Informationssicherheit als Frage der Kultur oder wie viel Sicherheit benötigt ein Unternehmen?

René Zimmermann

KPMG Fides Peat
Information Risk Management
Badenerstrasse 172
CH-8026 Zürich 4
rzimmermann@kpmg.com

Zusammenfassung: Eine realitätsgerechte Unternehmenskultur unterstützt das Unternehmen bei Koordinations- und Integrationsaufgaben. Aufgrund eines auf gemeinsame Werte und Normen gestützten Konsenses benötigen Mitarbeiter die sich mit der Unternehmenskultur identifizieren können erheblich weniger formale Absprachen und Weisungen um sich über die zu erreichenden Ziele zu verständigen. Die Sicherheitskultur, als der Teil der Unternehmenskultur, der die sicherheits-bezogenen Werte und Normen des Unternehmens umfasst, kann sich auf dieselbe Weise positiv auf die Informationssicherheit auswirken. Wenn jedoch die Sicherheitskultur nicht bewusst gefördert wird, kann sie zum Risikofaktor werden, da ihre „natürlich" Evolution nicht mit dem rasanten Tempo des technologischen Wandels und der damit verbundenen neuen Risiken mithalten kann. Die Sicherheitskultur muss gezielt beeinflusst werden, damit sie den Sicherheitsbedürfnissen des Unernehmens gerecht werden kann. Um geeignete Sicherheitsziele setzen zu können, muss das Unternehmen über ein Informationssicherheitsmanagement verfügen, das in der Lage ist, zu bestimmen, wie viel Informationssicherheit das Unternehmen benötigt.

1 Die Wurzel allen Übels: mangelndes Sicherheitsbewusstsein?

Eine Situation aus dem Beratungsalltag: Der IT-Leiter erhält auf Betreiben der Revision den Auftrag, etwas für die Verbesserung der Informationssicherheit zu tun. Es ist im Unternehmen niemandem klar, wie es um die Sicherheit der Informationen steht und ebenso wenig, wie es um sie stehen sollte. Er erfüllt diesen Auftrag, indem er bei einem externen Berater ein Informationssicherheitskonzept eingekauft und einen Informations-Sicherheitsbeauftragten eingestellt, der sich dem Problem annehmen soll. Trotzdem ändert sich die Situation kaum nennenswert. Die Vorschriften des Informations-Sicherheitskonzeptes werden kaum eingehalten, da kaum jemand das Dokument zu Kenntnis genommen hat.

Der Informationssicherheitsbeauftragte ist bereits nach kurzer Zeit frustriert. Er erkennt, dass er im Unternehmen kaum beachtet wird. Das Management will mit Sicherheitsproblemen nicht belästigt werden. Das sei sein Job, wird ihm gesagt. Die Ressourcen, die er anfordert, werden ihm aber auch nicht zu Verfügung gestellt. Weshalb findet sich der IT-Sicherheitsbeauftragte bei seinem Versuch die Informationssicherheit im Unternehmen zu stärken, in einer Situation wieder, die ihn an Don Quixotes Kampf mit den Windmühlenflügel erinnert?

Er verdankt seine Stelle nicht einem von seinen Vorgesetzten selbst erkannten Bedürfnis, sondern dem Druck der Revisionsstelle. Er kommt als Fremder in das Unternehmen, mit der Vorstellung, hier etwas zum Besseren verändern zu können. Er stellt jedoch bald einmal fest, dass seine Vorgesetzten auf seine Vorschläge keinen Wert legen und seine Mitarbeiter in seiner Arbeit keinen Nutzen zu erkennen vermögen.

Was den Sicherheitsbeauftragten in die Leere laufen lässt, ist eine Unternehmenskultur, in deren Werteordnung der Informations-Sicherheit keine Priorität zukommt.

2 Die Unternehmenskultur, die „graue Eminenz“ im Unternehmen

2.1 Die Unternehmenskultur

Jede menschliche Gesellschaft, aber auch viele Gruppe innerhalb einer Gesellschaft, weisen Kenntnisse und Verhaltensweisen auf, die für sie Kennzeichnend sind, und in ihrer Gesamtheit als Kultur bezeichnet werden [PP82]. Die Kultur von Teilgruppe wird als Subkultur bezeichnet. Die Subkultur im Rahmen eines Unternehmens wird als Unternehmenskultur bezeichnet. Der Begriff der Subkultur erweist sich zum Verständnis der von der Gesamtkultur abweichenden unternehmensspezifischen Glaubenssätze und Verhaltensweisen als hilfreich, da nicht alle davon alleine aufgrund der Erfordernisse der Geschäftstätigkeit erklärt werden können.

Obwohl es noch keine einheitliche Begriffsdefinition gibt, ist der Begriff der Unternehmenskultur heute gut etabliert. Die meisten Vorschläge für eine Definition schlagen vor, die Unternehmenskultur ein Konstrukt zu sehen, das sich aus den von den Mitarbeitern eines Unternehmens mehrheitlich geteilten Normen, Wertvorstellungen Denkhaltungen, Phantasien zusammensetzt. Die Unternehmenskultur prägt sowohl das Verhalten der Mitarbeiter (Umgangsformen, Arbeitsmoral etc.) wie auch das Erscheinungsbild des Unternehmens (Architektur, Raumgestaltung, Corporate Identity etc.). Die in einer (Unternehmens-) Kultur vorherrschenden Werte und Normen stützen sich ihrerseits auf implizite Grundannahmen über das Wesen der Welt im allgemeinen und des Daseinszweckes des Menschen und dem Sinn seiner Handlungen und Beziehungen im Besonderen. Obwohl die Kultur eines Unternehmens stark von der seines Umfeldes abhängig ist, entwickelt jedes Unternehmen, selbst wenn sie auf derselben Grundlage aufbauen, eine eigenständige, von seinen individuellen Besonderheiten geprägte, Kultur.

2.2 Die Unternehmenskultur als Orientierungshilfe

Den grössten Einfluss auf das Handeln der Mitarbeiter haben nicht durch formale Prozesse und Weisungen, sondern Elemente des informellen Systems (Werte, Normen, Glaubenssätze etc.) innerhalb der Unternehmenskultur. Den Beteiligten sind viele dieser Einflussfaktoren nicht bewusst, da sie den Status von Selbstverständlichkeiten haben und deshalb nicht hinterfragt werden.

Die in einem Unternehmen gepflegte Sprache, dient der Tradierung der Organisationskultur. Dabei bildet sich ein mehr oder weniger ausgeprägter organisationsspezifischer Sprachstil (Jargon).

