GRC-Tools im IT-Risikomanagement

Die heute anzutreffenden komplexen IT-Landschaften erfordern eine strukturierte Vorgehensweise bei der Analyse von Risiken und der Verwaltung von Gegenmaßnahmen – nur so entstehen Transparenz, Nachvollziehbarkeit und ein klarer Bezug zu Geschäftsprozessen. Governance-, Risk- und Compliance-(GRC)-Werkzeuge sind dabei ein kaum verzichtbares Hilfsmittel.

Von Steffen Gundel, Heilbronn

Jedes Unternehmen ergreift heute unterschiedlichste Sicherheitsmaßnahmen, um sich vor den zahlreichen Bedrohungen zu schützen, die aus dem Einsatz von IT entstehen können – große Unterschiede bestehen aber in der Art und Weise, *wie* diese Maßnahmen ermittelt werden.

In vielen Organisationen wird immer noch ohne vorherige strukturierte Bedrohungsanalyse und ohne ausreichende Einbeziehung der Anforderungen aus den Geschäftsprozessen über Maßnahmen entschieden. Leider bleibt bei dieser „bauchgetriebenen" Vorgehensweise in der Regel unklar, ob die getroffenen Maßnahmen wirklich ausreichend sind, um dem Schutzbedarf gerecht zu werden. Und auch umgekehrt ist unklar, ob alle ergriffenen Maßnahmen tatsächlich notwendig sind oder möglicherweise an der falschen Stelle (zu viel) Geld ausgegeben wurde.

Eines der Ziele eines strukturierten Risikomanagements in der IT ist die transparente und nachvollziehbare Ermittlung von Risiken, die durch den Einsatz von IT entstehen. Nur so kann man dem Management eine solide Entscheidungsgrundlage für die Frage liefern, ob ein Risiko akzeptiert werden kann oder ob man entsprechende Gegenmaßnahmen ergreifen muss – und wie die Umsetzung dieser Maßnahmen zu priorisieren ist. In diesem Ziel ist man sich in der Praxis überall einig, nur die Umsetzung ist oft ein steiniger Weg und mit vielen Problemen behaftet. IT-GRC-Werkzeuge versprechen hier eine Vereinfachung und Qualitätssteigerung.

Bei einer näheren Betrachtung des IT-Risikomanagements in größeren Unternehmen sind häufig zwei Kernprobleme festzustellen: Kaum jemand hat einen Überblick, welche Risiken derzeit „am kritischsten" für den eigenen Bereich oder Geschäftsprozess sind, welche Restrisiken nach der Einführung von Maßnahmen übrig bleiben und wer diese Restrisiken akzeptiert und damit die Verantwortung dafür übernommen hat – es fehlt also an Transparenz und Nachvollziehbarkeit. Darüber hinaus erfolgt die Erfassung der benötigten Informationen wie das Sammeln möglicher Bedrohungen, Schadenshöhen oder auch nur etablierter Maßnahmen oft sehr zeitaufwändig und ineffizient.

Viele Köche

Eine Ursache hierfür ist unbestritten die hohe Komplexität moderner IT-Landschaften. Viele weitere Ursachen sind jedoch „hausgemacht": Beispielsweise arbeiten verschiedene Bereiche oder Abteilungen, die Risiken betrachten, im Unternehmen meist völlig unabhängig voneinander. Dies führt dann dazu, dass diese Bereiche – etwa IT-Sicherheit, Revision, Internal Audit oder auch Fachabteilungen – eigenständig Daten erfassen, mit eigenen Methoden Überprüfungen durchführen beziehungsweise Risiken ermitteln, dafür eigene Werkzeuge verwenden und anschließend jeweils individuell aufgebaute Berichte erstellen. Neben einer mangelnden Vergleichbarkeit der Ergebnisse ist diese Vorgehensweise auch sehr ineffizient, da häufig dieselben Objekte (z. B. Applikationen) betrachtet und dementsprechend die zuständigen Personen (z. B. Applikationsverantwortliche) mehrfach befragt werden, wodurch zudem auch ein redundanter Datenbestand entsteht.

