

### 3.3 Risiko: Begriff und seine Funktionen

Der Begriff des Risikos spielt sowohl für die IT-Governance als auch für Prüfung & Revision eine zentrale Rolle.<sup>3</sup> Die dritte Facette für den Perspektivwechsel der Agilität ist deshalb ein umfassendes Verständnis des Risikobegriffs. Dieses erweiterte Verständnis weist über einen oft bei normativen Ansätzen zu beobachtenden Objektivitätsanspruch und über eine primär quantifizierende Perspektive hinaus. Im Unterschied zu der Darstellung in den anderen Abschnitten dieses Kapitels geht es in diesem Abschnitt deshalb NICHT um eine Gegenüberstellung von klassischer und agiler Sichtweise auf Risiko. Sowohl in klassischen wie in agilen Ansätzen der IT-Governance, Prüfung & Revision sind nämlich oft bereits verschiedene Aspekte aus diesem Spektrum vertreten. Es geht uns stattdessen darum, das generelle Spektrum des Begriffsverständnisses aufzuzeigen und je nach Situation angemessen einsetzen zu können. So kann bei gesicherten Wissensbereichen oder stabilen Umweltbedingungen durchaus ein quantitativer und Objektivität beanspruchender Ansatz im Umgang mit Risiken angemessen sein. In diesen Fällen ist eine historische Datenbasis vorhanden, aus der aussagekräftige Prognosen für die Zukunft getroffen werden können. Was natürlich immer erst bestätigt wird, wenn die Zukunft eintritt. Zudem haben sich einschlägige Experten auf bestimmte Arten der Risikomodellierung geeinigt. Je unbekannter und komplexer jedoch der Wissensbereich ist, umso mehr bedarf es eines anderen Umgangs mit Risiken, der die kommunikative Einbettung des Risikobegriffs und der Risikobewertung stärker einbezieht.

#### 3.3.1 Gefahr versus Risiko

Für einen wirksamen Umgang mit Risiken ist es zunächst wichtig, eine Unterscheidung zwischen *Gefahr* und *Risiko* vorzunehmen. Von *Gefahr* spricht man, wenn die Organisation potenziell von Wirkungen aus der Umwelt betroffen ist oder betroffen sein könnte. Die Ursache für den Schaden wird dem Umfeld zugeschrieben, die Organisation hat demnach keinen Einfluss. Gefahren bestehen in dieser Sichtweise unabhängig davon, wie Verhaltensentscheidungen von der Organisation getroffen werden.

Eine *Gefahr* wird zum *Risiko*, wenn die Organisation eine Entscheidung trifft, sich einer Gefahr auszusetzen oder eben nicht. Die möglicherweise daraus entstehenden Folgen des Risikos kann man der Organisation zurechnen – *weil* sie sich zuvor *entschieden* hat.

---

3. Zum Themenbereich von Unsicherheit, Gefahr und Risiko gibt es eine sehr umfassende Spezialliteratur. Das Spektrum reicht von versicherungsmathematischen hochkomplexen Berechnungsverfahren bis hin zu soziologisch-gesellschaftswissenschaftlichen Grundsatzüberlegungen wie z.B. in der Gesellschaftstheorie nach Luhmann. In unserer Darstellung werden wir jeweils nur ganz generelle Grundlagen davon nutzen.

Anders ausgedrückt: Einer Gefahr kann ich mich nicht generell entziehen, sie ist durch Umweltbedingungen gegeben. Ein Risiko hat dagegen immer mit einer vorher erfolgten *Entscheidung* angesichts einer Gefahr zu tun. Durch die Entscheidung bin ich aktiv daran beteiligt, ob eine Gefahr zu einem Risiko wird. Auch durch die entgegengesetzte Entscheidung kann übrigens ein Risiko entstehen. Das hängt dann von der Situation ab. Das ist insbesondere relevant für die IT-Governance, Prüfung & Revision: Auch eine Nicht-Entscheidung (oder Entscheidung *gegen* etwas, z.B. gegen die Einführung eines neuen Technologieprodukts in der Organisation) ist oft mit einem Risiko verbunden. Es könnte nämlich eine große Gewinnchance vertan worden sein.

