Information Security

Cyber-Resilienz vs. Anti-Fragilität

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur

eingereicht von

Christopher Simader, BSc

1710619817

im Rahmen des

Studienganges Information Security an der Fachhochschule St. Pölten

Betreuung

Betreuer: FH-Prof. Dr. Simon Tjoa

Mitwirkung: Dipl.-Ing. Philipp Reisinger, BSc

St. Pölten, 9. Februar 2020 _____ _____

(Unterschrift Verfasser) (Unterschrift Betreuer)

*

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehr- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, Datum *Unterschrift*

Kurzfassung

Schon in den 1950er Jahren gab es ein verstärktes Interesse an Fragestellungen zu menschlichen Entwicklungsmöglichkeiten. Es folgten zahlreiche Studien, um die menschliche Resilienz unter Extrembedingungen zu erforschen. Im technischen Zusammenhang kam der Begriff Resilienz das erste Mal in der Materialwirtschaft auf und beschreibt die Fähigkeit eines Materials, um nach einer elastischen Verformung wieder in den Ausgangszustand zurückzukehren. Auch in anderen Forschungsgebieten tritt die Resilienz auf - so auch im Cyber-Sicherheitsbereich.

Die Cyber-Resilienz wurde in den letzten Jahren als eine der wichtigsten Mechanismen für den Fortbestand von Systemen bezeichnet und gewann schnell an Anerkennung. Sie ist eine ganzheitliche Strategie zur Stärkung der Widerstandskraft der Informationstechnologien gegenüber Bedrohungen. Bisher verwendeten Sicherheitsinfrastrukturen in Informationstechnologien Sicherheitsmechanismen aus gängigen Normen und Standards, um sich gegen Angriffe zu schützen. Im Falle eines gelungenen Angriffes sind kritische Prozesse gefährdet und können nicht mehr ausgeführt werden. Hier soll die Cyber-Resilienz Abhilfe schaffen, denn neben dem Verhindern von Angriffen soll auch der laufende Geschäftsbetrieb gesichert werden beziehungsweise die schnelle Wiederaufnahme des Betriebs sichergestellt werden.

Zu Problemen kann es bei der Cyber-Resilienz mit „too big to fail“- Konstruktionen kommen. Bei Änderungen der Rahmenbedingungen reagieren große Organisationen nicht flexibel und agil genug um wieder stabile Verhältnisse herzustellen. Die Toleranz gegenüber Fehlern ist daher niedrig und die Fähigkeit zur Wiederherstellung ist nur schwer und langwierig zu bewältigen. Aus einem zweiten Blickwinkel ist die Abhängigkeit von wenigen Key-Playern auch für die gesamte Gesellschaft problematisch, denn das ist das genaue Gegenteil von Resilienz und verlangt in Zukunft einen neuen Denkansatz. Als Vorbild dafür könnte die Natur dienen. Sie schaffte viele Arten und Unterarten von Flora und Fauna - was die Chance zum Überleben steigert, da sich einige Arten an die sich ändernden und im Voraus unbekannten Bedingungen besser anpassen als andere. Systeme, die mit Stressoren, Fehlern oder Ausfällen umzugehen wissen und durch sie sogar noch verstärkt werden, bezeichnet man als anti-fragil. Die natürliche Evolutionsstrategie kann somit als anti-fragil angesehen werden. Auch im Cyber-Sicherheitsbereich möchte

man anti-fragile Systeme erschaffen - gelingen soll dies mit Mechanismen und Konzepten wie beispielsweise Chaos Engineering, Red Teaming Tests oder Fuzzing mit maschinellem Lernen.

Heutige Systeme müssen hochverfügbar sein und werden immer komplexer. Kommt es zu einzelnen Ausfällen, ist meist auch das Gesamtsystem davon betroffen. Um dies zu vermeiden, dürfen temporäre Ausfälle nicht zum Ausfall der gesamten Applikation führen; vielmehr muss mit einzelnen Störungen umgegangen werden können und passend darauf reagiert werden. Durch den Einsatz von anti-fragilen Mechanismen finden solche Ausfälle kontinuierlich und kontrolliert statt, um Schwächen eines verteilten Systems zu finden und um aus ihnen zu profitieren. Als einer der Vorreiter gilt das Tool Chaos Monkey vom Streaming-Portal Netflix, das laufend Amazon Web Services-Instanzen per Zufall zerstört, ohne dass der Kunde etwas davon mitbekommt. Ziel ist auch hier, das System aus Fehlern lernen zu lassen und gleichzeitig dem Kunden die größtmögliche Verfügbarkeit zu bieten. Beim Cyber Red Teaming gibt es zwei Betrachtungswinkel: das angreifende Team, auch „rotes Team“ genannt, mit dem Ziel intelligente und zielgerichtete Angriffsszenarien zu entwickeln, um Schwachstellen im System aufzudecken, und als Gegenstück dazu das abwehrende „blaue Team“. Ziel dieses Teams ist es, Angriffe effektiv abzuwehren und aufgedeckte Schlupflöcher im System zu schließen. Die Teams lassen sich mit Hilfe von künstlicher Intelligenz, wie sie beispielsweise bereits bei Computerspielen zum Einsatz kommt, automatisieren. Dieses simulierte Wechselspiel deckt laufend Sicherheitslücken auf, die vom blauen Team dann analysiert und behoben werden. Auch hier wird das System laufend angegriffen, mit dem Ziel, es sicherer zu machen. Automatisiertes Fuzzing ist ebenfalls eine Technik, die mit Hilfe von maschinellem Lernen Systeme mit mehr oder weniger intelligentem Input attackiert, um diese zu härten. In Kombination mit automatischen Patchtools lassen sich auch hier Strukturen erkennen, die in Richtung anti-fragiler Systeme gehen.

Inhaltsverzeichnis

1 Einleitung

Die Cybersicherheit ist schon lange im Gespräch; der Begriff bezieht sich auf Methoden und Prozesse zum Schutz elektronischer Daten und Systeme. [1] Cyberbedrohungen entwickeln sich rasant weiter - fast täglich tauchen sie, unter Verwendung neuer Angriffsvektoren, auf. [2] Beispielsweise wurde das österreichische Außenministerium Anfang 2020 Ziel eines Cyberangriffes [3], ebenso wie 2019 die Automobilhersteller BMW und Hyundai [4] und der deutsche Bundestag im Jahr 2015. [5] Anhand dieser Beispiele ist ersichtlich, dass trotz umfangreicher Sicherheitsvorkehrungen ein Cyberangriff jederzeit möglich ist. Althergebrachte Sicherheitskonzepte sind nicht mehr zeitgemäß und greifen in vielen Ausmaßen zu kurz, um den neuen Herausforderungen zu begegnen. [6, p. 3]

Komplexe Systeme reagieren anders als die bisherigen linearen Systeme. Kleine Ursachen können bereits zu großen negativen Folgen führen, die durch Dominoeffekte sogar noch verstärkt werden können. Aktuelle Themen wie Big Data, Industrie 4.0 und Internet of things sind komplexe Herausforderungen, die eine noch viel höhere Vernetzung versprechen und daher ein neues „vernetztes Denken“ verlangen. [7]

Der Begriff Cyber-Security bezeichnet bisherige Sicherheitskonzepte zur Verteidigung von Systemen. Aufgrund der oben genannten Themen reicht die Vorgehensweise der Cyber-Security nicht mehr aus. Hier kommt die Methodik der Cyber-Resilienz ins Spiel. Sie entwickelte sich zum Modewort in der Branche der Informationstechnologien, ist aber ein durchaus nützliches Konstrukt. Dabei werden Vorsorgemaßnahmen getroffen, die sich wie ein Schirm über das gesamte System erstrecken, damit es auch während einer Stresssituation voll funktionsfähig bleibt. Sollte es zu einem Störfall kommen, versucht das System den vorherigen Zustand wiederherzustellen. [8, p. 32] „Too big to fail“- Konstruktionen bringen jedoch auch die heutigen Lösungsansätze der Cyber-Resilienz an ihre Grenzen, denn große Organisationen haben eine niedrige Toleranz gegenüber Fehlern und machen eine Wiederherstellung des ursprünglichen Zustandes fast unmöglich. [9]

Ein neuer Denkansatz ist somit notwendig und wurde womöglich im Konzept der Anti-Fragilität gefun-

den. Doch was unterscheidet ihn von der derzeitigen Cyber-Resilienz? Und ist das Konzept der Anti-Fragilität zum Schutz der Informations- und Kommunikationstechniken anwendbar? Diese beiden Fragen sollen in dieser Diplomarbeit erläutert werden, um Denkanstöße für Verbesserungen bereits bestehender, beziehungsweise für neue Methoden, zu liefern.

Die Diplomarbeit gliedert sich in ingesamt sechs Kapitel. Im Kapitel 2 wird zuerst näher auf den Begriff Resilienz in den unterschiedlichen Fachdisziplinen eingegangen, um ein besseres Verständnis für die verschiedenen Einsatzszenarien zu schaffen. Kapitel 3 befasst sich mit der Resilienz im Cyber-Sicherheitsbereich und erleutert neben den Kernprinzipien auch notwendige Metriken zur Messung dieser. Das Konzept der Anti-Fragilität wird im Kapitel 4 näher behandelt. Dort werden unter anderem auch unterschiedliche Konzepte vorgestellt, die bereits in Richtung anti-fragiler Systeme gehen. Zum Schluss folgt der Vergleich der Begriffe Cyber-Resilienz und Anti-Fragilität, wo sich diese unterscheiden, welche Gemeinsamkeiten sie haben und ob das Konzept der Anti-Fragilität als erweiterte Form der Resilienz angesehen werden kann.

