TÜV AUSTRIA

AKADEMIE

Tom Vogt

# Risikomanagement in der Cybersecurity

TÜV AUSTRIA Fachverlag

# Impressum

## Risikomanagement in der Cybersecurity

1. Auflage
ISBN 978-3-903255-14-2

Autor: Tom Vogt, CISM, Senior Information Security Architect,
SPP, TÜV AUSTRIA Group

**Medieninhaber**

TÜV AUSTRIA AKADEMIE GMBH
Leitung: Mag. (FH) Christian Bayer, Rob Bekkers, MSc BSc
2345 Brunn am Gebirge, TÜV AUSTRIA-Platz 1
+43 5 0454-8000
akademie@tuv.at | www.tuv-akademie.at

Produktionsleitung: Mag. Judith Martiska
Layout, Satz und Grafiken: Markus Rothbauer, office@studio02.at,
Lukas Drechsel-Burkhard, luc@luc.at
Herstellung: druckwelten.at
Cover: Adobe Stock



Zur leichteren Lesbarkeit wurde die männliche Form gewählt. Selbstverständlich gelten alle Formulierungen für Männer und Frauen in gleicher Weise.

# Schutz im Cyberraum


Österreich wird gerne als eine „Insel der Seligen“ bezeichnet. Ein neutraler Staat, der als Mitgliedsstaat der Europäischen Union im größten Friedensprojekt der Welt eingebettet ist, umgeben von Freunden, prosperierend und sicher. Doch was für die reale, uns greifbare Welt sicherlich weitgehend richtig ist, gilt leider nicht für die virtuelle Dimension. Die Besonderheit dieser virtuellen Dimension, dem sogenannten Cyberraum, ist, dass hier keine klassischen Grenzen im Sinne einer Staatsgrenze gelten. Bedrohungen sind daher global zu betrachten. Unterschiedlichste Akteure halten sich oftmals nicht an Staatsgrenzen, noch weniger an Völkerrecht und leider auch nicht an nationale Rechtssysteme. Derzeit fehlende völkerrechtliche oder einfachgesetzliche Regelungen lassen bestimmten Gruppierungen im Cyberraum Möglichkeiten zu, die es im „realen“ täglichen Leben oftmals so gar nicht gibt. Erschwerend hinzu kommt, dass die sogenannte „Attribution“ oftmals nur sehr schwer möglich ist. „Cyber Attribution” dient der genauen Zuordnung einer Cyberattacke zu einem bestimmten Angreifer oder einer Gruppierung, um zumindest den Verursacher und dessen Absichten verstehen zu können und damit bessere Gegenmaßnahmen setzen zu können.

Eine ganz besondere Dimension stellt im Cyberraum der Faktor Zeit dar. Aktionen können im Cyberraum jederzeit und weltweit, mit hoher Frequenz, sehr schnell wirksam werdend, ohne Vorwarnzeit und überwiegend überraschend gesetzt werden. Dies erfordert ein hohes Maß an leistungsfähiger IKT-Sicherheitsarchitektur. Trotzdem muss man sich bewusst sein, dass selbst mit besten technischen Mitteln nie ein 100%iger Schutz gewährleitstet werden kann. Daher sind für den Fall eines Schadenseintritts zur Wiederherstellung der vollen Funktionalität Mittel für rasch zu setzende Wiederherstellungs- oder Gegenmaßnahmen vorzuhalten. Bestens ausgebildete und erfahrene Experten müssen im Anlassfall zielgerichtet agieren und reagieren können. Sowohl aus sicherheitstechnischer Sicht wie auch hinsichtlich der technischen Machbarkeit muss unter betriebswirtschaftlicher Betrachtung mit Hinblick auf die so genannte „Usability“, auf Basis eines unternehmensorientierten Risikomanagements in der Cybersicherheit jede Organisation seinen maßgeschneiderten Lösungsansatz finden („Security“ versus „Usability“ versus „Cost Effectiveness“).

**Neue Möglichkeiten – Neue Gefahren**

„Artificial Intelligence" (Künstliche Intelligenz; KI) wird diesen ausbalancierten Mix aus Gegenmaßnahmen zukünftig wesentlich beeinflussen. KI wird aber auch leider in gleichem Maße die Möglichkeiten der angreifenden Seite erhöhen. Insgesamt werden durch die KI die Quantität und Geschwindigkeit wie auch die Qualität der gesetzten Maßnahmen wesentlich verschärft.

In diesem Zusammenhang muss auch auf eine neue Herausforderung der Cybersicherheit verwiesen werden, welche sich durch den immer stärker werdenden Einsatz von KI ergibt. Es wird nämlich genau abzuwägen sein, welche Entscheidungen automatisiert durch die KI (z. B. durch „pre-authorized Actions") getroffen werden können und welche Entscheidungen tatsächlich noch immer vom Menschen zu treffen sind. Hier einen ausgewogenen Mix zu erzielen, wird Gebot der Stunde sein. Ein potenzieller Angreifer tut sich tendenziell generell leichter, Entscheidungen abzugeben und Maschinen selbständig agieren zu lassen. Kollateralschäden sind für einen Angreifer verkraftbar, der Verteidiger hingegen wird der KI wohl nie sämtliche Entscheidungen überlassen können und sollen.

