

Ein Fallbeispiel: Der Weg zu einem erfolgreichen IT-Risiko- und IT-Sicherheitsmanagement

So viel IT-Sicherheit wie nötig, so effizient wie möglich

Sie als Business- und IT-Verantwortliche stehen oft vor dem Problem, dass Sie nicht genau wissen, ob die Aufwendungen für IT-Sicherheitsmaßnahmen wirklich angemessen sind. Könnten Sie hier noch Kosten sparen oder sind die Unternehmensanwendungen vielleicht sogar noch nicht sicher genug? Und welche operativen Risiken aus dem IT-Einsatz bestehen wirklich? Dieser Artikel zeigt anhand eines Fallbeispiels, wie Sie den Aufwand für IT-Sicherheitsmaßnahmen minimieren und gleichzeitig das IT-Risiko- sowie das IT-Sicherheitsmanagement effizient gestalten können.

Die Anforderungen von Kapital- und Kreditgebern an das Risikomanagement eines Unternehmens werden insbesondere in Zeiten einer Wirtschaftskrise, die unter anderem durch lange unbekannt oder nicht deklarierte Risiken einiger Unternehmen entstanden ist, weiter steigen. Und in Zeiten knapper werdender Budgets lautet die nächste Frage an Sie: Wird die notwendige IT-Sicherheit mit dem geringstmöglichen Aufwand erreicht?

Der erste Schritt in gängigen Vorgehensweisen ist die Ermittlung von Risiken durch die Betrachtung von Schwachstellen und Bedrohungen, die auf IT-Systeme wirken. Aber was bedeutet das für Sie in der Praxis, wenn Ihnen die Sicherheitsanforderungen aus Unternehmenszielen und Geschäftsprozessen nicht bekannt sind? Wie können Sie dann die richtigen Entscheidungen über nötige Investitionen in IT-Sicherheitsmaßnahmen zielsicher treffen? Viele gebräuchliche Methoden des IT-Risikomanagements lassen diese wichtigen Aspekte unberücksichtigt.

Die 5 häufigsten Fehler bei IT-Risikomanagement- und IT-Sicherheitsmanagement-Prozessen

In unserem Fallbeispiel aus einem Großunternehmen offenbarte die Analyse der bestehenden, nicht immer einheitlichen Prozesse fünf kritische und für viele Unternehmen typische Mängel:

Fehler 1: Die Anforderungen an Sicherheitsmaßnahmen wurden häufig zu hoch angesetzt, da eine einheitliche Bemessungsgrundlage und konsequente Unterteilung in Schutzwerte (oder Sicherheitsdimensionen) wie z. B. Vertraulichkeit oder Verfügbarkeit fehlte.

Diese fehlende oder unzureichende Unterteilung in Schutzwerte führte in der Implementierung z. B. dazu, dass Anwendungen mit vertraulichen Daten, automatisch auch hoch verfügbar betrieben wurden. Das erhöhte die Betriebskosten unnötig.

Fehler 2: Es waren keine klaren Verantwortlichkeiten für das Risikomanagement definiert. Das führte dazu, dass Entscheidungen oft von Sachbearbeitern getroffen werden mussten, die dafür weder zuständig noch dazu ausgebildet waren. Diese bestellten dann natürlich lieber mehr Schutz, als zu riskieren, dass eine Anwendung aufgrund ihrer Entscheidung einmal ausfiel. Eine Bewertung der Auswirkungen von Schutzmaßnahmen auf Entwicklungs- und Betriebskosten fand deswegen nicht ausreichend statt.

Fehler 3: Einheitliche Auslöser für die Analyse der Sicherheitsanforderungen waren in der Entwicklungsmethodik nicht definiert. Als Folge wurden Sicherheitsanforderungen oft erst ermittelt, wenn die Entwicklung schon im Gange war oder wenn Aufträge an Software-Lieferanten schon unterschrieben waren. Die Kosten für die dann nachträglich durchzuführenden Sicherheitsmaßnahmen waren viel höher, als dies bei einer frühzeitigen Analyse der Fall gewesen wäre.

