Management von Projekten der Informationssicherheit

Auf Kurs

Ronny Frankenstein

Da beim Thema Informationssicherheit in Unternehmen und Behörden häufig das interne Know-how fehlt und das Projekt somit stark von der Qualität externer Experten abhängig ist, sind Projekte in diesem Bereich den üblichen Herausforderungen wie Verzögerungen, Budgetüberschreitungen oder auch eingeschränkten Projektergebnissen in besonderem Maße unterworfen. Wie kann man solche Projekte dennoch zum Erfolg führen?

Projekte in der Informationssicherheit benötigen spezielle Kompetenzen, die in der Regel nur durch das Einbinden externer Experten zur Verfügung stehen. Dies führt dazu, dass einerseits Unternehmen und Behörden intern fachliches Neuland betreten und nicht auf ausreichende Erfahrung und spezielles Know-how zurückgreifen können. Die betreffende Organisation muss es während des Projektes erst „erlernen".

Andererseits müssen die externen Berater die Organisationen während des Projektverlaufes oft erst kennenlernen, um in deren Kontext der Risikobereitschaft und der internen Kultur die Informationssicherheit oder das Informationsmanagementsystem (ISMS) zu implementieren. Die Projektziele lassen sich normalerweise nicht durch einfaches „Vorlesen" oder blindes Anwenden eines Sicherheitsstandards oder -frameworks erreichen.

Oft wünschen die Verantwortlichen im Unternehmen, dass effektive und effiziente Informationssicherheit etabliert oder ein nach dem Projekt weiter funktionierendes, also an die Organisation angepasstes ISMS aufgebaut wird. Sinnvoll kann es außerdem sein, eine Zertifizierung nach einem Standard wie BSI IT-Grundschutz oder ISO 27001 zu erreichen.

Die unterschätzte Partnersuche

Der Autor schätzt, dass Security-Projekte zwei bis drei Mal durchgeführt werden müssen, bis die eigentlich mit dem Projekt verbundene Erwartungshaltung erfüllt ist. Einige Aspekte, die zum sofortigen Erfolg eines Security-Projekts beitragen, sind nachfolgend geschildert.

iX-TRACT

- Security-Projekte sind den „klassischen" Schwierigkeiten des Projektmanagements in besonderem Maße unterworfen, da in Unternehmen und Behörden oft internes Fachwissen fehlt.
- Häufig greifen Unternehmen auf externe Spezialisten zurück, um Informationssicherheit im Betrieb einzuführen. Der Auswahl des „richtigen" Partners kommt eine besondere Bedeutung zu – Checklisten können hier helfen.
- Eine konstruktive Zusammenarbeit zwischen externen und internen Mitarbeitern, die auch kritische Diskussionen und einen adäquaten Umgang mit Fehlern beinhaltet, hilft dabei, die typischen Projekthürden zu meistern und das Geplante erfolgreich umzusetzen.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover

Projekte sind auf eine begrenzte, oft kurze Dauer ausgerichtet. Daher investieren Unternehmen und Behörden ebenfalls nur wenig Zeit und Aufmerksamkeit in die Projektpartnersuche. Wenn jedoch absehbar ist, dass in kurzer Zeit sowohl seitens der eigenen Organisation das Thema Informationssicherheit erlernt werden als auch mehr als ein Nullachtfünfzehn-Niveau des zugrundeliegenden Sicherheitsstandards im eigenen Hause ankommen soll, ist es sinnvoll, die Suche nicht auf den reinen Beschaffungs- oder Einkaufsvorgang zu beschränken.

Im Gegenteil, es zeugt von einer gewissen Weitsicht und ist eine Herausforderung, die zuständige Einkaufs- und Beschaffungsabteilung genau zu instruieren, was benötigt wird und in welcher Qualität. Die Abteilung hat im Regelfall nur ein Ziel, und das verfolgt sie gelegentlich gnadenlos und ohne gesunden Menschenverstand: Hauptsache billig! Das soll keine Kritik an denjenigen sein, die in solchen Abteilungen arbeiten. Vielmehr liegt der Fehler beim Einkaufsprozess der Organisationen.