Ein weiteres, verbreitetes großes Problem bei der Durchführung von Risikoanalysen ist die Verwendung hierfür völlig ungeeigneter Werkzeuge, allem voran Excel. Solche Tools unterstützen beispielsweise keine workflowgestützte Vorgehensweise mit mehreren beteiligten Gruppen und individuellen Sichten auf die Daten (von einer granularen Vergabe von Berechtigungen oder einer Nach-

vollziehbarkeit von Änderungen ganz zu schweigen) und führen zu einer Unmenge von Dateien auf dem Fileserver des jeweiligen Bereichs, die man – wenn überhaupt – nur sehr schwer übergreifend auswerten kann.

Problematisch ist auch die häufig anzutreffende fehlende ganzheitliche Betrachtung bei Risikoanalysen, was letzten Endes zu einer unzureichenden Risikotransparenz führt: Für einzelne Objekte finden zwar Risikobetrachtungen statt, jedoch endet die Betrachtung entsprechend der Zuständigkeit der Abteilung. Beispielsweise analysiert der IT-Betrieb nur die technische Systemebene, aber nicht die Auswirkungen der erkannten Risiken auf die im System betriebenen Applikationen. Die Fachabteilung wiederum betrachtet zwar die Applikationen, bezieht aber die Analysen des IT-Betriebs nicht ein und übergeht außerdem die Auswirkungen „ihrer" Risiken auf die Geschäftsprozesse, die von den Applikationen abhängig sind.

Viele dieser Probleme können heute mit dem Einsatz so genannter Governance-, Risk- und Compliance-(GRC)-Werkzeuge gemindert oder gar vollständig beseitigt werden. Derartige Werkzeuge haben das Ziel, die verschiedenen Teilprozesse und Aufgabenbereiche innerhalb eines Informationssicherheits-Managementsystems (ISMS) zu unterstützen – beispielsweise das IT-Risikomanagement, um dadurch Transparenz und Nachvollziehbarkeit zu schaffen und eine effiziente Durchführung zu ermöglichen.

Auch außerhalb der IT existieren sehr viele weitere Anwendungsgebiete für GRC-Werkzeuge: Überall dort, wo im Unternehmen Risiken betrachtet werden oder Compliance ein Thema ist, kann der Einsatz von GRC-Werkzeugen sinnvoll sein, beispielsweise im Finanz-Risikomanagement oder im unternehmensweiten Risikomanagement.

Die beiden großen US-Marktforscher Gartner und Forrester unterscheiden bei GRC zwischen den Marktsegmenten Enterprise GRC und IT-GRC, jedoch sind die Grenzen in der Praxis oft fließend. IT-GRC-Werkzeuge sind speziell auf das Informationssicherheitsmanagement (ISM) ausgerichtet und verfügen häufig über technische Schnittstellen in die IT. Einige dieser Werkzeuge sind aufgrund ihrer Architektur jedoch so flexibel, dass sie beispielsweise auch im Enterprise-Risk-Management eingesetzt werden.

Im Rahmen dieses Artikels wird die grundsätzliche Funktionsweise von IT-GRC-Lösungen am Beispiel des IT-Risikomanagements beschrieben. Viele Produkte bieten jedoch über das Risikomanagement hinaus gehende Möglichkeiten, beispielsweise Unterstützung im Compliance-Management oder bei der Verwaltung von Sicherheitspolicies. Bei Letzterem unterstützen die Produkte häufig das Versionsmanagement, die nachvollziehbare Verteilung der Policies an Endbenutzer oder die Verwaltung und Dokumentation von Policy-Ausnahmen.

Bestandsaufnahme

Bevor man das IT-GRC-Werkzeug seiner Wahl für die Unterstützung von Risikoanalysen sinnvoll einsetzen kann, müssen die im Rahmen der Analysen zu betrachtenden Objekte einmalig im System hinterlegt oder aus anderen Datenbanken (z. B. der Configuration-Management-Database, CMDB) importiert werden. Je nach Unternehmensorganisation, Aufgabenstellung und Betrachtungstiefe kann es sich bei den Objekttypen zum Beispiel um Gebäude, IT-Systeme, Applikationen, Geschäftsprozesse oder ganze Lokationen handeln.

