Nr. 4, August 2011

# <kes>

Die Zeitschrift für Informations-Sicherheit

ISSN 1611-440X

**BSI Forum**
offizielles Organ des BSI
Bundesamt für Sicherheit in der Informationstechnik

**Sonderdruck für**
CETUS Training & Consulting

## Szenario-technik:

Risikoanalysen mit mehr strategischem Wert

S. 23

## Süßes oder Saures?!

Malware-Trends und -Abwehr

ab S. 52

SecuMedia

# Szenariotechnik für Risikoanalysen

**Sicherheitsmaßnahmen sollen bei der Umsetzung der Geschäftsstrategie unterstützen – vorausgehende Risikoanalysen müssen dazu Geschäftsziele einbinden und strategische Einflüsse der IT, ihrer Risiken und Sicherheitsmaßnahmen ausreichend berücksichtigen. Die klassische Betrachtungsweise vieler IT-Normen greift hier zu kurz – helfen kann eine angepasste Szenariotechnik.**

*Von Frederik Humpert-Vrielink, Schüttorf*

Rein statische Betrachtungen entsprechen heute bei Risikoanalysen nicht mehr dem Stand der Technik, da sie einen zu geringen Erkenntnisgewinn produzieren: In vielen Risikomanagementprozessen sind die Handlungsoptionen nicht miteinander vernetzt und oft rein technisch orientiert. Es ist für Sicherheitsbeauftragte an der Zeit, sich anderer Methoden zur Risikoanalyse zu widmen.

Um Risiken angemessen zu analysieren, ihre Auswirkungen auf das Geschäft fundiert zu beschreiben und verantwortlichen Risikoträgern alle Konsequenzen möglicher Entscheidungen vorlegen zu können, benötigen Sicherheitsmanager eine Methodik, die nicht nur „eindimensional" denkt, sondern die Abhängigkeiten der Risiken voneinander und Wechselwirkungen von Risiken und Maßnahmen untereinander beschreibt. Nur dann ist eine Risikoanalyse aussagekräftig und nachvollziehbar.

Die vier wichtigsten Dimensionen, die man im Rahmen einer umfassenden, geschäftsorientierten Risikoanalyse berücksichtigen sollte, sind (vgl. Abb. 1):

- Geschäfts-/IT-Strategie,
- Geschäftsprozesse,
- IT-Systeme und
- Schwachstellen.

Verglichen mit Methoden des Informationssicherheitsmanagements (ISM) zur Risikoanalyse – etwa dem BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz" (www.bsi.bund.de/gshb/) – erscheinen diese Dimensionen sehr weit reichend, da sie sowohl IT-Strategie als auch Geschäftsprozesse und deren Logik einbeziehen. Dies erfordert, dass Informationen zu einer Geschäftsstrategie inklusive IT-Strategie und klar beschriebenen Geschäftsprozessen vorliegen.

## Einbinden der Strategie

Um den eingangs beschriebenen hohen Anforderungen an Risikoanalysen gerecht zu werden, bedarf es eines Wechsels des Betrachtungswinkels: Die strategische Ausrichtung des Unternehmens in die Analyse mit einzubeziehen, benötigt eine Methode, die sich für einen „Blick in die Zukunft" eignet – hier ist die Nutzung der Szenariotechnik (vgl. Kasten) ein sinnvoller Ansatz.

Bedingt durch die hohe Komplexität der Informationsverarbeitung ergeben sich heute viele Risiken aus der Prozesslogik, der Anwendungslogik und allgemein aus den eingesetzten IT-Systemen. Um die Auswirkungen eines Verlusts von Vertraulichkeit, Verfügbarkeit oder Integrität abzubilden, wird jedoch meist eine Art Ratespiel betrieben – die Kernfrage lautet dabei „Was passiert, wenn...?" und zielt in Richtung technischer Fehlerquellen oder menschlichen Versagens.