Beschaffungsparadoxon

Die zuständigen Abteilungen oder Bereiche sind sehr wohl in der Lage, weitere Parameter bei der Auswahl der Partner zu berücksichtigen, und haben sich beim Autor sogar schon einige Male dafür entschuldigt, dass sie vermutlich falsch beschaffen müssen, aber keine anderen Instruktionen bekommen haben. Die Ursache dafür ist ein Paradoxon: Es muss ja etwas Artfremdes beschafft werden, wie sollen da der zuständigen Fachabteilung oder der Stabsstelle die richtigen Parameter bekannt sein? Mit etwas Mühe gibt es im Internet bereits nach kurzer Suche eine Reihe von Hinweisen.

Beim BSI sind in den IT-Grundschutz-Maßnahmen zur Vertragsgestaltung mit externen Informationssicherheitsbeauftragten (zu finden über „Alle Links“ im blauen Kästchen) einige wichtige Punkte genannt, die sich für den eigenen Fall anpassen lassen. Die Seiten von Beratungshäusern zur Informationssicherheit sind ebenfalls eine gute Quelle, um Parameter für den Vergleich von Anbietern der benötigten Leistung zu ermitteln. Hier sind oft Referenzen, Qualifikationen der Mitarbeiter und eigene Zertifizierungen aufgeführt. Daraus lassen sich schon rund fünf bis sieben Aspekte zusammenstellen (siehe Tabelle „Generische Kriterien …“).

So kann es beispielsweise sinnvoll sein, einen Auditor einzusetzen, der die Zertifizierung zu einer Sicherheitsnorm vorbereitet. Denn nach Projektende ist es ebenfalls ein Auditor, der überprüft, ob das Zertifikat erteilt werden kann. Oder wenn ein Beratungsunternehmen angibt, an gängigen Standards mitzuarbeiten, so wird es wohl auch über Mitarbeiter verfügen, die sich in der betreffenden Thematik auskennen und kompetent beraten können. Deren Mitarbeiterprofile könnten Berücksichtigung finden. Ebenfalls kann das Vertrauen eine Rolle spielen. Projektreferenzen und Zertifizierungen, die ein potenzieller Auftraggeber auch stichprobenartig überprüfen sollte, können bei der Wahl eines zukünftigen Partners eine Rolle spielen.

Erlösung durch den externen Partner?

Zusammenarbeit ist nur möglich, wenn beide Partner bereit sind, ihren Teil zum Projekt beizutragen. Häufiger „fremdelt“ die Organisation mit dem Themengebiet, in das sie sich eigentlich einarbeiten müsste, was einer impliziten Verweigerung der Beschäftigung damit gleichkommt. Das kann verschiedene Ursachen haben. Es kann an der mangelnden Bereitschaft der verantwortlichen Personen liegen, sich auf etwas Neues einzulassen. Oder sie können fachlich oder persönlich etwa für die Stelle des Informationssicherheits-Beauftragten ungeeignet sein.

Oft stehen den Verantwortlichen weder ausreichend Zeit noch Geld zur Verfügung. Dies führt dann entweder zur falschen Beschaffung oder verlängert die Projektlaufzeit unter Umständen erheblich. Die internen Partner nutzen in solchen Fällen häufig das Projekt als Mittel, mit seinem Scheitern eine erhöhte Aufmerksamkeit in der Leitungsebene zu erhalten, selbst wenn sie das nicht bewusst tun. Das Scheitern ist dann natürlich die Schuld der Externen.

