

# Sicherheit im IT-Projektmanagement

Wolfgang Sidler

**Zu oft wird zu spät erkannt, dass sicherheitsrelevante Aspekte (z. B. Datenschutzgesetz, Verschlüsselung, Disaster Recovery etc.) nicht berücksichtigt worden sind und dann das Projekt verteuern und die Einführung verzögern.**

Projekte sind als innovative, einmalige und befristete Vorhaben definiert. Sie sind aber auch Chancen, mit begeisterten Mitarbeitern Neues anzupacken, echte Aufbauarbeit zu leisten und die Zukunft gemeinsam zu gestalten. Projektteams mit der richtigen Eigenmotivation setzen normalerweise ungeahnte Energien frei. Gut geführte Projekte erzeugen zudem Faszination und Ausstrahlung über das Unternehmen hinaus.

Die Anwender möchten möglichst rasch eine Lösung, die ihre sämtlichen Bedürfnisse abdeckt. Da sie das Projekt in Auftrag geben, ist es für sie selbstverständlich, dass der Anbieter bzw. der Projektleiter alles dafür nötige dazu beiträgt. Die Anbieter möchten ihre Lösungen unbedingt verkaufen und mit dem Kunden ins Geschäft kommen. Das Management jedoch sieht im Einsatz einer neuen IT-Lösung Möglichkeiten zur Produktionssteigerung, Prozessoptimierung, Unterstützung der Geschäftsprozesse und das Integrieren neuer Geschäftsideen.

Im Projektmanagement eines Software-Projektes oder generell eines IT-Projektes ist es sehr wichtig, dass ein definiertes

Vorgehensmodell (Phasenmodell) verwendet wird. In der Regel ist eine reine Projektorganisation der Matrix-Projektorganisation vorzuziehen. Die Mitarbeiter werden aus ihren angestammten Arbeitsstellen herausgelöst und zu einer neuen, zeitlich begrenzt bestehenden Organisationseinheit zusammengefasst. In dieser Organisationsform hat der Projektleiter vergleichsweise grössere Kompetenzen und Verantwortungen.

Für jeden Projekttyp wird ein angepasstes Vorgehen verwendet, basierend auf dem Standardmodell. Das entsprechend angepasste Vorgehen wird in der Vorstudie festgelegt. Dabei werden auch spezielle Projektsituationen (IT-Sicherheit, Gesetze, Terminvorgaben, Ressourcen etc.) mit einbezogen. Die Entscheidungswege sind der Projektgrösse anzupassen.

Häufig sind die Projektleiter mit den sicherheitsrelevanten Bedürfnissen wenig vertraut. Daher sollte man sicherstellen, dass bei allen im Unternehmen entwickelten und/oder eingekauften und integrierten Applikationen, Lösungen und Systemen eine phasenweise Begleitung durch einen IT-Sicherheits-Beauftragten

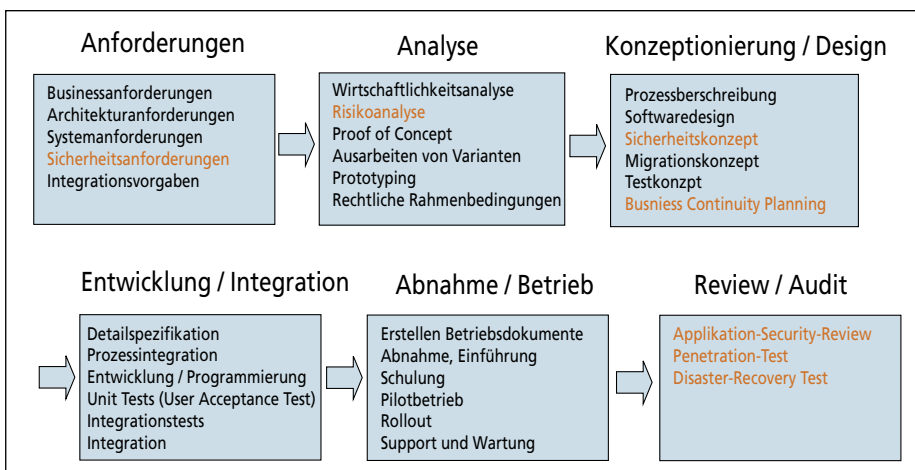
erfolgt. Somit können alle sicherheitsrelevanten Bereiche in enger Zusammenarbeit mit dem Projektteam rechtzeitig und proaktiv identifiziert und anforderungsgerechte Kontrollmassnahmen vorgeschlagen werden. Für die Betriebsaufnahme von Applikationen, die ohne oder nur mit marginaler interner Begleitung entwickelt worden sind, ist als zwingende Voraussetzung für die Betriebsaufnahme die Erstellung eines IT-Security-Konzepts bzw. eine Stellungnahme des IT-Sicherheits-Beauftragten erforderlich.

