ProjektMagazin
Das Fachportal für Projektmanagement
Ausgabe 05/2016

Fachbeitrag

Risiken erkennen und vermeiden

Informationssicherheit – Wann ist die Projektleitung in der Pflicht?

Wettbewerbsvorteile sichern, technologischen Vorsprung erreichen, Kundenanforderungen optimal bedienen – das sind mögliche Ziele, die durch Projekte erreicht werden können und mit denen Sie sich als Projektmanager sicher gerne identifizieren.

Wie sieht es aber aus, wenn im Projektverlauf technische Zeichnungen eines Lieferanten durch fehlgeleitete E-Mails versehentlich in falsche Hände geraten? Wenn aufgrund des unachtsamen Umgangs Speichermedien nicht mehr auffindbar sind, auf denen Sicherungen einer Kundendatenbank gespeichert waren? Oder wenn bei einem gezielten kriminellen Angriff auf ein Notebook des Projektleiters das Passwort geknackt wurde und darauf gespeicherte Details über eine neue Produktentwicklung gestohlen wurden? Wurden Details einer neu entwickelten Technologie nach außen getragen, können sich die Wettbewerbsvorteile eines Lieferanten, Kunden oder des eigenen Unternehmens in nichts auflösen.

Eine sichere Handhabung aller projektinternen Daten und Informationen sollte daher während des gesamten Projektverlaufs einen Missbrauch oder Diebstahl wichtiger Projektdaten verhindern, um mögliche Schäden für das eigene Unternehmen sowie Projektpartner abzuwenden. In diesem Artikel erfahren Sie, was eine "sichere Handhabung" im Sinne von Informationssicherheit in Bezug auf Unternehmen, Organisationen und Projekte bedeutet und welche rechtlichen Verpflichtungen zum Schutz von Daten Sie als Projektmanager kennen sollten. Um Ihnen bei der Überprüfung der IT-Sicherheit in Ihrem eigenen Projekt eine Hilfestellung zu geben, ist im Artikel ein Projekt-Check aus 20 Fragen zu Sicherheitsthemen eingebaut, der Ihnen auch Lösungsansätze für erkannte Bedrohungen bietet.

Autor

Cornelia Niklas

Betriebswirtin (VWA), langj. Erfahrung als Projektleiterin im IT-Bereich. Arbeitet als freie Fachautorin, Beraterin und Trainerin für Non-Profit-Organisationen und Unternehmen im In- und Ausland.

Kontakt: info@c-niklas.de

Mehr Informationen unter:
› projektmagazin.de/autoren

ähnliche Artikel

in den Rubriken

› Vertragswesen

› Risikomanagement

Definition von "Informationssicherheit" nach dem BSI (Bundesamt für Sicherheit in der Informationstechnik)

Das BSI hat den geläufigen Ausdruck *IT-Sicherheit* inzwischen durch die Bezeichnung *Informationssicherheit* abgelöst. Dieser Begriff drückt eine umfassendere Sicht aus: Infomationssicherheit bezeichnet die Sicherheit *aller* Daten in Unternehmen und Organisationen, die von Wichtigkeit sind und hat zum Ziel, die drei Grundwerte *Verfügbarkeit, Vertraulichkeit* und *Integrität* dieser Daten zu schützen.

Informationssicherheit beinhaltet folglich den Datenschutz (Schutz personenbezogener Daten nach BDSG) ebenso wie den Schutz von Unternehmensdaten, die verarbeitet oder auf Medien gespeichert bzw. übermittelt werden. Fokussiert werden dabei die IT-Infrastrukturen und IT-Systeme, die derartige Daten verwalten. Informationssicherheit betrifft aber auch die Sicherheit von "offline"-Datenträgern (z.B. Bandsicherungen) und umfasst Zugangs- und Zugriffssicherungen und Vorkehrungen für Notfälle.

Warum sind Projekte gefährdet?

Projekte haben oft einen hohen Vernetzungsgrad, verteilte Teams erfordern zudem häufig den Einsatz von Portalen zum Austausch von Informationen. Viele Projektbeteiligte kommunizieren von unterwegs über die verschiedensten Medien und Geräte - in Hotels, Flughäfen oder Bahnhöfen. Die Mailboxen von Projektmanagern und Projektmitarbeitern sind darüber hinaus ein wahrer Fundus an Dokumenten, die (als Anlagen an E-Mails) bei vielen Empfängern direkt und in Kopie landen; von Weiterleitungen mit oder ohne Wissen der Absender ganz zu schweigen. Im "normalen" Projektalltag ist es daher schwierig, eine derartige Informationsflut zu beherrschen.