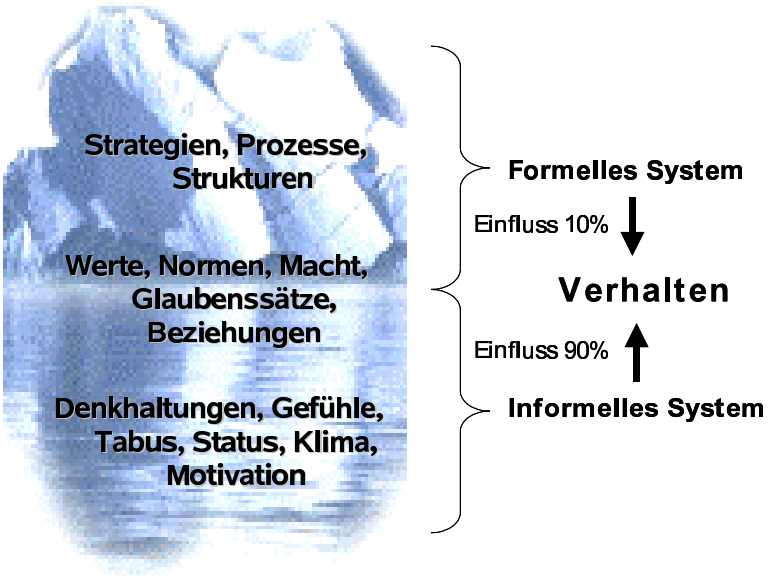

Abbildung 1: Der dominante Einfluss des informellen Systems

Die im Unternehmen gültigen „Normen“ werden in Weisungen und Geboten konkretisiert, welche die Mitarbeiter zu bestimmten Handlungen veranlassen. Je grösser jedoch der Verantwortungsbereich und damit auch der Handlungsspielraum des einzelnen Mitarbeiter ist, je weniger ist es möglich, seine Arbeit im Detail durch Weisungen und Arbeitsanweisungen zu lenken. Die Ausübung komplexer verantwortungsvoller Aufgaben lässt sich über das formale System nicht erschöpfend beschreiben. Deshalb wird die auf gemeinsamen Werte und Zielvorstellungen aufgebaute Unternehmenskultur bei der Koordination der Tätigkeit der Mitarbeiter in modernen Unternehmen immer wichtiger. Neben der Funktion zur Vereinfachung der Koordination übernimmt die Unternehmenskultur weitere wichtige Funktionen. Sie erleichtert es dem Mitarbeiter sich mit dem Unternehmen zu identifizieren. Sie hilft mit, verschiedene Interessensgruppen in die Gesamtheit des Unternehmens zu integrieren. Sie motiviert den Mitarbeiter sich für die Ziele des Unternehmens einzusetzen, in dem sie ihm Werte und Normen vermittelt, mit denen er sich identifizieren kann.

Die Unternehmenskultur wirkt auf den Handlungsspielraum der im Unternehmen tätigen Individuen, indem sie ihnen ein Verständnis für die im Unternehmen gültigen Werte und Normen vermittelt. Daraus können sie Ableiten, welche konkreten Handlungsweisen das Unternehmen, beziehungsweise in seiner Vertretung ihre Vorgesetzten und Mitarbeiter, von ihnen erwarten. Die Unternehmenskultur dient auf diese Weise als Orientierungshilfe. Sie bietet insbesondere dort eine Grundlage für das Handeln der Mitarbeiter, wo keine formalen Regelungen bestehen. Eine starke Unternehmenskultur kann durch die Schaffung eines Grundkonsenses auch den Bedarf an formalen Regelungen reduzieren und wenn Wiedersprüche auftreten, aber sogar dazu führen, das Aussagen in formalen Dokumenten ignoriert werden. Der Mitarbeiter erfährt beispielsweise über die Unternehmenskultur,

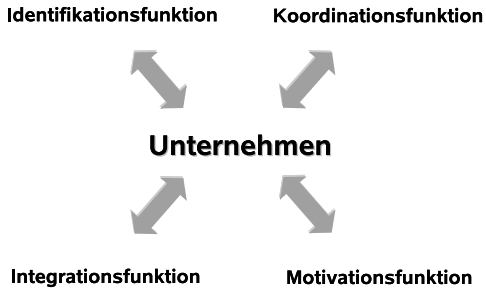

Abbildung 2: Die Funktionen der Unternehmenskultur

dass entgegen den im Leitbild erwähnten ideellen Werte in der Praxis alleine der Umsatz zählt. Er wird sich, wenn er sich für den einen oder anderen Wert entscheiden muss, für den entscheiden, der in der Unternehmenskultur verankert ist.

Eine gut funktionierende Unternehmenskultur kann für die Wettbewerbsfähigkeit eines Unternehmens von grosser Bedeutung sein, wenn sie es ermöglicht, durch ein informelles gemeinsames Verständnis der zu erreichenden Ziele, den Koordinationsaufwand zu reduzieren. Eine von den Mitarbeitern positiv gewertete Unternehmenskultur kann auch über eine verbesserte Motivation zu einer Effizienzsteigerung führen. Das Zugehörigkeitsgefühl der Mitarbeiter wird durch eine positiv wahrgenommene Unternehmenskultur intensiviert. Sie wirkt dadurch integrierend auf das Unternehmen als Gesamtsystem. Diese Funktion ist insbesondere für Unternehmen mit dezentralen Strukturen und einer flachen Hierarchie von grosser Bedeutung. Das dadurch entstehende Zusammengehörigkeitsgefühl wirkt sich zudem positiv auf das Betriebsklima aus.

Die Möglichkeit der Unternehmenskultur auf die Motivation der Mitarbeiter einzuwirken wird jedoch bei den heute stark ausgeprägten Werten des Individualismus und der Selbstbestimmung als weniger stark bewertet [BE97] als noch vor wenigen Jahren. Die Unternehmenskultur kann jedoch dafür sorgen, dass die Diskrepanz zwischen den individuellen Lebenszielen der Mitarbeiter und den Unernehmenszielen nicht allzu gross werden, und dadurch ein Schwinden der Motivation der Mitarbeiter vermeiden helfen. Möglicherweise hält heute die Unternehmenskultur ihre Identität auch weniger über die Einpassung beliebiger Individuen aufrecht, als über Selektion und Fluktuation der Mitarbeiter.

Die Analyse der Kultur eines Unternehmens kann Aufschluss über die Grundorientierungen des Unternehmens geben. Dazu gehören Informationen über die Kunden-, Innovations-, und Kostenorientierung des Unternehmens, aber auch über seine Sicherheitsorientierung. Dieser Sicherheitskultur genannte Teilbereich der Unternehmenskultur hat einen massgebenden Einfluss darauf, wie im Unternehmen mit dem Thema Sicherheit umgegangen wird.