Die Konsequenzen von Entscheidungen und Auswirkungen auf andere Risiken werden aber in der Regel nicht beleuchtet. Die üblichen Ansätze berücksichtigen nicht, was bei einer Verkettung von Vorkommnissen passiert oder welche Situation entsteht, wenn eine Entscheidung in die eine und nicht in die andere Richtung getroffen wird. Für Unternehmen und Behörden wird es daher leicht zum Glücksspiel, ob die erstellten Analysen auch wirklich alle Risiken erfassen. Dabei ist ein

| | |
|---|---|
| Geschäfts-/IT-Strategie | Geschäftsprozesslogik |
| Technik / IT-Systeme | bekannte und potenzielle Schwachstellen |

*Abbildung 1: Eingabedimensionen der Szenarioanalyse*

vernünftiger Blick in die (mögliche) Zukunft unerlässlich, denn nur dann kann man die Entwicklung erkannter Risiken in Abhängigkeit von Maßnahmen und Strategie fundiert analysieren.

Die aktuelle IT-Strategie spielt jedoch bei der Risikoanalyse auch unabhängig von der eingesetzten Technik eine große Rolle: Dieser Aspekt trägt vor allem der technischen Entwicklung und der Entwicklung in untersuchten Unternehmen oder Behörden Rechnung. Auch dies unterbleibt in den meisten, heute üblichen (standardisierten) Risikoanalysen. Viele Analysten nutzen stattdessen technisches Wissen und Expertengespräche mit Herstellervertretern zur Ergebnisfindung: Dabei produzieren sie lange Listen, die jedoch bei einem Strategiewechsel oder einer veränderten Plattformstrategie überflüssig werden oder an eine veränderte Risikolage anzupassen wären.

## Allgemeine Szenariotechnik

Die Szenariotechnik ist als Methode der Zukunftsforschung entwickelt worden, um Entwicklungen abzusehen und beschreiben zu können. Bei einem Szenario handelt es sich in der reinen Lehre um die Beschreibung der zukünftigen Entwicklung eines Prognosegegenstandes unter alternativen Rahmenbedingungen; abgebildet wird dies durch konkrete Zielvorstellungen und plausible beziehungsweise nachvollziehbare Visionen. Dabei beschreibt die Szenariotechnik vor allem Wirkungszusammenhänge und weniger Wahrscheinlichkeiten – ein Szenario ist damit eine beschriebene zukünftige Entwicklung unter Berücksichtigung verschiedener Variablen.

Szenarien, die im Rahmen der Szenariotechnik entwickelt werden, haben hypothetischen Charakter: Niemand kann garantieren, dass sie so eintreten wie prognostiziert – unvorhergesehene Ereignisse können die abgeleiteten Szenarien verändern. Dies ist jedoch zweitrangig, da es der vorrangige Zweck von Szenarien ist, auf Entscheidungen einzuwirken. Daher erfolgt der Einsatz von Szenarien in der Regel

- zur Frühwarnung vor unerwünschten Entwicklungen,
- als Orientierung vor der strategischen Planung,
- zur Prüfung der Unternehmenspolitik auf Nachhaltigkeit,
- als Methode zum Innovationsmanagement und
- als Methode der strategischen Planung.

Ein Szenariomodell arbeitet idealerweise mit einem so genannten Szenariotrichter: Dieser Trichter bildet den Raum der verschiedenen Möglichkeiten ab – je weiter man den Blick in die Zukunft richtet, desto breiter wird der Trichter. Sinnvoll ist ein Betrachtungszeitraum von zwei bis acht Jahren Dauer.

Um die Menge der Zukunftsbilder nicht zu komplex zu gestalten, werden in der Regel drei Zukunftsbilder gebildet:

- Das *Best-Case*-Szenario orientiert sich an einem bereits feststehenden Leitgedanken: Hier interessiert allem voran der Zusammenhang zwischen dem Ziel und den zugehörigen Faktoren.
- Das *Worst-Case*-Szenario analysiert, was schlimmstenfalls passieren kann: Welche Faktoren könnten die Zukunftsstrategie durchkreuzen? Als Ergebnis schnürt ein Worst-Case-Szenario Maßnahmenpakete, die eine Absicherung darstellen können.
- Das *Trend*-Szenario orientiert sich am „plausibelsten" Weg: Es liefert ein Mittel zwischen Best- und Worst-Case-Szenario.