Typische Schwachstellen in Projekten

Folgende Beispiele stellen nur einen Ausschnitt der vielen "typischen" Schwachstellen dar, die in Projekten erfahrungsgemäß vorhanden sind:

- Keine oder unzureichende Kommunikation von Sicherheitszielen im Projekt
- Unkenntnis über Schutzbedarf und Klassifikation von Daten sowie über Geheimhaltungspflichten
- Fehlendes Sicherheitsbewusstsein von Projektmitarbeitern und –beteiligten
- Fehlende Vorgaben für das Erkennen und Behandeln von Sicherheitslücken im Projekt
- Unzureichende Schulungen von Projektmitarbeitern für den Umgang mit Versionsverwaltungs- und Projektmanagementsystemen
- Ungenügende Dokumentation von Prozessen
- Ungeklärte Zuständigkeiten im Projekt für Dokumentation
- Unkenntnis von Richtlinien für den Umgang mit Datenträgern (z.B. Notebooks)
- Nutzung ungeschützter (öffentlicher) Kommunikationswege für die Projektkommunikation
- Unzureichende Sicherheitsmaßnahmen für Authentifizierung bei Projektmitarbeitern

Solche Schwachstellen sind ein Risiko für die Projektdaten, denn sie

- **erleichtern vorsätzliche (kriminelle) Aktivitäten**:
  Datendiebstahl, Diebstahl von Hardware (Datenträger, Smartphones, Notebooks, etc.),
  Industriespionage durch gezielte Angriffe auf Projektmitarbeiter und Projektinfrastrukturen über Angriffspunkte wie Phishing Mails, Social Engineering, Abhören von WLAN- Zugängen,
  Abziehen von Daten aus zentralen Datenbanken in der Cloud usw.
- **führen zu Fehlverhalten oder fahrlässigem Verhalten von Personen**:
  Unbedachter Umgang mit sicherheitsrelevanten Daten wie etwa ungeschütztes Versenden von E-Mails über offene Mail-Accounts, Nutzen unsicherer Portale im Internet für den Datenaustausch,
  Nutzen von Firmengeräten für ungeschützte (private) Internetkommunikation und Social Media,
  Nichtbeachtung von Grundregeln für Passwörter usw., Versehentliches Überschreiben oder Löschen wichtiger Projektdokumente, Benutzerverwaltung bzw. Vergabe von Berechtigungen hinkt der Projektorganisation

hinterher (Wenn etwa Mitarbeiter noch immer Zugriff auf Projektdaten haben, obwohl sie aus dem Projekt schon ausgeschieden sind.)

- **gefährden die Daten**:
  Unzureichender Schutz bei Verlust durch technische Ausfälle und höhere Gewalt, wie z.B. durch Hardware- oder Netzwerkausfälle, Fehlfunktion von Software etc. bzw. Schäden durch Brand, Unfälle, Blitzschäden etc.

Vieles davon ist sicherlich nichts Neues, doch leider rückt in Projekten recht häufig – durch die Konzentration auf inhaltliche Projektziele, den üblichen Zeitdruck und die Anforderung, möglichst schnell Ergebnisse zu liefern – der Sicherheitsgedanke in den Hintergrund. Dies geschieht sogar dann, wenn das Wissen über nötige Sicherheitsvorkehrungen oder vorbeugende Maßnahmen grundsätzlich vorhanden ist.

IT-Sicherheit ist jedoch nicht nur ein verständliches Bedürfnis der am Projekt beteiligten Unternehmen und Partner, sondern eine Verpflichtung: Die Absicherung aller schützenswerten Daten im Projekt vor unberechtigten Zugriffen oder auch vor Manipulation steht als klare rechtliche Verpflichtung des Projektauftragnehmers gegenüber Kunden und Lieferanten im Raum. Rechtsverletzungen, etwa des Bundesdatenschutzgesetzes (BDSG) ebenso wie der Bruch vertraglich vereinbarter Geheimhaltungspflichten können Schadenersatzforderungen auslösen und schlimmstenfalls strafrechtliche Konsequenzen haben.

