ITIL - IT Infrastructure Library

Zwischenfälle dank klarer Verantwortlichkeiten meistern

Im letzten Beitrag haben wir uns dem ISO Standard 27001 gewidmet, nun folgt die IT Infrastructure Library, kurz ITIL. Es handelt sich hierbei um eine Sammlung von Good Practices, die in einer Reihe von Publikationen eine mögliche Umsetzung eines IT Service Managements (ITSM) beschreibt und inzwischen als Defacto-Standard für Gestaltung, Implementierung sowie Management wesentlicher Steuerungsprozesse in der IT gilt.

Autor: Andreas Wisler

ITIL wurde von der Central Computing and Telecommunications Agency (CCTA), heute Office of Government Commerce (OGC), einer Regierungsbehörde in Grossbritannien, seit 1989 entwickelt. Als Version 1 wurden zwischen 1992 und 1998 insgesamt 34 verschiedene Dokumente veröffentlicht. 2001 wurde die Publikationen der Version 2 herausgegeben und am 1. Juni 2007 folgte die aktualisierte Version 3. Die Inhalte der ITIL V3 beschreiben in mehreren Büchern die verschiedenen Themenbereiche des Lebenszyklus von Serviceleistungen.

Das Ziel von ITIL besteht im Wesentlichen darin, die bislang technologiezentrierte IT-Organisation prozess-, service- und kundenorientiert auszurichten. Damit sind die ITIL-Empfehlungen eine entscheidende Grundlage für zuverlässige, sichere und wirtschaftliche IT-Services aus Sicht eines IT-Dienstleisters.

Das gesammelte ITIL-Wissen ist öffentlich uneingeschränkt zugänglich. Es ist in einer Bibliothek von circa 40 englischsprachigen Publikationen verfügbar:

- IT Service Provision and IT Infrastructure Management Sets
- Manager's Set (inkl. ITIL Security Management)
- Software Support Set
- Computer Operations Set
- Environmental Set
- Business Perspective Set

Die Sicherheitsanforderungen für die IT-Services werden auf Grundlage der Geschäftsprozesse und -anforderungen definiert. Abbildung 1 zeigt, welche Prozesse dabei im Vordergrund stehen.
Mit dem IT-Dienstleister werden die Anforderungen in Service Level Agreement (SLA) aufgenommen, abgestimmt, umgesetzt, evaluiert und dokumentiert. ITIL hat selber aber keine eigenen IT-Sicherheitsmassnahmen definiert. Dafür müssen andere Standards, wie das bereits erwähnte ISO 27001 herangezogen werden.

Incident / Problem Management

In vielen Betrieben, vor allem auch in kleineren Firmen, wird nicht das gesamte Framework umgesetzt, sondern nur Teile davon. Die zwei wichtigsten sind dabei sicherlich das Incident und das Problem Management. Aus diesem Grund wird hier kurz auf diese beiden Prozesse eingegangen.

Das Incident Management umfasst die gesamtheitliche Verwaltung aller Störungen. Als erstes wird beim Auftreten einer Störung eine Klassifizierung vorgenommen. Aus der Klassifizierung sollte ersichtlich sein, welche Sicherheitsziele verfolgt werden. Als Faktoren werden die Schadensauswirkung und die Dringlichkeit, also die zugeordnete Priorität, berücksichtigt. Die Analyse der Störung beginnt mit der Prüfung, ob es sich um eine bereits bekannte Störung handelt. Hier helfen sicherlich so genannte Trouble Ticket Systeme weiter. Falls es sich um ein bekanntes Problem handelt, wird ein zuvor definierter Lösungsweg eingeschlagen. Ist kein Weg bekannt und auch keine schnelle Lösung ersichtlich, wird die Störung zum Support-Team eskaliert (in der Regel First Level Support genannt). Das Incident Management gibt zwar die Störung weiter, muss jedoch den Fall bis zur Erledigung weiterverfolgen. Nicht immer kann das Problem auch durch den First Level Support gelöst werden, sondern muss an weitere Stellen weitergeleitet werden. So können auch

Zum Autor

Andreas Wisler, (Tel.: 052 320 91 20), Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. System Hardening rundet das Profil ab. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (INFONEWS) heruntergeladen werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.

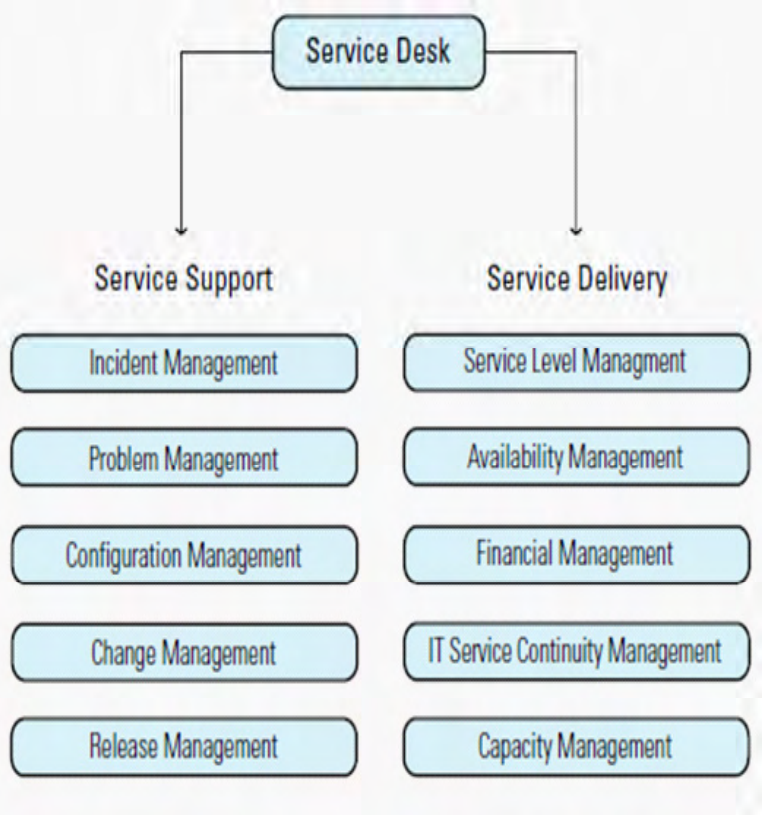

Abbildung 1: Sicherheitsanforderungen für die IT-Services auf Grundlage der Geschäftsprozesse und –anforderungen

Programmänderungen notwendig sein, was Zeit benötigt. Wichtig ist, dass die Nachvollziehbarkeit der Störung sowie der aktuelle Status gewährleistet sind. Daher muss die Störung mit folgenden Punkten dokumentiert werden:

- Eindeutige Störungsnummer
- Wann ist die Störung aufgetreten?
- Wo ist die Störung aufgetreten?
- Wer hat die Störung gemeldet?
- Eine Störungsbezeichnung (Schlagwort)
- Genaue Beschreibung der Störung
- Entstandener Schaden (dies darf auch geschätzt werden)
- Priorität
- Lösung

Das Problem Management beginnt dort, wo das Incident Management aufhört. Durch das Incident Management werden die Gründe für eine Störung nicht analysiert. Die Aufgabe des Problem Managements ist es nun, die Ursache(n) für die bereits aufgetretene Störung zu untersuchen und proaktiv Massnahmen zu treffen, damit diese Art von Störung nicht mehr auftreten kann. Häufig löst dies einen Änderungsantrag an das Change Management aus (ein sogenannter Request for Change).

Somit kann gesagt werden, dass beim Incident Management die Schnelligkeit der Lösung wichtig ist, während das Problem Management eine nachhaltige Identifizierung und Ausschaltung der Ursache darstellt.

Informationssicherheit als zyklischer Prozess

Im vorangehenden Artikel wurde bereits auf den PDCA-Zyklus hingewiesen. Dieses Ziel wird natürlich auch mit ITIL verfolgt. ITIL gliedert dabei die Informationssicherheit in die vier Bereiche: Richtlinien (Gesamtziele einer Organisation), Prozesse (Wie erreicht sie diese Ziele?), Vorgehensweise (Wer macht was und wann, um die Ziele zu erreichen?) sowie Arbeitsanweisungen für konkrete Aktionen. Hier die idealtypischen sieben Schritte innerhalb dieses Prozesses:

1. Über eine Analyse der Risiken (beispielsweise Softwarefehler, Betriebsfehler, Kommunikation unterbrochen, Wahrscheinlichkeit des Auftretens, potenzieller Einfluss auf Business, vergangene Erfahrungen) identifizieren die IT-Kunden ihre Sicherheitsanforderungen.
2. Die IT-Abteilung prüft die Machbarkeit dieser Anforderungen und vergleicht sie mit den in der Organisation festgesetzten Minimalrichtlinien für Informationssicherheit.
3. Der Kunde und die IT-Abteilung verhandeln und erarbeiten ein Service Level Agreement (SLA), das die Anforderungen an Informationssicherheit in messbaren Grössen definiert und genau festlegt, wie diese überprüfbar erreicht werden sollen.
4. Die IT-Organisation definiert Operational Level Agreements (OLA), die detailliert beschreiben, wie sie die Services für Informationssicherheit bereitstellt.
5. Die SLA und OLAs werden implementiert und überwacht.
6. Die Kunden erhalten regelmässig Berichte über die Effektivität und den aktuellen Status der Services, welche die Informationssicherheit garantieren sollen.
7. Die SLA and OLAs werden überarbeitet, falls es notwendig sein sollte.

Fazit

ITIL ermöglicht es Firmen die vorhandenen IT-Prozesse auf Grundlage von Best Practices strukturiert zu entwickeln und zu implementieren. Da ITIL Rollen und Verantwortlichkeiten für die verschiedenen involvierten Stellen klar definiert, steht auch während eines Zwischenfalls sofort fest, wer zuständig ist. Die Unterteilung zwischen Incident und Problem Management garantiert zudem, dass eine Störung schnell behoben und anschliessend auch analysiert wird. Eine «Pflästerli»-Politik wird damit klar verhindert.

ITIL etabliert dokumentierte Standards und Prozesse, die sich überwachen lassen, und fordert regelmässig Berichte über den aktuellen Stand. Daher ist die Firmenleitung jederzeit über die Effizienz der Prozesse informiert und kann auf fundierte Tatsachen ihre Entscheidungen treffen. Da ITIL, wie auch die anderen ISMS Richtlinien, eine ständige Überprüfung erfordert, sorgt es dafür, dass getroffene Massnahmen hinterfragt, verändert respektive verbessert oder neue Massnahmen dazu kommen, und sich somit veränderte Anforderungen oder Bedrohungen schnell integrieren lassen. ◆