Risikokommunikation in einer IT Schadenslage

Nikolaus Wlczek

IABG mbH
wlczek@iabg.de

Zusammenfassung

In kaum einer anderen Krisensituation ist die Wissenslücke (Knowledge Gap) zwischen der strategischen Managementebene und der operativen/taktischen (ausführenden) Ebene größer als bei IT Krisen- und Schadenslagen. Beispielhaft sei hier nur der Vergleich eines Hochwassers mit einer IT Krise aufgeführt: Bei einem Hochwasser auf der einen Seite ist dem Entscheider auf jeder Ebene (operativ, taktisch, strategisch) die Bedeutung des Sachverhalts eines Scheitelpunkts der Flut, die 0,3m über dem Deich liegt, offensichtlich. Auf der anderen Seite ist nicht jedem sofort verständlich, was ein Heartbleed Bug darstellt, der es dem versierten Angreifer ermöglicht, eine Lücke im OpenSLL Protokoll zur Ausspähung von Passwort Daten zu nutzen und vor allem welche inhärenten Sicherheitsrisiken in dieser Tatsache für die Unternehmung/die Behörde liegen. Dazu kann über alle Entscheidungsebenen der spezifische IT Wortschatz, die Nomenklatur, nicht in Kürze erlernt werden. Dieser Artikel beschreibt Risikokommunikation generell, stellt ihre Funktionen dar und beschreibt mögliche Probleme. Der Nachweis für Handlungsbedarf wird in diesem Artikel über die Methode der Informationsklassen abgeleitet, welche vorgestellt und in ihrer Anwendung beschrieben werden. Des Weiteren werden Forderungen für Cyber-Security-Personal abgeleitet und allgemein, sowie aus Human-Factors-Sicht dargestellt.

1 Generelles

Risikokommunikation erfasst als Grundverständnis, über alle Definition hinweg den Akt der Kommunikation über Risiken, sei es Bewertung, Management oder Identifikation. Als eine der Vielzahl von vorhandenen Definitionen, die obigen Grundsatz widerspiegeln, sei hier beispielhaft die Definition des Wirtschaftslexikons aus dem Gabler Verlag aufgeführt:

„Die Risikokommunikation hat als Managementdisziplin die Aufgabe, das Ausmaß (Risiken identifizieren und benennen) und die Relevanz der Risiken unternehmerischen Handelns zielgruppengerecht zu kommunizieren (Gefahren aufzeigen) und den angemessenen Umgang mit solchen Risiken zu unterstützen.“

Zweck und Ziel von Risikokommunikation kann jeder zielgerichtete Austausch von Informationen über Gesundheits- und Umweltrisiken zwischen Individuen und innerhalb interessierter Gruppen betrachtet werden. Die Informationen beziehen sich dabei vor allem auf:

a) die Höhe des Risikos
b) die Signifikanz oder Bedeutung des Risikos und
c) die Entscheidungen, Handlungen oder politische Maßnahmen, welche darauf abzielen, die Gefahren für Gesundheit und Umwelt zu begrenzen oder zu regeln.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 304-314.

Als interessierte Gruppen kommen politische Institutionen, Bundes- und Landesämter, einzelne Unternehmen und Unternehmensverbände, Gewerkschaften, Umweltverbände, Bürgerinitiativen, Wissenschaftler und Medien in Frage [CoSW86].

2 Risikokommunikation und Cyber Security

2.1 Funktionen der Risikokommunikation

Bei der wissenschaftlichen Diskussion wurde der Begriff der Risikokommunikation in der Literatur auf verschiedene Funktionen hin abgeleitet. Diese Funktionen werden in **Tab 1** anhand ihrer einzelnen Ziele erläutert:

Tab 1: Funktionen der Risikokommunikation

Funktion	Risikoprävention	Risikokontroverse	Risikoberatung
Ziel	Veränderung des Verhaltens einer Person oder einer Gruppe in Bezug auf das Risiko in einer bestimmten Situation.	Vorbeugen und Bewältigen von risikobezogenen Konflikten zwischen Individuen, Institutionen oder Parteien.	Unterstützen von Bedarfsträgern bei der Entscheidungsfindung in einem risikogebunden Kontext.

Dieser Artikel zeigt vornehmlich Wege auf, mittels der Anwendung von dedizierten Methoden die Risikoprävention und -beratung zu unterstützen und auszubauen. Risikokontroverse hingegen wird in diesem Artikel nicht weiter untersucht.