Der rechtliche Hintergrund für Informationssicherheit

In Deutschland gibt es sehr viele gesetzliche Regelungen, die von Unternehmen und Organisationen verbindlich einzuhalten sind, teils mit dem Hintergrund des Gläubigerschutzes oder der Besteuerung von Unternehmen. Für besonders schützenswerte personenbezogene Daten (Patientendaten oder Klientendaten, Gerichtsakten etc.) gelten auch besondere Regelungen. Das Bundesdatenschutzgesetz (BDSG) schreibt hier entsprechende Schutzmaßnahmen vor. Die nachfolgenden Beispiele veranschaulichen, wie sehr die Informationssicherheit im Unternehmen in vielen Bereichen auf gesetzlichen Rahmenbedingungen beruht:

- Maßnahmen zur Datensicherung und Archivierung sind erforderlich, um die nach der Abgabenordnung (AO) vorgeschriebene Aufbewahrungspflicht von Unterlagen zu sichern.
- Bei der Speicherung und Verarbeitung personenbezogener Daten wird auf die Zutritts-, Zugangs- und Zugriffskontrolle sowie Weitergabekontrolle vom BDSG ein großer Wert gelegt.
- Das neue IT-Sicherheitsgesetz verpflichtet die Betreiber besonders gefährdeter Infrastrukturen (sogenannten Kritischen Infrastrukturen) wie Energie, Wasser, Gesundheit oder Telekommunikation, Ihre Netze besser vor Hacker-Angriffen zu schützen.

Weitere Rahmenbedingungen können durch individuelle vertragliche Vereinbarungen über die Geheimhaltungspflichten von ausgehändigten Unterlagen (wie etwa Konstruktionszeichnungen von Lieferanten) gegeben sein oder durch Daten, die im Rahmen einer Dienstleistung verarbeitet werden (so etwa Datenbanken von Kunden). Auch die Vertragsgestaltung mit Projektpartnern kann durchaus einer Schweigepflicht unterliegen. (Bild 1).