Ob etwas als Risiko oder Gefahr angesehen wird, hängt von der Zuschreibung eines Beobachters ab. Wenn ein Schaden für eine Organisation eintritt, behauptet z.B. deren Leitung (Beobachter I), dass sie diesen Schaden nicht hätte voraussehen können. Ihrer Ansicht nach haben die äußeren Umstände, eine unbestimmte Gefahr, zu dem Schaden geführt. Eine externe Prüfungskommission (Beobachter II) wirft jedoch der Organisationsleitung »Nichtstun« vor. Aus Sicht der Prüfer wäre das Problem absehbar gewesen, die Organisation hätte sich durch ihr Stillhalten entschieden, ein Risiko einzugehen und hätte den Schaden bewusst in Kauf genommen. Die Prüfer »transformieren« so die Einschätzung als Gefahr in eine Einschätzung als Risiko. Wenn ein (solches) Risiko kommuniziert und bei bestimmten Adressen anschlussfähig wird, kann das weitreichende organisationale und gesellschaftliche Konsequenzen haben. In unserem Beispiel könnte die Organisationsleitung für ihr unterbliebenes Handeln als verantwortlich eingestuft und entsprechend zur Verantwortung gezogen werden.

Eine wesentliche Unterstützungsfunktion für die Entscheidung, ob eine Organisation ein Risiko eingeht, hat nun die *Risikobewertung*. Sie wird üblicherweise als *Eintrittswahrscheinlichkeit* \* *Schadenspotenzial* über einen bestimmten Zeithorizont quantifiziert.

Ein Risiko zeichnet sich also gegenüber der Gefahr dadurch aus, dass eine Entscheidung damit verbunden ist. Die Risikobewertung liefert dazu wiederum eine quantitative Entscheidungsgrundlage, die – da quantitativ daherkommend – oft den Anschein von Objektivität erweckt, obwohl in vielen Einzelschritten soziale Kommunikationsschritte, inklusive der Selektion von Annahmen der Modellierung auf der Ebene der Beobachtung (Zeithorizont, Datenpool), Erklärung (Ursache für Schäden, inkl. welche Schäden könnten passieren) und Bewertung (u.a. Eintrittswahrscheinlichkeit bzgl. Schäden usw.) wirksam waren, bis am Ende eine formelmäßige Berechnung steht.

Anders formuliert: Durch den *Risikobegriff* möchte man die generelle Unsicherheit der Zukunft, die sich in *Gefahren* äußert, greifbarer und kontrollierbarer machen. Von Risiken (statt von Gefahren) zu sprechen, ist deshalb ein großer, oft auch sehr hilfreicher erster Rationalisierungsschritt im Umgang mit der Unsicherheit der Zukunft. So wird beispielsweise die sehr weit gefasste und unbestimmt

bleibende *Gefahr* einer Cyberattacke in ein begrifflich viel konkreteres *operationelles Risiko* einer fehlenden IT-Kontrolle transformiert. Eine quantifizierende Risikobewertung z.B. durch die Aussage, dass die Schadenwahrscheinlichkeit über einen einjährigen Zeithorizont bei fehlender IT-Kontrolle um x% erhöht wird, ist dann ein zweiter und ebenfalls oft hilfreicher Schritt in Richtung einer *prinzipiellen Berechenbarkeit* der Zukunft.

Damit kann dann eine sehr objektiv anmutende Entscheidungssituation geschaffen werden, die am Ende leicht mit einer *objektiven Kontrollierbarkeit* der Zukunft verwechselt werden kann. Das wäre nun eine aus unserer Sicht unzulässige Vereinfachung, denn bis man überhaupt in der Lage ist, Risiken zu berechnen, sind ja vielfältige soziale Kommunikations- und Selektionsprozesse erfolgt und häufig auch schon viele Schäden entstanden. Daher sollten immer beim Umgang mit Risiken und mit Risikoberechnungen auf jeden Fall die Modellannahmen und ihre begrenzte Aussagekraft mitbetrachtet werden.

Die folgenden Abschnitte beschreiben im Anschluss an diese Überlegungen zwei wichtige Grundpositionen im Verständnis von und im Umgang mit Risiko und Risikobewertungen. Die beiden Positionen bilden die Pole, zwischen denen sich sowohl klassische wie auch agile Ansätze für die IT-Governance, Prüfung & Revision bewegen.

Der eine Pol ist eher naturwissenschaftlich-ingenieurwissenschaftlich motiviert und betont die Objektivierbarkeit, Messbarkeit und Eindeutigkeit von Risiken. Der Grund liegt weitestgehend in der Konstanz der Naturgesetze, denn die Beobachtungen der Naturwissenschaftler bewegten sich Jahrhunderte in einem Bereich, in denen Experimente leicht zu wiederholen waren. So fällt z.B. der Apfel Jahr um Jahr mit großer Sicherheit vom Baum auf die Erde.

