Fotonachlese RiskNET Summit 2015

Risikofaktor Mensch bleibt riskant

Volles Haus beim RiskNET Summit 2015.

Im Rahmen des RiskNET Summit 2015 in Ismaning bei München eröffnete Initiator Frank Romeike mit den Worten, dass es wichtig sei, von der Risikobuchhaltung wegzukommen. Vielmehr zähle es, dass sich Risikomanagement endlich zu einer strategischen Steuerungsrolle und strategischen Sicht entwickle. Wie wichtig eine solche Strategie ist, zeigte sich im Laufe der zweitägigen Fachkonferenz zu den Themen Risikomanagement, Governance und Compliance. Eine der Erkenntnisse bei allen Themen, Trends und Thesen: Am Menschen führt kein Weg vorbei. Eine weitere Erkenntnis: Ohne Methodenkompetenz bleibt der Wandlungsprozess ein Wunschtraum.

Der Mensch als Ursache einer „Welt ohne Weltordnung“

„Von 183 Staaten befinden sich nach Zahlen der Vereinten Nationen ein Drittel im Zerfall“, erklärte Dr. Günther Schmid zu Beginn seines Vortrags im Rahmen des RiskNET Summit 2015. Schmid, der als Experte für internationale Sicherheitspolitik und globale Fragen gilt, wurde vor den mehr als 100 Teilnehmern aus Wirtschaft und Wissenschaft am 14. Oktober in Ismaning deutlich. „Wir stehen vor einer historischen Zäsur“, brachte es der Sicherheitsexperte auf den Punkt und meinte, dass wir inmitten einer Welt „ohne Weltordnung“ stehen. Es gibt viele Fragen, vor denen auch die politischen Akteure im Hintergrund stehen.

Beispielsweise betreibe der Planungsstab des Auswärtigen Amts seine Krisenanalysen nur noch maximal vier Wochen im Voraus. Die Ursache liegt auf der Hand: Terror und Kriege lassen aktuell keine weitreichenden Planungen in die Zukunft zu. Und die Konfliktherde sind vielfältig, lokal, regional und global. Der beschleunigte Machtzerfall auf regionaler Ebene ist ein Dilemma. Angefangen von Syrien, dem Irak oder Libyen herrschen keine geordneten Strukturen mehr. „Die arabische Zivilisation ist zerfallen“, machte Schmid die Folgen von jahrelangen (Bürger-)Kriegen deutlich.

Nach Einschätzung Schmids stelle der Islamische Staat (IS) eine große Gefahr für die globale Gesellschaft dar. Zumal mit der Ausrufung des Kalifats durch den IS erstmalig eine Terrororganisation ein eigenes Staatsgebilde ausgerufen hat. Schafft es der IS, Grenzen seines selbsternannten Kalifats zu festigen, müssen zukünftig auch die Machthaber in Rakka in diplomatische Prozesse um regionale Fragen eingebunden werden. Spätestens dann, wenn das Assad-Regime fällt und es zu einer Neugliederung Syriens kommt. Dabei handele es sich nach den Worten Schmids beim IS um eine Terrororganisation mit neuer Qualität, die das Überwinden der nationalstaatlichen Ordnung sucht. „Der IS ist ein totalitäres System“, so der Sicherheitsexperte. Etwas weiter gefasst handelt es sich beim IS als Dschihadismus um den dritten großen Totalitarismus, der auf den Faschismus und Stalinismus folgt.

Wir leben in einer Welt „ohne Weltordnung“, brachte es der renommierte Sicherheitsexperte Dr. Günther Schmid auf den Punkt.

Köhler: „Das Sicherheitsniveau bei Cyberrisiken kommt erst voran, wenn es agiler wird.“

Robert Ebel, Chief Risk Officer: „Risikomanagement ist bei Hoerbiger als Bestandteil des Planungsprozesses integriert.“

Interaktion, Kommunikation und Orientierung standen im Vordergrund.

Als dritte Ebene benannte Schmid die globale Ebene als Herausforderung im geopolitischen Umfeld. Die Veränderungen der globalen Machtverhältnisse mit einem Globus ohne Gravitationspunkt führen zu einer sogenannten „Zero-Polaren-Welt“. Eine Verschiebung der bekannten Normen und Wertvorstellungen wirft gleichzeitig die Frage auf: Was heißt heute Dritte Welt, wenn die Zweite Welt zusehends zerfällt? Mit solchen Begriffen sei die Welt von heute und morgen nicht mehr abzubilden ist sich Sicherheitsexperte Schmid sicher. Im Grunde haben wir es mit einem Transformationsprozess auf allen drei Ebenen zu tun, mit einem ungewissen Ausgang. Es herrschen gleichzeitig Globalisierung und Fragmentierung, Integration und Zerfall, wie das Beispiel EU versus Afrika zeigt.