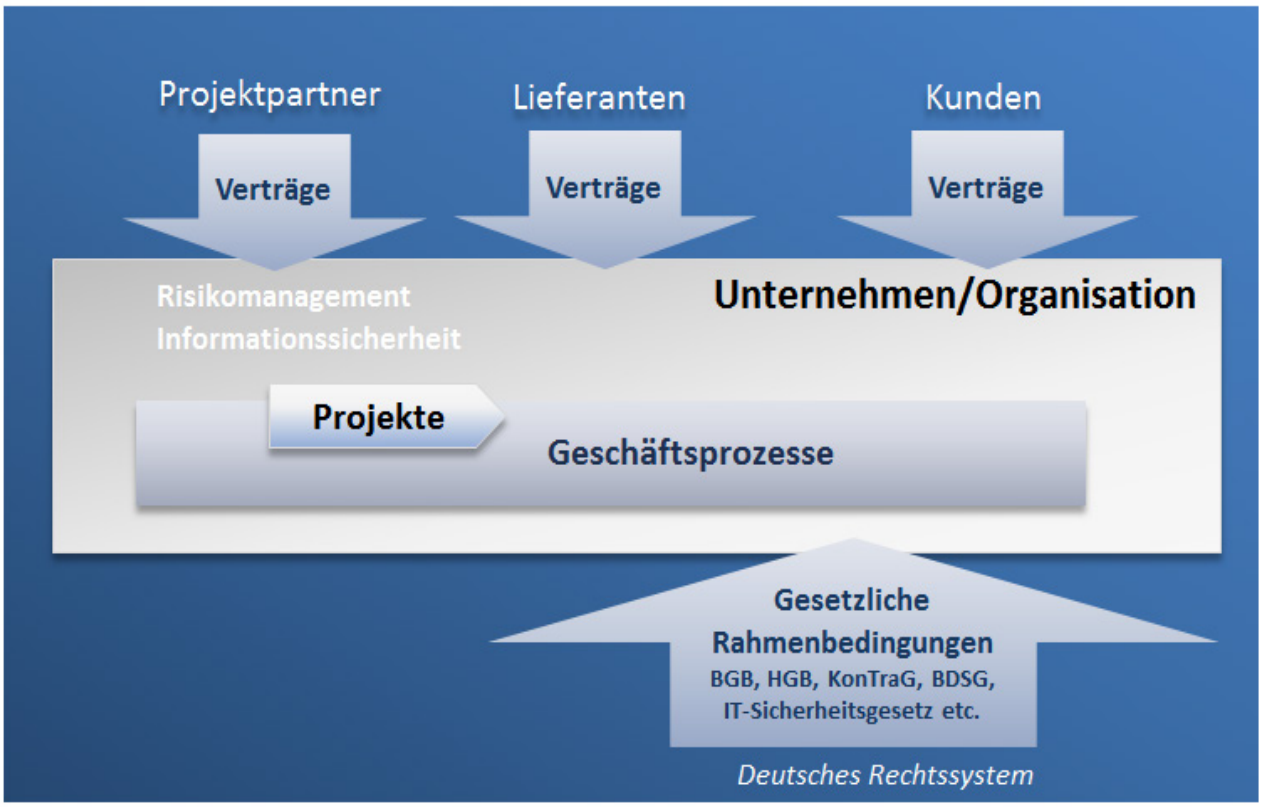

Bild 1: Rechtlicher Rahmen für Unternehmen und Projekte.

Was bedeutet dies für Projekte?

Die Verantwortung für Informationssicherheit liegt grundsätzlich (wie etwa im GmbH-Gesetz festgelegt) bei der Geschäftsführung bzw. dem Management. Gesetze und Verträge, die für ein Unternehmen oder eine Organisation gelten, sind jedoch auch in Projekten einzuhalten. Die Absicherung aller schützenswerten Daten vor unberechtigten Zugriffen oder auch vor Manipulation ist daher eine klare rechtliche Verpflichtung des Projektauftragnehmers gegenüber Kunden, Lieferanten und auch gegenüber dem Gesetzgeber. Daher sind schlimmstenfalls rechtliche Konsequenzen zu befürchten, wenn - wie in den eingangs genannten Beispielen - die Informationssicherheit im Projekt nicht gewährleistet ist:

- Geraten im Projektverlauf technische Zeichnungen eines Lieferanten durch fehlgeleitete E-Mails versehentlich in falsche Hände, könnte dies Schadensersatzforderungen des Lieferanten nach sich ziehen, die vertraglich beziffert sind. Zudem könnten dadurch die Geschäftsbeziehungen zum betroffenen Lieferanten schwer belastet werden, was indirekt auch negative Konsequenzen auf die Zusammenarbeit im Projekt nach sich ziehen kann.
- Sind Speichermedien mit Sicherungen einer Kundendatenbank aufgrund des unachtsamen Umgangs nicht mehr auffindbar, so könnten daraus schlimmstenfalls sogar strafrechtliche Folgen entstehen – falls es sich

dabei etwa um sicherheitskritische Datenbestände einer Rechtsanwaltspraxis handelt. Denn das Strafgesetzbuch sieht mit §203 StGB für bestimmte Berufsgruppen (beispielsweise Rechtsanwälte oder Ärzte) bei fahrlässigem Umgang Freiheitsstrafen vor, wenn Mandanten- oder Patientendaten ohne deren Einwilligung öffentlich gemacht wurden. Sollte also der Datenträger irgendwo im Müll auftauchen….

- Werden bei einem gezielten kriminellen Angriff Details über eine neue Produktentwicklung gestohlen, kann eine derartige erfolgreiche Industriespionage den wirtschaftlichen Erfolg eines Unternehmens massiv schmälern – wenn etwa ein Konkurrenzprodukt mit kopierter Technologie billiger oder früher auf den Markt gebracht wird.

Zudem kann ein möglicher Imageschaden entstehen, wenn eine derartige Sicherheitslücke im Umgang mit fremden Daten und Informationen im Projekt auffällt, da Kunden dies durchaus als Mangel an Professionalität und Kompetenz ansehen. Darüber hinaus ist zu bedenken, dass alle Verstöße gegen geltende Rechtsvorschriften mit Strafen geahndet werden können, auch wenn es sich nicht um geheime Daten handelt - so etwa schon beim Verstoß gegen Archivierungspflichten (nach §283b StGB). Der alte Spruch "Unwissenheit schützt vor Strafe nicht" trifft hier zu, wobei in erster Linie die Geschäftsführung haften muss.

Was müssen Sie also tun?

Überprüfen Sie Ihr Projekt systematisch, um Lücken festzustellen und zu beheben. Dabei sollten Sie als erstes klären, ob es in Ihrem Unternehmen bereits eine Sicherheitsorganisation oder ein ISMS (Informationssicherheits-Managementsystem) gibt.

