

25. November 2010

Risikoanalyse als Geschäftsmodell – Ein Bericht aus der Praxis

Die Kernkompetenz von Munich Re liegt darin, Risiken aller Art zu analysieren, zu bewerten und zu managen. Dies gilt für Risiken unserer Kunden sowie der eigenen.



Michael Lardschneider
Global Security and Continuity Risk
Management
Chief Security Officer

1 Gefahren und Risiken

Munich Re befasst sich seit über 125 Jahren mit Gefahren und Risiken aller Art. Diese lassen sich unter verschiedenen Überschriften zusammenfassen.

1.1 Naturgefahren

Gefahren können ausgehen

- von der Erde; sie äußern sich z.B. in Form von Erdbeben, Erdrutschen, Kraterbildungen
- vom Wasser; sie äußern sich z.B. in Form von Überschwemmungen, Tsunamis, der Senkung des Grundwasserspiegels
- von Feuer; diese zeigen sich z.B. in Form von Waldbränden, Vulkanausbrüchen
- von der Luft; diese zeigen sich z.B. in Form von Stürmen und Hurrikans, Starkregen
- vom Wetter; diese manifestieren sich in Form von überdurchschnittlichen Kälte-, Hitze-, Feuchtigkeits- und Trockenperioden sowie dem Klimawandel im Allgemeinen

1.2 Anthropogene Gefahren

Die nicht natürlichen sondern vom Menschen direkt oder indirekt verursachten Gefahren gliedern sich wie folgt.

1.2.1 Gefahren des Zusammenlebens und der Entwicklung

Gefahren können ausgehen

- vom Individuum und führen z.B. zu von Pandemien, Burn-out-Erkrankungen, menschlichen Fehlhandlungen
- von der Gesellschaft und äußern sich in Form vom Wandel der Werte, Terrorismus, Piraterie, organisierter Kriminalität, Krieg und kriegerischer Handlungen, Anonymität

- vom Fortschritt (im weitesten Sinne) und zeigen sich z.B. als Konsequenzen der Biotechnologie, Gentechnologie, Nanotechnologie sowie der Mode

1.2.2 Gefahren der Technik

Gefahren können ausgehen von der „Technik“. Sie stecken in

- Gebäuden wie z.B. Hochhäusern, anderen Bauwerke und Verkehrsmitteln deren Betrieb und Nutzung häufig die Grenzen der Beherrschbarkeit aufzeigen
- Versorgungsinfrastrukturen und zeigen sich z.B. in Form von Stromausfällen und Verbreitung von Computerviren die Steuerungsanlagen beschädigen
- der Informations- und Kommunikationstechnik und führen z.B. zu Identitätsdiebstahl, Informationsverlust und dem Verlust der Privatsphäre

1.2.3 Weitere Gefahren

Auch wenn die oben vorgenommene Einteilung nicht perfekt sein mag, so gibt es noch schwerer greifbare und damit einer Kategorie eindeutig zuordenbare Gefahren. Dazu gehören

- der Zeitdruck, der z.B. führt zu Qualitätsverlust, Überforderung des Menschen
- die Regulierung, die sich z.B. äußert in Form von Funktionseinschränkungen und gefühltem Verantwortungsentzug
- der Wettbewerb, der sich z.B. negativ zeigt in Form von Wirtschafts- und Konkurrenzspionage oder vorsätzlichen kriminellen bzw. unlauteren Handlungen

Diese Liste ließe sich noch um viele Gefahren fortführen und ist demnach nicht vollständig.