Um die Szenarien ausreichend beschreiben zu können, ist eine Sammlung, Beurteilung und Interpretation naturgegebener, sozialer, politischer sowie kultureller Trends und technischer Fakten auszuwerten. Diese Treiber umfassen mindestens

- absehbare Entwicklungen,
- Annahmen, über die keine Sicherheit besteht und
- so genannte „Wild Cards" (äußerst unwahrscheinliche Ereignisse).

Die idealtypische Szenariotechnik ist dabei vom Ablauf her folgendermaßen gegliedert:

- Strukturierung des Untersuchungsfelder,
- Aufgaben- und Problemanalyse,
- Untersuchung der Einflussbereiche und Wirkungsbeziehungen,
- Auswahl beschreibender Faktoren und Projektion,
- Szenario-Beschreibung und Interpretation und
- Störereignis- und Auswirkungsanalyse.

Nach Abschluss dieser Phasen werden die Szenarien in konkrete Pläne transferiert. Auch wenn eine exakte Projektion der Zukunft nicht möglich ist, kann die Szenariotechnik doch die Unsicherheit über planerische Aussagen reduzieren. Ferner ermöglicht sie es, eine Orientierung über zukünftige Entwicklungen und Auswirkungen auf das eigene Handeln zu erhalten.

## Szenariotechnik im Vergleich

Die Szenariotechnik geht auf den amerikanischen Zukunftsforscher Herman Kahn zurück: Sie wurde in den 50er-Jahren für militärische Zwecke entwickelt. Heute wird sie zumeist im betrieblichen Innovationsmanagement eingesetzt und verfolgt das Ziel, extreme Entwicklungen oder Wunschszenarien der Märkte derart abzubilden, dass man Maßnahmen ergreifen kann, um eine für das Unternehmen optimale Zukunft zu erreichen. Zusätzlich wird die Szenariotechnik in der Zukunftsforschung eingesetzt, um Trends zu erkennen und verschiedene Zukunftsvarianten abbilden zu können.

Natürlich kann niemand ernsthaft von einer Trendanalyse sprechen, sobald es um den Bereich des Risikomanagements oder der Risikoanalyse geht. Doch die Abhängigkeiten der Auswirkungen verschiedener Entscheidungen untereinander darstellen und analysieren zu können, ist in diesem Anwendungsfeld genauso wichtig! Damit qualifiziert sich die Szenarioanalyse als Methodik zum Risikomanagement: Sie ermöglicht es, anhand verschiedener Einflussfaktoren und simulierter Entscheidungen die Auswirkungen von Sicherheitsmaßnahmen darzustellen.

Betrachtet man im Gegensatz dazu gängige Methoden der Risikoanalyse im Bereich des Sicherheitsmanagements, so sind diese sehr technisch orientiert. Zusätzlich fehlt es an einer notwendigen Integration von Abhängigkeiten, um Entwicklungen korrekt abbilden zu können. Vor diesem Hintergrund sind die Ergebnisse heute üblicher Risikoanalysen statisch und „eindimensional". Ferner liefern sie Ergebnisse nur auf Basis einer Stichtagsanalyse oder einer unveränderlichen Evaluationsbasis: Zumeist wird mittels Expertenbefragungen der Risikolevel der technischen Komponenten ermittelt und man definiert Gegenmaßnahmen auf Basis der Ergebnisse dieser Gespräche. Als Experten werden meist die bereits erwähnten Herstellervertreter oder Systemintegratoren herangezogen: Diese beherrschen zwar die eingesetzte Technik, berücksichtigen jedoch nicht die Entwicklung des Gesamtumfelds inklusive der Auswirkungen des konkreten Geschäfts und seiner Strategien. Dies sorgt dafür, dass die Ergebnisse letztlich unscharf bleiben und keine ausreichenden Informationen für fundierte Entscheidungen liefern können.

