Corsecon
AGENTUR FÜR SICHERHEITSMANAGEMENT

# Sicherheitsbriefing

02/23 – Fokus neue Ansätze für Risikobeurteilungen

**Fokus im März 2023**
Sicherheitsstrategie

## Aktuelle Meldungen

### Sabotageakte durch Mitarbeiter

In den jüngsten Pressemitteilungen häufen sich Meldungen zu Sabotageakten in Unternehmen.
Neben dem prominentesten Beispiel ZDF und dem millionenteuren, absichtlich verursachten, Wasserschaden am Hauptsitz in Mainz, finden sich auch Skurrilitäten wie unter Kaffeebohnen gemischtes Schneckenkorn in einer BG-Klinik. Dass von 190 Kaffeetrinkern keiner gesundheitliche Beschwerden bekam, war ein glücklicher Umstand.
Auch wenn diese Art der Sabotage im ersten Moment spaßig anmutet, bedeutet sie für Unternehmen neben finanziellen Schäden negative Presse, das Risiko von Personenschäden, erhebliche Betriebsunterbrechungen und den Fokus der Ermittlungsbehörden.

*-> Corsecon-Kommentar:*
*Nach dem Gallup Engagement Index sind 20 % aller deutschen Angestellten derart frustriert, dass sie mit ihrem Verhalten ihren Arbeitgeber aktiv boykottieren (Loud-Quitting). In einigen Fällen bremst dies nur die Produktivität der Unternehmen, in anderen entstehen erhebliche Schäden durch die Straftaten, die die sogenannten Innentäter zu Lasten des Unternehmens begehen. Auf sie entfällt 73 % der verursachten Schadensumme. 26 % der Täter, die Cyberangriffe umsetzen, sind (ehemalige) Mitarbeiter, die beispielsweise absichtlich auf Links in Phishing-Mails klicken.*
*Sabotageakte können auch von Externen, wie z.B. staatlichen Akteuren ausgeübt werden. Aufgrund der Fokussierung auf Sabotageakte durch Dritte, wurde die vergangenen Jahre bei vielen Unternehmen die Risikobetrachtung von innen vernachlässigt. Zur Bewältigung ist ein ganzheitlicher Ansatz der Unternehmenssicherheit, Compliance- und Personalabteilung zur Stärkung der Mitarbeiterbindung, -zufriedenheit sowie Erhöhung der Sicherheitsmaßnahmen und arbeitsrechtlichen Konsequenzen notwendig.*
*Quelle: Allianz Trade 2022, Wirtschaftswoche, Gallup, Bitkom 2022*

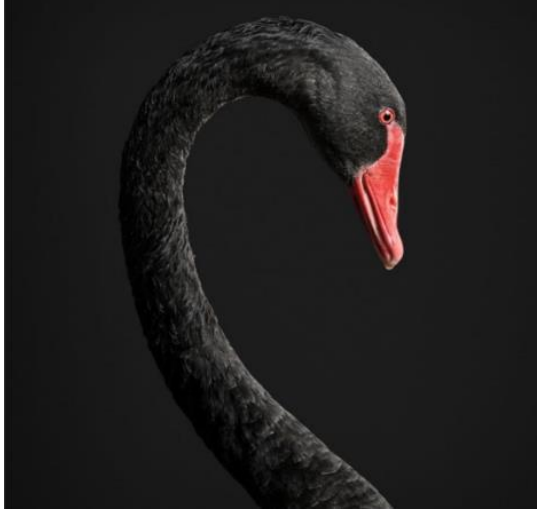
### Urteil: Sicherheitsrichtlinien befolgen zählt zu den Hauptpflichten von Arbeitnehmern

Eine Mitarbeiterin hatte wiederholt gegen eine Dienstanweisung, eine „Clean Desk Policy“, zum Verschluss von Geschäftsunterlagen bei eigener Abwesenheit verstoßen und wurde dafür von ihrem Arbeitgeber gekündigt.
Im Rahmen des folgenden Gerichtsverfahrens stellte das Landesarbeitsgericht Sachsen klar, dass es keine Rolle spielt, ob Externe oder lediglich andere Mitarbeiter (Need-to-know-Prinzip) Zugang zu den Daten erhalten. Die Urteilsbegründung verweist auf die Hauptpflicht von Mitarbeitern, die vom Arbeitgeber vorgegebenen Richtlinien einzuhalten.

*-> Corsecon-Kommentar:*
*Aus unserer Sicht hat das Urteil mit seiner Begründung wegweisenden Charakter für die Durchsetzung von Sicherheitsrichtlinien (betriebsinterne Verhaltensrichtlinien) in Unternehmen. Arbeitgeber müssen bei der Formulierung von bindenden Dienstanweisungen folgende Punkte beachten:*

- *Verhaltensregeln müssen allen Mitarbeitern bekannt sein*
- *Verhaltensregeln dürfen nicht unzumutbar sein*
- *Formulierungen müssen verständlich sein*
- *Bei nicht schwerwiegenden Verstößen sind Abmahnungen im Vorfeld einer außerordentlichen Kündigung erforderlich*
- *Verstöße aller Mitarbeiter müssen gleichermaßen geahndet werden (AGG)*

*Voraussetzung ist jedoch in erster Linie, dass Unternehmen gewillt sind, Verstöße aktiv aufzuklären und konsequent zu ahnden. Ansonsten bleiben viele Sicherheitsmaßnahmen weiterhin wirkungslos, weil Verstöße gegen sie bereitwillig geduldet werden.*
*Quelle: RA Ferner, LAG Sachsen (9 Sa 250/21)*



## Schwarze Schwäne im Sicherheitsmanagement

In der Sicherheitswelt bezeichnet der Begriff „Schwarze Schwäne“ unvorhersehbare und überraschend eintretende Ereignisse mit krisenhaften beziehungsweise katastrophalen Auswirkungen.
Besonderes Merkmal ist ihr äußerst seltenes Auftreten, die Eintrittswahrscheinlichkeit wird auf nahe null geschätzt. Aktuelle Ereignisse wie die Corona-Pandemie oder die Gasmangellage verdeutlichen, dass ihr Auftreten, wie im Vorfeld in öffentlich zugänglichen Analysen ermittelt, im Bereich des Möglichen liegt.
*-> Corsecon-Kommentar:*
*Die vergangenen Erkenntnisse sollten uns, insbesondere für aktuell diskutierte Zukunftsbilder, sensibilisieren. Zur Anpassung an die neue Gefährdungslage und die multiplen Krisen sind neue Ansätze im Risikomanagement erforderlich um auch Extremszenarien angemessen vorzubereiten. Zukunftsweisende Ansätze und Vorschläge zur Vorgehensweise im Unternehmen haben wir für Sie im Februar in den Fokus gestellt. Sie finden Sie in der PDF im Anhang. (Bildquelle: Pinterest)*

**Integration Schwarzer Schwäne in Risikobeurteilungen**

Integration Schwarzer Schwäne in Risikobeurteilungen
Im Anhang finden Sie konkrete Ansätze und Leitfäden wie alle Unternehmen, einschließlich kritischer Infrastrukturen, künftig Schwarze Schwäne identifizieren, systematisch analysieren und den Risiken angemessen begegnen können.

**Erforderliche Vorgaben zu Risikobeurteilung und –behandlung für KRITIS**
Die jüngsten Ereignisse haben in Deutschland auch bei Sicherheitslaien Zweifel an der Resilienz der KRITIS-Sektoren und öffentlichen Verwaltung aufkommen lassen. Sabotageakte oder die Corona-Pandemie führten in klassifizierten Unternehmen zu teils erheblichen Betriebsunterbrechungen mit weitreichenden Auswirkungen. Dies deutet auf mangelhaftes Sicherheitsmanagement von Staat und Unternehmen hin.
Aufgrund der zahleichen von ihren Dienstleistungen abhängigen Nutzern und dem Stabilisierungsfaktor, den sie für Staat und Gesellschaft darstellen, müssen diese Mängel und Versäumnisse der Vergangenheit auf beiden Seiten ausgeräumt werden und das künftige Sicherheitsniveau an den veränderten Umgebungsbedingungen und neuen Gefahren (geopolitisch, wirtschaftlich, …) ausgerichtet werden.
Diese Erkenntnis ist auch in der Politik angekommen, weshalb entsprechende EU-Richtlinien verabschiedet wurden (NIS-2, CER), die noch 2023 in nationales Recht, vermutlich mit einer Art IT-SiG 3.0 und KRITIS-Dachgesetz, umgewandelt werden.