**Steigende Bedeutung der Cybersicherheit („Cyber Security")**
**im Sinne des Schutzes der Kritischen Infrastruktur**

Das Funktionieren definierter Kritischer Infrastruktur im Normbetrieb, Krisenfall und Landesverteidigungsfall ist substanziell für eine funktionierende und handlungsfähige Gesellschaft. Die Koordinierungskompetenz hierfür liegt dazu für den Normbetrieb und Cyberkrisenfall im Innenministerium und geht im Cyberverteidigungsfall auf das Verteidigungsministerium über.

Das NIS-Gesetz definiert dazu in Österreich die entsprechenden Rahmenbedingungen und leitet damit Maßnahmen zur Erhöhung der Cybersicherheit ein. Mit diesem Gesetz wurden Standards geschaffen und Cybersicherheitserfordernisse definiert, an die sich die Unternehmen der Kritischen Infrastrukturen und Betreiber wichtiger digitaler Dienste zu halten haben. Letztlich soll damit die Cybersicherheit in diesen für die Republik wichtigen Bereichen erhöht werden.

Natürlich stellt die Cybersicherheit auch eine nachhaltige Herausforderung für alle anderen Unternehmen, die öffentliche Dienste, bis hin zu jedem einzelnen Bürger dar, welche die Vorzüge der Digitalisierung und Vernetzung nützen wollen. Maßgeschneiderte Lösungen auf Basis einer gediegenen Cyberrisikobeurteilung zu finden, wird wohl keinem erspart bleiben.

**Stark ansteigende Cyberkriminalität („Cyber Crime") als tägliche Herausforderung für die Privatwirtschaft und den Öffentlichen Dienst**

Obwohl die letzte Kriminalstatistik (für 2018) unter dem Titel „Österreich ist so sicher wie noch nie" firmierte, stieg die Anzahl der angezeigten Fälle von Internetkriminalität von 2017 auf 2018 um beinahe 17 %! Auch die vorläufigen Zahlen für 2019 bestätigen einen weiteren signifikanten Anstieg der Cyberkriminalität. Die fortschreitende Digitalisierung verlagert die „analogen" Straftaten immer mehr in den digitalen Cyberraum. Die KPMG Cyber Security Studie 2019 stellte dazu fest, dass zwei von drei heimischen Unternehmen innerhalb der letzten zwölf Monate von Cyberattacken betroffen waren. 41 % erlitten auf Grund eines Cyberangriffs auch einen finanziellen Schaden.

Diesem Phänomen muss mit einem adäquaten Cyberrisikomanagement nachhaltig entgegengetreten werden. Dazu ist aber auch klar festzuhalten, dass es nicht nur ein Thema von einzelnen Experten oder technischen Abteilungen in Unternehmen und öffentlichen Körperschaften ist, sondern voll in der Verantwortung der Geschäftsführung oder jeweiligen Leitungsebene angesiedelt ist.

**Stark zunehmende Bedeutung der Cyber Verteidigung („Cyber Defence") im Rahmen Hybrider Bedrohungsformen und Konventioneller militärischer Auseinandersetzungen**

Die IKT-Struktur des Österreichischen Bundesheeres, im Sinne einer der kritischen Infrastrukturen, ist ebenso durch entsprechende militärische Mittel und Services als Maßnahme der Cybersicherheit laufend entsprechend zu sichern. Damit wird in allen Anlassfällen die Führungsfähigkeit des Bundesheeres aufrechterhalten bzw. wiederhergestellt. Im Verteidigungsfall übernimmt das Verteidigungsressort zudem die Koordinierungskompetenz für die Cybersicherheit aller Kritischen Infrastrukturen.

In der IKT-Struktur des Österreichischen Bundesheeres werden bereits im täglichen Normbetrieb wöchentlich zwischen 400 000 und 500 000 Sicherheitsalarme ausgelöst. Performante IKT-Sicherheitssysteme können die Masse durch automatische Systeme abwehren. Trotzdem bleiben wöchentlich etwa 300 bis 400 Vorfälle zur Bearbeitung unserer Cyberspezialisten über, wovon etwa zwei bis drei als ernstzunehmende Cyberangriffe einzustufen sind.

Über die Herausforderungen im Norm- und Krisenbetrieb hinaus sind in der modernen Einsatzführung im Cyber-Verteidigungsfall weitaus breiter gesteckte Felder zu bedecken. Neben dem Cyberraum ist auch der Elektromagnetische Raum zu schützen. Neben den Führungs- und Einsatzsystemen sind zudem sämtliche Waffensysteme und

die gesamte Sensorik gefährdet, weil diese natürlich ebenso vernetzt sind. Darauf konzentrieren sich die Maßnahmen der Cyberverteidigung in den Komponenten „Cyber Intelligence", „CIS-Defence" und „Cyber Operations". Nahezu keinem aktuellen Bedrohungsszenario kann heutzutage ohne wirksame Cyberverteidigungs-Komponente erfolgreich entgegengetreten werden.