Die Produkte bieten in der Regel zusätzlich die Möglichkeit, die verschiedenen Objekte hierarchisch miteinander in Beziehung zu setzen: Beispielsweise könnte man auf der obersten Betrachtungsebene die Geschäftsprozesse anordnen – diesen werden dann die sie jeweils unterstützenden Anwendungen untergeordnet und den Anwendungen wiederum die IT-Systeme zugeordnet, auf denen die Anwendungen betrieben werden. Auf diese Weise entstehen hierarchische oder Netz-Strukturen, die es dem Werkzeug später beispielsweise ermöglichen, Risiken von IT-Systemen zu Anwendungen und von Anwendungen bis „ganz nach oben" zu den Geschäftsprozessen zu aggregieren und so den Geschäftsprozessverantwortlichen und dem Management das Gesamtrisiko zu verdeutlichen. In umgekehrter Richtung könnten zum Beispiel die Ergebnisse aus der Schutzbedarfsfeststellung für den Geschäftsprozess automatisch nach „unten" auf die Anwendungen und IT-Systeme vererbt und so in die Risikoberechnung mit einbezogen zu werden.

Baseline-Ansatz

Die unterschiedlichen Ansätze zur Ermittlung von IT-Risiken, wie sie beispielsweise im TR ISO/IEC 13335-3 „Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security" beschrieben sind, spiegeln sich auch in den am Markt verfügbaren IT-GRC-Lösungen wider. So gibt es Produkte, die ausschließlich die so genannte Baseline-Vorgehensweise unterstützen – die IT-Grundschutzvorgehensweise des BSI ist ein Paradebeispiel für den Baseline-Ansatz. Bei dieser Methodik wird im Rahmen so genannter Control-Assessments zunächst der Umsetzungsgrad von Sicherheitsmaßnahmen (Controls) aus einem vorgegebenen Maßnahmenkatalog – der so genannten Baseline – ermittelt.

Die Hersteller von IT-GRC-Lösungen liefern meist fertige Maßnahmenkataloge mit, die sich beispielsweise an den Controls aus den ISO-Standards 27001/27002 oder an den CobiT Control-Objectives orientieren. Grundsätzlich ist es aber auch möglich, eigene Kataloge zu hinterlegen, zum Beispiel die Maßnahmen der IT-Grundschutzkataloge oder unternehmensspezifische Maßnahmenkataloge – etwa Vorgaben aus einer internen Sicherheitsrichtline oder im technischen Bereich die Maßnahmen aus einer Härtungsanleitung.

Nach Auswahl der zu betrachtenden Maßnahmen lässt sich der Umsetzungsgrad bei den meisten Produkten dann entweder in Interviewform über elektronische Fragenkataloge ermitteln oder durch Auswahl eines konkreten Umsetzungsgrads direkt angeben.

Auf der technischen Ebene von IT-Systemen bieten einige Produkte zusätzlich die Möglichkeit, den Umsetzungsgrad der Maßnahmen automatisiert zu ermitteln: Hierzu meldet sich das IT-GRC-Werkzeug mit einem hinterlegten Benutzernamen am Betriebssystem an und fragt für jede Maßnahme des Katalogs über ein jeweils hinterlegtes Skript bestimmte Systemparameter ab (z. B. den Wert eines Registry-Keys). Anhand dessen ermittelt das Tool dann den Umsetzungsgrad der Maßnahme und berechnet gegebenenfalls einen Risikoindex, der ein Maß für den Grad der Nichtumsetzung darstellt.

Hersteller, die für das Risikomanagement ausschließlich den hier beschriebenen Baseline-Ansatz unterstützen, kommen historisch meist aus dem Compliance-Umfeld. Die Ermittlung des Umsetzungsgrads von Vorgaben beziehungsweise Maßnahmen ist ja gerade die Kernaufgabe im Compliance-Management und die zusätzliche Ermittlung eines Risikoindex' erlaubt es den Herstellern das Produkt dann auch als Risikomanagement-Werkzeug zu vermarkten.