Gerangel in den Fachabteilungen

Es gibt auch die Problematik der falschen organisatorischen Einbindung des Themas. Beispielsweise werden Security-Projekte oft aus der IT-Abteilung heraus gestartet. Diese „Revolution von unten“ funktioniert jedoch nur in wenigen Fällen, da das mit organisatorischen und technischen Sicherheitsmaßnahmen abteilungsübergreifend eingeführte Veränderungsmanagement bei anderen, „gleichrangigen“ Fachabteilungen auf Ablehnung stößt. Der erfahrene, externe Partner wird sich an solchen Projekten

Generische Kriterien zur Auswahl von Dienstleistern im Umfeld Beratung zur Informationssicherheit

Leistungsmerkmal	mögliche Angaben als Punkte in die Bewertung aufnehmen
Jahre, die das Unternehmen im Bereich Informationssicherheit am Markt tätig ist	> 10
Zertifiziertes Beratungsunternehmen in den Bereichen der angefragten Beratung	ISO-27001-Zertifizierung, ISO-9001-Zertifizierung, BSI-IT-Grundschutz-Zertifizierung,BSI-Zertifizierungen wie Pentest, IS-Revision[1] und IS-Beratung
Nachweis über Mitarbeit an nationalen und internationalen Standards (Bsp. Grundschutz, ISO27001 etc.)	Bausteine BSI-IT-Grundschutz, BSI-Standards, BSI-Studien, Mitgliedschaft in Normungsgremien …
Referenzen auf dem Gebiet der angefragten Beratungsleistung wie Zertifizierungsvorbereitung	> 10, und 50 % davon als ISO 27001 oder beides) konkrete Adressen zum Nachprüfen
Referenzen in der eigenen Branche	Pluspunkt besonders bei der ISO 27001 nativ
Referenzen in der vergleichbaren Größe (Anz. der Mitarbeiter, Anz. der Standorte)	Pluspunkt besonders bei der ISO 27001 nativ
Verfügt das Unternehmen über Beratungskompetenz sowohl im Bereich der technischen als auch der organisatorischen Informationssicherheit	Pluspunkt, falls sich im Projekt Schwerpunkte in die eine oder andere Richtung ergeben (agil)
Bei Zertifizierungsprojekten wie Vorbereitung oder Audit: Anzahl Mitarbeiter die ein Zertifikat als ISO-27001-Auditoren für Audits auf der Basis von BSI-IT-Grundschutz oder ISO 27001 nativ vorweisen können	Projektleiter plus 2 Personen als Reserve
Anzahl Mitarbeiter die eine Zertifizierung als Projektleiter (PMI, IPMA/GPM, PRINCE2) vorweisen können	> 3, sonst fehlt hier die generelle Projektleitungserfahrung

[1] IS – Informationssicherheit

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover

Weder klassisch noch agil: Sonderfall Security-Projekte

Security-Projekte lassen sich in keines der typischen Zieldreiecke des klassischen und des agilen Projektmanagements einordnen (obere Dreiecke). Zwar kommen beide Wesensarten bei ihnen vor, sind aber völlig anders parametrisiert.

Es gibt entweder klassische Umsetzungen, die dann aber komplett auf ein erstarrtes Ergebnis ausgelegt sind und in der Regel keinen Spielraum haben (Dreieck unten links). Oder die völlig losgelöste, offene Durchführung in der alle Parameter veränderlich sein können (Dreieck unten rechts). In dieser kompletten Agilität bewältigen die Organisationen zusammen mit den externen Partnern dann den Lerneffekt.

voraussichtlich nicht beteiligen, da er keinen erfolgreichen Verlauf erwarten kann.

Ein neuer Trend, der den Projektleitern zurzeit Schwierigkeiten bereitet, ist die ingenieurtechnische Betrachtung des Themas Informationssicherheit in der Industrie. Dort begreift man Informationssicherheit nicht als organisatorischen Veränderungsprozess, sondern als „Bauteil“, das sich nach Lieferung durch den Externen nahtlos in das „Getriebe“ des Unternehmens einpassen lassen soll. Da das Ingenieursprinzip hier nicht anwendbar und eine Lernphase vorzuschalten ist, verlängert sich daraus häufig das Projekt.