2.2 Zielgruppen

Die Zielgruppe für die Risikoberatung stellt die Führungsebene (Operateure) dar. Ziele einer solchen Beratung sind: Vermittlung des Risikos unter Einbeziehung von Wahrscheinlichkeiten, Informieren über Vor- und Nachteile mit Bezug zu den Folgen der Entscheidung.

Die Risikokontroverse kann als angeleitetes Für und Wider zwischen den verschiedenen Zielgruppen beschrieben werden. Dies erfolgt allerdings nur, wenn es sich bei den Zielgruppen um unterschiedliche Interessensgruppen handelt.

Die Funktion der Risikoprävention ist für alle Zielgruppen relevant und richtet sich schwerpunktmäßig auf die Risikoperzeption der jeweiligen Zielgruppe als das erste Glied in der Kette zur Generierung des Verhaltens in einer Krisensituation. Hier geht es darum, den Menschen das Risiko zu vergegenwärtigen. Ein zweiter zentraler Punkt der Risikoprävention ist die Aufklärung über effektive Schutzmaßnahmen gegen die Folgen einer risikoreichen Situation. Aus den dargestellten Überlegungen ergibt sich ein Funktionsgefüge der Teilelemente, bei der Modellierung der Umgebung in dem Risikokommunikation erfolgreich betrieben werden soll.

2.3 Faktoren der Risikoperzeption und des Risikourteils

Die große Herausforderung für Risikokommunikation stellt das Herstellen des Risikobewusstseins dar. Dabei spielen folgende Merkmale eine bedeutende Rolle für die Risikoperzeption und das daraus entstehende Verhalten: Verfügbarkeitsheuristik (wenn die möglichen Konsequenzen nicht vor Augen sind, werden diese unterschätzt), Affektheuristik (Nutzen beim Eingehen des Risikos), optimistischer Fehlschluss (empirisch belegtes Phänomen: unrealistischer Optimismus der Menschen [CoSW86]), persönliche Merkmale (Risikobereitschaft), situative

Einflüsse (Risikoinfolage, Stimmung, soziale Gruppe). Die Zusammenhänge dieser Faktoren zeigt Abbildung 1.

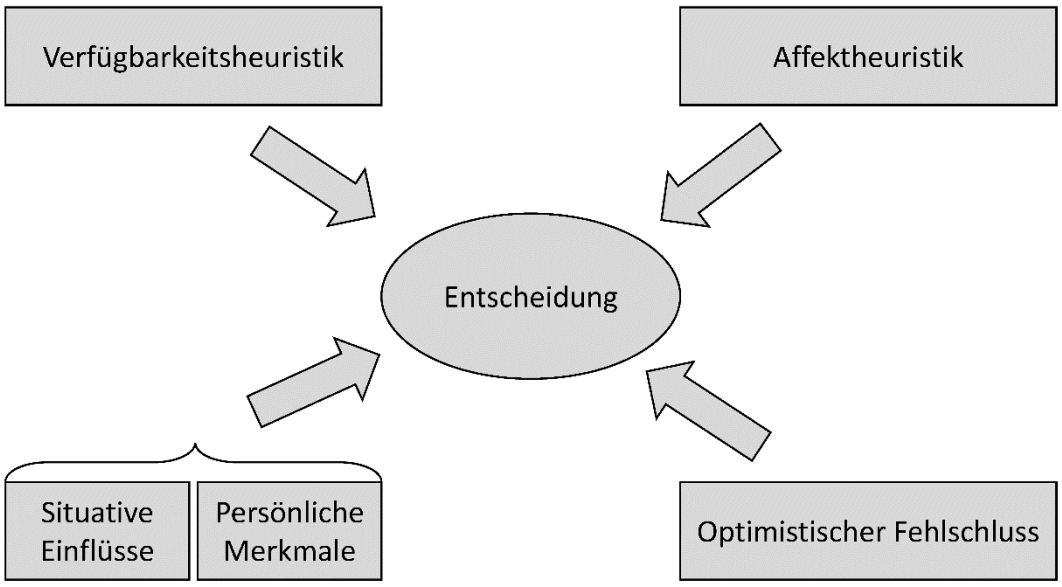

Abb. 1: Zusammenhänge der beeinflussenden Faktoren für Risikokommunikation

Aus dem Zusammenwirken obiger Faktoren ergeben sich folgende Probleme für die Risikokommunikation:

1. Problem der überzeugenden Darstellung des Risikos mit allen Folgen und Konsequenzen
2. Problem der Berücksichtigung der persönlichen Merkmale und der situativen Einflüsse
3. Problem der Verringerung des Einflusses von optimistischen Fehlschlüssen
4. Problem der „gesunden“ Einschätzung des Verhältnisses zwischen Verfügbarkeits- und Affektheuristik.

