amendos

Newsletter 04/2017

Inhalt:

Agilität und Multi-Providermanagement

Der Begriff Agilität ist in aller Munde: IT-Bereiche in Unternehmen sollen sich agil ausrichten, um den sich immer schneller ändernden Anforderungen des Business gerecht zu werden. Wir untersuchen, was das konkret heißt und welche Folgen sich hieraus für das Multi Providermanagement ergeben, wenn ein Unternehmen Services von verschiedenen externen Providern bezieht.

Agilitätsanforderung

Was bedeutet eine agile Ausrichtung zunächst einmal für den IT-Bereich:

- Bereits bestehende und neu zu entwickelnde IT-Applikationen werden permanent in kleinen Schritten (sogen. „Sprints“ lt. Scrum, siehe Abbildung 1) verändert und erweitert und
- die hierfür erforderliche Infrastruktur ist entsprechend dynamisch an diese Änderungen anzupassen.

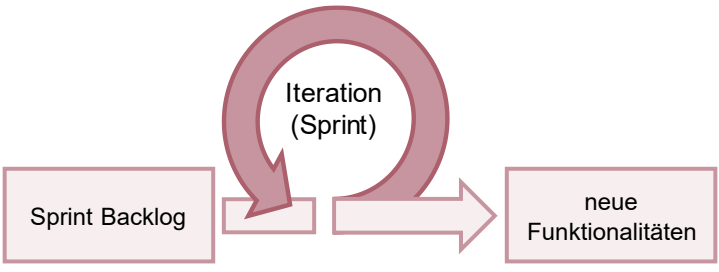

Abbildung 1: Sprint laut Scrum

Anforderungen an das IT Service Management

Eine agile Ausrichtung des IT-Bereiches kann nur dann erfolgreich sein, wenn im IT Service Management vorher die entsprechenden Rahmenbedingungen geschaffen wurden. Dies betrifft insbesondere die folgenden Aspekte:

Servicebeschreibung und -preis

Um die oben genannten inkrementellen Anpassungen ohne Reibungsverluste vornehmen zu können, sollten die jeweiligen Services so definiert sein, dass sie nicht nach jeder Funktionsänderung bzw. -erweiterung hinsichtlich Beschreibung und Preis angepasst werden müssen. Hier bietet sich das Pareto-Prinzip (80:20-Regel) an. Dies bedeutet im Umkehrschluss aber auch, dass es eine klare Definition geben muss, wann Changes einen Service tatsächlich verändern, d.h. sowohl Auswirkungen auf die Servicebeschreibung (als Teil des Servicekatalogs) als auch den Servicepreis haben. Die so ermittelten notwendigen Preisanpassungen sollten gebündelt und vor der nächsten Budgetplanungsrunde erfolgen.

Change-Management-Prozess

Da die Anzahl der Changes im agilen Umfeld pro Intervall zunehmen wird, kommt dem Change Management eine zentrale Rolle zu. Im Rahmen dieses Prozesses gilt es zunächst, zwei Arten von Changes zu definieren.

- **Major Changes:** Diese verändern in der Regel die Servicebeschreibung und/oder den -preis. Sie beinhalten zudem ein höheres Risikopotenzial und müssen daher sehr gut vorbereitet und sorgfältig abgewickelt werden. Das Change Advisory Board (CAB) muss sie stets autorisieren.
- **Vorautorisierte Standard Changes:** Diese Changes wirken sich weder auf die Servicebeschreibung noch auf den -preis aus und bergen geringe Risiken. Daher ist es möglich, sie im Vorweg zu autorisieren und weitestgehend automatisiert, also mit einem Minimum an manuellen Eingriffen, durchzuführen. Sie durchlaufen somit einen stark vereinfachten Standard-Change-Prozess, der sich im Wesentlichen auf Risikominimierung durch Qualitätsmanagement konzentriert.

Die Anzahl der Standard Changes am Gesamtvolumen aller Changes sollte möglichst hoch sein, um eine effiziente Abwicklung zu ermöglichen. Dennoch gilt es, unnötige Risiken zu vermeiden.