Wird nun eine Szenariotechnik im Rahmen der Risikoanalyse eingesetzt, ergibt sich hingegen eine fundierte Dokumentation verschiedener Handlungsalternativen: Diese unterschiedlichen Szenarien bedenken nicht nur einzelne Risiken, sondern simulieren gleichzeitig auch die Abhängigkeit unterschiedlicher Risikoträger untereinander. In der Matrix von Abbildung 2 wird als so genanntes Deskriptorengitter dargestellt, wie die einzelnen Risiken oder Entscheidungen aufeinander einwirken: je höher die Zahl, desto höher sind der Einfluss auf- oder die Abhängigkeit untereinander.

Das Ergebnis ermöglicht es Risikoentscheidern, sich mit ganz konkreten Risiken für das betrachtete Unternehmen und die Informationssicherheit auseinanderzusetzen. Die dynamische Entscheidungsbasis ermöglicht es gleichzeitig, Entscheidungen nach dem Einbinden neuer Faktoren zu hinterfragen und damit zusätzlich einen fortdauernden Risikomanagementprozess in Gang zu setzen. Gleichzeitig kann sich ein Entscheider, dessen Risiken auf Basis der Szenariotechnik analysiert worden sind, sicher sein, alle – oder zumindest die meisten – Alternativen und Szenariokaskaden vorgelegt zu bekommen.

## Notwendige Anpassungen

Die allgemeine Methodik muss jedoch für fundierte Risikoanalysen im Rahmen der Informationssicherheit leicht abgewandelt werden, wie in Abbildung 3 dargestellt. Der Ursprungsgedanke agiert mit *einem* so genannten Szenariotrichter (vgl. Kasten): Dieser fußt in der Originalmethode auf einem Zeitpunkt X als Gegenwartsbetrachtung. Durch verschiedene Aggregationen bildet er dann ein Trendszenario sowie je ein positives und negatives Extremszenario ab. Im Idealfall gibt es somit drei Ausprägungen der zu beleuchtenden Szenarien.

Im Rahmen einer Risikoanalyse wird der Analyst mit diesen drei Szenarien jedoch nicht auskommen.

| | Risiko 1 | Risiko 2 | Risiko 3 | Risiko 4 | Summe Aktiv |
|---|---|---|---|---|---|
| **Risiko 1** | | -1 | 0 | 2 | 1 |
| **Risiko 2** | 2 | | 1 | 0 | 3 |
| **Risiko 3** | -2 | 1 | | -1 | 2 |
| **Risiko 4** | 1 | 0 | 2 | | 3 |
| **Summe Passiv** | 1 | 0 | 3 | 1 | |

*Abbildung 2: Deskriptorengitter*

Das ergibt sich allein schon dadurch, dass getroffene Maßnahmen, um IT-Risiken zu minimieren, möglicherweise neue Risiken nach sich ziehen, die das Szenario beeinflussen können (vgl. Abb. 3). Daher gibt es selbst bei starker Aggregation der Ergebnisse in einer Risikoanalyse zur Informationssicherheit nicht nur drei Szenarien, sondern eine nicht vorab zu beziffernde Anzahl.

Die Herausforderung liegt nun darin, diese Szenarien abhängig von ihren beschreibenden Faktoren, den so genannten Deskriptoren, zusammenzufassen (Clustering) und die wahrscheinlichsten Szenarien zu identifizieren. Die hierbei betrachtete Wahrscheinlichkeit ist jedoch kein Ratespiel, sondern eine Ableitung aus der IT-Strategie: Denn diese lässt Rückschlüsse auf die zukünftige Entwicklung der eingesetzten Technik zu und beeinflusst damit, wie wahrscheinlich die ausgewählten Szenarien werden.

Für jedes dieser „wahrscheinlichen" Szenarien ist es dann sinnvoll, einen eigenen Szenariotrichter auf Basis der Entscheidungen zu verwenden: Dieser liefert dann die Projektionsfläche, um abzuschätzen, was passiert, wenn weitere Risiken hinzukommen oder man entsprechende Sicherheitsmaßnahmen trifft. Die Kombination verschiedener Trichter ermöglicht zudem, zusätzliche Abhängigkeiten untereinander abzubilden.