Da das bisherige Sicherheitsmanagement vieler kritischer Infrastrukturen als mangelhaft zu bewerten ist, müssen auch die Rahmenbedingungen geprüft werden, die dies aktuell ermöglichen.

Im Fall kritischer Infrastrukturen übernimmt der Staat klassische Governance-Aufgaben im Sicherheitsmanagement.
Dazu zählt die Festlegung der einzuhaltenden Vorgaben und damit der allgemeinen Sicherheitsstrategie sowie die Kontrolle und Sanktionierung. In allen drei Bereichen gibt es Optimierungspotenziale.

Vorgaben
Aktuell gilt die Öffentliche Verwaltung in Deutschland nicht als kritische Infrastruktur, obwohl vermutlich auch die Verantwortlichen nicht bestreiten würden, dass die Definition kritischer Infrastruktur: „[…]die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, […] ist […]“ auch auf diesen Sektor zutrifft.
Die Einstufung als kritische Infrastruktur hängt aktuell ausschlaggebend an der Anzahl der Dienstleistungsnutzer. Zudem ist es den Betreibern möglich, die Unternehmen beispielsweise in mehrere juristische Personen aufzuspalten, die jeweils nur 499.999 Nutzer angeben, um so die Vorschriften zu umgehen.
Die Abhängigkeit anderer KRITIS sowie die Lieferketten essentieller Güter aus dem selben oder anderen Sektoren, wird kaum berücksichtigt.

Kontrolle
Es fehlen bereits jetzt, vor der Umsetzung der NIS-2 Direktive sowie der CER-Richtlinie der EU und dem damit verbundenen deutlichen Anstieg der als KRITIS eingestuften Unternehmen (alleine durch NIS-2 von 2.000 auf ca. 29.000), ausreichend Prüfer. Aus diesem Grund ist es den Betreibern möglich, neben den offiziellen Prüfinstituten auch „freie“ Prüfer die Erfüllung aller Anforderungen (§8a Abs. 3 BSIG), bestätigen zu lassen. Als Nachweis der Kompetenz der prüfenden Person ist eine Selbsterklärung, dass die Anforderungen erfüllt werden, ausreichend.

Sanktionierung
Seit 2019 wurden in Deutschland nach dem

BSIG (§14) kein einziges Bußgeldverfahren durch das BSI eingeleitet.

Das Reporting über die Wirksamkeit des staatlichen Systems und Zielerreichung beim Schutz der KRITIS erfolgt, nach aktuellem Stand des KRITIS-Eckpunktepapiers, vom Innenministerium an die Organe der EU.
Die Übernahme der vierten Governance-Aufgabe, die Befähigung der Unternehmen zur Umsetzung der Vorgaben, könnte durch ein Fort- und Weiterbildungsangebot für die eingebundenen Sicherheitsexperten in den Unternehmen sowie die Bereitstellung von Methoden und Musterdokumenten erfolgen.

**Ansatz:**
**Angepasste Risikobeurteilungen für KRITIS**
Wie im Januar-Sicherheitsbriefing angesprochen, sind Anpassungen in den bestehenden Risikobeurteilungen kritischer Infrastrukturen, auf dem Weg zu mehr Resilienz, besonders relevant. Da die Wirksamkeit von Sicherheitsmaßnahmen direkt von der Qualität der Risikobeurteilungen abhängt, muss der Fokus auf deren Durchführung und eventuell erforderliche Anpassungen gerichtet werden.
Die Vorgabe der zu nutzenden Methodik für KRITIS, in Kombination mit der Anpassung der gegenwärtig genutzten Risikobeurteilung, kann zu den angestrebten Ergebnissen führen.
Einige Änderungen haben wir im Folgenden beschrieben:

**1. Risikoidentifikation**
Der erste Schritt bei der Absicherung von KRITIS ist die vollständige Erfassung aller relevanten Risiken. Die angemessene Vorbereitung der Sektoren auf Extremszenarien ist aus staatlicher Sicht besonders relevant, da ihnen im Ereignisfall eine besondere Bedeutung in Deutschland zukommt. Da mehrere dieser Sektoren gleichzeitig sowie einzelne oft überdurchschnittlich stark betroffen sind, sollte die Regierung die strategische Vorausschau und Antizipation der Zukunft Deutschlands zentral vornehmen (siehe PDF: Szenarioanalyse und Plausibilitätsansatz).
Die Ergebnisse sollten transparent mit den Betreibern der Infrastrukturen geteilt und deren Bedeutung für die bedeutenden Infrastrukturen besprochen werden. Aktuell werden diese Szenarien von den Betreibern kaum betrachtet.
Für die ermittelten Szenarien, wie z.B. einen drohenden Angriff Chinas auf Taiwan, einen koordinierten Angriff auf kritische Infrastrukturen oder einen flächendeckenden Stromausfall kann dann aus den zentralen Ergebnissen auch die Kombinationen der Einzelrisiken zu verschiedenen Zeitpunkten definiert werden, mit denen kritische Infrastrukturen voraussichtlich konfrontiert werden.
Zusätzlich müssen die gängigen Risiken aus den Gefahrenkatalogen von den Betreibern, wie in allen anderen Unternehmen auch, auf Relevanz für den individuellen Betrieb geprüft werden.
Dazu sollten Recherchen, beispielsweise zu der Lage der Standorte, z.B. in Hochwasser- oder in Erdbebengebieten, vorgenommen werden, vorbei auch auf Erkenntnisse der Sachversicherer zu den Elementargefahren zurückgegriffen werden kann.

**2. Risikoanalyse**
Bei der folgenden Analyse der Standardrisiken und Einzelrisiken der zentral ermittelten Schwarzen Schwäne können Vorgaben sinnvoll sein, um übliche Mechanismen in Unternehmen zu unterbinden, die in Folge zu unzureichender Absicherung der Unternehmen führen.
Hier sei insbesondere auf die häufig, teilweise unterbewusst, (siehe PDF: Denkfallen) zu klein angenommenen Eintrittswahrscheinlichkeiten und Schadenausmaße verwiesen, deren Multiplikation in Folge dann kleine Risikopotentiale ergeben.
An dieser Stelle könnte die zentrale Bereitstellung fundierter Daten z.B. zu Kriminalität und verursachten Schäden (Speisung aus Daten von Kommunen, Ländern und des Bundes sowie Versicherern) einen Mehrwert bieten. Alle Betreiber würden für ihre Berechnungen mit offiziellen, einheitlichen und vor allen Dingen überprüfbaren Zahlen und Werten durchführen.

**3. Risikobewertung**
Die Bewertung des Risikopotentials erfolgt meist durch die Eingruppierung der Werte in eine Matrix nach Ampelfarben.
Kleines und mittleres Risikopotential werden dem grünen und gelben Bereich zugeordnet, bei dem keine bzw. keine sofortige Umsetzung von Sicherheitsmaßnahmen, zur Regulierung des Risikos, vorgesehen sind. Hohes Risikopotential wird im roten Risikobereich eingeordnet, wo die zeitnahe Risikobehandlung angezeigt ist.
Unternehmen neigen dazu, sowohl im Rahmen der Risikoanalyse als auch der dazugehörigen Bewertung, das Risikopotential so zu berechnen, dass möglichst wenig Risiken im roten Bereich liegen, welche (teure) Sicherheitsmaßnahmen erforderlich machen.
Die o.g. validen Daten zu Eintrittswahrscheinlichkeit und Schadenausmaß der Elementargefährdungen sowie Vorgaben zur Abgrenzung der einzelnen Matrixbereiche anhand fester Schwellenwerte, würden einen Risikoanalyse- und bewertungs-Standard für kritische Infrastrukturen bieten.
Darüber hinaus sollte eine weitere Kennzahl durch die Unternehmen ermittelt werden, die das „Beeinflussungspotential“ des Ausfalls auf andere kritische Infrastrukturen abbildet.
Abhängig vom ermittelten Wert, müssen dann in den folgenden Schritten ebenfalls geeignete Maßnahmen zur besseren Intraoperabilität, beispielsweise übergreifende Notfallpläne und Erreichbarkeiten, entwickelt und am Ende umgesetzt werden.