1.3 Auswirkungen auf die Versicherungswirtschaft

Die genannten aber noch weitere Gefahren betreffen die Versicherungswirtschaft früher oder später. Schadensfälle wirken sich oft nicht nur auf eine sondern mehrere Versicherungsbranchen aus. Das sollen folgende Beispiele ansatzweise zeigen:

- Seebeben verursachen Tsunamis die u.a. erhebliche Schäden an Gebäuden, deren Inhalt (Hausrat) anrichten, Menschenleben kosten, Ernten vernichten, Verkehrswege unterspülen
- Lange anhaltende Regenfälle führen zu Überschwemmungen, die u.a. erhebliche Schäden an Gebäuden und deren Inhalt anrichten, Menschenleben kosten, Ernten vernichten, Seuchen verursachen
- Anarchie fördert in manchen Regionen dieser Welt die Piraterie. Diese wiederum hat Einfluss auf das einwandfreie Funktionieren von Lieferketten und damit die Produktion
- Übergewicht ist eine der Hauptursachen für Krankheiten und Todesfälle

- Globaler Reiseverkehr ermöglicht die schnelle Verbreitung von Viren und Krankheiten über tausende von Kilometer. Pandemien sind die Konsequenz. Gesundheit und Leben vieler Menschen sind bedroht. Aus Vorsorgegesichtspunkten führen sie auch zu Produktionsunterbrechungen
- Weltraumwetter ist eine in der Öffentlichkeit bislang nur wenig bekannte Ursache für Schäden, z.B. an Satelliten. Deren Ausfall oder Fehlfunktion beeinträchtigt Lieferketten und die Produktion
- Computerviren sind heute keine Besonderheit mehr, können aber inzwischen erheblichen globalen Schaden anrichten, z.B. an IT-basierten Steuerungssystemen. Von diesen wiederum hängt die Versorgungsinfrastruktur ab. Computerviren können zu Maschinenbruch führen, die Gesundheit bedrohen oder sogar den Tod einzelner Menschen zur Folge haben
- Digitalisierung, beispielsweise der Einsatz von IT-Technik in modernen Fahrzeugen äußert sich in zunehmenden Rückrufaktionen wegen Defekten, was wiederum die Produkthaftung betrifft
- Identitätsdiebstahl ist eine Form der Kriminalität. Dieser hat zur Folge, dass Menschen für Aktionen in Haftung genommen, die sie gar nicht durchgeführt haben

2 Risiken und Chancen für Munich Re

Munich Re beschäftigt sich aufgrund ihres Geschäftsmodells mit allen oben genannten und noch weiteren Risiken. Dabei wird streng darauf geachtet, dass es nicht dazu kommt, aufgrund der Interdependenzen, Risiken in einer, den gesteckten finanziellen Rahmen übertreffenden Höhe zu tragen. Ausgefeilte Maßnahmen kommen zum Einsatz, um die übernommenen Risiken managen und unter anderem Kumulsituationen kontrollieren zu können.

Sehr wichtig ist auch die Betrachtung des Reputationsrisikos. Munich Re's Reputation ist eng verknüpft mit der professionellen Art des Risikomanagement.

Aus dem Umgang mit Risiken aller Art lässt sich allerdings auch viel lernen und erfahren. Risiken die andere Unternehmen betreffen, sind häufig auch für den Betrieb von Munich Re relevant. Die an Munich Re gemeldeten Schäden und Schadenursachen lassen sich häufig gut in Statistiken überführen und damit zu einer Verbesserung des Risikomanagements nutzen.

Fazit: in der Tatsache dass sich Munich Re mit Risiken beschäftigt, liegt auch die große Chance das Wissen über Gefahren, Risiken und Schäden geschäftsfördernd einzusetzen.

Dieses Wissen wird in verschiedenen Datenbanken gepflegt. Ergebnisse von Gutachten, Knowhow der eigenen Experten, Inhalte spezieller externer Datenbanken, Resultate aus Kontakten mit externen Netzwerken, statistische Berechnungen etc. werden bei Munich Re zusammengeführt mit dem Ziel, zukünftige Entwicklungen immer präziser „vorhersagen“ zu können. Fakten und

Forschungsergebnisse, beginnende, mögliche und vollendete Katastrophen sind dort erfasst und dienen als Basis für Auswertungen. Informationen über das Beben der Erdkruste, die Höhe der Wellen auf den Meeren, Schmelzraten der Gletscher, Terrorvorfälle, Pandemien und Seuchen in allen Orten dieser Welt, Kriminalitätslagen, Zins- und Währungsschwankungen und weitere sind darin enthalten. Die Erkenntnisse zur Entwicklung der Nanotechnologie, der Ölförderung, des Schiffs-, Flugzeugs- und Satellitenbaus, der Piraterie vor Somalias Küste, das Weltraumwetter usw. fließen ebenfalls in die Modellierung der Risiken ein.

