Inventarisierung + Bewertung von IT-Risiken

Thomas Maus
Maus IT-Consulting
thomas.maus@alumni.uni-karlsruhe.de

26. DECUS Symposium

Inhalt

- Wo soll die Reise hingehen?
- Was ist Risiko eigentlich?
- Ein pragmatisches Modell für Risiko
- Die Risikokultur Ihrer Organisation
- Das Risikoinventar Ihrer Organisation
- Risikostruktur an Beispiel-Szenarien
- A-Risk-Methics
- Aus- und Rückblick

Wo soll die Reise hingehen?

- Verstehen der eigenen Sicherheitslage
- Kommunikationshilfsmittel für Gespräche zwischen Management, Fachseite + Administratoren
- Grundlage für nachvollziehbare, objektivierbare Entscheidungen
- Planungshilfsmittel für Sicherheitsarchitektur
- Priorisierung und Wirtschaftlichkeit von Maßnahmen

Was ist Risiko eigentlich?

- Mathematisch/Ingenieurswissenschaftlich
- Moralisch/Politisch
- Psychologisch

Was ist Risiko?

Mathematisch/Ingenieurswissenschaftlich

- DIN, VDE 31000:

Risiko(Schadensereignis)

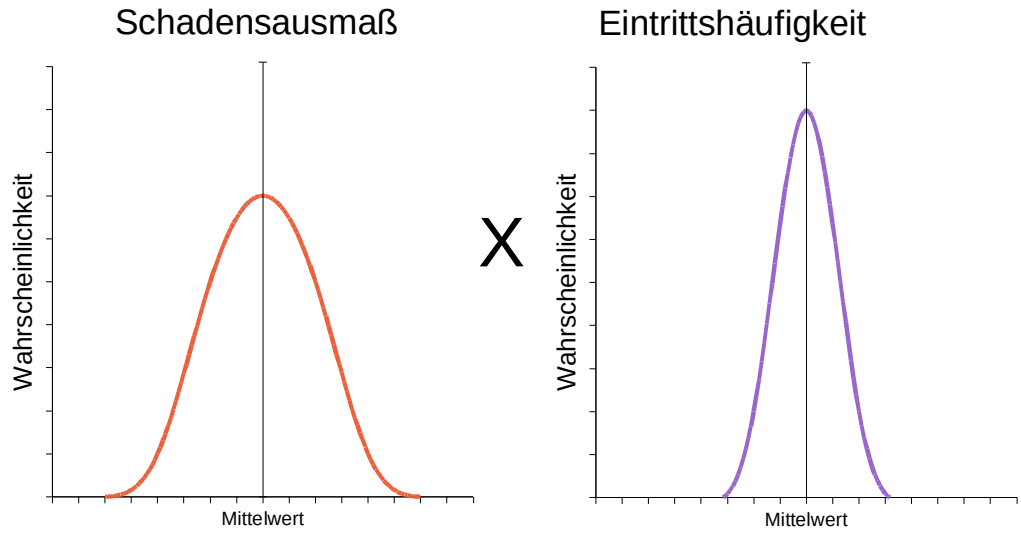
= (mittleres) Schadensausmaß

x (mittlere) Eintrittswahrscheinlichkeit

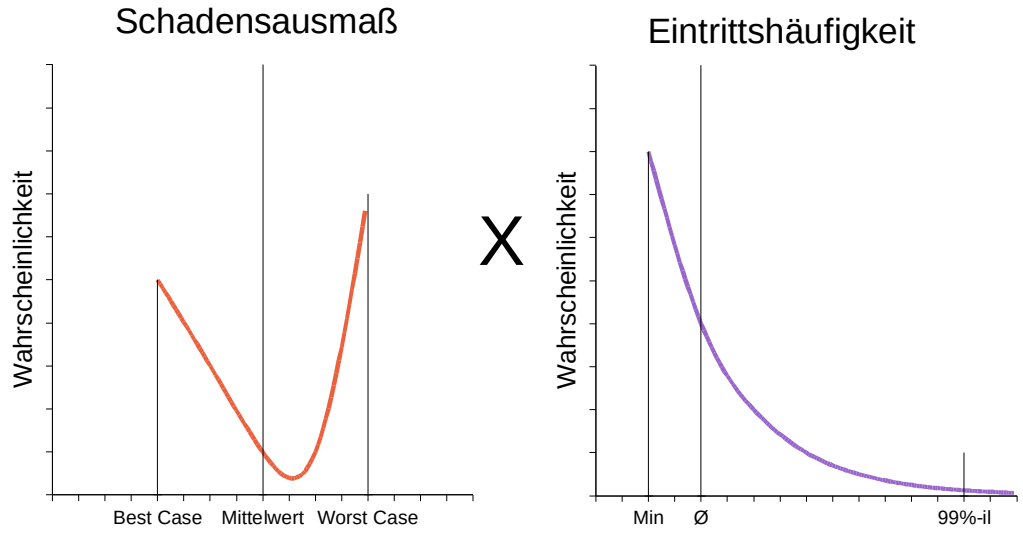
- aber:
  - wann gilt das?
  - Schadensausmaß?
  - Eintrittswahrscheinlichkeit?
  - Schadensverlauf und Beherrschbarkeit???

Was ist Risiko?

Mathematisch/Ingenieurswissenschaftlich



Was ist Risiko?
Mathematisch/Ingenieurswissenschaftlich



Was ist Risiko?
Moralisch/Politisch

Beispiel: Friedliche Nutzung der Kernenergie

- Statistisch (BRD):
  - 6–12 Tote/Kernkraftwerk/Jahr
  - ~ 200 Kernkrafttote/a << ~ 5000 Verkehrstote/a
- Schadensfall: SuperGAU Hüllenbruch > 10^7 a
  - 1–2 Millionen Tote
  - 10–20 Millionen Dauergeschädigte
  - weite Teile 100–200 Jahre unbewohnbar
- Akzeptabel? – Welche Prävention, Reaktion?

Was ist Risiko? Psychologisch

- Beispiel: Hausbesitzer
  - 100% Beitrag – normale Gebäudeversicherung
  - 120% Beitrag + Elementarschäden
  - 130% Beitrag + Allgefahrenversicherung
- Welchen Versicherungsschutz?
- Begrenztes Budget: lieber
  - Allgefahrengebäude- und kein Hausrat-V oder
  - Normale Gebäude- und Hausrat-V?

Was ist Risiko? Psychologisch

Saalexperiment – Was würden Sie wählen?

- **500 € Gewinn** / **Münzwurf: nichts oder 1.000 € Gewinn**
- **500 € Verlust** / **Münzwurf: nichts oder 1.000 € Verlust**
- **500 € Gewinn** / **Würfel: 6 = 10.000 € Gewinn**
- **500 € Verlust** / **Würfel: 6 = 10.000 € Verlust**

Was ist Risiko? Psychologisch

Gedankenexperiment zur IT-Sicherheit:

- Stellen Sie sich Ihren persönlichen GAU vor: Unter denen Zuhörern ohne blauen Hut wird einer ausgelost – den trifft sein persönlicher Gau …
- Sie können jetzt blaue Hüte kaufen, 500 €.
- Zweite Chance: Blaue Hüte zu 2.000 € …
- **Drei Hüte hab' ich noch. Gebote?**

Was ist Risiko? Psychologisch

Risiko-Psychologie:

- Chancen und Risiken werden asymmetrisch wahrgenommen
- Tendenz zur Verlustvermeidung
- Auswirkung von Informationsmangel/defiziten
- Wahrnehmbarkeit von Risiken
- Verdrängung von Risiken
- Gruppendynamische Effekte

Ein pragmatisches Modell für Risiko

Anforderungen an das Modell:

- Politische Grundsatzentscheidungen dokumentieren und abbilden
- Psychologischen Effekten entgegen wirken
- sinnvolle Risiko-Arithmetiken ermöglichen
- Schadensausmaß und Eintrittswahr-scheinlichkeiten handhabbar machen

Risiko-Modell: Eine Klasse für sich ...