Fest steht, dass gerade im Cyberraum eine komplette Risikovermeidung nahezu unmöglich ist. Vollumfängliches Risikomanagement ist von daher die einzig gangbare Möglichkeit, um die Grundlage für den Schutz der eigenen Systeme, Prozesse und Daten zu schaffen und die Einsatzfähigkeit von unternehmenskritischen Systemen zur Aufrechterhaltung der Funktions- und Einsatzfähigkeit zu gewährleisten („Bedrohung" versus „akzeptiertes Risiko" versus „verfügbare Funktionalitäten").

Nur wer seine „Key Assets", seine Prozesse, neuralgischen Punkte, potentiellen Schwachstellen und Systemabhängigkeiten kennt, kann entsprechende Schutz- und Gegenmaßnahmen setzen.

Risikomanagement ist aber mehr als das. Gewonnene Erkenntnisse und entwickelte Verfahren müssen in die eigenen Abläufe und Prozesse integriert werden und voll inhaltlich von der Führungsebene mitgetragen werden. So werden zukünftige Angriffe nicht nur erschwert – im Anlassfall ist die Organisation damit in der Lage, Schäden einzudämmen.

Als Kommandant des IKT & Cybersicherheitszentrum (IKT&CySihZ) des Österreichischen Bundesheeres kann ich Ihnen versichern, dass der Schutz im Cyberraum nicht eine einmalige, sondern eine kontinuierliche Anstrengung darstellt. Der Führungskreislauf – von der Beurteilung der Lage über die Planung der Durchführung hin zu Realisierung (Beauftragung) und Überwachung – kommt auch im Cyberraum zur Anwendung. Dieser Umstand sowie die Entwicklung standardisierter und auch eingeübter Abläufe ermöglichen eine zeitgerechte, klare, nachvollziehbare, lageangepasste und rechtlich haltbare Reaktion bei Cyberangriffen.

Das Österreichische Bundesheer und die TÜV AUSTRIA Akademie pflegen zu diesem Zwecke eine langjährige ausgezeichnete Kooperation und wechselseitige Wertschätzung.

Das nun hier vorliegende Buch soll dem geneigten Leser als Schulungs- und Nachschlagewerk dienen. Es reicht ein Werkzeug, um Cyberrisiken zu erfassen, zu beurteilen und Folgerungen zu treffen. Eine Grundlage, um den Cyberraum etwas sicherer zu machen.

In diesem Sinne wünsche ich allen Leserinnen und Lesern viel Vergnügen und vor allem nachhaltigen Erkenntnisgewinn beim Studium dieses hochaktuellen Buches.

Generalmajor Ing. Mag. Hermann Kaponig
Kommandant IKT & Cybersicherheitszentrum
Österreichisches Bundesheer

# Der Autor

Tom Vogt wurde in Hamburg geboren, wo er an der FH Wedel Wirtschaftsinformatik studierte und eine Karriere in der Cybersecurity begann, die ihn über Stationen wie einen Hamburger Verlag, ein E-Commerce-Start-up während der Dotcom-Phase und ein Jahrzehnt in der Telekommunikation schließlich nach Wien zum TÜV AUSTRIA brachten, wo er derzeit als Senior Information Security Architect in der Tochterfirma SPP Handelsges.m.b.H. tätig ist.

Neben einem lebenslangen Interesse an Computern hat er vielfältige Interessen von Philosophie und Psychologie bis zum asiatischen Kampfsport sowie Brett- und Rollenspielen. Er hat sich in mehreren ehrenamtlichen Funktionen engagiert, als Präsident des Vienna Speakers Club oder in Zusammenarbeit mit der amerikanischen EFF für digitale Bürgerrechte.

Seine Beiträge zur IT finden sich unter anderem im High-Availability Linux Projekt wie auch in seinen zahlreichen internationalen Vorträgen zu Security Enhanced Linux (SELinux), u. a. auf der Cebit in Hannover oder der PacSec Konferenz in Tokio.

# Inhaltsverzeichnis

# 1 Einführung

Unternehmerische Tätigkeit ist so eng mit Risiken verbunden, dass wir im Eingehen von Risiken das entscheidende Kriterium, das einen Unternehmer ausmacht, finden können.

Risikomanagement ist daher eine zentrale Unternehmensfunktion. Sie soll Risiken aufzeigen, begreifbar machen und – falls möglich – reduzieren. Dies geschieht auf unterschiedlichen Ebenen.

Auf der Unternehmens- oder Konzernebene findet sich das Enterprise Risk Management (ERM), das sich in zumeist abstrakter Form mit strategischen Risiken befasst. Fragen der Entwicklung von Märkten, Aktivitäten der Konkurrenz, wirtschaftlichen und relevanten politischen Entwicklung, aber auch von Forschungs- und Entwicklungsaktivitäten, des Personals und anderer Unwägbarkeiten sind hier Gegenstand.

Eine internationale Norm, die ISO 31000, beschreibt den Prozess des Enterprise Risk Managements.

Dieses Buch befasst sich nicht mit dem Enterprise Risk Management, auch wenn es viele Gemeinsamkeiten zwischen den Inhalten hier und dem Enterprise Risk Management gibt.