2 Der Begriff Resilienz

Der Begriff „Resilienz“ gewinnt mehr und mehr an Bedeutung und hat sich zu einem Schlagwort entwickelt, das nicht mehr wegzudenken ist. Der Begriff kam im technischen Zusammenhang das erste Mal in der Materialwirtschaft auf und beschreibt die Fähigkeit eines Materials, nach einer elastischen Verformung in den Ausgangszustand zurückzukehren. Mittlerweile findet der Begriff in unterschiedlichen Fachdisziplinen Einzug, so auch im Cyber-Sicherheitsbereich. [10]

2.1 Definitionen

Das Konzept der Resilienz umfasst diverse Forschungsgebiete und bietet daher auch Platz für unterschiedliche theoretische Definitionen. In der Soziologie wird der Begriff definiert als *„Fähigkeit von Gruppen oder Gemeinschaften, mit äußeren Belastungen oder Störungen infolge sozialer, politischer und ökologischer Veränderungen fertig zu werden“*. [11, p. 347] Im Bereich der Ökologie bezieht sich die Resilienz auf die Fähigkeit eines Ökosystems, trotz ökologischer Störungen seine grundlegende Organisationsweise zu erhalten. [12] So definiert Heinz Ellenberg in seinem Buch „Vegetation Mitteleuropas mit den Alpen“ die Resilienz mit: *„Resilienz ist die Fähigkeit, nach wesentlichen Artenverschiebungen (z. B. vom Wald zu krautigen Gesellschaften) durch eine mehr oder minder langfristige Sukzession (Aufeinanderfolge) von anderen Ökosystemen wieder zum ursprünglichen Artengefüge zurückzukehren“*. [13, p. 110] In der Psychologie wird die Resilienz unter anderem wie folgt verstanden: *„Die psychologische Resilienz beschreibt die Fähigkeit, eine Krise zu bewältigen beziehungsweise schnell in den Zustand vor der Krise zurückzukehren.“* [14, p. 353-355]

Auch im Cyber-Raum hält die Resilienz Einzug. So wird diese im Buch „Cyber Resilience – Fundamentals for a Definition“ folgendermaßen definiert: *„Die Cyber-Resilienz bezieht sich auf die Fähigkeit eines Unternehmens, trotz unerwünschter Cyber-Ereignisse, kontinuierlich das beabsichtigte Ergebnis zu liefern.“* [15, p. 311-315] Die Australian Securities and Investments Commission legt die Cyber-Resilienz wie folgt dar: *„Cyber-Resilienz ist die Fähigkeit, sich auf einen Cyber-Angriff vorzubereiten, darauf zu reagieren und sich davon auch zu erholen. Resilienz bedeutet dabei mehr als nur Verhindern oder Rea-*

gieren auf einen Angriff - sie berücksichtigt auch die Fähigkeit, während eines solchen Ereignisses zu operieren und sich davon zu regenerieren.“ [16, p. 4]

Bei der Cyber-Resilienz handelt es sich nicht um ein vollkommen neuartiges Konzept, denn das Business Continuity Management (BCM) und die IT-Notfallplanung verfolgen ähnliche Ziele. So werden beim BCM Präventions- und Wiederherstellungsmaßnahmen geschaffen, um potenzielle Bedrohungen in einem Unternehmen zu bewältigen. [17, p. 48] Das IT-Notfallmanagement hat das Ziel, Risiken, die das Überleben einer Institution gefährden, rechtzeitig zu erkennen und geeignete Maßnahmen zu treffen. Dieses soll zum einen die Robustheit des Systems erhöhen und zum anderen ein schnelles Reagieren im Notfall ermöglichen. [18, p. 1]

Die genannten Definitionen zur Resilienz richten sich an ihre jeweiligen Fachrichtungen, teilen aber folgende Punkte: die Widerstandsfähigkeit gegen Störungen jeder Art zu erhöhen, die Anpassungsfähigkeit an neue Bedingungen zu ermöglichen und flexibel auf Veränderungen zu reagieren, um den Normalzustand beziehungsweise den Zustand vor einer Störung wiederherzustellen.

2.2 Resilienz im historischen Kontext

Der Ursprung des Wortes stammt aus den 1620er-Jahren und setzte sich aus den lateinischen Begriffen „re-“ („zurück-“) und „salire“ („springen“) zusammen. [19] Das Wort hatte die Bedeutung „zurückspringen“ oder „abprallen“ und wurde erst um 1830 im übertragenen Sinne für Einzelpersonen und Personengruppen verwendet. Bis 1824 hatte sich der Begriff so weiterentwickelt, dass er auch die Bedeutung „Elastizität“ umfasste. [20]

In den 1950er-Jahren entstand ein verstärktes Interesse an Fragestellungen zu menschlichen Entwicklungsmöglichkeiten. Dadurch folgten etliche Studien mit Kindern und Jugendlichen, die sich mit den Themen Kompetenz, Risiko und Resilienz beschäftigten. So untersuchte die amerikanische Psychologieprofessorin Emmy Werner von der University of California gemeinsam mit einem Team aus Kinderärzten und Psychologen den Einfluss von biologischen und psychosozialen Risikofaktoren auf die Entwicklung von Kindern. Beobachtet wurden 698 Kinder, die im Jahr 1955 auf der Hawaii-Insel Kauai geboren wurden. Hierbei handelt es sich um eine Langzeitstudie, welche in der pränatalen[1] Entwicklungsstufe beginnt und mit dem Patientenalter von 40 Jahren endet. In der Studie kam man zur Erkenntnis, dass ein Drittel dieser Kinder ein hohes Entwicklungsrisiko hatten. Dies resultiert daraus, dass die Kinder

[1] Pränatal beschreibt die Zeit vor der Geburt; während der Schwangerschaft

in chronische Armut hineingeboren wurden, in Familien aufwuchsen, die durch dauerhafte Disharmonie belastet oder geburtsbedingten Komplikationen ausgesetzt waren. [21] Zwei Drittel der Kinder mit hohem Entwicklungsrisiko fielen als Jugendliche durch Lern- oder Verhaltensstörungen auf oder hatten straffällige beziehungsweise psychiatrische Auffälligkeiten. Das restliche Drittel von Kindern, der Gruppe mit hohem Entwicklungsrisiko, fielen äußerst positiv auf und entwickelten sich zu leistungsfähigen, zuversichtlichen und fürsorglichen Erwachsenen. Neben gutem Schulerfolg waren diese im sozialen Leben gut integriert und wiesen keine Verhaltensauffälligkeiten während der Untersuchung auf. [22] In der Gesamtgruppe erzielten sie beispielsweise die niedrigste Rate an: [21]

- chronischen Gesundheitsproblemen
- Scheidungen
- Konflikten mit dem Gesetz
- Sozialhilfebeziehung
- Arbeitslosigkeit
- Todesfällen

Außerdem blickten allesamt positiv in die Zukunft und hatten viel Mitgefühl für Menschen in Not. So kam es, mit Hilfe der Resilienzforschung, zu folgendem, überraschenden Ergebnis der Langzeitstudie: Auch wenn die Startbedingungen schlecht sind, kann das Leben gut gemeistert werden. Doch dies war nicht das einzige Forschungsprojekt zum Thema Resilienz, Risiko- und Schutzfaktoren.

2.2.1 Weitere Resilienzstudien

Auch der amerikanisch-israelische Wissenschaftler Aaron Antonovsky beschäftigte sich früh damit und entwickelte das Konzept der Salutogenese, das sich mit der Entstehung und Erhaltung der Gesundheit befasst. Er untersuchte die Anpassungsfähigkeit verschiedener Frauen, die großen Qualen und psychischen Ausnahmezuständen ausgeliefert waren. Diese Frauen stellten die Verumgruppe dar. Beim Vergleich dieser Gruppe mit einer Kontrollgruppe von Frauen, mit unauffälliger Biografie, stellte er fest, dass 29% der Verumgruppe als gesund bezeichnet werden können. [23] Er befragte diese 29% intensiv weiter, wie sie ihren enormen Stress bewältigten und entdeckte dabei, dass Stressoren eine wesentliche Rolle spielen. Diese sind Teil des Lebens und stellen uns laufend vor Herausforderungen, an denen wir wachsen. Die Tatsache, dass diese Frauen aus Herausforderungen lernen, daran wachsen und daran profitieren, geht bereits in Richtung Anti-Fragilität. Nassim Nicholas Taleb beschreibt dies in seinem Buch als „posttraumatisches Wachstum“. [24, p. 70] Menschen wachsen aufgrund belastender Ereignisse über sich selbst hinaus. [24, p. 70] Der Philosoph Friedrich Nietzsche lieferte bereits im 19. Jahrhundert in seinem Buch

Götzen-Dämmerung [25] das passende Zitat dazu: *„Was mich nicht umbringt, macht mich stärker.“*

Mannheimer Risikokinderstudie

Eine weitere Resilienzstudie ist die Mannheimer Risikokinderstudie, die sich mit Chancen und Risiken in der Entwicklung von Kindern beschäftigt, die durch biologische und psychosoziale Belastungen geprägt sind. Diese Studie ist ähnlich zur Kauai-Studie von Emmy Werner und behandelt die Frage, welche Kinder besonders entwicklungsgefährdet beziehungsweise vor Beeinträchtigungen in der Entwicklung geschützt sind. [22, p. 9-10]

Die Studie fasste eine Ausgangsstichprobe von 384 Kindern, wobei 58% davon als „Hochrisikokinder“ galten. Der Fokus der Studie lag einerseits auf der Erforschung der Resilienz, also die positive Entwicklung der Kinder trotz Belastungen und welche Schutzfaktoren ausschlaggebend waren, und andererseits auf der Erforschung der psychischen Störungen bei Risikokindern. Trotz widriger Umstände entwickelten sich viele Kinder positiv. [22, p. 9-10] Die häufigsten Gründe, auch Schutzfaktoren genannt, waren dafür:

Schutzfaktoren	**Beschreibung**
die Responsivität der Mutter	eine liebevolle und feinfühlige Kommunikation schon während des Säuglingsalters
die mütterliche Supportivität	ein unterstützendes Interaktionsverhalten von Seiten der Mutter
das positive Temperament des Kindes	ein gelegentliches Lächeln im Kontakt mit der Mutter
Kompetenz bei expressiver Sprache	Kinder mit ausdrucksstarker Sprache haben später weniger Verhaltensprobleme

Tabelle 2.1: Schutzfaktoren aus Befunden der Mannheimer Risikokinderstudie [26, p. 26-28]

Am Ende der Studie kam man zu der Erkenntnis, dass negative Folgen früherer Risiken bis zum Schulalter nachweisbar waren. Bei unbelasteten Familien, ohne Risikoexposition, lässt sich wie erwartet hingegen keine Resilienz nachweisen, da die Kinder auch keinen „Gefahren“ ausgesetzt sind. [27]

Bielefelder Invulnerabilitätsstudie

Die Bielefelder Invulnerabilitätsstudie war eine der ersten deutschen Resilienzstudien. [28, p. 30] Sie hatte sich zum Ziel gesetzt, Kinder mit hohem Entwicklungsrisiko auf ihre seelische Widerstandskraft hin zu untersuchen. Der Fokus der Forschung lag darauf, in Erziehungsfeldern außerhalb der eigenen Familie eine resiliente Entwicklung zu erkennen. [22, p. 10-11]

Untersucht wurden insgesamt 146 Jugendliche im Alter zwischen 14 und 17 Jahren, die im Heim aufgewachsen sind und in zwei Gruppen eingeteilt wurden. Im Endergebnis zeigte die Gruppe der Resilienten: [22, p. 10-11]

- eine realistischere Zukunftsperspektive,
- vertrauten mehr auf die eigenen Kräfte,
- waren leistungsmotivierter in der Schule,
- und hatten oft eine feste Bezugsperson außerhalb der eigenen Familie.

Besonders die enge Beziehung zu einer Bezugsperson außerhalb der eigenen Familie, wie beispielswiese ein/e Erzieher/in im Heim, begünstigte ein resilientes Verhalten der Jugendlichen. [28, p. 30]

2.3 Der Begriff Resilienz in anderen Fachdisziplinen

Es gibt viele unterschiedliche Definitionen zu Resilienz. *„Als Resilienz bezeichnet man in der Psychologie die Fähigkeit zu Belastbarkeit und innerer Stärke. Vor allem in der therapeutischen Arbeit wird verstärkt Wert darauf gelegt, Resilienz auszubilden und damit psychischen Störungen und anderen persönlichen Problemen vorzubeugen“*, [29] ist nur eine von vielen Definitionen. Eine Suchabfrage auf Google liefert ungefähr 106 Millionen Ergebnisse (Abfrage am 16. April 2019). Die Quantität von Ergebnissen lässt erkennen, dass die Resilienz auch abseits der Information Security von Relevanz ist. Auch die Ökologie, Sozialwissenschaften und andere Sparten von Technologie und Technik befassen sich mit diesem Thema.