Vorgehensweise:

- Definition von Klassen für
  - Schaden
  - Eintrittshäufigkeit
  - Risiko
- Verwendung von Liebert-Skalen
- Anpassung an Unternehmenssicht

Risiko-Modell: Eine Klasse für sich ...

Häufigkeitsklassen für Schadensereignisse

a	b	c	d
unvermeidbar	äußerst häufig	sehr häufig	häufig
tritt sicher ein	alle paar Tage	monatlich	jährlich
1,00E+000	2,00E-001	3,00E-002	2,74E-003
6,60E-001	1,32E-001	1,98E-002	1,81E-003

Risikokultur

Risiko-Klassifikation-Matrix

Die Risiko-Matrix definiert die Risikoklasse, die aus der Kombination bestimmter Häufigkeits- und Schadensklassen für Schadensereignisse resultiert

Häufigkeits-klassen für Schadenereignisse	Schadensklassen für Schadensereignisse					
Klasse *Umschreibung*	A katastrophal	B großer Schaden	C mittlerer Schaden	D kleiner Schaden	E unbedeutend	F vernachlässigbar
a unvermeidbar	irrationales Risiko	irrationales Risiko	irrationales Risiko	irrationales Risiko	extremes Risiko	kleines Risiko
b äußerst häufig	irrationales Risiko	irrationales Risiko	extremes Risiko	extremes Risiko	großes Risiko	minimales Risiko
c sehr häufig	irrationales Risiko	extremes Risiko	großes Risiko	großes Risiko	mittleres Risiko	kein Risiko
d häufig	irrationales Risiko	extremes Risiko	großes Risiko	mittleres Risiko	kleines Risiko	kein Risiko
e selten	irrationales Risiko	großes Risiko	mittleres Risiko	kleines Risiko	minimales Risiko	kein Risiko
f sehr selten	großes Risiko	mittleres Risiko	kleines Risiko	minimales Risiko	kein Risiko	kein Risiko
g äußerst selten	mittleres Risiko	kleines Risiko	minimales Risiko	kein Risiko	kein Risiko	kein Risiko
h eher unmöglich	kleines Risiko	minimales Risiko	unvermeidl. Restrisiko	kein Risiko	kein Risiko	kein Risiko
i praktisch unmöglich	unvermeidl. Restrisiko	unvermeidl. Restrisiko	kein Risiko	kein Risiko	kein Risiko	kein Risiko

Risikoinventar

- Werte
  - Image
  - Kundendaten
  - Geschäftsdaten
  - Unterstützende Daten- + Funktionsbestände
  - Betriebsgeheimnisse
  - I+K-Ressourcen
  - Produktivität
  - Mitarbeiter
- Prozeßwirkungen
  - Wertschöpfende Prozesse
  - Rechtswirksame Prozesse
  - Sonstige Prozeßwirkg.

Risikoinventar

- Rechtl.+Vertragl. Risiken
  - Bundesdatenschutzgesetz
  - Haftungspflichten (BGB, vertragl.)
  - KonTraG
  - Betriebsverfassungsgesetz
  - Fernmeldegeheimnis
  - Kryptoregulierungen
  - Telekommunikationsdienste-Gesetze
  - ...

Risikostruktur an Beispiel-Szenarien

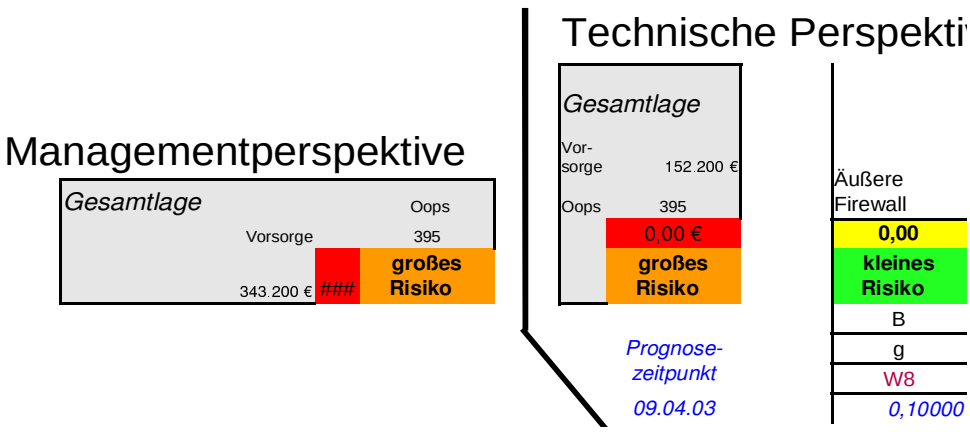
Zwei Beispielszenarien für Risikobewertung:

- K-Fall-Vorsorge für ein (kleines) fiktives RZ, Vergleich verschiedener Lösungsvarianten hinsichtlich Schutz und Wirtschaftlichkeit
- Sicherheitsanalyse, Vergleich von Sicherheitsarchitekturen, und Wirtschaftlichkeitsbetrachtung der Sicherheitsmaßnahmen

Risikobewertungstableaux *Szenario* *Ist-Zusta*

Vorschlag: Zwei unabhängige Firewalls, funktionales Interface zur DB, Grundschutz für Arbeitsplätze

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben w
Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und gesch
Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftliche



A-Risk-Methics

Ein Blick hinter die Kulissen:

- Schaurige Formeln in wohlweislich versteckten Zellen

Aus- und Rückblick

- Interview-Technik und resultierende Tabellen werden von Management und Technikern als hilfreich befunden.
- Viele Fragestellungen können nach Initial-aufwand effizient beleuchtet werden.
- Graphisches Werkzeug und etwas ausführlichere mathematische Modellierung wären wünschenswert.

Ende

Vielen Dank für Ihre Aufmerksamkeit!

Für Fragen:

thomas.maus@alumni.uni-karlsruhe.de

Risikobewertungstableaux *Szenario Vorschlag für Sicherheitsarchitektur*

Vorschlag: Zwei unabhängige Firewalls, funktionales Interface zur DB, Grundschutz für Arbeitsplätze

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden.
Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und geschäftlichen Bedrohungen her.
Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftlichen Einzelrisiken sowie Gesamtrisiken.