Auf der technischen Ebene existiert ebenfalls ein Risikomanagement, das sich mit konkreten technischen Gefahren befasst, oftmals mit dem Begriff Functional Safety tituliert. Hier werden Parameter von Maschinen, von Material und Werkstoffen sowie Qualität von Herstellung und Betrieb von technischen Anlagen beurteilt, um Fehler und Belastungen zu ermitteln, die zu einem technischen Versagen führen könnten. Aufzüge, Fahrzeuge, Roboter und viele andere technische Systeme werden so sicher und beherrschbar gemacht.

Dieses Buch befasst sich nicht mit Functional Safety, auch wenn es einzelne Überschneidungen in diesen Bereich gibt.

Ein vergleichsweise junger Zweig des Risikomanagements findet sich im Bereich der Informationssicherheit oder Cybersecurity. Anders als in der Functional Safety und wesentlich stärker als im Enterprise Risk Management sind hierbei Risiken zu beachten, die willentlich von bösartigen Akteuren verursacht werden. Dabei sind einerseits technische Systeme im Spiel, andererseits unterstützen diese aber Unternehmensfunktionen und müssen daher abstrakt und prozessual betrachtet werden.

Risikomanagement in der Informationssicherheit ist das zentrale Thema dieses Buches, wobei viele Kapitel auch darüber hinaus Anwendung finden können.

Anders als das Enterprise Risk Management und die Functional Safety ist Risikomanagement im Bereich der Informationssicherheit zurzeit (2019) noch wenig entwickelt. Es gibt eine internationale Norm (ISO 27005), die sich damit befasst, sie ist aber nicht zertifizierungsfähig, sondern stellt nur Empfehlungen im Rahmen einer übergeordneten Norm, des Informationssicherheitsmanagementsystems (ISMS, ISO 27001) dar.

Auch die Methoden und Werkzeuge im Bereich des Informationssicherheits-Risikomanagements (IS-RM) sind im Vergleich zu anderen Bereichen noch unterentwickelt.

Ich habe daher in diesem Buch neben einer Beschreibung des Risikomanagementprozesses auch die derzeit besten und am weitesten entwickelten Methoden und Verfahren zusammengetragen und gehe kritisch auf überholte, aber immer noch verbreitete Vorgehensweisen ein, um einen möglichst umfassenden Blick auf das gesamte Feld zu bieten.

Zur Eingrenzung noch ein Wort zum Begriff „Informationssicherheit". Dieser hat sich aus der Informationstechnik (IT) Sicherheit heraus entwickelt und beschreibt umfassender den Bereich von Daten und Datenverarbeitung. Während wir unter EDV oder IT im wesentlichen technische Systeme (Computer, Datenspeicher, Datennetzwerke etc.) verstehen, umfasst die Informationssicherheit auch Aspekte der physischen Sicherheit der nicht-elektronischen Daten, wie Aktenordner, Papierunterlagen etc., sowie von Personal, Verhalten und Prozessen. Diese Erweiterung entstand vor dem Hintergrund der Erkenntnis, dass oftmals nicht-technische Schwachstellen zu Sicherheitslücken in den IT-Systemen führen. Das bekannteste Beispiel mögen schwache Kennworte sein.

## 1.1 Anmerkungen zum Buch

Dieses Buch stellt keine besonderen Voraussetzungen an den Leser, wobei Grundkenntnisse im Bereich der Cybersecurity hilfreich sind.

An mehreren Stellen geht der Text intensiv auf statistische, stochastische oder andere angewandte Mathematik ein. Begrifflichkeiten, wie Mittelwert oder Standardabweichung, werden dabei vorausgesetzt und nicht erläutert. Tiefergehende Verfahren werden erläutert.

An wenigen Stellen werden im Text kurze Programme verwendet, um die Umsetzung einer Methodik exemplarisch darzustellen. Das Verständnis der abgedruckten Quellcodes ist für das Verständnis der Methodik nicht erforderlich und sie können von Lesern, die keinerlei Programmierkenntnisse haben, problemlos übersprungen werden. Lesern mit Programmiererfahrung hingegen werden die Quellcodes möglicherweise die Methodik deutlicher machen als die textuelle Erläuterung. Um allen Lesern gerecht zu werden, finden sich immer beide Darstellungsformen. Für die Programme wird die Programmiersprache Rust (https://www.rust-lang.org) verwendet.

Zum leichteren Verständnis werden die einzelnen Abschnitte des Buches von Beispielen begleitet. Dabei sind die Beispiele exemplarisch zu verstehen, da die gesamte Bandbreite an Möglichkeiten kaum in überschaubarem Umfang darzustellen ist. Die jeweils gewählten Werte, Kategorien, Bewertungen und Methoden sind ebenso beispielhaft zu verstehen, nicht etwa als einzig mögliche. Ziel der Beispiele ist es, den jeweiligen Inhalt verständlich zu machen, und gelegentlich werden dafür aus didaktischen Gründen Annahmen oder Ausschlüsse vorgenommen, insbesondere zur Vereinfachung.

Noch eine Anmerkung zur Grammatik: Dieses Buch verwendet das generische Maskulinum, Femininum oder Neutrum so, wie es der deutschen Sprache zu eigen ist. Es folgt damit den Regeln der deutschen Sprache, nach denen das grammatikalische Geschlecht (Genus) unabhängig vom biologischen Geschlecht (Sexus) ist.

Anders formuliert: „der Manager“ ebenso wie „die Führungskraft“ beinhaltet in beiden Fällen Personen jedweden Geschlechtes.