Über all diesen abgeleiteten Problemstellungen steht, wie bereits oben erwähnt, die Herstellung eines gemeinsamen Risikobewusstseins.

2.4 Anforderungen an Cyber-Security-Personal

Aus dem in Kapitel 2.3 beschriebenen Sachverhalt ergeben sich folgende Forderungen an die Fähigkeiten der Cyber-Security-Spezialkräfte im Bereich der Risikokommunikation:

- Vorhandensein des eigenen Risikobewusstseins als Grundvoraussetzung
- Schaffen von Vertrauen in die eigene Kompetenz beim Kommunikationspartner
- Fähigkeit zur Analyse von situativen Bedingungen und persönlichen Merkmale der jeweiligen Zielperson oder Zielgruppe
- Fähigkeit zur verständlichen und überzeugenden Erläuterung von Risiken
- Fähigkeit zur Zusammenarbeit mit anderen Experten aus dem Bereich Kommunikation oder anderen Risikobranchen
- Fähigkeit zu objektiven und sachlichen Darstellung des Risikos

Diese Forderungen sind unabhängig von der gerade relevanten Funktion und der Zielgruppe. Die Relevanz der Teilbereiche variiert je nach Auftrag und Lage. Die Zusammenarbeit mit an-

deren Experten aus dem Bereich der Massenkommunikation sowie weiteren internen und externen Medien ist besonders beim Erreichen einer großen Menge an Nutzern und evtl. sogar der allgemeinen Öffentlichkeit essenziell. Je weniger Personen beraten, bzw. aufgeklärt werden sollen, desto größer wird jedoch die Bedeutung der Face-to-Face-Kommunikation.

3 Folgerung aus der Human-Factors-Sicht

Das Risikobewusstsein kann bei der Masse der Nutzer und dem IT-Fachpersonal am besten über die Herstellung einer permanenten Verfügbarkeitsheuristik erreicht werden. Sensibilisierung in Form von Seminaren, Vorträgen, Lehrfilmen oder Simulationen mit Bezug zu den vergangenen Vorfällen/Angriffen und deren Folgen sind ein probates und wirkungsvolles Mittel. Das Drehen an dieser Stellschraube, gepaart mit der Aufklärung über die Wirkmechanismen des intrapersonellen Risikomanagements können mittel- und langfristig zur gewünschten Wahrnehmung und Optimierung des Verhaltens der Zielgruppe führen.

Bei der Zielgruppe Führung (strategische Management-Ebene) lohnt sich eine detaillierte Analyse der Personen, sowie der Rahmenbedingungen vor der eigentlichen Intervention und den gezielten Treatments zur Verbesserung des risikoinitiierten Verhaltens. Hier ist Expertise nicht nur im technischen Bereich gefragt, sondern vor allem auf der zwischenmenschlichen Ebene. Daher empfiehlt sich eine fundierte Schulung der Cyber-Security-Spezialkräfte in Analyse, Planung und Durchführung von Aufklärungsgesprächen zur Risikodarstellung und Bewertung. Im folgenden Kapitel wird eine dieser Maßnahmen dargestellt, welche bereits erfolgreich bei Krisenübungen in großen Unternehmen eingesetzt wurde. Aus Gründen der Vertraulichkeit sind alle Informationen, die Rückschlüsse auf echte Szenare oder gar Firmennamen zulassen, entfernt worden.

3.1 Vorstellung einer Messmethode

Die Krisenübung gilt allgemeinhin als die bestmögliche Vorbereitung für Krisen. Dies gilt auch im Zusammenhang mit Cyber Security und IT Schadenslagen. Um Verbesserungspotentiale durch diese Übung aber auch zu erkennen und zu nutzen ist es leider unbedingt erforderlich, den Finger erst einmal „in die Wunde zu legen“. Im Zuge dessen wurde durch den Autor die Methode der Informationsklassen entwickelt und bei diversen Projekten zur Anwendung gebracht. Folgende Anforderungen wurden an diese Methode gestellt:

1. Um die Ausprägung der Risikokommunikation zu bewerten, gilt es den Informationsaustausch und besonders dessen Qualität zu erfassen.
2. Keine Bewertung durch Personal außerhalb der untersuchten Firma. Daraus folgt die Anforderung, dass die Ergebnisse der Methode klar und von jedem auch ohne spezielle Fachkenntnisse klar zu interpretieren sind.
3. Keine Erfassung von personenbezogenen Daten, d.h. bei der Auswertung soll nicht ersichtlich sein, wer welche Antwort gegeben hat, niemand soll durch diese Auswertung angreifbar werden. Auch wenn dies den größten wissenschaftlichen Einschnitt bedeutet, ist diese Forderung für die Anwendung in der Privatwirtschaft unerlässlich.
4. Schnelle, möglichst automatisierte Auswertung mit Software Produkten, die in nahezu jedem Hause verfügbar sind, denn nur wenn das Wissen beim Kunden bleibt, und dies nachvollziehbar ist, ist ein Mehrwert aus Kundensicht zu generieren.
5. Nachzuweisen gilt, ob die durchführende Gruppe, also der „Untersuchungsgegenstand“, in diesem Fall meist der Krisenstab einer größeren Unternehmung, von einer Situation

ein gemeinsames Verständnis aufweist und ob die Kommunikation jeden in die Lage versetzt, seine Entscheidungen mit allen hierfür wichtigen Informationen zu treffen.

3.1.1 Vorstellung der Informationsklassen

Vorab sei angemerkt, dass die Bewertung der Qualität der Information selbst nicht Ziel dieser Methode ist. Information kann vielerlei Qualitätsmerkmale aufweisen, unter anderem:

- Inhalt
- Quantitative, qualitative, gemischte, … Information
- Information bezieht sich auf: Kritische Variable, Zentralvariable, Indikatorvariable
- Falschinformation, Desinformation, Gefälschte Information, …
- Gerücht, Spekulation, Vermutung, Behauptung, Hypothese, …
- Halbwahrheiten
- Genauigkeit, Alter, Beständigkeit, … der Information
- Zu schützende Information (VS-Grade)
- Attribute der Quelle (nicht der Information selber): Zuverlässigkeit, …
- Intentionalität (der Quelle, der Weitergabe)
- Aggregationsniveau der Information
- Stützungsgrad der Information: Anzahl identischer, ähnlicher Informationen (ggf. aus unterschiedlichen Quellen); Anzahl abweichender, gegenteiliger Informationen
- Zugänglichkeit (öffentlich, nicht öffentlich)
- Verbreitungsgrad, Bekanntheitsgrad
- Transportwege, Fluss, Verlauf, Kommunikation, … der Information
- Kulturgebundenheit, Möglichkeit der Dekodierung
- Uva.

Um diese Kriterien geht es hier dediziert nicht. Dies hat zwei Gründe: Erstens ist der externe Berater zumeist nicht in der Lage eine profundere Aussage zu treffen als die Experten vor Ort, welche hier der Bewertung unterliegen sollen und zweitens muss der Nachweis sich direkt aus den Handlungen der Übungsteilnehmer ableiten lassen, um den erwünschten Effekt, nämlich das Nachdenken über die Notwendigkeit von Prozessoptimierungsmaßnahmen, anzustoßen.

Demnach wird bei dieser Methode während einer Übung durch die Teilnehmer nur folgende Sachverhalte zu einigen vorab festgelegten Informationen bewertet:

War die Information für Sie verfügbar?

Haben Sie die Information benötigt?

Die Auswahl der zur Bewertung gestellten Informationen erfolgt anhand des Drehbuchs und des Analysegegenstands. Geht es demnach um Risikokommunikation, werden nur Informationen zur Bewertung gestellt, die die Bemessung und das Ausmaß von Risiken beinhalten.

Aus den beiden Antworten auf obige Fragen lassen sich nun die Informationsklassen ableiten, siehe hierfür **Abb. 2**.

Information	Verfügbar	Nicht verfügbar
Benötigt	Primärinformation	Defizitinformation
Nicht benötigt	Schatteninformation	Nichtinformation

Abb. 2: Darstellung der Informationsklassen

Die Auswertung und die Interpretation derselben werden im folgenden Anwendungstest beschrieben.

3.1.2 Anwendungstest der Methode

Bevor die Methode eingesetzt wurde, wurde sie ausgiebig anhand eines Planspiels getestet. Um die Erklärung möglichst beispielhaft zu halten, wird im Folgenden einer dieser Testszenarios vorgestellt.