3 Die Sicherheitskultur

3.1 Die Funktion der Sicherheitskultur

Bein der Sicherheitskultur handelt es sich um einen speziellen, jedoch untrennbar verbundenen Teilbereich der Unternehmenskultur. Die Frage, welche Haltung ein Unternehmen zu Sicherheit und Risiko einnimmt, wird im wesentlichen durch die Sicherheitskultur bestimmt. Ein wesentlicher Teil der Sicherheitskultur eines Unternehmens sind die sicherheitsbestimmenden informellen Normen und Regeln. Aus ihnen erfährt der Mitarbeiter, was tatsächlich als Gefahr für das Unternehmen zu sehen ist und was nicht. Nur ein geringer Teil dieser Normen und Regeln sind in einem formellen, aus Strategien, Konzepten und Weisungen bestehenden, System festgehalten. Der überwiegende Teil ist dem informellen System zuzurechnen, welches das formale System mit informellen Regeln, Normen, aber auch mit wenig bis gar nicht bewussten Glaubenssätzen und Werten ergänzt. Dieses informelle System dient den Mitarbeitern als Interpretationshilfe und Konkretisierung der Normen des formellen Systems. Neu in ein Unternehmen eintretende Mitarbeiter erhalten zwar Dokumente, die normative Festlegungen des Unternehmens enthalten. Über die für den Arbeitsalltag wesentlichen Normen werden sie aber durch die Erklärungen und das Vorbild ihrer Mitarbeiter, also informell, aufgeklärt. Auf diese Art erfahren sie auc, welche der formalen Regeln für die tägliche Arbeit effektiv relevant sind und welche in der Unternehmensrealität nicht umgesetzt werden.

Die Sicherheitskultur dient den Mitarbeitern als Orientierungshilfe in Sicherheitsfragen, in dem sie seinen Spielraum bei der Interpretation seiner Wahrnehmungen reduziert. Das gemeinsame Verständnis der Sicherheitsbedürfnisse des Unternehmens ermöglicht es den Mitarbeitern in Situationen im Sinne des Unternehmens zu handeln, für die keine explizite Handlungsanweisung vorhanden ist Sie lässt ihn aber auch erkennen, welche Bedeutung Sicherheit für das Unternehmen tatsächlich hat und nach welchen Kriterien Sicherheitsmassnahmen ausgewählt werden, auch wenn die Sicherheitsstrategie des Unternehmens ein anderes Bild zu vermitteln versucht.

Wenn davon gesprochen wird, dass in einem Unternehmen eine Sicherheitskultur aufgebaut werden müsse, wird von der falschen Vorstellung ausgegangen, dass es Unternehmen gebe, die keine Sicherheitskultur haben. Das ist aber sowenig möglich, wie eine Ethnie denkbar ist, die ohne jede Kultur ist. Die zentrale Frage im Zusammenhang mit der Sicherheitskultur ist nicht ob sie vorhanden ist, sondern ob sie den Sicherheitsbedürfnissen eines Unternehmens angemessen ist oder nicht.

3.2 Die Sicherheitskultur in Traditionsunternehmen

Der Begriff der Sicherheitskultur erfreut sich heute auch unter den Praktikern unter den Sicherheitsfachleuten recht grosser Beliebtheit. In der Regel wird er verwendet, wenn beklagt wird, dass das Bewusstsein der Mitarbeiter für die Bedürfnisse der Informationssicherheit mangelhafte sei. Was fehlt ist in der Regel ein tieferes Verständnis für den Inhalt des Begriffes. Die oberflächliche Verwendung des Begriffes verstellt die Möglichkeit, die Ursachen der Mängel der Sicherheitskultur verstehen und mit adäquaten Massnahmen beheben zu können.

Es gibt jedoch auch Unternehmen, in denen es um das Sicherheitsbewusstsein von Managern und Mitarbeitern besser steht, als in anderen. Wie das mangelhafte Sicherheitsbewusstsein des Managements und der Mitarbeiter als Auswirkung einer, den Sicherheitsbedürfnissen des Unternehmens nicht angemessenen Sicherheitskultur interpretiert werden kann, kann auch ein ausreichendes Sicherheitsbewusstsein mit einer den Sicherheitsbedürfnissen entsprechenden Sicherheitskultur erklärt werden.

Es fällt auf, dass dem Sicherheitsbewusstsein der Manager von Unternehmen, in denen Sicherheitsfragen traditionell einen hohen Stellenwert einnehmen, die besten Zeugnis ausgestellt werden. Das gilt auch für den Bereich der Informationssicherheit, der beispielsweise in Banken und Versicherungen, wie auch in Teilen der öffentlichen Verwaltung, auf Grund der grossen Bestände ausgeprägt sensibler Informationen die dort bearbeitet werden, sehr viel Aufmerksamkeit zukommt.

Die traditionell sehr sicherheitsbewussten Unternehmen taten sich aber mit den, durch die zunehmende Dezentralisierung und Vernetzung der Informationstechnologie neu erstandenen Risiken, teilweise erstaunlich schwer. Armeen beispielsweise, die ja vielerorts den Ruf haben, die Geheimhaltung über alles zu stellen, zeigen zwar beim physischen Schutz ihrer IT hervorragende Leistungen, bei der logischen Sicherheit, bei der sie ihre Kernkompetenzen offenbar weniger einbringen können, weisen sie jedoch auch Mängel auf. Einige Telekommunikationsunternehmen wiegen sich in einer falschen Sicherheit, da sie es für ausreichend halten, auf eine grosse Tradition bei Schutz ihrer Infrastruktur zurückblicken zu können. Es wurde jedoch nicht in allen Bereichen die Sicherheitsmassnahmen, die auf die elektromechanischen Systeme zugeschnitten waren, an die Bedürfnisse der aktuellen Technologien angepasst.

3.3 Vom technologischen und organisatorischen Wandel überfordert

Das Problem bei der Anpassung der Sicherheitskultur an die Anforderungen neuer Technologien liegt darin, dass eine Kultur auf veränderte Umweltbedingungen nur sehr träge reagieren. Tiefgreifende kulturelle Veränderungen in einer Gesellschaft erstrecken sich meistens über Jahre, wenn nicht sogar Jahrzehnte. Auch die Sicherheitskultur eines Unternehmens reagiert nur sehr träge auf veränderte Umweltbedingungen. Zu träge, um mit der sehr schnell Ändernden Bedrohungslage im Bereich der IT mithalten zu können. Wenn die Sicherheitskultur eines Unternehmens aber nicht in der Lage ist, sich der Geschwindigkeit des Wandels der Risiken anzupassen, kann sie sehr schnell selbst zum Risiko werden.

Die Dynamik dieser Entwicklung in der und durch die IT überfordert die „natürliche“ Innovationskraft der Sicherheitskultur. Die Unternehmen können deshalb nicht darauf vertrauen, dass die bisherigen Erfahrungen des Unternehmens im Umgang mit den Risiken der Geschäftstätigkeit im Allgemeinen und der in der Bearbeitung sensitiver Informationen im Besonderen, sie automatisch zur Bewältigung der aktuellen Risiken der elektronischen Informationsbearbeitung befähigen.

3.4 Wenig Akzeptanz für konservative Werte in jungen Unternehmen

Die Kultur junger, schnell wachsenden Unternehmen, ist aus anderen Gründen wenig geeignet, die Sicherheit der Informationsbearbeitung zu fördern. Die Unternehmenskultur

junger Unternehmen im Aufbruch, die in einem dynamischen Umfeld innovative Produkte im Entwickeln und Herstellen, ist von anderen Werten als dem der Sicherheit geprägt. Unternehmen in der Aufbauphase stecken, haben andere Prioritäten, als die Informationssicherheit. Sie sind stark auf die Entwicklung ihrer Produkte und die Stärkung ihres Marktpotentials konzentriert. Menschen in der Adoleszenz ähnlich, neigen sie dazu, ihre Möglichkeiten zu überschätzen und Risiken zu verdrängen.