**4. Risikostrategien / -behandlung**
Es bedarf bei kritischen Infrastrukturen, im Gegensatz zur Praxis rein privatwirtschaftlicher Unternehmen, zusätzlich einer Einschränkung bezüglich der Behandlungsoptionen von Risiken. Da die Anforderungen primär dem Schutz der Bevölkerung dienen, sind Bewältigungsstrategien, zumindest für Risiken mit hohem Potential, wie die Risikoakzeptanz oder der -transfer (Versicherung), nicht geeignet.

Cogsecon
AGENTUR FÜR SICHERHEITSMANAGEMENT

Die prinzipielle Toleranz des Ausfalls der Leistungen, durch das Unterlassen von Sicherheitsmaßnahmen, durch Betreiber im Rahmen der Beurteilung der Wirtschaftlichkeit muss eingeschränkt werden.

An dieser Stellekann die Bezuschussung bzw. Förderung von Sicherheitsmaßnahmen durch den Staat den daraus resultierenden finanziellen Mehraufwand der Betreiber reduzieren. Denkbar ist auch ein Deckel für von den Betreibern zu tragenden Kosten zur Umsetzung der Sicherheitsanforderungen. Investitionen darüber hinaus sind durch den Staat zu tragen. Damit würde auch der ungleichen Belastung, aufgrund verschiedener Risiken der Sektoren und betroffenen Organisationen, Rechnung getragen.
Damit Deutschland, angesichts künftiger Schwarzer Schwäne, „vor die Lage“ kommt, eignet sich die Vorgabe für Betreiber, regelmäßig Krisenstabsübungen zu den ermittelten Szenarien durchzuführen. Der Investitionsfokus sollte auf den Sicherheitsmaßnahmen liegen, die einen Effekt bei der Bewältigung verschiedener Szenarien bieten. Eine Vorplanung möglicher Handlungsoptionen sollte ergänzend gefordert werden.

**Frequenz & Monitoring**
Ein wesentliches Element von Resilienz ist die stetige Adaption an sich verändernde herausfordernde Umstände.
Die im KRITIS-Dachgesetz vorgesehene Frequenz der Risikoanalysen mindestens alle 4 Jahre erscheint, im Vergleich mit in der Wirtschaft gängigen jährlichen Analysen und Überarbeitungen bei jeder Änderung der Rahmenbedingungen im Unternehmen, ungewöhnlich lange und kaum ausreichend angesichts der rasanten Veränderungen in der VUCA-Welt. Das kontinuierliche Monitoring und die jährliche Prüfung der Risikobeurteilungen auf Aktualität scheinen auch für kritische Infrastrukturen angemessen.

**Aufsicht & Sanktionen**
Ein weiteres wichtiges Element auf dem Weg zu gut abgesicherten KRITIS-Unternehmen sind die regelmäßigen Kontrollen der Aufsichtsbehörden. Dazu gehören sowohl die Prüfung ob die Risikobeurteilungen den Vorgaben entsprechen und angemessene Sicherheitsmaßnahmen abgeleitet wurden, als auch die operative Umsetzung der Maßnahmen. Dazu sind zu den Dokumentenprüfungen ergänzende vor Ort-Begehungen notwendig. Verstöße sind konsequent zu sanktionieren um die definierten Vorgaben in letzter Konsequenz durchzusetzen.

Die Übernahme der vierten Governance-Aufgabe des Staates, die Befähigung der Unternehmen zur Umsetzung der Vorgaben, könnte durch ein Fort- und Weiterbildungsangebot für die eingebundenen Sicherheitsexperten in den Unternehmen sowie die Bereitstellung von Methoden und Musterdokumenten erfolgen. Experten (u.a. BSKI) könnten Leitfäden, Best Practices zusammenfassen und Betreibern zur Verfügung stellen.
Informationen zu Prüfsiegeln und zertifizierten Dienstleistern unterstützen die kritischen Infrastrukturen weiterführend zusätzlich beispielsweise in der Auswahl geeigneter Errichter.

Nach aktuellem Stand ist dringend eine Reformation des bestehenden Systems in dem sich KRITIS bewegen (staatliche Regulation) erforderlich, dasselbe gilt auch für viele der internen Sicherheitsmanagementsysteme der Betreiber.

Bei der Beschäftigung mit der Thematik wird deutlich, dass nur die Zusammenarbeit staatlicher und privater Akteure, die Umsetzung der wesentlichen Eckpfeiler für die angestrebte Resilienz von KRITIS ermöglicht:

- Fachkundiges Personal im Sicherheitsmanagement und der Prüfung der Unternehmen
- Gute und einheitliche Datenbasis für Risikobeurteilungen
- Vorgaben zur Analyse und
- Bewertung von Risiken
- Einschränkungen für Betreiber
- bei den Risikostrategieoptionen
- fachkundige Umsetzung von Sicherheitsmaßnahmen in den Betrieben und Lieferketten
- regelmäßige objektive Kontrolle der Dokumente und praktischen Umsetzung der Maßnahmen
- Erbringung von Nachweisen bzgl. Verantwortlichkeiten und Kompetenzen sowie dem Schulungsstand der Organisation und zur eingesetzten Technik
- Finanzielle Unterstützung der Betreiber durch den Staat

Coqsecon
AGENTUR FÜR SICHERHEITSMANAGEMENT

Die Resilienz des Gesamtsystems und aller Sektoren ergibt sich aus der Umsetzung der angesprochenen Anpassungen. Diese umfassen sowohl verbesserte innerbetriebliche Prävention- und Reaktionsstrukturen als auch die gesteigerte Interoperabilität im Makrokosmos.

Noch besteht, in der ausstehenden Gestaltung des KRITIS-Dach- und neuen IT-Sicherheitsgesetzes Spielraum die offensichtlichen Lücken im System zu schließen und so dem Ziel von echter Resilienz in den kritischen Infrastrukturen näher zu kommen.

Hoffentlich wird dieser optimal genutzt.

Die Integration Schwarzer Schwäne in das Risikomanagement von Unternehmen

von Franziska Englert
20. Februar 2023

**Was sich geändert hat…**

In der Sicherheitswelt bezeichnet der Begriff „Schwarze Schwäne“ unvorhersehbare und überraschend eintretende Ereignisse mit krisenhaften beziehungsweise katastrophalen Auswirkungen.

Besonderes Merkmal, analog der Tierwelt, ist ihr äußerst seltenes Auftreten, die Eintrittswahrscheinlichkeit wird auf nahe null geschätzt.

Für Sie und mich waren diese Schwarzen Schwäne, bevor wir sie zu Gesicht und zur Bewältigung auf den Schreibtisch bekamen, Geschehnisse wie eine globale Pandemie, Krieg in Europa, global gestörte Lieferketten oder ein drohender Gasmangel.

Die Geschwindigkeit in der wir mit immer neuen Szenarien konfrontiert wurden ist nicht nur atemberaubend, wie der Anblick eines echten schwarzen Schwans, sie treten zu unser aller Überraschung auch noch parallel, quasi im Schwarm, auf.

Die Auswirkungen erstrecken sich über meine berufliche Tätigkeit bis ins Privatleben, wenn Ersatzteile für das Auto seit rund 6 Monaten nicht geliefert werden können, ich mich nach einer vierten Corona-Impfung sehne oder den Feierabend mit zwei Pullis vor einer kalten Heizung verbringe.

Eigentlich waren die Schwäne, unter anderem für Wissenschaftler und namenhafte Experten der jeweiligen Gebiete, immer weiß. Ihr Erscheinungsbild war Bestandteil von Analysen und Studien, ihr Auftauchen lag, wie wir spätestens jetzt alle wissen, absolut im Bereich des Möglichen. Das sollte uns, insbesondere für aktuell diskutierte Zukunftsbilder, sensibilisieren.