Detaillierte Risikoanalyse

Andere GRC-Lösungen unterstützen zusätzlich die in deutschen und europäischen Unternehmen verbreitete detaillierte Risikoanalyse in Anlehnung an den Standard ISO/IEC 27005, bei der – stark vereinfacht – zunächst Bedrohungen ermittelt und anschließend bewertet werden.

Produkte, die diesen Ansatz unterstützen, arbeiten grundsätzlich wie folgt: Aus einem im Produkt hinterlegten Bedrohungskatalog werden zunächst die für das betrachtete Objekt relevanten Bedrohungen ausgewählt. Auch hier liefern die Hersteller in der Regel fertige Kataloge mit, beispielsweise basierend auf den im Anhang C der ISO/IEC 27005 enthaltenen Bedrohungen – selbstverständlich kann man auch hier eigene Kataloge entwickeln und hinterlegen.

Im nächsten Schritt ermöglicht das GRC-Werkzeug die Bewertung der Bedrohungen, beispielsweise im Hinblick auf den möglichen resultierenden Schaden und die Wahrscheinlichkeit für ein Schadensereignis. Die jeweiligen Werte können dabei vom Anwender wie bei den oben beschriebenen Control-Assessments entweder direkt aus einer Auswahlliste ausgewählt oder anhand eines Fragenkatalogs in Interviewform ermittelt werden.

Anschließend berechnet das Tool über hinterlegte Formeln das für die Bedrohung resultierende Risiko. Viele Produkte geben hier eine starre, nicht durch den Anwender anpassbare Berechnungsmethodik vor (z. B. Produkt von Eintrittswahrscheinlichkeit und Schaden), andere wiederum sind aufgrund ihrer Architektur so flexibel, dass man beliebige Formeln hinterlegen kann und somit die Abbildbarkeit der im Unternehmen eingesetzten Methodik zur Risikoermittlung sichergestellt ist.

Sind die Risiken bekannt, erfolgt im nächsten Schritt über die bereits angesprochenen Control-Assessments die Ermittlung des Umsetzungsgrads von Gegenmaßnahmen. Die Auswahl der zum Risiko „passenden" Maßnahmen kann dabei ebenfalls durch das Werkzeug unterstützt werden, da in vielen Produkten die Bedrohungen des Bedrohungskatalogs mit den Maßnahmen

des Maßnahmenkatalogs verknüpfbar sind – somit kann das Tool für jedes relevante Risiko einen Maßnahmenvorschlag präsentieren. In umgekehrter Richtung ermöglicht die Verknüpfung beispielsweise, dass das Werkzeug in Abhängigkeit vom ermittelten Umsetzungsgrad der Maßnahmen eine automatische Neuberechnung des (Rest-) Risikos vornehmen kann.

Sämtliche Arbeitsschritte einer Risikoanalyse werden durch ein GRC-Tool in ihrer Reihenfolge gesteuert: Durch die Möglichkeit zur Abbildung von Workflows lassen sich unterschiedliche Aufgaben an unterschiedliche Rollen oder Personen zur Umsetzung delegieren. Beispielsweise könnte die IT-Revision mit dem Werkzeug ein Control-Assessment initiieren und die für sie interessanten Maßnahmen auswählen; anschließend delegiert die IT-Revision die Beantwortung der Fragen zur Ermittlung des Umsetzungsgrads dieser Maßnahmen an den IT-Betrieb. Die entsprechenden Mitarbeiter würden vom Werkzeug über die anstehende Aufgabe per E-Mail benachrichtigt beziehungsweise nach der Anmeldung am Tool in ihrem persönlichen Aufgabenbereich die Aufgabe angezeigt bekommen. Nach Beantwortung der Fragen würde das Werkzeug dann automatisch wieder die IT-Revision informieren, welche daraufhin beispielsweise die Antworten prüft.

Darüber hinaus sind GRC-Werkzeuge mandantenfähig, sodass unterschiedliche Rollen oder Personen mit jeweils individuellen Sichten mit dem Werkzeug arbeiten können. Die Produkte verfügen zudem über ein granulares Berechtigungsmodell zur Steuerung des Zugriffs auf die meist sensitiven Informationen.