Besonders prekär ist die Situation paradoxerweise in jungen Unternehmen, in der die Informations- und Kommunikationstechnologie Teil der Kernkompetenz ist. Die Ressourcen dieser Unternehmen werden durch die Entwicklung und Einführung neuer Technologien und der dadurch ermöglichten neuen Produkte stark absorbiert. Unter dem Druck damit möglichst schnell an den Markt gehen zu können, werden Sicherheitsanforderungen vielfach wenig Aufmerksamkeit geschenkt.

Junge, aufstrebende Unternehmen suchen Mitarbeiter die stark Ergebnis- und zielorientiert sind, und werden selbst auch von solchen Menschen als Arbeitgeber bevorzugt. Aufgrund dieses gegenseitigen Selektionsverfahrens entwickelt das Unternehmen eine Kultur, die für konservative Werte, wie die Sicherheit einer ist, wenig Raum lässt. Das äussert sich darin, dass solche Unternehmen oft grosse Risiken eingehen, nicht nur im Umgang mit Informationen und der zu ihrer Bearbeitung eingesetzten Technologien. Der grosse Risikoappetit solcher Unternehmen war einer der Faktor, die für den Untergang etlicher Firmen, die auf dem eHype geschwommen sind, mitverantwortlich waren.

Oft zeigt es sich, dass die grössten Risiken dieser Unternehmen nicht auf der technischen Ebene alleine liegen. Durch das schnelle Wachstum der Unteernehmen sind Organisationsstrukturen teilweise „organisch“ gewachsen. Das führte dazu, dass Management- und Controllingprozesse der Grösse des Unternehmens bald einmal nicht mehr angemessen waren. Wenn anfänglich informelle Instrumente zur Führung des Unternehmens seinen Bedürfnissen adäquat waren, genügen diese Instrumente ab dem Erreichen einer kritischen Grösse nicht mehr. Im Bereich der Informationssicherheit führt dies, wie auch in anderen Bereichen, dazu, dass dem Management der Überblick darüber entgleitet, wer in welchen Bereichen des Unternehmens mit welchen Instrumenten welche Sicherheitsziele zu erreichen versucht. In einer solchen Situation ist es nicht weiter erstaunlich, wenn der CIO des Unternehmens keine Ahnung hat, wie es um die Informationssicherheit steht.

4 Wege zur risikogerechten Sicherheitskultur

4.1 Keine Patentrezepte

Sowenig es möglich ist den Traum einiger Sicherheitsbeauftragter wahr zu machen, die Mitarbeiter so zu manipulieren zu können, dass sie geflissentlich alle (Sicherheits-) Anforderungen des Unternehmens umsetzen, so wenig gibt es einfache Tricks, mit denen die Sicherheitskultur eines Unternehmens in ihrem Sinne beeinflusst werden kann.

Das heisst nicht, dass die Unternehmenskultur überhaupt nicht beeinflusst werden kann. Es ist einzelnen Menschen immer wieder gelungen, die Kultur ihrer Gesellschaft nachhaltig zu beeinflussen. Voraussetzung um die Kultur eines Unternehmens beeinflussen zu können, ist viel Verständnis für ihre Funktionsweise.

Es sind allgemein anerkannte Leitfiguren, denen ihre Mitmenschen vertrauen, denen es gelingt Kulturen zu verändern. In einem Unternehmen können die Mitglieder der Unternehmensleitung und des Managements eine solche Rolle einnehmen, wenn sie von den Mitarbeitern als dazu legitimiert anerkannt werden.

Es ist grundsätzlich eine Aufgabe der Unternehmensführung, die Sicherheitskultur des Unternehmens und deren allfälligen Defizite im Dialog mit den Mitarbeitern zu thematisieren. Das bedeutet jedoch nicht, dass sie den Mitarbeitern in schulmeisterlichem Ton Weisungen zu erteilen sollen, sondern dass sie die Notwendigkeit und den Nutzen von Veränderungen der Normen und Werte des Unternehmens und neuer Anforderungen an die Mitarbeiter für die nachvollziehbar begründen. Diese kommt die Aufgabe zu mit dem Setzen von Anreizen und dem delegieren von Verantwortung die Sicherheit der Informationsbearbeitung als zentralen Wert des Unternehmens fest zu setzen.

Die Erkenntnis, dass das Unternehmen nicht selbstverständlich „weis“ wie viel Sicherheit seiner Geschäftstätigkeit angemessen ist, müssen Prozesse etabliert werden, mit denen immer wieder überprüft werden kann, ob der gegenwärtige Stand der Informationssicherheit der aktuellen Situation des Unternehmens immer noch angemessen ist.

Wichtig ist schlussendlich vor allem eine lösungsorientierte Haltung. Auch Sicherheitsfachleute müssen in der Lage sein, die Selbstverständlichkeiten ihrer Zunft immer wieder darauf zu überprüfen, ob sie immer noch realitätsgerecht sind. Insbesondere wen seit Jahren immer wieder angewendete Massnahmen offensichtlich nicht zum erwünschten Ziel führen, sollte überprüft werden, ob die Lösung nicht mit untauglichen Mitteln angestrebt wird.

4.2 Die Unternehmenskultur verstehen

Projekte, mit denen die Sicherheitskultur eines Unternehmens verbessert werden sollen, scheitern nicht selten daran, dass die Personen, die es zum Erfolg führen sollten, die Unternehmenskultur nicht kennen oder zumindest nicht verstehen. Sie sehen zwar, dass die Mitarbeiter eines Unternehmens in ihrer subjektiven Sicht den Stand der Informationssicherheit im Unternehmen besser einschätzen, als er tatsächlich ist und deshalb Risiken nicht wahrnehmen. Was sie jedoch nicht berücksichtigen, sind die Gründe, die zu dieser Fehleinschätzung führen, da sie vorschnell von individuellen Fehlleistungen der Mitarbeiter ausgehen. Es würde sich aber lohnt zu überprüfen, ob die festgestellten Mängel der Informationssicherheit auf eine nicht mehr realitätskonforme Unternehmenskultur zurückgeführt werden können. Diese Erkenntnis würde es erleichten, geeignete Massnahmen zur Behebung der Mängel zu ergreifen.

Die Kenntnis der Unternehmenskultur reduziert das Risiko Massnahmen umsetzen zu wollen, die mit den Wertvorstellungen der Mitarbeiter kollidieren und dadurch unnötigen Widerstand hervorrufen. Besonders wichtig ist die Wahrnehmung des im Unternehmen üblichen Umgangs mit Vertrauen und Kontrolle. Sicherheitsfachleute neigen dadurch, dass sie sich in ihrer Tätigkeit stark auf Sicherheitsmängel konzentrierenden, Sicherheit einseitig über Kontrollen erreichen zu wollen.