Das Planspiel

Das genutzte Planspiel war eine Eigenentwicklung um verteiltes Arbeiten an einer gemeinsamen Problemstellung mit Hierarchien der Arbeitsebenen darzustellen: NetOpFeuer 2.0

Das Spiel NetOpFeuer 2.0
NetOpFeuer 2.0 ist eine Computersimulation, in der der Spieler die Rolle eines Feuerwehrkommandanten übernimmt. Auf dem Bildschirm sieht er eine Luftansicht eines Waldgebietes, in dem menschliche Siedlungen liegen. Auf der Karte sind Symbole für die Feuerwehreinheiten zu sehen, welche zur Verfügung stehen. Es handelt sich dabei um schwere Geländefahrzeuge, die einen großen Vorrat an Löschwasser mit sich führen. Außerdem gibt es Helikopter, die sich schneller bewegen können, dafür aber einen Löschwassertank mit geringerer Kapazität mit sich führen. Durch Anklicken einer Einheit sind Statusinformationen für diese abrufbar. Eine Windrose zeigt die Windrichtung an, ein Zahlenwert die Windgeschwindigkeit.

Des Weiteren sind auf der Karte Häuser als Symbol für bebaute Flächen zu sehen, zusätzlich Wiesen (die nicht brennen können) und zu Teichen aufgestaute Bachläufe (hier können die Einheiten Löschwasser nachtanken).

Die Feuerwehrkommandanten hatten in den genutzten Szenaren jeweils vier große Tanklöschfahrzeuge und zwei Hubschrauber unter ihrer Kontrolle. Jeweils vier von Ihnen arbeiteten gleichzeitig auf einer Karte. Diesen vier wurde jeweils ein Einsatzleiter vorangesetzt, der ebenfalls mit einem eigenen Computer vernetzt an der gleichen Karte arbeitete. Seine Aufgabe war die Koordination der einzelnen Feuerwehrkommandanten, welche wiederum ihre Fahrzeuge einsetzen und steuern mussten. Somit wurde ein gemeinsamer Problemraum (die gleiche Karte mit Wald, Wiesen und Häusern mit gelegentlichen Ausbrüchen des Feuers) mit einer Hierarchie (ein Einsatzleiter und vier Feuerwehrkommandanten) aufgestellt.

Leider reicht der Platz an dieser Stelle nicht aus um weitere Beschreibungen zu geben, weitere Informationen zu NetOpFeuer 2.0 können gerne via Email angefordert werden.

Die Geschichte von „Feuer“
Ausgehend von dem ursprünglichen Feuer-Programm von Brehmer (1995) (der das Programm für Studien zum verteilten Entscheiden nutzte) [Breh95] wurde eine Reihe von weiteren Feuerprogrammen erstellt und vor allem in der psychologischen Forschung eingesetzt. Dörner und Pfeifer (1991) haben eine DOS-, später eine Windows-Version (mit Pfeifer) für die Untersuchung komplexen Problemlösens erstellt [DöPf91]. Omodei und Wearing (1995) haben eine Netzwerkversion erstellt, um Gruppenprozesse zu untersuchen. Klögl und Puppe (1998) haben das Feuerszenario in der Multi-Agenten-Entwicklungsumgebung SeSAm reprogrammiert [OmWe95]. Buerschaper (2003) hat das Feuerprogramm in ein Kompetenztrainings-Planspiel (Smokejumper) eingebaut [Buer03]. Insbesondere die Programmversion von Dörner & Gerdes wurde und wird in einer Vielzahl von Studien und Seminaren verwendet.

Das Szenar
Das Szenar selbst, also wo welche Feuer ausbrechen, woher in welcher Stärke der Wind weht, wo Wald, wo Wiesen etc. sind, wurde vorab festgelegt. An dieser Stelle ist er nur wichtig zu wissen, dass alle Szenare über die folgenden Versuche gleich blieben.

Die automatische Auswertung
NetOpFeuer 2.0 gibt automatisch nach Ende jedes Szenars aus, wieviel Prozent der Waldfläche und wieviel Prozent der bebauten Fläche gerettet wurden. Bei keinerlei Verlusten wird also zwei mal 100% angezeigt.

3.1.3 Die Anwendung der Methode

Da das Szenar von uns selbst festgelegt wurde, konnten folgende 27 Informationen zur Bewertung vorab bestimmt werden:

1. Das gesamte Spielgeschehen konnte von dem Einsatzleiter auf seinem Bildschirm gesehen werden.
2. In den ersten Minuten des Spiels brach kein Feuer aus.
3. Das Feuer breitet sich schneller aus, wenn der Wind stärker ist.
4. Ein Tanklöschfahrzeug löscht schneller und erfolgreicher als ein Helikopter.
5. Das Whiteboard zeigte das gesamte Spielfeld an.
6. Der erste Brand brach in der oberen Hälfte des Spielfeldes aus.
7. Der Kommandant hatte nur einen Hubschrauber.
8. Der Wind kam während des Spielverlaufs aus verschiedenen Richtungen.
9. Die Geschwindigkeit eines Helikopters ist größer als die eines Tanklöschfahrzeuges.
10. Die Benzintanks waren ausreichend gefüllt.
11. Die Löschkapazität des Tanklöschfahrzeugs ist größer als die des Helikopters.
12. Die Ortschaften waren jeweils so nah am Wald, dass ein Feuer überspringen konnte.
13. Die Sichtweite eines Helikopters ist größer als die eines Tanklöschfahrzeuges.
14. Eine Ecke des Spielfeldes war jeweils ganz ohne Wald oder Bebauung.
15. Es gab 2 größere Ortschaften.
16. Im Chat wurde die aktuellste Nachricht rot angezeigt.
17. Jeder Gruppenführer hatte die gleiche Anzahl an Einheiten zur Verfügung.
18. Die Helikopter eigenen sich gut zum Patrouillieren von großen Gebieten.

19. Man kann durch eine gute Dislozierung der Einheiten die negativen Effekte des "Fog of War" verhindern.
20. Auch wenn der Einsatzleiter den groben Überblick hatte, war es sinnvoll, selbst aktiv nach Feuern zu suchen.
21. Der Einsatzleiter konnte sehen, welche Aktionen (Patrouillieren, Löschen, Tanken) die Feuerwehrkommandanten durchführen.
22. Das Spielfeld und die Karte des Whiteboards stellten dieselben Inhalte dar.
23. Es kam zu Ausfällen der Kommunikationsmittel.
24. Einheiten, die zu Fahrzeuggruppen zusammengefasst wurden, lassen sich effizienter über die Karte bewegen.
25. Die Automatismen der Fahrzeuge (z.B. Auto-Löschen) konnten nutzbringend angewandt werden.
26. Ein Brand konnte am besten gegen die Windrichtung bekämpft werden.
27. Manche Feuer gingen auch von alleine aus.

Diese Informationen wurden nun allen Spielern der Gruppe (1 Einsatzleiter, 4 Feuerwehrkommandanten) nach den Prinzipien der Informationsklassen zur Bewertung vorgelegt. **Abb. 3** zeigt eine Darstellung der Befragung, bei welcher MS Excel genutzt werden.

		Haben Sie diese Information gehabt?		Haben / hätten Sie diese Information benötigt?	
Frage 1	Das gesamte Spielgeschehen konnte von dem Einsatzleiter auf seinem Bildschirm gesehen werden.	◉ Ja	○ Nein	◉ Ja	● Nein
Frage 2	In den ersten Minuten des Spiels brach kein Feuer aus.	◉ Ja	○ Nein	◉ Ja	● Nein
Frage 3	Das Feuer breitet sich schneller aus, wenn der Wind stärker ist.	◉ Ja	● Nein	◉ Ja	● Nein
Frage 4	Ein Tanklöschfahrzeug löscht schneller und erfolgreicher als ein Helikopter.	◉ Ja	● Nein	◉ Ja	○ Nein
Frage 5	Das Whiteboard zeigte das gesamte Spielfeld an.	◉ Ja	● Nein	◉ Ja	○ Nein

Abb. 3: Die ersten 5 Informationen zur Bewertung

So wurde jede Information von jedem Mitspieler in einer der Klassen eingeteilt. **Abb. 4** zeigt die Zuordnung der Antworten zu den Fragen 1 – 27 gemäß den Informationsklassen. Greifen wir beispielsweise Frage 1 heraus, so ist zu erkennen, dass alle fünf Teilnehmer die Information als „Habe ich gehabt, aber nicht gebraucht“ bewertet haben.

Gruppe 1																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Primärinformation					3	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	
Defizitinformation		1	1	2	2	1			1		1							1									
Schatteninformation	5	1					1									1											
Nichtinformation		3	4	3				1		1		1	1	1	1		1										5

Abb. 4: Einteilung der Informationen in Klassen

Um eine schnellere visuelle Interpretation zu ermöglichen, wurden die Antworten farblich eingefärbt, jedoch zwingt der Schwarzweißdruck in dieser Publikation einen anderen Weg zu ge-

hen. Da die Auswertung mittels MS Excel erstellt wird, gibt **Abb. 5** die zugrundliegenden Regeln der Visualisierung an. Es sei angemerkt, dass eine Verwendung von einer Farbnomenklatur von Rot bis Grün (Grün = eine hoher Anteil der Teilnehmer teilt Information XY in diese Klassen ein) eine bessere Visualisierung und Interpretierbarkeit auf den ersten Blick ermöglicht.

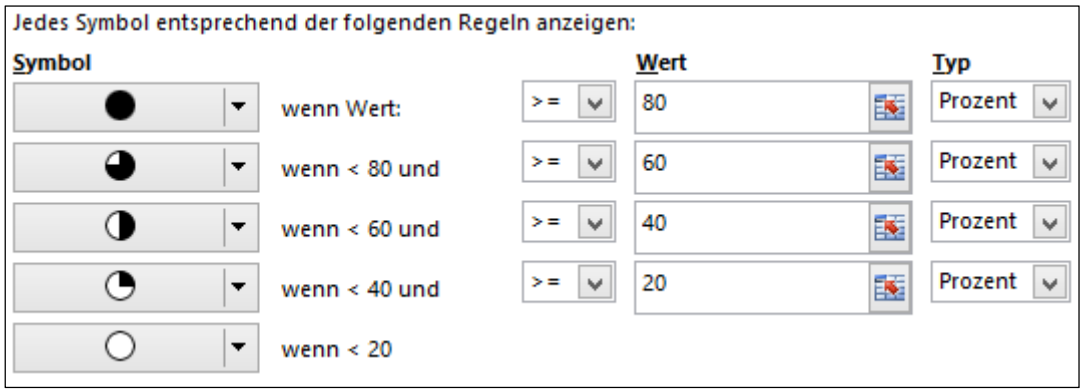

Abb. 5: Regeln der Visualisierung

Abb. 6 zeigt die Anwendung dieser Visualisierung.

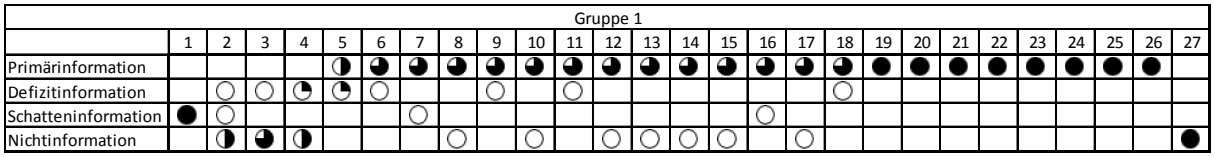

Abb. 6: Visualisierung

Natürlich kann noch ein prozentualer „Übereinstimmungswert“ errechnet werden. Wenn beispielsweise 4 von 5 Mitgliedern der Gruppe der entsprechenden Information die gleiche Klasse zuweisen, wäre der Übereinstimmungswert 80%. Der gemittelte Übereinstimmungswert über alle zur Bewertung gestellten Information war in den Versuchen mit dem Planspiel direkt proportional zu der Anzahl der geretteten Bäume und der Bebauung. Da jedoch nur insgesamt 8 Versuche mit jeweils 4 Gruppen durchgeführt wurden, kann man hier noch nicht von einer statistischen Signifikanz sprechen.

4 Anwendung in einer IT Schadenslage

Die Risikokommunikation wird bei einer IT Schadenslage vor besondere Herausforderungen gestellt. Folgende Gründe sind hierfür ausschlaggebend:

1. Nahezu jeder Bereich ist heutzutage mit IT ausgestattet, die für das Funktionieren des jeweiligen Bereiches essentiell ist. Letztlich bedeutet daher nahezu jeder Ausfall Stillstand und verursacht damit hohe Kosten.
2. Die zeitliche Komponente bei IT Schadenslagen ist als äußerst kritisch zu betrachten. Der Zeitdruck wird durch die Abhängigkeit von IT erhöht.
3. Die Wissensunterschiede zwischen den Entscheidern auf der Management-Ebene und den ausführenden Anteilen (taktische/operative Ebene) ist zumeist wesentlich höher als bei anderen krisenhaften Situationen.

Die Methode der Informationsklassen ist dazu geeignet, obigen Punkt 3 nachzuweisen und „erlebbar“ zu machen, wie den folgenden Unterkapiteln entnommen werden kann.

4.1 Anwendung

Um die Methode der Informationsklassen zur Anwendung zu bringen, wurden Information die das Risiko in diesem Szenar beschreiben, ausgewählt. Leider können diese Informationen hier nicht dargestellt werden, da sonst womöglich Rückschlüsse auf die entsprechende Unternehmung gezogen werden könnten. Es wurden insgesamt 15 Informationen an 10 teilweise dislozierte Mitglieder des Krisenstabs zur Bewertung gestellt. **Abb. 7** zeigt die Visualisierung:

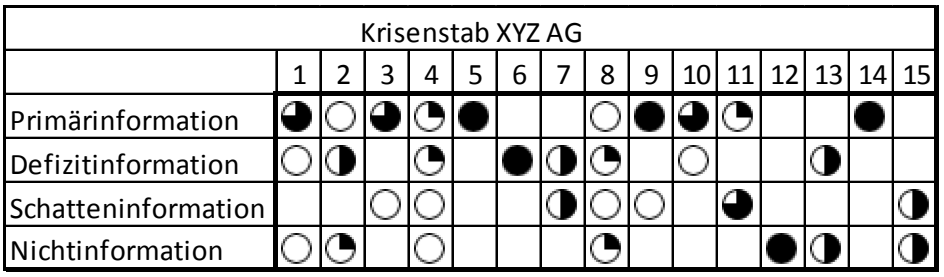

Abb. 7: Anwendung der Methode bei einem Krisenstab

4.2 Diskussion

Die größten Auffälligkeiten in Abbildung 7 werden im Folgenden diskutiert. Beispielsweise wurde Information 7 von etwa der Hälfte der Versuchspersonen als Defizitinformation eingestuft, d.h. sie war nicht verfügbar, wäre aber benötigt worden, und die andere Hälfte gab sie als Schatteninformation aus, d.h. sie war zwar verfügbar wurde aber nicht benötigt. In der nachgehenden Analyse lohnt es sich also Information 7 hinsichtlich folgender Gesichtspunkte genau zu untersuchen:

1. Wann wurde sie eingespielt?
2. Wer hat sie empfangen?
3. Wie wurde sie abgelegt bzw. verarbeitet?
4. Welche Prozesse waren betroffen?
5. Etc.

Hierdurch lässt sich gut erkennen, an welchen Prozessen die Stellschrauben neu zu justieren sind. Der größte Vorteil der Methode besteht darin, dass diese Auswertung ausreicht, jedem aufzuzeigen, dass hier ein fehlendes Verständnis bzw. Bewusstsein über den Wert dieser Information bestand. Der Impuls dies aufzuschlüsseln und zu lösen, kommt meist von den Beteiligten selbst.

Bei Information Nummer 4 ergab sich beispielsweise jede Informationsklasse mehr als einmal, ein sogenannter „bunter Hund“. Nach abschließender Analyse stellte sich heraus, dass diese Information in einem technischen Zustandsbericht enthalten war, und von den meisten Mitgliedern nicht vollumfänglich verstanden wurde. Auch das ließ Rückschlüsse auf Defizite bei der Risikokommunikation zu.

Leider ist es aus Platzgründen an dieser Stelle nicht mögliche, sämtliche Erkenntnisse darzustellen. Erneut kann der Autor bei weiterführendem Interesse gerne kontaktiert werden.

5 Fazit

Risikokommunikation wird bei IT Schadenslagen vor besondere Herausforderungen gestellt, die bereits im Vorfeld aktiv angegangen und über alle Ebenen hinweg umgesetzt werden sollten. Nicht nur gilt es ein breites Verständnis bei der Führungsebene aufzubauen, es gilt ebenso die operative Ebene (Techniker) zur Ausformulierung klarer Zustandsberichte zu befähigen. Dennoch kann man kaum allgemeingültigen, d.h. für jede Unternehmung/Behörde zutreffenden Aussagen zur Optimierung geben. Hier bietet sich die Krisenübung als perfektes Werkzeug an, die vorhanden Optimierungspotentiale bestmöglich auszuschöpfen, denn die Übung sollte nie reiner Selbstzweck sein sondern immer eine Verbesserung des Status Quo mit sich bringen.

Literatur

[Breh95] B. Brehmer: Feedback delays in complex dynamic decision tasks. In P. Frensch & J. Funke (Hrsg.), Complex problem solving. The european perspective, S. 103-130 (1995).

[Buer03] C. Buerschaper: Simulierte Szenarien in der Organisationsberatung. In S. Strohschneider (Hrsg.), Entscheiden in kritischen Situationen (2003).

[CoSW86] T. Covello, P. Slovic, D. von Winterfeldt: A Review of the Literature. Risk Abstracts, 3, 4, S. 172-182 (1986).

[DöPf91] D. Dörner, F. Pfeifer: Strategisches Denken, strategische Fehler, Stress und Intelligenz. Berlin: Projektgruppe Kognitive Anthropologie Max-Planck-Gesellschaft, Memorandum 11 (1991).

[OmWe95] M. Omodei, A. Wearing: The re chief microworld generating program: An ilustration of computer-simulated microworlds as an experimental paradigm for studying complex decision making behaviour. Behavior research methods, instruments and computers, 3, 303-316 (1995).