Der andere Pol ist eher sozialwissenschaftlich und psychologisch motiviert und betont die Bedeutung der kommunikativen Einbettung des Risikobegriffs und der Risikobewertung, was im Ergebnis zu einer stärkeren Kontingenz und Mehrdeutigkeit von dem, was als Risiko gilt, führt. Der Grund hierfür liegt vermutlich darin, dass der Forschungsgegenstand der Psychologie und Soziologie, wie die Psyche, das Team, die Organisation, die Gesellschaft, autonome Systeme sind, die sich – aus der Sicht eines Betrachters von außen – einmal so und einmal anders verhalten.

**Beispiel für das unterschiedliche Verhalten autonomer Systeme**

Ein Softwareentwickler nutzt ein besonders langes Passwort, um seine Softwareprogramme gut zu schützen. Damit übererfüllt er die Anforderungen der Passwortrichtlinie des Unternehmens. Ein Jahr lang spioniert ein Hacker den Entwickler aus und gelangt schließlich doch noch an das Passwort. Erstaunt stellt der Hacker fest, dass der Softwareentwickler dieses Passwort für sämtliche Softwareanwendungen nutzt, von separat vorgehaltenen, hochsensiblen Daten des Unternehmens über Computerspiele bis hin zu seinem privaten Internetbanking. Dies widerspricht erstens der Passwortrichtlinie des Unternehmens, die die Nutzung »privat verwendeter« Passwörter verbietet. Zweitens widerspricht es den in dem langen Passwort zum Ausdruck kommenden, hochgesteckten Informationssicherheitszielen des Softwareentwicklers. Der Softwareentwickler verhält sich einerseits regelkonform und stellt an sich besonders hohe Anforderungen zum Schutz von Daten, andererseits verstößt er gegen die unternehmensinternen Regeln und gegen minimale Anforderungen an die Informationssicherheit.

**3.3.2 Risiko als instrumentelle Kategorie**

In Anlehnung an das Vorbild der Natur- und Ingenieurwissenschaften gibt es auch in der IT-Governance, Prüfung & Revision eine oft angewendete Denkweise, dass man Risiken in diesen Bereichen am besten durch eine stark quantifizierende Vorgehensweise erfasst. Dabei wird mehr oder weniger stillschweigend die »Existenz« gewisser Risiken angenommen, die dann ziemlich direkt begrifflich ausgearbeitet werden. Die Finanzindustrie spricht beispielsweise weitgehend intuitiv von Adressenausfallrisiken, Marktpreisrisiken, Liquiditätsrisiken und operationellen Risiken. Wenn einmal die konzeptionelle Definition eines einzelnen Risikos erfolgt ist, wird oft sehr mathematisch vorgegangen. Im Kern geht es bei dieser Denkweise also darum, die Auswirkung von Unsicherheit auf Ziele quantitativ zu bewerten und in Zahlen auszudrücken.

Risiko hat hier vor allem die Funktion einer *Versicherung*, die bezifferbar ist. Entscheidungen sollen unter dem Aspekt der Risikominimierung erfolgen. Es soll die optimale Entscheidung erfolgen. Eine weitere Entlastung besteht in dem Objektivitätsanschein durch die starke Verwendung von Mathematik und z.B. von historischen Versicherungs- und Ausfallstatistiken.

Die Nützlichkeit dieser Denkweise soll hier nicht generell infrage gestellt werden. Allerdings kann es leicht passieren, dass die oft so objektiv daher kommenden Risikokennzahlen und die darauf gestützten Entscheidungen, die aus dieser Denkweise resultieren, häufig gar nicht so objektiv und eindeutig sind, wie sie auf den ersten Blick scheinen. Die Gefahren- und Risikoidentifikation und die anschließende Bewertung sind beispielsweise meist stark von subjektiven Präferenzen und Perspektiven abhängig. Auch darüber, ob ein Risikowert akzeptabel ist oder nicht, sagen die Zahlen alleine oft nichts aus.