Sicherheit durch Kontrolle mag Unternehmen, die nach den Grundsätzen Taylors Systems zur „wissenschaftlicher Betriebsführung“ geführt werden, angemessen sein. Unternehmen

die von ihren Mitarbeitern aktives Mitdenken und eigenverantwortliches Handeln erwarten, würden jedoch durch den Versuch, dieses von einem starken Machtgefälle zwischen Vorgesetzten und ihren Untergebenen geprägte, streng hierarchische Führungssystem einzuführen, rasch vom Markt eliminiert. Das Scheitern des Taylorismus weist auf die Notwendigkeit einer sinnvollen Verknüpfung des Technikeinsatzens mit den sozialen Bedürfnissen der Mitarbeiter hin [FR89]. Diese Voraussetzungen müssen auch berücksichtigt werden, wenn Massnahmen zur Verbesserung der Informationssicherheit ergriffen werden sollen. Von Mitarbeitern, die gewohnt sind, selbständig und selbstbestimmt zu arbeiten, kann nicht ohne weiteres erwartet werden, dass sie sich kooperativ zeigen, wenn im Sicherheitsbereich ein allzu autoritärer Stil gepflegt wird.

4.3 Die Unternehmenskultur beeinflussen

Zeigt es sich, dass die bestehende Unternehmenskultur den Sicherheitsbedürfnissen des Unternehmens nicht (mehr) angemessen ist, stellt sich die Aufgabe, den notwendigen Kulturwandel zu initiieren.

In einer Gesellschaft sind es nicht notwendigerweise die politischen Führer, die den grössten Einfluss auf die Kultur ausüben. Analog dazu hat in einem Unternehmen die Geschäftsleitung nicht notwendigerweise den grössten Einfluss auf die Unternehmenskultur. In grossen Unternehmen werden die Mitarbeiter stark von den Linienvorgesetzten beeinflusst, die sich noch „in Sichtweite“ befinden. Die Geschäftsleitung ist für sie in vielen Fällen zu wenig wahrnehmbar, um einen direkten Einfluss auf sie ausüben zu können. Dieser Effekt wird dadurch verstärkt, dass die durchschnittliche Firmenzugehörigkeit der Mitglieder der Geschäftsleitungen grosser Unternehmen auf wenige Jahre gesunken ist. Das fördert das Risiko, dass die Mitarbeiter das Top-Management nicht als legitime Vertretung der Unternehmensinteressen anerkennen. Im Extremfall kann das zur Vorstellung führen, zusammen mit dem mittleren Management das Unternehmen gegen die Firmenleitung verteidigen zu müssen.

Wenn nun die Sicherheitskultur gezielt beeinflusst werden soll, geschieht dies am besten über Personen, die das Vertrauen der Mitarbeiter geniessen und von ihnen als Vorbilder anerkannt werden. Der Informationssicherheitsbeauftragter gehört in den meisten Fällen nicht zu diesem Personenkreis. Deshalb ist es wenig aussichtsreich, wenn er auf eigene Faust antritt, die Sicherheitskultur zu verändern.

Es ist ein erheblicher Vorteil, wenn der CEO des Unternehmens zu diesen Personen gehört, da er am besten in der Lage ist, die Informationen, die über das formale beziehungsweise das informale System zu den Mitarbeitern gelangen, in Übereinstimmung zu bringen. Die im Unternehmen gültigen Werte und Normen, die der Unternehmenskultur zu Grunde liegen, können kaum mit Weisungen direkt beeinflusst werden. Es hilft wenig in einem Leitbild mit vielen schönen Worten ideelle Unternehmensziele zu propagieren, wenn den Mitarbeitern aufgrund der Erfahrung des Arbeitsalltags klar ist, dass letztlich alleine der Umsatz zählt. Die in Informationssicherheitsstrategien üblichen Formeln, mit denen die grosse Wichtigkeit der Sicherheit geschäftsrelevanter Informationen betont wird, sind unglaubwürdig, wenn die Mitarbeiter wissen, dass sie letztlich an der Einhaltung von Budgets und Terminen gemessen werden. Wenn die Geschäftsleitung bei der Kommunikation

von Werten und Normen, die sie im Unternehmen etablieren möchte, glaubwürdig sein will, muss sie sich an denen orientieren, die ihren geschäftlichen Entscheidungen auch tatsächlich zu Grunde liegen. Wenn die Mitarbeiter sehen, dass die Informationssicherheit zwar mit grossen Worten, ansonsten aber mit wenig Ressourcen bedacht wird, wissen sie, wie sie diese Signale zu deuten haben.

Wenn die Sicherheitskultur glaubwürdig beeinflusst werden soll, ist es wichtig, dass nicht Utopien kommuniziert werden, an die selbst die nicht glauben, die sie publizieren, sondern dass ein realistisches Bild der Ziele und der Mittel, die dem Unternehmen zu ihrer Erreichung zur Verfügung stehen gezeichnet wird. Wenn es dadurch gelingt, den Anspruch der Informationssicherheitsstrategie und die vom Mitarbeiter erlebte Wirklichkeit einander näher zu bringen, wirkt sich das positiv auf die Glaubwürdigkeit der Massnahmen zur Stärkung der Informationssicherheit aus. Es erwartet niemand, dass das Unternehmen die Informationssicherheit über alle anderen Ziele setzt, deshalb macht es auch keinen Sinn, in Leitbildern und Strategien diesen Eindruck erwecken zu wollen.

Wichtiger als blumige Worte sind konkrete, realistische Sicherheitsziele und die klare Delegation der Verantwortung für das Erreichen dieser Ziele. Wenn Konflikte zwischen Leistungszielen und Sicherheitszielen bestehen, können diese nicht dadurch gelöst werden, dass die Verantwortung für die Sicherheitsziele von den Linienverantwortungen getrennt wird. Im Gegenteil: Nur durch die Integration der Verantwortung für die Informationssicherheit in die Linienorganisation, kann ein Beitrag zur Überwindung des Konfliktes zwischen Leistungs- und Sicherheitsanforderungen geleistet werden. Als Grundlage für diese Bestrebungen könnte das Konzept eines »Total Safety Managements« verwendet werden, das analog dem Konzept des »Total Quality Management« zu verstehen ist, mit dem durch eine Integration der Verantwortung für die Qualität in die Linienorganisation, der Gegensatz zwischen Arbeitsleistung und -qualität überbrückt wurde. Wenn dabei eher nach pragmatischen, als nach perfekten Lösungen gestrebt wird, können die Fehler die bei der Einführung von Qualitätssystemen gemacht wurde, vermieden werden.

Einen wesentlichen Einfluss auf die Sicherheitskultur eines Unternehmens hat die Art und Weise, in denen die neuen Anforderungen im Rahmen der Corporate Governance im Unternehmen umgesetzt werden.

Bei der Definition der Verantwortungen für die Informationssicherheit ist zu beachten, dass die im Bereich der Corporate Governance geforderte Balance von Führung und Kontrolle auch im Bereich der Informationssicherheit eingehalten wird. Besonders wichtig ist die klare Trennung von Führung und Kontrolle Es soll vermieden werden, dass beispielsweise ein Informations-Sicherheitsbeauftrager seine eigene Arbeit kontrollieren muss.