# 2 Risiko

## 2.1 Was ist Risiko?

Gehen wir zunächst einen Schritt zurück. Was ist eigentlich Risiko?

Ist eine vereiste Straße ein Risiko? Auch wenn niemand darauf fährt? Ist die neue technische Schwachstelle, die gestern veröffentlicht wurde, ein Risiko? Der Ausgang der Wahlen im nächsten Jahr? Was ist mit der Pensionierung des einzigen SAP-Spezialisten im Unternehmen? Oder der Tatsache, dass die Konkurrenz jetzt das gleiche Produkt billiger anbietet?

Der Duden definiert das Wort „Risiko“ so:

> ***Risiko, das:*** möglicher negativer Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust, Schäden verbunden sind; mit einem Vorhaben, Unternehmen o. Ä. verbundenes Wagnis

Anschaulicher und systematischer können wir uns fragen, welche wesentlichen Faktoren zusammenkommen müssen, bevor wir etwas als ein Risiko bezeichnen. Diese Faktoren werden in der weiteren Betrachtung für uns noch von Bedeutung sein.

Der erste Faktor ist die **Zukunft.** Nur Ereignisse, die noch nicht eingetreten sind, betrachten wir als ein Risiko. Was in der Vergangenheit liegt, dessen Ausgang steht bereits fest und ist daher unabänderlich. Der Blick des Risikomanagements ist in die Zukunft gerichtet, auf Ereignisse, die noch nicht stattgefunden haben, aber geschehen könnten.

Hier sind wir beim zweiten Faktor: **Ungewissheit.** Ein Risiko ist uns grundsätzlich bekannt, aber nicht vollumfänglich.

Wäre es uns gänzlich unbekannt, würden wir von Ignoranz sprechen, etwas, das wir nicht wissen können oder wollen. Wenn wir einer Gefahr gegenüber ignorant wären, dann würden wir sie nicht als Risiko beschreiben und berücksichtigen, da sie in unseren Gedanken gar nicht vorkommt.

Wäre es uns hingegen in Gänze bekannt, wären wir im Bereich des gesicherten Wissens und würden es nicht als Risiko betrachten, sondern als einfachen, berechenbaren Vorgang, als Gewissheit.

Das Risiko dagegen bewegt sich im Graubereich dazwischen. Wir wissen oder ahnen genug, um es zu beschreiben, aber nicht genug, um es vollumfänglich vorauszusehen. Dem Risiko ist also eine Spannbreite inhärent, es stellt nicht einen Punkt im Raum der Möglichkeiten dar, sondern ein diffuses Feld. Einen oder mehrere Faktoren können wir nicht völlig fassen. Genau hier liegt ein Teil unserer Herausforderung und im Rest des Buches werden wir uns mit dieser Frage ausführlich befassen.

Ein dritter Faktor ist noch entscheidend, damit ein ungewisses Ereignis ein Risiko ausmacht: Es muss eine **Auswirkung** auf uns haben. Ein mögliches Ereignis, das uns in keiner Weise betrifft, würden wir nicht als Risiko bezeichnen, noch würden wir es in einem Risikomanagement betrachten. Die vereiste Straße, auf der niemand fährt, ist ein Beispiel.[1] Ein weiteres Beispiel ist eine technische Schwachstelle in einem System, das wir nicht benutzen – sie mag für uns theoretisch interessant sein, aber in unserem Risikomanagement wird sie nicht vorkommen. Sowohl für die Definition des Risikobegriffes als auch für die Risikoanalyse in Kapitel 6 *Risikoanalyse* (ab Seite 56) ist entscheidend, dass der Eintritt des ungewissen Ereignisses auch (negative) Folgen hat.

Noch ein Wort zum Begriff: In der ISO 27005 sowie an vielen anderen Stellen in den Normen und der Literatur wird gleichberechtigt von „Risiken und Chancen" gesprochen. In der Praxis genießen üblicherweise die Risiken Priorität und daher fokussieren wir uns auch in diesem Buch auf die Risiken. Der wesentliche Unterschied zwischen beiden Begriffen ist, dass die Auswirkungen bei Risiken negativ und bei Chancen positiv sind.

## 2.2 Randnotiz

Übrigens ist die Herkunft des deutschen Wortes „Risiko" nicht endgültig geklärt. Möglich ist eine Entlehnung aus dem Spanischen *risco,* „Klippe" in der Bedeutung als Abgrund oder als Gefahr für Schiffe. Eine andere Möglichkeit ist die Ableitung aus dem Lateinischen *rixāri,* „streiten, widerstreben" in der Bedeutung der Unwägbarkeit einer Auseinandersetzung. Eine andere Erklärung greift auf das arabische Wort رزق (Aussprache: *rizq*), „Lebensunterhalt" in der Bedeutung „das, was von Allah gegeben wird" zurück.