2.3.1 Resilienz in der Psychologie

Generell beschreibt die Resilienz in der Psychologie, die Fähigkeit von Menschen auf Situationen flexibel zu reagieren und auch stressreiche und schwierige Situationen ohne psychische Folgeschäden zu meistern. Emmy Werner war mit ihrer Kauai-Studie eine der ersten ForscherInnen, die sich mit dem Thema Resilienz beschäftigte. Sie zeigte auf, dass auch Kinder, denen ein desaströses Schicksal aufgrund

von ärmlichen Verhältnissen vorausgesagt wurde, ein gutes und erfülltes Leben haben können. [29] Die Resilienzforschung in der Psychologie zeigt, dass nicht nur Einzelpersonen, sondern sogar ganze Gruppen von Personen als resilient bezeichnet werden können.

Kollektive Resilienz

Besonders Mitglieder von Gruppen mit starkem Zusammenhalt und kollektivem Miteinander werden häufiger als resilient bezeichnet, im Gegensatz zu Personen, die sich weniger in gesellschaftliche Strukturen einfügen. Dass die Einbindung in soziale Netzwerken eine große Rolle spielt, beweisen unterschiedliche Längsschnittstudien. [30] Neben emotionaler Stabilität bieten sie das Gefühl von „Dazugehörigkeit". Soziale Netzwerke können dabei ganz unterschiedlich aussehen: Familie, Freunde, Nachbarn, berufliche Kontakte, oder Kontakte aus diversen Interessensgruppen.

2.3.2 Resilienz in Ingenieurwissenschaften

Die Wissenschaft, die sich mit der theoretischen Bearbeitung technischer Probleme und deren Technik befasst, nennt man Ingenieurwissenschaft. Darunter fallen diverse Disziplinen wie das Bauingenieurwesen, Maschinenbau, Elektrotechnik und weitere kleinere Fachdisziplinen. [31] Auch hier wird die Resilienz als Fähigkeit verstanden, auf störende Ereignisse zu reagieren, diese zu absorbieren, sich im Vorhinein schon darauf einzustellen und sich gegebenenfalls davon zu erholen. [32] Die betroffenen Systeme sollen dabei nie vollständig versagen, sondern die wesentlichen Dienste aufrechterhalten. [33] Damit dies erreicht werden kann, müssen die Strukturen der technischen Systeme gestärkt werden. Dazu gibt es unterschiedliche Methoden: [33]

- Schaffung verteilter Systeme
- Planung der Redundanz
- Schaffung anpassungsfähiger Systeme

Durch die Schaffung verteilter Systeme wird die Ausfallsicherheit eines Systems erhöht. Dabei werden Hardwaregeräte mit unterschiedlichsten Übertragungsmedien zu Netzwerken zusammengefasst. [34, p. 3-4] Der amerikanische Informatiker Andrew S. Tanenbaum definierte die verteilten Systeme folgendermaßen: *„Ein verteiltes System ist eine Menge voneinander unabhängiger Computer, die dem Benutzer wie ein einzelnes, kohärentes System erscheinen."* [35] Damit stehen mehr Ressourcen zur Verfügung und bestimmte Funktionalitäten werden von mehreren Rechnern angeboten, es wird somit auch Redundanz geschaffen. Durch die Selbstanpassung eines Systems sollen Situationen gemeistert werden, die zur Entwicklungszeit nicht vorhersehbar waren. Das System kann mit Situationen während der Laufzeit

umgehen, wo Fehler auftreten oder sich Anforderungen und Rahmenbedingungen ändern können. [36]

Praxisbeispiele zum Thema Resilienz in Ingenieurwissenschaften können im Flugverkehr und Schiffsbau gefunden werden. Obwohl ein Triebwerk für die Flugfähigkeit eines Flugzeuges ausreichen würde, werden zwei verwendet. Damit wird sichergestellt, dass die Flugfähigkeit auch bei einem Ausfall weiterhin gesichert ist. Die Resilienz wird somit durch Redundanz begünstigt. Dies kann auch beim Schiffsbau beobachtet werden, denn beim Bau eines Schiffes wird der Rumpf in einzelne Sektionen unterteilt. [33] Gemacht wird dies mittels Schotten[2]. Ein Schiffs-Leck würde damit nur die betroffene Sektion mit Wasser überlaufen lassen, die restlichen Schotten aber nicht, was ein Kentern verhindern soll. Aufgrund der Redundanz kann das Schiff weiterfahren, da die restlichen Schotten bis zu einem gewissen Grad ausreichend sind um das Schiff über Wasser zu halten.

2.3.3 Resilienz in der Energiewirtschaft

Die Energiewirtschaft fällt unter den Bereich kritischer Infrastrukturen und hat die Ausfallsicherheit als wichtigste Anforderung. Deshalb spielt die Resilienz auch hier eine enorme Rolle. Systeme sollen mit Hilfe der Resilienz die Fähigkeit erhalten, auch unter Stress und Belastung ihre Leistung zu erbringen, beziehungsweise diese, nach einer Extremsituation, innerhalb kürzester Zeit wieder zu erlangen. [38]

Extremsituationen können unterschiedlicher Natur sein. Von gezielten Anschlägen über Wetterextreme bis hin zu Rohstoffknappheit und Governance-Versagen[3] ist die Palette breit gefächert. Alle diese Bedrohungen können auf drei Arten bewältigt werden:

- Abbau von Stressoren
- Verwundbarkeit verringern
- Bewältigung der negativen Folgen

Diese schließen sich gegenseitig nicht aus, im Gegenteil: in Kombination bilden sie eine starke Resilienzstrategie. [39, p. 7-8]

Bisher befasste sich die Energiepolitik großteils mit Risiken, die bekannt und gut beschreibbar waren und als Produkte von Eintrittswahrscheinlichkeit und Schadensausmaß quantifizierbar sind. Auch die Aus-

[2] Schott ist ein Begriff für besonders feste Querwände in einem Schiff, die zwei Räume wasserdicht voneinander abschließen. [37]

[3] Von Governance-Versagen spricht man beispielsweise dann, wenn durch Fehlkalkulationen und -investitionen, von Seiten der Politik, keine ausreichende Flexibilität in der Energieversorgung gewährleistet ist. [39, p. 26]

wirkungen dieser Risiken, wie beispielsweise schwankende Energiepreise, konnten abgeschätzt werden. Unbekannte Bedrohungen und quantitativ unkalkulierbare Risiken, wie beispielsweise ein „Blackout“ [40], wurden weniger diskutiert. Unbekannte Bedrohungen unterliegen einem gewissen Überraschungseffekt, der im Vorhinein nicht geplant werden kann. [39, p. 14]

Ein Ausfall oder eine Beeinträchtigung ist somit nicht unabwägig und kann, speziell in der Energieversorgung, zu erheblichen Störungen der öffentlichen Ordnung und Sicherheit führen. So ist nicht nur die Stromversorgung der Haushalte alleine betroffen, auch andere Systeme, wie das Telekommunikationsnetz, die Wasserversorgung, die Treibstoffversorgung oder die Lebensmittelversorgung sind von elektrischer Energie abhängig. [41] Vor der Resilienzforschung wurde daher das Stromversorgungssystem robust ausgelegt, um die Ausfallsicherheit so gering wie möglich zu halten. Wenn die meisten voraussehbaren Störungen bewältigt werden können, ohne wesentlich in die Funktionsfähigkeit einzugreifen, gilt das System als robust. Dies wird beispielsweise durch das Redundanzprinzip (n-1) erreicht. [42, p. 4]

(n-1)-Prinzip

Für die Ausfallwahrscheinlichkeit in der Energietechnik wird das (n-1)-Prinzip, auch (n-1)-Regel oder (n-1)-Kriterium genannt, als Beurteilungskriterium angewandt. Grob zusammengefasst, sind für eine Aufgabe n-Objekte zuständig oder verfügbar. Wenn ein Objekt ausfällt, sollen die wesentlichen Funktionsfähigkeiten durch die anderen (n-1)-Objekte abgedeckt werden. Das minimale Ziel ist, die maximale Höchstlast mit dem (n-1)-Prinzip zu erfüllen. [43, p. 2-3] Bei einer geringeren Auslastung, und somit auch Erfüllung des Minimalziels, können sogar höhere Stufen wie, (n-2) angestrebt werden. Dies würde bedeuten, dass von den n-Objekten zwei Objekte ausfallen können, ohne die wesentlichen Funktionsfähigkeiten zu verlieren. [44, p. 499] Das bisherige Redundanzprinzip stößt, angesichts der steigenden Komplexität, mehr und mehr an seine Grenzen und reicht in Zukunft womöglich nicht mehr aus. [42, p. 13]

Gründe für neue Ansätze

Aus folgenden Gründen sollten zur Ausfallsicherung in der Energietechnik neue Ansätze gefunden werden: [42, p. 14-15]

- Energiewende
- Sektorenkopplung
- Digitalisierung

Die Energiewende beschreibt den Übergang der nicht-nachhaltigen Nutzung von fossilen Energieträgern zu einer nachhaltigeren Energieversorgung durch erneuerbare Energien. Beispielgebend sind hier die Wasserkraft und biogene Energien, die sich mehr und mehr in der Energieerzeugung wiederfinden.