## Risiken priorisieren

Die beschreibenden Faktoren der betrachteten Szenarien sind die im Vorfeld ermittelten Risiken für die Informationssicherheit. Der Einfachheit halber sollte man je Szenario maximal zehn Deskriptoren verwenden, damit das Konstrukt nicht zu komplex wird. Um herauszufinden, *welche* Risiken als deskriptive Faktoren besonders geeignet sind, wird die so genannte Risikopotenzialzahl herangezogen: Sie ergibt sich aus dem Produkt von Schadenshöhe und -wahrscheinlichkeit auf einer vordefinierten Bewertungsskala – oder man nutzt alternativ den aus Schadenshöhe (in Euro) und Eintrittswahrscheinlichkeit errechneten Erwartungswert. Je höher die ermittelte Zahl, desto wichtiger ist das Risiko als deskriptiver Faktor.

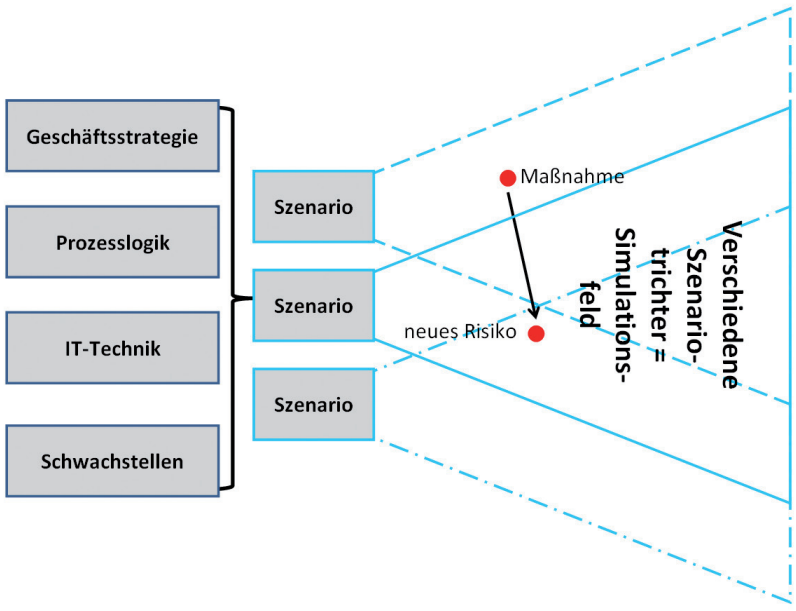
Für jeden der deskriptiven Faktoren ergründet man anschließend, wie er sich auf die jeweils anderen Faktoren auswirkt (Ergebnis vgl. Abb. 2). Je höher dabei die Zahl, desto höher die Auswirkung der Faktoren aufeinander: Eine positive Zahl bedeutet eine fördende Auswirkung des Risikos in Zeile X auf das Risiko in Spalte Y – dadurch kann ein Kumulationseffekt entstehen. Eine negative Zahl bedeutet hingegen, dass Risiko X einen hemmenden Effekt auf Risiko Y ausübt. Somit werden Abhängigkeiten transparent dargestellt und es entsteht ein konsistentes Ursache-Wirkung-Diagramm.

## Einflüsse eigener Steuerung

Welche Informationsbasis reflektiert jedoch das Ursache-Wirkung Diagramm? Ein wichtiger Faktor ist wie bereits ausgeführt die IT-Strategie: Im Gegensatz zur klassischen Szenariotechnik, welche die Einflüsse externer Faktoren auf Entscheidungen betrachtet, ist bei der hier beleuchteten Szenarioanalyse die eigene Steuerung ein gravierender Faktor. Insoweit eignet sich diese Methodik auch für das kritische Hinterfragen von IT-Strategiedokumenten und Geschäftsprozessmodellen vor dem Hintergrund der diesen Planungen innewohnenden Risiken. Je nach Ausrichtung bergen diese Dokumente oder Planungen starke Einflussfaktoren für die zu betrachtenden Risiken.