Die Bedeutung der Informations-Sicherheitsbeauftragten wird durch diese klare Verantwortungszuordnung nicht geschmälert. In dem er von der Verantwortung für die Sicherheit und auch von Kontrollaufgaben befreit wird, kann er sich uneingeschränkt seiner Kernaufgabe, der Beratung der Verantwortlichen, zuwenden.

Gegenstand seiner Beratertätigkeit sollten vor allem Fragen der Sicherheitsorganisation und -prozesse sein. Er sollte aber auch wissen, wo innerhalb und ausserhalb des Unternehmens welches Know-how verfügbar ist. Dadurch kann er die Funktion einer Informationsdrehscheibe wahr nehmen.

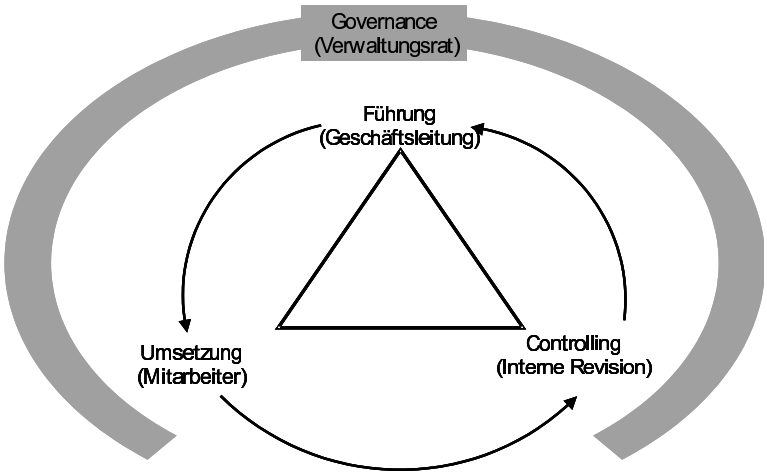

Abbildung 3: Balance zwischen Führung, Umsetzung und Controlling

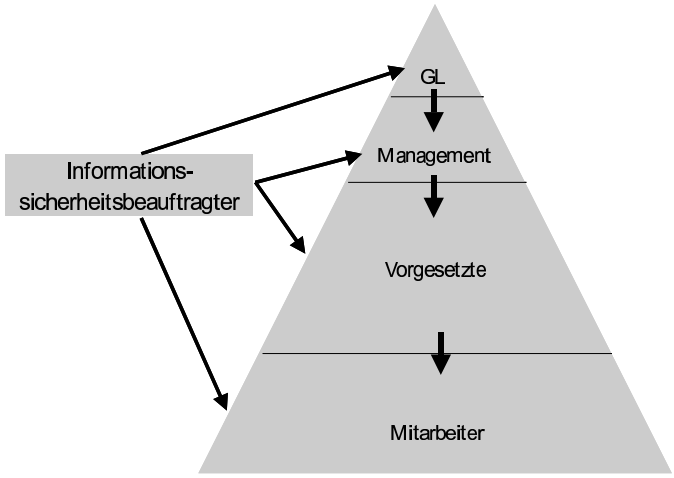

Abbildung 4: Der Informationssicherheitsbeauftragte in der Rolle des internen Beraters

Er ist der interne „Springpartner“ der Prozess- und Projektverantwortlichen. Zusammen mit ihm können sie überprüfen, ob sie alle sicherheitsrelevanten Aspekte berücksichtigt haben. Der Sicherheitsbeauftragte muss in der Lage sein, die richtigen Fragen zu stellen, nicht aber, selbst auch die richtigen Antworten zu geben. Die Evaluation konkreter Sicherheitsmassnahmen fällt in die Verantwortung der operativ Verantwortlichen.

4.4 Die Balance von Kompetenz und Technik

Informationssicherheit ist durch technische Massnahmen alleine nicht realisierbar. Die Gültigkeit dieser Aussage ist heute unbestritten. Unterschiedliche Auffassungen gibt es noch hinsichtlich der, aus dieser Aussage abzuleitenden, Massnahmen.

Wie bereits dargelegt, übt die Sicherheitskultur grossen Einfluss auf die Informationssicherheit aus. Sie hat deshalb einen massgebenden Einfluss darauf, wie mit den üblicherweise als grösstes Risiko der Informationssicherheit bezeichneten „Irrtümern und Nachlässigkeiten“ der eigenen Mitarbeiter umgegangen wird.

Wenn der Mensch im soziotechnischen System eines Unternehmens primär als Risikofaktor betrachtet wird, wird darauf hingearbeitet, seinen Handlungsspielraum technisch und organisatorisch einzuengen, um seine Möglichkeiten die Informationssicherheit zu gefährden, zu reduzieren. Die Annahme, dass alleine durch eine verstärkte Übernahme von Handlungsabläufen durch technische Systeme menschliche Fehler und Unzulänglichkeiten verhindert würden, erwies sich jedoch in anderen Technologiebereichen wie der Aviatik als falsch. Menschliche Fehler wurden dadurch bloss „enttrivialvisiert“. Wenn die Mitarbeiter, welche die technischen Systeme betreuen müssen, die Möglichkeiten und Grenzen dieser Systeme und der zu deren Absicherung eingesetzten Technologien nicht mehr überschauen, sind sie vom korrekten Funktionieren der Technik abhängig. Es zeigt sich immer wieder, dass schwerwiegende Sicherheitsvorfälle gerade auf das Versagen von technischen Sicherheitslösungen zurückzuführen sind. Deshalb ist es sinnvoller, den Menschen als Sicherheitsfaktor zu betrachten und Technik und Arbeitsabläufe so zu gestalten, dass er von ihnen bei der eigenverantwortlichen und sicheren Ausführung seiner Aufgaben unterstützt wird. Die Mitarbeiter sind zu befähigen, bei unerwarteten Ereignissen schnell und der Situation angemessen zu reagieren.

Die Situation der Mitarbeiter, welche die Informations- und Kommunikations-technologie bei ihrer Arbeit lediglich als Werkzeug einsetzen, ist allerdings eine völlig andere. Das Verstehen der Funktionsweise der von ihnen verwendeten Technologien, gehören nicht zu seinen Kernkompetenzen. Deshalb sollte beim Design, der von ihm verwendeten Geräte darauf geachtet werden, dass Fehlmanipulationen möglichst weitgehend ausgeschlossen werden. Ausgehend von der Einsicht, dass jeder prinzipiell mögliche Fehler irgendwann einmal gemacht wird, sollten wie beim Flugzeugbau darauf geachtet werden, dass die Fehlermöglichkeiten so weit wie möglich reduziert werden.

5 Das angemessene Sicherheitsniveau

5.1 Ohne Risiko kein Gewinn

Unternehmen können sich nicht mehr darauf verlassen, dass ihr über die Sicherheitskultur überliefertes Verständnis der Informationssicherheit, den tatsächlichen Sicherheitsbedürfnissen des Unternehmens immer noch angemessen ist. Es sind deshalb Strukturen und Prozesse zu etablieren, mit denen das Unternehmen in die Lage versetzt wird, die zum Schutz seiner geschäftsrelevanten Informationen und zu deren Bearbeitung eingesetzten Infrastruktur, laufend an die sich verändernde Bedrohungslage anzupassen. Dadurch kann das der Geschäftstätigkeit angemessene Sicherheitsniveau aufrecht erhalten werden.

