Leitfaden zur Softwareauswahl und -implementierung

Security Incident & Case Management Tools (SICT)

ASW Bundesverband

Herausgeber: ASW Bundesverband
Autor: Stefan Rohrwasser
Titelfoto: fotolia.com: ©sepy
Stand: November 2016

Schutzgebühr: 10 Euro

Inhalt

Einleitung

Wirtschaftsunternehmen sehen sich in einer globalisierten Welt immer neuen Sicherheitsbedrohungen ausgesetzt.

Cyberkriminalität steigt exponentiell an, die Angriffsvektoren werden stetig verfeinert und weiterentwickelt, um Zugriff auf Unternehmensressourcen aller Art zu erhalten. Neben Kriminellen, die gut organisiert und arbeitsteilig unterwegs sind, rücken in den letzten Jahren zunehmend geheimdienstliche Spionageaktivitäten in den Vordergrund, um vertrauliche und wettbewerbsrelevante Informationen abzugreifen. Die Gefährdungslage von Mitarbeitern international agierender Unternehmen wächst angesichts vielfältiger politischer Brennpunkte und bewaffneter Konflikte. Gleichzeitig zeigt sich der hohe Anteil von Schäden wenigverändert, die den Unternehmen durch deliktische Handlungen eigener Mitarbeiter intern entstehen, zumal das Thema Loyalität in einer volatilen Welt eine immer geringere Rolle spielt.

Damit steigt der Bedarf nach aktuellen Informationen zur Sicherheitslage im Unternehmen, um Bedrohungen frühzeitig zu erkennen, zu bearbeiten, zu reduzieren und Schäden möglichst im Vorfeld abzuwenden.

IT-Tools zur systematischen Erfassung und Auswertung von Fraudfällen und sonstigen (non-IT) Sicherheitsvorfällen[1] können einen wesentlichen Beitrag dazu leisten. Diese Tools, die Thema der weiteren Ausführungen sind, werden im Folgenden als Security Incident & Case Management Tools, kurz SICT bezeichnet.

[1] In diesem Leitfaden geht es ausschließlich um Tools zur Erfassung von Sicherheitsvorfällen im Nicht-IT-Bereich. Der Markt für spezielle IT-Security Tools zur Härtung der eigenen IT und zur Identifikation und Abwehr von Cyberangriffen wird also nicht betrachtet.

Noch eine Anmerkung vorweg: Der nachfolgende Praxisbericht beruht auf den Erfahrungen und Gegebenheiten in einem mehrstufig gegliederten, internationalen Großkonzern mit zahlreichen Beteiligten und einer fünfstelligen Anzahl von Sicherheitsvorfällen pro Jahr. Bei der Anwendung des Vorgehensmodells auf Unternehmen von geringerer Größe und schlankerer Struktur ist davon auszugehen, dass die Einführung eines SICT in vielen Fällen in vereinfachter Form wird stattfinden können.

I. Besonderheiten von SICT

Angebotene Tools unterscheiden sich mitunter deutlich in ihrer Leistungsfähigkeit und Zielrichtung. Komplexe SICT sind geeignet, sehr unterschiedliche sicherheitsrelevante Ereignisse zu erfassen, von der „offen stehenden Tür“ im Werksgebäude bis hin zur detaillierten grafischen Beschreibung des modus operandi bei einem raffinierten Betrugsdelikt.

Während einige Tools eher der Dokumentation dienen, ermöglichen andere umfangreiche Auswerte- und Reportingfunktionen zur Analyse und Beschreibung der Sicherheitslage oder einzelner Fälle, wie sie auch von Strafverfolgungsbehörden genutzt werden.

Sofern nicht rein statistische Erhebungen stattfinden, sind SICT zudem dadurch charakterisiert, dass in ihnen in aller Regel höchst sensible personen- bzw. mitarbeiterbezogene Daten verarbeitet werden.

Wenn beispielsweise Verdachtsfälle deliktischer Handlungen von Mitarbeitern im Rahmen von internen Ermittlungen dokumentiert und ausgewertet werden, wird klar, dass diese Informationen nur einem sehr kleinen, exklusiven Kreis von Personen zugänglich gemacht werden dürfen und die Daten in einer speziell gesicherten Umgebung am besten aufgehoben sind.

Es bestehen somit höchste Anforderungen hinsichtlich Compliance und Datenschutz, der Zuverlässigkeit der an diesen Systemen arbeitenden Mitarbeiter sowie an die Vertraulichkeit und Integrität der erfassten Daten.

Daraus ergeben sich erhebliche Auswirkungen auf die funktionalen und nicht-funktionalen Anforderungen, die eine wesentliche Rolle bei der Auswahl und Entwicklung einer Lösung spielen. Hierzu später mehr.

II. Anwendungsbeispiele und Nutzen eines SICT

a. Portfolio eines SICT

Ein komplexes SICT ist ein mächtiges Tool, das je nach Bedarf sehr unterschiedlichen Zwecken dienen kann. Treten in einem Unternehmen zahlreiche Sicherheitsvorfälle auf, so hilft ein solches Tool, den Überblick zu behalten und Entwicklungen frühzeitig zu erkennen. Und: Die Sicherheit kann effizienter und effektiver gesteuert werden.

Kernstück sind dabei die Auswertemöglichkeiten, begründet durch ein möglichst mehrstufiges Datenmodell, das es gestattet, empfängerorientierte Reports unterschiedlicher Detailstufe zu erstellen.

Voraussetzung für alles ist eine möglichst vollständige Erfassung von Vorfällen nach einheitlichen Kriterien. Ereignisse können mit Personen-, Betriebsstätten-, Orts-, Zeit- und Tatmittelinformationen verknüpft und im Datenpool miteinander abgeglichen werden, um Auffälligkeiten zu erkennen wie Häufungen von bestimmten Tätern oder auch Tatmitteln[2]. Werden Daten über einen längeren Zeitraum gepflegt, können neben der jeweiligen Ist-Situation auch Entwicklungen und aktuelle Trends abgebildet werden.

Aber das ist längst nicht alles, was ein SICT leisten kann. Zusammengefasst unterstützt es folgende wesentlichen Zwecke:

- Schaffung von Transparenz über Sicherheitsrisiken und -lage
- Steuerung der Sicherheitsorganisation nach Risiko-, Effizienz- und Qualitätskriterien
- Erfüllung rechtlicher Vorgaben und Nachweispflichten, z. B. im Datenschutz und Risikomanagement

Von der Vielzahl von Möglichkeiten, die ein SICT bietet, können im Folgenden lediglich einige Anwendungsbeispiele skizziert werden.

[2] Tatmittel können KfZ, Internet, gestohlene Zutrittskarten, Werkzeuge, Social Engineering etc. sein.

b. Sicherheitslage- und Risikotransparenz

Hat ein Unternehmen eine sehr große Zahl von Mitarbeitern/ Kunden, sollte es sich dafür interessieren, welche Schäden durch deliktische Handlungen entstehen, in welcher Form und wo es angegriffen wird und wie hoch der Anteil von internen Tätern ist.

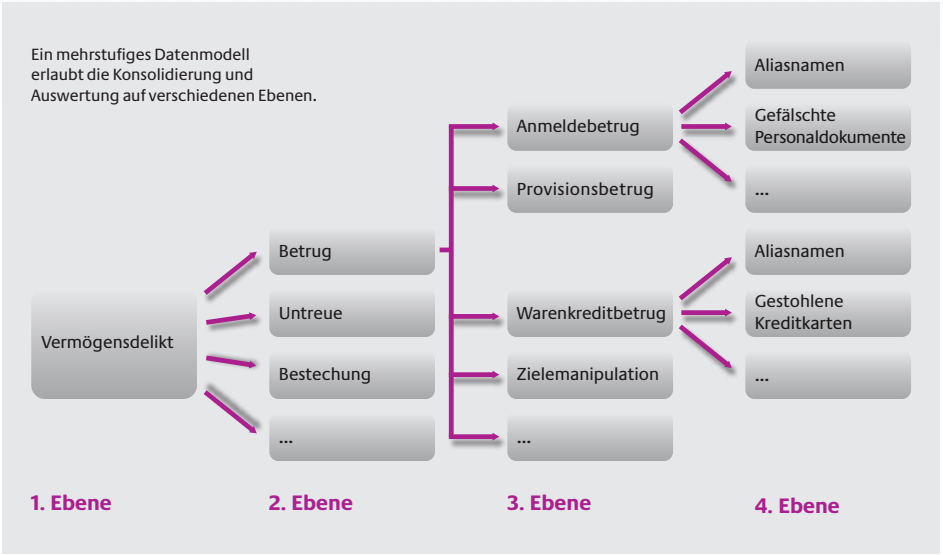
Für ein weltweit agierendes Unternehmen dürfte es ebenso von Interesse sein, wie es um die Sicherheit der einzelnen Landesgesellschaften bestellt ist. So lassen sich Vergleiche anstellen und lokale und überregionale Sicherheitsrisiken werden frühzeitig erkannt. Ein SICT, das eine Mandantentrennung[3] unterstützt, ist dafür ein geeignetes Instrument.

Die Zuordnung der erfassten Ereignisse erfolgt nach bestimmten Deliktclustern, die sich nach der Art und den Schwerpunkten des jeweiligen Unternehmens richten sollten. In der Firma des Verfassers waren das auf oberster Betrachtungsebene Vermögensdelikte, Eigentumsdelikte, Sachbeschädigung sowie „Sonstige Delikte“, die sich in weitere „Unterdeliktarten“ aufteilen lassen. Das Prinzip wird in folgendem Schaubild anhand des Vermögensdelikts „Betrug“ verdeutlicht.