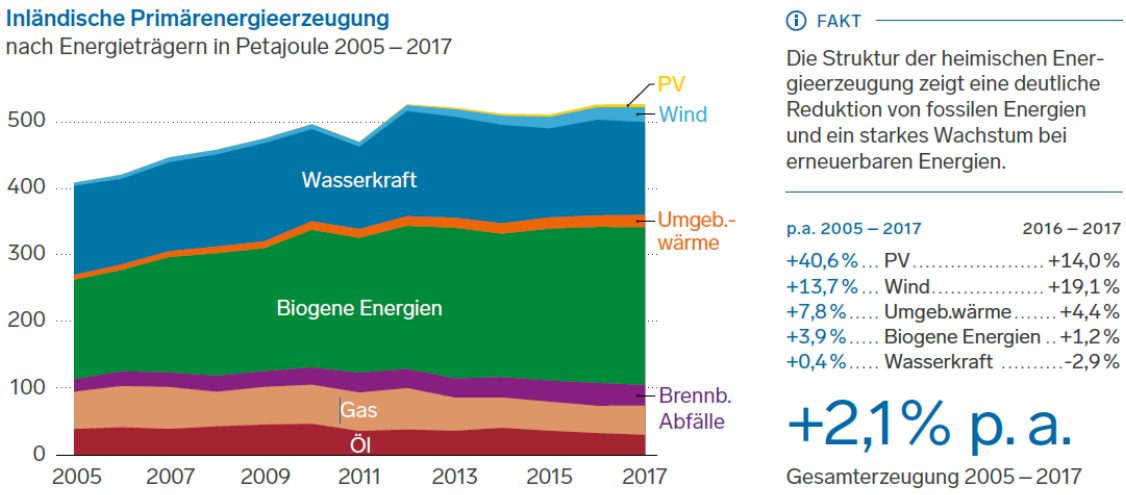

Abbildung 2.1: Inländische Primärenergieerzeugung nach Energieträgern von 2005 bis 2017 [45, p. 8]

In der Abbildung 2.1 ist gut zu erkennen, dass Wasserkraft, biogene Energien und Wind insgesamt ein starkes Wachstum bei der Stromerzeugung in Österreich verzeichnet, ganz im Gegensatz zu fossilen Energien. Dies führt aber auch zur Dezentralisierung der Kraftwerke beziehungsweise Erzeugungsanlagen, was ein zusätzliches Erschwernis im Bezug auf die Ausfallsicherheit bedeutet, da nicht alle Systeme redundant angebunden werden können. Alleine die Vorstellung, dass der Trend von wenigen großen Kraftwerken zu mehreren Tausend Erzeugungsanlagen geht, lässt erahnen, wie komplex ein Energieversorgungsnetzwerk werden kann. Wetterbedingte Schwankungen, beispielsweise durch turbulente Windänderungen bei der Windenergie oder vorbeiziehende Wolken bei der Sonnenenergie [46], bilden eine zusätzliche Herausforderung.

Unter Sektorkopplung versteht man die Vernetzung der beteiligten Sektoren in der Energiewirtschaft, was zu einer Vielzahl neuer Verbraucher führt. Früher betrachtete man die Sektoren Elektrizität, Verkehr und Industrie unabhängig voneinander. Um aber eine ganzheitliche Betrachtung aller Sektoren zu erlangen wurden die Sektoren untereinander vernetzt. Dies geschah nicht ohne Grund, denn dadurch lassen sich folgende Vorteile generieren: [47, p. 556-565]

- Dekarbonisierung[4] der Wirtschaft mithilfe von erneuerbaren Energien

[4]Dekarbonisierung bedeutet die Abkehr von der Nutzung kohlenstoffhaltiger Energieträger in der Energiewirtschaft

- Senkung des Energieverbrauchs durch intelligente Kopplung der Sektoren
- Schaffung funktionaler Speicher, die große Flexibilität in der Nachfrage abdecken und teure Energiespeicher ersetzen
- Energiesicherheit

Die Sektorenkopplung und der Einsatz dezentraler Kraftwerke macht eine Digitalisierung von Netz, Vetrieb und Endverbrauchern notwendig. Dadurch lassen sich beispielsweise viele Systeme zeitnah steuern und sind in der Lage mittels Sensoren Echtzeitdaten zu liefern, auch bei dezentralen Sytemen.

Es ist ein enormer Aufwand notwendig all diese Herausforderungen zu meistern, um weiterhin die Stabilität und Qualität der Stromversorgung zu garantieren. Ein effektiverer Weg zur Reduzierung der Ausfallsicherheit in zukünftigen Elektrizitätsversorgungssystemen ist daher die Resilienz oder näher betrachtet die Cyber-Resilienz. Energiesysteme müssen in der Lage sein, auf unvorhersehbare Störungen zu reagieren und die notwendigen Funktionsfähigkeiten zu behalten beziehungsweise diese so rasch wie möglich wieder zu erlangen.

Digitalisierung als Voraussetzung für Resilienz in der Energiewirtschaft

Die Digitalisierung in der Energiewirtschaft wird als große Chance angesehen, da diese Wissen, Flexibilität und Geschwindigkeit erzeugt. Die Digitalisierung bietet aber im Gegenzug auch Platz für Cyber-Attacken, vor denen das System geschützt werden muss. Daher ist es wichtig, organisatorische, personelle und technische Maßnahmen zu treffen, die das System robuster machen. Die eingesetzten Informations- und Kommunikationstechnologien können aber auch zur Resilienz beitragen, indem Störungen frühzeitig erkannt werden, Gegenmaßnahmen automatisch eingeleitet und Systemdienstleistungen übernommen werden. Zu einer Systemdienstleistung zählt beispielsweise die Fähigkeit, nach einem kompletten Stromausfall die Energieversorgung wieder fortzuführen. Im Fachjargon wird dies „Schwarzstartfähigkeit“ genannt. [42, p. 6-7] Diese Fähigkeit ist vor allem bei einem flächendeckenden Stromausfall wichtig, da ohne sie die erforderliche Leistung zum Start einer Energieerzeugungseinheit die Energie für den Start aus dem Stromnetz genommen wird. Bei einem totalen Stromausfall ist aber nicht mehr genug Energie im Netz, um ein reibungsloses Hochfahren zu gewährleisten. [48] Es zeigt außerdem die wechselseitige Abhängigkeit, weil das Wiederhochfahren der Anlagen über die Telekommunikationsinfrastruktur koordiniert werden muss. [42, p. 6-7]

Generell kann gesagt werden, dass die Digitalisierung der Stromnetze noch hohe Schwankungsbreiten aufweist. Während Hoch- und Höchstspannungsnetze mit modernster Sensoren und IT-Infrastruktur aus-

gestattet sind, ist die Digitalisierung bei Niederspannungsnetzen noch nicht so weit fortgeschritten. [42, p. 7]

Technologien der Digitalisierung im Bereich Energiewirtschaft

In der folgenden Tabelle wird die Wirkungsweise der Digitalisierung nach technischen Lösungen differenziert und beschrieben: [42, p. 8-9]

Technoligien und technologische Lösungsansätze	**Beschreibung**
Sensorik und Aktorik	Das Verhalten der Netzwerke zu analysieren, wird durch Sensoren vereinfacht. Außerdem kann die Planbarkeit verbessert werden, indem Prognosen aus Ableitungen der Messwerte erzeugt werden. Aktoren bieten, beispielsweise durch Abschalten überschüssiger Erzeugungsanlagen, Flexibilität. Durch den Einsatz von Sensoren und Aktoren wird eine flexible Optimierung von Versorgungs- und Verteilnetzen, und auch eine regelmäßige Überwachung aus der Ferne, ermöglicht.
Prosumer	Ist ein zusammengesetzter Begriff aus den Worten Producer (Hersteller) und Consumer (Verbrauch) und drückt aus, dass ein Konsument auch gleichzeitig ein Produzent sein kann, und in intelligenten Energienetzen eine wesentliche Rolle spielt. Verbraucher, wie etwa Besitzer von Solaranlagen am privaten Hausdach, nehmen damit aktiv als Prosumer am Energiemarkt teil. Schiebt sich beispielsweise eine Wolke vor die Sonne, obwohl der Strombedarf hoch ist, muss Strom vom Markt bezogen werden. Gibt es jedoch einen Stromüberschuss, wird der überflüssige Strom ins Netz eingespeist. [49]
Microgrids	Beschreiben ein lokales, abgegrenztes Stromnetz, das nur aus einem oder wenigen Elektrizitätswerken besteht und im Störfall weniger von großen Kraftwerken abhängig ist. Als gutes Beispiel dient die Sicherheitsstromversorgung in einem Krankenhaus oder Rechenzentrum, wo für einen kurzen Zeitraum Autarkie ermöglicht wird. Solche Microgrids sollen zukünftig im größeren Maßstab genutzt werden und zur Resilienz beitragen.

Fortsetzung auf der nächsten Seite

Tabelle 2.2 – *Fortsetzung von der vorigen Seite*

Technoligien und technologische Lösungsansätze	**Beschreibung**
Übergreifende Sektoren	Übergreifende Sektoren, auch integriertes Energiesystem genannt, sind auch heute schon in vielen klassischen Stadtwerken ein Thema. Der Blick richtet sich dabei nicht nur auf den Strom alleine, sondern auch auf andere Sektoren wie Wasser, Wärme oder Gas. Informations- und Kommunikationstechnologien erleichtern die Kopplung dieser Sektoren. Diese Kopplung bietet Vorteile im Hinblick auf Flexibilität in der Speichernutzung und -kapazität sowie der Abhängigkeitenreduktion.
Intelligente Ortsnetzstationen	Diese ermöglichen eine Anpassung des Spannungsniveaus an die aktuelle Netzsituation, um Aufnahmekapazitäten für eine bestimmte Zeit zu erhöhen.
Predictive Maintenance	Predictive Maintenance lässt sich mit dem Begriff „vorausschauende Wartung“ übersetzen und verfolgt einen vorausschauenden Ansatz, in dem Maschinen und Anlagen proaktiv gewartet werden, um Ausfallzeiten so gering wie möglich zu halten. [50]

Tabelle 2.2: Technologien und technologische Lösungsansätze [42, p. 8-9]

Herausforderungen der Digitalisierung in der Energieversorgung

Im Gegensatz zu anderen Energiesystemen, wie Gas oder Wärme, hat das elektrische Netz keine puffernde Funktion. Dadurch ergibt sich die Tatsache, dass es in Echtzeit geregelt werden muss. Mittels Sektorenkopplung soll die Flexibilität anderer Sektoren zur Erleichterung der Regelung der Stromversorgung genutzt werden. Daraus folgt aber auch, dass eine gemeinsame Systemverantwortung von Übertragungsnetzen und Verteilernetzen unabdingbar ist. Unterstützt werden soll dies durch die voranschreitende Digitalisierung. Auch in der Energiewirtschaft sind disruptive Veränderungen wahrscheinlich, was zu einer zusätzlichen Komplexität führt. Auch Schlagworte wie Internet of Things (IoT), künstliche Intelligenz (KI), Blockchain und Cloud-Lösungen sind in der Energiewirtschaft omnipresent. Dazu kommen vernetzte Geräte bei Endkunden, in Form von Smart-Meter-Systemen. [42, p. 9-10]

Der Einsatz all dieser Technologien bietet zweifelsohne viele Vorteile, gleichzeitig aber auch einen Zuwachs an Angriffsvektoren. Somit müssen auch in der Energiewirtschaft die Digitalisierung und die Cyber-Security Hand in Hand gehen. Sobald vernetzte Geräte eingesetzt, Energieressourcen dezentral gesteuert werden oder digitale Prozesse stattfinden, gibt es Angriffsoberflächen. [42, p. 9-10]

Fachgerechte und tagesaktuelle Maßnahmen der IT-Sicherheit sind daher unabdingbar. Technische Mittel wie Datenverschlüsselung, Firewalls und Virenscanner sind zwar notwendig, reichen alleine aber nicht mehr aus. Eine immer gewichtigere Rolle spielen organisatorische Maßnahmen, wie Zutrittskontrollen, Berechtigungsstufen mit Least Privilege und Gefahrenbewusstein der Mitarbeiter durch Schulungen. Die Bundesnetzagentur hat einen eigenen IT-Sicherheitskatalog für Strom- und Gasnetze veröffentlicht. [51] Dieser dient als Unterstützung, um einen angemessenen Schutz gegen Bedrohungen für Informations- und Kommunikationstechnologien zu etablieren.