## Projektmanagement

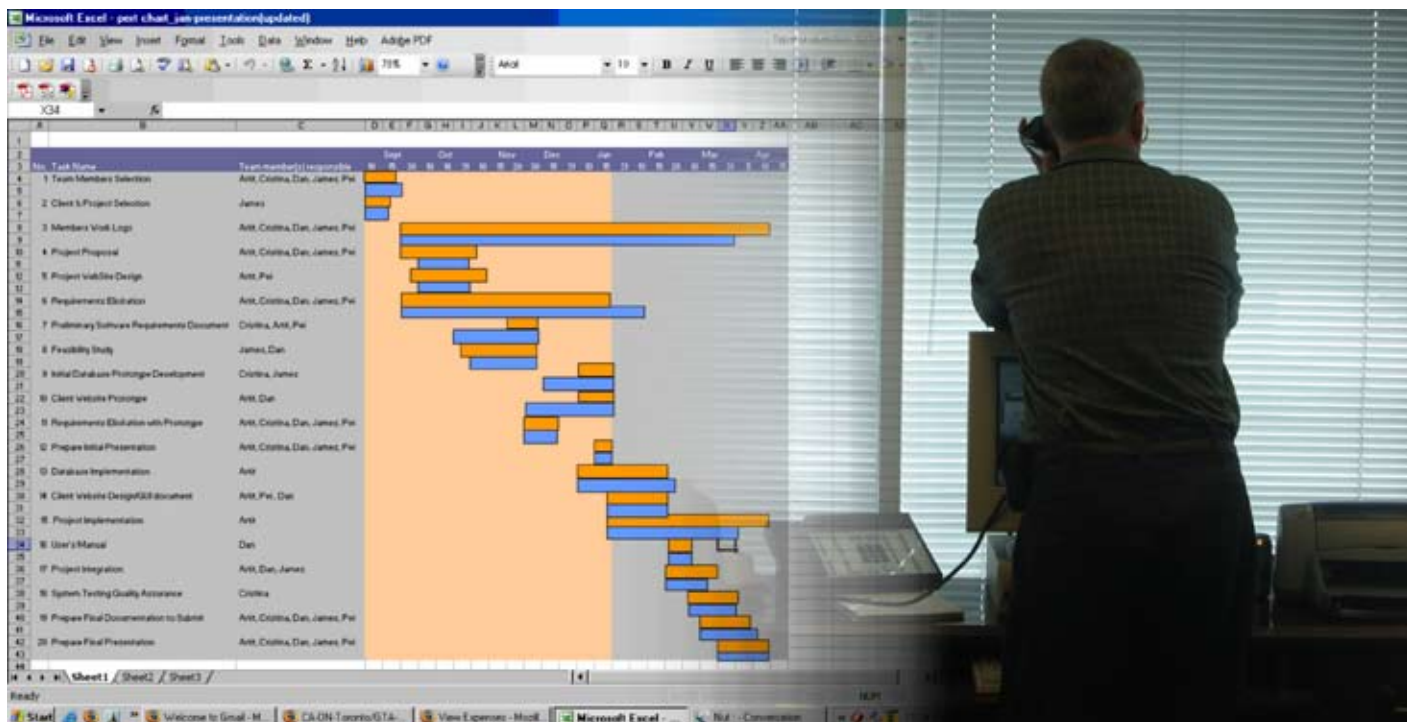
Projektmanagement ist ein systematischer Prozess zur Führung komplexer Vorhaben. Es umfasst die Organisation, Planung, Steuerung und Überwachung aller Aufgaben und Ressourcen, die notwendig sind, um die Projektziele zu erreichen. Projektmanagement ist damit eine Führungsaufgabe, die von den Ausführungsaufgaben der operativen Projektarbeit abzugrenzen ist. Ihr Beitrag zum Erfolg eines Projektes ist nicht zu unterschätzen.