Definition Informationssicherheits-Managementsystem (ISMS) laut BSI-Standard 100-1:

Ein ISMS bezeichnet ein ganzheitliches Informationssicherheits-Managementsystem. Dieses Managementsystem gibt – von der Geschäftsführung ausgehend – die strategische Linie in der Organisation / im Unternehmen in Bezug auf Sicherheit vor, bestimmt die geeigneten Instrumente und Methoden für die praktische Umsetzung und gewährleistet durch die Einrichtung regelmäßiger Verbesserungszyklen die langfristige Aufrechterhaltung eines angemessenen Sicherheitsstandards. Das ISMS umfasst Management-Prinzipien (wie ein "Commitment"), ein passendes Sicherheitskonzept, das technische, organisatorische und rechtliche Bereiche abdeckt sowie eine funktionierende und "lebbare" Informationssicherheitsorganisation in der Organisation / im Unternehmen. Damit kann Informationssicherheit als ein kontinuierlicher Prozess erfolgreich betrieben und gelebt werden.

In diesem Fall finden nicht nur technische Sicherheitsmaßnahmen im Projekt Anwendung, sondern Vorgaben und Regeln des Sicherheitskonzeptes (Bild 2) haben für alle Projektmitarbeiter während des gesamten Projektlebenszyklus Gültigkeit und müssen befolgt werden. Diese Vorgaben sollten dabei die Besonderheiten der Projektarbeit im Gegensatz zu den Linienaufgaben (wie etwa verteilte Teams, Kommunikation über gemeinsame Verzeichnisse, viele externe Beteiligte etc.) berücksichtigen und etwa Sonderregelungen für die Herausgabe von Unternehmensdaten an Projektbeteiligte liefern, die im Rahmen eines speziellen Projekts gelten.

Bild 2: Eine Sicherheitsorganisation unterstützt die Projekte im Unternehmen.

Ein Projekt-Check zur Informationssicherheit

Um zu überprüfen, ob die eingangs aufgeführten Bedrohungen auch für Ihr Projekt relevant sein könnten, beantworten Sie die nachfolgenden Fragen dieses Projekt-Checks mit "Ja" oder "Nein", ggf. auch mit "teilweise" oder mit "in Ansätzen" – je nach Ihrer Einschätzung.

1. Gibt es eine Sicherheitsorganisation / ein Sicherheitskonzept in Ihrem Unternehmen bzw. Ihrer Organisation?
2. Gibt es die Rolle des Informationssicherheits-Beauftragten und Datenschutz-Beauftragen (und falls ja, kennen Sie die Personen?)
3. Gibt es klare Vorgaben und Richtlinien für die Klassifikation und Handhabung von Daten?
4. Sind diese in Ihrem Projekt bekannt und werden sie verlässlich angewendet?

Können Sie die ersten beiden Fragen mit Ja beantworten, so können Sie bereits auf einer bestehenden Sicherheitsorganisation aufsetzen, die Ihr Projekt unterstützt. Inwieweit Sie dies bereits im Projekt umsetzen, prüfen die Fragen 3 und 4 ab; hier sollten Sie im Idealfall ebenfalls mit Ja antworten. Falls nicht, so sind die nächsten Schritte vorgegeben: Setzen Sie sich mit ihren Ansprechpartnern der Sicherheitsorganisation in Verbindung, informieren Sie sich über die geltenden Regeln und Richtlinien und setzen Sie diese im Projekt um. Sie können dabei Unterstützung erhalten, insbesondere um die weiteren Fragen 5 und 6 zu bearbeiten.

Wenn Sie jedoch die ersten 4 Fragen bereits mit Nein beantworten, so haben Sie keine Organisation "im Rücken". Trotzdem stehen Sie mit der Fragestellung nicht allein auf weiter Flur: Im Rahmen des Risikomanagements im Projekt lassen sich die Bedrohungen systematisch bearbeiten, die Risiken einschätzen und Maßnahmen für das Projekt festlegen.

Arbeiten Sie den folgenden Fragenkatalog systematisch ab. Einzelne Fragen bzw. Aufgabenstellungen, die sich aus dem weiteren Fragebogen ergeben, können Sie auch an interne Abteilungen wie Personal, Vertrieb, Beschaffung, IT etc. delegieren, um Unterstützung zu erhalten. Auch eine gemeinsame Bearbeitung im Projektteam im Rahmen eines Workshops zur Informationssicherheit kann hilfreich sein.