IT-Sicherheitskatalog für Strom- und Gasnetze

Gemeinsam mit dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) brachte die Bundesnetzagentur einen IT-Sicherheitskatalog speziell für Strom- und Gasnetze heraus. Er dient in erster Linie dem Schutz gegen Bedrohungen, die sich gegen Strom- und Gasnetze richten und den sicheren Betrieb von notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme beeinflussen. Des Weiteren soll dadurch die Integrität der verarbeiteten Informationen und die Vertraulichkeit verarbeiteter Daten geschützt werden. Die Umsetzung der Mindeststandards des Sicherheitskataloges ist für Strom- und Gasnetzbetreiber gleichermaßen verpflichtend. Eine Kernforderung des IT-Sicherheitskataloges ist die Etablierung eines Informationssicherheits-Managementsystems (ISMS) gemäßg DIN ISO/IEC 27001 und dessen Zertifizierung. [51]

In Österreich trat das Netz- und Informationssystemsicherheitsgesetz (NIS-Gesetz) mit 28. Dezember 2018 in Kraft. [52] Dabei wurde die EU-Richtlinie aus 2016 über Maßnahmen zur Gewährleistung eines EU-weiten hohen Sicherheitsniveaus von Netz- und Informationssystemen umgesetzt. Betreiber wesentlicher Dienste müssen dabei geeignete Sicherheitsmaßnahmen treffen und Sicherheitsvorfälle unverzüglich an das Computer-Notfallteam des jeweiligen Sektors melden. Im NIS-Gesetz §17/Abs. 1 [53] heißt es dazu wörtlich: *„Zur Gewährleistung der NIS haben Betreiber wesentlicher Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wesentlichen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar*

ist, angemessen zu sein.“ Betreiber von Strom- und Gasnetzen müssen die Aufrechterhaltung der öffentlichen Versorgung mit Energie gewährleisten, führen daher wesentliche Dienste aus und fallen unter das Netz- und Informationssystemsicherheitsgesetz, sofern eine Voraussetzung im §4 in der Netz- und Informationssystemsicherheitsverordnung (NISV) [54] erfüllt ist.

2.3.4 Resilienz im Ökosystem

Die Ökosystemforschung strebt danach, unter Einbeziehung aller relevanten Faktoren, Entwicklungen innerhalb von Ökosystemen zu verstehen. Untersucht werden dabei die Eigenschaften von Ökosystemen und deren Komponenten, wie etwa die Artenvielfalt oder Stoffkreisläufe. [55]

Die Ökosystemforschung verwendet den Begriff Resilienz ähnlich zu anderen Fachdisziplinen. Es beschreibt die Fähigkeit eines Ökosystems, auf eine Störung reagieren zu können, indem es Schäden widersteht und sich schnell von dem Ereignis erholt. Solche Ereignisse können Brände, Überschwemmungen, Windstürme, Insektenplagen oder aber auch vom Mensch initiierte Aktivitäten sein. Vor allem der Mensch greift mit Abholzung, Bodenfracking zur Ölförderung, Pestiziden oder dem Einschleppen von exotischen Pflanzen- und Tierarten immer mehr in das Ökosystem ein und schwächt dessen Widerstandsfähigkeit. [56, p. 210]

Der Begriff Resilienz wurde das erste Mal vom kanadischen Ökologen Crawford Stanley Holling mit der Ökosystemforschung in Verbindung gebracht. Er führte das Konzept der Widerstandsfähigkeit von ökologischen Systemen ein, um die Persistenz dieser zu beschreiben. [57, p. 4] Crawford Stanley Holling und andere Ökologen beschreiben die Resilienz mit vier kritischen Aspekten [58] : Spielraum, Resistenz, Prekarität und Panarchie.

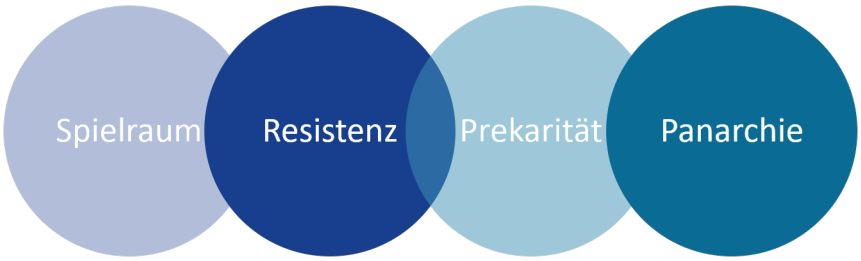

Abbildung 2.2: Die vier kritischen Aspekte der Resilienz in der Ökosystemforschung [58]

Der Spielraum, beziehungsweise Handlungsspielraum, beschreibt den maximalen Betrag, den sich ein System ändern kann, bevor es sich aus eigener Kraft nicht mehr wieder erholen kann. Die Resistenz zeigt, wie widerstandsfähig ein System ist. Respektiv beschreibt es, wie einfach oder schwierig es ist, ein System zu ändern. Die Prekarität gibt an, wie nah der aktuelle Zustand des Systems an einer Grenze oder an einem Schwellenwert liegt. Der Grad, bei dem eine bestimmte Hierarchieebene eines Ökosystem von anderen Ebenen beeinflusst wird, wird Panarchie genannt. So können Organismen, die beispielsweise in Gemeinschaften isoliert voneinander leben, anders organisiert werden als die gleiche Art von Organismen, die in einer großen, kontinuierlichen Population integriert leben.

Menschliche Einflüsse auf die Resilienz des Ökosystems

Es gibt viele Bereiche, in denen menschliche Aktivitäten Auswirkungen auf die Resilienz des terrestrischen[5], aquatischen[6] Ökosystems haben. Eine intensive Landwirtschaft, um der Nahrungsmittelnachfrage gerecht zu werden, in Kombination mit der Verwendung von Herbiziden zur Bekämpfung von Unkraut oder Insekten, führen zum Insektensterben und zur Verringerung der Pflanzenvielfalt, sowie zur Verringerung der Bodenfruchtbarkeit. [59] Eine nachhaltigere Landwirtschaft würde die Resilienz des Nährbodens berücksichtigen.

Weitere Beispiele für den menschlichen Einfluss auf das Ökosystem sind die Abholzung oder der Raub-

[5] Terrestrische Ökosysteme sind Ökosysteme der festen Landoberfläche
[6] Aquatische Ökosysteme sind im Gegensatz zu terrestrischen Ökosystemen alle Ökosysteme mit Wasserbezug

bau von Wäldern. Man spricht dann von der Abholzung, wenn die Resilienz des Waldes überschritten wurde. Er verliert somit die Fähigkeit, seinen ursprünglichen stabilen Zustand wiederherzustellen. Um sich erholen zu können, benötigt das Ökosystem des Waldes ein optimales Zusammenspiel aus Klimabedingungen und genügend Fläche. Die Resilienz eines Waldsystems ist ohnehin nicht stark ausgeprägt und ermöglicht nur eine Erholung von einem relativ geringen Schadensausmaß, wie beispielsweise einem Blitzschlag oder einem Erdrutsch. [60]

Die Überfischung ist ebenfalls ein menschlicher Eingriff in das Ökosystem. Sie bedroht die Resilienz des marinen Ökosystems und ist eine der treibenden Kräfte für den Rückfall der Meeresfauna. Der Fischfang wird vom WWF[7] als prinzipiell „nicht schlecht“ empfunden, außer wenn Schiffe schneller Fische fangen, als das Meer seine Bestände wieder auffüllen kann. [61] Geschuldet ist dies zum einen der hohen Nachfrage nach Fisch und zum anderen der rasanten Entwicklung der Fischereitechnologie. [62]
Weitere, nicht weniger nennenswerte, menschliche Einflüsse in Ökosysteme, welche mit resilienten Ansätzen erforscht werden, sind beispielsweise die Müllablagerung in marinen Systemen oder die Vergiftung durch Öl von marinen Systemen.

Nachhaltige Entwicklung

In der Bevölkerung wächst das Bewusstsein, dass ein besseres Verständnis und eine stärkere Gewichtung auf die Resilienz im Ökosystem erforderlich ist um die Ziele der nachhaltigen Entwicklung zu erreichen. [63] Im September 2015 wurden am UNO-Gipfel die 17 Ziele für nachhaltige Entwicklung definiert und von 193 Ländern einstimmig angenommen. Neben der Bekämpfung von Armut und Hunger, schmutziges Wasser und der Gewährleistung für ein gesundes Leben für Menschen allen Alters, sind auch der nachhaltige Konsum und die Produktion, sowie Maßnahmen zum Klimaschutz, Thema. [64]

In Schweden wurde beispielsweise das Stockholm Resilience Center (SRC) als gemeinnütziges, unabhängiges Forschungsinstitut gegründet, das sich auf nachhaltige Entwicklung und Umweltfragen spezialisiert hat. Es befasst sich unter anderem mit den Themen Klimawandel, Landschaftsnutzung, Wasserressourcen, Ernährungssicherheit, Meeressysteme und städtische Systeme mit dem Ziel, Erkenntnisse zu gewinnen, wie diese nachhaltiger genutzt oder vermieden werden können. Das Institut legt dabei den Schwerpunkt auf die Resilienz dieser Gebiete. [63]

[7] Die World Wide Fund For Nature ist eine non-profit Umweltschutzorganisation

2.3.5 Resilienz in der Soziologie

Die Soziologie beschäftigt sich einerseits mit dem individuellen menschlichen Verhalten, andererseits mit dem kollektiven Handeln und dessen Auswirkungen auf das Zusammenleben von Menschen. Sie umfasst die Grundlagen sozialer Beziehungen, sozialer Interaktionen und gesellschaftlicher Probleme und deren Bewältigung. [65, p. 3-5]

Die Resilienz hält auch in der Soziologie Einzug und beschreibt die Fähigkeit von Gesellschaften, wie diese externe Störungen, wie beispielsweise Naturkatastrophen, mittels aller verfügbaren Ressourcen (Energie, Kommunikation, Transport,...) bewältigen und aus ihnen lernen können. Durch den Lernfortschritt sollen sich Gesellschaften besser an zukünftige Herausforderungen anpassen können.

Charlie Edwards hat beispielsweise das 4-R-Modell entwickelt, um zu erforschen, welche Faktoren die Resilienz einer Gesellschaft steigern sollen. Das Modell beschreibt die Faktoren der Resilienz gegenüber Naturkatastrophen oder terroristischen Anschlägen; kennzeichnet eine hoch resiliente Gesellschaft und besteht aus folgenden vier Punkten: [66, p. 75-76]

- Robustheit (Robustness)
- Redundanz (Redundancy)
- Einfallsreichtum (Resourcefulness)
- Schnelligkeit (Rapidity)

Die Robustheit beschreibt das Potential eines Systems, mit Belastungen umzugehen, ohne wesentliche Funktionen einzubüßen. Dies soll auch mit Hilfe der Redundanz geschehen. Sie soll alternative Funktionen zu den Hauptfunktionen bieten, damit lebenswichtige Aufgaben eines Systems fortgeführt werden können. Die Robustheit und Redundanz dienen in erster Linie der Schadensbegrenzung und -vorsorge. Der Einfallsreichtum hilft als Indikator, wie kreativ ein System auf Schadensereignisse reagiert, während sich die Schnelligkeit mit der (raschen) Reaktions- und Regenerationsfähigkeit eines System beschäftigt.