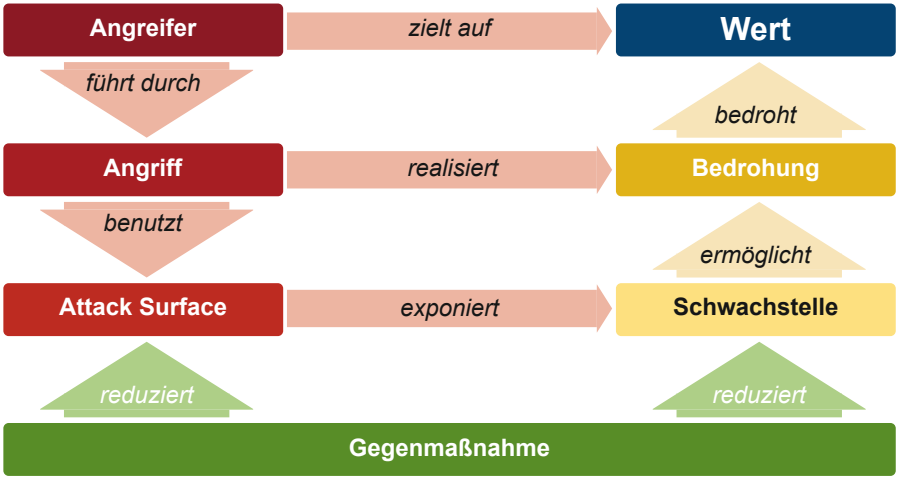
1 Einwand: Aber es *könnte* jemand auf der Straße fahren. Wenn dem so ist, dann handelt es sich um ein Risiko. Es war dagegen hier postuliert, dass niemand auf ihr fährt.

## 2.3 Weitere Begriffe

Andere Begriffe, die im Zusammenhang mit Risikomanagement in der Cybersecurity regelmäßig auftauchen, sind in der folgenden Tabelle angeführt. Da ein Großteil der Literatur zum Thema in englischer Sprache geschrieben ist, sind auch die jeweils englischen Fachbegriffe genannt.

| Englisch | Deutsch | Bedeutung |
|---|---|---|
| Risk | Risiko | Möglicher negativer Ausgang |
| Threat | Bedrohung | Aktion eines Angreifers gegen Wert(e) |
| Attack | Angriff | Aktivität eines Angreifers (ungeachtet der Auswirkung auf Werte) |
| Attack Surface | Angriffsfläche | Exponierte Teile der Infrastruktur, Dienste oder Schnittstellen, die für einen Angreifer zugänglich sind |
| Threat Actor | Angreifer | Jemand, der eine Bedrohung auslöst |
| Vulnerability | Schwachstelle | Eigenschaft von Hard-, Software, Person, Prozess etc., die eine Bedrohung ermöglicht |
| Countermeasure (also: Control) | Gegenmaßnahme (auch: Kontrolle) | Maßnahme, welche eine Schwachstelle reduziert oder verhindert |
| Asset | Wert | Etwas von Wert für die Organisation |
| Event (also: Incident) | Ereignis (auch: Vorfall) | Eintritt eines Risikos |
| Impact | Auswirkung | (Negative) Konsequenz des Risikos |

Diese Begriffe hängen wie im folgenden Schaubild dargestellt zusammen:



Wir gehen also (rechts oben) von einem Wert aus, was in unserem Kontext alles ist, das für die Organisation wertvoll ist. Es kann sich um Gegenstände (z. B. IT-Ausrüstung, Firmenfahrzeuge, Büroeinrichtung) handeln, aber auch um immaterielle Werte (z. B. Geld auf dem Firmenkonto, Geschäftsgeheimnisse, Vertragsunterlagen, Forschungsergebnisse) ebenso wie um ideelle Werte (z. B. Ansehen bei Kunden, Verbundenheit von Mitarbeitern, gute Kontakte zur Politik oder Journalisten).

Dem gegenüber steht (links oben) der Angreifer. Er hat es auf den Wert abgesehen, kann ihn aber nicht direkt erreichen. Wir betrachten dabei auch Umweltereignisse und unabsichtliche (aber schädliche) Handlungen, wie Benutzerfehler als „Angreifer". Alle Quellen von Risiken auf diese Weise zusammenzufassen, erleichtert das weitere Vorgehen, da wir nicht je nach Angreifertyp unterschiedliche Systematiken anwenden müssen.

Eine für die meisten Anwendungsfälle vollständige Übersicht möglicher Angreifer ist in der folgenden Tabelle gegeben:

| Akteur | Erläuterung/Beispiele |
|---|---|
| Umweltereignis | Feuer, Wasser, Erdbeben, Stromausfall, externer Netzwerkausfall |
| Defekt | Technische Fehler oder Fehlfunktionen, interner Netzwerkausfall etc. |
| Fehlbedienung | Unabsichtliche Fehler von Benutzern, Irrtümer, Eingabefehler |
| Zufallsfund | Benutzer, Besucher, fällt durch Zufall, Softwarefehler etc. etwas in die Hände. |
| Neugieriger Angreifer | Jemand (Insider oder Outsider), der ohne tiefere Absicht „ausprobiert". |
| Automatisierter Angriff | das „Internet-Hintergrundrauschen", automatisierte, ungezielte Angriffe |
| „Script Kiddies" | manuelle Angreifer mit geringer technischer Kompetenz, aber bösartiger Absicht |
| Fortschrittliche Malware | 0-day Angriffe, neuartige Malware, aktuelle und bedrohliche Gefahren, meist kurzfristig hohe Bedrohung, bis Virenfilter- oder Softwareupdates erscheinen |
| Motivierter Angreifer | ein kompetenter Angreifer, der gezielt vorgeht. Möglicherweise ein Insider. |
| Organisiertes Verbrechen | systematische Angreifer mit hoher Motivation und erheblichen Ressourcen |
| Staatlicher Akteur | in der Praxis selten von Bedeutung – Kompetenz und Ressourcen sind eher von der Bedeutung des Ziels als von anderen Beschränkungen abhängig |