Verbindet man Deliktarten noch mit Personen-, Orts- und Zeitangaben sowie Tatmitteln, ergeben sich mehrdimensionale Auswertemöglichkeiten. Modi operandi können abgebildet und Häufungen bestimmter Delikte in regionaler und zeitlicher Hinsicht erkannt werden.

[3] Die Mandantentrennung oder Mandantenfähigkeit ist in Deutschland eine datenschutzrechtliche Anforderung, wenn Daten unterschiedlicher rechtlicher Einheiten über die gleiche Anwendung erhoben werden. Die Vermischung und übergreifende Auswertung personenbezogener Daten ist zwar unzulässig, aber rein statistisch Daten, z. B. für Vergleichsanalysen, können erhoben werden.

Abbildung I:
Deliktstruktur am Beispiel des Vermögensdelikts „Betrug“



Ein ähnliches Vorgehen bietet sich bei der Erfassung nicht-deliktischer Sicherheitsvorfälle an, wo auf oberster Betrachtungsebene unterschieden werden könnte, welche Klasse von Unternehmens-Assets (z. B. Mensch, Systeme/Daten, Infrastruktur) durch den Sicherheitsvorfall primär betroffen ist.

Die Vorfälle können zudem nach Wertgrenzen (Höhe des Schadens) oder Schwere des Delikts/Ereignisses in Kategorien wie A, B, C eingeordnet und entsprechend der Wertigkeit mit unterschiedlicher Priorität bearbeitet werden.

c. Steuerung der Sicherheitsorganisation nach Risiko-, Effizienz- und Qualitätskriterien

Es ist evident, dass mit derartigen Informationen „teure“ interne Ermittlungen und andere risikoreduzierende Maßnahmen zielgerichtet gesteuert werden können. Ressourcen können entsprechend Werthaltigkeit und Risiko sinnvoll allokiert werden.

Des Weiteren können über sicherheitsanalytische Auswertungen der in einem SICT erfassten Daten konkrete Anhaltspunkte für eine Kontaktaufnahme mit Sicherheitsbehörden und/ oder für präventive Maßnahmen zum Schutz des Betriebsvermögens gewonnen werden.

Gelingt es beispielsweise, Sicherheitsrisiken regional einzugrenzen, ergeben sich Vorteile bei der Umsetzung risikominimierender Maßnahmen. Statt eines mitunter aufwändigen überregionalen präventiven Ansatzes können gezielt örtliche Schritte ergriffen werden. Finanzmittel zur Erhöhung der Sicherheit können durch die Möglichkeit, aufgetretene Sicherheitsvorfälle einzelnen Unternehmensbereichen exakt zuzuordnen, entsprechend Kritikalität effizient verteilt werden.

Einige Beispiele aus der Praxis:

- Werden regionale/örtliche Unterschiede bei Betrugsdelikten erkannt, in denen mit gefälschten Personaldokumenten agiert wird, könnten in betroffenen Regionen oder Orten nach Kosten-Nutzen-Erwägungen gezielt Ausweisprüfgeräte eingesetzt werden.
- Hat ein Unternehmen eine ausgeprägte Vertriebsstruktur oder eine große Flächenorganisation lassen sich Auffälligkeiten in Vertriebspunkten oder Firmengebäuden hinsichtlich Diebstahlhäufigkeiten feststellen. Eventuell müssen lokale Schutz-

konzepte angepasst und Mitarbeiter betroffener Betriebsstätten für Sicherheitsmaßnahmen sensibilisiert werden. Oder es werden in Zusammenarbeit mit Polizeibehörden temporär Überwachungskameras installiert.

- Häuft sich in einer bestimmten Region die Zahl deliktisch bedingter Betriebsausfälle, weil Firmeninfrastruktur durch Vandalismus oder Sabotage beschädigt oder entwendet wird, sind lokale Maßnahmen zum physischen Schutz von Gebäuden und Einrichtungen zu prüfen und gegebenenfalls mit Hilfe von Polizeibehörden umzusetzen. Eventuell sind lokale Banden am Werk, denen nur mit Hilfe der Polizei begegnet werden kann.
- Zeigen Analysen von Sicherheitsvorfällen eine Häufung von Meldungen über offen stehende Fenster und Türen, nicht befugte Personen und Bürodiebstählen in einem wichtigen Betriebsstandort, könnte am Standort die Präsenz von Sicherheitspersonal erhöht oder mittels einer Awareness-Kampagne das Sicherheitsbewusstsein der Mitarbeiter gestärkt werden.

Ein SICT kann auf diese Weise das Management bei der Entscheidung für risikominimierende Maßnahmen ebenso unterstützen wie bei der genauso wichtigen Frage der bewussten Risikoakzeptanz.

Zusätzlich lassen sich mit Hilfe eines SICT noch eine Vielzahl weiterer betrieblich relevanter Kennzahlen und Informationen zur Qualitäts- und Performancesteigerung gewinnen.

Auch hier nur einige Beispiele:

- Über die Beobachtung von generellen Mengenentwicklungen und wiederkehrenden Häufungen von Delikten in bestimmten Zeitabschnitten[4] lassen sich Hinweise auf eine Über- oder Unterauslastung der Sicherheitsmitarbeiter und notwendige Ressourcenanpassungen gewinnen.

- Durch elektronische Zeitstempel für die einzelnen Bearbeitungsphasen eines Sicherheitsvorfalls lassen sich Durchlaufzeiten ableiten und die Einhaltung von Service Level Agreements dokumentieren. Engpässe in einzelnen Phasen werden transparent und können ausgeregelt werden.
- Die Erfassung monetärer und qualitativer Größen wie die Art und Zahl bearbeiteter Vorgänge, Schadenssummen, erfolgreiche Regressforderungen, Zahl von Strafanzeigen, Zahl arbeitsrechtlicher Maßnahmen geben eine gute Indikation über die Leistungen der Sicherheitsorganisation.
- Optimierung der Zusammenarbeit der Sicherheitsorganisation mit anderen Unternehmenseinheiten durch nachvollziehbares Zahlenwerk über die jeweilige Sicherheitslage. Reibungsflächen werden so reduziert, Diskussionen versachlicht.
- Automatisierte und anonymisierte Kundenbefragungen[5] nach Fallabschluss ergeben ein zuverlässiges Bild über die Zufriedenheit mit der Sicherheitsabteilung. Das Feedback kann genutzt werden für qualitätsverbessernde Maßnahmen.
- Durch nachvollziehbare Mengengerüste kann ein SICT bei Bedarf die faktische Grundlage für die innerbetriebliche Verrechnung von Security-Leistungen bereitstellen.

[4] Die konkrete Auswertung von Tatzeitpunkten ergab in der Praxis z. B., dass bestimmte Betrugsdelikte vorzugsweise nachts und am Wochenende ausgeführt wurden. Außerdem waren je nach Delikt teils große jahreszeitliche Schwankungen zu beobachten. Offenbar machen auch Täter Urlaub und schauen Fußball-WM. Sachbeschädigungen häuften sich jedes Jahr an Silvester.

[5] Der Begriff Kunde bezieht sich in diesem Zusammenhang auf „interne Kunden“, die Sicherheitsvorfälle an die zentrale Sicherheitsorganisation melden und diese quasi mit der Ausregelung beauftragen.

d. Erfüllung rechtlicher Vorgaben und Nachweispflichten

Werden in Zusammenhang mit Sicherheitsvorfällen oder deliktischen Handlungen personenbezogene Daten erfasst (z. B. über Tatverdächtigte, Zeugen, Kunden etc.) greifen unmittelbar die Anforderungen des deutschen Datenschutzgesetzes.

Zudem sind Geschäfte durch die verantwortlichen Personen generell mit der erforderlichen Sorgfalt zu führen, Risiken sind in geeigneter Weise zu managen. Letzteres ergibt sich aus dem Aktiengesetz. Das bezieht auch den Umgang mit gravierenden Sicherheitsrisiken ein, bei denen ein Unternehmen gut beraten ist, das Vorgehen nachvollziehbar zu dokumentieren. Denn die Erfüllung der Sorgfaltspflichten muss im Zweifel nachgewiesen werden können. Bei Verstößen drohen Haftungsrisiken für das Unternehmen wie für handelnde Personen.

Ein entsprechend konzipiertes SICT, ergänzt um ein Datenschutzkonzept, ein IT-Sicherheitskonzept sowie klare Handlungsanweisungen für Mitarbeiter im Umgang mit personenbezogenen Daten, kann hier unmittelbar dazu beitragen, diese Risiken zu reduzieren.

So bietet ein geeignetes SICT sensiblen Daten eine „sichere“ Umgebung. Mit gegebenenfalls mehrstufigen Anmeldeprozeduren, Berechtigungskonzepten, automatisierter Datenverschlüsselung und automatisierten Löschfristen werden wesentliche Vorgaben des Bundesdatenschutzgesetzes erfüllt. Zudem ermöglicht ein SICT die sogenannte elektronische Fallakte, die aufwändige Papierarchive überflüssig macht, zumal eine doppelte Datenhaltung ohnehin dem Grundsatz der Datensparsamkeit widerspricht. Über Logging können alle Aktivitäten am System aufgezeichnet und der Umgang mit vertraulichen Daten im Einzelfall revisionssicher nachvollzogen werden.