Klassifizierung von Gefahren

In der Soziologie wird die Resilienz als Fähigkeit der Gesellschaft verstanden, mit externen Störungen, unter Einbeziehung der verfügbaren Ressourcen, umzugehen, und aus diesen zu lernen. Der Tragweite der gesellschaftlichen Resilienz wirkt nicht nur gegenüber Naturkatastrophen, sondern umfasst auch von Menschen verursachte Ereignisse. Neben den bekannten Naturkatastrophen wie Orkane[8], Erdbeben,

[8] Als Orkane gelten Winde mit mindestens 117 km/h [67, p. 125-126]

Feuer, Tsunami und vielen mehr, kann beispielsweise auch ein Cyberkrieg als externe Störung gelten.

Zusammenfassend lassen sich diese, wie im NIST-Leitfaden [68, p. 25] beschrieben, in drei Gefahrenklassifizierungsstufen unterteilen:

- routinemäßige Ereignisse
- aufbauende Ereignisse
- extreme Ereignisse

Unter routinemäßige Ereignisse fallen jene, die regelmäßig auftreten und in der Regel begrenzte Auswirkungen haben und bei denen die Wiederherstellung rascher vonstatten geht. Im Gegensatz dazu gibt es extreme (Gefahren-) Ereignisse, die wahrscheinlich erhebliche und irreparable Schäden verursachen. Auch die Erholungsphase ist bedeutend länger als bei routinemäßigen Ereignissen. Extreme Ereignisse treten jedoch seltener in Erscheinung als routinemäßige, sollten aber auf keinen Fall außer Acht gelassen werden.

2.4 Zusammenfassung der Resilienzforschung

Die Resilienz ist mittlerweile in vielen Fachdisziplinen zum festen Bestandteil geworden. Sie beschreibt ein Szenario, dem zumindest ein negatives Ereignis zu Grunde liegt. Durch die Resilienz kehrt das betroffene Individuum oder System wieder zum ursprünglichen Zustand, welcher vor diesem Ereignis bestand, zurück.

Vereinfacht beschreibt die Resilienz die Widerstandsfähigkeit auf Stressoren. Die zuvor beschriebenen Beispiele aus unterschiedlichen Forschungsgebieten sollen deutlich machen, dass sich Individuen oder Systeme unterschiedliche Strategien aneignen, wenn sie auf Stressoren treffen, um danach wieder in den ursprünglichen Ausgangszustand zurückzukehren. Es ist daher nicht weit gegriffen, dass auch Computersysteme Strategien entwickeln können, um resilient gegen Stressoren zu werden.

Zum besseren Verständnis der folgenden Kapitel ist die Begriffsdefinition der allgemeinen Resilienz notwendig, da im weiteren die Anti-Fragilität auf der Cyber-Resilienz aufbaut, und somit die grundlegende Aufgabe der Resilienz benötigt wird.

3 Cyber-Resilienz

Unternehmen haben ein sich wandelndes Verhältnis zur Technologie, wobei Unternehmen meist von den Fähigkeiten dieser abhängig sind. So bietet der Einsatz von Informationstechnologien für Unternehmen beträchtliche Vorteile, um beispielsweise Produkte, Dienstleistungen und Leistung zu verbessern oder Betriebskosten zu senken. Diese Möglichkeiten führen jedoch mit hoher Wahrscheinlichkeit zu neuen Schwachstellen und zusätzlichen Bedrohungen, die zu direkten finanziellen Verlusten oder zum Verlust des geistigen Eigentums führen, was teilweise Reputationsschäden für die Organisation oder das Unternehmen bedeutet. [69] Die Zunahme der Cyberangriffe ist heutzutage offensichtlich und wird auch noch in absehbarer Zukunft eine bestehende Gefahr bleiben. In Anbetracht dieser Realität muss auch davon ausgegangen werden, dass Ausfälle irgendwann unvermeidlich sind. Das Ziel einer jeden Organisation beziehungsweise eines jeden Unternehmens sollte daher sein, bei Eintritt eines Cybervorfalls den normalen Betrieb so gut wie möglich fortfahren zu können, beziehungsweise so schnell wie möglich wiederherzustellen. [70, p. 16] Hier kommt der Begriff „Resilienz“ bei Systemen ins Spiel. Dabei wird primär nicht von der Verhinderung von Störungen gesprochen, sondern von der Fähigkeit, nach einer Störung wieder eine Stabilität herzustellen und womöglich sogar aus dieser zu lernen.

3.1 Cyber-Resilienz und die Abgrenzung zur Cyber-Security

Der Begriff „Cyber“ steht oft im Zusammenhang mit anderen Worten. So sind die Schlagworte Cyberkriminalität, Cyber-Mobbing oder Cyber-Security laufend zu lesen und werden täglich von Medien, Fachpersonal, aber auch Endbenutzer verwendet.

3.1.1 Cyber

Cyber ist ein Wortbildungselement und wird im Duden [71] mit der Bedeutung *„die von Computern erzeugte virtuelle Scheinwelt betreffend“* beschrieben.

Das Wort stammt ursprünglich aus dem Griechischen und hatte dort die Bedeutung „Steuerung“. Verwendet wurde es im Zusammenhang mit der Navigation eines Schiffes. Wissenschaftlich wurde der Begriff das erste Mal vom Mathematiker Norbert Wiener im Jahr 1948 verwendet. [72] In die deutsche Spra-

che übernommen bedeutet „Kybernetik“ die Wissenschaft der Steuerung und Regelung von Maschinen, lebenden Organismen und sozialen Organisationen. [73, p. 278-279] Mit der Informationstechnik in Verbindung kam der Begriff das erste Mal in den 70er-Jahren auf, wo er als Markenname für den damals leistungsstärksten Großcomputer der Welt diente. [72]

3.1.2 Cyber-Security vs. Cyber-Resilienz

Für Cyber-Security existieren viele unterschiedliche Definitionen. Das Oxford Dictionary beschreibt diese wie folgt: *„Der geschützte Zustand vor der kriminellen oder unbefugten Verwendung elektronischer Daten oder die dafür zu treffenden Maßnahmen.“* [1] Im Merriam-Webster's Collegiate Dictionary wird sie folgendermaßen formuliert: *„Maßnahmen zum Schutz eines Computers oder Computersystems vor unbefugtem Zugriff oder Angriffen.“* [74] Auch bei Organisationen wird der Begriff Cyber-Security in unterschiedlichen Zusammenhängen verwendet. Das Normungskomitee ISO/IEC JTC 1 definiert die Cyber-Security mit: *„Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen im Cyberspace.“* [75, p. 15] Unter Vertraulichkeit wird verstanden, dass Daten nur von Personen, die berechtigt sind, eingesehen beziehungsweise verändert werden. Die Verfügbarkeit beschreibt simpel die Zeit, in der ein System funktionsfähig ist. Das Ziel ist, das System permanent beziehungsweise so lange wie möglich funktionstüchtig zu halten. Im Glossar des Bundesamtes für Sicherheit in der Informationstechnik [76] wird die Integrität wie folgt dargelegt: *„Die Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.“* Das bedeutet, dass die gesendeten Daten nachweislich, unverändert und mit dem korrekten Inhalt den Empfänger erreichen. Das National Institute of Standards and Technologie (NIST) ist eine Bundesbehörde für Standardisierungsprozesse in den Vereinigten Staaten, die 2011 eine eigene Definition zur Cyber-Security herausbrachte: *„Cybersecurity ist die Fähigkeit, die Nutzung des Cyberspaces vor Cyberangriffen zu schützen oder zu verteidigen.“* [75, p. 17]

Die Resilienz charakterisiert generell die Widerstandsfähigkeit gegen Störungen jeder Art, Anpassungsfähigkeit an neue Bedingungen und eine flexible Reaktionen auf Veränderungen. [76] Auch in der Informationstechnologie findet die Resilienz Einzug. Als Cyber-Resilienz beschreibt sie die Fähigkeit eines Systems, unter Berücksichtigung der Eigenschaften der Resilienz, mit Veränderungen umgehen zu können. Die MITRE Corporation definiert Cyber-Resilienz folgendermaßen: *„Cyber-Resilienz ist die Fähigkeit sich von widrigen Bedingungen, Belastungen oder Angriffen bezüglich Cyberressourcen zu antizipieren, sich von ihnen zu erhohlen, ihnen zu widerstehen und sich ihnen anzupassen.“* [77, p. 1] Auch die Europäische Zentralbank liefert eine ähnliche Definition: *„Cyber-Resilienz bezieht sich auf die*

Fähigkeit, elektronische Daten und Systeme vor Cyberangriffen zu schützen und den Geschäftsbetrieb im Falle eines erfolgreichen Angriffs schnell wieder aufzunehmen.“ [78] Das resiliente System soll somit selbstständig und dynamisch nach einem gelungenen Angriff, die „richtigen“ Dinge tun und kritische Dinge unterbinden, um kontinuierlich das beabsichtigte Ergebnis zu erzielen.

Zusammenfassend kann beschrieben werden, dass die Cyber-Security vielen Definitionen unterliegt, aber im Mittelpunkt immer der Schutz des Systems steht. Gelingen soll dies mit einer starken Verteidigung, um Angriffe erfolgreich abzuwehren. Die Cyber-Resilienz hat als zusätzliche Features noch die Fähigkeiten, sich auf Vorfälle einzustellen, ihnen entgegenzuwirken und das System nach einem gelungenen Angriff wiederherzustellen.

3.2 Google Trend Analyse

Eine Suchabfrage - Ergebnisse auf Österreich begrenzt - nach dem Begriff „Cyber“ liefert ungefähr 1 200 000 Ergebnisse (Stand: 01.07.2019, 15:00 Uhr). Dieses Ergebnis lässt erahnen, wie umfangreich, komplex und vielschichtig das Kapitel rund um die Informationstechnologie mittlerweile geworden ist.

