Wieviel Redundanz brauchen wir?

IT-Sicherheitsaudits überprüfen ein Unternehmen auf ihren aktuellen Sicherheitszustand in der Informatik. Ein IT-Sicherheitsaudit kann aber die Frage nicht beantworten, wieviel Redundanz notwendig ist. Dazu ist mittels eines Risikodialoges die Frage zu beantworten, wie lange das Unternehmen ohne Informatik weiterarbeiten kann, ohne dass grössere Auswirkungen auf das Kerngeschäft und/oder die Kunden hingenommen werden müssen.

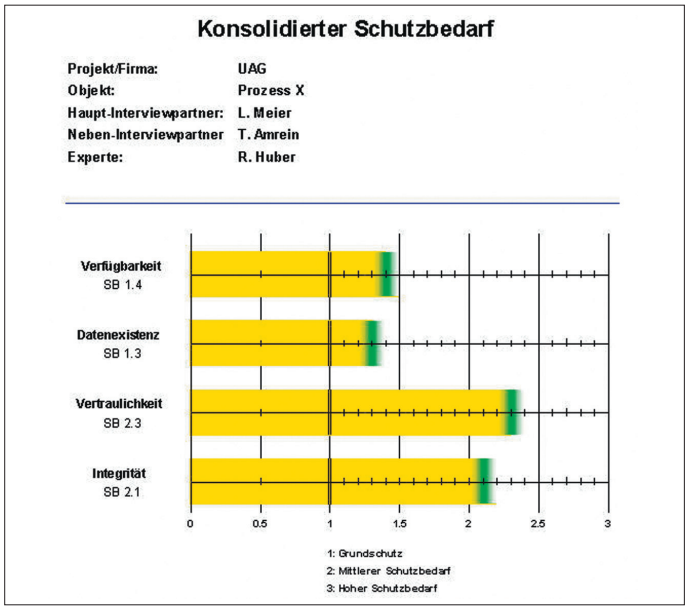
VON MARTIN DIETRICH

IT-Sicherheit ist mittlerweile zu einem ständigen Thema in IT- und Management-Fachzeitschriften geworden. Dadurch hat sich das Informatik-Sicherheits-Bewusstsein der Hauptverantwortlichen (Verwaltungsrat und Geschäftsleitung) aber auch der Mitarbeiter erhöht. Wenn es aber darum geht, herauszufinden, wieviel Sicherheit notwendig ist und welche konkreten Massnahmen implementiert werden sollen, tut man sich schwer, denn auch die oft zitierten Standards helfen in der praktischen Anwendung nicht viel weiter: Entweder sind sie nicht umfassend genug (ISO 17799[1]), zu allgemein gehalten (COBIT 3rd Edition[2]) oder zu detailliert (Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnologie[3]). Die BSG arbeitet mit einer selbst entwickelten und in der Praxis bewährten integrierten Sicherheitsmethodik, die inhaltlich mit ISO 17799 und CoBIT 3rd Edition abgeglichen ist, aber zusätzlich konkrete Handlungsanweisungen enthält.

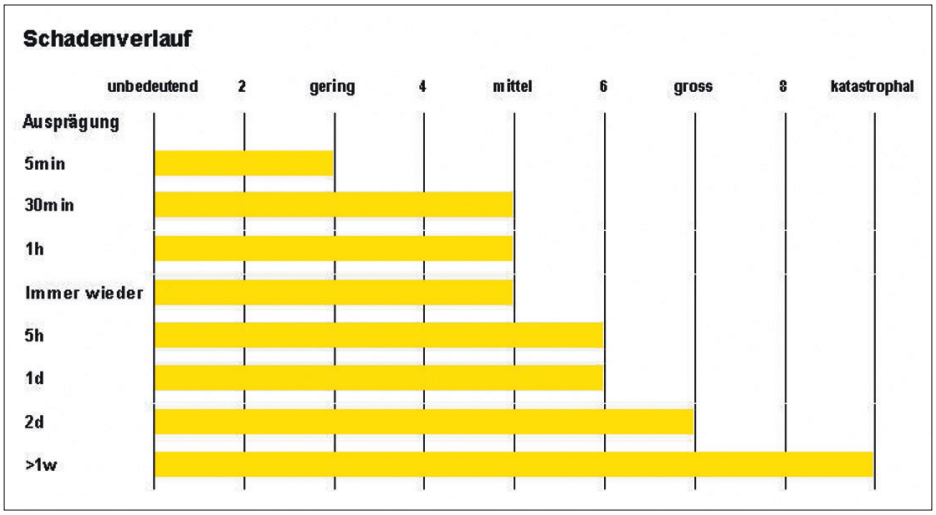
Vom Risikodialog...