Werden in einem SICT außerdem die Prozessschritte zur Bearbeitung eines Sicherheitsvorfalls sowie zu durchlaufende Prüf- und Kontrollpunkte (inkl. Dokumentation) abgebildet, kann ein ordnungsgemäßer, sorgfältiger Umgang mit dem Risiko jederzeit dokumentiert und nachgewiesen werden.

Soviel zu den grundsätzlichen Möglichkeiten eines komplexen SICT. Aber nicht jedes Unternehmen braucht gleich die „ganz große“ Lösung. Insofern ist es sinnvoll, zunächst einige grundlegende Überlegungen anzustellen, bevor der eigentliche Auswahlprozess startet.

III. Grundgedanken zur Auswahlentscheidung

Welchen Aufwand ein einzelnes Unternehmen in den Auswahl prozess steckt, wird davon abhängen, welche Bedeutung ein solches Tool im jeweiligen Unternehmenskontext genießt und welche Ressourcen und Investitionssummen zur Verfügung stehen. Ähnliches gilt für die Auswahl des Tools selbst.

Eine generelle ex-ante Eignungsbewertung am Markt existierender IT-Tools ist schwerlich möglich, da sich Bedarfe von Unternehmen im Hinblick auf Anforderungen grundsätzlich sehr stark unterscheiden.

Vereinfacht gesagt, wird die Beschaffung tendenziell umso schneller und kostengünstiger, je mehr auf vorhandene Standardlösungen ohne größere Anpassungen zurückgegriffen werden kann. Die Wahrscheinlichkeit, dass eine am Markt angebotene IT-Lösung ohne jegliche Anpassung zu einem Unternehmen eins zu eins „passt“, sinkt mit der Zahl unternehmensspezifischer Anforderungen.

Entscheidet man sich von vornherein für eine Neuentwicklung von Teilen oder der Gesamtheit eines Systems, ergibt sich das Risiko, dass die ursprüngliche Zeit- und Aufwandsplanung bei Weitem überschritten wird. So kann sich das Projekt als deutlich komplexer herausstellen als geplant oder der Anbieter sich schlicht verkalkuliert haben, da er vielleicht nicht über die notwendigen Erfahrungen/Ressourcen verfügt.

Zudem ist zu berücksichtigen, dass Anbieter solcher Tools im Hinblick auf die erfolgreiche Auftragsakquisition teilweise dazu neigen, Versprechungen zu machen, die sie nicht halten können, und ihre Lösung als leistungsfähiger und umfassender darzustellen, als sie tatsächlich ist.[6]

[6] Dieser Umstand wird oftmals dadurch forciert, dass man es in der Akquisitionsphase mit Vertriebsmitarbeitern zu tun hat, aber nicht unbedingt mit IT-Entwicklern, die solche Versprechen umsetzen müssen.

Hieraus resultiert die Notwendigkeit, die Angebote vor Vertragsabschluss genau zu prüfen und in einem geordneten Verfahren die jeweils „optimale“ Lösung zu finden.

Im Laufe des Auswahlprozesses für ein Tool ist darauf zu achten, die Leistungsfähigkeit der jeweiligen Lösungen umfänglich zu verstehen. Gleichzeitig sollte Klarheit über die eigenen Erwartungen an ein solches Tool und die betrieblichen Notwendigkeiten entwickelt werden, um diese dann mit der jeweiligen angebotenen Lösung abzugleichen. Denn ein Tool, das wesentliche Anforderungen nicht erfüllt, ist mitunter genauso unbefriedigend wie eine überdimensionierte, teure Goldrandlösung, die keiner wirklich nutzt.

Letztendlich gilt für „kleine“ wie für „große“ Lösungen, dass der Nutzen größer sein sollte als der mit der Einführung eines Tools verbundene Aufwand. Unüberlegte Schnellschüsse und reine Bauchentscheidungen erscheinen vor diesem Hintergrund eher ungeeignet, weil so häufig der Zeit- und Ressourcenaufwand durch erforderliches Nachregeln oder Fehlinvestitionen höher sind als bei einem strukturierten Vorgehen.

Aber welches Tool, welcher Anbieter ist nun das/der jeweils „Richtige“? Dazu gibt es einige Hilfsmittel, die im Folgenden vorgestellt werden.

IV. Hilfsmittel zur Softwareauswahl

a. Überblick

Hilfsmittel zur Softwareauswahl dienen dazu, basierend auf Anforderungen einen Markt systematisch abzusuchen und die Zahl der infrage kommenden Anbieter sukzessive auf eine überschaubare Größe zu reduzieren.

Im Wesentlichen bieten sich vier Gruppen von Hilfsmittel zur Softwareauswahl an, die bedarfsweise miteinander kombiniert werden können:

- Marktübersichten
- Kriterienlisten
- Internationale IT-Standards
- Ablauforientierte Phasenschemata

Ihnen allen ist zumindest eigen, dass sie ein strukturiertes Vorgehen nahelegen. Und sie machen deutlich, dass es bei der Auswahlentscheidung nicht allein um die Prüfung des Vorhandenseins funktionaler, nicht-funktionaler und technischer IT-Anforderungen geht, sondern um einen strukturierten Entscheidungsprozess, in dem auch kommerzielle und organisatorische Aspekte Berücksichtigung finden.

b. Marktübersichten

Brauchbare Marktübersichten zeichnen sich dadurch aus, dass sie möglichst aktuell, ungefiltert und vollständig sind. Idealerweise ermöglichen sie zudem den Zugang zu vertiefenden Informationen. Qualitätsbewertungen können hilfreich sein, sofern die Voraussetzungen und Messkriterien ihres Zustandekommens transparent sind. Sie ersetzen aber bei heterogenen Angeboten keinesfalls eine eigene Bewertung, da schnell sehr subjektive Einschätzungen einfließen können.

Eine regelmäßig gepflegte, qualitätsgesicherte, umfassende Marktübersicht über aktuelle SICT scheint derzeit nicht vorhanden, obwohl Bedarf hierfür besteht. Schließlich ist der Markt recht vielfältig und unübersichtlich, Marktrecherchen erfordern einigen Aufwand.

Um die Identifikation des jeweils richtigen Tools zu erleichtern, hat der Verfasser eine per Internetrecherche zusammengestellte Übersicht aktueller SICT erstellt.[7] Diese soll lediglich den Einstieg in die Materie erleichtern, aber nicht eigene Recherchen ersetzen oder gar Auswahlentscheidungen determinieren[8].

Es sei an dieser Stelle nochmals daran erinnert, dass es grundsätzlich immer die Möglichkeit einer völligen Neuentwicklung gibt, um die eigenen Anforderungen bestmöglich abzubilden, wobei das aus Zeit- und Kostengründen eher die ultima ratio darstellt.

c. Kriterienlisten

Kriterienlisten helfen, die einzukaufende Softwarelösung unter sehr unterschiedlichen Aspekten und Perspektiven systematisch zu bewerten. Im Internet finden sich hierzu teils sehr ausführliche Ausarbeitungen, die sich wie eine Checkliste abarbeiten lassen. In diesem Zusammenhang sei beispielhaft auf folgende Website verwiesen: **www.softguide.de/software-kriterien**

Allein aus dem Umfang dieser Listen wird klar, dass es nicht darum gehen kann, einfach ohne weiteres Nachdenken jeden einzelnen Punkt dezidiert und mit der gleichen Intensität abzuarbeiten. Stattdessen sollte eine Prioritätensetzung entsprechend der Projektbedeutung, des Projektumfangs und der unternehmensspezifischen Anforderungen erfolgen. [9]

[7] Die Zusammenstellung (Sachstand Februar 2016) befindet sich im Anhang dieses Leitfadens. **Vollständigkeit war nicht intendiert und kann somit nicht garantiert werden.**

[8] Empfehlenswert ist in diesem Zusammenhang die Nutzung von Testzugängen, die manche Softwarefirmen anbieten, um ein erstes Kennenlernen des Tools zu ermöglichen.

[9] Einige Hinweise über relevante Kriterien zur Bewertung eines SICT aus Sicht des Verfassers finden sich weiter unten, wenn ein Beispiel für ein ablauforientiertes Vorgehen vorgestellt wird.

d. IT-Standards

In der Literatur werden unterschiedliche standardisierte **Vorgehensmodelle** zur Softwareauswahl beschrieben wie Reifegradmodelle, COBIT etc.

Ihnen allen ist gemein, dass der Auswahlprozess anhand definierter Anforderungen oder Kontrollzielen erfolgt. Für welches Modell man sich entscheidet, ist sicherlich auch eine Frage der persönlichen Präferenz und eventuell vorhandener Vorkenntnisse. Es würde hier den Rahmen sprengen, diese Modelle im Einzelnen auf Stärken und Schwächen zu analysieren. Ein Überblick findet sich unter: **https://de.wikipedia.org/wiki/Softwarebeschaffung**

e. Ablauforientierte Phasenschemata

Ein Ablaufmodell bildet im Wesentlichen chronologisch die notwendigen oder zumindest überlegenswerten Schritte zur Auswahl der geeigneten Software ab. Im Internet findet sich ein generisches Vorgehensmodell in der Enzyklopädie der Wirtschaftsinformatik[10].