**…und weshalb unser Risikomanagement am Denken scheitert.**

Wie in der Einleitung beschrieben, muss heute davon ausgegangen werden, dass bislang undenkbare Szenarien tatsächlich eintreten und sich negativ auf die Unternehmen auswirken.

Zur Vorbereitung werden im Sicherheitsmanagement im ersten Schritt der Risikobeurteilung teilweise noch vereinzelt, unwahrscheinliche aber grundsätzlich denkbare, Zukunftsbilder identifiziert.

Durch die Angabe und Annahme der Eintrittswahrscheinlichkeit von 0 werden sie jedoch, gemäß der Systematik, als für das jeweilige Unternehmen nicht relevant betrachtet.

In den meisten Fällen wird keine fundierte, auf die eigenen Standorte zugeschnittene, Recherche vorgenommen. Dies ist auch bei bisher in klassischen Risikokatalogen geführten Gefahren zu beobachten. Beim Risiko Umwelteinflüsse (Hitze, Hochwasser, Stromausfall,…) werden häufig verfügbare Informationen, z.B. Hochwasserkarten oder der SIDI-Index, nicht abgefragt und ausgewertet. Auch in vorgesehenen jährlichen Aktualisierungen der Risikobeurteilungen wird ein Großteil der Risiken, samt folgender Einschätzung, ungeprüft für die Zukunft übernommen.

Aktuell in der Öffentlichkeit diskutierte Ereignisse wie ein Blackout in Europa, ein Angriff Chinas auf Taiwan oder eine gelungen Störung kritischer Infrastruktur, aus dem digitalen oder physischen Raum, werden in den meisten Sicherheitsabteilungen aktuell nicht konsequent berücksichtigt.

Selbst wenn ein Unternehmen die genannten Risiken als für sich bedeutsam identifiziert hat, ergeben im zweiten Schritt, der Risikoanalyse, die geschätzte Eintrittswahrscheinlichkeit von 0, multipliziert mit dem angenommenen maximalen Schaden, ein Risikopotenzial von null.

Damit werden, gemäß der bisherigen Logik, keine weiteren Maßnahmen zur Senkung des Potenzials durch das Unternehmen ergriffen.

Die Qualität der aktuell durchgeführten Risikoanalysen ist zu großen Teilen abhängig von subjektiven Einschätzungen.

Dabei ist unsere Art im Risikomanagement zu denken aus vielerlei Gründen selbst ein Risiko.

Dieser Umstand ergibt sich aus folgenden Faktoren:

- Wir antizipieren die Zukunft auf Basis der Vergangenheit.

„Das ist uns bisher noch nie passiert“ ist ein, im Sicherheitskontext oft ausgesprochener, Satz der die Beendigung einer Auseinandersetzung mit einem Thema rechtfertigen soll. Dass die Wahrscheinlichkeit des Ereignisses in diesem Fall statistisch dann so hoch wie nie ist wird ausgeblendet.

Bei den meisten Unternehmen ist bis dato alles „gut gegangen“, daraus folgt häufig die Annahme, dies sei auch künftig und für das eigene Unternehmen zu erwarten.

Diese Herangehensweise scheitert in der VUCA-Welt an der Komplexität der Strukturen und Wechselwirkungen. Die kommenden Entwicklungen basieren auf nie dagewesenen Ursachen und nicht zu überblickenden Abhängigkeiten.

- Wir glauben Erfahrung sei der Schlüssel für eine erfolgreiche Zukunft.

Dieses Phänomen greift beispielsweise auch im Recruiting wo nicht das Potenzial eines Bewerbers, sondern seine bisherigen und bis dato zum Erfolg führenden Erfahrungen ausschlaggebend sind. Diverse Studien haben gezeigt, dass dieses Vorgehen zu schlechten Ergebnissen führt. Beispielsweise sind Führungskräfte aus der zweiten Reihe, die weder vorher anderswo einen CEO-Posten innehatten, noch aus der Ebene direkt unter dem CEO rekrutiert werden, in der CEO-Position (wirtschaftlich) deutlich erfolgreicher, als auf diesem Posten erfahrene Kandidaten.

Wie bei Bewerbern ist das Potenzial eines Risikos, die für Unternehmen relevante Komponente, nicht die bisher beobachtbaren Auswirkungen.

- Wir vergessen tiefgreifende Situationen aus der Vergangenheit, die uns an den Rand der Handlungsfähigkeit gebracht haben.

Wir erinnern die Situationen, angesichts einer mehr oder weniger erfolgreichen Bewältigung, als weniger unangenehm und riskant, als wir sie zum Zeitpunkt des Ereignisses empfunden haben. Hier kann beispielsweise die Corona-Krise angeführt werden. Deren Bewältigung (die nicht allen gelang) wägt uns in fragiler Sicherheit. Krisen sind jedoch nicht vergleichbar, was ihre Dynamik (Corona war eine langsame Krise, die den Unternehmen genug Zeit für Anpassung und Reaktion lies) und Auswirkungen angeht. Reputationskrisen und deren Auslöser werden häufig beispielsweise nicht betrachtet.

- Wir schreiben Erfolge unserem Können und Misserfolge unglücklichen Zufällen zu. Das bildet nicht die Realität ab und leitet uns bei Bewertungen vergangener und darauf aufbauenden künftigen Entscheidungen in die Irre.

- Wir leben nach dem Pipi-Langstrumpf-Prinzip (PLP-Prinzip).

Wir schaffen uns in Gedanken die Realität die wir uns wünschen und die unsere Meinungen und Handlungen positiv bestätigt. Dazu blenden wir beliebig Erlebtes, Fakten und Lehren aus den Fehlern anderer aus. Dafür beziehen wir immer die in unsere Planungen ein, die unserer Einschätzung am ehesten entsprechen.

- Wir überschätzen unsere Fähigkeit komplexe Situationen schnell durchdenken zu können.

Je routinierter und erfahrener wir sind, desto eher erliegen wir dem Irrglauben einfache und schnelle Lösungen für komplexe Probleme finden zu können.

Dabei ist zwischen zwei Denkweisen zu unterscheiden, wovon die zweite für komplexe Probleme, Strategie und Zukunftsplanung geeignet ist (siehe Kahnemann: Schnelles Denken, langsames Denken).

•System 1: Schnell, automatisch, immer aktiv, emotional, stereotypisierend, unbewusst

•System 2: Langsam, anstrengend, selten aktiv, logisch, berechnend, bewusst.

- Die Angst vor Ungewissem lässt uns in gewohnter Routine verharren.

Auch wenn veränderte Maßnahmen unter Umständen deutlich Erfolg versprechender sind als aktuelle, meiden wir die Unsicherheitskomponente die jeder Entscheidung anhaftet. Wir sichern den Status quo und leben mit den uns, immerhin bekannten, Nachteilen.

- Wir ergreifen die Maßnahmen die schnellen Erfolg und Belohnung versprechen.

Dafür stellen wir auch deutlich erfolgversprechendere und damit relevantere Maßnahmen zurück, die sich allerdings erst in Zukunft auszahlen. Das ist einer der Gründe weshalb Präventivmaßnahmen im Sicherheitsmanagement häufig zurückgestellt und sich im Zweifel auf (teurere) Reaktionsmaßnahmen in der Zukunft verlassen wird.

Dass diese unter Umständen nicht ausreichen um die gesetzten Schutzziele noch zu erreichen, wird vielfach nicht berücksichtigt.

Wenn auf Basis falscher Annahmen und klassischer Denkfallen in Risikobeurteilungen keine oder falsche Sicherheits- und Präventionsmaßnahmen für die angesprochenen außergewöhnlichen Szenarien ergriffen werden, ergeben sich unerwünschte Sicherheitslücken.

Diese können, durch das hohe Schadenpotential im Ereignisfall, die Existenz des Unternehmens bedrohen.

Umso relevanter ist es, dass im Sicherheits- und Risikomanagement verwendete Methoden und Analysen unsere kognitiven Schwächen berücksichtigen und systematisch ausgleichen.

**Erste Integration ins Risikomanagement mit der Szenario-Technik…**

Es braucht neue Ansätze für Unternehmenssicherheiten um sicher zu stellen, dass die in Zukunft häufiger auftretenden „Schwarzen Schwäne“, in den Risikobeurteilungen der Unternehmen angemessen berücksichtigt werden.

