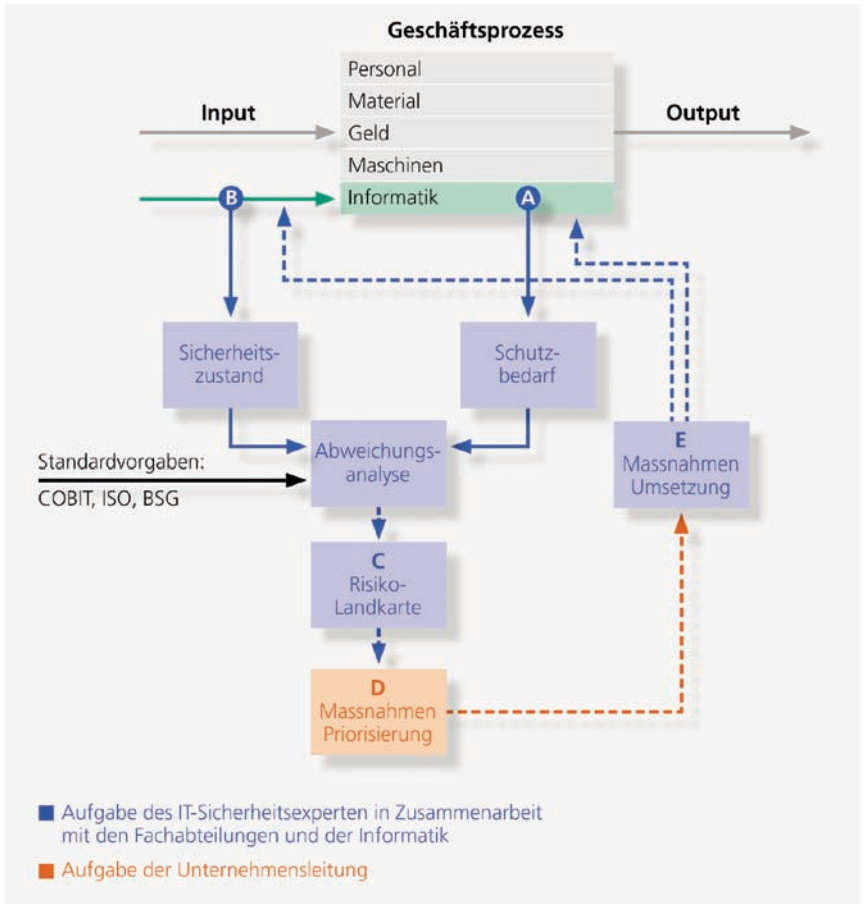
Finanzen: Investitionen in die IT-Sicherheit

Wirtschaftlichere IT-Sicherheitsinvestitionen durch Kenntnis der Anforderungen der Geschäftsprozesse



Das A und O für gezielte IT-Sicherheitsinvestitionen ist die Ermittlung der effektiven Schutzbedarfsanforderungen der Geschäftsprozesse. Mittels eines Risikodialoges mit den Prozessverantwortlichen wird die Frage beantwortet, wie lange die Organisation ohne Informatik weiterarbeiten kann, ohne dass grössere Auswirkungen auf das Kerngeschäft und/oder die Kunden hingenommen werden müssen.

Text: Martin Dietrich und Roman P. Büchler

IT-Sicherheit ist mittlerweile zu einem ständigen Thema in IT- und Management-Fachzeitschriften geworden. Dadurch hat sich das Informatik-Sicherheits-Bewusstsein des Managements aber auch der Mitarbeitenden erhöht. Doch die Ermittlung, wieviel Sicherheit tatsächlich notwendig ist und welche konkreten Massnahmen implementiert werden sollen ist nach wie vor keine leichte Aufgabe. Die oft zitierten Standards helfen in der praktischen Anwendung nicht viel weiter: Entweder sind sie nicht umfassend genug (ISO 27002, vormals 17799[1]), zu allgemein gehalten (COBIT Version 4[2]) oder zu detailliert (Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnologie[3]).

Vom Schutzbedarf über den Sicherheits-Ist-Zustand...

Mittels des Risikodialogs wird den Geschäftsprozessverantwortlichen ermöglicht, den Schutzbedarf, also die Anforderungen an die Informatiksicherheit sowie die Anforderungen an die Geschäftsprozesskontinuität, zu benennen, ohne dass sie sich mit der Technik direkt auseinandersetzen müssen. Im Risikodialog beantworten Geschäftsprozesseigentümer Fragen nach der Wirkung von Fehlern und Unterbrüchen im Geschäftsprozess. Damit werden die Verantwortlichen abgeholt, wo sie sich auskennen: Bei der täglichen Arbeit. Die Ursache der Fehler kann (muss aber nicht) in der Informatik liegen. Entsprechend der Schwere der Auswirkungen kann nun abgeleitet werden, wie hoch die Anforderungen an die Informatiksicherheit sind. Diese Anforderungen werden in den vier Sicherheitsdimensionen Verfügbarkeit, Datenexistenz, Integrität (Richtigkeit) und Vertraulichkeit ausgewiesen.

