Entwicklung einer Test-Umgebung für Risiko-Assessmenttools

Stefan Schauer[1] · Johannes Göllner[2] · Andreas Peer[2] · Stefan Rass[3]

[1]AIT Austrian Institute of Technology GmbH
stefan.schauer@ait.ac.at

[2]Bundesministerium für Landesverteidigung und Sport (BMLVS)
{johannes.goellner | andreas.peer}@bmlvs.gv.at

[3]Alpen-Adria Universität Klagenfurt
stefan.rass@aau.at

Zusammenfassung

Das sogenannte Doppelvektormodell umfasst Klassifikationsmethoden, um mögliche Strategien bei einem Angriff auf eine Kommunikationsinfrastruktur einzugrenzen. Im vorliegenden Beitrag beschreiben wir die Anwendung des Doppelvektormodells anhand eines Risiko-Assessments des Kommunikationsnetzwerks eines fiktiven Unternehmens namens „Pharma AG“. Diese wurde im Rahmen des Projekts RSB (Risikomanagement für simultane Bedrohungen) als virtuelle Organisation zu Evaluationszwecken und als Demonstrator für neue Verfahren des quantitativen Risikomanagements definiert. Es wurde hierbei ein global agierendes Unternehmen mit etwa 18.000 Mitarbeitern in Zweigstellen auf allen Kontinenten entworfen. Der vorliegende Beitrag beschreibt die Details dieses Testfalls für Risiko-Management und demonstriert hieran die Anwendung des Doppelvektormodells für die Identifikation von Angriffsstrategien. Darüber hinaus bestehen potentiell Anwendungen der fiktiven Unternehmensstruktur der Pharma AG auch über die Projektziele hinaus im Sinne der Entwicklung und Evaluierung neuer Risiko-Assessment Methoden.

1 Einleitung

Risiko-Management stellt ein zentrales Werkzeug für die Sicherheit innerhalb von Organisationen dar, das im Wesentlichen auf die Erfahrung und die Kenntnis von Best Practice Methoden aufbaut. Diese bestehen primär aus einer, durch systematische Methoden, Expertenwissen und Erfahrung gestützten, Einschätzung der Risiko-Situation basierend auf Modellen der Geschäftsprozesse und der Infrastruktur innerhalb der Organisation. Damit unterstützen diese Modelle die Identifikation von potentiellen Risiken und die Entwicklung von entsprechenden Schutzmaßnahmen. Ein quantitativer Ansatz für das Risiko-Management steht dabei meist nicht im Vordergrund, da der Aufwand für den Entwurf eines entsprechend hochwertigen Modells dessen Mehrwert übersteigen kann.

Die Entwicklung neuer allgemeiner Verfahren und Methoden zur qualitativen oder quantitativen Risikobewertung gestaltet sich, aufgrund potentiell fehlender Möglichkeiten das Verfahren in realen Infrastrukturen zu testen, oftmals schwierig. In Ermangelung von Infrastrukturen für

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 157-169.

experimentelle Evaluationen im Bereich Risiko-Management wurde daher innerhalb von RSB eine fiktive Organisation definiert (siehe [RaGP13]), in welcher neue Risiko-Managementverfahren evaluiert und bewertet werden können, um den Reifegrad einer Best-Practice oder Empfehlung untersuchen bzw. belegen zu können. Neben diesem primären Anwendungsfall für die nachfolgend vorgestellte Infrastruktur, welche *explizit nicht* auf Anwendungen innerhalb des RSB-Projektes beschränkt ist, setzen die meisten Risiko-Managementverfahren auch eine umfassende Identifikation von potentiellen Angriffsstrategien voraus. Speziell dieser Vorgang kann durch das sogenannte Doppelvektormodell [GMPP11], [GMP+14], [Göll09] unterstützt werden.

In diesem Artikel wollen wir die, im RSB-Projekt entwickelte, fiktive Organisation beschreiben und auf ihre Anwendung im Rahmen des Risiko-Managements eingehen. Dafür geben wir in Abschnitt 2 eine kurze Übersicht über das RSB-Projekt und die im RSB-Prototyp verwendeten Methoden. In Abschnitt 3 gehen wir genauer auf die Modellierung und den Aufbau der fiktiven Organisation sowie die Charakteristika des Doppelvektormodells ein. Schließlich beschreibt Abschnitt 4 in Grundzügen den Einsatz der beschriebenen Modelle und Methoden in einem Risiko-Assessment.

2 Der RSB-Prototyp

Im Projekt „RSB – Risiko-Management für simultane Bedrohungen“ wird ein solches quantitatives Risiko-Management im Bereich der IT-Security von Unternehmen verfolgt. Dies wird durch eine vereinfachte Modellierung der IKT-Infrastruktur mit Hilfe von Elementen der Graphentheorie sowie durch die Verwendung von Algorithmen und Modellen aus der Spieltheorie erreicht (wie auch schon in [ScRR12] und [ScRS12] beschrieben). Die Kommunikationsinfrastruktur einer fiktiven Testumgebung („Pharma AG“) wird hierbei zum Gegenstand und Anwendungsfall einer quantitativen Risiko-Analyse [RaGP13]. Das Projekt wird durch das KIRAS-Programm der österreichischen Forschungsförderungsgesellschaft (FFG) gefördert (Projekt-N. 836287). Beteiligt sind das Austrian Institute of Technology (als Projekt-Koordinator), die Alpen-Adria-Universität Klagenfurt, die Firma Bechtle IT Systemhaus, sowie das Bundesministerium für Inneres (BM.I) und das Bundesministerium für Landesverteidigung und Sport (BMLVS, Abteilung für Zentraldokumentation und Information / Landesverteidigungsakademie Wien). Als Betreiber hochsensibler Netzwerke fungieren die beiden Ministerien in diesem Projekt zusätzlich als Bedarfsträger.

Zu den Hauptzielen des Projekts zählt der Aufbau einer sicheren Kommunikation innerhalb der IKT-Infrastrukturen eines Unternehmens, wobei simultan das Risiko für Ausfälle, Abhören und Authentizität optimiert werden soll [RSPG13]. Hierfür wird eine Methodik entwickelt, welche eine – im Sinne multikriterieller Optimierung beste – Risiko-Abschätzung für jedes der drei spezifizierten Sicherheitsziele liefert. Zusätzlich werden die potentiell vorhandenen Wechselwirkungen bei der Optimierung der separaten Risiko-Abschätzungen implizit berücksichtigt (erfordern somit keine explizite Modellierung oder Kenntnis eventuell komplizierter Abhängigkeiten). Vergleichbar mit einem Virtual Private Network (VPN) ist der Zweck des RSB-Systems der Aufbau hochsicherer Kommunikationskanäle, welche sowohl verfügbar, als auch vertraulich und authentisch sind. Im Vergleich zu anderen Systemen aus dem VPN-Bereich ist hierbei *keine* Public-Key Kryptographie notwendig, sondern es wird auf codierungstheoretische Ansätze und Verfahren zurückgegriffen. Somit entfällt weitgehend das sonst übliche Zertifikats- und Schlüsselmanagement für diese Art der Kommunikation, welche durch den Einsatz von Public-Key Kryptographie impliziert wäre.

In diesem Zusammenhang wird das Risiko für eine Kommunikation als die Wahrscheinlichkeit für eine Verletzung der drei Sicherheitsziele (Informationsverlust, Ausfall des Kanals oder Einschleusen von Nachrichten) gemessen. Dadurch fällt diese Methode zur Risiko-Bewertung in den Bereich des quantitativen Risiko-Managements. Wir gehen nachfolgend kurz auf die eingesetzten Techniken ein.

2.1 Mehr-Wege-Kommunikation

Wie bereits in [ScRR12] beschrieben, wird im RSB-Prototyp (wie auch schon im Vorgänger-Projekt SERIMA [ScRS12]) für die sichere Übertragung der Informationen zwischen Sender und Empfänger die Mehr-Wege-Kommunikation (MWK) eingesetzt (das bekannte *One-Time Pad* (OTP) Verschlüsselungs-Verfahren stellt einen Spezialfall hiervon dar).

Die MWK bedient sich bei der Übertragung von Informationen mehrerer, disjunkter Wege in einem Kommunikationsnetzwerk. Die zu übermittelnde Nachricht wird in einzelne Teile aufgespaltet und auf diesen Wegen vom Sender zum Empfänger übertragen. Dabei gilt die Annahme, dass ein Angreifer höchstens $(n-1)$ Knoten (bzw. $(n-1)$ Wege) im Netzwerk kontrollieren bzw. abhören kann. Um die Sicherheit der MWK zu gewährleisten, wird die Nachricht mit einem One-Time Pad k verschlüsselt (bitweise XOR-Verknüpfung der Nachricht mit k), und k wiederum in $(n-1)$ Teilschlüssel „zerlegt“, deren bitweises XOR den Schlüssel k reproduziert. Daraufhin wird die Nachricht zusammen mit den $(n-1)$ Teil-Schlüsseln über n disjunkten Wegen übertragen. Um eine Nachricht abzuhören, müsste ein Angreifer nun sowohl das Chiffrat als auch alle Teil-Schlüssel der Übertragung besitzen. Nachdem der Angreifer aber maximal $(n-1)$ Teile abhören kann, ist es ihm nicht möglich, die Nachricht aus den abgehörten Informationen zu rekonstruieren. Dies ist erst beim Empfänger möglich, da er alle n Teile der Nachricht erhält.

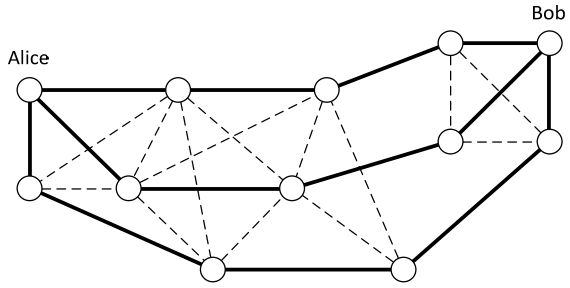

Abb. 1: Mehrwegeübertragung auf 3 Pfaden

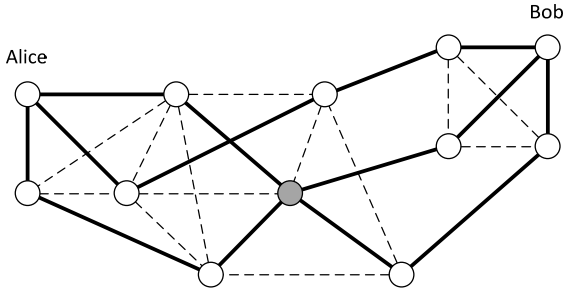

Abb. 2: Problem bei kreuzenden Pfaden

Ein Vorteil dieser Kombination aus MWK und OTP besteht darin, dass *kein* Schlüsselaustausch wie etwa durch Public-Key Infrastrukturen erfolgen muss, da sowohl das Chiffrat als auch der Schlüssel vom Sender erzeugt und übertragen werden. Wie oben beschrieben garantiert dabei die MWK, dass durch die Übertragung des Schlüssels die Sicherheit des Chiffrats nicht kompromittiert wird. Sollte nämlich ein Angreifer alle $(n-1)$ Teil-Schlüssel abfangen und den ursprünglichen Schlüssel rekonstruieren, so kann er dennoch nichts mit dieser Information anfangen, da bei der nächsten Übertragung ein neuer Schlüssel verwendet wird (*one-time* pad). Somit entfallen sonst übliche Mechanismen zur Verteilung und dem Management von Schlüsseln.

Diese Kombination der One-Time-Pad Verschlüsselung mit der Mehr-Wege-Kommunikation stellt im Wesentlichen das einzige, klassische Verfahren zur informationstheoretisch sicheren Übertragung von Informationen dar, wie in [WaDe08] untersucht und gezeigt wurde.

2.2 Risiko-Assessment und Spieltheorie

Es bleibt anzumerken, dass in den meisten heute verwendeten Netzwerk-Strukturen von Unternehmen es oft nicht möglich ist, die, für die MWK benötigten, *n* disjunkten Pfade von einem Sender zu einem Empfänger zu realisieren. Vielmehr gibt es bestimme Punkte in einem Netzwerk (Switches, Router, etc.) über die eine Vielzahl von Kommunikationspfaden führen und somit einen potentiellen Angriffspunkt bei einer MWK bilden. Ein Angreifer hätte somit die Möglichkeit, Informationen über die übertragene Nachricht zu erhalten, auch wenn er lediglich $(n-1)$ oder auch weniger Pfade abhören kann. Daher besteht die Grundüberlegung der im RSB-Prototyp angewendeten spieltheoretischen Methode darin, die Kommunikationspfade *zufällig* zu wählen. Dies geschieht in einer Weise, dass dem Angreifer eine möglichst geringe Chance bleibt, aus den abgehörten Daten Informationen über die ursprüngliche Nachricht abzuleiten (*Risiko-Streuung*).

Im RSB-Prototyp (sowie auch im Vorgänger-Projekt SERIMA) wird die Netzwerk-Struktur als ungerichteter Graph dargestellt, wobei jede (aktive) Komponente im Netzwerk als Knoten und jeder physikalische Kanal als Kante modelliert wird. Zudem gibt es zwei ausgezeichnete Knoten, Alice und Bob, die als Sender bzw. als Empfänger auftreten. Wie im vorherigen Abschnitt beschrieben wird eine Nachricht m vom Sender Alice in mehrere Teile $m_1, m_2, \dots, m_n$ zerlegt und über die n Pfade $p_1, p_2, \dots, p_n$ im Netzwerk an den Empfänger Bob gesendet. Dieser erhält nun die n Teil-Nachrichten und kann daraus (und nur daraus) wieder die ursprüngliche Nachricht m rekonstruieren.

Die Strategie des Angreifers ist es nun, eine maximale Anzahl von Knoten unter seine Kontrolle zu bringen, um die darüber übermittelten Teil-Nachrichten m_i abzuhören. Eine entsprechende Strategie des Senders ist es, die Übertragung der Teil-Nachrichten so durchzuführen, dass die Chance des Angreifers, diese Nachrichten abzuhören, so gering wie möglich ist. Diese beiden Strategien lassen die Übertragung als „Nullsummenspiel“ modellieren. Ein Nullsummenspiel ist dadurch charakterisiert, dass der Gewinn der einen Partei gleichzeitig den Verlust der anderen Partei darstellt. Im angegebenen Fall ist somit das Abhören einer Nachricht gleichgesetzt mit dem Verlust vertraulicher Information. Formal kann man den Gewinn (aus Sicht des Senders) folgendermaßen festlegen:

$$u(x,y) = \begin{cases} 1, & \text{falls die Übertragung erfolgreich und geheim ablief} \\ 0, & \text{sonst.} \end{cases} \quad (1)$$

Hierbei stellen x und y die jeweiligen Strategien des Senders und des Empfängers dar. Diese lassen sich mathematisch als Wahrscheinlichkeitsverteilungen über den zugehörigen Aktionenräumen PS_1 und PS_2 des Senders und des Angreifers beschreiben, wobei die Menge PS_1 die Menge aller Parameter des Senders (z.B. die gewählten Pfade zur Übertragung der Nachricht) und die Menge PS_2 die Menge aller Parameter des Angreifers (z.B. die durch den Angreifer kontrollierten Knoten) darstellt. Für die Erfolgswahrscheinlichkeit

$$v := u(x^*, y^*) \geq u(x^*, y) \text{ für } \textit{beliebiges } y. \quad (2)$$

Im Detail bedeutet dies, dass der Gewinn für den Sender stets größer oder gleich dem Gewinn ist, welcher sich ergibt, wenn der Angreifer sich anders verhält als durch das Nullsummenspiel prognostiziert. Obgleich eine Nullsummenspielannahme dem Angreifer ein sehr bestimmtes (und in Folge dessen wahrscheinlich nicht reales) Verhalten unterstellt, kann gezeigt werden [Rass09], dass die oben angeführte Ungleichung (2) eine *scharfe* Schranke darstellt, welche auch bei anderem Verhalten des Angreifers erreicht werden kann.

Der Wert $\rho := 1 - v$ stellt somit eine quantitative Risiko-Schätzung für die Wahrscheinlichkeit eines Angriffes auf die Übertragung einer Nachricht im gegebenen Kommunikationsnetzwerk dar (vgl. [AcRa05] für einen verwandten Ansatz). Der RSB-Prototyp ermittelt nicht nur diesen Wert ρ, sondern auch die dadurch notwendige Auswahl der Kommunikationspfaden im Netzwerk. Die Gewährleistung, dass die Kommunikation auch über diese Wege durchgeführt wird, wird in weiterer Folge von eigens hierfür entwickelten Protokollen und Network-Provisioning-Komponenten übernommen.

2.3 Multikriterielle Spiele

Die in Abschnitt 2.2 beschriebene Methode ist auf die Risiko-Abschätzung (Abschätzung der Wahrscheinlichkeit eines erfolgreichen Angriffs) für eine sichere Übertragung mittels MWK ausgelegt. Neben Abhörsicherheit berücksichtigt das RSB-System auch *Authentizität* und *Ausfallsicherheit* eines Übertragungskanals. Für diese beiden Sicherheitsziele wurden im RSB-Projekt ebenfalls geeignete Übertragungsverfahren (analog zu MWK) eingesetzt.

Die Authentizität einer Nachricht wird dabei durch eine „Mehr-Wege"-Version einer einfachen MAC-Authentifizierungsmethode (message authentication codes) realisiert. Die Methode stützt sich dabei auf einen „Web-of-Trust"-Ansatz, wie er etwa in PGP verwendet wird (vgl. [Zimm92]), bei dem Vertrauensbildung durch „Leumunde" erreicht wird. Die Idee basiert dabei auf der Verifikation einer handschriftlichen Unterschrift: wird eine Unterschrift auf einem Dokument von hinreichend vielen, unabhängigen Personen verifiziert, wird ihre Authentizität anerkannt. Die Umsetzung im RSB-Prototyp verwendet dazu einen geheimen Authentifizierungs-Schlüssel, die ein Sender sich mit seinen *direkt* (physikalisch oder logisch) *verbundenen* Nachbarn teilt und mit dem ein MAC über einer Nachricht verifiziert werden kann. Genauere Details sind in [RaSc10] nachzulesen. Die Modellierung und Sicherheits-Analyse im spieltheoretischen Sinne erfolgt analog wie für MWK.

In gleichem Sinne wie Mehr-Wege-Kommunikation und Mehr-Wege-Authentifizierung kann auch Ausfallsicherheit als Spiel modelliert werden, wobei der Spielausgang in diesem Fall anhand der erfolgreichen oder erfolglosen Zustellung der Nachricht gemessen wird. Auch hier verläuft die Analyse analog zu MWK oder der oben skizzierten Authentifizierung.

Die Erweiterung der in Abschnitt 2.2 angeführten Berechnung zur Risiko-Abschätzung kann jedoch nicht direkt auf mehrere Sicherheitsziele durchgeführt werden. Dies beruht insbesondere auf der Eigenschaft der $\leq$-Relation in Gleichung (2), welche bei der Anwendung auf mehrere Dimensionen (also gleichzeitiger Betrachtung mehrerer Sicherheitsziele) nicht mehr transitiv ist. Deshalb wurde für das RSB-Projekt ein axiomatischer Ansatz gewählt (vgl. auch [Rass13], [RSPG13], sowie Vorgängerarbeiten in [Ghos91], [Voor99] oder [AcRa05]), in dem Risiko-Zusicherungen bei mehreren potentiell wechselseitig abhängigen Sicherheitszielen folgendermaßen charakterisiert werden: Gegeben seien k Sicherheitsziele, welche durch die Gewinn-Funktionen $u_1, \ldots, u_k$ (wie in (1) im vorigen Abschnitt definiert) modelliert werden. Diese mes-

sen den jeweiligen Erfolg oder Misserfolg einer Übertragung in Abhängigkeit eines Sicherheitsziels Eine sog. *effiziente Risiko-Zusicherung* $(v_1, v_2, \dots, v_k)$ im Sinne von k gegebenen Zielen, gemessen durch $u_1, u_2, \dots, u_k$ bei jeweiligen Verhaltensprofilen $(x, y) \in PS_1 \times PS_2$ ist dann charakterisiert durch folgende Eigenschaften:

1. **Zusicherung**: Es existiert ein Verhaltensprofil x^* (eine Wahrscheinlichkeitsverteilung über PS_1), mit der Eigenschaft, dass $v_i \geq u_i(x^*, y)$ für *beliebiges* y (analog möge somit Ungleichung (2) für jedes Sicherheitsziel einzeln gelten), wobei für jedes Sicherheitsziel ein Angriffsprofil y_i existiert, bei welchem genau der Gewinn v_i erreicht wird (die Schranke soll *scharf* sein).
2. **Effizienz**: Es gibt kein Verhaltensprofil $x' \neq x^*$ für das in allen Belangen echt bessere Zusicherungen $v_1' > v_1, v_2' > v_2, \dots, v_n' > v_n$ existieren (d.h. die Zusicherung ist nicht gleichmäßig verbesserbar).

Ein Vorteil dieser Definition vor Risiko-Zusicherung ist, dass kein explizites Modell für die wechselseitigen Abhängigkeiten zwischen den Sicherheitszielen notwendig ist. Vielmehr werden diese Abhängigkeiten durch die Funktionen $u_1, u_2, \dots, u_k$ berücksichtigt. Zusätzlich wurde im RSB-Prototyp die Möglichkeit geschaffen, einzelnen Sicherheitszielen unterschiedliche Gewichtungen zuzuweisen, um eine individuelle Anpassung der Bedeutung zu ermöglichen. Zusammen mit dem generischen Unternehmensmodell (wie im nächsten Abschnitt genauer beschrieben) bietet das RSB-Projekt einen Ansatz zum Risiko-Assessment, der auf vielfältige Anforderungen zugeschnitten werden kann.

3 Modellierung

Für die Risikoanalyse von Kommunikationsbeziehungen – insbesondere bei quantitativen Ansätzen wie im RSB-Projekt – ist es zweckdienlich, die IKT-Netzwerkstruktur des betrachteten Unternehmens als (ungerichteten) Graph darzustellen, in welchem zwei ausgezeichnete Knoten einen Kommunikationskanal aufbauen (möchten). Hierbei entsprechen die Switches, Router, Server etc. im Netzwerk den Knoten und die Verbindungen den Kanten im Graphen. Um die Verwundbarkeit bzw. Angreifbarkeit eines Knotens zu beschreiben, kann dieser durch eine Reihe von Charakteristika genauer spezifiziert werden. Dazu zählen in etwa die physikalischen Gegebenheiten des Raumes bzw. generell des Standorts der Hardware, deren Hersteller sowie die installierte Firmware-Version, aber auch Informationen aus dem Bereich Human Resources, z.B. über den Administrator der Hardware. Durch die Abbildung der IKT-Netzwerke und der internen Prozesse eines Unternehmens (wie am Beispiel der „Pharma AG“ im folgenden Abschnitt) lassen sich diese Charakteristika an die unternehmensspezifischen Details anpassen und erlauben somit eine realitätsnahe Darstellung einer Organisationsstruktur für Testzwecke.

In weiterer Folge können anhand der Charakteristika eines Knotens unterschiedliche Angriffsstrategien definiert werden. Um dies konsistent umsetzen zu können, bedarf es einer entsprechenden Kategorisierung, welche zum Beispiel durch das Doppelvektormodell erreicht werden kann (für Details siehe Abschnitt 3.2).

3.1 Virtuelles Unternehmen „Pharma AG“

Zu Demonstrationszwecken und als Anwendungs- und Testfall für die im Rahmen des RSB Projektes entwickelten Methode und Prototyp-Software wurde ein virtuelles, internationales Unternehmen geschaffen [RaGP13]. Dies sollte dabei helfen, die Anforderungen der Bedarfsträger (BMLVS und BM.I) aus dem Projekt schematisch darzustellen, ohne sensible

Informationen über die Netzwerke der beiden Ministerien zu verwenden. Es sei hier darauf hingewiesen, dass mögliche Anwendungen dieses Modells keineswegs auf RSB beschränkt sind, da das Modell allgemein gehalten wurde. Die „Pharma AG“ kann somit auch für das Studium und die Illustration anderer Risiko-Managementmethoden herangezogen werden.

Das betrachtete Unternehmen ist ein weltweit agierender Pharma-Konzern mit drei wesentlichen Produktlinien im Medikamentenbereich (bestimmt durch die Verabreichungsform):

- Tabletten
- Kapseln
- Flüssigkeiten

Insgesamt sind mehr als 18.000 Mitarbeiter in 18 Zweigstellen auf 5 Kontinenten beschäftigt. Dabei wurden sämtliche Strukturen inklusive Mitarbeiter und der entsprechenden IT-Ausstattung modelliert. Der nachfolgenden Abbildung ist die Struktur der Konzernleitung bzw. des Hauptquartiers zu entnehmen.

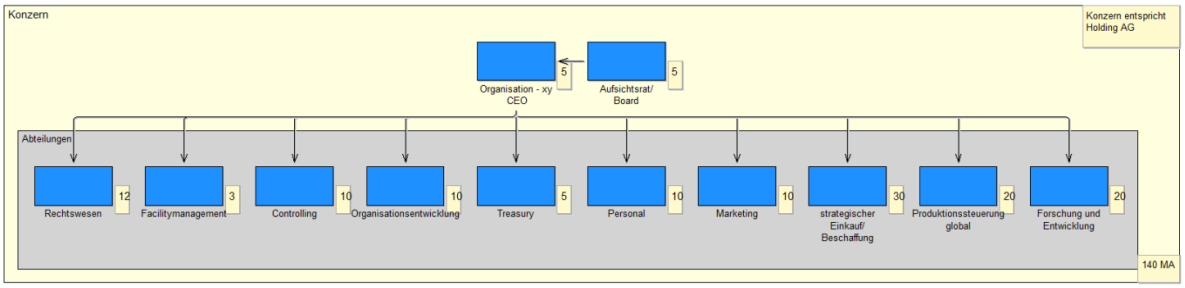

Abb. 3: Struktur des HQ [RaGP13]

Für die weitere Analyse wurden neben den konzerninternen Abhängigkeiten die entsprechenden Anbindungen an das Supply Chain Network (wie etwa Energieversorgung, Informations- und Kommunikationstechnologie) der verschiedenen strukturierten Elemente dargestellt. Dadurch ist es in weiterer Folge möglich, Risiko-Betrachtungen durchzuführen.

Im Detail sind für die Risiko-Betrachtung in RSB (aber auch bei alternativen Ansätzen) die Informations- und Kommunikationssysteme von Bedeutung. Hierbei wurde sowohl ein Intranet (firmeninterne Netzwerke), ein Extranet (firmeneigene, gemietete oder selbst betriebene Netzwerke für die Verbindung der Niederlassungen) als auch das Internet (in Form von Providern zugekaufter Kommunikationsdienstleistungen) modelliert.

Die verwendete IT-Infrastruktur ist dabei an Referenz-Architekturen bzw. an Empfehlungen namhafter Hersteller (etwa Cisco) angelehnt, um ein möglichst realitätsnahes Modell zu erhalten (siehe Abbildung 4). Im Detail wird zum Zwecke der Ausfallssicherheit eine durchgängig 2-fach redundante Anbindung aller Arbeitsplätze an das Netzwerk angenommen. Im Kern befinden sich zwei Core-Switches (CS), welche sich via Virtual Switching System logisch von außen wie ein einziger Switch verhalten. Jeder Verteilerswitch (VS) ist durch physikalisch getrennte Glasfaserleitungen an jeden der beiden Core-Switche angebunden. Außenstellen werden durch intern betriebene oder extern zugekaufte (gemietete) Glasfaserkabel in einer Ring-Topologie entweder direkt an den beiden Core-Switches oder an zwei Verteiler-Switches angebunden. Der Zugang ins Internet führt über zwei Border-Gateways, welche auch als Firewall agieren.

Dieses Modell ist dabei für jede Niederlassung umgesetzt und entsprechend ihrer Größe und Anzahl der Mitarbeiter angepasst. Als Basis wird eine Versorgung von 1.500 Mitarbeitern angenommen, was somit eine Netzwerkgröße von etwa 60 Switches ergibt (WLAN-Verbindungen wurden hierbei nicht berücksichtigt). Somit ermöglicht das Modell der „Pharma AG“ einen ausführlichen Test von Risiko-Bewertungsmethoden, insbesondere der RSB-Methode.

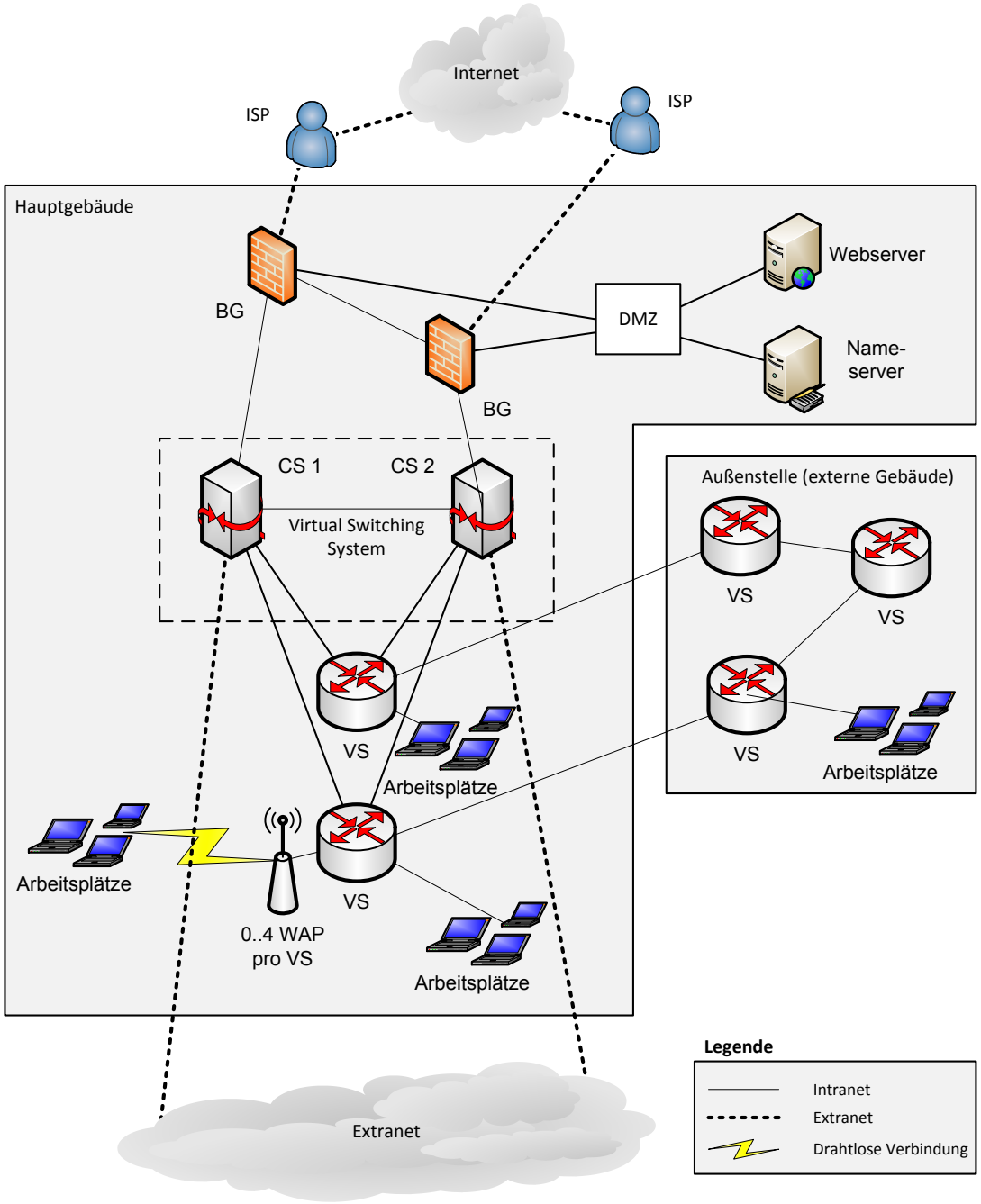

Abb. 4: Netzwerk-Struktur eines Standorts [RaGP13]

3.2 Doppelvektormodell

Die Komplexität von Systemen und die Etablierung einer gemeinsamen Terminologie machen Kategorisierungsmodelle erforderlich, um Systemkomponenten und -elemente klassifizieren zu können. Dieser Ansatz garantiert einen normierten und analytischen Prozess, um Ergebnisse und verschiedene Elemente und Komponenten miteinander vergleichen zu können. Dazu wurde das sogenannte Doppelvektorenmodell auf Basis einer ersten Kategorisierungsebene (Metakategorisierungsebene) im Rahmen des BMLVS-internen Forschungsprojektes „Szenarioplanung und Wissensmanagement im ÖBH“ im Zeitraum 2010 – 2013 durch Johannes Göllner, Klaus Mak, Christian Meurers, Andreas Peer und Günther Povoden entwickelt [Göll09], [GMPP11], [GMP+14].

Das Doppelvektorenmodell stellt ein dreidimensionales, mehrstufiges Meta-Klassifikationssystem dar, in dem jedes Element über die vektorale Zuordnung von definierten Eigenschaften und Attributen dargestellt und beschrieben werden kann. Die erste Ebene unterscheidet die Ordinaten nach zeitlichen und räumlichen Aspekten und bietet zusätzlich einen organisations- bzw. ebenenspezifischen Abstraktionslevel an (politisch, strategisch, (militär-) strategisch, operativ, taktisch, (gefechts-) technisch).

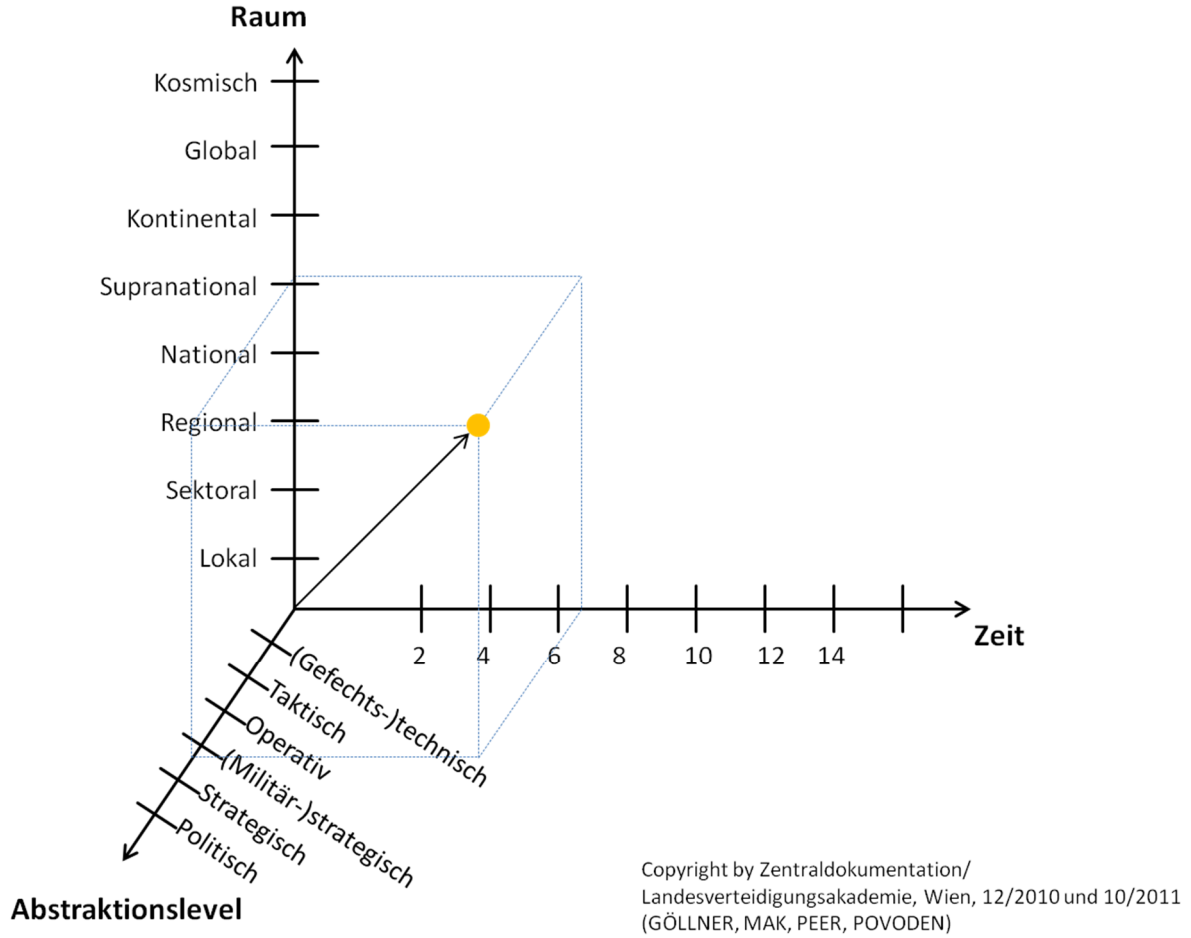

Abb. 5: Doppelvektormodell – Vektor 1

In der zweiten Ebene basiert die Kategorisierung auf der Unterscheidung eines Ereignisses hinsichtlich des Verursachers und der Einwirkung organisationsimmanenter Gefahren. Zusätzlich wird das Ereignis im Rahmen der Ereignisprinzip-Achse auch unter Berücksichtigung des Ursprunges (terrestrisch, extraterrestrisch) weiter kategorisiert.

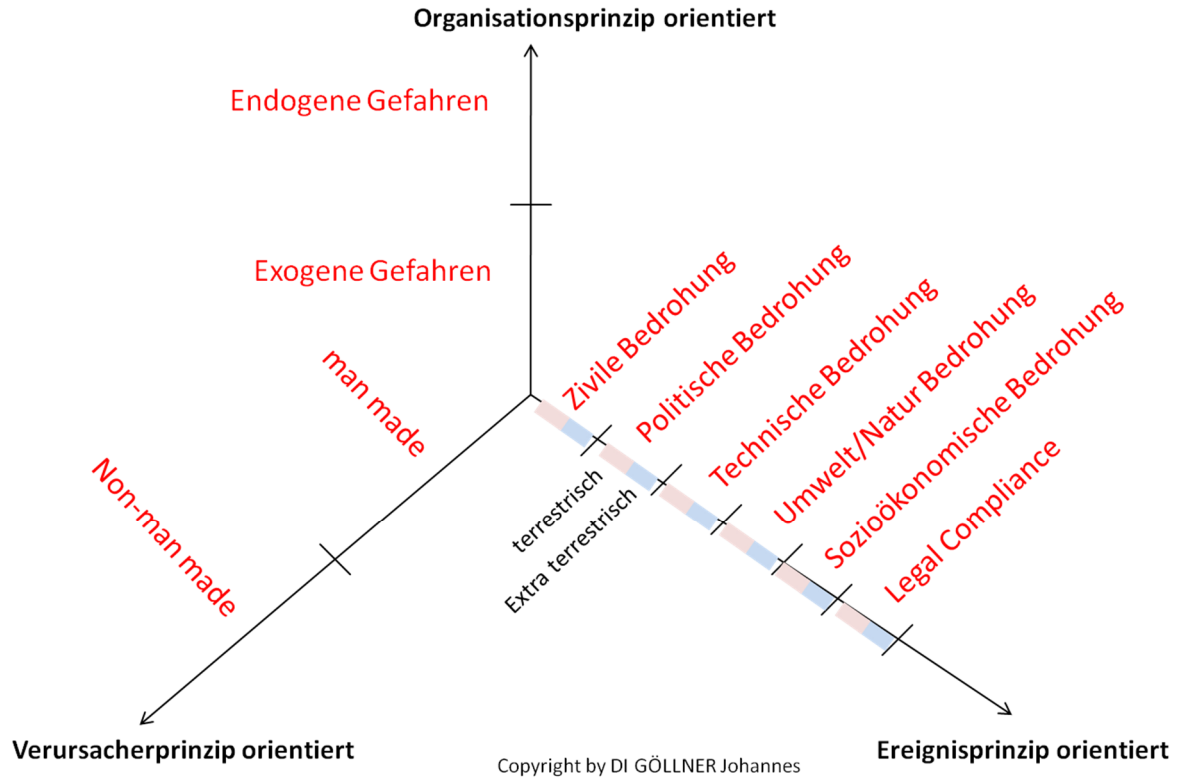

Abb. 6: Doppelvektormodell – Vektor 2

Durch das Doppelvektormodell lässt sich prinzipiell jedes Ereignis entsprechend kategorisieren und dokumentieren. In Verbindung mit diversen Akteuren und Wissensrollen lassen sich daraus entsprechend Zusammenhänge und Wechselwirkungen erkennen und ableiten. Ein zusätzlicher Mehrwert ergeht auch aus der Möglichkeit, Muster von Ereignissen in den diversen Kategorien zu identifizieren. Dies dient nicht nur Analysten, sondern kann auch für die Beurteilung von zusätzlich erforderlichem Informationsbedarf zweckmäßig sein.

Auf diese Weise lassen sich unter Anwendung des Doppelvektorenmodelles und der Pharma AG einerseits rasch die wesentlichen (ebenen- bzw. themenspezifischen) Netzwerkknoten identifizieren und zusätzlich die entsprechenden generellen und spezifischen Attribuierungen festlegen. Für eine Anwendung auf ein „reales“ Unternehmen gilt es, entsprechendes, unternehmensinternes Know How in die Bewertung mit einzubeziehen. Dadurch lassen sich relativ einfach und rasch die spezifischen Parameter, Einflussfaktoren und Attribuierungen eines realen Unternehmens identifizieren.

4 Durchführung eines Risiko-Assessments

Die modellierte Pharma AG dient im Rahmen des Projektes RSB als Grundlage zur Entwicklung des Prototyps. Sie kann aber auch als Test-Umgebung für ein Risiko-Assessment im Allgemeinen herangezogen werden. Das Modell der Pharma AG bietet die Möglichkeit, auf Basis

einer zwar fiktiven, jedoch realitätsnahen Organisationsstruktur die Einflussfaktoren für die Sicherheit der IKT-Infrastruktur in einem Unternehmen zu analysieren. Entsprechend können im RSB-Prototyp die Knoten des analysierten Netzwerks mit zusätzlichen Informationen annotiert werden, um eine realitätsnahe Beschreibung des Netzwerks zu ermöglichen [RSPG13]. Im Rahmen der derzeitigen Aktivitäten im RSB-Projekt wurden u.a. folgende Einflussfaktoren für diese Knoten des Netzwerks betrachtet:

- Technisch: BIOS-Version, Firmware-Version, Betriebssystem (Version, Servicepack, etc.), Applikations-Software, etc.
- Personal: Administratives Personal, User, Rollen-Modell, etc.
- Lokation: Standort, physikalischer Zugangsschutz (Zutrittskontrollen, Überwachung, etc.), (rollen-basierte) Zugriffskontrollen, etc.

Diese Einflussfaktoren stellen eine Basis für die Sicherheitsanalysen durch den RSB-Prototyp dar. So kann etwa durch diese Faktoren die Angreifbarkeit von bestimmten Knoten bei einer speziellen Angriffsstrategie genauer spezifiziert werden. Nachdem die Pharma AG ein generisches Unternehmen darstellt und der RSB-Prototyp ein weitgehend offenes System ist, können diese Faktoren je nach Bedarf erweitert und angepasst werden, um die konkreten Anforderungen eines realen Unternehmens adäquat widerspiegeln zu können. Dafür ist eine systemische Erfassung der diversen Knoten des Netzwerks im Rahmen eines Risiko-Assessments erforderlich, um die, für ein Unternehmen relevanten Faktoren identifizieren zu können. Die dadurch identifizierten Faktoren können dann zu den bereits bestehenden hinzugefügt und in die Risiko-Abschätzung des RSB-Prototyps mit einbezogen werden. Auf diese Weise kann in weiterer Folge ein umfassender Katalog an potentiellen Einflussfaktoren erstellt werden. Aufgrund der Verwendung verwandter Systeme und Strukturen innerhalb einer Branche (oder auch branchenübergreifend) ist ein solcher Katalog nicht nur für ein spezielles Unternehmen nützlich, sondern kann auch bei anderen Unternehmen Anwendung finden.

Auf Basis des Doppelvektormodells erfolgt die Erstellung eines Bewertungsmodells, um die identifizierten Einflussfaktoren entsprechend gewichten und bewerten zu können. Dabei wird das Bewertungsmodell so konzipiert, dass es branchen- und unternehmensunabhängig eingesetzt werden kann, was einen wesentlichen Vorteil der Methode gegenüber alternativen Ansätzen darstellt. Der Einsatz des Doppelvektormodells als Kategorisierungsmethode unterstützt dieses Bestreben, da das Modell von seinem Ursprung her bereits auf einem generischen Ansatz basiert und damit kein Anwendungsgebiet a priori ausschließt.

Im Rahmen eines Risiko-Assessments werden nun alle Einträge des Faktorenkatalogs entsprechend den Vorgaben des Bewertungsmodells bewertet und damit die relevanten Faktoren und deren entsprechende Attribute herausgefiltert. In Abhängigkeit der konkreten Anforderungen eines Unternehmens (Zielsetzung, Schwerpunkte, etc.) erfolgt die spezifische Gewichtung der einzelnen Achsen des Doppelvektormodells in Abhängigkeit des gesamten vorliegenden Systems. Daraus resultieren in weiterer Folge sowohl die Bewertungen der einzelnen Knoten, als auch die wesentlichen Faktoren und Attribute für die Analyse, welche dann mit dem RSB-System durchgeführt werden kann.

Gerade diese spezifische Identifizierung von relevanten Einflussfaktoren und Attributen stellt einen markanten Mehrwert der Kombination des Modells der Pharma AG und des Doppelvektormodells dar, da für unterschiedliche Unternehmen die jeweiligen relevanten Aspekte berücksichtigt und als Grundlage für weitere Analyse herangezogen werden können. Durch die Ver-

flechtung des RSB-Prototyps mit dem Modell der Pharma AG kann dieser für eine solche Analyse verwendet werden, wobei sichergestellt ist, dass der Prototyp unabhängig der Unternehmensgröße, des Unternehmensziele oder der Branche zielgerichtet eingesetzt werden kann.

5 Zusammenfassung und Ausblick

Das Organisationsmodell des fiktiven Unternehmens „Pharma AG“, welches aus dem RSB-Projekt entstanden ist, kann nicht nur als einzelner Anwendungsfall in dem Projekt gesehen werden, sondern auch als eine generische Test-Umgebung für Risiko-Assessments im Allgemeinen. Durch die detaillierte Abbildung der wichtigsten Aspekte eines global agierenden Unternehmens wird die Basis für ein entsprechend detailliertes Risiko-Assessment geschaffen. Dabei stellt der Bezug zur Pharmaindustrie, der bei der Erstellung des Modells gewählt wurde, keinerlei Einschränkung dar: die Organisationsstruktur kann (eventuell mit kleinen Anpassungen) auf andere Branchen übertragen werden. Gleichsam ist aber durch die Verwendung des generischen Modells der Pharma AG die Methodik bzw. der Prototyp, welcher aus dem RSB-Projekt resultiert, so ausgelegt, dass ein branchenübergreifender Einsatz der in RSB entwickelten Methode selbst ebenso möglich ist.

Aus dem Modell der Pharma AG entsteht die Möglichkeit, einen Faktorenkatalog abzuleiten, in dem sich die konkreten Rahmenbedingungen und Anforderungen eines realen Unternehmens wiederfinden. Ein derart erstellter Faktorenkatalog lässt sich durch die gewonnen Informationen aus einem Risiko-Assessment kontinuierlich erweitern und stellt somit die Basis für weitere Analysen dar. Dafür müssen lediglich die im Modell bestehenden Strukturen hinsichtlich der Abläufe in einem realen Unternehmen zielgerichtet adaptiert und an die organisationalen bzw. baulichen Rahmenbedingungen angepasst werden. Mit Hilfe des Faktorenkatalogs der Pharma AG kann aber bereits ein Großteil der Abläufe in einem realen Unternehmen abgedeckt werden. Durch den Einsatz des Doppelvektormodells lassen sich danach die relevanten Faktoren aus dem bestehenden Katalog herausfiltern und entsprechend der Vorgaben des Unternehmens bewerten. Basierend auf dem generischen Charakter der Pharma AG sowie des Doppelvektormodells lassen sich in weiterer Folge Muster für andere Unternehmen ableiten.

Literatur

[AcRa05] F. Acosta Ortega, C. Rafels Pallarola: “Security Strategies and Equilibria in Multiobjective Matrix Games”. Working Papers in Economics 128, Universitat de Barcelona. Espai de Recerca en Economia (2005).

[Ghos91] D. Ghose: “A necessary and sufficient condition for Pareto-optimal security strategies in multicriteria matrix games”. Journal of Optimization Theory and Applications, 68, 3 (1991), 463-481.

[GMPP11] J. Göllner, C. Meurers, A. Peer, G. Povoden: “Hybridisation of Social Network Analysis in Context with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria”. In: 7th Social Network Conference, University of Greenwich, London, (2011).

[GMP+14] J. Göllner, C. Meurers, A. Peer, L. Langer, M. Kammerstetter: „Bedeutung des Risikomanagements von Smart Grids“. Symposium Energieinnovation 2014, Graz, (2014).

[Göll09] J. Göllner, „Definition iRd LV Risikomanagement“, Vorlesungspräsentation an der Donau Universität Krems iRd ULG Risk Management, (2009).

[RaGP13] S. Rass, J. Göllner, A. Peer: RSB Deliverable. “Beschreibung einer fiktiven Unternehmensstruktur”. Deliverable iRd RSB Projekts, (2013).

[RaSc10] S. Rass, P. Schartner: “Multipath Authentication without shared Secrets and with Applications in Quantum Networks”. In: Proceedings of the International Conferenceon Security and Management (SAM), CSREA Press (2010), Bd. 1, 111-115.

[Rass09] S. Rass: “On Information-Theoretic Security: Contemporary Problems and Solutions”, Dissertation, Alpen-AdriaUniversität Klagenfurt, 2009.

[Rass13] S. Rass: “On Game-Theoretic Network Security Provisioning”. Springer Journal of Network and Systems Management, 21, 1 (2013), 47-64.

[RSPG13] S. Rass, S. Schauer, A. Peer, J. Göllner: „Sicherheit auf Basis Multikriterieller Spieltheorie“. DACH Security 2013, Nürnberg; 17.09.2013 - 18.09.2013; in: P. Schartner, P. Trommler: „DACH Security 2013“, S. 289-301, (2013).

[ScRR12] S. Schauer, S. Rass, B. Rainer: „IT-Security Risiko Management mit Elementen der Spieltheorie“. In: P. Schartner, J. Taeger (Hrsg.), *DACH Security 2012*, syssec (2012), 106-117.

[ScRS12] S. Schauer, B. Rainer, R. Schmid: „Ein spieltheoretischer Ansatz für das IT-Security-Risikomanagement“. Datenschutz und Datensicherheit DuD, 7, S. 492-496, (2012).

[WaDe08] Y. Wang, Y. Desmedt: “Perfectly Secure Message Transmission Revisited”, in IEEE Transactions on Information Theory, 2008, vol. 54, S. 2582-2595.

[Zimm92] P. Zimmermann: “PGP Pretty Good Privacy / Web of Trust” (1992). http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html