Dafür sind Anpassungen von der Identifikation über die Analyse, bis zur Risikobewertung und abschließenden Risikobehandlung notwendig.

Die von Sicherheitsabteilungen ergriffenen Sicherheitsmaßnahmen und damit die Allokation des Budgets und der anderen Ressourcen basieren auf den Ergebnissen der Risikobeurteilungen (Identifikation, Analyse, Bewertung). Je valider die einzelnen Schritte umgesetzt werden, desto erfolgreicher sind die nachfolgenden Präventions- und Reaktionsmaßnahmen eines Unternehmens.

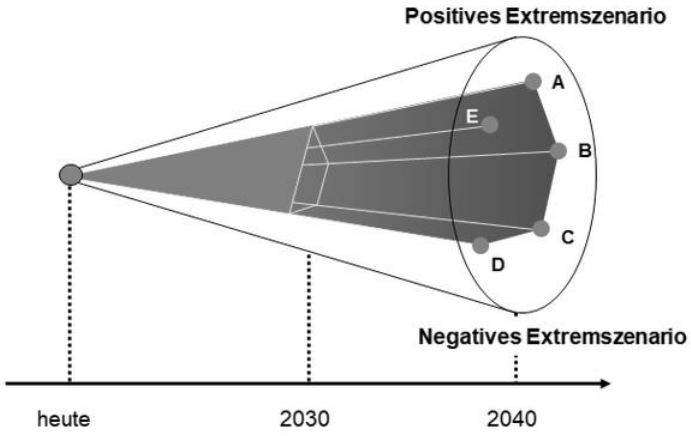
In der Geschäftsstrategieentwicklung und Sicherheitspolitik hat die Szenario-Technik als Methode zur strategischen Vorausschau bereits Einzug gehalten.

Die explorative Methode verschafft den Anwendern einen Überblick über Variationen, Risiken und Chancen der verschiedenen möglichen zukünftigen Entwicklungen und zeigt damit die Handlungsspielräume und Leitplanken auf. Damit eignet Sie sich auch zur Anwendung im Kontext der Unternehmenssicherheit.

Übersicht:

- Beteiligte
  Sicherheitsrelevante Abteilungen (Unternehmenssicherheit, IT-Sicherheit, Arbeitssicherheit/Brandschutz)
- Umsetzung
  z.B. Workshop
- Ergebnis
  Basis für zu ergreifende Sicherheitsmaßnahmen (Entscheidungsvorlage Unternehmensführung | Leiter Unternehmenssicherheit) und Input für die Sicherheitsstrategie (einschl. strategischer Planung)

1. Risikoidentifikation:
   Ausgangspunkt ist die Identifikation Schwarzer Schwäne (z.B. Blackout, Angriff Chinas auf Taiwan, Hitzewelle in Deutschland, Spionageangriff)
2. Risikoanalyse und -bewertung:
   Für jedes Szenario werden drei Fälle (Erscheinungsformen) als Betrachtungsrahmen entwickelt: Best-Case, Angenommener Trend-Case bzw. Base-Case, Worst-Case




*Bildquelle: Dr. Fleig (www.business-wissen.de)*

Die Grundlage für die Identifikation und Bewertung der angenommenen Entwicklungen (Cases) basiert auf möglichst diversen und tiefgehenden Recherchen (Studienergebnisse, Expertenmeinungen, …) und ihrer strukturierten Auswertung.

Best- und Worst-Case (siehe A und D) bilden die sehr unwahrscheinlichen Varianten und damit die Ränder des Betrachtungsfelds ab.

In der Mitte des Trichters liegt die, als am wahrscheinlichsten angenommene, Trendentwicklung (siehe B) des Szenarios.

Je weiter der Blick in die Zukunft gerichtet wird, desto mehr Unsicherheitsfaktoren und Abhängigkeiten bestehen für die Entwicklung des Gesamtszenarios und damit der einzelnen angenommenen Fälle.  Beachten Sie bei Ihrer Case-Planung auch die, in Teil 2 vorgestellten, Denkfallen, die Ihnen auf dem Weg zu guten Ergebnissen im Wege stehen.

-Beispiel Blackout/flächendeckender Stromausfall

Folgende Case-Annahmen sind, aus heutiger Sicht, denkbar:

- Worst-Case: Deutschlandweiter, ggf. sich auf EU-Nachbarstaaten erstreckender, Blackout (bis zu 2 Wochen)
- Trend-Case: Blackout/Stromausfall bis 3 Tage an einem Unternehmensstandort und dem umliegenden Stadtgebiet
- Best-Case: Regional begrenzter Blackout/Stromausfall für maximal 12 h in einem Bundesland / Landkreis, in dem das Unternehmen einen Standort hat

Hätten Sie, mit Ihrem Wissen und der Recherche, andere Cases erstellt ?

Vermutlich. Hier wird eine der Schwächen der Methode deutlich, sie ist maximal abhängig von den zu Grunde liegenden Rechercheergebnissen und der subjektiven Bewertung der Wahrscheinlichkeiten des Analysten.

Nichtsdestotrotz ist die Annahme der oben genannten Cases, im Szenario Blackout / Stromausfall, aktuell unsere Empfehlung in der Corsecon-Beratungspraxis. Sie basieren auf vertieften Recherchen, Expertengesprächen (Netzspezialisten, Elektroingenieure und Sachverständige) und Fallstudienauswertungen.

3. Risikobehandlung:

Zu Beginn werden die Umgebungsbedingungen und zu erwartenden Einflüsse auf das eigene Unternehmen, vorwiegend im Trend-Case, entlang eines Zeitstrahls vom Ereigniseintritt bis Ereignisende (so im Szenario definierbar) eruiert. An Tag eins eines Stromausfalls im Sommer ist mit anderen Einflüssen und Ereignissen zu rechnen, wie am vierten Tag eines Stromausfalls im Sommer. Auf diesem Weg werden Zusatzinformationen generiert, die Hinweise für die Ausgestaltung der Sicherheitsmaßnahmen liefern.

Dazu zählen u.a.:

- Leistungsfähigkeit der Behörden, die für die öffentliche Ordnung sorgen (z.B. Möglichkeiten der Polizei durch Präsenz flächendeckend Plünderungen zu vermeiden, Unterstützung durch die Feuerwehr in akzeptablem Zeitrahmen erwartbar,…)

- Szenariospezifische Faktoren wie Trinkwasserverseuchung (Legionellen), Bargeldmangel, Beschlagnahmungen von Eigentum durch Behörden, Kraftstoffmangel, …
- Arbeitsbereitschaft der Mitarbeiter im zeitlichen Verlauf
- In welchen Fällen (geographische Betroffenheit) ist nicht nur ein, sondern mehrere und für den Betrieb wichtigere oder unwichtigere Unternehmensstandorte betroffen ?

Im nächsten Schritt werden Einzelrisiken des Szenarios identifiziert und analysiert. Der Fokus liegt hierbei auf dem Trend-Case.

Identifikation der Einzelrisiken eines flächendeckenden Stromausfalls:

- Aufzüge bleiben stecken
- Sicherheitstechnik funktioniert nicht mehr (BMA, EMA, Zutrittskontrolle,…)
- BOS stehen nur eingeschränkt und nicht wie gewohnt zur Verfügung
- Kommunikation über reguläre Netze und das Internet ist nicht möglich
- Tankstellen funktionieren nicht
- Es wird bei Zahlungen nur noch Bargeld akzeptiert, dieses kann aber nicht mehr abgehoben werden
- Plünderungen
- Überhitzung von Räumen/Tanks durch ausgefallene Kühlung

Nach der gängigen Analyse (Eintrittswahrscheinlichkeit x Schadenausmaß) & Bewertung (qualitativ/quantitativ in Matrix) folgt die Risikobehandlung. Es werden angemessene (wirtschaftliche) Sicherheitsmaßnahmen (personell, technisch, organisatorisch) zur Minimierung, Überwälzung oder dem Ausschluss der ermittelten konkreten Gefährdungen ergriffen.