Mittels des Risikodialogs wird den Geschäftsprozessverantwortlichen (Process Owners) ermöglicht, den Schutzbedarf, also die Anforderungen an die Informatiksicherheit sowie an die Grundversorgung (Kontinuitäts- und Katastrophenvorsorge), 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 zu einem Wert konsolidiert.

Durch den Einsatz von Ausprägungen («wie lange funktioniert der Geschäftsprozess nicht?», oder «welcher Teil der Informatik funktioniert nicht?») kann gleichzeitig der Schadenverlauf aufgezeigt werden. Während für den normalen Betrieb die Wahrscheinlichkeit eines entsprechend lange anhaltenden oder umfassenden Problems miteinbezogen werden muss, darf für die Anforderungen an die Grundversorgung (Kontinuitäts- und Katastrophenvorsorge) die Wahrschein-



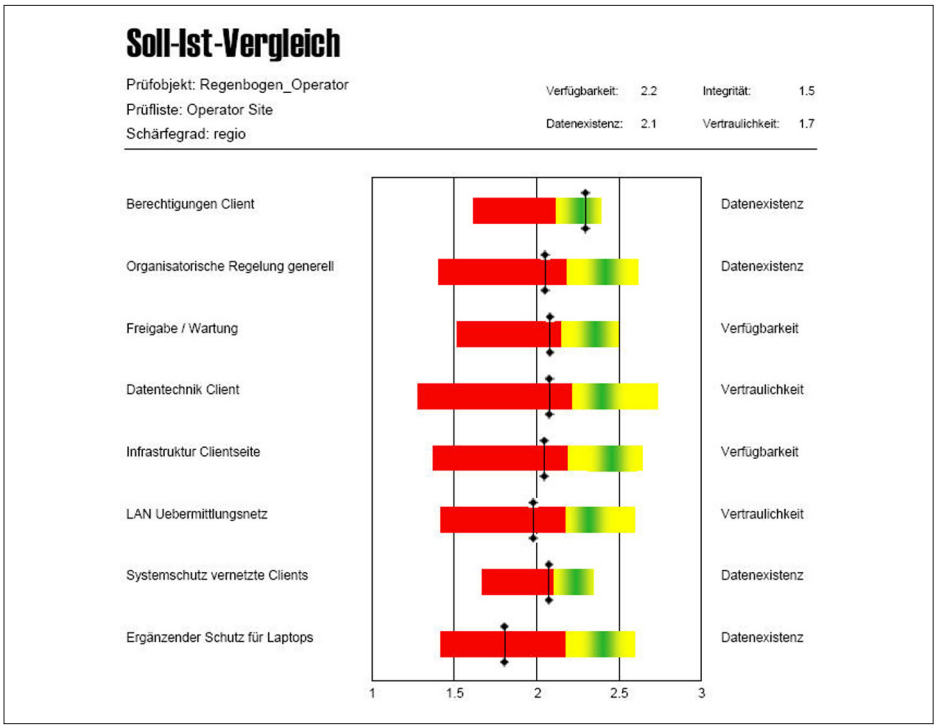
Die Anforderungen werden in vier Sicherheitsdimensionen zu einem Wert konsolidiert.