Fehler 4: Oft waren die Geschäftsbereiche wohl oder übel gezwungen, hohe Risiken zu akzeptieren, da die Anwendungen dringend benötigt wurden und nachträglich eingebaute Sicherheitsmaßnahmen die Inbetriebnahme verzögert und den Budgetrahmen gesprengt hätten.

Fehler 5: In der IT-Entwicklung wurden zwar Risikoanalysen durchgeführt, aber die Ergebnisse waren für die Geschäftsbereiche meist nicht aussagefähig. Die Formulierungen waren rein technisch oder es wurden Schwachstellen als Risiken aufgeführt, die der Betreiber durch einfache Maßnahmen hätte beseitigen können. Das Ergebnis waren Restrisikodeklarationen, die nicht monetär bewertet worden waren und für die Geschäftsbereiche oft nicht einschätzbar waren. Aus Geschäftssicht brachte der ganze Prozess kaum Nutzen, eine Überarbeitung war dringend erforderlich.

Der Weg zu erfolgreichen IT-Risikomanagement- und IT-Sicherheitsmanagement-Prozessen

In unserem Fallbeispiel wurde nun – ganz entgegen den meisten gängigen Methoden im Risikomanagement – zur Lösung der Situation folgende Methode angewendet: Statt die Risikoanalyse an den Anfang des Prozesses zu setzen, beschäftigte man sich zunächst mit der Ermittlung der Business-Anforderungen an die IT-Sicherheitsmaßnahmen.