Zusätzlich gilt vor allem für Betriebsrisiken oder operationelle Risiken, dass die bei der Risikoschätzung verwendeten historischen Daten nur begrenzt hilfreich sind. Entdeckt eine Organisation einen Schaden, so wird sie sich umorgani-

sieren, Kontrollen einführen oder Versicherungen abschließen, um zukünftige Schäden klein zu halten oder auszuschließen. Somit sind die vergangenen Schadendaten aus der Datenbank für operationelle Risiken nicht mehr aussagekräftig, denn die Ursachen für die Schäden, die die Grundlage für die Schadendatenbank bildeten, wurden ja zwischenzeitlich abgestellt. Mit anderen Worten, Betriebsrisiken und operationelle Risiken sind »flüchtig« und jede getroffene Maßnahme gegen diese Risiken entwertet schrittweise die historische Datenbasis.

### 3.3.3 Risiko als soziale Konstruktion

In Anlehnung an Vorarbeiten und Denkansätze der Sozialwissenschaften, der Psychologie und Philosophie gibt es einen zur objektivistischen Denkweise alternativen Ansatz im Umgang mit Risiko.<sup>4</sup> Der Risikobegriff wird auch hier als Rationalisierungsversuch im Umgang mit der zwangsläufigen Unsicherheit der Zukunft angesehen. Es wird aber zugleich berücksichtigt, dass während der Bildung eines Risikobegriffs vielfältige soziale und methodische Selektions- und Verhandlungsprozesse stattfinden. Es wird auch einberechnet, dass Gefahren- und Risikoidentifikation und die anschließende Bewertung oft stark von subjektiven Präferenzen und Perspektiven abhängig sind. Ein sehr klar scheinender Begriff eines bestimmten Risikos stellt sich im Verlauf dieser Prozesse ganz anders dar, als die Teilnehmer anfänglich dachten. Zugleich haben auch die jeweils aktuelle Risikokommunikation beispielsweise in der (Fach-)Presse, die aktuelle eigene Betroffenheit und die zeitliche Nähe oder Entfernung zum Sachverhalt maßgeblichen Einfluss darauf, was als Risiko angesehen wird und wie die quantitative Bewertung ist. Vor diesem Hintergrund bekommt die quantitative Behandlung konkreter Risikodefinitionen einen anderen Stellenwert: Die Quantifizierung kann immer noch nützlich sein, aber sie ist zugleich relativer und kontingenter<sup>5</sup> geworden. Der Eindeutigkeits- und Objektivitätsanspruch tritt dagegen in den Hintergrund. Die Quantifizierung kann nämlich nun dieses oder auch ein anderes Ergebnis liefern – es kommt eben darauf an. Denn aus dieser Sichtweise sind Risiken in der Regel nicht einfach gegeben, sondern müssen immer wieder neu entwickelt und bestätigt werden.

---

4. Wir fassen in diesem Abschnitt pauschal sehr verschiedene Ansätze zum Risikobegriff zusammen.

5. Kontingent bzw. Kontingenz meint die Möglichkeit, dass etwas anders sein *könnte*, als es aktuell *ist*. Beispielsweise könnte ein Risiko, das von einem Experten aufgrund seiner Modellbildungen und Quantifizierungsschritte als hoch eingestuft wurde, von einem anderen Experten möglicherweise anders eingestuft werden, weil er eine andere Modellbildung und Quantifizierung verwendet hat. Die Risikoeinstufung als hoch ist damit kontingent: Sie kann *so* sein, wie sie aktuell *ist*, sie *könnte* aber auch *anders* sein.

**Beispiel: Die Entstehung der operationellen Risiken als Begriff**

Michael Power beschreibt unter dem Titel »Die Erfindung operationeller Risiken« sehr anschaulich den sozialen Konstruktionsprozess eines Risikos<sup>a</sup>:

Wir sind es heute gewohnt, operationelle Risiken als einen der zentralen Risikobegriffe in der Finanzindustrie anzusehen, der – weil so offensichtlich – doch eigentlich schon immer da gewesen sein muss. Wie Power detailliert herausarbeitet, ist dieser Begriff aber erst wenige Jahrzehnte alt. So gab es bis Anfang der 1990er-Jahre in der Finanzindustrie zwar bereits eingeführte Risikokategorien z.B. für die Bewertung von Kreditrisiken. Aber was die Risiken aus der Durchführung der Bankaktivitäten selbst anging, war bis zu den 1990er-Jahren lediglich ein diffuses gesellschaftliches Gefühl vorhanden, dass mit dem Bankgeschäft eine intrinsische Gefahr verbunden ist. Daraufhin entwickelte sich ein mehrjähriger Fachdiskurs, um diese diffuse gespürte Gefahr endlich begrifflich fassen und damit besser greif-, kommunizier- und letztlich kontrollierbar zu machen. Außer Begriffen wie Kreditrisiko war jedoch dazu kein Begriff verfügbar. So wurde der Begriff »operationelle Risiken« geboren und ist seitdem aus der Bankenregulierung nicht mehr wegzudenken.