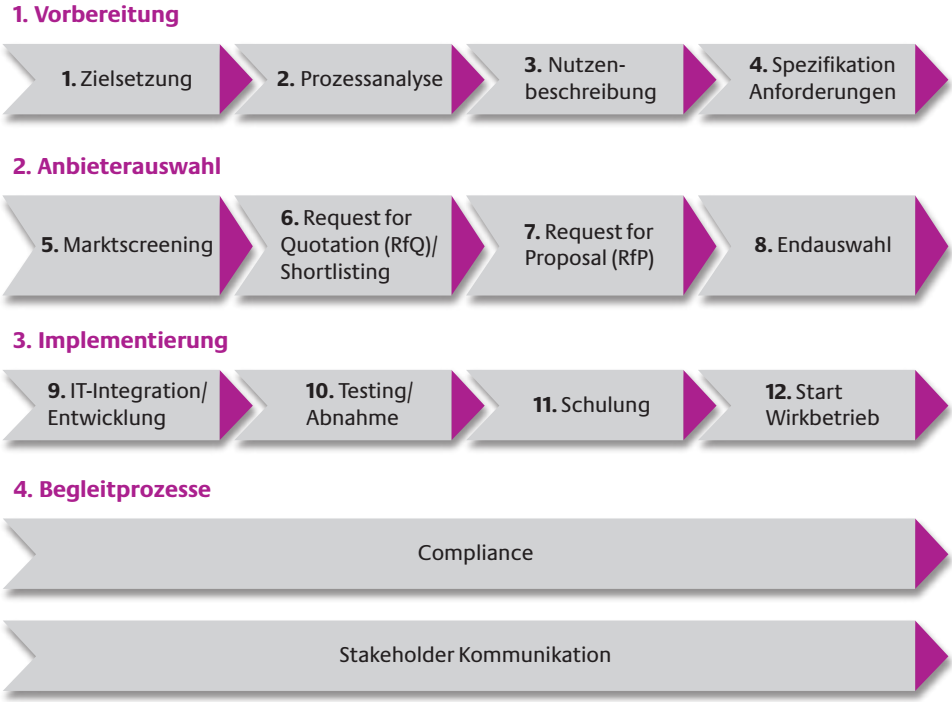
Ein **phasenorientiertes Vorgehensmodell** – ergänzt um Hinweise über besonders beachtenswerte Kriterien bei der Auswahl eines SICT – wird im folgenden Abschnitt detailliert vorgestellt. Es handelt sich selbstverständlich lediglich um ein Beispiel für einen effektiven Entscheidungsfindungsprozess bei großen, komplexen IT-Projekten, der sich aus Sicht des Verfassers allerdings bewährt hat.

[10] Prof. Dr. Norbert Gronau, Enzyklopädie der Wirtschaftsinformatik, Online- Lexikon, Kapitel „Softwareauswahl“;
http://www.enzyklopaedie-der-wirtschaftsinformatik.de/wi-enzyklopaedie/lexikon/daten-wissen/Informationsmanagement/Informationsmanagement--Aufgaben-des/Softwareauswahl

V. Beispiel eines phasen-orientierten Vorgehensmodells

Die folgende Abbildung II zeigt ein mögliches Ablaufmodell für die Auswahl einer beliebigen Software, bestehend aus drei Hauptphasen mit zwölf Realisierungsschritten und zwei Begleitprozessen[11].

Abbildung II: Prozess Softwareauswahl



Das Schaubild und der Prozess werden auf den Folgeseiten näher erläutert.

[11] Der Verfasser möchte hier nochmals betonen, dass es sich bei dem dargestellten Prozessablauf um ein mögliches Vorgehensmodell handelt. Inwiefern Phasen weggelassen, in ihrer Reihenfolge vertauscht oder verkürzt werden, ist in Abhängigkeit von der Größe des IT-Projekts und den organisatorischen Rahmenbedingungen des einkaufenden Unternehmens unter Kosten-Nutzen-Gesichtspunkten zu entscheiden.

Erläuterungen

1. Zielsetzung

- Grund der Softwareeinführung
- Optimierungsziel
- Orientierung

In dieser Phase ist zu klären und zu beschreiben, welches konkrete Ziel mit der Softwarebeschaffung erreicht werden soll, welches Problem, welche Schwachstellen beseitigt beziehungsweise welche Optimierung erreicht werden sollen. Je klarer die Ziele formuliert werden, desto mehr können sie in der Umsetzungsphase als Orientierungspunkt dienen. Damit wird das Risiko vermindert, dass der eigentliche Zweck des IT-Projekts, das sich oft über einen längeren Zeitraum hinziehen kann, aus den Augen verloren wird. In Abhängigkeit von der Bedeutung der Softwareeinführung sollte zudem die Leitung und Zusammensetzung des internen Teams zur Realisierung des Projekts zumindest vorläufig festgelegt werden.

2. Prozessanalyse

- Komplexität IT-Architektur
- Prozessunterstützung
- Prozess- und IT-Integration
- „Stand-alone“-Lösung

Die Bedeutung dieser Phase korrespondiert stark mit der Größe des jeweiligen Unternehmens, der Komplexität der bestehenden IT- und Prozesswelt und dem Umfang der Arbeitsteilung. Wird eine vollständige prozessuale Integration der neuen Lösung angestrebt, so sind mitunter zahlreiche IT-Schnittstellen zu implementieren. Dies erleichtert den automatisierten Datenaustausch und bietet tendenziell die beste Workflowunterstützung[12].

Eine Stand-alone-Lösung[13] hingegen ist vergleichsweise einfacher in Betrieb zu nehmen und erlaubt eine bessere Kontrolle über den

[12] Hier sollte immer ein optimaler, ggf. neu zu gestaltender Prozess im Vordergrund stehen. Der Eins-zu-eins-Nachbau einer Ist-Situation ist oftmals weder erforderlich, noch zielführend und kann die Realisierung signifikanter Kostensenkungspotenziale verhindern.

[13] Unter „Stand-alone“- Lösung wird hier ein System verstanden, dass zwar den Import und Export von Daten zulässt, aber über keine voll- oder teilautomatisierten Schnittstellen zu anderen Systemen verfügt.

Zugriff und den Verbleib hochsensibler Daten. Wie oben dargelegt, ein nicht ganz unwichtiges Thema bei einem SICT!

Um die organisatorischen und finanziellen Auswirkungen einer IT-Lösung abschätzen zu können, kann es durchaus sinnvoll sein, sich detailliert Gedanken zu machen, welche Bereiche und Geschäftsprozesse im Unternehmen in welchem Ausmaß betroffen sind.

- Management-information
- Information Betriebsrat
- Information betroffener Bereiche
- Transparentes Vorgehen
- Förderung Userakzeptanz
- Qualitätszirkel

Letzteres ist wichtig, um frühzeitig mit der **Stakeholder-Kommunikation** zu beginnen. So lassen sich durch Einbezug aller für das Projekt relevanten Akteure Missverständnisse und Widerstände bei der Softwareeinführung vermeiden.

Beispiele für Stakeholder im weiteren Sinne sind die Anwender[14], der Betriebsrat, die Schwerbehindertenvertretung, die Management-/ Entscheiderebene, Reportempfänger, prozessual verbundene Bereiche, interne Regelungsgeber, die IT- Sicherheit, der IT-Betrieb und der Einkauf.

Je besser es gelingt, beteiligte Personen und Bereiche im Hinblick auf eine gemeinsame Zielsetzung positiv einzubinden, desto größer sind die Chancen für eine erfolgreiche und schnelle Implementierung. Nach der Wirkbetriebsaufnahme kann die weitere Einbindung von Usern und nutzenden/betroffenen Bereichen über regelmäßig tagende Qualitätszirkel sichergestellt werden. Hierin wird über den Umgang mit aktuellen Problemen sowie über sinnvolle Change Requests (Änderungsanforderungen) zur Verbesserung und Weiterentwicklung des IT-Systems entschieden.

Es ist somit dringend zu empfehlen, das Softwareeinführungsprojekt über alle Projektphasen kommunikativ zu begleiten.

[14] Die Einbindung zukünftiger Anwender sollte spätestens in der Phase der Prozessanalyse erfolgen, um ihr Know-how über Optimierungspotenziale zu nutzen und ihre Erwartungen für ein neues IT-Tool aufzunehmen.

- Datenschutzkonzept
- Sicherheitskonzept
- Barrierefreiheit
- Betriebskonzept
- Betriebsfreigabe
- Beteiligungsrechte
- ADV

Damit eng zusammen hängt die Berücksichtigung **Compliance relevanter Faktoren** (gesetzliche Regelungen, interne Policies, Datenschutz, Beteiligungsrechte von Sozialpartnern), die ebenfalls das gesamte Projekt begleiten. Hierzu gehört insbesondere eine saubere Dokumentenlage durch Vorlage eines Datenschutz- und Sicherheitskonzepts. Und eingedenk der Tatsache, dass SICT aufgrund seiner Datenhaltung und Auswertemöglichkeiten die uneingeschränkte Aufmerksamkeit von Sozialpartnern finden werden, ist Wert auf formal einwandfreie Vorlagedokumente zur Wahrnehmung der Beteiligungsrechte zu schaffen. In vielen Fällen wird dazu auch ein Gutachten zur Barrierefreiheit gehören.

Sollen über die neue IT-Lösung zudem Daten anderer rechtlicher Einheiten, z. B. im Rahmen eines Konzernverbunds, verarbeitet werden, muss man sich mit dem Thema Mandantentrennung und Auftragsdatenverarbeitung (ADV) auseinandersetzen.