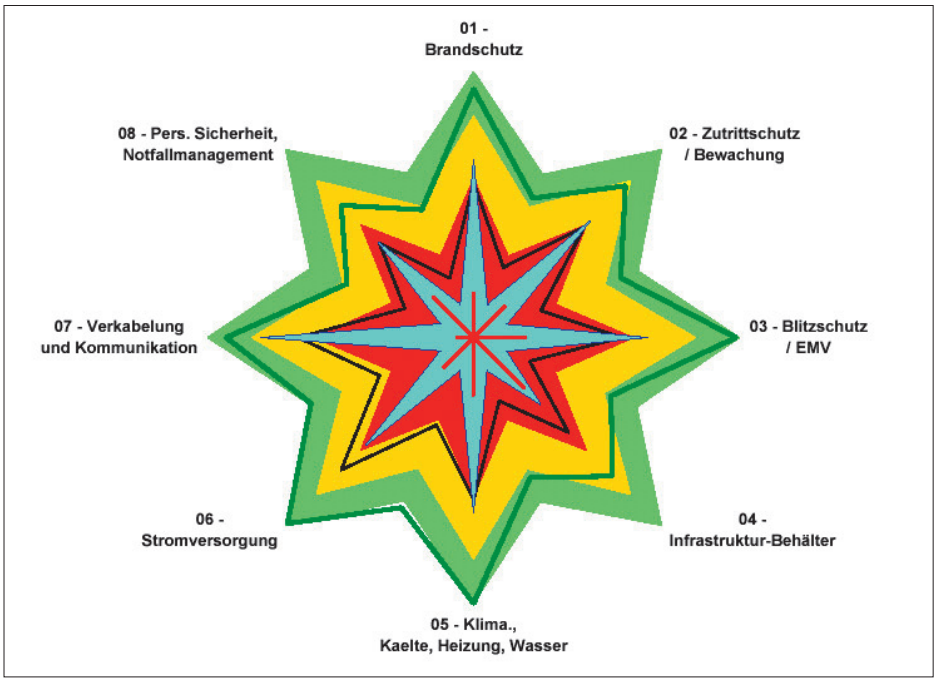
Die Anforderungen an die Grundversorgung müssen immer gewährleistet werden.

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

Martin Dietrich
lic.oec.HSG, CISA, studierte Informationsmanagement. Er leitet die Entwicklung der BSG ITSEC ToolBox der BSG Unternehmensberatung St.Gallen, führt Sicherheitsaudits durch und ist Projektleiter.



Aussagekräftiger Vergleich zwischen Soll- und Ist-Zustand.



Unternehmensübergreifendes Benchmarking des Sicherheits-Ist-Zustandes.

lichkeit nicht beachtet werden, da diese immer gewährleistet werden muss.

...zum Sicherheits-Soll-Zustand, Benchmarking...

Aus dem Schutzbedarf, der mittels des beschriebenen Risikodialogs ermittelt wurde, kann der Sicherheits-Soll-Zustand abgeleitet werden. Dieser wird allerdings nicht mehr auf der Ebene der Geschäftsprozesse, sondern bei den einzelnen Komponenten des Systems produziert. Unter System verstehen wir in diesem Zusammenhang das Zusammenspiel von Infrastrukturen (z.B. Gelände, Gebäude, Büroräume, Rechenzentren), Kommunikationseinrichtungen (z.B. WAN, MAN, LAN, Telefonie), Servern, Operatoren (Administratoren) und Anwendern. Der Sicherheits-Soll-Zustand sagt aus, wieviel Sicherheit vom System, beziehungsweise von den erwähnten Einzelkomponenten produziert werden muss, um den Schutzbedarf aller Geschäftsprozesse, die von den Einzelkomponenten bedient werden, befriedigen zu können. Der Sicherheits-Ist-Zustand wird mittels Kontrollfragen (Controls) ermittelt. Die Kontrollfragen beziehen sich auf Aspekte der Einzelkomponenten des Systems. Jeder Kontrollfrage sind drei verschiedene mögliche Zustände (Antworten) zugeordnet:

► **Grundschutz:** Als Grundschutz akzeptierte Massnahmen sind implementiert

► **Hoher Schutz:** Der Grundschutz wurde übertroffen

► **Ungenügender Schutz:** Der Grundschutz wurde verfehlt

Der Einfluss jeder Kontrollfrage auf die vier Sicherheitsdimensionen Verfügbarkeit, Datenexistenz, Integrität und Vertraulichkeit ist in den eingesetzten Tools hinterlegt und wird dazu verwendet, einen aussagekräftigen Vergleich zwischen dem Sicherheits-Soll- und dem Sicherheits-Ist-Zustand zu ziehen. Ebenso lassen sich die Sicherheits-Ist-Zustände gleicher Einzelkomponenten innerhalb eines Unternehmens oder mit anderen Unternehmen vergleichen. Damit können die Forderungen von CoBIT und ISO erfüllt werden, die das Benchmarking des Sicherheits-Ist-Zustandes empfehlen, aber selber keine Möglichkeit dazu bieten, da sie keine Grundlage für eine vergleichbare Messung (konkrete Massnahmen, um den Grundschutz zu erreichen) vorgeben.

...und zur Grundversorgung

Ein Sicherheitsaudit, also eine Ueberprüfung des aktuellen Sicherheitszustandes, kann nur die Art und Weise der Erfüllung einer Kontrollfrage («Ist eine Brandfrüherkennung implementiert?») beantworten. Fragen zu den zentralen Themen der Grundversorgung (Kontinuitäts- und Katastrophenvorsorge) können aber per Definition nicht beantwortet werden.