Cyberraum und menschliche Gigantonomie

Globalisierung und Fragmentierung herrschen auch in einem anderen Bereich – meist im Stillen, Verborgenen, um aber nicht weniger brutal, sprich am Ende mit voller Wucht zuzuschlagen. Die Rede ist von Cybercrime. Das „Digitale Universum“ steigt von 1,8 ZB im Jahr 2011 auf 44 ZB im Jahr 2020 (Anmerkung der Redaktion: Zettabyte (ZB) 1021Byte = 1.000.000.000.000.000.000.000 Byte).

Und bis 2020 rechnen Analysten mit 50 Milliarden Geräten, die mit dem Internet verbunden sind. Gigantische Zahlen, die in einer „Gigantonomie“ münden. Diese Ergebnisse präsentierte Tom Köhler, Leiter des Geschäftsbereichs Infokom bei dem Analyse- und Testdienstleistungsunternehmen IABG Industrieanlagen-Betriebsgesellschaft mbH, das unter anderem den Gesamtzellen-Ermüdungsversuch am Airbus A380 durchgeführt hat. Ein Blick in die Praxis zeigt, woran es hapern kann.

Die sprunghafte Nutzung von Smartphones stellt ein weiteres Risikofeld dar. Von Köhler als das „dritte Auge“ bezeichnet, gibt es aktuell rund zwei Milliarden Smartphone-Nutzer – Tendenz steigend. Die digitalen Technologien inklusive einer zunehmenden Vernetzung bieten für alle Wirtschaftsbereiche große Potenziale und Chancen. Gleichzeitig dürfen die Risiken im Umgang mit mobilen Endgeräten nicht vergessen werden. Und die lauern in Form von diversen Einfallstoren für Angreifer. Rund 100 Milliarden Applikation befinden sich aktuell auf Apple-Endgeräten. Jüngst wurde bekannt, dass der Apple-Store von Hackern angegriffen wurde. Die Folgen solcher Angriffe auf Applikationsplattformen können immens sein. Gerade aufgrund der Tatsache, dass viele Anwender das Endgerät als digitalen Aktenkoffer nutzen, versehen mit allen sensiblen Unternehmensinformationen.

In vielen Punkten hinkt ein Risikomanagement 1.0 der digitalen und eng vernetzten Welt hinterher. Köhler stellte in diesem Kontext die Frage, ob die einfache zweidimensionale Risk-Map überhaupt noch ausreiche, um solche komplexen und hochgradig vernetzten Zukunftsszenarien abzubilden?

Frank Romeike (Geschäftsführer RiskNET und Chefredakteur RISIKO MANAGER) und Kurt Meyer (Chief Risk Officer, Swissgrid).

Michael Reisp im Dialog mit Dr. Dr. Manfred Stallinger.

Paneldiskussion zum Thema: Droht den Risikomanagern das Schicksal der Kassandra?

Hendrik F. Löffler, Funk Gruppe.

Vorausschau, Teamwork, der Mensch in der Kommunikation

Nein, wie auch Robert Ebel, Head of Corporate Risk & Insurance Management bei der Hoerbiger Holding AG, in seinem Vortrag feststellte. Seine Devise: „Risk Management ist operativ – oder nicht wirksam" und meint, dass der operative On-site-Ansatz Risiken reduziert und Mitarbeiter sowie Assets schützt. Vorausgegangen war eine Anpassung von Corporate Risk und Insurance Management an die sich stark veränderten Aufgabeninhalte der Organisation in den letzten Jahren. Hierzu gab es in den Jahren 2009 bis 2014 einen Optimierungs- und Weiterentwicklungsprozess des Risk Management. Hierzu gehörten der Rollout des EBIT@Risk sowie der Betriebsunterbrechungsanalyse, ein Umweltrisikomanagement, eine umfangreiche Maßnahmendokumentation sowie der Weiterentwicklung der Risikoquantifizierung, unter anderem Expected Shortfall und Stresstests. Im Bereich des Versicherungsmanagements wurden unter anderem alle Prozesse überarbeitet – beispielsweise die Interaktion zwischen Makler, Versicherer und Hoerbiger. Außerdem wurden neue Schadenverhütungskonzepte entwickelt und umgesetzt.