Dies alles ist aufwändig, aber gelingt das gut, so werden unerfreuliche und unerwartete Stolpersteine vermieden. Ein in anderen Fällen im Sinne der Beschleunigung des Prozesses eher unternehmerisch geprägtes Vorgehen des „handle jetzt, erkläre später“ kann bei solch Compliance relevanten Tools nicht empfohlen werden. Das wird besonders deutlich, wenn die letztendliche Betriebsfreigabe von der Zustimmung des Betriebsrates und des Datenschutzbeauftragen abhängt.

In Abbildung II finden sich entsprechend die **Stakeholder-Kommunikation** und der Themenblock **Compliance** als **Begleitprozesse** über alle Phasen der IT-Einführung.

Hierauf wird im Folgenden nicht weiter eingegangen.

3. Nutzenbeschreibung

Hier gilt es, ausgehend von der Zieldefinition, möglichst transparent zu beschreiben, welche quantitativen (möglichst monetären) und qualitativen Verbesserungen durch die einzuführende Softwarelösung zu erwarten sind.

- Kosten- Nutzen-Transparenz
- Leistungstransparenz
- Business Case
- Projektkosten
- Folgekosten
- Management-entscheidung
- Budgetfreigabe

Gute Gründe für die Einführung eines SICT können sich allein schon aus Compliance-Aspekten oder Risiko-Überlegungen (z. B. wegen fehlender Transparenz zur Sicherheitslage, verbunden mit einer Häufung von Sicherheitsvorfällen) ergeben. Die Gewährleistung von Sicherheit ist zur Erkennung, Ausregelung und Abwehr von Bedrohungen unerlässlich, kostet aber definitiv Geld. Aber welchen Wert haben Schäden, die durch ein erhöhtes Sicherheitsniveau gar nicht erst eingetreten sind? Versucht man sich idealerweise an einem Business Case (BC), kann es passieren, dass er wenig Aussagekraft besitzt und der Aufwand zur Erstellung eines BC höher als der Nutzen ist. Ein Ansatz könnte sein, abzuschätzen, was das Unternehmen aufwenden müsste, wenn es Sicherheitsleistungen extern vom Markt bezieht, und das den Kosten einer internen Bereitstellung gegenüber stellt. Ein SICT kann aus betriebswirtschaftlicher Sicht zumindest dazu beitragen, die Leistungen einer Sicherheitsabteilung oder der Sicherheitsbeauftragen transparenter zu machen, wenn in ihm neben der Erfassung der Sicherheitsvorfälle auch der Umgang mit ihnen dokumentiert wird.

Insofern empfiehlt es sich, den Nutzen und die Vorteile der angepeilten Lösung möglichst greifbar zu beschreiben. Zugleich ist es hilfreich, die zu erwartenden Kosten (Projektkosten, sonstige Einführungskosten sowie Folgekosten aus Betrieb und Change Requests) zu erfassen und dem Nutzen gegenüber zu stellen.

Hieraus lassen sich mit etwas Geschick Grenzwerte des maximalen Investitionsvolumens für ein SICT ableiten und begründen. Damit werden wesentliche Grundlagen für eine positive Managemententscheidung sowie die Budgetfreigabe gelegt.

4. Spezifikation Anforderungen

- Datenmodell
- Datenfelder
- Vorgangs-Clusterung
- Reporting-Funktionen
- Datenverknüpfung
- Datenanalyse

Die generelle Zielsetzung wird hier in operative, möglichst konkrete Teilziele herunter gebrochen, die zum Ausdruck bringen, was die zukünftige IT-Lösung letztendlich leisten soll. Es geht unter anderem um die Konkretisierung des Datenmodells, in dem beschrieben wird, welche Daten in welcher Struktur erfasst werden sollen. Hierzu gehört auch die Definition der Datenfelder und ihre Unterscheidung in Pflichtfelder und optionale Angaben sowie die Clusterung von Sicherheitsvorfällen[15]. Bei einem SICT ist das im Hinblick auf die spätere Verknüpfung und Auswertbarkeit der erfassten Angaben für statistische oder präventive Zwecke von wesentlicher Bedeutung. Damit eng verbunden ist die Frage, welche Reporting-Standards sowie -Funktionalitäten erwartet werden, um eigene Reports zu generieren, eingedenk der Tatsache, dass sich Informationsbedarfe über die Zeit weiterentwickeln[16].

- Anmeldeprozedur
- Mandantenfähigkeit
- Dokumentation
- Datenintegrität
- Logging
- Schnittstellen
- Datenhaltung
- Datentransport
- Verschlüsselung
- Löschfristen
- Benutzerrechte

Aus **Compliance- und Datenschutzgründen** sind bei einem SICT mit hochsensiblen Daten besondere IT-technische und funktionale Anforderungen[17] zu erfüllen. Hierzu gehören unter anderem: Zugangs-/Anmeldeprozeduren (z. B. mehrstufige Verfahren), Mandantenfähigkeit, revisions-sichere Dokumentation, Datenintegrität, Logging (zur Nachweisbarkeit, wer und wann Zugriff auf

[15] Eine sinnvolle Clusterung, verbunden mit Orts- und Zeitinformationen, ist Grundlage, um die Mengenentwicklung von Sicherheitsvorfällen nach Art und Kritikalität analysieren zu können.

[16] Gerade bei komplexen SICT mit zahlreichen Datensätzen kommen erfahrungsgemäß über die Zeit sehr viele neue Informations- und Auswertebedarfe hinzu. Dann ist es vorteilhaft, ein flexibles Reportingtool und ein umfangreiches Datenmodell zu haben. Je mehrdimensionaler die erfassten Daten sind, desto komplexere Auswertungen sind möglich. Um den Erfassungsaufwand zu begrenzen, wird in Pflichtfelder und optionale Felder unterschieden. Für vertiefende Auswertungen kann es aber sinnvoll sein, grundsätzlich optionale Datenfelder zumindest phasenweise obligatorisch befüllen zu lassen.

[17] Es würde den Rahmen dieses Leitfadens sprengen, auf die einzelnen Punkte und die möglichen technischen Realisierungsvarianten detailliert einzugehen. Daher nur einige Stichworte, die bedarfsweise durch die Einholung von Expertenrat in konkrete Anforderungen zu überführen sind.

Daten hatte), Art der Datenhaltung und des Datentransports (Datensicherung/-speicherung, extern/intern, Verschlüsselungstechnik, Serverstandort Inland/Ausland, Betriebskonzept etc.), Lösch- und Anonymisierungspflichten sowie Benutzerrechte und das Rollenkonzept zu beschreiben.

- Usability
- Systemperformance
- Systemstabilität
- Service Level
- Workflow-unterstützung
- Systemschnittstellen
- Flexibilität/ Anpassbarkeit

Aus **betrieblicher Sicht** treten Fragen der Usability, der Systemperformance, der Systemstabilität (Ausfallzeiten), Service Level sowie der gewünschten Workflowunterstützung und der Schnittstellen (Import- und Exportfunktionen) zu anderen IT-Systemen in den Vordergrund.

Dies alles erfordert in Abhängigkeit vom Umfang der Anforderungen sehr viel Detailarbeit, die sich aber im Hinblick auf die Auswahl der richtigen Lösung lohnt. Im Ergebnis entsteht ein Lastenheft als Grundlage für den Ausschreibungsprozess. Dies erlaubt es, den diversen Softwareanbietern im Auswahlprozess die relevanten Fragen zu stellen und in der Entwicklungs-, Implementierungs- und Testphase zu prüfen, ob die gewünschten Funktionalitäten und Anforderungen tatsächlich realisiert wurden.

Münden die oben genannten Überlegungen bereits in dieser Phase in die Erstellung einer Feinspezifikation (detailliertes Lastenheft), kann das zwar für den weiteren Auswahlprozess hilfreich sein, ist aber aus der Erfahrung des Verfassers nicht zwingend erforderlich[18]. Sie könnte auch nach Abschluss der Anbieterauswahl gemeinsam mit dem ausgesuchten Realisierer und seiner Fachexpertise erfolgen, zumal sich zumindest bei komplexeren IT-Projekten zahlreiche Anforderungen und Änderungen erst in der Realisierungsphase herauskristallisieren.

[18] Es gibt die durchaus ernstzunehmende Ansicht, dass dies sogar kontraproduktiv sein kann, weil durch kategorische Festlegungen ggf. bessere Lösungen, die sich im Rahmen eines IT-Entwicklungsprojekts erst ergeben, nicht weiter Beachtung finden, da sie von den Vorgaben abweichen. Die Empfehlung lautet: Besser genau wissen, was man als Ergebnis haben möchte, und die technische Umsetzung den IT-Experten überlassen.

Ein Hinweis an dieser Stelle noch: Ein möglichst vollständiger Katalog der fachlichen Anforderungen ist sehr hilfreich, denn eventuell notwendige Change Requests nach Abschluss der IT-Einführung sind erfahrungsgemäß kostspieliger und aufwändiger, als wenn ihre inhaltliche Umsetzung bereits in die Erstentwicklung einfließt.

Andererseits sollten die Erwartungen nicht zu hoch geschraubt werden. Denn bei komplexen IT-Projekten ist es normal, dass man auf der Wegstrecke und später im Wirkbetrieb schlauer wird. Besser, es wird zeitnah eine 80-Prozent-Lösung realisiert, als jahrelang ohne Ergebnis die perfekte Lösung anzustreben.

5. Marktscreening

- Standardlösung
- Individuallösung
- Informations-sammlung
- Recherche
- Request for Information
- Start Einkaufsprozess

Nachdem mit den genannten vier Punkten die Grundlagen gelegt wurden, beginnt spätestens nun die Phase der Identifikation eines geeigneten Realisierers/Anbieters einer Softwarelösung. Hierzu gilt es, den Markt nach vorhandenen Lösungen abzusuchen und sich einen Überblick zu verschaffen.