Seminar

Grundlagen IT-Providermanagement – Steuerung externer IT-Provider in der Betriebsphase

Themen:

- **Einführung IT-Providermanagement**
- **Rahmen und Einbindung**
- **Steuerung des Providers im Betrieb**

Termin: 26.02.-27.02.2018 in Hamburg

Kooperation, Kommunikation und Kollaboration

Sowohl in der Entwicklungs- als auch in der Betriebsphase ist eine intensive Zusammenarbeit zwischen Entwicklungs- und Betriebseinheiten erforderlich – in diesem Zusammenhang fällt oftmals der Begriff „DevOps“, der genau diese Kollaboration bezeichnet. Um dies zu erreichen, ist eine gemeinsame Kultur der „Kooperation in der steten Veränderung“ zu schaffen.

Damit die sich ständig ändernde IT-Servicelandschaft stets in angemessener Qualität betrieben werden kann, sind angemessene Mechanismen zum regelmäßigen Austausch aller Beteiligten (so beispielsweise Gremien und Kollaborationsplattformen) inklusive Regeln für deren Einsatz zu definieren. Zudem sind verschiedene Prozesse, wie etwa das Serviceportfolio- und Servicekatalog Management, das Knowledge und Reporting / Performance Management sowie einzelne Informationsrunden und Schulungskonzepte darauf auszurichten, alle Stakeholder auf einem aktuellen Stand zu halten.

Schließlich gilt es noch, Mechanismen zu etablieren, um die Kunden laufend über die erfolgten Serviceänderungen zu informieren und ihnen Feedbackmöglichkeiten anzubieten. Über diese Rückkopplung lässt sich sicherstellen, dass die Entwicklung in die gewünschte Richtung geht.

Plakat: IT-Providermanagement

Abgeleitete Anforderungen an das Providermanagement

Aus den oben genannten Auswirkungen auf das IT Service Management lassen sich verschiedene Anforderungen an das Providermanagement ableiten:

Verträge für technische Services (dies sind in der Regel Infrastrukturservices wie Server, Storage, Netz) mit externen Providern müssen so gestaltet sein, dass dynamisch sowohl die Leistung als auch die Mengengerüste verändert werden können.

Die klar definierten Changes (Major Changes, vorautorisierte Standard Changes) sowie der definierte Ablauf des Change Prozesses selbst müssen auch mit den betreffenden Providern vereinbart sein. Für die korrekte Handhabung der Changes gemäß ihrer Kategorie Lösungen zu finden, ist insbesondere bei Providern von hochstandardisierten Public-Cloud-Services eine Herausforderung, da diese individuelle Prozessanpassungen für Kunden naturgemäß vermeiden wollen.

Ebenso ist es unerlässlich, dass die Provider in dem Change Prozess – wie in allen weiteren übergreifenden Prozessen des Service Management – einheitlich und gut integriert sind.

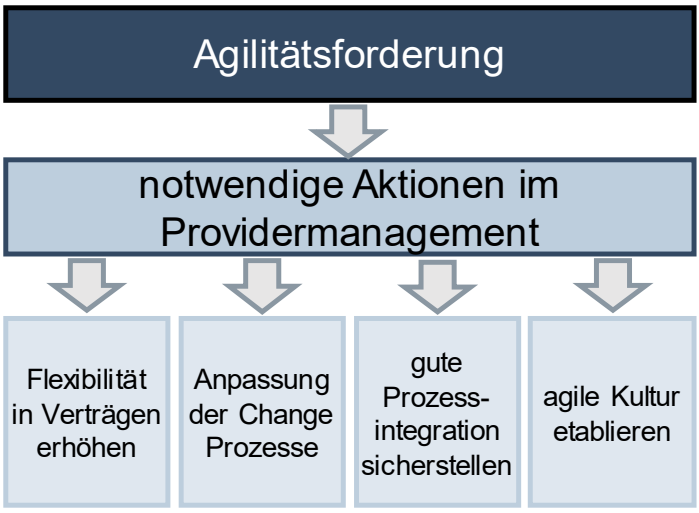

Abbildung 2: Maßnahmen im Providermanagement

Die gemeinsame Kultur der „Kooperation in der steten Veränderung“ ist auch im Providermanagement zu etablieren und sollte in der IT-Governance des Unternehmens verankert sein. Die Providermanager dehnen sie auf die Provider aus und entwickeln sie im Rahmen des Beziehungsmanagements weiter.