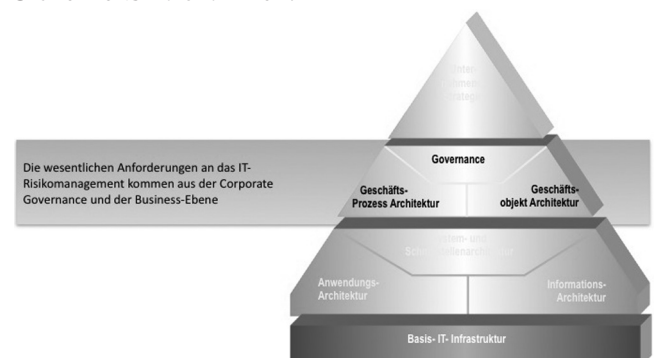


Abb. 1: Quellen der Anforderungen an das IT-Risiko- und -Sicherheitsmanagement

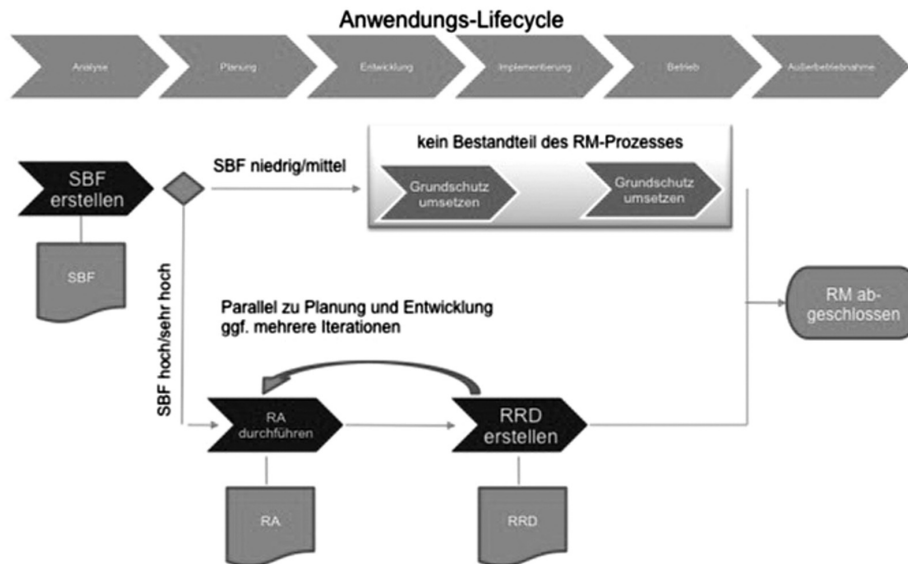


Abb. 2: Risikoanalyse im Anwendungs-Lifecycle

Die Krux dabei: Als natürliche und von allen Beteiligten akzeptierte „Schnittstelle“ zwischen den Geschäftsbereichen und der IT wurden IT-Anwendungen vereinbart. Sie wurden als abstrakte Objekte beschrieben, die einen oder mehrere Geschäftsprozesse ganz oder teilweise unterstützen. Sowohl die Geschäftsbereiche als auch der IT-Dienstleister konnten mit dem neu geschaffenen Geschäftsobjekt „Anwendung“ die Eigenschaften verknüpfen, die für das Management ihrer jeweiligen Prozesse benötigt wurden.

Die Anforderungen an Sicherheitsmaßnahmen wurden nur noch an die Anwendungen gestellt. Verantwortlich für die Anforderungen war eine neu eingeführte Rolle: der Anwendungsverantwortliche im Fach- oder Geschäftsbereich. Die Anforderungen wurden unter Einbindung weiterer Verantwortlicher wie dem zuständigen IT-Sicherheitsmanager des jeweiligen Geschäftsfeldes, den Fachverantwortlichen mitnutzender Geschäftsbereiche und dem IT-Sicherheitsmanager des Konzerns in einer Schutzbedarfsfeststellung verbindlich dokumentiert. Um den Aufwand für die Ermittlung der Anforderungen an IT-Sicherheitsmaßnahmen gering zu halten, wurde eine standardisierte Schutzbedarfsermittlung eingeführt. Diese beinhaltete auch ein Bewertungsschema für die Einstufung der Anforderungen in verschiedene Schutzkategorien. Durch dieses einheitliche Verfahren wurde der Aufwand für die Ermittlung und Dokumentation der Sicherheitsanforderungen für eine Anwendung im Durchschnitt auf unter zwei Stunden reduziert. Auch bei komplexeren Anwendungen mit mehreren mitnutzenden Unternehmensbereichen lag der Zeitbedarf selten über vier Stunden.

Das Ergebnis der Schutzbedarfsfeststellung war eine Einstufung der Sicherheitsanforderungen in die vier Schutzwerte: Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit. Für jeden Schutzwert konnte eine der vier Einstufungen „niedrig“, „mittel“, „hoch“ und „sehr hoch“ gewählt werden. Diese Einstufungen wurden jeweils aus Einstufungen in verschiedenen

Schadenskategorien (Auswirkungen auf Datenschutz, Verstöße gegen Verträge oder Gesetze usw.) gebildet, wobei jede Einstufung mit einer kurzen Beschreibung begründet werden musste.

Das weitere Vorgehen im IT-Risikomanagement wurde nun von der Einstufung der Sicherheitsanforderungen abhängig gemacht. War die Einstufung in keinem der Schutzwerte höher als mittel, wurde die Anwendung mit Standardschutzmaßnahmen implementiert und in Betrieb genommen. War die Einstufung in einem Schutzwert hoch oder sehr hoch, wurde eine formale Risikoanalyse durchgeführt und nur bei Bedarf wurden individuelle Schutzmaßnahmen geplant und implementiert. Nach Abschluss der Entwicklung oder Integration, spätestens aber zum Start des Betriebs einer Anwendung musste eine unterschriebene Dokumentation (Restrisikodeklaration) der Risiken vorliegen, die nicht beseitigt werden konnten oder deren Beseitigung nicht wirtschaftlich war. Jede Anwendungsverantwortliche konnte in Abstimmung mit den Fachverantwortlichen seiner Anwendung entscheiden, welche Risiken er beseitigen und welche er vorübergehend oder dauerhaft akzeptieren wollte. Damit war eine der Hauptanforderungen an das IT-Risiko- und IT-Sicherheitsmanagement, nämlich die Ausrichtung der Sicherheitsmaßnahmen an den Geschäfts- und Unternehmensanforderungen (Business Alignment), erreicht. Das erste Ziel war damit erreicht: Die Risiken im Unternehmen des Fallbeispiels werden seither wirtschaftlich und transparent gemanagt. Das Unternehmen kennt nun seine IT-Risiken und entscheidet daher gemäß den Geschäftsanforderungen. Neben der Schutzbedarfsfeststellung musste auch die Restrisikodeklaration vom Anwendungsverantwortlichen, den beteiligten Fachverantwortlichen sowie dem IT-Sicherheitsmanager des zuständigen Bereichs und dem des Konzerns unterschrieben werden. Da dieses Dokument eine hohe juristische Bedeutung hatte, mussten teilweise auch disziplinarisch Vorgesetzte mit unterschreiben.