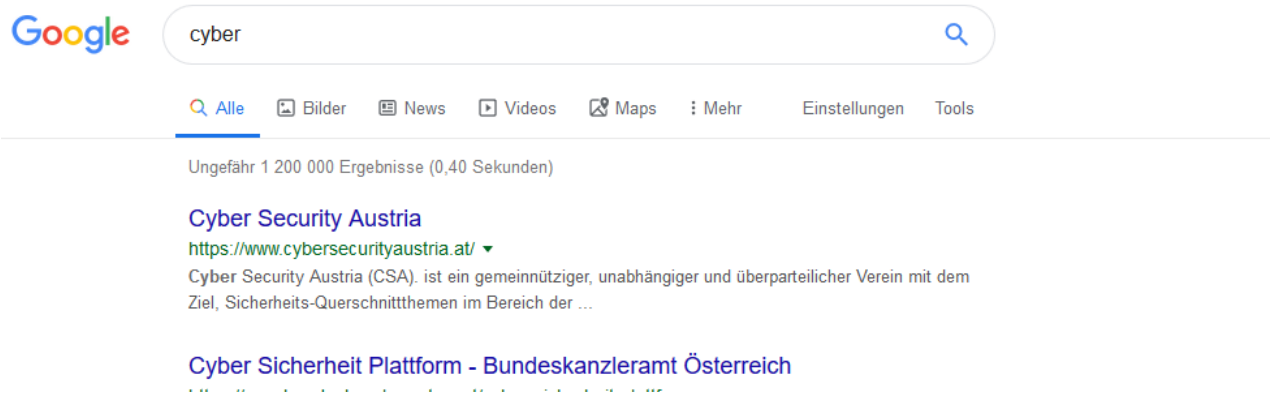

Abbildung 3.1: Google-Suche nach „Cyber“ (Stand: 01.07.2019, 15:00 Uhr)

Schnellere, billigere, digitale Technologien bieten eine beispiellose Reihe von sozialen und wirtschaftlichen Vorteilen, und der Prozess der Digitalisierung wird nicht langsamer. Dies bringt aber eine Reihe neuer Risiken mit sich und lässt das Thema „Cyber-Security“ bei Wirtschafts- und Regierungschefs ganz oben auf der Agenda stehen. So liefert die Abfrage nach dieser ein fast ebenso hohes Ergebnis (ungefähr 1 100 000 Ergebnisse (Stand: 01.07.2019, 16:20 Uhr)), wie die Abfrage nach „Cyber“ selbst:

Abbildung 3.2: Google-Suche nach „cyber security“ (Stand: 01.07.2019, 16:20 Uhr)

Auch die Abfrage zum Begriff „cyber security“ beschränkte sich auf das Land Österreich. Nicht nur die Sicherheit selbst ist von großer Bedeutung, sondern auch die Resilienz bei Informationstechnologien, wie das World Economic Forum [79] in diesem Artikel schreibt: Um einerseits das volle Potenzial der digitalen Landschaft auszuschöpfen, andererseits das Schadenspotenzial gering zu halten, sollte die „Cyber-Resilienz“ als strategisches Ziel betrachtet werden.

In den letzten Jahren ist eine stark steigende Anzahl von bekannten Schwachstellen bei Computersystemen erkennbar. Alleine im Jahr 2017 [80] explodierte die Anzahl neu publizierter Sicherheitslücken auf der Common Vulnerabilities and Exposures-Liste (CVE®)[1] mit 14714. Dieser Spitzenwert wurde 2018 [82] mit 16556 Sicherheitslücken nochmals übertroffen und wird in der nahen Zukunft womöglich noch weiter steigen. Es ist somit nicht verwunderlich, dass gleichzeitig die Ausgaben für die Cyber-Security ansteigen. Wie die Abbildung 3.3, repräsentativ für die Vereinigten Staaten, zeigt, steigen die Investitionen in die Sicherheit von Informationssystemen von Jahr zu Jahr an und haben 2017 bereits 0,35% des Bruttoinlandsprodukts der USA betragen.

[1] CVE ist eine Liste mit bekannten, öffentlich zugänglichen Sicherheitslücken. Jeder Schwachstelle ist dabei eine eindeutige CVE-Nummer von einer CVE-Numbering Authority (CNA) zur Identifikation zugewiesen. Mehrfachbenennungen von Sicherheitslücken werden zusammengefasst - mit dem Ziel, eine einheitliche Namenskonvention für Schwachstellen bei Computersystemen zu schaffen. [81]

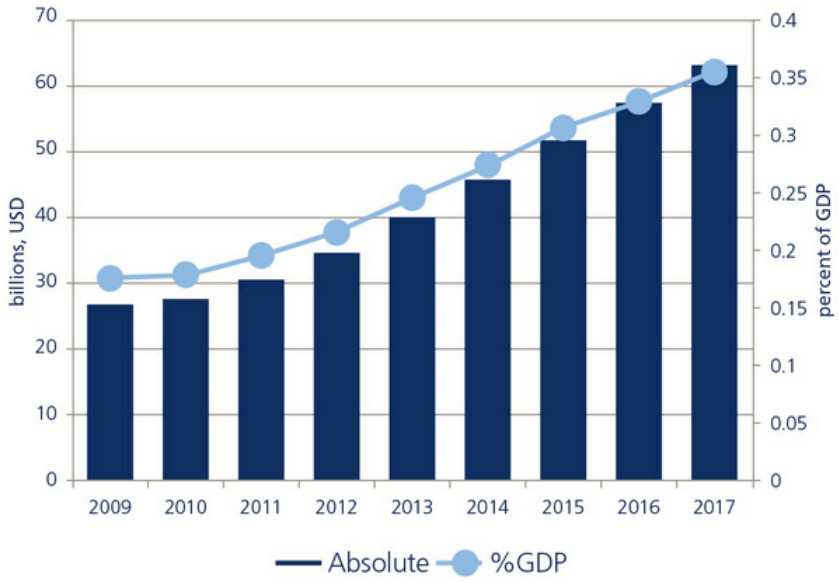

Abbildung 3.3: Cybersicherheitsausgaben in den USA [83]

Unternehmen können aber auch Tools und Richtlinien zur Vermeidung oder Minderung von Gefahren entwickeln. Hier tritt die Idee der (Cyber-) Resilienz auf den Plan. Die Grundidee der Cyber-Resilienz ist eine Bewertung dessen, was passiert vor, während und nachdem ein digital vernetztes System auf eine Bedrohung stößt. Der Begriff „Resilienz“ sollte dabei nicht als Synonym für die Wiederherstellung verstanden werden, sondern eine auf lange Sicht entstehende „Widerstandskraft“ mit einem breiten Spektrum an Fähigkeiten. Aus zwei Gründen sollten Unternehmens- und Regierungschefs über die Cyber-Resilienz nachdenken: [79]

- Durch den Alles-oder-Nichts-Ansatz bei der Cyber-Security (Verhindern des Netzwerkeintritts als einziger Plan der Verteidigung) ist ein totaler Ausfall möglich.
- Die Cyber-Resilienz stellt sicher, dass die Kommunikation über Informationstechnologien und der Cyber-Security hinausgeht.

So ist es nicht verwunderlich, dass die Suche nach (Cyber-) Resilienz - Ergebnisse auf das Land Österreich begrenzt - mit ungefähr 457 000 beziehungsweise 35 300 Ergebnissen (Stand: 01.07.2019, 16:12 Uhr) eine beachtliche Trefferanzahl liefert.

Der Interessenanstieg für die Cyber-Resilienz lässt sich mittels der Google Trend Analyse bestätigen. Wie in Abbildung 3.4 erkennbar, stieg das Suchinteresse seit 01.06.2009 weltweit an.

Abbildung 3.4: Google Trend Analyse für den Begriff „cyber resilience“ von 01.06.2009 bis 01.06.2019

Die Trend Analyse von Google geht dabei vom höchsten Wert von Suchanfragen aus, der 100% ergibt und rechnet die Werte der anderen Tage und Monate im Vergleich aus. Die Werte geben somit das Suchinteresse relativ zum höchsten Punkt im Diagramm wieder.

Vor allem in den Ländern Australien, Vereinigtes Königreich, die Vereinigten Staaten, Indien und Deutschland ist das Suchinteresse für die Cyber-Resilienz groß, wie bei Abbildung 3.5 erkennbar. Der Wert 100 wird an den Standort vergeben, an dem anteilig zur Gesamtzahl der Suchanfragen die höchste Beliebtheit erzielt wurde, in diesem Fall Australien.

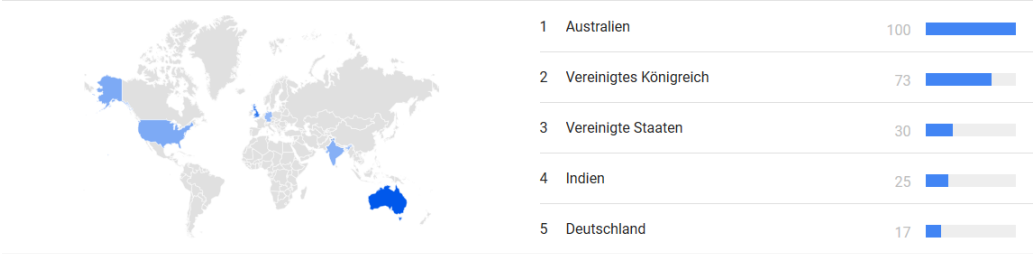

Abbildung 3.5: Google Trend Analyse für den Begriff „cyber resilience“ nach Ländern

3.3 Akzeptanz für Cyber-Resilienz schaffen

Cyber-Risiko und Cyber-Resilienz spielt nicht nur in der Informationstechnologie oder in Fachgebieten des Ingenieurwesens eine Rolle, es ist vielmehr ein Thema für die Entscheidungsgremien des Unternehmens, die letztlich die Verantwortung für die Überwachung des Cyber-Risikos und der Resilienz inne haben. Unternehmen werden zunehmend für ihre Cybersicherheit zur Verantwortung gezogen, auch deshalb sollten Cyber-Risiken und -Resilienz Kernthemen in der unternehmerischen Entscheidungsfindung sein. Oft werden diese Themen an die IT-Abteilung abgeschoben. Diese sollte zwar mit einbezogen werden, die letztliche Verantwortung liegt aber bei der Unternehmensführung. [69] Walter Bohmayr und

Alexander Türk von der Boston Consulting Group definierten dies so: *„Die Cyber-Resilienz in einer Organisation muss sich über den technischen IT-Bereich hinaus auf die Bereiche Menschen, Kultur und Prozesse erstrecken. Die Schutzstrategien einer Organisation sollten für alles gelten - für jeden Prozess auf jeder Ebene, über Abteilungen, Einheiten und Grenzen hinweg - um eine angemessene Sicherheitskultur zu fördern.“* [84]

Dazu empfiehlt der BSI Standard 31111 [69] ein eigenes Richtlinien-Dokument zu Cyber-Risiko und -Resilienz zu erstellen, dieses zu pflegen und regelmäßig zu aktualisieren. Es beinhaltet die wichtigsten Erwartungen und Grundsätze für das Unternehmen, und richtet sich an Managementstandards, wie den der ISO/IEC-27000-Reihe [85] oder der ISO 31000. [86] Die Geschäftsführung sollte dadurch in der Lage sein, folgende Punkte beantworten zu können: [69]

- Sind alle Assets eines Systems, die Bedrohungen zu diesen Assets, und die Anfälligkeit des Systems auf die Bedrohungen identifiziert?
- Sind ausreichend Präventions- und Reaktionsfähigkeiten verfügbar, um einen Cyber-Vorfall zu bewältigen?
- Wie reagiert die Organisation auf Veränderungen in der Cyber-Landschaft und wie versteht sie diese?
- Werden angemessen viele Ressourcen (Geldleistung, Arbeitsleistung, Technologie) zur Verfügung gestellt, um die Ziele der Cyber-Resilienz zu erreichen?