Durch den Einsatz von Ausprägungen («wie lange funktioniert der Geschäftsprozess nicht?», bzw. «welcher Teil der Informatik funktioniert nicht?») kann gleichzeitig der Schadenverlauf aufgezeigt werden.

> *„Investitionen in die IT-Sicherheit gehören auf ein sinnvolles Niveau"*

Ein IT-Sicherheitsaudit mittels Kontrollfragen und Interviews mit den Informatikverantwortlichen sowie Inspektionen vor Ort (Rechenzentrum, Dokumentation, Büroräumlichkeiten etc.) gibt Aufschluss über den Sicherheits-Ist-Zustand der Informatik.

Die Kontrollfragen beziehen sich auf Aspekte der Einzelkomponenten des Systems. Die Sicherheits-Ist-Zustände gleicher Einzelkomponenten lassen sich innerhalb eines Unternehmens oder mit anderen Unternehmen vergleichen.

...zum Sicherheits-Soll-Zustand...

Aus dem Schutzbedarf, der mittels des beschriebenen Risikodialogs ermittelt wurde, kann der Sicherheits-Soll-Zustand abgeleitet werden. Dieser wird nun auf die einzelnen Komponenten der Informatik adaptiert. Der Sicherheits-Soll-Zustand sagt aus, wieviel Sicherheit vom System, bzw. von den Einzelkomponenten produziert werden muss, um den Schutzbedarf aller Geschäftsprozesse, die von den Einzelkomponenten bedient werden, befriedigen zu können.

Dieses Vorgehen ermöglicht einen aussagekräftigen Vergleich zwischen dem Schutzbedarf (Soll) und dem Sicherheitszustand (Ist).

...und zur Grundversorgung

Fragen zu den zentralen Themen der Grundversorgung (Kontinuitäts- und Katastrophenvorsorge) müssen aus den Resultaten des Risikodialogs beantwortet werden. Dadurch sind die Geschäftsprozessverantwortlichen in der Lage, ihrem Informatik-Dienstleister (in-house oder Outsourcer) die Anforderungen an die Grundversorgung zu formulieren. Dabei ist es wichtig, dass das «WAS» (wo ist wieviel Sicherheit notwendig), aber nicht das «WIE» (mit welchen Sicherheitsmassnahmen) vorgegeben wird. Dies ist deshalb entscheidend, weil (fast) jede Grundversorgung mit unterschiedlichen Massnahmenbündeln erreicht werden kann. Die Wahl, mit welchen Mitteln eine bestimmte, von den Geschäftsprozessverantwortlichen geforderte, Grundversorgung tatsächlich erreicht werden soll, soll in der Kompetenz (und Verantwortung) des Informatik-Dienstleisters bleiben.

> *„Wie hoch sind die Anforderungen an die Informatiksicherheit?"*

Sicherheit gehört in die Projekte

Mit den heute vorhandenen technischen Mitteln ist es möglich, Ausfall- und Datenverlustzeit gegen Null zu bringen. Die dazu notwendigen Massnahmen sind aber mit den entsprechenden Investitionen verbunden, die sich allerhöchstens in Hochsicherheitsbereichen vernünftig begründen lassen. Damit die Investitionen in die Informatiksicherheit auf einem sinnvollen Niveau bleiben können, ist es unumgänglich, die Sicherheitsaspekte nicht nur auf der technischen, sondern auch auf der organisatorischen Seite zu berücksichtigen.

Wenn organisatorische Massnahmen zu tieferen Anforderungen an die Informatikgrundversorgung führen, führt dies automatisch zu tieferen Investitionen in die technischen Massnahmen. Es muss also die optimale Aufteilung zwischen organisatorischen und technischen Massnahmen gefunden werden. Meistens ist die nachträgliche Implementierung organisatorischer und technischer Massnahmen sehr schwierig und teuer. Entsprechend hoch fallen deshalb die Informatik-Budgets aus. Die Lösung für dieses Problem ist, die Anforderungen an die Informatiksicherheit von Anfang an in die Projekte einzubauen. Der Risikodialog muss also bereits während des Erstellens der Pflichtenhefte geführt werden, auch wenn die Aussagen zu diesem Zeitpunkt erst aufgrund von Erwartungen gemacht werden können.

Autorenportrait

Martin Dietrich studierte Informationsmanagement (lic.oec.HSG, CISA). Er ist Partner in der BSG Unternehmensberatung, St. Gallen und leitet die Entwicklung der BSGITSEC ToolBox®.

Roman P. Büchler ist Berater in der BSG Unternehmensberatung St. Gallen. Er ist Dozent an der Wirtschaftsinformatikschule Schweiz (WISS) für IT-Risikomanagement.

Siehe dazu:
[1] http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf
[2] www.isaca.org
[3] www.bsi.de