Diese Fragen müssen aus den Resultaten des Risikodialogs beantwortet werden. Namentlich auf Basis des «Konsolidierten Schutzbedarfs» und des «Schadenverlaufs» sind die Geschäftsprozessverantwortlichen in der Lage, ihrem Informatik-Provider (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) verlangt wird. Dies ist deshalb entscheidend, weil fast jede Menge Grundversorgung mit unterschiedlichen Mitteln (Massnahmenbündeln) erreicht werden kann. Die Wahl, mit welchen Mitteln eine bestimmte, von den Geschäftsprozessverantwortlichen geforderte, Grundversorgung tatsächlich erreicht werden soll, bleibt in der Kompetenz (und Verantwortung) des Informatik-Providers.

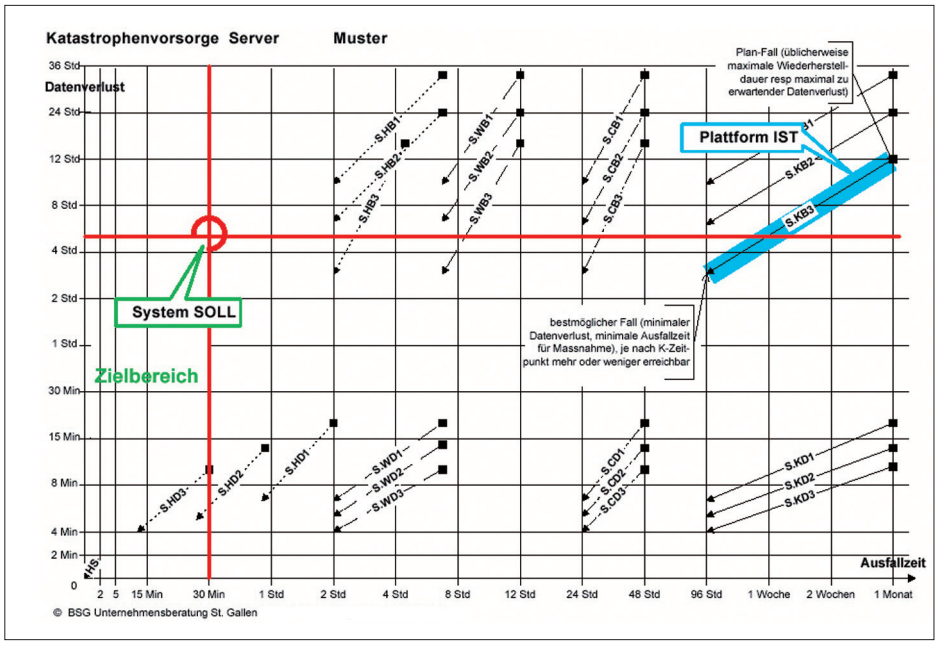
Bezüglich den Anforderungen, die an die Informatik-Provider zu stellen sind, unterscheidet die BSG zwischen zwei Anforderungstypen:

► **Systemdesign:** Verlangt gewisse grundlegende technischen und organisatorischen Sicherheitsmassnahmen und Vorkehrungen

► **Technische Ausführungen:** Zeigen auf, welche technischen Massnahmen möglich sind, um die Anforderungen erfüllen zu können.

Systemdesign

Der Konsolidierte Schutzbedarf in den Dimensionen Verfügbarkeit, Datenexistenz, Integrität und Vertraulichkeit ist



der Ausgangspunkt für die Festlegung der grundlegenden Sicherheitsmassnahmen und Vorkehrungen für die Systeme respektive deren Komponenten. Dabei werden in zwei Matrizen die je einander nahestehenden Sicherheitsdimensionen Verfügbarkeit und Datenexistenz respektive Integrität und Vertraulichkeit einander gegenübergestellt und Klassen gebildet. Mit den Resultaten des Risikodialogs kann nun in den Matrizen die Sicherheitsklasse abgelesen werden, in die das System respektive jede Einzelkomponente fällt.