Projektmaßnahmen

Sind die Risiken ermittelt worden, muss man im nächsten Schritt für jedes Risiko entscheiden, ob es vom Management getragen oder durch geeignete Aktivitäten auf ein akzeptables Maß gemindert werden soll. GRC-Tools ermöglichen in dieser Phase unter anderem die Dokumentation dieser Entscheidungen sowie die Verwaltung der beschlossenen Projektmaßnahmen zur Risikominderung. Darüber hinaus unterstützen sie meist auch deren Verteilung an den verantwortlichen Personenkreis, ähnlich eines Ticketing-Systems – gängige Funktionen sind etwa die Pflege des Erledigungsstatus oder eine automatische Erinnerung vor Fälligkeit der Aufgabe.

Eine wichtige Komponente in GRC-Produkten ist zudem die Auswertung und Aufbereitung der durchgeführten Risikoanalysen: Ziel ist dabei, allen im Risikomanagement-Prozess beteiligten Rollen und Personen jederzeit die Ergebnisse im jeweils benötigten Detaillierungsgrad zu liefern. Bei den meisten Herstellern sind einige Standardreports im Lieferumfang enthalten, die man jedoch typischerweise noch an das jeweilige Einsatzfeld anpassen oder komplett neu entwickeln muss. Einige Hersteller bieten darüber hinaus Schnittstellen für den direkten Zugriff auf die Datenbasis, sodass beliebige Auswertungen durchgeführt und Reports erstellt werden können.

Die eingangs beschriebene Verknüpfung der verschiedenen Objekte zu einer hierarchischen Struktur oder einer Netzstruktur ermöglicht darüber hinaus übergreifende Auswertungen. Beispielsweise können die in den einzelnen Risikoanalysen erkannten Risiken entlang der Hierarchie nach oben propagiert und somit Gesamtrisiken für Geschäftsprozesse transparent gemacht werden. Auf dieser Basis lässt sich dann für die Geschäftsprozessverantwortlichen oder für das Management jederzeit ein aussagekräftiger Bericht zum Risikostatus erstellen.

Fazit

Heutige IT-GRC-Lösungen bieten ein großes Potenzial zur Erhöhung der Nachvollziehbarkeit, Transparenz und Effizienz im Informationssicherheitsmanagement. Alle Risiken sind damit an zentraler Stelle nachvollziehbar dokumentiert und das Management erhält eine fundierte Grundlage, um Aktivitäten zur Risikobehandlung sinnvoll zu priorisieren. Aufgrund der im Werkzeug vorgenommenen Verknüpfung zwischen den bestehenden Objekten können Risiken entlang der Hierarchie nach oben propagiert und somit zum Beispiel Risiken für einen bestimmten Geschäftsprozess „auf Knopfdruck" transparent gemacht werden. Es besteht somit für jede Zielgruppe die Möglichkeit, sich einen aktuellen Statusüberblick über die Risikosituation oder die vereinbarten Maßnahmen zu verschaffen.

Um diesen Mehrwert tatsächlich zu erzielen, ist eine sorgfältige Produktauswahl erforderlich; die Produkte unterscheiden sich in ihrem Funktionsumfang und „Reifegrad" teils erheblich. Ein weiterer entscheidender Unterschied zwischen den Produkten ist ihre Anpassbarkeit an die eigene Methodik und Vorgehensweise: Während viele Tools feste Formeln zur Risikobewertung vorgeben oder beispielsweise keine Erweiterung der drei Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität zulassen, kann man in anderen Produkten beliebige Formeln und Berechnungslogiken hinterlegen. Die Praxis zeigt, dass am Ende eines Auswahlprozesses fast immer eines der zuletzt genannten flexiblen Produkte zum Einsatz kommt – schließlich soll sich das Werkzeug an die Vorgehensweise des Unternehmens anpassen und nicht umgekehrt. ■

Steffen Gundel ist Leitender Berater bei der cirosec GmbH.