### Die 10 Grundfragen des Projektmanagements:

- Ist das Projekt für die anstehende Aufgabe die richtige Organisationsform und Phasen-Modell?
- Sind die Projektziele eindeutig?
- Gibt es einen klaren Projektauftrag?
- Hat die Geschäftsleitung bzw. der Sponsor die Projektziele und Meilensteine gebilligt?
- Verfügt der Projektleiter über die erforderlichen Kompetenzen?
- Welche Mitarbeiter und Ressourcen werden für das Projekt benötigt?
- Liegen mit den Projektbeteiligten abgestimmte Projektpläne vor?



Typisches Standardmodell eines Projekt-Phasenplans.



- Funktioniert die Zusammenarbeit im Projektteam?
- Unterliegt das Projekt einer ständigen Evaluation, Wirtschaftlichkeitsbetrachtung und Steuerung?
- Wird eine angemessene Dokumentation geführt?

## Vertrag

Ein Vertrag zwischen dem Anbieter und dem Kunden sollte die Meinungen der Parteien bezüglich genauem Inhalt des Projekterfolges (Funktionalitäten, Performance, notwendige Hardware und Standardsoftware etc.) den Weg, welchen man zum Projekterfolg gemeinsam beschreitet (wer macht wann was) und wichtige Fragen wie Urheberrechte, Abnahmeprozedere etc. regeln.

## Risikoanalyse

Aufgabe der Risikoanalyse ist es, Faktoren die eine Gefahr für den Projekterfolg (die im Projektauftrag definierte Leistung in geplanter Zeit mit den geplanten Ressourcen im vorgegebenen Budget zu erbringen) darstellen, zu identifizieren, zu bewerten und entsprechende Gegenmassnahmen vorzubereiten bzw. einzuleiten.

### Typische Projektrisiken generell sind:

- Ausfall von wichtigen Mitarbeitern (Key-Personen)

- Nichteinhaltung zugesagter Termine (Lieferanten etc.)
- Fehlende Akzeptanz bei den potenziellen Nutzern
- Fehlendes Know-how
- Schlechte Kommunikation zwischen den Partnern (Erwartungen werden nicht erfüllt)
- Zuwenig Unterstützung durch die Geschäftsleitung (fehlender Sponsor)
- Kulturelle Unterschiede bei internationalen Projekten
- Fehlende Projektkontrolle (Projekt Office)
- Zu optimistische Planung
- Kein Vertrag zwischen Leistungsbezüger und Leistungserbringer
- Verzögerung aufgrund unklarer Definition der Projektrollen (Kompetenzkonflikte)
- Konflikte zwischen Teammitgliedern

### Typische Projektrisiken in Bezug auf die IT-Sicherheit sind:

- Nicht Erfüllen gesetzlicher Anforderungen (Datenschutz, GebäV etc.)
- Nicht Einhalten der internen Weisungen und Standards
- Integration in die bestehende IT-Infrastruktur/-Architektur nicht möglich
- Nicht Erfüllen der Daten-Vertraulichkeit, -Integrität und -Verfügbarkeit
- Fehlende Integration in den Business Continuity Plan

## Umsetzung

Die Projektleitung hat in Zusammenarbeit mit dem IT-Sicherheitsbeauftragten bereits zu Projektbeginn die spezifischen Sicherheitsanforderungen an das zu entwickelnde Schutzobjekt schriftlich zu formulieren. Der IT-Sicherheitsbeauftragte ist umfassend in den projektbezogenen Informationsfluss zu integrieren, insbesondere ist er in das Antrags- und Genehmungsverfahren einzuschalten.

Die Projektleitung ist dafür verantwortlich, dass die Sicherheitsanforderungen in jeder Phase umfassend berücksichtigt werden und deren Umsetzung in nachvollziehbarer Form in den Projektunterlagen dokumentiert wird. Es empfiehlt sich, dass ein IT-Sicherheits-Beauftragter das Projekt während der ganzen Projektzeit begleitet und den Projektleiter in sicherheitsrelevanten Fragen unterstützt. Damit mögliche Mehrkosten, welche für Sicherheits-Massnahmen benötigt werden, nicht negativ auf die Projektkosten wirken, wird empfohlen, zu Beginn jedes IT-Projektes 5% der gesamten Projektkosten für Sicherheits-Massnahmen bereit zu stellen. Der IT-Sicherheits-Beauftragte ist für die abschliessende Kontrolle und Freigabe verantwortlich. ■