Das bei Munich Re in Entwicklung befindliche Early Warning System hat erst kürzlich bewiesen, dass man auf dem richtigen Weg ist. Retrospektiv konnte damit nachgewiesen werden, dass die im Internet verfügbaren Informationen ein sehr gutes Indiz für bestimmte Entwicklungen sind. So „wusste“ das Internet schon zwei Wochen bevor es in Mexiko in 2008 offiziell zum Ausbruch der Schweinegrippe kam, dass sich eine Pandemie entwickelt. Dieses Early Warning System wird weiter ausgebaut, um noch bessere Ergebnisse zu liefern.

3 Risikomanagement

Der Risikomanagementprozess ist bereits in einer Vielzahl von Veröffentlichungen beschrieben. Hier wird auf diesen Prozess nur im Zusammenhang mit Security und Continuity Risiken eingegangen.

Er wird initiiert durch die Erkennung einer oder mehrerer Gefahren.

Aus diesen Gefahren werden Risiken für das Unternehmen, das Projekt, das Vorhaben, das Individuum oder die Gesellschaft abgeleitet (Risikoidentifikation). Dabei spielt vor allem die subjektive Wahrnehmung dieser Risiken eine bedeutende Rolle. Die als relevant erkannten Risiken gilt es zu analysieren und möglichst objektiv zu bewerten. Dabei werden insbesondere die Eintrittswahrscheinlichkeit und die potenzielle Schadensauswirkung unter Beachtung der Verwundbarkeit betrachtet und soweit möglich mit Zahlen (quantitative Bewertung) belegt.

Die anschließende, zur angemessenen Risikobehandlung zu treffende Entscheidung über den Umgang mit dem analysierten Risiko basiert einerseits auf den gewonnenen Erkenntnissen aber auch auf der Art und Weise wem und wie diese präsentiert werden.

Wurde die Entscheidung einmal getroffen und bestimmte Maßnahmen zur Handhabung des Risikos beauftragt oder dieses als unabwendbar festgelegt, gilt es, die Entwicklung des Risikos zu verfolgen und ggf. erneute Entscheidungen zu treffen.

3.1 Risikoidentifikation

Vor allem sozio-kulturelle Faktoren spielen im Prozessschritt der Risikoidentifikation eine Rolle. Sie beeinflussen die subjektive Wahrnehmung eines Risikos:

- **Wahlmöglichkeit:** Besteht die Möglichkeit selbst zu entscheiden, ob man ein Risiko eingeht oder ist man dazu gezwungen? Beispiel: ein Hobby-Fallschirmspringer geht mit seinem Sport freiwillig ein Risiko ein.
- **Kontrollierbarkeit:** Hat man das Gefühl, ein Risiko selbst kontrollieren zu können? Beispiel: Als Fahrer eines Kfz ist man häufig der Meinung, das Risiko eines Unfalls selbst in der Hand zu haben, als Beifahrer fühlt man sich dagegen oft nicht in dieser Rolle.
- **Abwägung:** Kann man das Risiko mit dem Nutzen vergleichen? Beispiel: ein Unternehmensgründer muss ein gewisses Risiko eingehen, um seine Geschäft aufzubauen. Diese Abwägung verläuft anders als bei einem bereits gut etablierten Unternehmen.
- **Persönliche Betroffenheit:** Risiken von denen man selbst nicht direkt betroffen ist, werden häufig als geringer angesehen. Beispiel: Atomkraftgegner die in unmittelbarer Nachbarschaft von atomaren Anlagen wohnen, sehen die mit dieser Art der Energieerzeugung verbundenen Risiken kritischer als Menschen, die vermeintlich unerreichbar weit weg von diesen Anlagen wohnen.
- **Schrecklichkeit des möglichen Schadens:** Die Vorstellung einer Bombenexplosion auf einem stark von Menschen frequentierten Platz führt zu einem höheren Unwohlgefühl als die Vorstellung eines weniger blutigen, Vorfalles.
- **Vertrauensgrad:** Risiken, die von einer glaubwürdigen Institution dargestellt werden, führen zu einer kritischeren Auseinandersetzung mit diesen als Risiken, die von Einrichtungen aufgezeigt werden, die damit vermeintlich Eigeninteressen verfolgen oder nicht glaubhaft erscheinen.
- **Verantwortlichkeit:** Risiken, die ihren Ursprung in der Natur haben, z.B. die eines Vulkanausbruchs, erfahren eine andere Betrachtung als Risiken, die menschengemacht sind, wie zum Beispiel die der Instabilität von Wolkenkratzern.
- **Schadenseintrittstermin:** Je diffuser der Zeitpunkt ist, wann ein Schadensereignis eintritt, zum Beispiel die Erkrankung an Lungenkrebs, desto weniger setzt sich der Mensch mit diesem Risiko auseinander.