Insbesondere, wenn man Informationssicherheit zum ersten Mal in einem Projekt umsetzen will oder einen neuen Partner dafür verpflichtet, ist eine Erhebung des aktuellen IST-Zustandes in Form einer sogenannten GAP-Analyse oder Reifegradbestimmung empfehlenswert. Dieses Vorgehen bietet beiden Seiten eine Möglichkeit, die gegenseitige Kennenlernphase stark zu verkürzen, was der Qualität und Laufzeit des Projekts zugutekommt.

Security-Know-how erwerben

Wie eingangs geschildert muss die Organisation das bisher fehlende Security Know-how neu „erwerben“. Dazu ist es zielführend, sich die der Bewertung des IST-Zustands zugrundeliegende Methode des Partners erklären zu lassen. Danach ist es zumindest teilweise möglich, eine solche Bewertung auch intern durchzuführen oder bei zukünftigen Bewertungen den Einsatz des externen Know-hows zu begrenzen.

Auf der anderen Seite bietet sich dem externen Partner die Chance, die Behörde oder das Unternehmen besser kennenzulernen. Durch die in der Regel mit einem hohen Interview-Anteil durchgeführte Anfangsanalyse kommt der Externe zwangsläufig mit Personen und damit mit der Kultur der Organisation in Berührung. Da Informationssicherheit auch als Projekt immer wieder die Balance zwischen Risiken und Chancen finden muss, ist die Kenntnis, wie der Kunde „tickt“ ein entscheidender Parameter für die spätere Abwägung beider Anteile.

Klassisch oder agil – (k)eine schwierige Entscheidung

Ebenso erhalten Externe dadurch einen Einblick in das vorhandene Know-how der Organisation. In der Regel wird der Projektleiter danach die notwendigen Spezialisten in seinem Projektteam noch einmal neu zusammenstellen oder er hat aus Erfahrung ohnehin die konkrete Ausprägung des Teams auf den Zeitpunkt nach dieser Erstphase gelegt. Auch bekommt der externe Partner durch diese ersten Sondierungsgespräche einen Einblick, wie (erfolgreich) bisher Veränderungsmanagement mit den betroffenen Mitarbeitern seitens der Organisation durchgeführt wurde, und kann für dieses Arbeitspaket mehr oder weniger Aufmerksamkeit einplanen.

Bei Security-Projekten gibt es die Besonderheit, dass diese niemals vollständig klassisch, also mit vordefinierten Projektziel ablaufen können (siehe Kasten „Weder klassisch noch agil“). Beide Seiten sollten sich daher grundsätzlich immer wieder darüber abstimmen, welche Projektänderungen das Erreichen des

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover

Ziels beeinflussen. Hier ist ein fairer Umgang miteinander erforderlich, statt sturer Fehlersuche oder Schuldzuweisungen, wie sie hierzulande insbesondere aufgrund der fehlenden deutschen Fehlerkultur verbreitet sind.

Wie erwähnt lernen beide Seiten bewusst voneinander, damit am Ende das passende Projektergebnis herauskommt. Insbesondere bei Erstprojekten hat der Externe hier großen Einfluss. Da das Thema Informationssicherheit ja intern noch völlig neu ist, ist es für die Organisation erforderlich, erst einmal ein Gespür für das notwenige Security-Know-how zu bekommen. Dies enthebt sie aber nicht von der Pflicht, die von außen mitgebrachten Methoden und Verfahrensweisen zu diskutieren, zu hinterfragen und sich erklären zu lassen – es sei denn, beide Seiten sind sich beispielsweise aufgrund einer äußerst kurzen Projektlaufzeit einig, dass hier nur ein geringer Reifegrad im Projekt erreicht werden soll.