Managementperspektive

Gesamtlage

Vorsorge	Oops
343.200 €	395
	großes Risiko

Technische Perspektive

Gesamtlage

Vor-sorge	152.200 €
Oops	395
	großes Risiko

Prognose-zeitpunkt 09.04.03

Risikoinventar	Risikoaggregation Ind.	Klasse	W'keit Aggregation	*Schadensklasse* *Begründung*	Äußere Firewall	Web-Server in der DMZ (Web-Portal)	Schwach-stellen in der Applikations-logik	Innere Firewall	DB-Server mit Kunden- und Vertrags-daten für Web-Portal	Interne Server mit kritischen Geschäfts-prozessen	interne Arbeitsplätze	Admin-Arbeitsplätze	Bedrohungen
													Akzeptanz-Indikator
					kleines Risiko	**minimales Risiko**	**großes Risiko**	**unvermeidl. Restrisiko**	**minimales Risiko**	**kleines Risiko**	**großes Risiko**	**großes Risiko**	Risiko-Aggregation
					B	B	B	B	B	B	B	B	Schadensaggregation
					g	h	e	i	h	g	e	e	Häufigkeitsaggregation
					W8	W9	W6	W8	W3	W4	W4	W4	Wirksames Schutzniveau
					0,10000	*0,10000*	*0,10000*	*0,00000*	*0,00000*	*0,30000*	*0,50000*	*0,01000*	*Innentäter*
					1,00000	*1,00000*	*1,00000*	*0,00000*	*0,00000*	*0,01000*	*0,01000*	*0,00500*	*Externe Profis*
					1,00000	*1,00000*	*1,00000*	*0,00000*	*0,00000*	*0,00100*	*0,00100*	*0,00010*	*Cyber-Terroristen*
					500,00000	*500,00000*	*500,00000*	*0,00231*	*0,00005*		*10,00000*	*10,00000*	*klass. Hacker*
					60.000,00000	*60.000,00000*	*60.000,00000*	*0,27727*	*0,00557*		*900,00000*	*900,00000*	*Cyber-Punks*
					01.01.03	*01.01.03*	*01.04.02*	*01.01.03*	*11.11.99*	*01.01.03*	*01.01.03*	*01.01.03*	*Letzte Aktualisierg des Schutzniveaus*
					W8	*W9*	*W7*	*W8*	*W3*	*W5*	*W5*	*W5*	*Schutzniveau (Schätzung)*
					vor allem Piercing-Risiko, löst Risiken des Web-Servers aus!	gehärtet und über FW abgeschottet	Zugriff auf Kundendaten über URL-Manipulationen o.ä.	löst alle inneren Risiken aus, angreifbar nur über äußere FW oder Web-Server	vom Web-Server aus nur fixe Funktionsaufrufe zugänglich	nur von innen zugänglich, Grundschutz	Grundschutz (externe Angriffe via Mail oder Web)	Admin-WS sind normale Arbeitsplätze	Begründung
Werte			j										
Image des Unternehmens		**großes Risiko**	d	*C* per Definition	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	
Kundendaten (Vertraulichkeit)		**großes Risiko**	d	*C* per Definition	(löst Web-Server-Risiken aus)	x	x	(löst innere Risiken aus)	x		x	x	
Kundendaten (Verlust+Manipulation)		**mittleres Risiko**	d	*D* schwere Betriebsstörung	(löst Web-Server-Risiken aus)	x	x	(löst innere Risiken aus)			x	x	
Geschäftsdaten (Vertraulichkeit)		**großes Risiko**	e	*B* mind. Image-Schaden, wahrscheinl. geschwächte Verhandlungspositionen				(löst innere Risiken aus)		x	x	x	
Geschäftsdaten (Verlust+Manipulation)		**kleines Risiko**	e	*D* schwere Betriebsstörung				(löst innere Risiken aus)		x	x	x	
Unterstützende Daten- + Funktionsbestände		**minimales Risiko**	e	*E* kleine Betriebsstörung				(löst innere Risiken aus)		x		x	
Betriebsgeheimnisse (Vertraulichkeit)		**großes Risiko**	e	*B* Verlust von Kunden und Verhandlungspositionen				(löst innere Risiken aus)		x	x	x	
I+K-Ressourcen (Verfügbarkeit)		**kleines Risiko**	e	*D* schwere Betriebsstörung	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)		x		x	
Produktivität		**minimales Risiko**	e	*E* Ausfallzeiten/Hemmnisse in der Produktion				(löst innere Risiken aus)		x	x	x	
Mitarbeiter (Vertraulichkeit der Mitarbeiterdaten)		**mittleres Risiko**	e	*C* schwere BDSG-Verletzung, Verlust von Kernmitarbeitern				(löst innere Risiken aus)		x		x	
Prozeßwirkungen			j										
			j										
Wertschöpfende Proz.													
Internet-Portal		**mittleres Risiko**	e	*C* Image-Schaden, Verlust von Kunden, schwerste Produktionsausfälle	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)	x		x	x	
			j										
Rechtswirksame Proz.													
Leistungszusagen über das Internet-Portal		**großes Risiko**	e	*B* Gewinnausfälle	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)				x	
			j										
Sonstige Prozeßwirkg.													
Mißbrauch der I+K als Angriffsvehikel		**mittleres Risiko**	e	*C* Risiko einer Verurteilung wegen ungenügender Absicherung	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)				x	
			j										
Rechtl.+Vertragl. Risiko													
Bundesdatenschutzgesetz		**kleines Risiko**	e	*D* Strafgelder ...			dürfte Sicherungs-pflichten verletzen						
Haftungspflichten		**großes Risiko**	e	*B* Verurteilungen, Schadensersatz-forderungen	(löst Web-Server-Risiken aus)	möglicherweise	ziemlich sicher	(löst innere Risiken aus)				?	
...		**kein Risiko**	j	*F* zahlreiche weitere rechtl. + vertragl. Risikopotentiale									

Geschätzte Angriffe/Jahr der jeweiligen Tätertypen

Risikobewertungstableaux *Szenario Ist-Zustand Internet-Portal-zentriertes Unternehmen*

Internet-Portal stellt den Hauptgeschäftsprozeß des Unternehmens dar. Absicherung über eine Firewall mit DMZ und Intranet. DB im Intranet.

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden.
Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und geschäftlichen Bedrohungen her.
Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftlichen Einzelrisiken sowie Gesamtrisiken.

