keine IT-Sicherheitsmanagement-Tätigkeiten im engeren Sinn, daher ist dieser Dienstleistungsvertrag für eine IT-Grundschutz-Zertifizierung **nicht** relevant.

Natürlich muss der Auftraggeber dafür sorgen, dass alle relevanten IT-Grundschutz-Maßnahmen wie beispielsweise M 2.90 *Überprüfung der Lieferung*, M 4.65 *Test neuer Hard- und Software* oder M 2.226 *Regelungen für den Einsatz von Fremdpersonal* umgesetzt und beachtet werden.

1. Fall: Outsourcing stellt eine unbedeutende Gefährdung für den Untersuchungsgegenstand dar

Man kann nur dann von einer unbedeutenden Gefährdung der Geschäftstätigkeit durch Outsourcing ausgehen, wenn alle nachfolgenden Bedingungen erfüllt sind:

- Es sind nur unwesentliche Komponenten des IT-Verbunds ausgelagert **und**
- die ausgelagerten Komponenten des IT-Verbunds haben höchstens mittleren Schutzbedarf **und**
- durch kumulierte Schadensereignisse wird der Schutzbedarf nicht erhöht.

Die Empfehlungen des Outsourcing-Bausteins sind in diesem Fall optional.

Eine Prüfung des Dienstleisters ist im Rahmen des Audits nicht notwendig. Nur die Schnittstelle zwischen Auftraggeber und Dienstleister ist zu prüfen.

Es sind auch keine Bausteine auf den Dienstleister anzuwenden.

Beispiel: Der Internetauftritt eines Unternehmens wird von einem externen Dienstleister betrieben. Die Web-Seite enthält nur allgemeine Informationen zum Unternehmen, die weder hoch vertraulich noch hoch verfügbar sind. Auch Veränderungen an den dargebotenen Inhalten führen zu keinem größeren Schaden. In diesem Fall sind die oben genannten Bedingungen erfüllt.

Beispiel: Ein Unternehmen hat das SAP-System zu einem externen Dienstleister ausgelagert. Kein SAP-Modul hat für sich genommen einen hohen Schutzbedarf. Ein Totalausfall des SAP-Systems für mehrere Tage hätte aber große geschäftsschädigende Auswirkungen, da alle geschäftlichen Aktivitäten stillstehen würden. In diesem Fall ist der Schutzbedarf des SAP-Systems hoch, auch wenn

der der einzelnen Module nur mittel ist (Kumulationseffekt). In diesem Fall trifft eine oben genannte Bedingung nicht zu, das Audit muss den Dienstleister umfassen.

2. Fall: Ausgelagerte Komponenten sind bedeutenden Gefährdungen ausgesetzt

Von bedeutenden Gefährdungen der Geschäftstätigkeit muss immer dann ausgegangen werden, wenn eine der folgenden Bedingungen gegeben ist:

- Komponenten des ausgelagerten IT-Verbunds haben hohen oder sogar sehr hohen Schutzbedarf **oder**
- wesentliche Teile des IT-Verbunds sind ausgelagert.

Der Baustein Outsourcing ist in diesem Fall anzuwenden.

Bei der Modellierung sind alle relevanten Bausteine des IT-Grundschutzhandbuchs sowohl für den Auftraggeber als auch für den Dienstleister zu berücksichtigen.

Folgende Bausteine sind für Auftraggeber und Dienstleister immer getrennt anzuwenden:

IT-Sicherheitsmanagement, Organisation, Personal, Hard- und Software-Management, Notfallvorsorge-Konzept, Behandlung von Sicherheitsvorfällen

Abweichungen von den Empfehlungen des IT-Grundschutzhandbuchs (insbesondere des Outsourcing-Bausteins) und den Vorgaben des Zertifizierungsschemas müssen stichhaltig begründet werden:

Beispiel: Wenn Aufgaben vollständig auf den Dienstleister übertragen sind, ist der entsprechende Baustein für den Auftraggeber entbehrlich. Ein Beispiel ist der Betrieb einer Firewall durch einen Dienstleister (Hardware, Patches, Konfiguration etc.). Der Baustein Firewall ist in diesem Fall nur einmal beim Dienstleister anzuwenden.

Beispiel: Die Mitarbeiter des Dienstleisters arbeiten im Gebäude des Dienstleisters und die jeweilige Informationstechnik wird im Gebäude des Dienstleisters betrieben. Die Bausteine für Gebäude, Verkabelung und Räume sind dann auch auf die Liegenschaft des Dienstleisters anzuwenden.

Beispiel: Die Mitarbeiter des Dienstleisters arbeiten vor Ort beim Auftraggeber und die jeweilige Informationstechnik wird im Gebäude des Auftraggebers betrieben. Die Infrastruktur-Bausteine müssen dann nicht auf die Liegenschaft des Dienstleisters angewendet werden.