Gute Partner liefern brauchbare Lösungen auch bei Zertifizierungen

Gute Partner werden beispielweise auch bei Zertifizierungsprojekten, bei denen die Projektlaufzeit häufig durch den Termin zum Zertifizierungsaudit ein hartes Projektende hat, Lösungen liefern, die eine Einflussnahme durch den Kunden ermöglichen, wenn ein interner, zukünftiger Mehrwert zu erwarten ist. Natürlich ist der Partner gehalten, den Kunden zu stoppen, wenn er die erforderliche Konformität derart verlassen würde, dass ein Zertifikat gefährdet ist. Aber das erwartet der Kunde in der Regel ja auch.

Insofern starten die Projekte oft mit dem klassischen Projektansatz, werden aber zwischendurch immer wieder agil – was für die Projektleiter, die das „Schiff“ auf Kurs halten sollen, eine größere Herausforderung als bei anderen IT-Projekten ist, und von der sie wissen sollten. Aber auch die Organisation sollte die Lernphase einplanen und gegebenenfalls die Änderungen im Projektverlauf mittragen, statt an den vorher im Angebot definierten Arbeitspaketen festzuhalten. Es kommt schließlich ihr selbst zu Gute.

Fazit

Die Suche nach einem externen Partner wird häufig unterschätzt und so kommt das Briefing des Einkaufs in vielen Beschaffungsprozessen zu kurz. Auch können die Partner das Unternehmen oder die Behörde nicht von ihrer Verantwortung für das Thema Informationssicherheit erlösen. Nur Zusammenarbeit und Vertrauen in einem fairen Umgang miteinander führen jedoch zum gewünschten Projekterfolg. Viele Organisationen binden sich nach erfolgreich abgeschlossenen Erstprojekten für lange Zeit an den Partner, denn daraus resultieren in vielen Fällen weitere Optimierungspotenziale. Beim ersten Mal ist eine IST-Bestandsaufnahme für beide Seiten sinnvoll, um einander kennenzulernen. (ur)

Ronny Frankenstein
ist Director bei HiSolutions AG in Berlin und zertifizierter Grundschutzauditor.

Alle Links: www.ix.de/ix1713127

MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover

Redaktion: Telefon: 0511 5352-387, Fax: 0511 5352-361, E-Mail: post@ix.de
Abonnements: Telefon: 0541 80009-120, Fax: 0541 80009-122, E-Mail: leserservice@heise.de