Strategische und operative Risiken werden innerhalb der Organisation in etablierten Analyse-Routinen bearbeitet. Risikomanagement ist bei Hoerbiger als Bestandteil des Planungsprozesses integriert. Robert Ebel: „Wenn Unternehmen nur mit historischen Informationen arbeiten, betreiben sie reine Risikobuchhaltung. Wichtig ist eine vorausschauende Sicht auf potenzielle Risiken, um die Chancen für die eigene Organisation zu wahren."

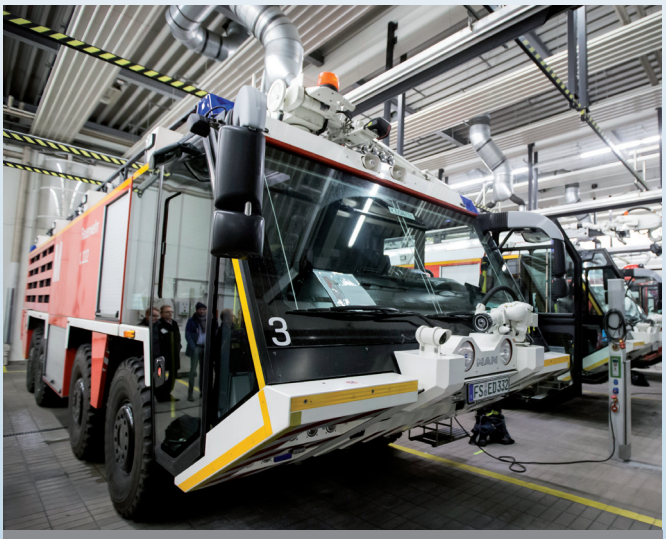
Risiken der Weltwirtschaft, Unsicherheiten bei den Menschen

Die Risikolandkarte ist groß, eng vernetzt und muss daher im globalen Maßstab und unter Beachtung des Wachstumsdilemmas aufgeschlagen werden. Ein Beispiel bieten die Turbulenzen an den weltweiten

Frank Romeike: „Wir müssen uns von einer Risikobuchhaltung verabschieden. Wir müssen aus der Zukunft lernen."

Prof. Dr. Bernd Weber, Center for Economics and Neuroscience, Universität Bonn.

„Bei Lawinen geht es – ähnlich wie in Unternehmen – um komplexe, mitunter schwer durchschaubare Abläufe, die zu Gefahrensituationen führen können", bestätigt Dr. Rudi Maier, seit 2009 Leiter des Lawinenwarndienstes Tirol.



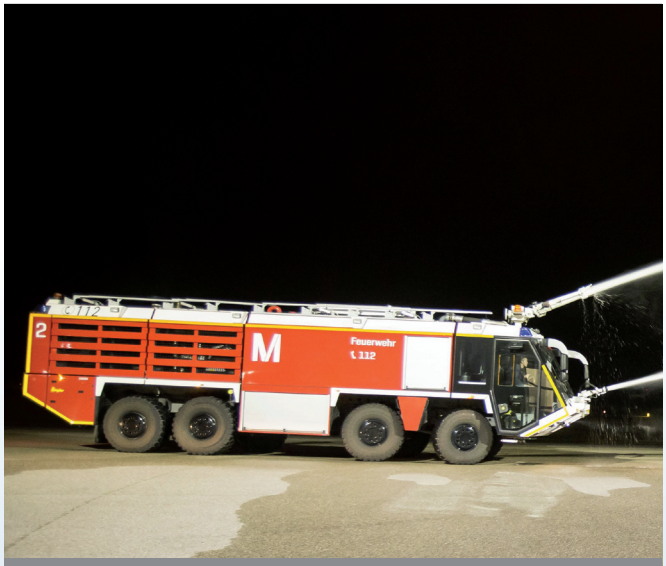
Am Abend waren die Teilnehmer des RiskNET Summit zu Gast bei der Flughafen-Feuerwehr München.

Finanzmärkten. Dr. Martin W. Hüfner, Chief Economist bei Assenagon Asset Management S.A. und zuvor Chefökonom der Hypovereinsbank, stellte klar, dass das Wachstum der Weltwirtschaft einen klaren Trend nach unten zeigt.