3. Fall: Begrenztes Schadensausmaß (Sonderfall)

Der Sonderfall ist erfüllt, wenn die folgenden Bedingungen **alle** zutreffen:

- Der Outsourcing-Dienstleister verpflichtet sich vertraglich auf die Einhaltung von IT-Grundschutz **und**
- im Einflussbereich des Outsourcing-Dienstleister kann nur finanzieller Schaden entstehen, d. h. Menschen können nicht zu Schaden kommen, Verstöße gegen Gesetze und Beeinträchtigungen des informationellen Selbstbestimmungsrechts sind ausgeschlossen **und**

- ein möglicher Schaden lässt sich so eindeutig beschreiben (Schadensdefinition, Höhe des Schadens, Schadensfolgen usw.), dass vertraglich Schadensersatz oder eine andere Wiedergutmachung vereinbart werden kann.

Der Baustein Outsourcing ist in diesem Fall anzuwenden.

Wenn Schadensersatzansprüche im Dienstleistungsvertrag geregelt und die Solvenz des Dienstleisters gesichert sind, muss der Dienstleister aber nicht ins Audit einbezogen werden. Die vertragliche Zusicherung von IT-Grundschutz ist hier ausreichend. Der Auditor muss die Anwendbarkeit dieses Sonderfalles im Auditreport stichhaltig begründen.

Es sind keine Bausteine auf den Dienstleister anzuwenden.

4. Fall: Der Outsourcing-Dienstleister verfügt über ein IT-Grundschutz-Zertifikat

Ein Auftraggeber eines Outsourcing-Dienstleisters beantragt ein IT-Grundschutz-Zertifikat. Der zu zertifizierende IT-Verbund des Auftraggebers enthält Komponenten, die zum Outsourcing-Dienstleister ausgelagert sind. Es müssen die folgenden Bedingungen erfüllt sein:

- Der Outsourcing-Dienstleister verfügt über ein IT-Grundschutz-Zertifikat (ein Antrag oder eine Selbsterklärung sind nicht ausreichend) **und**
- die betroffenen Komponenten sind Teil des zertifizierten IT-Verbunds des Outsourcing-Dienstleisters.

Der Baustein Outsourcing ist in diesem Fall anzuwenden.

Bei der Modellierung müssen alle relevanten Bausteine getrennt auf Auftraggeber und Dienstleister angewendet werden. Der Auditor muss überprüfen, welche ausgelagerten Komponenten (bzw. Bausteine) bereits von der Zertifizierung abgedeckt sind. Alle Zielobjekte, die bereits geprüft sind, müssen dann nicht wieder geprüft werden. Der Auditor muss im Auditreport seine Entscheidung, das Zertifikat des Outsourcing-Dienstleisters anzuerkennen, genau dokumentieren und begründen.

Wird eine Zertifizierung des Dienstleisters angerechnet, gelten folgende Regelungen:

1. Wird dem Outsourcing-Dienstleister das Zertifikat aufgrund schwerwiegender Gründe durch die Zertifizierungsstelle entzogen, verliert auch das davon abhängende Zertifikat seines Auftraggebers zeitgleich seine Gültigkeit.

2. Ist zum Zeitpunkt der Zertifizierung des Auftraggebers das Zertifikat des Dienstleisters noch länger als ein Jahr gültig, ist das Zertifikat für den IT-Verbund des Auftraggebers volle 2 Jahre gültig.

3. Läuft zum Zeitpunkt der Zertifizierung des Auftraggebers das Zertifikat des Dienstleisters innerhalb eines Jahres aus, verliert mit Ablauf seiner Gültigkeit auch das Zertifikat des Auftraggebers seine Gültigkeit. Es gibt zwei Wege, wie das Zertifikat des Auftraggebers seine normale Gültigkeit behalten kann.

3 a) Im Fall einer Re-Zertifizierung des Outsourcing-Dienstleisters (für denselben IT-Verbund) behält das Zertifikat des Auftraggebers seine normale Gültigkeit. Zwischen Ablauf des Zertifikats des Outsourcing-Dienstleisters und der Re-Zertifizierung dürfen höchstens 60 Tage liegen.

3 b) Zertifiziert der Outsourcing-Dienstleister einen neuen IT-Verbund, der den ursprünglichen umfasst, kann durch einen (beliebigen) lizenzierten IT-Grundschutz-Auditor bestätigt werden, dass der IT-Verbund des Auftraggebers weiterhin zertifikatswürdig ist. In diesem Fall behält das Zertifikat des Auftraggebers seine normale Gültigkeit von zwei Jahren. Zwischen Ablauf des Dienstleisterzertifikats und dem Tag der Bestätigung des Auditors über die andauernde Zertifikatswürdigkeit des Auftraggebers dürfen höchstens 60 Tage liegen.