Hier ist sehr schön ersichtlich, wie aus einer Gefahr, die schon immer beim Bankgeschäft vorhanden war, ein Risiko gemacht wurde. Das operationelle Risiko ist also nicht etwas objektiv Gegebenes, sondern eine Projektion und Rationalisierung eines gesellschaftlichen Unbehagens und Ausdruck des Wunsches, die mit dem Bankbetrieb verbundene latente Gefahr kontrollierbar zu machen. Oder, in direkter Anlehnung an [Power 2007, S. 140]: Die Entwicklung des Begriffs der operationellen Risiken ist »ein Versuch, zu erfassen, was nicht zu erfassen ist, um tiefstzitzende Ängste vor dem Versagen gesellschaftlicher Kontrolle zu besänftigen«.

a. Vgl. dazu auch die ausführliche Darstellung bei [Power 2007].

**3.3.4 Umgang mit Risiko in der Agilität**

In den vorigen Abschnitten wurden zwei Risikobegriffe unterschieden: Risiko *als instrumentelle Kategorie* und Risiko *als soziale Konstruktion*. Gemeinsam ist diesen Risikobegriffen, dass beide den Anspruch haben, bewusst(er) mit der prinzipiellen Unsicherheit der Zukunft umzugehen. Zugleich wurde herausgearbeitet, dass in beiden Risikobegriffen zwar mehr oder wenig objektive Anteile enthalten sind, aber dass sie in der Regel nicht einfach objektiv gegeben sind, sondern stets auch soziale Konstruktionen sowie Entscheidungen mitenthalten sind. Mithin sollte bei der Arbeit mit Risiken immer auch ihr Kontingenzgehalt berücksichtigt werden.

Für den Perspektivwechsel zur Agilität ist es wichtig, über die besonderen Eigenschaften beider Ansätze informiert zu sein. In Anwendungsgebieten mit klar(er) anerkannten Wissensbeständen, stabiler Organisation und stabilem Umfeld, kann der Umgang mit Risiken stärker quantitativ basiert sein und damit normativer organisiert werden. Hier ist man näher am Risikobegriff als instrumentelle Kategorie. In innovativen oder sich dynamisch verändernden Anwendungsgebieten dagegen ist es besser, sich am Risikobegriff als soziale Konstruktion zu orientieren. Hierbei werden zunächst verschiedene Experten zurate

gezogen und die verschiedenen Perspektiven werden dann in der Kommunikation zusammengeführt, um so zu einer gemeinsamen Einschätzung zu gelangen.

Zugleich kann es gerade bei der Exploration von Themenstellungen hilfreich sein, Risiken als Instrument der Aufmerksamkeitsbindung einzusetzen, ohne zugleich alles quantifizieren zu wollen oder zu müssen. Damit können Risiken über ihre engere Funktion als Rationalisierungsinstrument für diffuse Gefahren zu einem wirkungsvollen Führungsinstrument werden.

Das führt auch dazu, dass das Thema der Risikokommunikation immer mehr an Bedeutung gewinnt. Hier ist jedoch zugleich Aufmerksamkeit geboten. Wie Untersuchungen aus der Psychologie zeigen, lässt sich die Risikowahrnehmung bei Menschen nämlich stark durch aktuelle Risikokommunikation beeinflussen und verzerren. Aufgrund psychologischer Prozesse kann sich dadurch die subjektive Einschätzung von Risiken schnell von objektiven (nicht zwangsläufig nur quantitativen) Grundlagen entfernen. So fließt oft schon die Häufigkeit der Erwähnung eines Risikos in den Tagesnachrichten oder das Verschwinden der Erwähnung in die subjektive Bewertung der Relevanz eines Risikos ein. Oder auch die zeitliche bzw. räumliche Nähe oder Entfernung eines Risikos hat einen großen Einfluss.