Jede Geschäftstätigkeit ist mit Risiken verbunden, zu denen auch die Sicherheitsrisiken der Informatik gehören. Jedes Unternehmen versucht seine Risiken auf ein vertretbares Mass zu reduzieren. Doch sowenig das beste Business Risk Management eine risikofreie Geschäftstätigkeit ermöglicht, garantiert selbst ein optimales Informations-Sicherheitsmanagement eine absolut sichere Informationsbearbeitung.

5.2 Wirtschaftliche Sicherheitslösungen

Die Sicherheitsrisiken der Informatik können – wie alle Geschäftsrisiken – entweder vermieden, reduziert, überwälzt (z.B. versichert) oder selbst getragen werden. Es ist die Aufgabe des Informations-Sicherheitsmanagements zu entscheiden, welchem Sicherheitsrisiko mit welcher Strategie am wirtschaftlichsten begegnet werden kann.

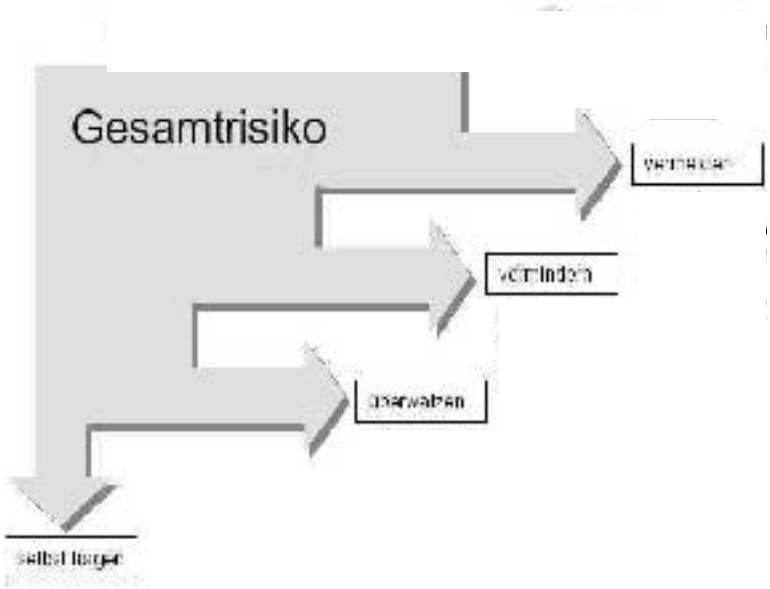

Abbildung 5: Strategien für den Umgang mit Informationsrisiken

Einbrecher entwenden mehrere Notebooks. Das betroffene Unternehmen verliert dadurch vertrauliche Dokumente, für die keine Sicherungskopien bestehen. Wie soll diesem Risiko in Zukunft begegnet werden? Das Risiko zu vermeiden würde bedeuten, auf Notebooks zu verzichten. Ein Versicherungsschutz deckt zwar den materiellen Wert der Geräte ab, aber nicht die Umtriebe, die mit dem Verlust der Dokumente verbunden sind. Möglich wäre die Verbesserung des Einbruchschutzes, doch würden die Kosten den materiellen Wert der Notebooks wesentlich übersteigen. Das Diebstahlrisiko ausserhalb des Gebäudes, bliebe zudem bestehen. Kostengünstig ist hingegen die Lösung, die Daten auf den Notebooks zu verschlüsseln (Schutz der Vertraulichkeit) und eine benutzerfreundliche Lösung zur Datensicherung einzuführen (Schutz der Verfügbarkeit der Informationen).

Dieses einfache Beispiel zeigt exemplarisch, wie mit Sicherheitsrisiken der Informatik umgegangen werden kann. Die Aufgaben, die sich dem Informations-Sicherheitsmanagement stellen, sind zwar in der Regel wesentlich komplexer, doch die grundsätzlichen Fragen bleiben dieselben: Welche Risiken will oder kann ein Unternehmen tragen? Mit welchen Massnahmen können die übrigen Risiken am wirtschaftlichsten reduziert werden?

Das Sicherheitsniveau, das ein Unternehmen für seine Informatik wählt, muss den Sicherheitsbedürfnissen der Geschäftstätigkeit angemessen sein, soll aber zur Vermeidung unnötiger Kosten auch nicht wesentlich darüber hinausgehen. Die Kosten der Informatiksicherheit steigen nicht linear mit den Sicherheitsanforderungen an, sondern exponentiell dazu. Es besteht deshalb die Versuchung, das Sicherheitsniveau aus Spargründen unter das der Geschäftstätigkeit angemessene Niveau zu reduzieren. Dabei geht das Unternehmen aber Risiken ein, die im Ereignisfall zu substantiellen Verlusten führen können. Sinnvoller ist es, das Sicherheitsniveau beizubehalten, aber darauf zu achten, es mit kostengünstigen Massnahmen zu erreichen. Wirtschaftlichkeitsüberlegungen und nicht technische Perfektion alleine, sollen deshalb für die Wahl einer Lösung entscheidend sein. Sicherheitsziele können teilweise mit kostengünstigen organisatorischen Lösungen erreicht werden. Anstelle von Investitionen in teure technische Lösungen zur Minderung des Ausfallrisikos einer Applikation beispielsweise, kann die Abhängigkeit von der Applikation durch Ausweichlösungen vermindert werden.

Ein effizienter Einsatz der Mittel erfordert, dass keine unkoordinierten Einzelmassnahmen ergriffen werden. Ein Informations-Sicherheitsmanagement, das eine Gesamtsicht der Informatiksicherheit gewährleistet, vermeidet Doppelspurigkeiten und verhindert, dass wesentliche Risiken unberücksichtigt bleiben. Zur Überprüfung der Vollständigkeit der getroffenen Massnahmen sind Standardwerke (z.B. ISO 17799) hilfreich, die einen Überblick über die zu berücksichtigenden Themen geben. Mit Hilfe eines Standards kann zudem ein ausgewogener Grundschutz aufgebaut werden. Nur wo Sicherheitsbedürfnisse nachgewiesen werden können, die mit dem Grundschutz nicht abgedeckt sind, sind zusätzliche Investitionen erforderlich. Besonders kritische Geschäftsapplikationen und Informationen werden individuell auf ihre Risiken überprüft. Zeigt es sich, dass der Grundschutz nicht ausreicht, um ihre Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität ausreichend zu gewährleisten, sind zusätzliche Sicherheitsmassnahmen erforderlich.