Fazit: Es gilt die Fähigkeiten, Risiken wahrzunehmen und deren Höhe zu sachlich beurteilen, zu schärfen.

3.2 Risikobewertung

Im Versicherungswesen spielt die quantitative Bemessung von Eintrittswahrscheinlichkeit und Schadenhöhe eine sehr große Rolle. Viele Risiken können heutzutage bereits gut berechnet, das heißt quantifiziert werden. Manche Risiken allerdings, und dazu gehören Risiken die die öffentliche

Sicherheit betreffen, lassen sich eher qualitativ bewerten. Trotzdem steigt der Druck auch dafür Quantitäten festzulegen. Zahlen dienen dem modernen Menschen sehr häufig bei der Erfüllung der Sehnsucht nach etwas Greifbarem.

Ab einem gewissen Abdeckungsgrad und damit der Möglichkeit repräsentative Aussagen treffen zu können, ist die Zuverlässigkeit der Mathematik eine sehr wichtige Grundlage für die Bewertung von Risiken. Bei der quantitativen Bewertung von Risiken spielt auch die Betrachtung von Akkumulations- und Kaskadeneffekten eine Rolle.

Weitere Kriterien sind folgende:

- Ubiquität: Lässt sich die räumliche Ausbreitung eines potenziellen Schadens bestimmen, z.B. bei einem Erdbeben oder ist diese kaum greifbar wie beispielsweise bei der Verbreitung eines Computervirus via Internet?
- Persistenz: Ist es möglich die zeitliche Ausdehnung eines Schadens weitgehend einzugrenzen, z.B. bei einem Sturmereignis oder ist dies nicht möglich wie bei der pandemischen Verbreitung einer neuen Erkrankung?
- Reversibilität: Kann der Ursprungszustand wieder hergestellt werden, z.B. bei dem Einsturz einer Brücke oder ist dies kaum möglich wie bei asbestverursachten Erkrankungen?
- Latenzzeit: Tritt der Schaden unmittelbar nach Eintreten des Ereignisses auf, z.B. bei Stromausfall oder liegen zwischen Ereignis und Schaden ggf. mehrere Monate oder Jahre wie beispielsweise bei Informationsdiebstahl?
- Ungewissheit: Wie vorhersagbar sind Verlauf und Konsequenzen eines Schadensereignisses?

Fazit: Es gilt, die Risikobewertungsverfahren weiter zu verbessern, z.B. durch die zielgerichtete Auswertung von Schäden und Erzeugung von Statistiken und Trendanalysen.