Die Provider sind ebenfalls in die oben beschriebenen Mechanismen zum regelmäßigen Austausch und in die Kunden-Interaktion einzubinden.

Was ist nun zu ändern?

Wenn die Organisation sich IT-Service-Management-seitig schon sehr gut aufgestellt hat, sind die soeben genannten Anforderungen in der Regel schon etabliert und durch stete Optimierung über die Jahre sehr effizient ausgestaltet worden. In diesem Fall, hat der Providermanager üblicherweise auch die Integration der Provider in diese Mechanismen schon vorangetrieben. Ist dies gegeben, so ist der schon eingeschlagene evolutionäre Weg weiter zu gehen, d.h. Kultur und Mechanismen sind stets weiterzuentwickeln und neuen Rahmenbedingungen anzupassen. Wesentliche und herausforderndste Aufgabe ist hierbei die aktive Weiterentwicklung der eigenen Kultur in Richtung Agilität.

Ist der Reifegrad der eigenen Organisation jedoch noch nicht so hoch, so ist zunächst seitens des IT Service Managements die Basis zu schaffen, um dann – oder parallel dazu – die Zusammenarbeit mit den Providern nahtlos in die interne IT-Bereitstellung zu integrieren und eine agile Kultur zu fördern.

Jörg Bujotzek

Modernisierung des IT-Grundschutzes

Die in den vergangenen Jahren stark gestiegene Anzahl erfolgreicher Cyber-Attacken zeigt: Viele Unternehmen haben Schwierigkeiten bei der Entwicklung und Umsetzung ihrer IT-Sicherheitsstrategie. Der IT-Grundschutz bietet zwar seit vielen Jahren bewährte Leitlinien für die IT-Sicherheit, er konnte jedoch durch die rasante Entwicklung der Angriffsszenarien in der Vergangenheit nicht in gleicher Taktung aktualisiert werden. Daher hat das BSI jetzt eine modernisierte Version des IT-Grundschutzes veröffentlicht. Doch wie sehen die Änderungen aus und können die neuen BSI-Standards den Unternehmen bei ihren Problemen helfen?

Jedes zweite Unternehmen in Deutschland ist innerhalb der letzten zwei Jahre Opfer von Cyber-Angriffen geworden, so eine aktuelle Studie des Digitalverbandes Bitkom. Dies zeigt deutlich, dass es auf dem Gebiet der Cyber-Sicherheit in Deutschland noch Nachholbedarf gibt. Zwar sind viele große Konzerne und insbesondere die Betreiber kritischer Infrastrukturen gut aufgestellt, viele kleine und mittlere Unternehmen (KMUs) aber scheinen die Bedrohungen nicht ernst genug zu nehmen.

Um gerade die KMUs bei der Lösung dieser Probleme zu unterstützen, wurde in den vergangenen Jahren der 1994, zunächst für Behörden bzw. öffentliche Einrichtungen eingeführte, IT-Grundschutz des BSI modernisiert. Außerdem wurde er um viele in den letzten Jahren entstandene Themen, wie Virtualisierung, Cloud oder Internet-of-Things, ergänzt. Der überarbeitete, sowie in der Strukturierung optimierte, IT-Grundschutz besteht jetzt aus

- einem **IT-Grundschutz-Kompendium**, das die IT-Grundschutzkataloge ersetzt,
- die neuen **BSI-Standards 200-1, 200-2 und 200-3** als Ersatz für die bisherige 100-x-Reihe sowie
- einem **„Leitfaden zur Basisabsicherung“**.

Feedback

Ihre Meinung zählt!

Sie haben Fragen, Anregungen oder möchten eingehender informiert werden?