Hierzu tragen nach Einschätzung von Hüfner beispielsweise Fragen um die wirtschaftliche Entwicklung Chinas, die Zinserhöhung in den USA sowie schlechte Unternehmensnachrichten, unter anderem bei VW oder Glencore, bei. Zugleich sieht Hüfner Licht am Ende des Tunnels oder die Lage nicht so pessimistisch wie Teile der Medien, kritische Ökonomen oder Globalisierungsgegner. „Ich halte eine Rezession der Weltwirtschaft dennoch nicht für wahrscheinlich", so Hüfner. Ein positives Beispiel sieht Hüfner im Wachsen der Realwirtschaft in Europa. Der europäische Wirtschaftsraum sei nach der Eurokrise auf dem Weg der Erholung. Spanien wächst um drei Prozent. Dort habe nach Hüfners Worten die Reformpolitik gefruchtet, und das Land wird sich zum Wachstumstreiber entwickeln. Auch in Italien ist eine Besserung in Sicht. In Deutschland sei die Situation noch gut, aber es herrsche ein Stillstand bei Reformen. Ein Thema, das übrigens EU-weit zu beobachten ist. Die Unsicherheit über den weiteren Reformkurs in Europa trägt zu weiterer Unsicherheit bei den Menschen bei, so Hüfner in seinem Fazit.

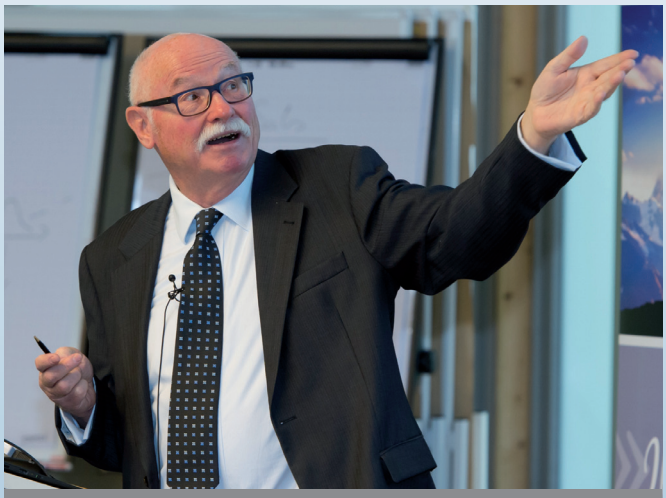
Compliance und menschliche Schwächen

Was passiert, wenn Menschen in der Organisation „quer laufen" erörterte Jan Hansen, Head of Compliance Strategy & Risk, Siemens AG, in seinem Vortrag zu „Compliance Risk Assessment @ Siemens". Siemens, 2006 selbst von einer immensen Compliance-Panne betroffen, stellte nach diesem Vorfall die Uhren neu. Das heißt, der Gesamtprozess des Compliance-Managements wurde fundamental umgebaut und verbessert. Hierzu heißt es im Siemens-Geschäftsbericht 2007: „Vor dem Hintergrund der Ende des Jahres 2006 bekannt geworde-



52 Tonnen Gesamtgewicht, bis 1.400 PS Motorleistung, 8x8 Allradfahrgestell, bis 19.000 Liter Löschmittel.

Hochkarätige Referenten und Teilnehmer.



Dr. Martin W. Hüfner analysierte die wesentlichen volkswirtschaftlichen Entwicklungen und Risiken.

Was passiert, wenn Menschen in der Organisation „quer laufen“ erörterte Jan Hansen, Head of Compliance Strategy & Risk, Siemens AG.

nen Korruptionsvorwürfe gegen Mitarbeiter des Unternehmens hat Siemens im Laufe der vergangenen zwölf Monate eine Reihe von wesentlichen Schritten unternommen, um seine Compliance-Verfahren und internen Kontrollen zu verbessern. Das Compliance-Programm wurde unter den Eckpunkten Vorbeugen, Erkennen und Reagieren neu strukturiert.“

Compliance-Manager Hansen: „Für Siemens war der Vorfall ein Auslöser, das Thema Compliance kulturell ganz anders anzugehen.“ Im Jahr 2006 war der Konzern zunächst damit beschäftigt, eine Analyse zu betreiben und die Fälle aufzuarbeiten. Ab dem Jahr 2009 startete das Unternehmen mit der Compliance-Risikoanalyse.