Um zum Wert zu kommen, führt der Angreifer nun einen Angriff durch. Damit realisiert er eine Bedrohung des Wertes. Die Bedrohung ist die unmittelbare Vorstufe zum Risiko. Der wesentliche Unterschied zwischen Bedrohung und Risiko besteht darin, dass die Bedrohung die Höhe der Auswirkungen nicht berücksichtigt. Eine Bedrohung ist etwa eine spezifische Art von Cyberangriff oder ein Stromausfall im Rechenzentrum. Sie enthält noch keine Information über den betroffenen Wert, sondern sie wirkt auf einen Wert.

Wenn wir die Bedrohung näher betrachten, erkennen wir, dass sie auf einer Schwachstelle basiert. Die Schwachstelle ist das, was die Bedrohung ermöglicht. Wäre die Schwachstelle nicht vorhanden, wäre die Bedrohung nicht möglich. Hätte die Software nicht diesen speziellen Fehler gehabt, wäre der Cyberangriff nicht erfolgreich gewesen. Hätte die Sekretärin dem charmanten Social-Engineering[2]-Experten das Kennwort nicht verraten, hätte er sich nicht in das System einloggen und dort Schindluder treiben können. Wäre das Auto abgeschlossen gewesen, hätte der Dieb das Notebook mit den wichtigen Vertragsunterlagen nicht stehlen können. Und so weiter.

Diejenigen Teile unserer Infrastruktur, die für einen Angreifer erreichbar sind, nennen wir auch die Angriffsfläche oder engl. Attack Surface. Sie ist oftmals die „Außenhaut" unserer Infrastruktur, kann aber auch tiefer liegende Systeme beinhalten, wenn diese für einen Angreifer erreichbar sind.

Gegen die Schwachstelle schließlich setzen wir Gegenmaßnahmen. Nicht jede Schwachstelle kann direkt ausgemerzt werden und auch zumeist nicht zuverlässig oder hundertprozentig geschlossen werden. Darauf gehen wir im Detail in Kapitel 7 *Risikobehandlung* (ab Seite 115) ein. Eine Gegenmaßnahme kann sowohl eine Schwachstelle als auch die Angriffsfläche reduzieren.

Noch ein Wort zum immer noch oft gehörten Pseudo-Argument „Bei uns gibt es nichts zu holen": Erstens doch und zweitens ist das dem Angreifer oftmals vollkommen egal.

Es gibt doch etwas zu holen, nämlich die IT-Ressourcen. Manche Angreifer haben es gar nicht auf Firmengeheimnisse abgesehen, sondern suchen Computersysteme, von denen aus sie weitere Angriffe starten können oder auf denen sie illegale Daten ablegen können (und bei manchen Daten ist schon der Besitz strafbar, etwa bei Kinderpornographie) oder mit denen sie Cryptomining betreiben oder andere rechenaufwändige Aktivitäten durchführen können.

Darüber hinaus sind heute viele Angriffe automatisiert und werden von Maschinen ungezielt auf ganze Netzbereiche gestreut durchgeführt. Ein Angreifer entdeckt eine neue Schwachstelle und schreibt ein Programm, um diese Schwachstelle auszunutzen. Statt gezielt bestimmte Ziele auszuwählen, probiert sein Programm den Angriff auf alle erreichbaren Ziele. Erst wenn ein Angriff erfolgreich war, wird der menschliche Angreifer benachrichtigt, und erst dann interessiert er sich dafür, wen oder was er tatsächlich gehackt hat. Der Schaden auf Seite des Opfers ist dann möglicherweise schon entstanden.

2 Social Engineering beschreibt einen Angriff über soziale statt technische Wege, etwa ein Anruf des Angreifers, bei dem er vorgibt, in der IT-Abteilung zu sein, oder eine gefälschte SMS des Geschäftsführers aus dem Ausland mit vorgeblicher Dringlichkeit. Beim Social Engineering wird ein Mensch getäuscht und dazu gebracht, durch seine Handlungen dem Angreifer Informationen zu geben oder seine Aktivitäten zu erleichtern.