Aus Kosten-, Effizienz- und Gründen der Produkteinführungszeit empfiehlt es sich grundsätzlich, nach Standardlösungen Ausschau zu halten, die eventuell an eigene zusätzliche Anforderungen angepasst werden. Eine völlige Neu- oder gar Eigenentwicklung (Individuallösung) lohnt sich zumindest bei komplexen Anforderungen in aller Regel nicht und bildet nur dann eine valide Option, wenn der Markt nichts Standardisiertes hergibt oder die vorhandenen Lösungen nachweislich unbrauchbar sind.

Entsprechende Informationen über die Marktsituation sind durch Internetrecherchen, Marktübersichten[19], Expertenbefragung, Unternehmensverbände, Fachtagungen etc. zu gewinnen.

[19] Vgl. oben Kapitel IV. 1 (Seite 17)

In aller Regel lässt sich auf dieser Basis relativ schnell eine Eingrenzung der überhaupt in Frage kommenden Anbieter durchführen. Falls nicht, könnte der Kreis durch einen zwischengeschalteten Request for Information (RfI, Leistungsanfrage)[20] reduziert werden, über den bei den Firmen angefragt wird, ob sie einen definierten Bedarf unter konkreten zeitlichen Rahmenbedingungen überhaupt befriedigen können. Des Weiteren empfiehlt es sich spätestens an dieser Stelle, sofern vorhanden, hausinterne Einkaufsabteilungen über das Vorhaben zu informieren und in die kommerzielle Abwicklung mit einzubeziehen[21].

6. Request for Quotation (RfQ, Preisanfrage) und Shortlisting

In dieser Phase gilt es, die potenziellen Anbieter im Rahmen eines sogenannten RfQ um ihren Realisierungsvorschlag unter Angabe eines Zeit- und Finanzrahmens zu bitten, wobei die preislichen Angebote in dieser Phase noch unverbindlich bleiben.

- Einholung unverbindlicher Angebote
- Lastenheft
- Ausschlusskriterien
- Eingrenzung der Anbieter

Basis für die Angebotseinholung bilden der Anforderungskatalog (Lastenheft) sowie die generelle Beschreibung der mit der IT-Lösung verbundenen Zielsetzung. Um die Vergleichbarkeit der Angebote sicherzustellen, sind die Anbieter aufzufordern, zu den einzelnen Punkten des Pflichtenheftes ihren Realisierungsansatz zu erläutern. Wichtig ist zudem, in der Antwort einen Eindruck zu erhalten, in welcher Form sich der jeweilige Anbieter die Implementierung bzw. Übergabe der Software vorstellt. Gerade wenn größere Anpassungen von Standardsoftware auf die Unternehmensanforderungen hin vorzunehmen sind, die sich über Monate hinziehen können, ist es erforderlich, einen Eindruck über die Projektorganisation und -methode zu erhalten (klare Ansprechpartner, klare Verantwortlichkeiten, definierte Ressourcen).

[20] Vgl. zu den verschiedenen Ausschreibungsverfahren: https://de.wikipedia.org/wiki/Ausschreibung

[21] Dieses Vorgehen ist in vielen Unternehmen Teil des Complianceprozesses.

Für die Angebotsabgabe ist ein verbindlicher Endtermin zu nennen. Es empfiehlt sich, die Zahl der beteiligten Firmen im einstelligen Bereich zu halten, denn die Prüfung der Angebote kostet Zeit. Mitunter können bei interessanten Anbietern durch Rückfragen offene Punkte gleich in dieser Phase geklärt werden. Nach Abschluss des Prüfungsprozesses sollten die Anforderungsdokumente weiter konkretisiert und verfeinert und die Zahl der in die finale Auswahl zu nehmenden Anbieter weiter reduziert werden. Ideal wären circa drei Anbieter mit überzeugenden Realisierungsvorschlägen, die dann zum Request for Proposal (RfP, Angebotsabgabe) eingeladen werden. Hierzu kann es sehr hilfreich sein, wenn bereits Klarheit über KO-Kriterien besteht, die im Grunde bestimmte Mindestanforderungen definieren, die die Anbieter in jedem Fall einhalten müssen.

7. Request for Proposal (RfP, Aufforderung zur Angebotsabgabe)

- Einholen verbindlicher Angebote
- Referenzen
- Detailliertes Pflichtenheft
- Angebotspräsentation

Hiermit beginnt nun die eigentliche Ausschreibung insofern, als dass Angebote der teilnehmenden Firmen durch Annahme des beauftragenden Unternehmens verbindlich werden. Spätestens in dieser Phase sollten Referenzen zu vergleichbaren IT-Projekten der Anbieter eingeholt und eventuell vorhandene Testzugänge zur Software genutzt werden.

Grundlage für die Angebotseinholung bildet ein weiter detailliertes und konkretisiertes Pflichtenheft[22], das es dem Anbieter erlaubt, eine valide Projektkostenkalkulation zu erstellen und sich zu einem bestimmten Realisierungstermin zu bekennen.

Die teilnehmenden Firmen sollten idealerweise eingeladen werden, ihre Vorschläge jeweils im Rahmen einer ausführlichen Präsentation vorzustellen und offene Punkte zu klären. Es ist zu

[22] Hier sei aber nochmals auf die Ausführungen oben in Fußnote 18 verwiesen. Das Pflichtenheft sollte, was die Art der Realisierung anbelangt, nicht zum Korsett werden, das die Kreativität der IT-Entwickler unnötig einengt.

empfehlen, dass zu diesen Terminen auf beiden Seiten die Hauptakteure eingeladen werden, die für die Entscheidung sowie die operative Umsetzung verantwortlich sind, um jeweils einen persönlichen Eindruck zu ermöglichen.

Besonders wenn es um ein komplexeres IT-Projekt mit entsprechendem Zeitaufwand und großem Interaktionsbedarf geht, ist es ganz entscheidend, dass neben den objektiven, fachlichen Fakten auch die menschliche Komponente passt. Schließlich geht es bei der Entwicklung von IT um eine vertrauensvolle Zusammenarbeit. Denn schnell verliert ein Projekt sein Ziel aus dem Auge, weil es nur noch um kleine Streitereien um kommerzielle Aspekte geht[23].

8. Endauswahl

- Checkliste
- Zuverlässigkeit
- Betriebswirt. Stabilität
- Projektteam
- Kommerzielle Konditionen
- Auftreten und Commitment
- Juristische Vertragsprüfung
- Fallback-Lösung

Es empfiehlt sich, die letztendliche Auswahl der IT-Lösung/des Anbieters auf Basis einer einheitlichen, bewertbaren Checkliste durchzuführen, in der zwischen den verbleibenden Firmen alle fachlichen, finanziellen und persönlichen Komponenten möglichst objektiv miteinander verglichen werden können.

Relevante Kriterien können sein: Bekanntheit, Größe, betriebswirtschaftliche Stabilität[24] und Image des Anbieters, Referenzprojekte, Klarheit von Verantwortlichkeiten und Entscheidungswegen[25], Bereitschaft zu verbindlichen (zeitlichen) Commitments, Erfüllungsgrad IT-Anforderungen, Art des Projektmanagements[26],

[23] Daher kann es durchaus sinnvoll sein, mit dem IT-Realisierer eine Gesamtsumme statt einer im Zweifel wenig nachvollziehbaren Abrechnung auf Stundenbasis zu vereinbaren.

[24] Ein Softwareanbieter, bei dem ein hohes Risiko besteht, dass er bald wieder vom Markt verschwindet, ist kein verlässlicher Partner.

[25] Ein wesentlicher Punkt, wenn im Eskalationsfall schnell die richtigen Entscheidungsträger zu finden sind.

[26] Z. B. Fähigkeit und Bereitschaft zu „Agiler Softwareentwicklung“

Zahl und Expertise von Projektmitarbeitern[27], Umgang mit Compliance und Datenschutz[28], Service Level[29], kommerzielle Konditionen (Investitionshöhe, Folgekosten, Lizenzmodell[30] etc.), Überzeugungskraft der Akteure, Qualität der Präsentation, Identifikation mit dem Auftrag und dem Auftraggeber.[31]

Die Kriterien und ihre Gewichtung sind letztlich unternehmens- und projektindividuell entsprechend den jeweiligen Rahmenbedingungen festzulegen.

Nach Identifikation des präferierten Partners sind die Vertragsverhandlungen zu führen. Eine eingehende juristische Vertragsprüfung ist zu empfehlen. Hierzu gehören auch Fragen des Zugriffs auf den Quellcode, falls eine eingekaufte Anwendung selbst weiterentwickelt werden muss, weil ein Anbieter vom Markt verschwindet.

Diese Phase kann durchaus noch zum Umdenken führen, falls sich in den Verhandlungen in wesentlichen Punkten keine Einigung erzielen lässt oder sich neue Aspekte ergeben. Insofern empfiehlt es sich, bis zum erfolgreichen Vertragsabschluss anderen möglichen Anbietern noch keine finale Absage zukommen zu lassen, um eine Rückfalllösung zu behalten.

[27] Es sollte darauf geachtet werden, dass insbesondere der Projektleiter des Realisierers, die entsprechende fachliche Expertise vorausgesetzt, möglichst exklusiv zur Verfügung steht.

[28] Gerade bei einem SICT ein valider Punkt!