Ein weiterer Faktor für die Einflussnahme der Risiken und Szenarien untereinander ist die Logik der Geschäftsprozesse: Mittlerweile dürfte hinreichend bekannt sein, dass IT nicht nur Kostenfaktor, sondern Unterstützer des Geschäfts und untrennbar mit den Geschäftsprozessen einer Unternehmung verbunden ist – vor allem, da die IT-Integration in geschäftliche Abläufe die Logik der Geschäftsprozesse untereinander beeinflusst. Somit liefern mittels Szenariotechnik durchgeführte Risikoanalysen auch optimale Dokumente,

*Abbildung 3: Angepasste Methodik mit Simulationsfeld*



um in ein Risikomanagement gemäß dem COSO-Framework eingebunden zu werden.

## Vorteile

### Bessere Entscheidungsfindung

Eine Szenarioanalyse ist ein arbeitsaufwändiges Projekt, keine Frage – der Aufwand hierfür ist mit den Ansätzen für heute übliche Risikoanalysen „nicht zu vergleichen". Doch wer diese Methodik aufgrund des erhöhten Aufwands verwirft, verzichtet auch auf ihren erhöhten Nutzen! Denn die Entscheidungsfindung auf Basis einer Szenarioanalyse ist mehrdimensional: Somit lassen sich wirklich zukunftsfeste Entscheidungen über die Umsetzung von Maßnahmen treffen. Aufgrund der Abhängigkeitsanalyse stehen dabei verschiedene wichtige Fragen im Mittelpunkt:

_____ Was passiert, wenn ich auf Risiko A mit Maßnahme X reagiere?
_____ Welche Auswirkungen hat Maßnahme X auf Risiko B und die Gesamtsumme der Risiken?
_____ Welches Ausmaß nimmt Risiko B an, wenn ich kumulativ Risiko A trage?

Die durchzuspielenden realistischen Szenarien sind also ineinander verschachtelt. Das mag auf den ersten Blick die Entscheidungsfindung erschweren – der zweite Blick offenbart aber den unschätzbaren Vorteil dieser Analysemethodik: Anders als die Delphi-Methode oder rein technische Analysevorgänge verbindet sie nämlich die Konsequenzen von Entscheidungen miteinander. Daraus können sich unmittelbar andere Handlungsoptionen ergeben. Gerade bei der Diskussion mit den Verantwortlichen für die Risiken und das betriebliche Risikomanagement ist dies ein Vorsprung gegenüber anderen Verfahren.

Bedenkt man darüber hinaus, dass das Management der Informationssicherheit Bestandteil der Gesamtrisikosteuerung ist, ergibt sich eine integrierte und durchdachte Methodik, welche die Anforderungen verschiedener beteiligter Parteien erfüllt: Dadurch, dass CIO oder Security-Manager einen Entscheidungsvorschlag vorlegen können, der alle Konsequenzen einer oder mehrerer Entscheidungen bedenkt, richten sich diese Rollen gleichzeitig stärker in Richtung der Geschäftsziele aus und wirken so am sinnvollen Wandel der Rolle von IT und IT-Sicherheit im Unternehmen mit.

### Mehr Wirtschaftlichkeit

Auch der Kerngedanke, dass Informationssicherheit wirtschaftlich sein soll, wird durch den Einsatz der Szenariotechnik unterstützt: Häufig werden Sicherheitsmaßnahmen umgesetzt, weil sie vordergründig ein Risiko minimieren. Dabei werden jedoch oft die Auswirkungen auf andere Risiken unterschlagen, wodurch zusätzliche Sicherheitsmaßnahmen fällig werden können. Kumuliert man alle letztlich anfallenden Kosten, so können diese oft höher sein als bei einer strukturierten Betrachtung im Gesamtzusammenhang einer Szenarioanalyse.

Unstreitig ist, dass – gleichgültig welche Methode man anwendet – eine *exakte* Prognose der Auswirkungen bestimmter Entscheidungen nicht möglich ist. Dies liegt schon darin begründet, dass die Entscheidungsfindung in Prozessen nicht immer homogen ausgestaltet ist. Dennoch hilft die Szenariotechnik, die Unsicherheit über die Auswirkungen von Risikoentscheidungen massiv zu reduzieren. ■

*Frederik Humpert-Vrielink ist ISO-27001-Auditor und Handlungsbevollmächtigter der CETUS Consulting GmbH.*