Zu jeder Klasse gibt es grundlegende Sicherheitsmassnahmen und Vorkehrungen, die die Einzelkomponenten erfüllen müssen:

► **Verfügbarkeit/Datenexistenz:** Systemredundanz, Alarmplanung, Mitarbeiterschulung und Notfallsystem

► **Integrität/Vertraulichkeit:** Zugriffs- und Mutationsrechte von Benutzergruppen, Authentifizierungsmechanismen und Datenverschlüsselung

Technische Ausführung

Neben der Sicherstellung eines sicheren Betriebes muss auch gewährleistet werden, dass im Notfall das Geschäft weitergeführt werden kann. Das Eintreten eines Notfalls oder einer Katastrophe kann mit der Wahrscheinlichkeit nicht in Beziehung gebracht werden, da deren Eintreten mit präventiven Massnahmen nie vollständig verhindert werden kann. Deshalb muss aus dem Risikodialog der Schadenverlauf betrachtet werden, aus dem herausgelesen werden kann, wie lange der Geschäftsprozess ohne Unterstützung der Informatik aufrecht erhalten werden kann und wieviel Datenverlust akzeptabel ist, um die Geschäfte weiterführen zu können. Diese Zeiten werden in Nomogramme eingetragen, wobei wir von drei Grundversorgungsbereichen sprechen: Server, Netzwerke und Infrastrukturen.

In den Nomogrammen sind die Mittel (Massnahmenbündel) enthalten, welche aus technischer Sicht implementiert werden können. Ein solches Massnahmenbündel im Bereich Server besteht zum Beispiel aus den Einzelmassnahmen Ersatz-Rechenzentrum cold verfügbar, zweimal täglicher Backup, Backup-Tapes werden sofort ins Fernlager verschoben und Datenrestore ist möglich und geübt. Jedes Massnahmenbündel wird mit einem Pfeil in das Nomogramm eingezeichnet, wobei das Ende des Pfeils die garantierte maximale Ausfallzeit und den garantierten maximalen Datenverlust anzeigt, während die Pfeilspitze die kürzest mögliche Ausfallzeit und den kürzest möglichen Datenverlust anzeigt, der mit dem entsprechenden Massnahmenbündel erreicht werden kann.

In das Nomogramm werden neben den möglichen Massnahmenbündel das Soll, bestehend aus maximal tolerierbarer Ausfallzeit und maximal tolerierbarem Datenverlust, der Ist-Zustand, also das zur Zeit gewählte und implementierte Massnahmenbündel sowie die Anforderungen aus dem SLA eingetragen. Damit lassen sich folgende Fragen einfach aus dem Nomogramm beantworten:

► Erfüllen die heute vorhandenen technischen Ausführungen das Soll, das auf Grund des Schadenverlaufs ermittelt wurde?

► Erfüllen die vertraglich festgelegten SLAs die Anforderungen aus den Geschäftsprozessen ausreichend, sind sie ungenügend oder gehen sie sogar zu weit?

► Welche Massnahmenbünden wären notwendig, um die Anforderungen aus den Geschäftsprozessen erfüllen zu können?

Abstimmung der Massnahmen

Um die Anforderungen an die Grundversorgung zu erfüllen, sind technische Ausführungen in folgenden Bereichen notwendig:

► **Server:** Hardware-und Software-Redundanzen, Backup-Techniken und Backup-Organisation

► **Netzwerk:** Netzwerk-Redundanzen in der Raumverkabelung, in den Netzwerkknoten, in LAN und WAN

► **Infrastruktur:** Ausweichmöglichkeiten auf den Ebenen «Stockwerk» und «Gebäude»

Die Soll-Anforderungen müssen in allen Bereichen erfüllt werden. Wenn das gesamte Firmengelände aufgrund einer Ueberflutung nicht benutzt werden kann, nützt ein redundantes Rechenzentrum nichts, ohne dass die Benutzer einen Ersatzarbeitsplatz haben. Hier macht der Autor oft die Erfahrung, dass die Massnahmen nur einseitig vorgekehrt werden, so dass in einem Katastrophenfall die IT zwar weiterlaufen oder sehr schnell wieder laufen würde, ohne dass in den anderen Bereichen der Weiterbetrieb in der vergleichbaren Zeit wieder aufgenommen werden könnte. Solche unausgewogenen Katastrophenvorsorgemassnahmen kosten unnötig Geld, da der zusätzliche Nutzen nicht zum Tragen kommt.

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 auf Grund von Erwartungen gemacht werden können. Denn wenn die Kosten für die notwendigen Sicherheitsmassnahmen in das Projekt einfliessen, werden die Projektverantwortlichen versuchen, diese so tief wie möglich zu halten. So kann der optimale Punkt in der Abgrenzung zwischen organisatorischen und technischen Massnahmen gefunden werden. ■