Managementperspektive

Gesamtlage

Vorsorge	Oops
1.883.000 €	3.618
	extremes Risiko

Technische Perspektive

Gesamtlage

Vorsorge	902.200 €
Oops	3.618
	extremes Risiko

Planungszeitpunkt *09.04.03*

Risikoinventar	Ind.	Klasse	W'keit Aggregation	*Schadensklasse* *Begründung*	Äußere Firewall	Web-Server in der DMZ (Web-Portal)	Schwachstellen in der Applikationslogik	Innere Firewall	DB-Server mit Kunden- und Vertragsdaten für Web-Portal	Interne Server mit kritischen Geschäftsprozessen	interne Arbeitsplätze	Admin-Arbeitsplätze	Bedrohungen
													Akzeptanz-Indikator
					kleines Risiko	minimales Risiko	großes Risiko	kleines Risiko	minimales Risiko	großes Risiko	extremes Risiko	extremes Risiko	Risiko-Aggregation
					B	B	B	B	B	B	B	B	Schadensaggregation
					g	h	e	g	h	e	d	d	Häufigkeitsaggregation
					W8	W9	W6	W8	W3	W3	W3	W3	Wirksames Schutzniveau
					0,10000	0,10000	0,10000	0,10000	0,00000	0,30000	0,50000	0,01000	*Innentäter*
					1,00000	1,00000	1,00000	1,00000	0,00000	0,01000	0,01000	0,00500	*Externe Profis*
					1,00000	1,00000	1,00000	1,00000	0,00000	0,00100	0,00100	0,00010	*Cyber-Terroristen*
					500,00000	500,00000	500,00000	500,00000	0,00005		10,00000	10,00000	*klass. Hacker*
					60.000,00000	60.000,00000	60.000,00000	60.000,00000	0,00557		900,00000	900,00000	*Cyber-Punks*
					01.01.03	01.01.03	01.04.02	01.01.03	11.11.99	09.10.02	01.04.00	01.04.00	*Letzte Aktualisierg des Schutzniveaus*
					W8	W9	W7	W8	W3	W4	W3	W3	*Schutzniveau (Schätzung)*
					vor allem Piercing-Risiko, löst Risiken des Web-Servers aus!	gehärtet und über FW abgeschottet	Zugriff auf Kundendaten über URL-Manipulationen o.ä.	nur eine Firewall, also gleiche Exposition, löst alle inneren Risiken aus	über SQL vom Web-Server aus zugänglich!	nur von innen zugänglich, wird aber gepflegt	installiert + gehärtet (externe Angriffe via Mail oder Web)	Admin-WS sind normale Arbeitsplätze	*Begründung*
Werte			j										
Image des Unternehmens		großes Risiko	d	*C* per Definition	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	
Kundendaten (Vertraulichkeit)		großes Risiko	d	*C* per Definition	(löst Web-Server-Risiken aus)	x	x	(löst innere Risiken aus)	x		x	x	
Kundendaten (Verlust+Manipulation)		mittleres Risiko	d	*D* schwere Betriebsstörung	(löst Web-Server-Risiken aus)	x	x	(löst innere Risiken aus)	x		x	x	
Geschäftsdaten (Vertraulichkeit)		extremes Risiko	d	*B* mind. Image-Schaden, wahrscheinl. geschwächte Verhandlungspositionen				(löst innere Risiken aus)		x	x	x	
Geschäftsdaten (Verlust+Manipulation)		mittleres Risiko	d	*D* schwere Betriebsstörung				(löst innere Risiken aus)		x	x	x	
Unterstützende Daten- + Funktionsbestände		kleines Risiko	d	*E* kleine Betriebsstörung				(löst innere Risiken aus)		x		x	
Betriebsgeheimnisse (Vertraulichkeit)		extremes Risiko	d	*B* Verlust von Kunden und Verhandlungspositionen				(löst innere Risiken aus)		x	x	x	
I+K-Ressourcen (Verfügbarkeit)		mittleres Risiko	d	*D* schwere Betriebsstörung	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)		x		x	
Produktivität		kleines Risiko	d	*E* Ausfallzeiten/Hemmnisse in der Produktion				(löst innere Risiken aus)		x	x	x	
Mitarbeiter (Vertraulichkeit der Mitarbeiterdaten)		großes Risiko	d	*C* schwere BDSG-Verletzung, Verlust von Kernmitarbeitern				(löst innere Risiken aus)		x		x	
Prozeßwirkungen			j										
			j										
Wertschöpfende Proz.													
Internet-Portal		großes Risiko	d	*C* Image-Schaden, Verlust von Kunden, schwerste Produktionsausfälle	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)	x		x	x	
			j										
Rechtswirksame Proz.													
Leistungszusagen über das Internet-Portal		extremes Risiko	d	*B* Gewinnausfälle	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)				x	
			j										
Sonstige Prozeßwirkg.													
Mißbrauch der I+K als Angriffsvehikel		großes Risiko	d	*C* Risiko einer Verurteilung wegen ungenügender Absicherung	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)				x	
			j										
Rechtl.+Vertragl. Risiko													
Bundesdatenschutzgesetz		kleines Risiko	e	*D* Strafgelder ...			dürfte Sicherungspflichten verletzen						
Haftungspflichten		extremes Risiko	d	*B* Verurteilungen, Schadensersatz-forderungen	(löst Web-Server-Risiken aus)	möglicherweise	ziemlich sicher	(löst innere Risiken aus)				?	
...		kein Risiko	j	*F* zahlreiche weitere rechtl. + vertragl. Risikopotentiale									

Geschätzte Angriffe/Jahr der jeweiligen Tätertypen

Risikobewertungstableaux *Szenario Muster*

Das Risiko-Tableaux stellt Management- und IT-technische Perspektive gegenüber und in Beziehung.

Technische Komponenten werden nach ihrem jeweiligen Schutzniveau und dem Expositionsgrad gegenüber den Angreifertypen klassifiziert, die geschäftlichen nach ihrer Schadensklasse.

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden.

Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und geschäftlichen Bedrohungen her.

Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftlichen Einzelrisiken sowie Gesamtrisiken.

Managementperspektive

Gesamtlage

Vorsorge 3.618 | Oops

1.883.000 € | extremes Risiko

Technische Perspektive

Gesamtlage

Vorsorge 902.200 € | Oops 3.618

extremes Risiko

Planungszeitpunkt 09.04.03

Risikoinventar	Ind.	Klasse	Risikoaggregation	W'keit Aggregation	*Schadensklasse* *Begründung*	Äußere Firewall	Web-Server in der DMZ (Web-Portal)	Schwachstellen in der Applikationslogik	Innere Firewall	DB-Server mit Kunden- und Vertragsdaten für Web-Portal	Interne Server mit kritischen Geschäftsprozessen	interne Arbeitsplätze	Admin-Arbeitsplätze	Bedrohungen
						kleines Risiko	minimales Risiko	großes Risiko	kleines Risiko	minimales Risiko	großes Risiko	extremes Risiko	extremes Risiko	Akzeptanz-Indikator
						kleines Risiko	minimales Risiko	großes Risiko	kleines Risiko	minimales Risiko	großes Risiko	extremes Risiko	extremes Risiko	Risiko-Aggregation
						B	B	B	B	B	B	B	B	Schadensaggregation
						g	h	e	g	h	e	d	d	Häufigkeitsaggregation
						W8	W9	W6	W8	W3	W3	W3	W3	Wirksames Schutzniveau
						0,10000	0,10000	0,10000	0,10000	0,00000	0,30000	0,50000	0,01000	Innentäter
						1,00000	1,00000	1,00000	1,00000	0,00000	0,01000	0,01000	0,00500	Externe Profis
						1,00000	1,00000	1,00000	1,00000	0,00000	0,00100	0,00100	0,00010	Cyber-Terroristen
						500,00000	500,00000	500,00000	500,00000	0,00005		10,00000	10,00000	klass. Hacker
						60.000,00000	60.000,00000	60.000,00000	60.000,00000	0,00557		900,00000	900,00000	Cyber-Punks
						01.01.03	01.01.03	01.04.02	01.01.03	11.11.99	09.10.02	01.04.00	01.04.00	Letzte Aktualisierg des Schutzniveaus
						W8	W9	W7	W8	W3	W4	W3	W3	Schutzniveau (Schätzung)
						vor allem Piercing-Risiko, löst Risiken des Web-Servers aus!	gehärtet und über FW abgeschottet	Zugriff auf Kundendaten über URL-Manipulationen o.ä.	nur eine Firewall, also gleiche Exposition, löst alle inneren Risiken aus	über SQL vom Web-Server aus zugänglich!	nur von innen zugänglich, wird aber gepflegt	installiert + gehärtet (externe Angriffe via Mail oder Web)	Admin-WS sind normale Arbeitsplätze	Begründung
Werte				j										
Image des Unternehmens		großes Risiko		d	C per Definition	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	prakt. jede Sicherheitspanne schädigt den Ruf	
Kundendaten (Vertraulichkeit)		großes Risiko		d	C per Definition	(löst Web-Server-Risiken aus)	x	x	(löst innere Risiken aus)	x		x	x	
Kundendaten (Verlust+Manipulation)		mittleres Risiko		d	D schwere Betriebsstörung	(löst Web-Server-Risiken aus)	x	x	(löst innere Risiken aus)	x		x	x	
Geschäftsdaten (Vertraulichkeit)		extremes Risiko		d	B mind. Image-Schaden, wahrscheinl. geschwächte Verhandlungspositionen				(löst innere Risiken aus)		x	x	x	
Geschäftsdaten (Verlust+Manipulation)		mittleres Risiko		d	D schwere Betriebsstörung				(löst innere Risiken aus)		x	x	x	
Unterstützende Daten- + Funktionsbestände		kleines Risiko		d	E kleine Betriebsstörung				(löst innere Risiken aus)		x		x	
Betriebsgeheimnisse (Vertraulichkeit)		extremes Risiko		d	B Verlust von Kunden und Verhandlungspositionen				(löst innere Risiken aus)		x	x	x	
I+K-Ressourcen (Verfügbarkeit)		mittleres Risiko		d	D schwere Betriebsstörung	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)		x		x	
Produktivität		kleines Risiko		d	E Ausfallzeiten/Hemmnisse in der Produktion				(löst innere Risiken aus)		x	x	x	
Mitarbeiter (Vertraulichkeit der Mitarbeiterdaten)		großes Risiko		d	C schwere BDSG-Verletzung, Verlust von Kernmitarbeitern				(löst innere Risiken aus)		x		x	
Prozeßwirkungen				j										
				j										
Wertschöpfende Proz.														
Internet-Portal		großes Risiko		d	C Image-Schaden, Verlust von Kunden, schwerste Produktionsausfälle	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)	x		x	x	
				j										
Rechtswirksame Proz.														
Leistungszusagen über das Internet-Portal		extremes Risiko		d	B Gewinnausfälle	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)				x	
				j										
Sonstige Prozeßwirkg.														
Mißbrauch der I+K als Angriffsvehikel		großes Risiko		d	C Risiko einer Verurteilung wegen ungenügender Absicherung	(löst Web-Server-Risiken aus)	x		(löst innere Risiken aus)				x	
				j										
Rechtl.+Vertragl. Risiko														
Bundesdatenschutzgesetz		kleines Risiko		e	D Strafgelder ...			dürfte Sicherungspflichten verletzen						
Haftungspflichten		extremes Risiko		d	B Verurteilungen, Schadensersatz-forderungen	(löst Web-Server-Risiken aus)	möglicherweise	ziemlich sicher	(löst innere Risiken aus)				?	
...		kein Risiko		j	F zahlreiche weitere rechtl. + vertragl. Risikopotentiale									

Geschätzte Angriffe/Jahr der jeweiligen Tätertypen

Risikobewertungstableaux *Szenario RZ an beiden Standorten*

Das RZ wird auf beide Standorte verteilt, die Stand-Bys stehen also an verschiedenen Standorten. Die Standorte werden über eine Laser-Richtstrecke vernetzt. Telefonie per VoIP.

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden.
Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und geschäftlichen Bedrohungen her.
Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftlichen Einzelrisiken sowie Gesamtrisiken.

Technische Perspektive

Managementperspektive

Gesamtlage	Oops	Vorsorge
	0	100 €
	minimales Risiko	

Gesamtlage	Oops	Vor-sorge
	0	200 €
	minimales Risiko	

Risikoinventar	Risikoaggregation Ind.	Klasse	W'keit Aggregation	Schadensklasse Begründung	Hochwasser vernichtet Server und Datensicher-ungsmedien	Hochwasser vernichtet nur Server, Datensicherg wird gerettet	Feuer,Lösch-wasser oder Kontaminatio n vernichten Server und Datensicherg	Feuer,Lösch-wasser oder Kontaminatio n vernichten nur Server	Erdbeben führt zu Gebäude-einsturz	zerstörg (t>USV)	dauerhafter Kommunikat-ionsausfall durch Leitungs-zerstörg
Bedrohungen											
Akzeptanz-Indikator					kein Risiko	kein Risiko	unvermeidl. Restrisiko	kein Risiko	minimales Risiko	kein Risiko	minimales Risiko
Risiko-Aggregation					B	C	B	C	B	C	B
Schadensaggregation					j	j	i	i	h	i	h
Häufigkeitsklasse (Schätzung)					ausgeschlossen	ausgeschlossen	Bänder lagen nicht im Safe	Produktion ist brandgefährdeter	eigentl. kein Erdbebengebiet	zB Sturm zerlegt Oberleitgsring	zB Bagger zerreißt Kabel
Begründung											
Werte			j								
Image des Unternehmens		unvermeidl. Restrisiko	h	C per Definition			offensichtliche Schlamperei				nicht erreichbar
Kundendaten (Vertraulichkeit)		kein Risiko	j	C per Definition							
Kundendaten (Verlust+Manipulation)		kein Risiko	h	D schwere Betriebsstörung	x		x		x		x
Geschäftsdaten (Vertraulichkeit)		kein Risiko	j	B mind. Image-Schaden, wahrscheinl. geschwächte Verhandlungspositionen							
Geschäftsdaten (Verlust+Manipulation)		kein Risiko	h	D schwere Betriebsstörung	x		x		x		x
Unterstützende Daten- + Funktionsbestände		kein Risiko	h	E kleine Betriebsstörung	x		x		x	vorübergehend	x
Betriebsgeheimnisse (Vertraulichkeit)		kein Risiko	j	B Verlust von Kunden und Verhandlungspositionen							
I+K-Ressourcen (Verfügbarkeit)		kein Risiko	h	D schwere Betriebsstörung	x	x	x	x	x	x	x
Produktivität		kein Risiko	h	E Ausfallzeiten/Hemmnisse in der Produktion	x	x	x	x	x	x	
Mitarbeiter (Vertraulichkeit der Mitarbeiterdaten)		kein Risiko	j	C schwere BDSG-Verletzung, Verlust von Kernmitarbeitern							
			j								
Prozeßwirkungen											
			j								
Wertschöpfende Proz.											
Internet-Portal		unvermeidl. Restrisiko	h	C Image-Schaden, Verlust von Kunden, schwerste Produktionsausfälle	x	x	x	x	x	x	x
			j								
Rechtswirksame Proz.											
Leistungszusagen über das Internet-Portal		kein Risiko	j	B Gewinnausfälle							
			j								
Sonstige Prozeßwirkg.											
Mißbrauch der I+K als Angriffsvehikel		kein Risiko	j	C Risiko einer Verurteilung wegen ungenügender Absicherung							
			j								
Rechtl.+Vertragl. Risiko											
Bundesdatenschutzgesetz		kein Risiko	j	D Strafgelder ...							
Haftungspflichten		minimales Risiko	h	B Verurteilungen, Schadensersatz-forderungen	gegenüber Aktieninhabern?		gegenüber Aktieninhabern?		gegenüber Aktieninhabern?		
...		kein Risiko	j	F zahlreiche weitere rechtl. + vertragl. Risikopotentiale							

Risikobewertungstableaux

Szenario RZ in Outsourcing

RZ-Outsourcing mit entsprechenden SLAs..

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden.
Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und geschäftlichen Bedrohungen her.
Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftlichen Einzelrisiken sowie Gesamtrisiken.

Managementperspektive

Gesamtlage

Vorsorge 174.100 € | Oops 119

großes Risiko

Technische Perspektive

Gesamtlage

Vorsorge 410.100 € | Oops 119

extremes Risiko

Risikoinventar	Risikoaggregation Ind.	Klasse	W'keit Aggregation	Schadensklasse / Begründung	Hochwasser vernichtet Server und Datensicherungsmedien	Hochwasser vernichtet nur Server, Datensicherung wird gerettet	Feuer,Löschwasser oder Kontamination vernichten Server und Datensicherung	Feuer,Löschwasser oder Kontamination vernichten nur Server	Erdbeben führt zu Gebäudeeinsturz	zusätzliche Datenspionage + -sabotage-Risiken	dauerhafter Stromausfall durch Leitungszerstörung (t>USV)	dauerhafter Kommunikationsausfall durch Leitungszerstörung
Bedrohungen												
Akzeptanz-Indikator					kein Risiko	kein Risiko	unvermeidl. Restrisiko	kein Risiko	minimales Risiko	mittleres Risiko	kein Risiko	extremes Risiko
Risiko-Aggregation												
Schadensaggregation					B	C	B	C	B	B	C	B
Häufigkeitsklasse (Schätzung)					*j*	*j*	*i*	*i*	*h*	*f*	*i*	*d*
Begründung					ausgeschlossen	ausgeschlossen	per SLA ausgeschlossen (bzw. Haftung)	per SLA ausgeschlossen (bzw. Haftung)	eigentl. kein Erdbebengebiet	eigentl. kein Erdbebengebiet	per SLA ausgeschlossen (bzw. Haftung)	unser Kommunikationsproblem besteht!
Werte			j									
Image des Unternehmens		großes Risiko	d	*C* per Definition			offensichtliche Schlamperei			ist ungerecht, ttrifft uns aber trotzdem		nicht erreichbar
Kundendaten (Vertraulichkeit)		kleines Risiko	f	*C* per Definition						x		
Kundendaten (Verlust+Manipulation)		mittleres Risiko	d	*D* schwere Betriebsstörung	x		x		x	x		x
Geschäftsdaten (Vertraulichkeit)		mittleres Risiko	f	*B* mind. Image-Schaden, wahrscheinl. geschwächte Verhandlungspositionen						x		
Geschäftsdaten (Verlust+Manipulation)		mittleres Risiko	d	*D* schwere Betriebsstörung	x		x		x	x		x
Unterstützende Daten- + Funktionsbestände		kleines Risiko	d	*E* kleine Betriebsstörung	x		x		x	x	vorübergehend	x
Betriebsgeheimnisse (Vertraulichkeit)		mittleres Risiko	f	*B* Verlust von Kunden und Verhandlungspositionen						x		
I+K-Ressourcen (Verfügbarkeit)		mittleres Risiko	d	*D* schwere Betriebsstörung	x	x	x	x	x	x	x	x
Produktivität		kein Risiko	f	*E* Ausfallzeiten/Hemmnisse in der Produktion	x	x	x	x	x	x	x	
Mitarbeiter (Vertraulichkeit der Mitarbeiterdaten)		kleines Risiko	f	*C* schwere BDSG-Verletzung, Verlust von Kernmitarbeitern						x		
Prozeßwirkungen			j									
			j									
Wertschöpfende Proz.												
Internet-Portal		großes Risiko	d	*C* Image-Schaden, Verlust von Kunden, schwerste Produktionsausfälle	x	x	x	x	x	x	x	x
			j									
Rechtswirksame Proz.												
Leistungszusagen über das Internet-Portal		mittleres Risiko	f	*B* Gewinnausfälle						x		
			j									
Sonstige Prozeßwirkg.												
Mißbrauch der I+K als Angriffsvehikel		kleines Risiko	f	*C* Risiko einer Verurteilung wegen ungenügender Absicherung						x		
			j									
Rechtl.+Vertragl. Risiko												
Bundesdatenschutzgesetz		minimales Risiko	f	*D* Strafgelder ...						x		
Haftungspflichten		mittleres Risiko	f	*B* Verurteilungen, Schadensersatz-forderungen	gegenüber Aktieninhabern?		gegenüber Aktieninhabern?		gegenüber Aktieninhabern?	gegenüber Aktieninhabern?		
...		kein Risiko	j	*F* zahlreiche weitere rechtl. + vertragl. Risikopotentiale								

Risikobewertungstableaux

Szenario *RZ in Produktionsgebäude auf dem Berg umziehen*

Das RZ könnte in den Produktiontrakt verlegt werden. Dieser liegt deutlich hangaufwärts.

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden.
Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und geschäftlichen Bedrohungen her.
Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftlichen Einzelrisiken sowie Gesamtrisiken.

Managementperspektive

Gesamtlage

Vorsorge	Oops
182.000 €	196
	großes Risiko

Technische Perspektive

Gesamtlage

Vorsorge	510.100 €
Oops	196
	extremes Risiko

Bedrohungen	Hochwasser vernichtet Server und Datensicher-ungsmedien	Hochwasser vernichtet nur Server, Datensicherg wird gerettet	Feuer,Lösch-wasser oder Kontaminatio n vernichten Server und Datensicherg	Feuer,Lösch-wasser oder Kontaminatio n vernichten nur Server	Erdbeben führt zu Gebäude-einsturz	dauerhafter Stromausfall durch Leitungs-zerstörg (t>USV)	dauerhafter Kommunikat-ionsausfall durch Leitungs-zerstörg
Akzeptanz-Indikator	**kein Risiko**	**kein Risiko**	**großes Risiko**	**großes Risiko**	**minimales Risiko**	**mittleres Risiko**	**extremes Risiko**
Risiko-Aggregation	B	C	B	C	B	C	B
Schadensaggregation	*j*	*j*	*e*	*d*	*h*	*e*	*d*
Häufigkeitsklasse (Schätzung)	ausgeschlossen	ausgeschlossen	Bänder lagen nicht im Safe	Produktion ist brandgefährdeter	eigentl. kein Erdbebengebiet	zB Sturm zerlegt Oberleitgsring	zB Bagger zerreißt Kabel
Begründung							

Risikoinventar	Risikoaggregation Ind.	Klasse	W'keit Aggregation	*Schadensklasse* *Begründung*								
Werte			j									
Image des Unternehmens		**großes Risiko**	d	*C* per Definition			offensichtliche Schlamperei				nicht erreichbar	
Kundendaten (Vertraulichkeit)		**kein Risiko**	j	*C* per Definition								
Kundendaten (Verlust+Manipulation)		**mittleres Risiko**	d	*D* schwere Betriebsstörung	x		x		x		x	
Geschäftsdaten (Vertraulichkeit)		**kein Risiko**	j	*B* mind. Image-Schaden, wahrscheinl. geschwächte Verhandlungspositionen								
Geschäftsdaten (Verlust+Manipulation)		**mittleres Risiko**	d	*D* schwere Betriebsstörung	x		x		x		x	
Unterstützende Daten- + Funktionsbestände		**kleines Risiko**	d	*E* kleine Betriebsstörung	x		x		x	vorübergehend	x	
Betriebsgeheimnisse (Vertraulichkeit)		**kein Risiko**	j	*B* Verlust von Kunden und Verhandlungspositionen								
I+K-Ressourcen (Verfügbarkeit)		**mittleres Risiko**	d	*D* schwere Betriebsstörung	x	x	x	x	x	x	x	
Produktivität		**kleines Risiko**	d	*E* Ausfallzeiten/Hemmnisse in der Produktion	x	x	x	x	x	x		
Mitarbeiter (Vertraulichkeit der Mitarbeiterdaten)		**kein Risiko**	j	*C* schwere BDSG-Verletzung, Verlust von Kernmitarbeitern								
Prozeßwirkungen			j									
Wertschöpfende Proz.			j									
Internet-Portal		**großes Risiko**	d	*C* Image-Schaden, Verlust von Kunden, schwerste Produktionsausfälle	x	x	x	x	x	x	x	
Rechtswirksame Proz.			j									
Leistungszusagen über das Internet-Portal		**kein Risiko**	j	*B* Gewinnausfälle								
Sonstige Prozeßwirkg.			j									
Mißbrauch der I+K als Angriffsvehikel		**kein Risiko**	j	*C* Risiko einer Verurteilung wegen ungenügender Absicherung								
Rechtl.+Vertragl. Risiko			j									
Bundesdatenschutzgesetz		**kein Risiko**	j	*D* Strafgelder ...								
Haftungspflichten		**großes Risiko**	e	*B* Verurteilungen, Schadensersatz-forderungen	gegenüber Aktieninhabern?		gegenüber Aktieninhabern?		gegenüber Aktieninhabern?			
...		**kein Risiko**	j	*F* zahlreiche weitere rechtl. + vertragl. Risikopotentiale								

Risikobewertungstableaux *Szenario Altes RZ im Verwaltungsgebäude*

Das RZ liegt im Keller des Verwaltungsgebäude, hinter dem Hochwasserdech, also hochwassergefährdet.Was tun?

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden.
Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und geschäftlichen Bedrohungen her.
Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftlichen Einzelrisiken sowie Gesamtrisiken.

Managementperspektive

Gesamtlage

Vorsorge	Oops
141.100 €	125
	großes Risiko

Technische Perspektive

Gesamtlage

Vorsorge	432.100 €
Oops	125
	extremes Risiko

Risikoinventar	Risikoaggregation Ind.	Klasse	W'keit Aggregation	*Schadensklasse* *Begründung*	Hochwasser vernichtet Server und Datensicher-ungsmedien	Hochwasser vernichtet nur Server, Datensicherg wird gerettet	Feuer (und Löschwasser) vernichten Server und Datensicherg	Feuer (und Löschwasser) vernichten nur Server	Erdbeben führt zu Gebäude-einsturz	dauerhafter Stromausfall durch Leitungs-zerstörg (t>USV)	dauerhafter Kommunikat-ionsausfall durch Leitungs-zerstörg	Bedrohungen Akzeptanz-Indikator
					kleines Risiko	**kleines Risiko**	**mittleres Risiko**	**mittleres Risiko**	**minimales Risiko**	**mittleres Risiko**	**extremes Risiko**	Risiko-Aggregation
					B	C	B	C	B	C	B	Schadensaggregation
					g	*f*	*f*	*e*	*h*	*e*	*d*	*Häufigkeitsklasse (Schätzung)*
					Jahrhunder-HW + unglückl. Umstände	Jahrhunderthoch-wasser	Bänder lagen nicht im Safe	Bänder sollen in Safe liegen	eigentl. kein Erdbebengebiet	zB Sturm zerlegt Oberleitgsring	zB Bagger zerreißt Kabel	*Begründung*
Werte												
Image des Unternehmens		**großes Risiko**	d	*C* per Definition			offensichtliche Schlamperei				nicht erreichbar	
Kundendaten (Vertraulichkeit)		**kein Risiko**	j	*C* per Definition								
Kundendaten (Verlust+Manipulation)		**mittleres Risiko**	d	*D* schwere Betriebsstörung	x		x		x		x	
Geschäftsdaten (Vertraulichkeit)		**kein Risiko**	j	*B* mind. Image-Schaden, wahrscheinl. geschwächte Verhandlungspositionen								
Geschäftsdaten (Verlust+Manipulation)		**mittleres Risiko**	d	*D* schwere Betriebsstörung	x		x		x		x	
Unterstützende Daten- + Funktionsbestände		**kleines Risiko**	d	*E* kleine Betriebsstörung	x		x		x	vorübergehend	x	
Betriebsgeheimnisse (Vertraulichkeit)		**kein Risiko**	j	*B* Verlust von Kunden und Verhandlungspositionen								
I+K-Ressourcen (Verfügbarkeit)		**mittleres Risiko**	d	*D* schwere Betriebsstörung	x	x	x	x	x	x	x	
Produktivität		**minimales Risiko**	e	*E* Ausfallzeiten/Hemmnisse in der Produktion	x	x	x	x	x	x		
Mitarbeiter (Vertraulichkeit der Mitarbeiterdaten)		**kein Risiko**	j	*C* schwere BDSG-Verletzung, Verlust von Kernmitarbeitern								
Prozeßwirkungen			j									
Wertschöpfende Proz.			j									
Internet-Portal		**großes Risiko**	d	*C* Image-Schaden, Verlust von Kunden, schwerste Produktionsausfälle	x	x	x	x	x	x	x	
Rechtswirksame Proz.			j									
Leistungszusagen über das Internet-Portal		**kein Risiko**	j	*B* Gewinnausfälle								
Sonstige Prozeßwirkg.			j									
Mißbrauch der I+K als Angriffsvehikel		**kein Risiko**	j	*C* Risiko einer Verurteilung wegen ungenügender Absicherung								
Rechtl.+Vertragl. Risiko			j									
Bundesdatenschutzgesetz		**kein Risiko**	j	*D* Strafgelder ...								
Haftungspflichten		**mittleres Risiko**	f	*B* Verurteilungen, Schadensersatz-forderungen	gegenüber Aktieninhabern?		gegenüber Aktieninhabern?		gegenüber Aktieninhabern?			
...		**kein Risiko**	j	*F* zahlreiche weitere rechtl. + vertragl. Risikopotentiale								

Risikobewertungstableaux *Szenario Muster*

Das Risiko-Tableaux stellt Management- und IT-technische Perspektive gegenüber und in Beziehung.

Die technischen Bedrohungen müssen nach ihrer jeweiligen Eintrittswahrscheinlichkeit klassifiziert werden, die geschäftlichen nach ihrer Schadensklasse.

Die Eingabefelder sind blau hervorgehoben. Es sollte jeweils ein Grund für die Entscheidung angegeben werden.

Beliebige Texteinträge (z.B. Entscheidungsgründe) stellen die Verbindung zwischen technischen und geschäftlichen Bedrohungen her.

Die Kalkulationslogik berechnet auf Grundlage der Eingaben die kumulierten technischen und geschäftlichen Einzelrisiken sowie Gesamtrisiken.

Managementperspektive

Gesamtlage

	Oops
Vorsorge	125
141.100 €	großes Risiko

Technische Perspektive

Gesamtlage

Vor-sorge	432.100 €
Oops	125
	extremes Risiko

Risikoinventar	Risikoaggregation Ind.	Klasse	W'keit Aggregation	*Schadensklasse* *Begründung*	Hochwasser vernichtet Server und Datensicher-ungsmedien	Hochwasser vernichtet nur Server, Datensicherg wird gerettet	Feuer (und Löschwasser) vernichten Server und Datensicherg	Feuer (und Löschwasser) vernichten nur Server	Erdbeben führt zu Gebäude-einsturz	dauerhafter Stromausfall durch Leitungs-zerstörg (t>USV)	dauerhafter Kommunikat-ionsausfall durch Leitungs-zerstörg	Bedrohungen Akzeptanz-Indikator
					kleines Risiko	kleines Risiko	mittleres Risiko	mittleres Risiko	minimales Risiko	mittleres Risiko	extremes Risiko	Risiko-Aggregation
					B	C	B	C	B	C	B	Schadensaggregation
					g	*f*	*f*	*e*	*h*	*e*	*d*	*Häufigkeitsklasse (Schätzung)*
					Jahrhunder-HW + unglückl. Umstände	Jahrhunderthoch-wasser	Bänder lagen nicht im Safe	Bänder sollen in Safe liegen	eigentl. kein Erdbebengebiet	zB Sturm zerlegt Oberleitgsring	zB Bagger zerreißt Kabel	*Begründung*
Werte												
Image des Unternehmens		großes Risiko	d	*C* per Definition			offensichtliche Schlamperei				nicht erreichbar	
Kundendaten (Vertraulichkeit)		kein Risiko	j	*C* per Definition								
Kundendaten (Verlust+Manipulation)		mittleres Risiko	d	*D* schwere Betriebsstörung	x		x		x		x	
Geschäftsdaten (Vertraulichkeit)		kein Risiko	j	*B* mind. Image-Schaden, wahrscheinl. geschwächte Verhandlungspositionen								
Geschäftsdaten (Verlust+Manipulation)		mittleres Risiko	d	*D* schwere Betriebsstörung	x		x		x		x	
Unterstützende Daten- + Funktionsbestände		kleines Risiko	d	*E* kleine Betriebsstörung	x		x		x	vorübergehend	x	
Betriebsgeheimnisse (Vertraulichkeit)		kein Risiko	j	*B* Verlust von Kunden und Verhandlungspositionen								
I+K-Ressourcen (Verfügbarkeit)		mittleres Risiko	d	*D* schwere Betriebsstörung	x	x	x	x	x	x	x	
Produktivität		minimales Risiko	e	*E* Ausfallzeiten/Hemmnisse in der Produktion	x	x	x	x	x	x		
Mitarbeiter (Vertraulichkeit der Mitarbeiterdaten)		kein Risiko	j	*C* schwere BDSG-Verletzung, Verlust von Kernmitarbeitern								
			j									
Prozeßwirkungen												
			j									
Wertschöpfende Proz.												
Internet-Portal		großes Risiko	d	*C* Image-Schaden, Verlust von Kunden, schwerste Produktionsausfälle	x	x	x	x	x	x	x	
			j									
Rechtswirksame Proz.												
Leistungszusagen über das Internet-Portal		kein Risiko	j	*B* Gewinnausfälle								
			j									
Sonstige Prozeßwirkg.												
Mißbrauch der I+K als Angriffsvehikel		kein Risiko	j	*C* Risiko einer Verurteilung wegen ungenügender Absicherung								
			j									
Rechtl.+Vertragl. Risiko												
Bundesdatenschutzgesetz		kein Risiko	j	*D* Strafgelder ...								
Haftungspflichten		mittleres Risiko	f	*B* Verurteilungen, Schadensersatz-forderungen	gegenüber Aktieninhabern?		gegenüber Aktieninhabern?		gegenüber Aktieninhabern?			
...		kein Risiko	j	*F* zahlreiche weitere rechtl. + vertragl. Risikopotentiale								