Zum Abschluss noch eine Übersicht möglicher Motivationen von Angreifern, ohne Anspruch auf Vollständigkeit, als Anregung dafür, über die typischen Hacker-Szenarien hinaus zu denken:

| Motiv / Ziel | Erläuterung/Beispiele |
|---|---|
| keines | Umweltereignisse, Defekte etc. |
| Neugierde | Interne Benutzer, Webseitenbesucher, „Old-school Hacker“[3] |
| Irrtum | Fehlbedienung, fehlerhafte oder missverständliche Arbeitsanweisungen |
| Egoismus/Profilierung | Hacker, Script-Kiddies |
| Persönliche Vorteile | Mitarbeiter und andere Insider, ehemalige Beziehungspartner etc. |
| Aktivismus | Hacktivisten, verärgerte Mitarbeiter, Einzeltäter |
| Vandalismus | Hacktivisten, Hacker, verärgerte Externe |
| Persönliche Bereicherung | Organisierte oder unorganisierte Kriminalität, Insider |
| Datendiebstahl | Hacktivisten (zwecks Leaking) |
| Erpressung | Ransomware, DDoS etc. |
| Industriespionage | Konkurrenten oder Hacker (mit dem Ziel des Weiterverkaufs an die Konkurrenz) |

## 2.4 Beispiele

Diskutieren wir zur Klärung der Begriffe einige Beispiele:

**Beispiel 1: Der Reifen hat kaum noch Profil.**

Aus dieser Information ist kein Risiko erkennbar. In unserem Kopf mögen wir ein Risiko konstruiert haben, aber es entsteht ausschließlich mit Hilfe von Informationen, die hier nicht gegeben sind. Insbesondere ist keine Aussage darüber getroffen, ob der Reifen sich überhaupt an einem Fahrzeug befindet. Er könnte auch auf dem Schrottplatz liegen, als Blumenbeet dienen oder mit einem Seil an einem Baum befestigt sein und als Schaukel verwendet werden.

Ohne diese Information ist kein Risiko abzuleiten, da die Auswirkung weder spezifiziert ist, noch sich ohne Interpretation ableiten lässt.

**Beispiel 2: Die Tür zum Warenlager steht häufig offen.**

Hier handelt es sich gemäß der weiter oben eingeführten Terminologie um eine Schwachstelle, aber nicht um ein Risiko. Es fehlt der Angreifer, der die Schwachstelle ausnutzt. Ohne diese Information ist keine Risikoabschätzung möglich.

3 Als IT-Netze noch weitgehend auf Universitäten beschränkt waren und der Begriff „Hacker“ geprägt wurde, bezeichnete er technisch begabte Studenten, die aus Neugierde und ohne die Absicht, Schaden anzurichten, die Grenzen dieser neuen Technik austesteten.

**Beispiel 3: Die Aktivität von Cyberterroristen hat zugenommen.**

Dies kann eine Bedrohung beschreiben, aber kein Risiko. Hier ist der Angreifer gegeben, aber um ein Risiko zu sein, bräuchten wir zusätzliche Informationen darüber, ob uns diese Aktivität betrifft, also ob wir im Fokus von Cyberterroristen stehen – z. B. ob sie in unserem Threat Model vorkommen, siehe Kapitel 5.3 *Threat Modeling* (ab Seite 41) – und welche unserer Werte von ihnen bedroht sind.

**Beispiel 4: Der entlassene Mitarbeiter hat gedroht, geheime Finanzdaten zu veröffentlichen.**

Auch wenn wir für die konkrete Bewertung weitere Details benötigen, ist hier ein Risiko klar erkennbar. Das Element der Ungewissheit ist vorhanden – wird er es tun? – und ebenso sind negative Auswirkungen erkennbar, da die Finanzdaten nicht umsonst geheim sind.

Wir haben hier also ein Risiko identifiziert, das im Weiteren durch zusätzliche Detailinformationen bewertbar zu machen ist.

**Beispiel 5: Ein erfolgreicher Cyberangriff hat unsere Webseite für mehrere Stunden lahmgelegt.**

Hier handelt es sich nicht um ein Risiko, da der Schaden bereits eingetreten ist. Wir sind im Bereich des Sicherheitsvorfalls und der anzuwendende Prozess ist das Incident Management, nicht das Risikomanagement.

**Beispiel 6: Der gleiche Angriff könnte zukünftig wieder passieren.**

Hier ist der Ausgang dagegen ungewiss, der Angriff könnte sich wiederholen, muss aber nicht und unklar ist auch, wie oft. Wir können davon ausgehen, dass der Ausfall der Webseite uns schädigt, daher handelt es sich hier klar um ein Risiko.

Anders als bei Beispiel 1 können wir hier davon ausgehen, ohne dass es explizit gesagt ist: Unsere Organisation hat ja nicht ohne Grund eine Webseite, sondern weil das Vorhandensein der Webseite einen Vorteil darstellt. Dieser Vorteil leidet bei einem Ausfall. Ob wir über die Webseite tatsächlich E-Commerce betreiben oder nur eine Firmendarstellung online stellen, wird sich in der Höhe der Auswirkung niederschlagen, aber eine Auswirkung ist in jedem Fall gegeben.

**Beispiel 7: Ein Anrufer könnte mittels Social Engineering Kennworte erfahren und somit Remotezugang zu den Buchhaltungsdaten gewinnen.**

Auch hier haben wir einen ungewissen Ausgang („könnte“) mit negativen Auswirkungen (die Buchhaltungsdaten sind sicher ein schützenswertes Gut) und somit ein Risiko.

Ähnlich wie bei Beispiel 6 müssen wir in diesem Schritt noch nicht in der Lage sein, die Auswirkungen konkret zu benennen oder ihre Schwere zu bewerten. Entscheidend für die Feststellung, dass es sich um ein Risiko handelt, ist lediglich die Tatsache, dass negative Auswirkungen gegeben sind.