Differenziert werden kann grob zwischen nachstehenden Sicherheitsmaßnahmen, die zu verschiedenen Zeitpunkten mit unterschiedlichem Aufwand vorbereitet und umgesetzt werden. Ihr Schwerpunkt liegt entweder auf Prävention oder Reaktion und im Optimalfall wird eine Kombination aller Maßnahmen umgesetzt.

➡️Konkrete Sicherheitsmaßnahmen für die einzelnen Cases (Schwerpunkt Trend-Case)

Planung und Umsetzung von Präventionsmaßnahmen und die Vorbereitung von Reaktionsmaßnahmen (z.B. die Beschaffung von Taschenlampen/Anbringung von Leuchtstreifen für die Evakuierung von Gebäuden bei Dunkelheit, Schulung von Personal, Beschaffung von Satellitentelefonen/Vereinbarung von Treffpunkten zur persönlichen Abstimmung)

➡️Betriebliche Kontinuitätsplanung bzw. Business Continuity Management (für das Szenario allgemein, konkret für die 4 verschiedenen BC-Szenarien: Ausfall Personal, Infrastruktur, Dienstleister, IT)

- Erstellung von Notfallplänen (organisatorisch) zur Fortführung des Betriebs (Notbetrieb) und Wiederherstellung des Normalbetriebs für den Ausfall betriebsnotwendiger Ressourcen

- Ableitung technischer Konzepte (Notstromkonzept beinhaltet die Einrichtung eines Notstromnetzes und die Dimensionierung von Notstromanlagen (Installation/Nutzung von PV-Anlagen als Insellösung mit LI-Speicher oder Notstromaggregate))

➡️ Erstellung eines Krisenplans (für das Szenario allgemein)

Der Plan beinhaltet vorbereitete Optionen und Handlungsleifäden für den Notfall-/Krisenstab:

- Notwendige Sofortmaßnahmen in Form von Checklisten (Notablass der Aufzüge, Brandwache durch Mitarbeiter, Aufstockung Sicherheitspersonal, interne Kommunikation, …)
- Mittelfristige Maßnahmenoptionen (Kontaktaufnahme mit Behörden, …)
- Eskalationsschwellen

Im Normalfall geraten klassische BC-Pläne bei Schwarzen Schwänen, genauer den Worst-Cases und teilweise auch Trend-Cases, an ihre Grenzen. Die Hauptursache liegt darin, dass bei vielen Schwarzen Schwänen nicht nur ein BC-Szenario eintritt, für das die Notfallpläne konkrete Maßnahmen zur Überbrückung und Wiederherstellung der Ressourcen vorsehen, sondern eine Kombination aus mehreren BC-Szenarien.

Dies lässt sich am Beispiel Blackout bzw. einem einfachen Stromausfall (Baggerbiss) nachvollziehen. Es ist mit der folgenden Kombination der BC-Szenarien zu rechnen:

- Ausfall von Sicherheitsdienstleistern
- Personalausfall (Mitarbeiter erscheinen nicht zur Arbeit)
- Ausfall IKT (IT-Systeme, Mobilfunk)
- Ausfall Infrastruktur (Gebäude, Sicherheitstechnik, …)

Die dezentrale Steuerung in den Abteilungen des Unternehmens reicht nicht aus um die komplexen Auswirkungen für das Unternehmen zu bewältigen. Für diese Fälle greift das Krisenmanagement (zentral mit dem Krisenstab) zur Minimierung von Schäden und der schnellen Rückkehr in den Normalbetrieb.

Bisher wurden die Schwarze Schwäne-Szenarien, mit dem Argument der Unwahrscheinlichkeit, ausgeklammert und in den meisten Unternehmen und ihren Sicherheitsabteilungen generell nicht ernsthaft betrachtet. In Folge traf die Corona-Pandemie und der russische Angriffskrieg Politik, Wirtschaft und Gesellschaft gänzlich unvorbereitet und kostete viele Institutionen die Existenz oder bedeuten massive Verluste.

Die Szenario-Technik bietet einen ersten Ansatz zur Integration Schwarzer Schwäne in das Risikomanagement aller Sicherheitsabteilungen. Im Kern stützt sie sich auf die gängige und bekannte Methodik der Risikoanalyse.

Neu und von Vorteil ist, dass durch die Anwendung der Technik auch globale, standortübergreifende Risiken abseits der gängigen Gefahrenkataloge betrachtet werden und Sicherheitsverantwortliche sich frühzeitig mit möglichen großen Sicherheitsherausforderungen der Zukunft auseinandersetzen.

Dadurch entsteht ein neuer Horizont, zwischen Worst- und Best-Case, der gleichzeitig die Spanne des Einsatzes finanzieller und personeller Ressourcen für die Sicherheit von morgen abbildet. In

Folge werden unternehmensindividuelle Präventions- und Reaktionsmaßnahmen ergriffen und wenn nötig mittel und langfristig Anpassungen in der Sicherheitsorganisation vorgenommen (Sicherheitsstrategie).

Die Qualität der Methode zur Risikobeurteilung ist (zu) stark von den subjektiven Schlussfolgerungen Einzelner abhängig. Zum Ausgleich eignen sich standardisierte Verfahren für die Identifikation Schwarzer Schwäne (Bindung an Trend- und Sicherheitsforschung) sowie qualifizierte Analysen und Bewertungen anhand einheitlicher Parameter.

Die aktuelle Zeitenwende erfordert Anpassungen der bisherigen Denk- und Arbeitsweisen, dies gilt auch für Unternehmenssicherheiten.

**… und die Königsdisziplin – Risikobeurteilungen mit dem Plausibilitätsansatz**

Als extrem unwahrscheinlich galt bis vor Kurzem noch das Szenario, das sich jüngst in Frankfurt abspielte. Das Unternehmen, aber auch auf die Dienstleistungen angewiesenen Nutzer, waren darauf nicht angemessen vorbereitet, die Lage eskalierte innerhalb weniger Stunden. Die Durchtrennung eines einzelnen zuführenden Glasfaserkabels eines Rechenzentrums einer großen deutschen Fluggesellschaft hat zu deutlichen Auswirkungen auf den Flugverkehr, nicht zuletzt durch die Schließung eines der größten deutschen Flughäfen, geführt. Ein Rechenzentrum wird im Bereich der kritischen Infrastruktur üblicherweise von drei redundanten Kabeln unabhängiger Telekommunikationsanbieter versorgt. Wie die Durchtrennung eines Einzelnen bereits diese Auswirkungen haben konnte ist selbst Experten ein Rätsel.

Denkbar war die Situation die sich abgespielt hat zwar grundsätzlich, sie galt nur als extrem unwahrscheinlich. Bei der Risikoanalyse der meisten Unternehmen fallen diese Art der Szenarien aktuell in den meisten Fällen aus diesem Grund heraus.

Die Ursache liegt darin, dass selbst das angenommene extrem hohe Schadenpotential, multipliziert mit der (fälschlicherweise) angenommenen Eintrittswahrscheinlichkeit nahe 0, ein sehr kleines Risikopotential für ein solches Ereignis ergibt.

Nach bisheriger Logik, für die Ergreifung wirtschaftlicher Maßnahmen zur Risikobehandlung, werden die Szenarien spätestens ab diesem Punkt nicht weiter betrachtet, Investitionen in Sicherheitsmaßnahmen bleiben in Folge aus.

Dass diese Szenarien dennoch betrachtet werden sollten, weil ihr Schadenpotential maximal hoch ist, zeigt der beschriebene Fall ebenso wie die unwahrscheinliche globale Pandemie die hinter uns liegt oder der Angriffskrieg Russlands auf die Ukraine der das Potential hat die Weltordnung auf ungeahnte Weise ins Wanken zu bringen.

Der Plausibilitätsansatz, ursprünglich für die Erstellung besserer Geschäftsstrategien eingesetzt, bietet auch aus Sicherheitsperspektive erhebliches Potenzial.

Mit ihm lassen sich unwahrscheinliche zukünftige Szenarien und Risikokombinationen – die Schwarzen Schwänen, in die heutigen Risikobeurteilungen integrieren. Möglich wird dies, weil mit dem Ansatz grundsätzlich alle denkbaren und damit plausiblen Extremszenarien in den Risikobeurteilungszyklus einbezogen werden, unabhängig ihrer Eintrittswahrscheinlichkeit.

