Eberhard von Faber

IT-Outsourcing – Sicherheit neu denken!

Hintergrund

Anwenderorganisationen können über eine eigene, produzierende IT-Abteilung verfügen oder die Bereitstellung der IT-Services an eine andere Firma, einen externen IT-Dienstleister „auslagern“. Oft wird gar keine Hard- und Software per Migration ausgelagert; vielmehr werden IT-Dienste von vornherein extern von Dritten bezogen. Der Begriff „IT-Outsourcing“ soll so verstanden werden. Mit dem IT-Outsourcing sind drei Veränderungen verbunden:

- ♦ Die Verantwortung für die Bereitstellung der IT- oder TK-Dienste geht auf den Dienstleister über. Das mit deren Nutzung verbundene Geschäftsrisiko verbleibt allerdings primär beim Anwenderunternehmen. Risiko und Herstellungsprozess sind getrennt.
- ♦ Durch die Trennung entsteht ein über den Markt vermittelte Schnittstelle zwischen Anwenderorganisation und Dienstleister. Die Anwenderorganisation hat weniger Einflussmöglichkeiten. Sie werden durch den Mangel an direkter Weisungsbefugnis und durch die Standardisierung der IT-Dienste begrenzt.
- ♦ Die Anwenderorganisation verfügt ad-hoc über ein geringeres Wissen bezüglich integrierter Sicherheitsmaßnahmen, weil die Gestaltung von Technik und Bereitstellung in der Hand des Dienstleisters liegt. Nutzung und Eigentum sind voneinander getrennt.

Komplizierter wird die Lage dadurch, dass große IT/TK-Dienstleister sehr arbeitsteilig organisiert sind und dass viele Leistungen von anderem, zum Lieferantennetzwerk gehörenden Unternehmen bereitgestellt werden. Das betrifft nicht nur technische Komponenten, sondern auch das IT-Service-Management (Help-Desk, Überwachung, Diagnose, Instandhaltung u.v.a.m.).

Interessen

Anwenderorganisation und IT-Dienstleister bzw. IT-Dienstleister und Lieferant haben verschiedene Interessen:

- ♦ Der Käufer erwartet ein hohes Sicherheitsniveau und einen geringen Preis. Der Verkäufer ist an geringen Herstellungskosten und zufriedenen Kunden interessiert. Da IT-Sicherheit Geld kostet, muss ein Kompromiss gefunden werden sowohl innerhalb der jeweiligen Anforderungskataloge beider Parteien als auch zwischen ihnen.
- ♦ Der Käufer erwartet Transparenz bezüglich der integrierten IT-Sicherheit, will bzw. kann sich um Details aber eigentlich nicht kümmern – sonst würde er nicht „outsourcen“. Der Verkäufer betrachtet viele Details als sein Eigentum, möchte aber seine Kunden zufriedenstellen. Der Austausch von Informationen und Kontrollen bedeuten für beiden Seiten Kosten. Jeder Partner muss für sich und mit der anderen Seite einen Kompromiss finden.

IT-Sicherheit

Die IT-Sicherheit konzentriert sich traditionell auf Maßnahmen zur Abwehr von Bedrohungen bzw. Verminderung von Risiken und (hoffentlich auch) auf die Prozesse der Implementierung und Pflege. **Keine** der oben aufgeworfenen Schwierigkeiten betrifft jedoch die Existenz oder Qualität der Sicherheitsmaßnahmen.

Das sind neue Herausforderungen für gemeinsames, erfolgreiches und sicheres IT-Outsourcing:

- ♦ Vertrauenswürdigkeit,
- ♦ Kunden- und Lieferantenmanagement,
- ♦ Kostenmanagement, Standardisierung und Industrialisierung.

Vertrauenswürdigkeit: Es muss sich die Einsicht durchsetzen, dass es nicht allein um die „IT-Sicherheit“ (Abwesenheit von nicht akzeptierten Risiken), sondern um das „Wissen über IT-Sicherheit“ (Vertrauenswürdigkeit) geht. Das ist kaum eine technische Disziplin. *Sicherheitsmanagement betrifft zunehmend das Management von Vertrauenswürdigkeit.* ISO 27001- und ähnliche Zertifizierungen sind nur ein kleiner Teil der Antwort.

Kunden- und Lieferanten-Management: Anforderungslisten und Pflichtenhefte sind wichtig; aber wie setzt man sie konkret ein? Sicherheit wird zum Teil von Beschaffungs- bzw. Angebotsprozessen, in denen IT-Sicherheit nur ein Aspekt ist und seine Eigenständigkeit als Domäne verliert. *Sicherheitsmanagement betrifft zunehmend das Management von Beziehungen zwischen Marktteilnehmern* auch in der Betriebsphase.

Kostenmanagement, Standardisierung und Industrialisierung: Vor einigen Jahren kam „Green-IT“. Der Hintergrund war die „Entdeckung“, dass IT hohe Stromkosten verursacht. Danach kam „Cloud“. Dahinter stand die Idee, IT billiger und einfacher zu machen. Wenn jetzt „IT-Sicherheit“ ein Thema ist, wird das Kosten-Nutzen-Verhältnis diskutiert werden. Die IT-Sicherheitsexperten haben sich (vergeblich) bemüht, die Nutzenargumentation zu verbessern. Jetzt lernen die Unternehmen ganz automatisch (über eigene und fremde Schmerzen). Haben wir eine Antwort auf die Kostenfrage?

Lesen Sie doch einmal im Schwerpunkt nach. *Die IT-Sicherheit darf bei der Industrialisierung der IT nicht auf der Strecke bleiben; sie muss sich industrialisieren und zur Stütze der Digitalisierung werden.* Auch interessant: Der Studiengang Security-Management der Technischen Hochschule Brandenburg bereitet ein Seminar zum Schwerpunkt dieses Heftes vor.

Eberhard.vonFaber@th-brandenburg.de