5. Wissen Sie, welche Art von Daten (personenbezogen, Kunden, Lieferanten etc.) mit hohem Schutzbedarf in Ihrem Projekt genutzt, verarbeitet oder generiert werden?

Um Frage 5 zu beantworten, klären Sie der Reihe nach ab, welches Datenmaterial im Projekt genutzt wird. Unterstützung sollten Sie sich hierzu aus verschiedenen Bereichen des Unternehmens holen:

- bei der Personalabteilung (was die Verarbeitung personenbezogener Daten wie Zeitmeldungen, Urlaubsanträge und andere Daten der eigenen Mitarbeiter angeht).
- beim Vertrieb bzw. dem Kundenbetreuer im eigenen Haus oder direkt bei Ihren Ansprechpartnern des Kunden, für den Sie das Projekt durchführen (ob interne/geheime Kundendaten, etwa eines ERP-Systems oder technische Produktdaten etc. betroffen sind). Hier erfahren Sie auch, wie sensibel das Material ist.
- beim Einkauf/der Beschaffung (Ggf. Für Lieferantendaten wie etwa Konstruktionszeichnungen).

6. Kennen Sie den rechtlichen Hintergrund für den Schutzbedarf der im Projekt verwalteten Daten wie etwa das BDSG, vertraglich vereinbarte Geheimhaltungspflichten etc.?

Informieren Sie sich auch über Verträge bezüglich der Geheimhaltung von Daten. Üblicherweise sind Klauseln über die Vertraulichkeit/Geheimhaltungspflicht von Daten in Dienstleistungsverträgen, Kooperationsverträgen oder Werkverträgen mit Lieferanten zu finden. Derartige Verträge können – je nach Unternehmensorganisation – im Einkauf, der Rechtsabteilung oder im Bereich der kaufmännischen Geschäftsführung erfragt werden.

7. Kennen Sie die rechtlichen Folgen für das Unternehmen etwa bei Datendiebstahl oder –verlust?

Fragen 5 bis 7 sind die zentralen Anhaltspunkte, um zu klären, welchen Schutz Sie in Ihrem Projekt benötigen – um die Verhältnismäßigkeit von Maßnahmen und damit zusammenhängenden Aufwänden und Kosten zu gewährleisten. Und, um Sie abzusichern, damit keine rechtlichen Vorschriften oder Vereinbarungen im Projekt verletzt werden.

Aus den Antworten auf die Fragen 5 bis 7 erhalten Sie die Information, welches Datenmaterial besonderen Schutz verdient. Gibt es eine Anleitung zur Klassifikation von Daten (Frage 3), so können Sie diese gleich nutzen, um die identifizierten Daten entsprechend zu klassifizieren. Falls nicht, so geben die Antworten auf Frage 6 und 7 Hilfestellung, ob es sensibles oder sogar hochsensibles Datenmaterial im Projekt gibt – je nach Tragweite der Folgen, die ein Diebstahl oder Missbrauch nach sich ziehen kann.

Um einen angemessenen Schutz für das Projekt zu gewährleisten, können Sie mit diesen Ergebnissen in den zweiten Teil des Checks einsteigen, der die informationssicherheitsspezifischen Risiken bzw. Bedrohungen im Projekt abfragt:

8. Werden Datensicherheitsrisiken im Projektrisikomanagement angemessen behandelt?

Frage 8 soll Aufschluss darüber geben, ob bereits im Risikomanagement des Projekts entsprechende Maßnahmen entwickelt wurden, die genutzt werden können.

9. Kennen Sie die Bedrohungen, denen die Daten in Ihrem speziellen Projekt ausgesetzt sind?

Sollten Sie in diesem Punkt noch keine Vorstellung haben, so nutzen Sie als Einstieg in eine Risikoanalyse die Liste der typischen Bedrohungen, die zu Beginn des Artikels aufgeführt sind.