Treten Sie mit uns in Verbindung. Wir freuen uns auf Sie!

info@amendos.de

Seminare 1. Halbjahr 2018

PM	**IT-Projekte erfolgreich aus der Krise führen** Hamburg, 25.01.-26.01.2018 **Project Management Offices im IT-Umfeld** Hamburg, 04.06.-05.06.2018 **Kommunikationskompetenz in Projektkrisen** Hamburg, 04.06.-05.06.2018 **Soft Skills für Projektleiter/innen** Hamburg, 06.06.-07.06.2018
ITSM	**Einführung in die Prozessoptimierung** Hamburg, 16.04.-17.04.2018 **Prozessdokumentation gestalten** Hamburg, 18.04.2018 **IT Service Management und Agilität** Hamburg, 18.06.2018 **Erstellung von IT-Servicekatalogen** Hamburg, 19.06.2018
Outsourcing	**Grundlagen IT-Providermanagement** Hamburg, 26.02.-27.02.2018 Hamburg, 07.06.-08.06.2018 **IT-Providerwechsel** Hamburg, 28.02.2018 **IT-Providermanagement – live im Betrieb** Hamburg, 01.03.-02.03.2018 **Öffentliche IT-Ausschreibungen** Hamburg, 19.04.-20.04.2018 **IT-Outsourcing** Hamburg, 23.04.-24.04.2018

www.amendos.de/seminare

Das **IT-Grundschutz-Kompendium** umfasst den Inhalt der früheren Grundschutz-Kataloge in einer verschlankten und klarer gegliederten Form. Neben einer grundlegenden Einführung in die IT-Grundschutz-Methodik beinhaltet es 80 modernisierte Prozess- und System-Bausteine, die Unternehmen bei der Modellierung einer sicheren IT-Infrastruktur helfen sollen. Innerhalb eines solchen Bausteins werden beispielsweise im Betrieb Verantwortliche, spezielle Gefährdungslagen sowie Anforderungen genannt, die dem jeweiligen Schutzbedarf (Basis, Standard, erhöht) des umsetzenden Unternehmens entsprechen. Separate Hinweise zur Umsetzung sowie Referenzen auf weiterführende Informationen erleichtern die Implementierung geeigneter Schutzmaßnahmen.

Der aktualisierte **BSI-Standard 200-1** enthält die allgemeinen Anforderungen an ein Managementsystem für Informationssicherheit (ISMS). Im Vergleich zum 100-1 Standard wurden sowohl generelle Aktualisierungen vorgenommen als auch der Aspekt der kontinuierlichen Informationssicherheitsverbesserung berücksichtigt. Er wurde am neuen BSI-Standard 200-2 zur IT-Grundschutz-Vorgehensweise und an der überarbeiteten ISO 27001:2013 ausgerichtet.

Neu im **BSI-Standard 200-2** sind insbesondere drei Vorgehensweisen bei der Umsetzung des IT-Grundschutzes, die jeweils unabhängig voneinander verwendet werden können:

- Die erste Vorgehensweise, auch Basis-Absicherung genannt, liefert einen Einstieg zur Initiierung eines Managementsystems für Informationssicherheit (ISMS) mit dem Ziel, eine grundlegende Erst-Absicherung über alle relevanten Geschäftsprozesse zu erlangen.
- Mit der zweiten Vorgehensweise, der Kern-Absicherung, können zunächst besonders gefährdete Geschäftsprozesse und Assets vorrangig abgesichert werden.
- Die Standard-Absicherung als dritte Vorgehensweise entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise, die grundsätzlich angestrebt werden sollte, um alle Bereiche eines Unternehmens angemessen und umfassend zu schützen.

Diese neue Herangehensweise soll insbesondere Verantwortlichen in kleinen und mittelständischen Betrieben den Einstieg in die Thematik vereinfachen.

Der **BSI-Standard 200-3** behandelt das Risikomanagement und bündelt erstmals alle risikobezogenen (relevanten) Arbeitsschritte bei der Umsetzung des IT-Grundschutzes. Damit soll der Aufwand für Anwender reduziert werden, wenn diese bereits mit IT-Grundschutz

arbeiten und eine Risikoanalyse an die IT-Grundschutz-Analyse anschließen möchten. Die Risikoanalyse aus dem bisherigen BSI-Standard 100-3 wurde in ein vereinfachtes Gefährdungsmodell überführt.

Der BSI-Standard 100-4 zeigt einen systematischen Weg auf, um in einem Unternehmen ein Notfallmanagement aufzubauen, welches die Kontinuität des Geschäftsbetriebs sicherstellt. Er wurde im Rahmen der Modernisierung nicht betrachtet und behält seine normale Gültigkeit sowie die 100er Bezeichnung.

Der komplett neue „Leitfaden zur Basisabsicherung“ richtet sich speziell an kleine und mittlere Unternehmen sowie kleinere Behörden, die sich erstmals mit dem Thema IT-Sicherheit auseinandersetzen. Er erläutert, unter Anwendung der Basis-Absicherung aus dem BSI-Standard 200-2, schematisch den Prozess zur Etablierung eines ISMS und beschreibt auf nur 44 Seiten (anstatt mehr als 150) die drei grundlegenden Schritte zur Umsetzung erster Sicherheitsmaßnahmen (siehe Abbildung 1).

Alle Dokumente stehen auf den Seiten des BSI zum Download zur Verfügung.

1. Initiierung des Sicherheitsprozesses
- der Informationssicherheitsbeauftragte übernimmt als zentrale Rolle die Verantwortung
- Geltungsbereich: der Informationsverbund
- Sicherheitsziele festlegen und Leitlinie erstellen

2. Organisation des Sicherheitsprozesses
- Aufbau einer Organisation zur Informationssicherheit
- Integration in bestehende Abläufe und Prozesse
- Konzeption und Planung des Sicherheitsprozesses

3. Durchführung des Sicherheitsprozesses
- Auswahl und Priorisierung der Bausteine (Modellierung)
- IT-Grundschutz-Check
- Umsetzung der Sicherheitskonzeption

Abbildung 1: drei grundlegende Schritte zur Informationssicherheit

Fazit

Gerade kleine und mittlere Unternehmen werden durch die neuen BSI-Standards dabei unterstützt, das oft komplexe und vielschichtige IT-Sicherheitsmanagement in ihrem Unternehmen einzuführen. Beginnend mit der oben ge-

nannten Kern-Absicherung bei größeren IT-Infrastrukturen oder mit der Basis-Absicherung kann die IT-Sicherheit jetzt modular aufgebaut werden.

Bei der Auswahl, welche Bereiche zuerst im IT-Sicherheitsmanagement abgebildet und mit den dem Schutzbedarf entsprechenden IT-Sicherheitsmaßnahmen abgesichert werden sollen, empfiehlt sich eine Risikoanalyse.

Risikobasierte und modulare Vorgehensweisen führen zwar weiterhin zwangsläufig dazu, dass man sich als Unternehmen auf bestimmte Bereiche der IT konzentriert und andere zurückstellt. Was auf den ersten Blick jedoch wie eine lückenhafte Absicherung aussieht, erweist sich stattdessen aber als ein praxisorientierter Weg, der sich an der Realität in kleinen und mittleren Unternehmen ausrichtet.

Es ist immer besser, mit einigen Bereichen der IT anzufangen und diese sicherer zu machen, als vor der Komplexität einer Sicherheitskonzeption für die gesamte IT zu kapitulieren.

Michael Pfitzmann

Impressum:
amendos gmbh I Frankenstraße 3 I 20097 Hamburg I Tel (040) 248 276 00
Fax (040) 248 276 01 I www.amendos.de I info@amendos.de
Geschäftsführer: Dipl. Oec. Jörg Bujotzek
Handelsregister: AG Hamburg HRB 105648 I Umsatzsteueridentifikationsnummer: DE 814989917
Erscheinungsweise: 4 / jährlich I Bezug: kostenfrei als PDF