Hansen ging im Rahmen seines Vortrags auf zwei Kernprozesse innerhalb der Siemens-Organisation ein. Hierzu zählt der „Compliance Risk Assessment: Bottom-up Compliance risk process”. Ein relativ einfacher Prozess in Form eines Workshops. Ziel war es, dass der jeweilige CEO oder CFO Workshops mit den Compliance-Officern in der jeweiligen Einheit (Lead Country/Division) durchführt. Identifizierte Top-Risiken werden danach vor Ort in den Ländern besprochen, systematisiert, dokumentiert und zentral ausgewertet. Der Vorteil dieses Prozesses liegt für Hansen darin, dass man ein anders Bild über die speziellen Risiken vor Ort bekommt und kulturelle und nationale Aspekte besser berücksichtigt.

Zum zweiten Kernprozess zählt die „Compliance Risk Analysis: Top-down Compliance risk process”. Hierbei werden vier bis fünf Einheiten pro Jahr von zentraler Stelle ausgewählt. Es folgt eine detaillierte interne und externe Analyse des gesamten Umfelds. Die Informationen werden gesammelt und konsolidiert, um daraus Fragen für das Management abzuleiten. „Das Ziel ist der Dialog mit dem Management vor Ort“, erklärt Hansen den Prozess. Ebenso ausführlich wird der externe Markt nach möglichen Compliance-Schwachstellen abgeklopft und analysiert – inklusive des Marktumfelds und der Entwicklung, Wettbewerber sowie das juristische Umfeld. Im Grunde geht es nach Hansens Worten darum, mit dem

Thema von Kurt Meyer: Risikomanagement der Swissgrid AG: Chancen nutzen – Risiko-Awareness fördern.

Dr. Karsten Prause, Leiter Risikocontrolling, SWM – Stadtwerke München.

Prof. Dr. Werner Gleißner deckte Unsinnigkeiten im Risikomanagement auf – ohne ein Blatt vor den Mund zu nehmen.

Steffen Scholz (DB Schenker) und Prof. Dr. Michael Huth (Hochschule Fulda).

Kollegen offen zu diskutieren und die Frage zu stellen, wie sie mit der Beobachtung zu einem potenziellen Risiko umgehen.

Blackout von Systemen und Menschen im Gesamtprozess

Hacker und Saboteure – hinter denen immer auch Menschen mit unterschiedlichen Motiven stecken – haben es mittlerweile auf die kritischen Infrastruktureinrichtungen abgesehen, wozu auch die Energieversorgung zählt. Im Sommer 2014 attackierte eine Hacker-Gruppe mit dem Namen „Dragonfly“ Energieversorger mit der Schadsoftware „Havex“, um explizit industrielle Steuerungssysteme von Energieanlagen anzugreifen. Und ein Hacker-Team testete 2014 einen Angriff auf die Stromversorgung eines Versorgers mit dem Ergebnis, dass die Steuersoftware der Leitstelle beeinflusst wurde. Solch ein Szenario im reellen Leben mit Erfolg durchgeführt, und Kriminelle sowie Saboteure haben leichtes Spiel mit dem Kappen der Energieversorgung. Auch weil vielfach veraltete Systeme zum Einsatz kommen, die für Cyberangriffe anfällig sind. Die Folgen eines Stromausfalls vermittelte Kurt Meyer, Head of Risk Management, Chief Risk Officer, Swissgrid AG, am Beispiel eines Blackout. Die Kernfrage hierbei: Was würde passieren, wenn über mehrere Tage der Strom ausfällt? Es zeigt sich, die komplette Infrastruktur bricht ohne Stromversorgung zusammen – vom Verkehr über Kommunikationsnetze bis zum Ausbruch von Seuchen. Kritisch auch, weil die Notfallsysteme nur für 48 Stunden ausgelegt sind.

Innerhalb des Unternehmens Swissgrid arbeiten Meyer und seine Kollegen daran, die Mitarbeiter in der Organisation stärker zu sensibilisieren und ihnen klarzumachen: „Jeder sollte sein eigener Risikomanager sein“, so Meyer. Und er ergänzt: „Es zeigt sich leider immer wieder, dass Unternehmen in die Awareness-Falle tappen. Sprich, vielen Unternehmensvertretern ist nicht klar, welche Chancen die Sensibilisierung der eigenen Mitarbeiter im Umgang mit Risiken für die eigene Organisation bietet.“