Risikoklassen

R1	R2	R3	R4	R5	R6	R7	R8	*Klasse*
irrationales Risiko	**extremes Risiko**	**großes Risiko**	**mittleres Risiko**	**kleines Risiko**	**minimales Risiko**	**unvermeidl. Restrisiko**	**kein Risiko**	*Umschreibung*
inakzeptabel	inakzeptabel	inakzeptabel	übergangsweise (Genehmigung!)	notfalls akzeptabel (Genehmigung!)	akzeptabel	akzeptabel	akzeptabel	*Akzeptabilität (Genehmigung CSO nötig?)*
5.000.000,00 €	400.000,00 €	50.000,00 €	10.000,00 €	1.000,00 €	100,00 €	0,00 €	0,00 €	*Risiko-Vorsorge in €*
inakzeptabel	inakzeptabel	inakzeptabel	CSO-Genehmigg.	CSO-Genehmigg.	akzeptabel	akzeptabel	akzeptabel	*Policy-Indikator*

Schadensklassen für Schadensereignisse

A	B	C	D	E	F	*Klasse*	
katastrophal	großer Schaden	mittlerer Schaden	kleiner Schaden	unbedeutend	vernachlässigbar	*Umschreibung*	
30.000.000,00 €	10.000.000,00 €	1.000.000,00 €	100.000,00 €	10.000,00 €	10,00 €		*- finanzieller Schaden in €*
z.B. Verlust von Großkunden	z.B. Gewinnausfall, Strateg. Planung	z.B. Image-Schädigung	z.B.Betriebsstörg. Verärgerung von Kunden	z.B. kleinere Produktions-störungen		*Kriterien der Schadens-kategorien*	*- Schädigung eigener Interessen*
	z.B. Verurteilung wegen grober Fahrlässigkeit	z.B. Verurteilung wegen einfacher Fahrlässigkeit					*- Pflicht-verletzungen*
	z.B. Verrat von Geheimnissen der Vertragspartner	z.B. massive Datenschutz-verletzungen	z.B. vereinzelte Datenschutz-verletzungen				*- Schädigung Dritter*
1.000.000,00	50.000,00	20.000,00	100,00	10,00	1,00	*in **Peanuts**-Einheiten*	
660.000,00	33.000,00	13.200,00	66,00	6,60	-1,00	*Schwellwerte*	

Häufigkeitsklassen für Schadensereignisse

a	b	c	d	e	f	g	h	i	j	*Klasse*
unvermeidbar	äußerst häufig	sehr häufig	häufig	selten	sehr selten	äußerst selten	eher unmöglich	praktisch unmöglich	absolut unmögliches Ereignis	*Umschreibung*
tritt sicher ein	alle paar Tage	monatlich	jährlich	> 10 Jahre	> 100 Jahre	> 1000 Jahre	nach Experten-meinung	nach allgemeiner Expertenmeinung		*Kriterien der Häufigkeits-kategorien*
1,00E+000	2,00E-001	3,00E-002	2,74E-003	2,74E-004	2,74E-005	2,74E-006	1,00E-009	1,00E-010		*Wahrscheinlichkeit (1/Tag)*
6,60E-001	1,32E-001	1,98E-002	1,81E-003	1,81E-004	1,81E-005	1,81E-006	6,60E-010		-1,00E+000	*Schwellwerte*

Widerstand-Klassifikation-Matrix

Die Widerstandswert-Matrix definiert die Wahrscheinlichkeit, mit der ein bestimmtes Schutzniveau von einem bestimmten Angreifertyp überwunden werden kann.

Schutzniveau		Angreifertyp						
		A1 Innentäter	A2 Externe Profis	A3 Cyber-Terroristen	A4 klass. Hacker	A5 Cyber-Punks	*Klasse Benennung*	
		von innen, weitreichende Zugangsrechte	koordiniert von innen und außen	eher von außen	eher von außen	von außen	*Kriterien der Angriffs-kategorien*	*- Angriffs-position*
		eher wenig Aufwand und Ausrüstung	großes Budget, erstklassige Ausrüstung	erheblicher Aufwand und gute Ausrüstung	eher geringer Aufwand bei guter Ausrüstung	gering: vorhandene Angriffswerkzeuge		*- Ressourcen*
		technisch oder fachlich sehr gute Detailkenntnisse	technisch und fachlich sehr gut	technisch gut bis sehr gut	technisch gut bis sehr gut	technisch gering		*- Qualifikation*
Klasse	*Bezeichnung* / *Lebensdauer (in Tagen)*	Vorteil, Sabotage, risikobewußt, evtl. irrational	Spionage, evtl. Sabotage, rational + risikobewußt	Sabotage/Publicity irrational, risikobereit	eher risikoscheu und rational	eher irrational, nicht risikobewußt "Fame+Fun"		*- Angriffs-motivation*
W1	ungesichert 300000	unvermeidbar	unvermeidbar	unvermeidbar	unvermeidbar	äußerst häufig		
W2	Lieferzustand 300000	unvermeidbar	unvermeidbar	unvermeidbar	unvermeidbar	sehr häufig		
W3	einmalig gehärtet 300000	äußerst häufig	unvermeidbar	sehr häufig	sehr häufig	häufig		
W4	regelmäßig gehärtet 180	häufig	äußerst häufig	häufig	häufig	selten		
W5	Grundschutz 90	selten	sehr häufig	selten	selten	sehr selten		
W6	hochsicher 180	sehr selten	häufig	selten	sehr selten	äußerst selten		
W7	Reviewed 360	äußerst selten	häufig	sehr selten	sehr selten	eher unmöglich		
W8	State of the Art 180	äußerst selten	selten	äußerst selten	äußerst selten	praktisch unmöglich		
W9	Redundant State-o/t-Art 360	eher unmöglich	sehr selten	eher unmöglich	eher unmöglich	praktisch unmöglich		