Vor dem Hintergrund der hier vorgestellten Überlegungen zum Risikobegriff ist deshalb das zentrale Merkmal der Agilität, in kleinen Schritten vorzugehen, ein idealtypisch risikoorientierter Ansatz:

- Durch das Vorgehen in kleinen Schritten wird das noch unkalkulierbare Risiko nicht unangemessen groß. Es werden zunächst erste Erfahrungen gesammelt, indem die Organisation verschiedene Methoden ausprobiert, um das Risiko zu behandeln. Aus der Reaktion von Organisation und ihren Umwelten auf die Risikobehandlung kann das Verhalten des Risikos und damit mögliche Risikoursachen besser eingeschätzt werden.
- Bereits die naturwissenschaftliche Begriffsbildung und unsere persönlichen Erfahrungen mit der Wettervorhersage zeigen, wie wichtig der Zeithorizont für die Prognosegüte des Risikos ist. Ein Schaden in naher Zukunft (Hochwasser trifft Rechenzentrum in den nächsten fünf Minuten) lässt sich besser vorhersagen als ein Schaden für eine weit entfernte Zukunft (Hochwasser trifft Rechenzentrum im nächsten Jahr).

Agile Organisationsformen priorisieren daher die – nach Übereinkunft der Stakeholder – größten Herausforderungen und versuchen zunächst für die wichtigsten Probleme eine Lösung zu finden. Statt lange zu planen, wie das Risiko gemessen und gemanagt werden könnte, werden in kurzer Zeit erste Ideen zur Risikobewältigung umgesetzt und ihre Wirksamkeit ausprobiert, um dann im Dialog mit den Stakeholdern die gemeinsamen Erfahrungen zu diskutieren. Aus den Erfahrungen heraus werden dann weitere Hypothesen zur Bearbeitung des

Risikos aufgestellt und daraus weitere Maßnahmen zur Risikobehandlung entschieden und beobachtet, wie sie dann wirken.

#### **Denkanstöße zum Risikobegriff**

Die folgenden Fragen haben sich als Denkanstöße für eine Standortbestimmung in Bezug auf einen differenzierten Umgang mit dem Risikobegriff bewährt. Wenn wir in unserer Organisation von Risiko reden:

- Wo verwenden wir eher das instrumentelle Verständnis im Umgang mit Risiken?
- Wo verwenden wir eher das Verständnis eines sozial ausgehandelten Begriffs?
- Erscheint uns der Umgang mit Risiken vor dem Hintergrund des hier beschriebenen Spektrums angemessen? Oder (zu) einseitig? (Zu) Einseitig zu welcher der beschriebenen Seiten hin?
- Werden vor allem bei neuen Themen auch entsprechende Konsultationen für die Definition und Bewertung von Risiken durchgeführt? Wer ist vertreten? Wer fehlt? Erscheint die Beteiligungsmöglichkeit angemessen?
- Wird Risiko als etwas gesehen, was die Organisation durch nachhaltige Handlungen dauerhaft bewältigen kann? Oder ist Risiko vielmehr eine Begleiterscheinung der Organisation, die von vielen Mitarbeitern beobachtet und kommuniziert wird? Erfolgt eine permanente Nachadjustierung der organisatorischen Risikobehandlung?
- Wie wird bei uns Risikokommunikation betrieben? Wird sie als Führungsinstrument eingesetzt? Geschieht dies angemessen oder tendenziös?

### **3.4 Wirklichkeit ist immer die Wirklichkeit eines Beobachters**

Die Facette der beobachterabhängigen Wirklichkeit mag zunächst sehr theoretisch klingen. Aber sie ist unseres Erachtens von höchster praktischer Bedeutung für den agilen Perspektivwechsel. Wir beschreiben zunächst erkenntnistheoretische Grundlagen, wonach Wirklichkeit immer nur indirekt über Beobachtungen wahrnehmbar ist. Anschließend gehen wir darauf ein, wie Agilität diese Einsicht konstruktiv nutzt und warum kommunikative Aushandlungsprozesse so wichtig dabei sind.

#### **3.4.1 Die Rolle des Beobachters bei der Erzeugung von Wirklichkeit**

Wann immer wir von Wirklichkeit reden, sind Beobachter beteiligt, die mit ihren Sinnen (z.B. Augen und Ohren) zunächst Reize in der Welt wahrnehmen. Diese Reize sind nach aktuellem Stand der Forschung jedoch nicht unmittelbar schon selbst die Information, um die es geht, sondern lediglich Anregungsbedingungen für die Eigenaktivität unserer Wahrnehmungssinne. Diese Eigenaktivitäten, z.B. Selektion und Konstruktion, machen erst daraus etwas in unserem Kopf, was