Der Ansatz ist weniger als klassische Methode, wie beispielsweise die bereits vorgestellte Szenariotechnik, zu verstehen sondern als neuer Denkansatz, der es in der heutigen VUCA-Welt ermöglicht zukunftsgerichtetere Entscheidungen vorzubereiten. Neue Gefahren werden mitgedacht, in die Sicherheitsstrategie und operative Planung einbezogen und Unternehmen damit entsprechend systematisch anpassungsfähig.

Risikobeurteilungen bestehen aus den Schritten

- Risikoidentifikation
- Risikoanalyse
- Risikobewertung

und sind die Basis für die Risikobehandlung, die Ergreifung geeigneter Risikostrategien (Minimierung, Akzeptanz, Vermeidung, Überwälzung) zur Bewältigung der Risiken (konkrete Sicherheitsmaßnahmen innerhalb der Strategie).

Eine Möglichkeit den Plausibilitätsansatz in den einzelnen Schritten der gängigen Risikobeurteilungen zu nutzen, die Integration Schwarzer Schwäne zu ermöglichen und Risikobeurteilungen auch für Extremszenarien nutzbar zu machen, ist im Folgenden dargestellt.

Schritt 1 – Schwarze Schwäne identifizieren

Es gilt alle Zukunftsszenarien zu identifizieren, deren Eintreten in Zukunft denkbar und damit plausibel erscheinen und die massive Auswirkungen für die Existenz bzw. Leistungserbringung des Unternehmens erwarten lassen.

Eine grundlegende Recherche zu möglichen Entwicklungen in den Feldern Politik, Gesellschaft, Technik und Wirtschaft bildet den Ausgangspunkt. Dafür können Einschätzungen staatlicher Stellen wie dem TAB (Büro für Technikfolgenabschätzung), Publikationen und Aussagen von Wissenschaftlern sowie eigene Umfragen herangezogen werden. Auch ein Blick auf die vom Zukunftsinstitut ermittelten Megatrends eröffnet einen neuen Horizont. Nicht nur bekannte Katastrophenbilder bedrohen Unternehmen mit ihren Auswirkungen, sondern auch disruptive Technologien, die beispielsweise von (Cyber-)Kriminellen genutzt werden können (KI, Quantencomputing).

Aktuell diskutierte Zukunftsbilder, die für viele Unternehmen massive Auswirkungen mit sich bringen würden, sind u.a.:

- Blackout in Deutschland
- Längerer Wegfall kritischer Infrastruktur nach Unfall oder gezieltem Angriff
- Hitzewelle in Deutschland mit Trinkwassermangel

Je nach Branche und Unternehmensstruktur sind weitere Ereignisse relevant:

- Angriff Chinas auf Taiwan
- Weitere Eskalation des Ukraine-Kriegs

Die Identifikation der Schwarzen Schwäne erfolgt im Optimalfall bereits auf strategischer Ebene, beispielsweise bei der Erstellung der Geschäfts- und Sicherheitsstrategie, denn ihre Betrachtung hat auch Auswirkungen auf die strategische Ausrichtung des Unternehmens. In diesem Fall kann

das Sicherheitsmanagement die betrachteten Szenarien aufgreifen und für die weiteren Schritte der Risikobeurteilung berücksichtigen.

Jedes Szenario wird unternehmensindividuell auf mögliche primäre und sekundäre negative Auswirkungen geprüft. Diese können im Wesentlichen in Personen– oder finanzielle Schäden sowie eine Unterbrechung der Betriebskontinuität unterteilt werden.

Der Fokus bei der Auswahl der Extremszenarien liegt, mit der Verfolgung des Plausibilitätsansatzes, nur auf dem Schadenausmaß und nicht auf der Eintrittswahrscheinlichkeit. Damit wird grundsätzlich ein hohes Risikopotential für das Unternehmen angenommen, was einer Regulation im Anschluss bedarf.

Der erste Schritt der Integration schwarzer Schwäne in die Risikobeurteilungen ist damit erfolgt.

Ist ein Szenario denkbar, also plausibel und hat es im Eintrittsfall Auswirkungen auf das Unternehmen wird es in den folgenden Schritten näher betrachtet und vorbereitende Maßnahmen ergriffen.

Schritt 2 –Risikoanalyse und -bewertung mit neuen Ansätzen

Die Basis der Planung für Sicherheitsprojekte und -maßnahmen einer Unternhemenssicherheit sind im Wesentlichen Risikoanalysen -bewertungen. Ihre Qualität und Aktualität bestimmt damit den Schutz des Unternehmens.

Im Regelfall werden Gefahrenkataloge, wie der des BSI, mit einer Auflistung von (aktuell 47) gängigen Risiken herangezogen. Alternativ oder ergänzend werden Risiken von Unternehmen zu BC-Szenarien (Ausfall der Prozessressourcen Dienstleister, IT, Personal oder Infrastruktur) zusammengefasst, auf die sich Unternehmen mit Notfallplänen (BC-Pläne) vorbereiten.

Beide Varianten geraten, bei der Betrachtung von Extremszenarien an ihre Grenzen. Die Kombination auftretender Risiken bzw. der parallele Ausfall mehrerer Prozessressourcen lässt sich nicht mit den bisherigen Methoden analysieren und bewerten.

Ein anschauliches Beispiel ist das Risiko Hochwasser, welches als Elementargefahr im Gefahrenkatalog auftaucht und von Unternehmen standortindividuell bewertet wird.

Das Hochwasser im Ahrtal hat Behörden und Unternehmen jedoch eindrücklich gezeigt, dass bei einem solchen Szenario diverse, bisher nicht betrachtete, Risiken hinzukommen und in Kombination auftreten. Hier sind beispielsweise die eingeschränkte Unterstützung der Behörden, Plünderer die als Helfer getarnt sind oder die Überlastung der Versicherer bei der Schadenregulierung im Nachgang zu nennen.

Daher ist es sinnvoll ergänzend zu den üblichen Einzelrisikoanalysen (z.B. Standortanalysen) Schwarze Schwäne, also Situationen bei denen Unternehmen mit einer Vielzahl an Risiken, u.U. an mehreren Standorten parallel, konfrontiert sind, zu analysieren.

Zur Ermittlung der Einzelrisiken eines Extremszenarios ist deren spezifische Auflistung erforderlich. Es empfiehlt sich die Darstellung der Risiken entlang eines Zeitstrahls. Dabei werden alle denkbaren Risiken, ebenfalls nach dem Plausibilitätsansatz, einzeln und in ihrer Kombination

berücksichtigt und analysiert. Dazu zählen auch die auf Grund von Wechselwirkungen oder in Folge von Kaskadeneffekten auftreten.

Auch in diesem Schritt steht erneut das Schadenausmaß und nicht die Eintrittswahrscheinlichkeit im Mittelpunkt. Risiken, die gravierende Auswirkungen haben können, wird ein hohes Risikopotential zugeschrieben. Damit ist sichergestellt, dass im nächsten Schritt geeignete Maßnahmen (Risikostrategien) ergriffen werden und das Unternehmen am Ende angemessen auf die Schwarzen Schwäne vorbereitet ist.

Schritt 3 – Die Realoptionsanalyse im Rahmen der Risikobehandlung

Für alle Risiken mit hohem Risikopotential sind die bereits angesprochenen Risikostrategien festzulegen um mit zugeordneten Sicherheitsmaßnahmen Risiken zu regulieren. Bei Schwarzen Schwänen sind die Strategieoptionen Risikovermeidung und Risikoakzeptanz im Regelfall keine Option. Auch die Versicherung von Risiken gerät in den betrachteten Fällen schnell an ihre Grenzen, durch den Ausschluss eben dieser Szenarien (höhere Gewalt) in den Versicherungsbedingungen.

Der Fokus der Unternehmen sollte deshalb auf der Risikominimierung liegen um das Schadenausmaß zu reduzieren. Dies kann über Maßnahmen erfolgen, die entweder die Eintrittswahrscheinlichkeit des Szenarios (bei Schwarzen Schwänen nicht möglich) oder das Schadenausmaß zu Gunsten des Unternehmens beeinflussen. Letzteres kann durch präventiv ergriffene Maßnahmen (Krisenstabsschulungen, Einrichtung von Georedundanzen, Beschaffung von nützlicher Technik im Vorfeld) oder Reaktionsmaßnahmen (vorübergehende Geschäftsaufgabe in einem Land oder einer Region, Budgetbereitstellung für Sofortmaßnahmen) erfolgen.