Die folgenden Fragen können als Bestandteile der Risikoanalyse dienen, die weitere Aspekte und Bedrohungen im Projekt abdecken soll:

10. Gibt es ausdrückliche Sicherheitsziele im Projekt und werden diese kommuniziert?
11. Ist bei Projektmitarbeitern und Projektbeteiligten ein angemessenes Sicherheitsbewusstsein vorhanden?
12. Sind die Dokumentation von Projektdaten und erstellten Ergebnissen, eine verlässliche Versionsverwaltung und eine regelmäßige Sicherung für Projektdokumente selbstverständlich?
13. Gibt es eine funktionierende Berechtigungs- und Zugriffsverwaltung, die sicherstellt dass nur autorisierte Personen auf Projektdaten zugreifen können?
14. Gibt es "sichere" Passwörter und ist der sorgsame Umgang damit für alle Projektbeteiligten selbstverständlich?
15. Ist eine kompetente und sorgsame Handhabung aller Daten und Datenträger im Projekt für alle Mitarbeiter selbstverständlich?
16. Tragen Sie selbst das Thema Sicherheitsbewusstsein im Projekt voran und greifen bei unbedachtem, gedankenlosen oder fahrlässigem Handeln mit Daten und Datenträgern selbst ein?
17. Sind technisch zeitgemäße Sicherheitsvorkehrungen wie etwa die Nutzung verschlüsselter Speichermedien, Diebstahlschutz für Geräte, Virenschutz, Nutzung ausschließlich gesicherter WLANS bzw. Netzzugänge etc. eine Selbstverständlichkeit?
18. Genügt die Nutzung von Diensten in der Cloud den Anforderungen der IT-Sicherheit in Bezug auf die Werte der Vertraulichkeit, Verfügbarkeit und Integrität?
19. Wird beim Ausscheiden von Projektmitarbeitern sichergestellt, dass kein Zugriff mehr auf Projektdaten möglich ist?
20. Gibt es Regeln für den Umgang mit unerwarteten Situationen, die auf Gefährdungen oder kriminelle Aktivitäten mit dem Ziel des Datendiebstahls etc. hindeuten?

Anhand der Fragestellungen 10 – 20 können Sie die häufigsten Sicherheitsrisiken für Ihr Projekt analysieren und ggf. entsprechende Maßnahmen entwickeln, die ein projektspezifisch angemessenes Sicherheitsniveau erreichen lassen. Dies ist jedoch keine Lösung, die sich einfach und ohne weiteres auf andere Projekte im Unternehmen übertragen lässt – denn Informationssicherheit ist mehr als ein Bündel von Maßnahmen in einem einzigen Projekt!

Sichere Daten – sichere Projekte

Angenommen, es gibt ein Sicherheitskonzept im Unternehmen, das auch für alle initiierten Projekte gilt. Alle Daten, die in den einzelnen Beispielfällen verwendet werden, sind durch das ISMS nach deren Schutzbedarf klassifiziert und gekennzeichnet, die beteiligten Projektmitarbeiter kennen die Regeln für deren Handhabung und wenden sie sicherheitsbewusst und verlässlich an. Unter diesen Voraussetzungen könnten die drei am Artikelanfang benannten Schadensfälle vom Sicherheitssystem abgefangen werden:

Beispiel: Im Projektverlauf können technische Zeichnungen eines Lieferanten nicht durch fehlgeleitete E-Mails versehentlich in falsche Hände geraten.

Eine Auswahl von Vorgaben des ISMS, die dies sicherstellen können:

Die technischen Zeichnungen des Lieferanten sind als "Intern" eingestuft und gekennzeichnet. Die Mitarbeiter wissen, dass sie keinem Dritten zugänglich gemacht werden dürfen. Sie werden also nicht per Mail versendet. Die Dateien liegen auf einem durch Zugriffsberechtigungen abgesicherten Laufwerk, auf das nur ausdrücklich autorisierte Personen Zugriff erhalten.

Beispiel: Der Umgang mit Speichermedien ist dem darauf gespeicherten Inhalt angemessen, achtsam und nachvollziehbar, so dass die Sicherungen einer Kundendatenbank nicht einfach verloren gehen können.

Eine Auswahl von Vorgaben des ISMS, die dies sicherstellen können:

Der Prozess der Handhabung von Kundendaten ist genau beschrieben und bekannt.
Kundendaten gelten grundsätzlich als sensibel und dürfen nur mit den Vorsichtsmaßnahmen für sensible Daten transportiert und an dafür vorgesehenen Orten aufbewahrt werden. Die Aushändigung von Datenträgern ist nur an qualifizierte und autorisierte Personen erlaubt und ist zu quittieren und zu dokumentieren.