Herausgeber: Christian Heise, Ansgar Heise
Chefredaktion: Jürgen Seeger (js) -386, Stellv.: Oliver Diedrich (odi) -616
Konzeption: Jürgen Diercks (jd) -379, Barbara Lange
Redaktionelle Leitung: Jürgen Diercks (jd) -379,
Redaktion: Ute Roos (ur) -535, Bert Ungerer (un) -368, Dr. Jan Bundesmann (jab) -384, Moritz Förster (fo), Tilman Wittenhorst (tiw) -787, Redaktionsassistenz: Carmen Lehmann (cle) -387, Michael Mentzel (mm) -153
Autoren dieser Ausgabe: Kai Altenfelder, Jean Pierre Berchez, Johannes Bergsmann, Karin Brünnemann, Jürgen Diercks, Lars Dittmann, Richard Brenner, Frank Düsterbeck, Andreas Falk, Lukas Feiler, Ronny Frankenstein, Tam Hanna, Andrea Herrmann, Klaus Hörmann, Jez Humble, Andreas Johannsen, Dirk Jahnke, Siegfried Kaltenecker, Uta Kapp, Axel Keller, Horst Kostal, Anne Kramer, Barbara Lange, Klaus Leopold, Tilo Linz, Christoph Mathis, Markus Müller, Joanne Molesky, Barry O'Reilly, Markus Peter, Fritz-Ulli Pieper, Stefan Roock, Andreas Rüping, Ewa Sadowicz, Michaela Stach, Florian Theißing, Maik Wienströer, Bastian Witte, Henning Wolf, Jörg Zimmer
Layout und Satz: Enrico Eisert, Matthias Timm, Hinstorff Media, Rostock
Korrektorat: Ninett Wagner, Hinstorff Media, Rostock
Fotografie: Martin Klauss Fotografie, Despetal/Barfelde
Titel: Idee: *iX*; Titel- und Aufmachergestaltung: Martin Klauss
Verlag und Anzeigenverwaltung:
Heise Medien GmbH & Co. KG, Postfach 61 04 07, 30604 Hannover;
Karl-Wiechert-Allee 10, 30625 Hannover; Telefon: 0511 5352-395, Fax: 0511 5352-129
Geschäftsführer: Ansgar Heise, Dr. Alfons Schräder
Mitglieder der Geschäftsleitung: Beate Gerold, Jörg Mühle
Verlagsleiter: Dr. Alfons Schräder
Anzeigenleitung: Michael Hanke -167, E-Mail: michael.hanke@heise.de, www.heise.de/mediadaten/ix
Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 28 vom 1. Januar 2017.
Leiter Vertrieb und Marketing: André Lux -299
Werbeleitung: Julia Conrades -156
Druck: Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel
Sonderdruck-Service: Julia Conrades -156
Verantwortlich: Textteil: Jürgen Seeger; Anzeigenteil: Michael Hanke
***iX* erscheint monatlich**
Einzelpreis € 6,90, Österreich € 7,40, Schweiz CHF 10,70, restl. Europa € 8,10, sonst. Länder € 9,30
Das Abonnement für 13 Ausgaben kostet: Inland € 81,90, Österreich € 89,05, Schweiz CHF 128,90, restl. Europa € 96,20, sonst. Länder € 106,60; 13 Digitalausgaben im Abonnement kosten weltweit € 81,90; Studentenabonnement: Inland € 49,40, Österreich € 54,60, Schweiz CHF 90,20, restl. Europa € 59,80, sonst. Länder € 66,30; nur gegen Vorlage der Studienbescheinigung, Luftpost auf Anfrage.
iX Plus-Abonnements (inkl. Online-Zugriff auf das *iX*-Artikel-Archiv und die digitale Ausgabe für Android/iOS) kosten pro Jahr € 13 (Schweiz CHF 16,95) Aufpreis.
Für Mitglieder von AUGE, BvDW e. V., /ch/open, GI, GUUG, JUG Switzerland, Mac e. V., VBIO, VDE und VDI gelten ermäßigte Abonnementpreise (gegen Mitgliedsausweis). Bitte beim Abo-Service nachfragen.
Kundenkonto in der Schweiz: UBS AG, Zürich, Kto.-Nr. 206 P0-465.060.0
Abo-Service: Heise Medien GmbH & Co. KG, Leserservice, Postfach 24 69, 49014 Osnabrück, Telefon: 0541 80009-120, Fax: 0541 80009-122, E-Mail: leserservice@heise.de
Vertrieb Einzelverkauf (auch für Österreich, Luxemburg und Schweiz):
VU Verlagsunion KG, Meßberg 1, 20086 Hamburg, Telefon: 040 3019-1800, Fax: 040 3019145-1800, info@verlagsunion.de, Internet: www.verlagsunion.de
Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Die gewerbliche Nutzung abgedruckter Programme ist nur mit schriftlicher Genehmigung des Herausgebers zulässig.
Printed in Germany © Copyright by Heise Medien GmbH & Co. KG
ISSN 0935-9680

LAC/2011

Die Inserenten

B1 Systems GmbH	www.b1-systems.de	131
bytec	www.bytec.de	132
dpunkt	www.dpunkt.de	9, 43
Hostserver	www.hostserver.de	2
Successfactory	www.originalscrum.com	11
Veränderungskraft	www.veraenderungskraft.de	75

Die hier abgedruckten Seitenzahlen sind nicht verbindlich. Redaktionelle Gründe können Änderungen erforderlich machen.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover