Prieß, Andreas; Hoppe, Gabriela

Working Paper

Modellierung der Sicherheit von Informationssystemen mit DROPS

Diskussionsbeitrag, No. 301

Provided in Cooperation with:
School of Economics and Management, University of Hannover

Suggested Citation: Prieß, Andreas; Hoppe, Gabriela (2004) : Modellierung der Sicherheit von Informationssystemen mit DROPS, Diskussionsbeitrag, No. 301, Universität Hannover, Wirtschaftswissenschaftliche Fakultät, Hannover

This Version is available at:
https://hdl.handle.net/10419/22413

Modellierung der Sicherheit von Informationssystemen mit DROPS[1]

Dipl.-Ök. Andreas Prieß[2] und Dipl.-Ök. Gabriela Hoppe[3]
priess@ccc.uni-hannover.de und hoppe@iwi.uni-hannover.de

Diskussionspapier Nr. 301
Juli 2004
ISSN 0949-9962

JEL-Klassifikation: O39, Z0
Schlüsselworte: Sicherheitsmanagement, Sicherheit von Informationssystemen, IT-Sicherheit, Sicherheitsmodell, Sicherheitsanforderungen, Sicherheitsaspekte, Sicherheitsmaßnahmen

Universität Hannover

Wirtschaftswissenschaftliche Fakultät

---

1 Dieser Beitrag wurde eingereicht bei der „7. internationalen Tagung Wirtschaftsinformatik 2005“ (www. wi2005.de).

2 Niedersächsisches Hochschulkompetenzzentrum für SAP (CCC), Universität Hannover, Welfengarten 1, PF 114, D-30167 Hannover. Tel.: +49-(0)511-762 19889, Fax: +49-(0)511-762 19782. www.ccc.uni-hannover.de.

3 Institut für Wirtschaftsinformatik, Universität Hannover, Königsworther Platz 1, D-30167 Hannover. Tel.: +49-(0)511-762 9078, Fax: +49-(0)511-762 4013. www.iwi.uni-hannover.de.

Inhaltsverzeichnis

Modellierung der Sicherheit von Informationssystemen mit DROPS

Dipl.-Ök. Andreas Prieß und Dipl.-Ök. Gabriela Hoppe

Niedersächsisches Hochschulkompetenzzentrum für SAP (CCC)
und Institut für Wirtschaftsinformatik
Universität Hannover
priess@ccc.uni-hannover.de
hoppe@iwi.uni-hannover.de

Abstract: *Durch die Modellierung der Sicherheit betrieblicher Informationssysteme kann die Komplexität des Sicherheitsproblems in einer Organisation und ihren Geschäftsprozessen reduziert werden. Das Erkennen von Sicherheitsanforderungen sowie optimaler Handlungsalternativen in Form geeigneter Sicherheitsmaßnahmen wird erleichtert. DROPS (dimensions-relationales organisations- und problembezogenes Sicherheitsmodell) ist ein Modell der Sicherheit von Informationssystemen, das dieses ermöglicht. Der DROPS zugrunde liegende Ansatz ist ganzheitlich und erweiterbar. Beispielsweise werden Sicherheitsbetrachtungen im Zusammenhang mit Informationssystemen häufig auf eine technische Perspektive (IT-Sicherheit) beschränkt. DROPS erlaubt jedoch sowohl die Modellierung einer rein technischen Sichtweise als auch die Integration nicht-technischer Systemkomponenten (z.B. personelle Systembestandteile). Zudem können auch nicht-technische Sicherheitsmaßnahmen (z.B. organisatorischer Art) in das Modell einbezogen werden. Durch den Aufbau von DROPS ist es möglich, organisationsindividuell die für spezifische Geschäftsprozesse wesentlichen Elemente eines Sicherheitsproblems sowie deren Beziehungen in das Modell zu integrieren. So kann in der praktischen Anwendung zum einen die Auswahl geeigneter Sicherheitsmaßnahmen erleichtert werden. Zum anderen kann DROPS zur Modellierung aktueller und/oder angestrebter Sicherheitsanforderungen sowie des Sicherheitssystems einer Organisation eingesetzt werden.*

Schlüsselworte*: Sicherheitsmanagement, Sicherheit von Informationssystemen, IT-Sicherheit, Sicherheitsmodell, Sicherheitsanforderungen, Sicherheitsaspekte, Sicherheitsmaßnahmen*

1 Einleitung

Die **Sicherheit von Informationssystemen** ist ein aktuelles und vieldiskutiertes Thema. Dies liegt vor allem daran, dass Organisationen und Privatpersonen durch die Durchdringung aller Bereiche des öffentlichen und privaten Lebens mit Informations- und Kommunikationstechnologien verstärkt auf Informationssysteme (IS) angewiesen sind. Die Sicherheit von IS muss als Grundvoraussetzung für effektive und effiziente technikgestützte Geschäftsprozesse angesehen werden – nicht zuletzt, da die Akzeptanz der Nutzer von IS wesentlich vom Vertrauen in die zugrunde liegenden technischen Systeme abhängt.

Organisationen, die Informationssysteme im Rahmen ihrer Geschäftsprozesse einsetzen, sehen sich einem **Sicherheitsproblem** gegenüber, da sich nicht alle verfolgten Sicherheitsziele zu 100% realisieren lassen. Das Sicherheitsproblem, das eine Organisation lösen muss, liegt in der Erkennung aller Risiken im Zusammenhang mit der Informationsverarbeitung und in der Auswahl geeigneter Gegenmaßnahmen. Eine Auswahl geeigneter Sicherheitsmaßnahmen ist aufgrund der Komplexität des Sicherheitsproblems kein triviales Problem: Es sind mehrere Dimensionen des Problems sowie deren Beziehungen zueinander zu berücksichtigen. Als **Dimensionen der IS-Sicherheit** müssen fünf unterschiedliche Gesichtspunkte berücksichtigt werden: betroffene Komponenten, Sicherheitsaspekte, Gefahren, Schwachstellen und Maßnahmen [HP03]. Werden nicht alle Dimensionen berücksichtigt, wird das Sicherheitsproblem nicht vollständig dargestellt.

Ein Modell der IS-Sicherheit zur Unterstützung der Entscheidungsfindung ist „**DROPS**“ (dimensions-relationales organisations- und problembezogenes Sicherheitsmodell). DROPS integriert die verschiedenen Dimensionen der Sicherheit von Informationssystemen und erlaubt es Organisationen, ihre individuelle Sicht auf das Sicherheitsproblem zu modellieren. Diese Sicht kann organisationsbezogen oder problembezogen sein, sie kann sowohl technische Elemente (im Sinne der IT-Sicherheit) als auch nicht-technische Elemente beinhalten. Im Folgenden werden die Dimensionen der Sicherheit von Informationssystemen kurz beschrieben sowie Aufbau und Verwendung von DROPS erläutert.

2 Dimensionen der Sicherheit von Informationssystemen

2.1 Komponenten von Informationssystemen

Betriebliche Systeme zur Beschaffung, Erfassung, Speicherung, Übertragung, Transformation und Bereitstellung von Informationen werden als Informationssysteme (IS) bezeichnet. Dabei handelt es sich um soziotechnische Systeme, deren Zielsetzung die Informationsverarbeitung für eine Organisation darstellt. Diese Systeme lassen sich in technische und nicht-technische Komponenten zerlegen. Zu den technischen Komponenten gehören **Hardware** (HW) und **Software** (SW). Die nicht-technischen Bestandteile sind organisatorische Regelungen und Konzepte (**Orgware**, OW) sowie die Menschen, die mit dem IS als Anwender, Betreuer oder Verantwortliche arbeiten (**Manware**, MW). Diese vier IS-Komponenten können sowohl Ansatzpunkte von Gefahren als auch Ausgangspunkte bzw. Ursachen von Schwachstellen sein [HP03]. Grundsätzlich können noch zwei weitere IS-Komponenten, **Daten** (D) und **Informationsmanagement** (IM), betrachtet werden.

Daten sind das Objekt der technikgestützten Verarbeitung und haben einen rein passiven Charakter, da sie lediglich durch die anderen Komponenten beschafft, verarbeitet und bereitgestellt werden. Das Informationsmanagement, zu dem auch das Sicherheitsmanagement gehört, ist eine betriebliche Funktion, die von der Manware ausgeübt wird, und daher ebenfalls weder Ansatzpunkt von Gefahren noch Ausgangspunkt von Schwachstellen sein kann.

Neben den Komponenten HW, SW, OW und MW eines IS sind unter Sicherheitsgesichtspunkten auch bestimmte Elemente der **Umwelt** bedeutsam, beispielsweise die durch das Informationssystem genutzte und grundsätzlich ebenfalls schützenswerte Infrastruktur (sowohl technische Infrastruktur, z.B. das Internet, als auch Räume und Gebäude) oder Menschen, die nicht Bestandteil der Manware des IS sind (z.B. Servicepersonal, Lieferanten, Kunden, Hacker o.ä.). Das Schalenmodell der IS-Sicherheit veranschaulicht die genannten sicherheitsrelevanten Elemente (Abbildung 1).

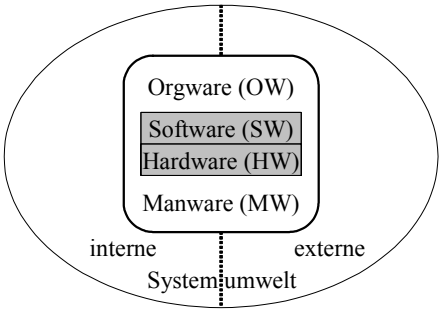


Abbildung 1: Schalenmodell der IS-Sicherheit

2.2 Sicherheitsaspekte

Der Begriff Sicherheit wird sowohl in der Theorie als auch in der Praxis uneinheitlich verwendet und i.d.R. abhängig vom Betrachtungsgegenstand mit einem bestimmten Schwerpunkt untersucht. So finden sich viele Abhandlungen zu speziellen Anwendungsbereichen (z.B. Datensicherheit, Kommunikationssicherheit), aber beispielsweise auch eine Unterscheidung von „safety“ (Funktionssicherheit) und „security“ (Informationssicherheit) [z.B. Ec03].

Grundsätzlich bezeichnet **Sicherheit** den Zustand des Sicherseins vor Gefahr oder Schaden. Betrachtet man soziotechnische IS, müssen alle Facetten des Sicherheitsbegriffs gemeinsam und integriert betrachtet werden. Die IS-Sicherheit beinhaltet dabei mindestens vier verschiedene Aspekte[4] [HP03]:

- **Vertraulichkeit** (Vt) bedeutet, dass ausschließlich autorisierte Personen Zugriff auf Daten bzw. Zugang zu Systemen haben.
- **Integrität** (In) ist gewährleistet, wenn Daten korrekt, aktuell, vollständig und widerspruchsfrei bzw. konsistent sind sowie absichtliche oder unabsichtliche Änderungen an Programmen, die zu falschen, unvollständigen oder nur vorgetäuschten Abläufen führen, ausgeschlossen sind.
- **Verfügbarkeit** (Vf) ist gegeben, wenn keine Beeinträchtigungen der Funktionalität eines IS vorliegen und das System einschließlich der Daten autorisierten Nutzern uneingeschränkt zur Verfügung steht.
- **Verbindlichkeit** (Vb) in einem IS ist gewährleistet, wenn Authentizität und Nachweisbarkeit gegeben sind. Authentizität besagt, dass die Erstellung,

[4] In der Literatur werden teilweise weitere Sicherheitsaspekte betrachtet [z.B. Ec03], die ebenfalls in das Modell integriert werden können. Sie werden hier vernachlässigt, da sie bei der Informationsverarbeitung in einer Organisation weniger häufig betrachtet werden.

Verarbeitung oder Übertragung von Daten den auslösenden Systemnutzern zweifelsfrei zugeordnet werden kann. Nachweisbarkeit bezeichnet Nicht-Abstreitbarkeit und betrifft die Umstände der Erstellung, Verarbeitung oder Übertragung der Daten, z.B. den Zeitpunkt oder die Reihenfolge der Datenerstellung.

2.3 Gefahren, Schwachstellen und Sicherheitsmaßnahmen

Gefahren bezeichnen objektive Möglichkeiten eines Schadeneintritts, losgelöst von konkreten IS. In der Literatur werden sehr unterschiedliche Kategorisierungen vorgenommen [z.B. FHW01, Sc01, Bu02 oder Ec03]. Grob unterscheiden lassen sich **Angriffe**, die bewusst bzw. vorsätzlich verursacht werden, und **Störungen**, die entweder unbewusst bzw. fahrlässig verursacht werden oder auf höhere Gewalt zurückzuführen sind. Angriffe lassen sich weiter unterteilen in Sabotageangriffe, die eine Beeinträchtigung, Veränderung oder Zerstörung von IS-Komponenten umfassen, und Spionageangriffe, die auf die Gewinnung von Informationen beschränkt sind.

Voraussetzung dafür, dass Gefahren wirksam werden können, stellen geeignete Schwachstellen dar. Gefahren, sowohl Angriffe als auch Störungen, setzen grundsätzlich an Komponenten des IS an. Wird eine Gefahr nicht durch eine geeignete Sicherheitsmaßnahme abgefangen, liegt eine **Schwachstelle** vor.

Während Gefahren grundsätzlich ohne Bezug zu einem IS existieren, beziehen sich Sicherheitsmaßnahmen auf die konkrete Sicherheitssituation in einer Organisation und auf die konkrete Ausgestaltung des IS. **Sicherheitsmaßnahmen** umfassen grundsätzlich alle Tätigkeiten, die durch menschliche oder maschinelle Aufgabenträger ausgeführt werden können und der IS-Sicherheit dienen. Sie werden im Rahmen des Sicherheitsprozesses ausgewählt und in einem Sicherheitskonzept dargestellt. Das Sicherheitskonzept ist das zentrale Element des Sicherheitsmanagements und dient der Verknüpfung strategischer und operativer Aufgaben, indem sicherheitsbezogene Ziele mit konkreten Handlungsanweisungen in Beziehung gesetzt werden [HP03].

Alle IS-Komponenten, die von eingesetzten Sicherheitsmaßnahmen betroffen sind und deren übergeordnetes Ziel die Sicherheit der Informationsverarbeitung in der Organisation ist, bilden das **Sicherheitssystem** einer Organisation.

Maßnahmen können sowohl für eine einmalige als auch für periodische oder dauerhafte Durchführung vorgesehen sein. Zudem können durch Sicherheits-maßnahmen neue IS-Komponenten entstehen und neue Maßnahmen notwendig werden. Beispielsweise führt die Maßnahme „Installation einer Firewall“ dazu, dass dem IS neue Komponenten (zusätzliche HW, SW, OW, MW) zugefügt werden; nach Inbetriebnahme wird eine neue Sicherheitsmaßnahme „Administration und Wartung der Firewall“ notwendig. Zu unterscheiden sind

präventive Maßnahmen, die das Wirksamwerden einer Gefahr verhindern sollen, **detektive Maßnahmen**, die Gefahreneintritte entdecken und anzeigen sollen, und **korrigierende Maßnahmen**, die im Schadensfall diesen minimieren und ggf. Verluste wieder herstellen sollen.

3 Dimensions-relationales organisations- und problembezogenes Sicherheitsmodell (DROPS)

Zur Darstellung der Dimensionen der IS-Sicherheit finden unterschiedliche Klassifikationen in der Literatur Verwendung [z.B. HP03, BZ00]. Diese stellen einzelne Dimensionen und zum Teil auch bestimmte Zusammenhänge zwischen Dimensionen theoretisch dar. Ein Beispiel für ein verhältnismäßig komplexes Klassifikationsschema ist der Sicherheitskubus, der die Dimensionen IS-Komponente (als Gefährdungsebene bezeichnet), Sicherheitsaspekt und Sicherheitsmaßnahme theoretisch vollständig beschreibt [HP03].

Oftmals erlaubt die Komplexität sicherheitsrelevanter Fragestellungen es in den genannten Ansätzen jedoch nicht, die Sicherheitssituation – vor allem die Sicherheitsanforderungen – in ihrer Komplexität zu erfassen und daraus Handlungsalternativen in Form möglicher Sicherheitsmaßnahmen abzuleiten. Daraus leitet sich die **Notwendigkeit eines umfassenden Modells für die Sicherheit von Informationssystemen** ab.

Ein **Modell** der Sicherheitssituation kann zur übersichtlichen Darstellung und Analyse komplexer Zusammenhänge herangezogen werden, diese vereinfachen und die Entscheidungsfindung unterstützen. Modelle bilden reale Sachverhalte vereinfachend ab. Ein Modell stellt dabei das Ergebnis einer Konstruktion dar, die ein Modellierer als „Repräsentation eines Originals zu einer Zeit“ als relevant erachtet und für einen Modellnutzer mit Hilfe einer Sprache erstellt [Sc98]. Ein Modell muss einerseits alle entscheidungsrelevanten Größen enthalten und andererseits so stark abstrahieren, dass die im Hinblick auf die Entscheidungsfindung relevanten Zusammenhänge deutlich werden. Dabei muss ein Kompromiss zwischen Detailliertheit des Modells und Aufwand für die Entscheidungsfindung gefunden werden.

Ein Modell für die Sicherheit von Informationssystemen, das die praktische Anwendbarkeit fokussiert, ist „**DROPS**“. Ziel der Anwendung von DROPS im Rahmen des Sicherheitsmanagements ist die Modellierung der sicherheitsrelevanten Geschäftsprozesse einer Organisation auf der einen Seite und des sich daraus ergebenden Sicherheitsproblems auf der anderen Seite. Die systematische und strukturierte Zusammenfassung und Gegenüberstellung der sicherheitsrelevanten Punkte ermöglicht die Ableitung von Sicherheitsanforderungen ebenso wie von geeigneten Sicherheitsmaßnahmen für eine spezifische Organisation.

DROPS ist **dimensions-relational**, da die verschiedenen Dimensionen der IS-Sicherheit integriert und die relevanten Beziehungen (Relationen) zwischen ihnen abgebildet werden. DROPS unterstützt zwei verschiedene Sichten auf die IS-Sicherheit, die Organisationssicht und die Problemsicht, und ist daher ein **organisations-**[5] und **problembezogenes Sicherheitsmodell**. Abbildung 2 stellt die Dimensionen von DROPS im Überblick dar.

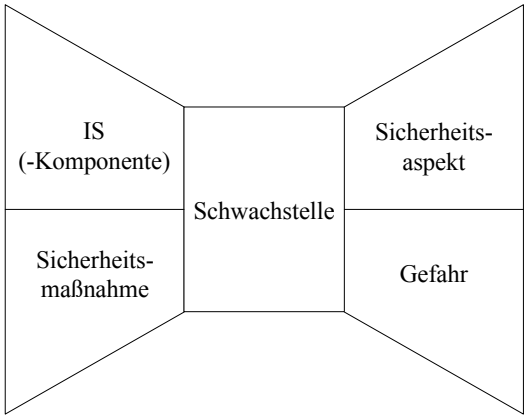


Abbildung 2: Die Dimensionen von DROPS im Überblick

Die **Anordnung der Dimensionen** in Abbildung 2 verdeutlicht bereits die grundlegenden Strukturen des Modells. Jede Dimension wird zunächst durch eine Fläche dargestellt. Aneinander angrenzende Flächen weisen auf einen engen Zusammenhang der Dimensionen in DROPS hin (Sicherheitsmaßnahmen beziehen sich auf Komponenten, Gefahren betreffen Sicherheitsaspekte etc.). Alternative Anordnung der Dimensionen wären natürlich grundsätzlich möglich, da alle Dimensionen eng miteinander verbunden sind; allerdings würde dabei das hier zugrunde gelegte Verständnis der IS-Sicherheit nicht adäquat abgebildet werden. Besondere Bedeutung kommt demnach den Schwachstellen zu, die in DROPS an alle anderen Dimensionen angrenzen: Sie sind gleichzeitig Ursache des Sicherheitsproblems, Ansatzpunkt für die Lösung des Problems und Ausgangspunkt für die Komplexitätsreduktion in DROPS.

Die Dimensionen werden in DROPS durch Elemente (Objekte bzw. Entitäten) konkretisiert. Die Anordnung der Dimensionen im Modell wird bei der Beschreibung der beiden Sichten deutlich. Im folgenden Abschnitt werden daher

[5] Gemeint ist hier der Organisationsbegriff im institutionellen Sinn: DROPS kann z.B. gleichermaßen zur Modellierung des Sicherheitsproblems privatwirtschaftlicher Unternehmen und öffentlicher Verwaltungen eingesetzt werden. Der Tatsache, dass jede institutionelle Organisation eine funktionelle Organisation hat, wird in der expliziten Berücksichtigung der Orgware eines IS Rechnung getragen.

die Sichten beschrieben, die jeweiligen Elemente benannt und auf die Beziehungen bzw. Relationen zwischen diesen eingegangen.

4 Sichten und Verwendung von DROPS

4.1 Organisationssicht

Die **Organisationssicht von DROPS** umfasst die IS-Komponenten HW, SW, MW und OW einer Organisation (einschließlich kritischer Infrastrukturkomponenten) sowie die im Zusammenhang mit den Komponenten bestehenden Schwachstellen und die als Reaktion auf die Schwachstellen ergriffenen Sicherheitsmaßnahmen (Abbildung 3). Für jede dieser drei Dimensionen müssen bei der Modellierung alle Elemente (Objekte bzw. Entitäten) identifiziert werden, die in das Modell der Organisationssicht aufgenommen werden müssen.

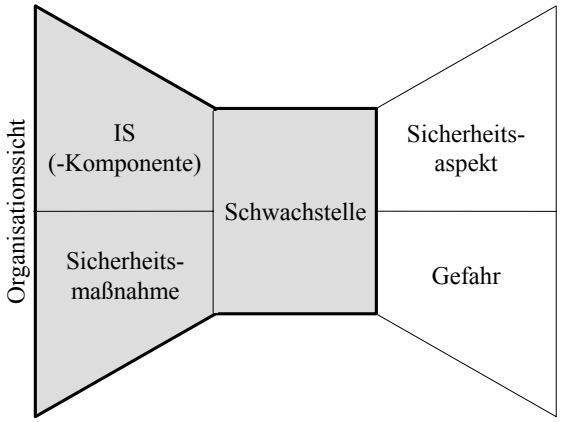


Abbildung 3: Organisationssicht von DROPS

Ausgangspunkt der Modellierung der Organisationssicht stellen die **Komponenten** des IS dar, die im Rahmen der Durchführung der Geschäftsprozesse einer Organisation zum Einsatz kommen. Die Unternehmung kann und sollte auf bestehende Modelle einzelner **Komponenten** zurückgreifen (z.B. Hardwarearchitektur, Softwarearchitektur, Organigramm, Geschäftsprozessmodell), um die relevanten Elemente zu ermitteln. Dabei ist es zum einen möglich, sowohl das IS insgesamt als auch Subsysteme in den Mittelpunkt der Betrachtung zu stellen. Diese Subsysteme können unter funktionalen, organisationsbezogenen oder anderen Perspektiven gebildet werden, und müssen sukzessive bis zum benötigten Abstraktionsgrad in Form hierarchischer

Abhängigkeitsbeziehungen dargestellt werden. Zum anderen können die Komponenten eines IS gemeinsam oder separat betrachtet werden (Tabelle 1).

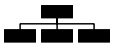
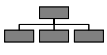
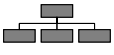
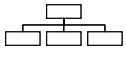
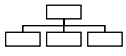
		IS gesamt	HW	SW	OW	MW	Externe Komponenten
	IS gesamt						
Funktionale Teilsysteme	WWW						
	CRM						
Organisationale Teilsysteme	IS Standort X						
	IS Standort Y						

Tabelle 1: Mögliche Detaillierungsgrade für die Komponenten der DROPS-Organisationssicht

Zu den Elementen der Organisationssicht gehören neben den Komponenten die **Schwachstellen** eines IS. Diese werden im Rahmen der Risikoanalyse ermittelt[6] und können anschließend den Teilsystemen und/oder den Komponenten eines IS zugeordnet werden. Eine Schwachstelle kann dabei grundsätzlich auf verschiedenen Ebenen bestehen (z.B. kann eine Schwachstelle „fehlende Zugangskontrollen“ sowohl im Hinblick auf das IS insgesamt als auch auf eine bestimmte Teilkomponente, beispielsweise einen Datenbankserver, bestehen). In DROPS muss die entsprechende Relation zwischen Komponente und Schwachstelle auf allen Ebenen ins Modell aufgenommen werden.

Weiterer Bestandteil der Organisationssicht sind die **Sicherheitsmaßnahmen**, die im Sicherheitskonzept spezifiziert werden. Diese beziehen sich immer auf Schwachstellen des IS und müssen den Komponenten auf allen betroffenen Ebenen zugeordnet werden.

Abbildung 4 verdeutlicht die Relationen zwischen den Elementen der Komponenten, Schwachstellen und Sicherheitsmaßnahmen. Hier und bei allen

6 Die Risikoanalyse setzt sich aus den Schritten Wertanalyse, Gefahrenanalyse, Schwachstellenanalyse und Risikobewertung zusammen [HP03].

folgenden Relationen werden die Beziehungen zwischen Elementen durch **Kardinalitäten** konkretisiert, die in der **(min,max)-Notation** angegeben sind.

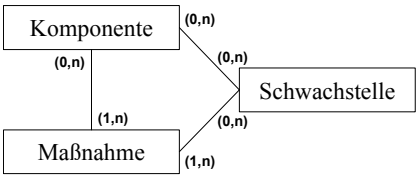


Abbildung 4: Relationen der Organisationssicht

Eine Komplexitätsreduktion ist bereits möglich, indem nur Komponenten mit Schwachstellen in das Modell aufgenommen werden; es besteht jedoch die Gefahr, das Sicherheitsproblem nicht vollständig zu erfassen, falls nicht alle Schwachstellen erkannt werden und/oder nicht modellierte Komponenten bei späteren Betrachtungen der Sicherheitssituation nicht mehr berücksichtigt werden.

4.2 Problemsicht

Die **Problemsicht von DROPS** umfasst die Gefahren für die IS-Sicherheit, die betroffenen Sicherheitsaspekte sowie die Schwachstellen, die Ausgangspunkt oder Ansatzpunkt der Gefährdungen darstellen (Abbildung 5).

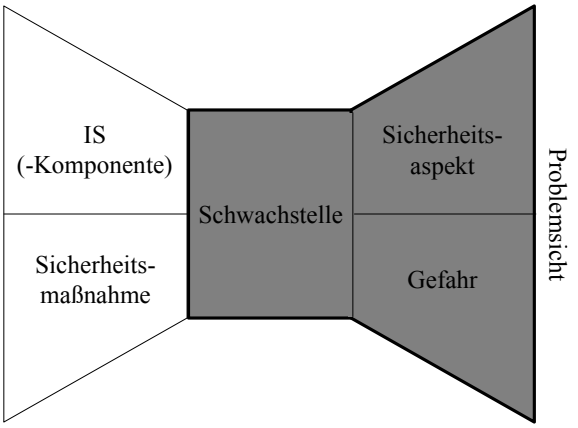


Abbildung 5: Problemsicht

Auch hier müssen bei der Modellierung für die drei Dimensionen alle Elemente identifiziert werden, die in das Modell aufgenommen werden sollen. Ausgangspunkt sind die **Gefahren** der IS-Sicherheit. Die Problemsicht ist abstrakter als die Organisationssicht, da diese Dimension (im Gegensatz zu den IS-Komponenten) nicht grundsätzlich auf eine konkrete Organisation bezogen ist.

Hier kann bei Bedarf ein beliebig umfassendes Kontinuum potenzieller Sicherheitsprobleme aufgespannt werden.

Für die Ermittlung der in das Modell aufzunehmenden Elemente kann auf die grundsätzliche Unterteilung von Gefahren in Angriffe und Störungen zurückgegriffen werden. Diese können beliebig weiter hierarchisch untergliedert werden; verschieden Kategorisierungsmöglichkeiten sind in der Literatur zu finden [z.B. Mo93, FHW01, Bu02, Ec03 oder HP03]. Zudem ist für das Sicherheitsproblem die Frage relevant, wer oder was die Ursache für die Gefahr darstellt. Menschliche Gefahrenverursacher können dabei sowohl Angriffe als auch Störungen verursachen, alle anderen Verursacher können nur Störungen in Form höherer Gewalt hervorrufen (Tabelle 2). Auch die Gefahrenursachen lassen sich beliebig weiter untergliedern [z.B. HP03].

	Gefahren-ursache	Menschen		Andere Ursachen	
		Zutritts-berechtigte	Nicht Zutritts-berechtigte	IS-intern	IS-extern
Angriff	Spionage			-	-
	Sabotage			-	-
Störung	Fahrlässigkeit			-	-
	Höhere Gewalt	-	-		

Tabelle 2: Mögliche Detaillierungsgrade für die Gefahren in der DROPS-Problemsicht

Die **Schwachstellen** eines IS stellen ebenfalls Elemente der Problemsicht dar. Hier können grundsätzlich alle potenziellen Schwachstellen aller theoretisch denkbaren IS berücksichtigt werden; zu empfehlen ist hier in Sinne der Komplexitätsreduktion die Beschränkung auf Schwachstellen, die das IS der Unternehmung aufweist oder zumindest aufweisen könnte. Auch hier besteht allerdings die Gefahr, nicht modellierte Schwachstellen bei späteren Analysen des Sicherheitsproblems der Organisation zu übersehen. Die Modellierung der Problemsicht sollte somit als zweiter Schritt nach der Modellierung der Organisationssicht erfolgen.

Die **Sicherheitsaspekte**, die durch das Wirksamwerden einer Gefahr verletzt werden, werden in DROPS durch genau vier Elemente abgebildet (Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit). Wird für ein zu modellierendes Sicherheitsproblem die Betrachtung weiterer Aspekte benötigt, können entsprechende Elemente ergänzt werden.

Die Relationen zwischen den Elementen, die die Gefahren, Schwachstellen und Sicherheitsaspekte konkretisieren, sind in Abbildung 6 dargestellt.

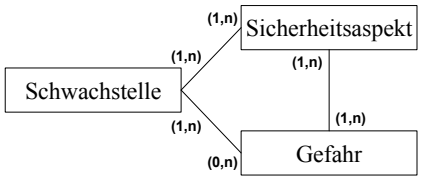


Abbildung 6: Relationen der Problemsicht

4.3 Verwendung von DROPS

Die unterschiedlichen Sichten auf DROPS können grundsätzlich unabhängig voneinander modelliert werden. In der **Organisationssicht** ist eine vollständige Abbildung aller geschäftsprozessrelevanten Komponenten des Informationssystems und der spezifizierten Teilsysteme im Rahmen der gewählten hierarchischen Detaillierung zu empfehlen: Die Vollständigkeit dieser Sicht auf das Modell sollte gewährleistet bleiben, da sich alle Elemente im Einflussbereich der Unternehmung befinden. Eine Komplexitätsreduktion durch Abstraktion ist theoretisch aber möglich. In der **Problemsicht** kann, wenn das Modell der Organisationssicht vorliegt, eine Komplexitätsreduktion durch Beschränkung auf relevante Schwachstellen vorgenommen werden: Die hier modellierten Elemente befinden sich nicht im Einflussbereich der Unternehmung und müssen daher intensiver auf nicht modellierte Sachverhalte überprüft werden, zumal eine vollständige Abbildung, genau wie eine vollständige Gewährleistung der IS-Sicherheit, grundsätzlich unmöglich ist.

Die **Komplexitätsreduktion** durch DROPS erfolgt somit einerseits durch die gewählte Strukturierung und Hierarchisierung der Elemente beider Sichten. Die IS-Komponenten sollten vollständig modelliert werden (Abbildung 7), auch wenn sie keine Schwachstellen aufweisen; dies ist durch die gestrichelte Linie in nachstehender Abbildung 7 dargestellt. Andererseits erfolgt Komplexitätsreduktion durch die modellierten Schwachstellen eines IS, die das Bindeglied zwischen den beiden DROPS-Sichten darstellen.

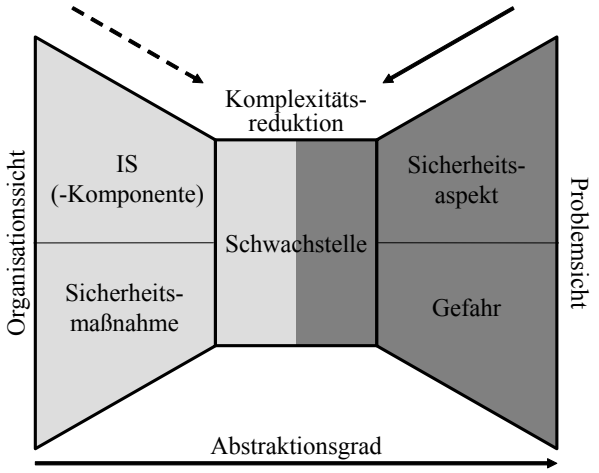


Abbildung 7: Problem- und Organisationssicht in DROPS

Auf die Modellierung der Beziehungen zwischen Elementen der beiden unterschiedlichen Sichten, beispielsweise zwischen Sicherheitsmaßnahmen und Sicherheitsaspekten, kann in diesem Modell aus Vereinfachungsgründen verzichtet werden. Alternativ können diese übergreifenden Relationen nach Erstellung der beiden DROPS-Sichten ergänzt werden (vgl. für eine ausführliche Betrachtung der Beziehungen zwischen Sicherheitsmaßnahmen und Sicherheitsaspekten z.B. [HP03]). Die vollständigen DROPS-Relationen sind Abbildung 8 zu entnehmen. Die durch eine gestrichelte Linie eingezeichnete Beziehung zwischen Sicherheitsmaßnahmen und Sicherheitsaspekten ist optional.

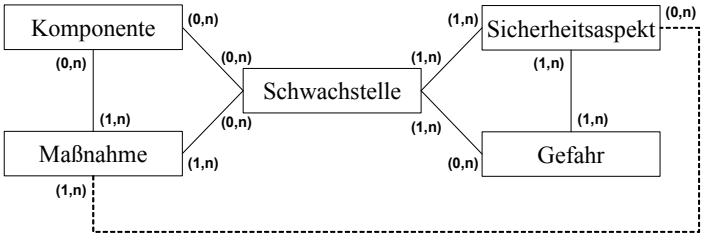


Abbildung 8: Vollständiges DROPS-Relationenmodell

5 Fazit und Ausblick

IT-Sicherheit und die noch umfassendere Sicherheit des gesamten Informationssystems stellt sich als aktuelles und komplexes Entscheidungs-

problem dar. Mit dem **neuen Ansatz „DROPS“** wurde ein Modell der Sicherheit geschäftsprozessrelevanter Informationssystemkomponenten vorgestellt, das in allen Organisationen eingesetzt werden kann. DROPS integriert IS-Komponenten, Sicherheitsmaßnahmen, Sicherheitsaspekte und Gefahren, die über Schwachstellen verknüpft werden. Es ist eine Modellierung sowohl aus Organisationssicht als auch aus Problemsicht möglich. Optional können sichtübergreifende Beziehungen modelliert werden.

DROPS kann in verschiedenen **Anwendungsszenarien** zum Einsatz kommen:

- Mit DROPS kann das Sicherheitsproblem einer Unternehmung modelliert werden, um die Komplexität der Realität zu reduzieren. So wird das Erkennen der für die Unternehmung relevanten Aspekte, Gefahren, Komponenten und Maßnahmen leichter.
- Mit DROPS kann das aktuelle Sicherheitsniveau (Ist-Sicherheit) sowie das angestrebte Sicherheitsniveau (Soll-Sicherheit) modelliert werden. Dabei werden die notwendigen Schritte zur Überführung des Ist-Zustandes in den Soll-Zustand leichter erkennbar. Geeignete Sicherheitsanforderungen sowie Sicherheitsmaßnahmen können hieraus abgeleitet werden.
- Mit DROPS kann das Sicherheitssystem einer Unternehmung modelliert werden. In dieser Anwendung wird es als Hilfsmittel zur systematischen und strukturierten Dokumentation eingesetzt.

DROPS kann im Wesentlichen als **Hilfsmittel für das Sicherheitsmanagement** aufgefasst werden. Im Rahmen des Sicherheitsmanagements wird unter anderem das individuelle Sicherheitsproblem einer Unternehmung analysiert und geeignete Sicherheitsmaßnahmen werden in einem Sicherheitskonzept niedergelegt.

Zu beachten ist, dass die Gewährleistung der Sicherheit von Informationssystemen niemals zu 100% möglich ist. Das liegt zum einen daran, dass nicht alle potenziellen Gefahren und Schwachstellen antizipiert bzw. erkannt werden können. Zum anderen ist dies durch die Begrenzung der verfügbaren Ressourcen bedingt. Dabei sind neben dem verfügbaren Know-How vor allem finanzielle Mittel angesprochen. Es kann aus diesem Grund nicht immer die für eine Unternehmung optimale Kombination von Sicherheitsmaßnahmen realisiert werden. Bei der Auswahl von Sicherheitsmaßnahmen spielen Wirtschaftlichkeitsgesichtspunkte eine wesentliche Rolle. Neben den Kosten für eine Sicherheitsmaßnahme wird bei der Wirtschaftlichkeitsbetrachtung ihr Nutzen bewertet. Eine Erweiterung von DROPS um Elemente der Kosten-/Nutzen-Bewertung von Sicherheitsmaßnahmen ist daher zumindest im Hinblick auf den Einsatzzweck der Maßnahmenauswahl sinnvoll und angedacht.

Literatur

[Bu02] Bundesamt für Sicherheit in der Informationstechnik (BSI, Hrsg.): IT-Grundschutzhandbuch. http://www.bsi.de/gshb/deutsch/etc/inhalt.htm, 2002, Abruf am 2004-06-18.

[BZ00] Baer, R.; Zängerle, P.: Wie misst man IT-Sicherheit? In: HMD, Heft 216, 2000., S. 67-77.

[Ec03] Eckert, C.: IT-Sicherheit. Konzepte, Verfahren, Protokolle. Oldenbourg: München, 2003.

[FHW01] Fuhrberg, K.; Häger, D.; Wolf, S.: Internet-Sicherheit. Browser, Firewalls und Verschlüsselung. Hanser Fachbuch: München u.a., 2001.

[HP03] Hoppe, G.; Prieß, A.: Sicherheit von Informationssystemen. NWB: Herne/Berlin, 2003.

[Mo93] Mohr, K.-L.: Art der Bedrohung. In: Pohl, H.; Weck, G. (Hrsg.): Einführung in die Informationssicherheit. Oldenbourg: München u.a., 1993, S. 34–43.

[Sc01] Schneier, B.: Secrets & Lies. IT-Sicherheit in einer vernetzten Welt. dpunkt Verlag: Heidelberg, 2001.

[Sc98] Schütte, R.: Grundsätze ordnungsmäßiger Referenzmodellierung. Konstruktion konfigurations- und anpassungsorientierter Modelle. Gabler: Wiesbaden, 1998.