[29] Hier geht es vor allem um Störungsbeseitigung und Wartungsfenster.

[30] Dies ist besonders relevant, wenn eine spätere Erhöhung der Userzahl erwartet werden kann (Stichwort „Konzernlizenz“).

[31] Weitere Anregungen zu Checklisten finden sich selbstverständlich auch im Internet: http://www.seikumu.com/de/auswahl-und-erwerb/softwareauswahl.php

9. IT-Integration/-Entwicklung

- Systemverantwortung
- Administration
- Umsetzung Betriebskonzept
- BCM
- IT-Entwicklungs-projekt

Spätestens nach der Beschaffungsentscheidung sollte Klarheit darüber bestehen, wer die künftige fachliche Verantwortung für das neue IT-System im Hinblick auf Qualitätssicherung und Weiterentwicklung der Anwendung, wer die Administration und den IT-Betrieb übernimmt. Hierzu ist das Betriebskonzept zu verfeinern.

So sind Wartungsfenster, Betriebszeiten, Serverstandorte, betriebliche (Sicherheits-) Anforderungen festzulegen und zu entscheiden, ob der Betrieb intern oder extern erfolgen soll. Zudem ist zu prüfen, ob die Geschäftskritikalität der Anwendung die Entwicklung eines BCM-Konzepts[32] begründet, das unter Umständen möglichst noch vor der Wirkbetriebsaufnahme fertiggestellt werden sollte.

Wird eine Standardlösung, die kaum oder gar nicht weiter angepasst werden muss, erfolgt im nächsten Schritt sukzessive ihre Integration in die bestehende IT-Architektur (sofern keine Standalone-Lösung) und in die Geschäftsprozesse. Dies erfolgt idealerweise zunächst im Rahmen einer Testumgebung, wie unten in der Phase Testing und Abnahme weiter beschrieben.

Sind größere Anpassungen der Software an die betrieblichen Erfordernisse notwendig, erfolgt in dieser Phase die eigentliche Detailarbeit, in der im engen Schulterschluss mit dem ausgewählten Anbieter die angestrebte Lösung im Rahmen eines IT-Entwicklungsprojektes hergestellt wird. Ein Projektteam wird etabliert, bestehend aus den IT-Experten des Realisierers und den Fachexperten des beauftragenden Unternehmens, das offene Punkte und aufkommende Fragestellungen in enger Interaktion gemeinsam abarbeitet, die Feinspezifikation weiterentwickelt und eine Softwarelösung zu Testing und Abnahme bereitstellt.

[32] Vgl. bspw. Business Continuity Management (BCM) nach ISO 22301.

10. Testing/Abnahme

- Testumgebung
- Anwendungsfälle
- Test Systemlast
- Fehlerbereinigung

Hier ist darauf zu achten, dass durch den Realisierer eine geeignete Testumgebung (Test-/Schulungssystem) und Testdaten[33] bereitgestellt werden. Damit soll einerseits ermöglicht werden, zunächst auf Expertenebene die grundsätzlichen Funktionen zu testen, um grobe Fehler zu identifizieren und bereinigen zu lassen.

Andererseits können einzelne (zukünftige) Anwender einbezogen werden, die in dieser Phase auf Basis von Anwendungsfällen (Use Cases) und Testdaten nochmals die Usability (Anwenderfreundlichkeit), die Sinnhaftigkeit und Plausibilität des Aufbaus sowie die Stabilität und die Performance (Leistungsfähigkeit) des Systems prüfen können.[34]

Unzulänglichkeiten sollten benannt und bereinigt werden, bevor eine formale Abnahme nach Abschluss eines finalen, intensiven Testverfahrens erfolgt.

11. Schulung

- Schulungskonzept
- Motivation
- Umstellung Arbeitsprozesse
- Abbau von Ängsten

In dieser Phase sollte es Ziel sein, die zukünftigen Anwender nicht nur in die Funktionen und die Bedienung des Systems einzuweisen, sondern sie möglichst zu überzeugen und zu motivieren, dass das neue System eine Arbeitserleichterung und einen Fortschritt zur bisherigen Lösung darstellt. Dies ist in der Regel ein nicht ganz einfacher Schritt, weil sich viele Mitarbeiter schwer tun, gewohnte Arbeitsprozesse umzustellen und sich an neue Eingabemasken und Datenfelder zu gewöhnen.

[33] Eine Eigenerstellung kann recht teuer werden!

[34] Die Anwender sollten bei einer Individuallösung möglichst schon im Entwicklungsprojekt frühzeitig einbezogen werden (Stichworte: Nutzung, Anwenderknow-how, Userakzeptanz)

Die Empfehlung lautet hier einfach, genügend Zeit für die Entwicklung eines geeigneten, praxisnahen Schulungskonzepts einzuplanen und die Mitarbeiter über Hintergründe und Zielsetzung der neuen IT-Lösung abzuholen. Dazu gehört explizit auch, eventuelle Ängste vor elektronischer Überwachung abzubauen, indem offen darüber informiert wird, welche anwenderbezogenen Daten erfasst und verarbeitet werden.

Letztendlich sollte allen Projektbeteiligten klar sein, dass der Erfolg einer neuen IT-Lösung ganz maßgeblich von der Akzeptanz der Anwender und ihrer Bereitschaft abhängt, das neue System positiv zu nutzen.

12. Wirkbetriebsaufnahme

- Betriebsfreigabe
- Begleitung Systemstart
- Monitoring
- Qualitätssicherung

Sind Anwender geschult, Testing und Abnahme abgeschlossen und die Betriebsfreigabe durch die relevanten Gremien erfolgt, steht der Wirkbetriebsaufnahme nichts mehr im Wege.

Dennoch sollte gerade diese Startphase, wenn zum ersten Mal in größerem Umfang Wirkdaten verarbeitet werden, durch die fachlich Verantwortlichen intensiv begleitet werden. Idealerweise stehen Projektmitarbeiter mit eingehender Kenntnis des Systems als Ansprechpartner weiter zur Verfügung. Denn die Zahl der Fehleingaben und -bedienungen ist in dieser Phase erfahrungsgemäß noch recht hoch, was gerade bei Wirkdaten zu unerwünschten Nebenwirkungen führen kann. Insbesondere wollen die Anwender selbst in dieser Phase mit ihren Unsicherheiten nicht allein gelassen werden.

Darüber hinaus ist zu prüfen, ob die Performance unter Last weiterhin zufriedenstellend ist, der Betrieb reibungslos funktioniert, eventuelle Zugangsprozeduren funktionieren und die Datenqualität sichergestellt ist, um gegebenenfalls korrigierend einzugreifen.

Zudem kommen erfahrungsgemäß nach kurzer Zeit der Nutzung bereits erste Wünsche für eine eventuelle Weiterentwicklung der IT-Lösung auf. Diese gilt es einzusammeln, sie zum Beispiel im Rahmen von Qualitätszirkeln zu bewerten und gegebenenfalls umzusetzen. Eingedenk des Mottos:

Das System lebt!

Anhang I.

Mindestanforderungen für die Erfassung von Sicherheitsvorfällen

Wie im Leitfaden weiter oben dargelegt, wird sich die gewählte Toollösung und der Auswahlprozess je nach Anwendungszweck von Unternehmen zu Unternehmen teils deutlich unterscheiden. Viele, vor allem kleinere Unternehmen werden den dargestellten Auswahlprozess als zu kompliziert empfinden. Was aber sind die Grundsätze bzw. Mindestanforderungen, die aus Sicht des Verfassers für alle Unternehmen Relevanz haben sollten, wenn Sicherheitsvorfälle systematisch erfasst werden? Dies ist Thema der folgenden zusammenfassenden Ausführungen. Dabei wird von der Annahme ausgegangen, dass nicht nur statistische, sondern auch personenbezogene Daten erfasst sowie ein elektronisches Aufzeichnungssystem genutzt werden (keine Handaufzeichnungen).

Anforderung 1: Datenschutz

Wer personenbezogene Daten von Mitarbeitern, Kunden, Lieferanten oder sonstigen Personen erfasst, muss im Zweifelsfall nachweisen können, dass er datenschutzrechtliche Bestimmungen einhält. Dazu gehören die Zweckbindung der Datenerhebung, Nachweisbarkeit der Datenverwendung, Einhaltung von Lösch-/Anonymisierungspflichten, Datensparsamkeit, Begrenzung des Datenzugriffs und sichere Aufbewahrung. Excel-Lösungen und einfache Datenbankanwendungen genügen diesen Anforderungen in aller Regel nicht! Erforderlich sind daher zumindest ein grundlegendes Datenschutzkonzept und die Aufbewahrung der Daten in einer sicheren Umgebung. Letzteres lässt sich über sogenannte Secure/Virtual-Dataroom-Lösungen realisieren. Die Daten liegen hier vergleichsweise sicher und es lässt sich über eingebaute Logging-Funktionen nachvollziehen, wer wann Zugriff genommen hat. Sicherheits-

spezifische Dokumentations-, Analyse- und Reporting-Möglichkeiten bietet ein solches Tool im Gegensatz zu einem SICT allerdings nicht.

Schließlich ist es erforderlich, die Einhaltung datenschutzrechtlicher Bestimmungen regelmäßig zu prüfen.