Beispiel: Der Datendiebstahl vom Notebook des Projektleiters wird durch Schutzmaßnahmen auf mehreren Ebenen verhindert: Notebooks sind technisch gegen Angriffe abgesichert, Passwörter folgen hohen Sicherheitsstandards, unsichere Netze werden nicht genutzt etc. Dazu gibt es organisatorische Richtlinien für die Datenhaltung, Projektbeteiligte sind dahingehend sensibilisiert und handeln sehr kompetent, sodass keine sicherheitskritischen Daten am Notebook des Projektleiters abgespeichert werden.

Eine Auswahl von Vorgaben des ISMS, die dies sicherstellen können:

- Technische Produktdaten in der Entwicklung werden grundsätzlich als hochsensibel eingestuft und gekennzeichnet. Sie werden nur an speziell abgesicherten Speicherorten (internes, physikalisch getrenntes Netz mit eigener Firewall usw.) abgelegt und nicht auf lokalen Festplatten gespeichert.
  Sie sind nur ausdrücklich autorisierten Personen zugänglich und werden nicht per Mail versendet.

- Daneben werden Notebooks nur mit verschlüsselter Festplatte ausgegeben. Passwörter müssen den Sicherheitsrichtlinien für Passwortregeln entsprechen.
- Die Nutzung offener WLAN-Zugangspunkte (in Hotels, Flughäfen,..) mit Firmennotebooks ist nicht möglich.
- Bei Anzeichen, die möglicherweise auf einen unberechtigten Zugriffsversuch oder einen externen Angriff hindeuten, ist sofort das Gerät vom Netz zu nehmen und der zuständige IT-Notfallmanager zu informieren.

Für diese Beispiele ist mit einem ISMS das Risiko für einen Missbrauch oder Verlust der Daten deutlich gemindert. Auch wenn es eine hundertprozentige Sicherheit natürlich nicht geben kann, ist die genannte Kombination geeigneter technischer und organisatorischer Schutzmaßnahmen für die Projektbeteiligten von großem Vorteil: Sie liefert neben technischem Schutz klare Handlungsvorgaben und Regeln für den Umgang mit ungewöhnlichen Vorgängen, die ggf. sicherheitskritisch sein können.

Fazit

Mit der Methodik eines projektspezifischen Risikomanagements lassen sich Risiken der Informationssicherheit durchaus abdecken. Um einen angemessenen Sicherheitsstandard (auch langfristig) zu gewährleisten, reichen jedoch erfahrungsgemäß Sicherheitsvorkehrungen im Einzelprojekt nicht aus - auch wenn technische Einrichtungen kurzfristig "gefühlte Sicherheit" vermitteln. Wesentlich leistungsfähiger ist ein ganzheitliches Sicherheitskonzept, das sich sowohl organisatorischer, technischer als auch rechtlicher Aspekte widmet und einen kontinuierlichen Verbesserungsprozess beinhaltet.

Dies kann aus einem Einzelprojekt heraus nicht aufgebaut werden – die Verantwortung hierfür liegt beim Management bzw. der Unternehmensführung. Die Erkenntnisse aus dem Projekt-Check können aber als Diskussionsgrundlage für eine Erörterung des Themas auf Unternehmensebene dienen, um die Unternehmensführung für das Thema zu sensibilisieren.

Literaturhinweise

Für eine intensivere Auseinandersetzung mit dem Thema Informationssicherheit sind die folgenden Quellen zu empfehlen:

- Download-Angebot des BSI (Bundesamt für Sicherheit in der Informationstechnik): https://www.bsi.bund.de/DE/Themen/themen_node.html
- Leitfaden Informationssicherheit des BSI: http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile
- Vorgehensmodell für Informationssicherheit für den Mittelstand (Bayerisches IT-Sicherheitscluster): http://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html
- Informationsportal Secupedia: http://www.secupedia.info/wiki/IT-Sicherheitsgesetz
- Informationsportal der Zeitschrift KES: https://www.kes.info/aktuelles

- Informationsseiten des BVMW (Bundesverband mittelständische Wirtschaft) zur IT-Sicherheit: http://www.mit-sicherheit.bvmw.de

Hat Ihnen dieser Artikel gefallen?

Bewerten Sie ihn im Projekt Magazin online und teilen Sie so Ihre Meinung anderen Lesern mit. Wählen Sie dazu den Artikel im Internet unter http://www.projektmagazin.de/ausgaben/2016 oder klicken Sie hier, um direkt zum Artikel zu gelangen.