5.3 Konzentration auf die Kernaufgaben

Ein effektiver Einsatz der Ressourcen bedingt, dass sie nur für Massnahmen eingesetzt werden, die tatsächlich der Informatiksicherheit dienen. Es kommt vor, dass Mitarbeiter ihre Arbeitszeit für persönliche Zwecke, wie die private Nutzung des Internetzugangs, missbrauchen. Einige wenden sich dabei auch Inhalten zu, die ethisch bedenklich sind. Tools, mit denen sich das Verhalten der Mitarbeiter am PC überwachen lässt, sind für relativ wenig Geld erhältlich, was ihren Einsatz attraktiv erscheinen lässt. Abgesehen davon, dass solche Massnahmen rechtlich problematisch sind und das Vertrauensverhältnis zwischen Mitarbeitern und Unternehmen beeinträchtigen können, ist zu beachten, dass der Betrieb solcher Tools mit teilweise erheblichem Aufwand verbunden ist. Soweit die Sicherheit der Informatikmittel nicht direkt betroffen ist, ist aber weder Inhalt noch Ausmass der privaten Informatiknutzung eine Angelegenheit der Informatiksicherheit. Es ist Sache

der Linienvorgesetzten dafür zu sorgen, dass ihre Mitarbeiter ihrer Treuepflicht nachkommen.

5.4 Die Kunst das Richtige zu tun

Das Billigste nicht immer das Günstigste, auch in der Informatiksicherheit nicht. Nur eine enge Zusammenarbeit mit den von einer Sicherheitsmassnahme betroffenen Geschäftsbereichen erlaubt es, bei der Evaluation von Sicherheitsmassnahmen auch deren Folgekosten ausserhalb der Informatik zu berücksichtigen. Der Kostenvorteil einer Massnahme kann leicht zunichte gemacht werden, wenn sie die Effizienz von Arbeitsabläufen gefährdet, oder von den Mitarbeitern als schikanös empfunden wird, wodurch Arbeitsmotivation und -leistung gemindert werden. Ein rein technikorientiertes Verständnis der Informatiksicherheit reicht nicht aus, um die wirtschaftlich gesehen optimalen Lösungen zu finden. Nur ein professionelles Informations-Sicherheitsmanagement ermöglicht eine ganzheitliche Sicht. Der Mehraufwand für konzeptionelle und planerische Aktivitäten, wird durch Einsparungen aufgrund von effektiveren und effizienteren Massnahmen mehr als ausgeglichen.

Es gibt keine absolute Sicherheit. Deshalb gibt es auch im Informationssicherheits-Management keine absolut sicheren Entscheidungen. Manchmal zeigt sich im Ereignisfall, wenn aufgrund der getroffenen Massnahmen Schäden verhindert wurden (oder eben auch nicht) ob eine Entscheidung richtig war. Vielfach wird man es jedoch nie erfahren.

Es braucht auch im Informations-Sicherheitsmanagement den Mut, Entscheidungen zu treffen, die unter umständen erhebliche Auswirkungen auf die Geschäftstätigkeit haben könnten. Wichtig ist deshalb, dass auch die Informationssicherheit betreffende Entscheidungen auf der Hierarchiestufe getroffen werden, die tatsächlich die Kompetenz für Entscheidungen mit dieser Tragweite hat. Dadurch wird sichergestellt, dass mit im Umgang mit den Informationsrisiken angewendete Strategie in einem vernünftigen Verhältnis zum Umgang mit den übrigen Risiken der Geschäftstätigkeit steht.

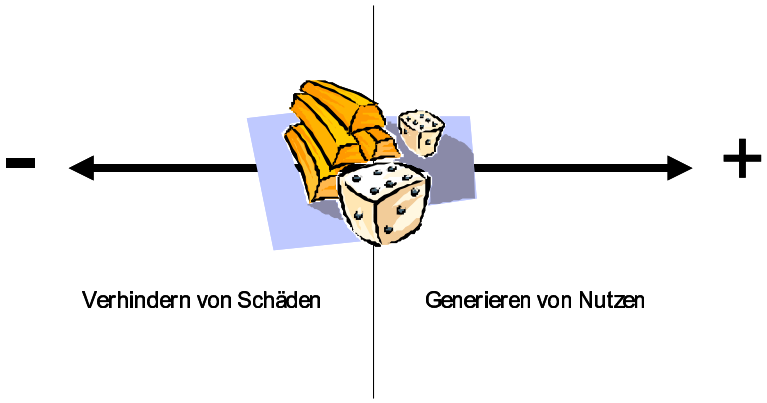

Abbildung 6: Auch in der Informationssicherheit braucht es den Mut zu unsicheren Entscheidungen

5.5 Lösungsorientiertes Vorgehen

Ein Mangel, der im Bereich der Informationssicherheit immer wieder angetroffen wird ist eine starke Problemorientierung. Es werden Risiken aufgezeigt und aufgrund dieser Risiken den Mitarbeitern Handlungsrestriktionen auferlegt. Ein häufig anzutreffendes Beispiele sind Restriktionen im Ungang mit vertraulichen Dokumenten. Zuwenig beachtet wird, dass den Mitarbeitern zugleich auf Möglichkeiten eröffnet werden müssen, wie sie vertrauliche Dokumente effizient weiterleiten können, ohne die Sicherheitsvorschriften zu verletzen. Der einzelne Mitarbeiter wird mit dem Dilemma, ob der nun Effizienz- oder Sicherheitszielen der Vorrang geben will, alleine gelassen. Ein Lösungsorientiertes Informations-Sicherheitsmanagement zeigt dem Mitarbeiter, wie er vorgehen muss um Sicherheitsanforderungen einzuhalten und stellt ihn auch die dafür notwendigen Mittel zur Verfügung.

Zu einem lösungsorientierten Informationssicherheits-Management gehört es auch, die eigenen Selbstverständlichkeiten immer wider in Frage zu stellen. Wenn bei einigen Themen, beispielsweise im Bereich der Arbeitspatzsysteme seit Jahren mit denselben Massnahmen erfolglos versucht wird, Risiken zu reduzieren, kann die Ursache für das Versagen der Problemlösungsstrategie entweder bei anderen Mitarbeitern gesucht werden, oder es kann überprüft werden, ob die gewählte Strategie effektiv zum Erreichen des Sicherheitszieles geeignet ist. Auf das leidige Thema sicherer Passwörter angewendet, könnte das bedeuten, statt das mangelhafte Sicherheitsbewusstsein der Mitarbeiter zu beklagen, sicherere Authentifizierungsverfahren einzuführen. Wenn die Wirtschaftlichkeitsprüfung alternativer Lösungen zu einem negativen Ergebnis kommen sollte, müsste daraus möglicherweise der Schluss gezogen werden, dass das Risiko aufgrund des beklagten unsorgfältigen Umgangs mit Passwörtern offenbar nicht so gross ist, wie bisher angenommen, da es keine risikoreduzierenden Investitionen zu rechtfertigen vermag.

Literatur

[PP82] Panoff, M.; Perrin, M: Taschenwörterbuch der Ethnologie. Dietrich Reimer Verlag, Berlin, 10820.

[BE97] Berkel, K.: Unternehmenskultur und Ethik. I. H. Sauer-Verlag. Heidelberg, 1997

[FR89] Frese, E.: Aufbauorganisation. Gabler. Wiesbaden, 1989