3.3 Risikobehandlung

Mit identifizierten Risiken lässt sich sehr unterschiedlich umgehen. Die Konsequenzen der diesbezüglich zu treffenden Entscheidung lassen sich dem Bereich Risikokontrolle (aktive Maßnahmen, ein Risiko zu reduzieren) oder dem der Risikofinanzierung (Abwälzung und finanzielle Vorsorge) zuordnen. Bedingt besteht die Möglichkeit Kontrolle und Finanzierung zu kombinieren.

Die Risikokontrolle ist in dreierlei Hinsicht möglich:

- Vermeiden: Es werden alternative Lösungen gesucht, die das festgestellte Risiko nicht aufwerfen oder es wird Verzicht geübt, indem bestimmte Risiken nicht eingegangen werden und damit auch Chancen unterbleiben.
- Vorbeugen: Es werden Präventionsmaßnahmen ergriffen, um Schäden soweit möglich und sinnvoll vorzubeugen bzw. um im Schadenfall angemessen vorbereitet zu sein.
- Minimieren: Es werden bauliche, technischen, organisatorische bzw. juristische sowie Schulungsmaßnahmen ergriffen, um Risiken zu minimieren.

Im Bereich der Risikofinanzierung wird unterschieden zwischen folgenden zwei Aspekten:

- Transferieren: Das Risiko wird auf einen oder mehrere Dritte abgewälzt, z.B. indem eine Versicherung abgeschlossen wird, die eintretende Schäden ganz oder teilweise übernimmt.
- Behalten: Das Risiko wird als solches in vollem Umfang akzeptiert. Um die finanziellen Konsequenzen eines daraus resultierenden potenziellen Schadens tragbar zu machen, wird für den Fall der Fälle ausreichend Kapital reserviert.

4 Entscheidungsfindung

Wie oben beschrieben, sind Risiken nicht ausschließlich auf Basis deren Eintrittswahrscheinlichkeit und den mit Gegenmaßnahmen oder Schäden verbundenen finanziellen Konsequenzen zu behandeln. Daher gilt es, dem haftenden Entscheider bzw. dem Entscheidungsgremium alle relevanten Informationen, die mit der zu treffenden Entscheidung zusammenhängen darzustellen. Folgenden Punkten ist dabei entsprechende Aufmerksamkeit zu widmen:

- Finden des richtigen Entscheidungsträgers: Die Aussage „Ich trage das Risiko“ ist, je nach subjektiver Risikowahrnehmung der betreffenden Person, schnell getan. Die Frage, ob diese Person oder das Gremium ein bestimmtes Risiko überhaupt tragen kann, ist zu stellen. Ggf. ist die Entscheidung zu eskalieren bzw. durch die übergeordnete Instanz zu prüfen und freizugeben.
- Sachverhalt und Risiko verständlich vermitteln: Häufig ist die Komplexität eines Vorgangs sehr hoch und die damit verbundenen Risiken wenig konkret. Damit ist beides kaum greifbar. Wichtig ist es, insbesondere wenn Entscheider fachlich wenig Wissen über einen bestimmten Sachverhalt oder ein Risiko haben, beides auf geeignete Weise darzustellen.
- Potenzielle Schadensauswirkungen sachlich darstellen: Die Risikowahrnehmung hängt unter anderem von der persönlichen Betroffenheit und der Schrecklichkeit des potenziellen Schadens ab. Es gilt auf sachliche Art und Weise die wahrscheinlichen Schadensszenarien so darzustellen, dass weder Angst geschürt noch Zweckoptimismus verbreitet wird.
- Eintrittswahrscheinlichkeit greifbar präsentieren: Häufig lassen sich keine Zahlen dafür finden. In diesen Fällen eignet sich der Versuch, eine Vergleichbarkeit mit Schadenswahrscheinlichkeiten ähnlicher Risiken herzustellen.
- Vermitteln der Haftungssituation des Entscheidungsträgers: Entscheider die für die Konsequenzen ihrer Entscheidung zwar verantwortlich sind, aber nicht in der rechtlichen Haftung stehen, befinden über den Umgang mit Risiken häufig anders als die haftenden Personen selbst. Daher gilt es die Haftungsfrage aufzuwerfen und die Situation zu vermitteln bevor die Diskussion über die Art, ein bestimmtes Risiko zu managen zu weit fortgeschritten ist.