Damit war auch das zweite Ziel erreicht: Durch dieses differenzierte und anforderungsgerechte Vorgehen ist eine enorme Aufwandsreduktion erreicht worden. Risikoanalysen werden seither nicht mehr für alle Anwendungen oder gar ganze IT-Landschaften durchgeführt. Dadurch wird dieser Aufwand jetzt nur noch bei den Anwendungen erbracht, die tatsächlich hohe Anforderungen an IT-Sicherheitsmaßnahmen haben. Deutlich mehr als 50 % aller Anwendungen haben höchstens mittlere Sicherheitsanforderungen und können mit Standardschutzmaßnahmen und einem vereinfachten IT-Risikomanagement-Prozess in Betrieb genommen werden. Außerdem ist durch die Analyse der Sicherheitsanforderungen eine relativ einfache Ermittlung von Risiken möglich geworden. Ein Risiko ergibt sich im ersten Ansatz immer aus einer nicht erfüllten Sicherheitsanforderung, wobei natürlich Risiken aus der Integration in die Betriebslandschaft und aus anderen Quellen dazukommen können.

So umgehen Sie die Stolpersteine bei der Umsetzung in der Praxis

In der ersten Zeit nach der Einführung des neuen Prozesses war die geforderte monetäre Bewertung von Risiken die Ursache für viele Diskussionen mit Fachbereichen und IT-Dienstleistern. Anfangs war der Hauptgrund für alle Diskussionen der, dass diejenigen, die die Risikoanalysen durchführten, noch nicht gewohnt waren, aus technischen und organisatorischen Schwachstellen fachlich bewertbare Risiken zu bilden und diese in der Sprache der Fachabteilungen zu formulieren. Für die Anwendungsverantwortlichen aus dem Fachbereich war es beispielsweise eine unlösbare Aufgabe, das Risiko des Ausfalls eines Servers monetär zu bewerten. Nachdem die ausführenden Personen entsprechend in-

formiert und geschult sowie durch einige „Reklamationen“ und Eskalationen wegen nicht vorher abgestimmter Mehraufwendungen sensibilisiert waren, wurde dieses Problem gelöst. Die Fachbereiche konnten die – nun fachlich formulierten – Risiken meist problemlos bewerten. Für Ausnahmen, wie z. B. das Risiko eines Imageverlustes, wurden einfache Lösungen gefunden oder Ausnahmen vereinbart.

Zusammenfassung

Durch die Optimierung der IT-Risiko- und Sicherheitsmanagement-Prozesse wurde mehr Sicherheit bei geringeren Kosten erreicht. Schlüsselfaktoren dazu waren:

- Die Geschäftsanforderungen an Sicherheit zum Ausgangspunkt machen
- Differenzierung der Sicherheitsanforderungen durch Schutzwerte
- Fokussierung des Instrumentes der Risikoanalyse auf Bereiche mit hohen Sicherheitsanforderungen

In einer der folgenden Ausgaben werde ich darauf eingehen, wie der Prozess fest im Unternehmen etabliert wurde, welche Erfahrungen das Unternehmen in der Folge mit dem Prozess gemacht hat und wie man anschließend die Rahmenbedingungen optimiert hat.

Rolf Steinecke
rolf.steinecke@syracom.de

Artikel-ID: THBA

Alle Artikel finden Sie unter
www.managing-it.de