Anforderung 2: Mitbestimmung und Beteiligungsrechte

Die Einführung von technischen Verfahren zur (potenziellen) Leistungs- und Verhaltenskontrolle sind mitbestimmungspflichtig. Diese Formulierung ist recht weit und unkonkret. Es ist aber davon auszugehen, dass jede Erfassung von Sicherheitsvorfällen mit personenbezogenen Daten in elektronischer Form hierunter zu subsumieren und damit der Mitbestimmung unterliegt. Firmen, die einen Betriebsrat haben, sind daher gut beraten, Mitbestimmungsrechte adäquat zu beachten und den Sozialpartner frühzeitig einzubinden. Eine Nichtbeachtung kann bei Klage des Betriebsrates dazu führen, dass der Betrieb des technischen Verfahrens untersagt wird.

Anforderung 3: Erfüllung sonstiger rechtlicher Anforderungen

Aus der gesetzlich verankerten unternehmerischen Sorgfaltspflicht[35] ergibt sich, dass Geschäfte durch die verantwortlichen Personen generell mit der erforderlichen Sorgfalt zu führen sind, um Haftungsrisiken zu vermeiden. Der Nachweis muss durch die handelnden Personen im Streitfall selbst erbracht werden. Die Erfassung von und der Umgang mit gravierenden Sicherheitsvorfällen sollte daher in nachvollziehbarer, am besten revisionssicherer Weise dokumentiert werden, um zu belegen, dass die Risiken in geeigneter Weise gemanagt wurden. Welches elektronische Werkzeug man immer einsetzt, so sollte es diesen Anforderungen genügen. Der Vorteil vieler SICT ist es, dass sie entsprechende Funktionen bereits per se an Bord haben.

[35] Z. B. § 276 BGB, § 79 AktG, § 43 GmbHG

Anforderung 4: Mitarbeiterkommunikation

Die Erfassung von Sicherheitsvorfällen mit Personenbezug, insbesondere wenn ggf. Daten eigener Mitarbeiter wegen möglicher Beteiligung bei deliktischen Handlungen oder bei sonstigen sicherheitsrelevanten Ereignissen erfasst werden sollen, ist ein hochsensibles Thema, das kommunikativ begleitet werden sollte, um Gerüchten und dem Entstehen einer Misstrauenskultur gegenzusteuern. Daher sollte frühzeitig und offen über die Gründe und Ziele einer geplanten Erfassung von Sicherheitsvorfällen informiert werden. Dies hat den weiteren Vorteil, dass sich die Sensibilität der Mitarbeiter für die Unternehmenssicherheit erhöht, indem die Geschäftsleitung ihre Aufmerksamkeit für das Thema nachdrücklich unterstreicht.

Anforderung 5: Zielsetzung und Kosten-/Nutzenüberlegungen

Aus den obigen Ausführungen zu den Anforderungen 1–4 wird deutlich, dass die Einführung eines Systems zur Erfassung von Sicherheitsvorfällen kein triviales Thema ist. Dennoch ist sie für Unternehmen zumindest einer bestimmten Größe und Struktur absolut erforderlich. Auch das wurde dargelegt. Schon allein aus diesen Gründen empfiehlt es sich, sich vor der Einführung eines elektronischen Erfassungssystems unter Berücksichtigung absehbarer zukünftiger Entwicklungen eingehende Gedanken zu machen, welche Ziele damit verfolgt werden und welchen konkreten Nutzen sich das Unternehmen davon verspricht. Von wenig überlegten „Bauchentscheidungen“ ist abzuraten, denn entweder führt ein Schnellschuss bald zu Enttäuschungen, weil das System doch nicht das kann, was eigentlich gebraucht wird, oder aber es kann viel mehr als benötigt, ist überdimensioniert, zu komplex und dann meist auch zu teuer.

Anhang II.

Security Incident & Case Management Tools – eine Übersicht

Stand 11/2016; ohne spezifische IT Security Incident Tools
Hyperlinks zuletzt geprüft am 03.11.2016

abmintellicase	Vereinigtes Königreich
ABM	Investigative incident management software. www.abmsoftware.com/products/abmintellicase

Case Point Pro	Vereinigte Staaten von Amerika
Case Point	Investigative case management software for the private detectives and process servers. www.casepointdb.com

Column Case Management	Vereinigtes Königreich
Column Technologies	Helps enterprise level organizations capture, investigate, & manage cases. Includes relationship mapping to license plates, people, etc. www.columnit.com/uk

Corporate Security Reporting System	Schweiz
Verismo	Softwarelösungen für das unternehmensweite Reporting des Sicherheitsmanagements. http://www.verismo.ch/sites/default/files/Verismo_ITtools_SecurityReportingsystem_0.pdf

Crime-S	Vereinigtes Königreich
Crime-s	with the ability to capture, track, manage and generate reports on all possible incidents at the workplace. www.crime-s.com/Crimes/Templates/Home_162_9_189_Graphical.aspx

Digital Investigation Manager	Italien
DFLabs	Manages incident response and forensic acquisition procedures in full compliance with digital investigation standards. http://www.dfresponse.com/index.php

EnCase Enterprise	Vereinigte Staaten von Amerika/Filiale D
Guidance Software	Enables analysis to respond to security incidents, perform investigations and conduct audits. www.guidancesoftware.com/Lang/Pages/de/Losungsubersicht.aspx

FireFiles	Vereinigte Staaten von Amerika
Albanese Consulting	Software for fire and bomb investigation case management; manage, share, search and report on cases. www.albx.com/solutions/govt/firefiles.asp

FormDocs	Vereinigte Staaten von Amerika
FormDocs	Manage your case files including incident reports, arrest reports and follow-up reports. www.formdocs.com

GS1	Vereinigte Staaten von Amerika
GuideSTAR Technologies	Tool for national law enforcement to facilitate collaboration in detecting potential threats and investigating criminal events. www.guidestartech.com/index.php

ICMS	Vereinigte Staaten von Amerika
InfoStrat	The Investigative Case Management System (ICMS) covers all the phases of an investigation and is used by several U.S. Federal agencies. www.infostrat.com/solutions

Investigative Software	Vereinigte Staaten von Amerika
L.E.A. Data Technologies	Investigation management software specialized for tracking different types of crimes. www.leadatatech.com

Investigator Report	Vereinigte Staaten von Amerika
MDansby	Full range of case and client management functionality, ideal for investigators, detectives and law enforcement. www.mdansby.com/Software/mdx_page2_InvestigatorReport.html

iTrak	Kanada/ Vereinigte Staaten von Amerika
iView Systems	Highly secure, multi property, multi departmental solution for security, surveillance and risk management departments. www.iviewsystems.com/itrak-incident-reporting-risk-management

Incident Managemant Software	Kanada
Resolver	Resolver's incident management software is an end-to-end, total solution for responding to, reporting on, and investigating incidents. It's an invaluable knowledge base that will help you understand what's happening and why, so that you can manage resources, minimize impact, and prevent incidents. www.resolver.com/incident-management-software

PiMS	Vereinigte Staaten von Amerika
Polonious	Powerful investigation management software for investigation companies and investigation units. Improve your outcomes for your clients. www.poloniouslive.com

Police Investigation Software	Vereinigte Staaten von Amerika
PTS Solutions	Keeps track of all records relating to everything involved in a law enforcement investigation. www.ptssolutions.com/police-software.html

Report Exec	Vereinigte Staaten von Amerika
Competitve Edge Software	Report Exec Professional is a law enforcement and security management incident report writing software package designed to assist organizations in streamlining and optimizing the traditional paper reporting of incidents that occur on a daily basis. www.reportexec.com

Residence Life	Vereinigte Staaten von Amerika
Incident Tracker	Track and investigate inquiries and see the outcome with the click of a button. www.incident-tracker.com

rsCIRS	Deutschland
rola security solutions	Auswertung für Konzernsicherheit und Revision: Die Spanne reicht vom Diebstahl über Markenrechtsverletzungen bis zu Korruptionsfällen in Millionenhöhe und Bilanzmanipulationen. Mit **rs*CIRS*®** unterstützt rola konzernweite Ermittlungen, ermöglicht Datenabgleich, grafische Analysen und Desaster Management, erfüllt die gesetzlichen Auflagen sowohl des Datenschutzes als auch des Anlegerschutzes und enthält zahlreiche Funktionen für ein unkompliziertes Berichtswesen. www.rola.com/produkte.html

SCOUT	Vereinigte Staaten von Amerika
Virtual Advantage	Secure, web-based case management software built for conducting and managing investigations. www.scoutcms.com

Trackops	Vereinigte Staaten von Amerika
Trackops	Web-based case management application helps investigative companies become more organized, efficient, and profitable with less effort. www.trackops.com

VCM	Vereinigte Staaten von Amerika
Virtual Case Management	Paperless database case management solution for investigators, process servers, intelligence analysis and the security industry. www.virtualcasemanagement.com

VideOversight	Vereinigte Staaten von Amerika
Microception	Online video monitoring, recording, archiving and case management tool for law enforcement agencies. www.microception.com/videoversight.php

vSOC	Kanada
D3 Security Management Systems	Web-based solution for incident reporting, investigations management, guard tour, dispatch, and post orders. www.futureshield.com/brochures/D3_VSOC_Brochure_FutureShield.pdf

XIM	Vereinigtes Königreich
Xanalys	Intelligence and investigating platform with a range of advanced data management, workflow, and intelligent indexing features. www.xanalys.com

ASW Bundesverband

Allianz für Sicherheit
in der Wirtschaft e. V.

Neue Schönhauser Straße 20
10178 Berlin

Telefon: +49 (0)30 200 77 200
Telefax: +49 (0)30 200 77 056
info@asw-bundesverband.de

www.asw-bundesverband.de

Bundesverband