Es wird in unterschieden, die im Vorfeld entwickelt werden.

Die Realoptionsanalyse führt zur Entwicklung umfangreicher Maßnahmensets mit technischen, organisatorischen und personellen Optionen, die beispielsweise in einem Krisenplan für das jeweilige Ereignis zusammengefasst werden.

Die Umsetzung aller analysierten Realoptionen ist zum einen aus Kostengründen und zum anderen aufgrund der Ungewissheit welche Optionen im tatsächlichen Szenario wirklich einen Effekt erzielen können, nicht sinnvoll.

Die nachgelagerte Kosten-Nutzen-Analyse legt deshalb den Fokus darauf welche Maßnahmen in mehreren der ermittelten Schwarzer-Schwan-Szenarien Effekte erzielen können. Investitionen in diesen Bereichen haben den höchsten Effekt, unabhängig davon welches Szenario am Ende tatsächlich eintritt.

Zudem wird in die Realoptionsanalyse miteinbezogen welche Pläne das Unternehmen allgemein verfolgt und ob die entwickelten Realoptionen gegebenenfalls in diesem Rahmen einen Beitrag leisten können, deren Umsetzung also auch im regulären Betrieb einen Mehrwert bietet.

Die Realoptionsanalyse befähigt zu fundierten Investitionsentscheidungen, sie verpflichtet nicht dazu. Die Unternehmensführung kann sich mit der entsprechenden Allokation von Budget und Umsetzung konkreter Maßnahmen zielgerichtet auf existenzbedrohende Szenarien vorbereiten.

Der Pool an übrigen Optionen, die aktuell kein adäquates Kosten-Nutzen-Verhältnis aufweisen, ermöglicht in Zukunft, bei einer Veränderung der Lage und Prognosen, jederzeit eine Umsetzung vorgeplanter effektiver Maßnahmen.

Schritt 4 – Prognostik für resiliente Unternehmen

Die gängige Frequenz der Risikobeurteilungen, einmal jährlich, ist aufgrund der vielfältigen, sich heute schnell ändernden Einflussfaktoren, auf die Entstehung, den tatsächlichen Ereigniseintritt und die Ausmaße Schwarzer Schwäne zu gering.

Aufgrund der Komplexität der betrachteten Situationen und Interdependenzen ist eine fortlaufend angepasste Prognose sinnvoll. Auf deren Basis kann die Einstellung laufender, die Ergreifung vorgeplanter oder die Neuentwicklung geeigneter Maßnahmen in der Vorbereitung auf Schwarze Schwäne erfolgen.

Die kontinuierliche Analyse von Veränderungen (Informationsgehalt), welche das Ereignis wahrscheinlicher werden lassen oder einen detaillierteren Überblick über zu erwartende Schäden ermöglichen, ist die Voraussetzung für eine gelungene Prognose.

Um die kontinuierliche Risikobeurteilung handhabbar zu machen, werden für das Monitoring des erwarteten Eintrittszeitpunkts und des zu erwartenden Schadenausmaßes Kennzahlen und Grenz- sowie Schwellenwerte definiert. Diese können quantitativ und qualitativ (z.B. bestimmte Äußerungen politischer Funktionsträger) sein.

Eingehende Informationen werden, beispielsweise durch die Sicherheitsabteilung, analysiert und ihr Einfluss auf die Kennzahlen geprüft.

Je nachdem welche Kennzahlen sich verändern und ob festgelegte Grenz- und Schwellenwerte überschritten werden sind, nach dem Ampelschema, verschiedene Folgeschritte einzuleiten. Diese reichen von der Aktualisierung der Risikobeurteilung bis hin zur Auslösung der Umsetzung bereits im Vorfeld geplanter Maßnahmen.

1. Information hat keinen Einfluss auf die Kennzahlen/festgelegten Grenzwerte, es handelt sich um eine bekannte Informationskategorie

   🟢 –> kein Veränderungsbedarf bei den Sicherheitsmaßnahmen

2. Information ist grundlegend neu oder verändert die Kennzahlen so, dass sie einzelne Grenzwerte tangieren

   🟠 -> Sicherheitsmaßnahmen prüfen und anpassen, ggf. umsetzen

   - Information näher analysieren und ggf. neue Kennzahl einführen
   - Risikobeurteilung aktualisieren und Realoptionsanalyse ergänzen
   - Vordefinierte Sicherheitsmaßnahmen vorbereiten/umsetzen

3. Information verändert die Kennzahlen deutlich, mehrere Grenzwerte werden überschritten

   🔴-> Sicherheitsmaßnahmen umsetzen/korrigieren, Krisenmanagement aktivieren

   - Vorbereitete Maßnahmen umsetzen
   - Kurskorrektur des Unternehmens erforderlich

Unternehmen die Informationen zu den, für sie relevanten Schwarzen Schwänen, kontinuierlich analysieren und systematisch in Handlungsschritte übersetzen, stellen sich kontinuierlich die Leitfrage „Sollten wir unseren Kurs ändern ?“.

Damit verschaffen Sie sich entscheidende Zeitvorteile zur Vorbereitung und Umsetzung von Maßnahmen.

Zusammenfassend lässt sich festhalten:

Folgen Sie dem Grundsatz: Was denkbar ist gilt als plausibel und damit als relevant.

Zur Integration schwarzer Schwäne in die Risikobeurteilung der Unternehmen ist es sinnvoll,

- im Optimalfall auf strategischer Ebene, die, das Unternehmen betreffenden Zukunftsszenarien zu identifizieren (Schritt 1)
- auf Managementebene (Abteilung Unternehmenssicherheit) die Kombination der Einzelrisiken zu bestimmen (Schritt 2)
- um im Anschluss angemessene Sicherheitsmaßnahmen entwickeln und zum richtigen Zeitpunkt umsetzen zu können (siehe Schritt 3 und 4).

Der Plausibilitätsansatz lässt in den verschiedenen Schritten des Risikomanagements offener über neue Gefahren unserer Zeit und Zukunft nachdenken und Risiken realistischer erfassen.

Mit der beschriebenen Vorgehensweise folgen Unternehmen dem im Risikomanagement empfohlenen Worst-Case Ansatz. Es wird, zur adäquaten Vorbereitung des Unternehmens, zunächst sowohl der ungünstigste Eintrittszeitpunkt wie auch das maximale Schadenausmaß künftiger Szenarien angenommen. Auf dieser Basis können dann fundierte Planungen erfolgen und Investitionen bewertet werden.

Dieses Vordenken ist wichtiger Bestandteil einer neuen Sicherheitskultur in Unternehmen. Auf alleiniger Basis der Erfahrungen der Vergangenheit lassen sich viele Herausforderungen der Zukunft nicht mehr bewältigen.

Die Fähigkeit des Unternehmens sich stetig an veränderte Rahmenbedingungen anzupassen wird als Resilienz bezeichnet. Sie ist die Voraussetzung für die Erreichung der Geschäftsziele, die die Unternehmenssicherheit unterstützt. Frühzeitig zu erkennen wann aus Unbekannten Bekannte werden und in Folge angemessene Schritte abzuleiten ist nur durch kontinuierliches Monitoring und konsequentes Sicherheitsmanagement möglich. Dabei muss auch der Kreislauf aus Planung,

Handlung, Prüfung und Anpassung in den Unternehmen beschleunigt werden. Nur so können Unternehmen „vor die Lage“ kommen und die Existenz auch in Extremszenarien sichern.

Mit der Dokumentation der Schritte 1-3 und Umsetzung des vierten Schritts erfüllen Unternehmen zudem die gesetzlichen Anforderungen zur Risiko- und Krisenfrüherkennung sowie dem Krisenmanagement.

*Quellen: HBM 10/22, BAKS, Haufe*

Weitere Fachartikel unserer Experten erhalten Sie mit unserem Sicherheitsbriefing.