- Realistische Handlungsoptionen aufzeigen: Aussagen, bestimmte Technologien einzusetzen, um manche Risiken zu reduzieren, sind oft Blendwerk. Wichtig ist realistische Ansätze herauszuarbeiten und der Entwicklung unrealistischer entgegen zu wirken.
- Handlungsempfehlungen durch Fachexperten aussprechen: nicht jeder wird als kompetent angesehen, bestimmte Risiken zu bewerten. Daher macht es der Mix aus Autoritätspersonen, Fachexperten und neutraler Beobachter aus, Risiken darzustellen und vor allem Maßnahmen für den geeigneten Umgang mit diesen zu erläutern.
- Erfahrung mit ähnlich gelagerten Fällen einbringen: nicht jedes Risiko ist völlig neu. Es gibt Parallelen zu anderen Risiken und Bewertungs- und Entscheidungsvorgängen. Diese sind aus Gründen der besseren Orientierung anzuführen. Auch die daraus resultierenden Erfahrungen dienen sehr häufig dazu, Entscheidungen zur richtigen Risikobehandlung positiv zu beeinflussen.

Grundvoraussetzung für das erfolgreiche Durchlaufen des gesamten Prozesses ist, dass dieser von „neutraler“ Stelle aus getrieben wird. Neutral ist eine Stelle im Unternehmen, der Behörde oder der Einrichtung, wenn sie selbst nicht als Risikoträger (aktiver Verstärker oder Reduzierer des betreffenden Risikos) auftritt. Nur so lässt sich ein risikoorientiertes Vorgehen erreichen. Diese Stelle muss außerdem eine fachliche übergreifende Rolle einnehmen, das heißt die Risiken im Gesamtzusammenhang betrachten können.

5 Praktische Umsetzung bei Munich Re

Munich Re besteht derzeit aus vier Geschäftsfeldern, die Munich Re Rückversicherung, Munich Health (Gesundheitsversicherung), ERGO (Erstversicherung) und MEAG (Asset Management). Die Verantwortung für das Management aller in diesen Geschäftsfeldern übergreifenden Risiken obliegt dem Chief Risk Officer (CRO) und seinem Team im Integrierten Risk Management.

Dazu gehört auch die Schaffung und Verbesserung der Verfahren, um Security und Continuity Risiken zeitnah zu identifizieren, zu bewerten, zur Entscheidung zu bringen und die Umsetzung der Maßnahmen sicherzustellen. Der Chief Security Officer (CSO) und seine Organisation sind dafür fachlich übergreifend zuständig.

Diese Zuständigkeit wurde in einem Modell zusammengefasst, dem sogenannten „Security and Continuity Risk Management Modell (SCRM Modell)“. In diesem wird die fachliche übergreifende Zuständigkeit dargestellt:

- Security Risk Management mit dem Ziel, die Eintrittswahrscheinlichkeit von Schäden zu reduzieren (Vorbeugung und Vorsorge)
- Continuity Risk Management mit dem Ziel, die Auswirkungen von Schäden auf ein tragbares Maß zu reduzieren (Vorfallsmanagement und Nachsorge)
- Escalation Management mit dem Ziel, die Gefahrenlage zu beobachten und zu bewerten, die Bearbeitung abstrakter und konkreter Gefahren auf Basis

dieser Bewertung zu eskalieren als auch im Fall der Fälle die Lageberichterstattung zu gewährleisten

Da Security und Continuity Risk Management bei Munich Re gesamtheitlich betrieben wird, ist dieses Modell auf folgende Schutzziele ausgerichtet:

- Schutz von Leib und Leben sowie der Handlungs- und Willensfreiheit von eigenen und Fremdfirmenmitarbeitern als auch Besuchern und Gästen
- Schutz von Veranstaltungen mit rechtlicher Relevanz bzw. erhöhter öffentlicher Aufmerksamkeit, z.B. Hauptversammlung
- Schutz der Vertraulichkeit, Integrität und Verfügbarkeit digitaler und nicht-digitaler Informationen
- Schutz der Verfügbarkeit und Funktionsfähigkeit der Infrastruktur (Informations- und Kommunikationstechnik, Gebäude und Inventar)
- Gewährleistung der Aufrechterhaltung des Geschäftsbetriebs entlang der gesamten Wertschöpfungskette, d.h. Management von Security und Continuity Vorfällen, Notfallmanagement, Krisenmanagement, Wiederherstellungsmanagement

Um diese Schutzziele zu erreichen und die dafür erforderlichen strategischen Maßnahmen ausgestalten zu können, wurde dem CSO und seiner Organisation vom Gesamtvorstand ein Mandat erteilt, das Security und Continuity Risk Management in allen Geschäftsfeldern von Munich Re umfasst.

6 Ausblick

Verschiedene technische Trends (Miniaturisierung, Vernetzung, Digitalisierung und Künstliche Intelligenz) sowie gesellschaftliche Trends (Globalisierung, Wettbewerb, Monopolisierung, Mobilität, Information, Mode) werden in der Zukunft weiterhin vorhandene aber auch neue Risiken bergen für die Arbeitsplatzsicherheit, Informationsauthentizität, Demokratie, Privatsphäre, Meinungsfreiheit, Gesundheit, Finanzsystemstabilität und weitere Aspekte.

Damit verbunden sind auch, wie anfangs schon beschrieben, diverse Chancen, die es zu nutzen gilt. Ein professionelles Risikomanagement ist damit zugleich die Grundlage für ein gutes Chancenmanagement.

Je früher also Risiken identifiziert und bewertet werden können, desto besser lassen sich daraus Chancen ableiten bzw. diese frühzeitig nutzen.

25. November 2010

Munich Re
Risikoanalyse als
Geschäftsmodell – Ein Bericht
aus der Praxis
Seite 10/10

Autor und Referent

Der Autor ist seit 1983 Mitarbeiter von Munich Re. Erste Berufserfahrungen sammelte er im Bereich der Einbruchdiebstahl- und Raubversicherung als Berater in der Schadensprävention. Aufgrund seiner Affinität zu IT-Fragestellungen wechselte er 1989 in den Zentralbereich IT. Dort begegnete er sehr bald der Herausforderung, Computerviren zu analysieren und mit Schadsoftware befallene IT-Systeme und –Netzwerke von diesen zu befreien. Er war der erste Computervirenschutzbeauftragte von Munich Re.

1994 wurde er zum IT-Sicherheitsbeauftragten des Mutterhauses in München benannt und verantwortete 1997/98 die Leitung des internationalen Security-Projekts namens „Alcatraz“. Ergebnisse dieses Projekts waren das erste globale Informationssicherheitsregelwerk für die Rückversicherungsgruppe und die gruppenweite Sicherheitsorganisation. Er übernahm als Chief Information Security Officer (CISO) 1999 deren Leitung. In dieser Rolle berichtete er an den CIO der Rückversicherungsgruppe.

Anlässlich einer Umorganisation von Munich Re wurde die Rolle des Chief Security Officers (CSO) geschaffen und organisatorisch als Teil des Integrierten Risikomanagement etabliert. Seit 2008 leitet der Autor als CSO die gruppenweite Security und Continuity Risk Management Organisation. Er trägt damit die fachliche wie organisatorische Verantwortung, dass Verfahren zur Gewährleistung des Schutzes von Mitarbeitern, Informationen und der Infrastruktur sowie zur Aufrechterhaltung des gesamten Geschäftsbetriebs entlang der Wertschöpfungskette erarbeitet werden und deren Umsetzung sichergestellt ist.

Michael Lardschneider
Tel.: +49 (89) 3891-5403
Fax: +49 (89) 3891-75403
MLardschneider@munichre.com

Münchener Rückversicherungs-Gesellschaft
Aktiengesellschaft in München
Königinstraße 107, 80802 München