Die Geschäftsleitung sollte ihr Verständnis, ihre Verantwortung und ihre Führungsrolle in der gesamten Organisation unter Beweis stellen, indem angemessene Governance-, Risikomanagement- und Investitionsentscheidungen getroffen werden, die die Resilienz gegen Cyberangriffe und andere disruptive Events erhöhen. [69]

IT-Manager leiden oft unter Problemen in der Kommunikation mit der Geschäftsführung über Sicherheitsprobleme, mit denen das Unternehmen konfrontiert ist. Oft hilft es die Folgen klarzumachen, denn Cyber-Bedrohungen werden immer ausgefeilter und bisher gesetzte Maßnahmen sind oft unzureichend, was in Folge zu kostspieligen Konsequenzen und kostenintensivem Reputationsverlust führen kann. [87] Sicherheitsvorkehrungen in der Cyber-Landschaft alleine berücksichtigen oft nicht ausreichend die allgemeinen Faktoren des Geschäftsrisikomanagements, die sich negativ auf die Resilienz der Organisation auswirken können. Ein zu eng gefasster Scope führt unter anderem zu [69]:

- Durchführung von Projekten, die sich auf die Vorteile eines digitalen Systems konzentrieren, ohne

die aktuellen und teilweise auch erwarteten Bedrohungen zu berücksichtigen

- Potenzial für erhebliche Kaskadeneffekte[2]

3.4 Cyber-Resilienz Design Principles

Wie sieht ein resilientes System aus beziehungsweise wie kann ein resilientes System erstellt werden? Im „Cyber Resiliency Design Principles"-Paper [89] der MITRE Corporation werden hierfür mehrere Design Principles für unterschiedliche Phasen, von der Identifizierung der Anforderungen bis hin zur Wartung des Systems, vorgestellt. Sie dienen als Grundlage für ein resilientes System. Dabei wird zwischen strategischen und strukturellen Design Principles unterschieden.

3.4.1 Strategische Design Principles

Die strategischen Design Principles richten sich an das Risikomanagement eines Unternehmens. Sie umfassen Annahmen über mögliche Bedrohungen, die Entscheidungsfindung im Risikomanagement und die Prioritätensetzung im Zusammenhang mit dem Erreichen der Cyber-Resilienz-Ziele. [89, p. 8] Das Risikomanagement eines Unternehmens wird durch Faktoren, wie beispielsweise finanzielle Ressourcen, rechtliche und vertragliche Anforderungen, begrenzt. [90]

Fokus auf verbreitete kritische Assets

Da Ressourcen limitiert sind, müssen sie dort eingesetzt werden, wo sie den größten Nutzen bringen. Das Risikomanagement sollte sich daher in erster Linie auf Assets konzentrieren, die kritisch und weit verbreitet sind. [89, p. 10] Kritische Assets können mit Hilfe von Analysetechniken identifiziert werden. Hierfür bietet sich etwa die Business-Impact-Analyse (BIA) [91] aus dem Business Continuity Management (BCM) [92, p. 4] an.

Agilität und eine anpassungsfähige Architektur

Die Bedrohungslandschaft ändert sich nicht nur aufgrund der Entwicklung des Gegners, sondern auch wegen der eingesetzten Technologien und der Art, wie diese verwendet werden. Mit diesem Prinzip soll die Notwendigkeit von Flexibilität und Anpassungsfähigkeit als Teil des Risikomanagements anerkannt werden. [89, p. 11] Mit Hilfe der Agilität soll dem System und den betrieblichen Prozessen die Möglich-

[2] Unter Kaskadeneffekt versteht man eine unvermeidliche und manchmal unvorhergesehene Kette von Ereignissen, die auf eine bestimmte Handlung zurückzuführen sind. [88]

keit geboten werden, neue Technologien einzubeziehen und sich an ändernde Fähigkeiten des Gegners anzupassen. [89, p. 11]

Angriffsoberfläche reduzieren

Je größer die Angriffsoberfläche[3] ist, desto schwieriger ist diese zu verteidigen. Sie erfordert eine ständige Überwachung auf Anomalien. Diese müssen anschließend analysiert und darauf reagiert werden. Durch die Reduzierung der Angriffsoberfläche können Ressourcen eingespart werden und die Überwachung sowie die Verteidigung konzentrieren sich auf eine kleine Anzahl von Standorten, Ressourcen oder Umgebungen. [94, p. 175-176]

Akzeptieren, dass Ressourcen kompromittiert sein können

Bei vielen Systemen wird der Großteil der verbundenen Ressourcen als nicht böswillig betrachtet. Die Devices innerhalb eines Netzwerkes werden als vertrauenswürdig angesehen und der Sicherheitsgedanke gerät in den Hintergrund. Die bessere Annahme wäre jedoch, alle Ressourcen als kompromittiert anzusehen beziehungsweise das Netzwerk als nicht vertrauenswürdig zu erachten. [89, p. 13] Die US-amerikanische stellvertretende Verteidigungsministerin für Forschung und Technik fasste dies folgendermaßen zusammen [95]: *„Unabhängig davon, wie sicher ein Computernetzwerk oder dessen Umgebung ist, scheint es besser zu sein, wenn der Benutzer einfach davon ausgeht, dass es kompromittiert ist.“* Früher stellte man sich die Netzwerksicherheit bildlich in Form einer Mauer rund um das Netzwerk vor. Sobald sich ein Benutzer darin befindet, kann er sich frei bewegen. Ein resilientes System erfordert allerdings mehr als nur die Errichtung einer Barriere um das Netzwerk. Der Trend geht zur „Zero-Trust-Architektur“, in der das Netzwerk in kleine Zonen unterteilt wird, wo besondere Zugriffsrechte für diese Mikronetze erforderlich sind. [95]

Akzeptieren, dass sich der Gegner weiterentwickelt

Angreifer werden immer fortschrittlicher und verwenden ausgeklügelte Angriffsvektoren, um Systeme zu kompromittieren. Ein mehr als aktuelles Thema ist beispielsweise der Angriff auf kritische IT-Infrastrukturen mittels Advanced Persistent Threats (APTs). [96] Bei diesen Angriffen werden Hackergruppierungen oft von Staaten unterstützt, die viel Zeit, Geld und Informationen investieren. Diese An-

[3] Die Angriffsoberfläche wird im Cybersecurity Test and Evaluation Guidebook vom Department of Defense (DoD) wie folgt beschrieben: *„Sie ist die Exposition des Systems gegenüber erreichbaren und ausnutzbaren Schwachstellen. Mit anderen Worten: Jedes Hardware, Software, Datenverbindung, Service, Wechselmedium, etc. die das System potenziellen Bedrohungszugriffen aussetzen könnten.“*[93, p. 24]

griffe gehen üblicherweise über einen längeren Zeitraum und kombinieren oft mehrere Angriffsvektoren mit dem Ziel, das Opfer auszuspionieren, wie beispielsweise Wirtschaftsspionage, oder Sabotage zu betreiben. [97] Da diese Angriffe nicht im Vorhinein genau planbar sind, müssen resiliente Systeme auch gegen unerwartete Angriffe stabil sein. Herkömmliche Schwachstellenscans reichen da alleine nicht mehr aus. Vielmehr spricht sich dieses Prinzip für eine Analyse aus, bei der intelligente Akteure die Rolle des Gegners einnehmen, wie beispielsweise beim Cyber Red Teaming. [89, p. 13-14]

3.4.2 Strukturelle Design Principles

Wie zuvor beschrieben, befassen sich die strategischen Design Principles mit der Risikomanagementstrategie einer Organisation. Die strukturellen Design Principles sollen sie dabei unterstützen. [89, p. 14] Sie bieten einen Leitfaden für Implementierungsentscheidungen über den gesamten Systemlebenszyklus hinweg mit Blick in Richtung Risikominderung. [98, p. 105]

Begrenzung vertrauenswürdiger Systemelemente

Die Idee hinter diesem Prinzip ist, die Anzahl von jenen Systemelementen zu verringern, denen vertraut werden kann. Dies reduziert den Aufwand, der betrieben werden muss, um das System zu Überwachen und so folglich die Sicherheit laufend zu gewährleisten. [98, p. 105] Die Reduzierung der Gruppe von vertrauenswürdigen Entitäten senkt dabei auch die Angriffsoberfläche, da die Entitäten außerhalb dieser Zone ohnehin als kompromittiert angesehen und auch so behandelt werden. [89, p. 16]

Sichtbarkeit und Verarbeitung einschränken

Ein wichtiger Punkt ist, die Kontrolle darüber zu behalten, was entdeckt, beobachtet und verwendet werden kann. Das erhöht den Aufwand für den Gegner, potenzielle Ziele zu identifizieren, erheblich. [98, p. 106] Die Sichtbarkeit der Daten kann mit Hilfe von Mechanismen, wie Datenverschlüsselung, Data Hiding[4] oder Obfuscation[5] eingeschränkt werden. Ein straffes und aktuell gehaltenes Berechtigungskonzept mit dem Least Privilege Prinzip hält einen Angreifer, bei einem gelungenen Einbruch, ebenfalls in einem kleinen Bereich fest. [89, p. 17-18]

[4] Data Hiding ist ein Konzept in der objektorientierten Programmierung, wo Daten unterschiedlich gekapselt werden. Die Daten werden dabei so gekapselt, dass nur die Daten sichtbar sind, die zu einem gewissen Zeitpunkt auch sichtbar sein sollen. [99]

[5] Bei Obfuscation wird ein Programmcode mit Absicht verändert. So können beispielsweise Variablennamen absichtlich anders benannt werden, als sie eigentlich bedeuten. Dies wird gemacht, um den Quellcode für Menschen schwer verständlich zu machen beziehungsweise das Reverse Engineering zu verkomplizieren. [100]

Verhaltensweise kontrollieren und limitieren

Eingeschränkte Handlungsmöglichkeiten verringern das Ausmaß einer Ausbreitung von Störungen über Komponenten oder Services hinweg. Das Ausschließen von bestimmten Verhaltensweisen verhindert, dass diese zu unerwünschten Konsequenzen führen. So könnten beispielsweise bestimmte Benutzeraktivitäten außerhalb eines bestimmten Zeitfensters blockiert werden. Diese Limitierung erfordert jedoch ein laufendes Monitoring, damit Anomalien abweichend vom normalen Verhalten erkannt werden können. [89, p. 19] Im Fachjargon wird dies User Behavior Analysis (UBA) [101] genannt. Ursprünglich ist dieses Werkzeug zur Analyse des Kaufverhaltens von Kunden für Marketingzwecke erstellt worden. Heute wird es im Security-Kontext erstens zum Aufzeichnen des normalen User-Verhaltens zur Verbesserung des eigenen Systems und zweitens zum Aufdecken von böswilligem Verhalten verwendet.

Schutz durch den Einsatz mehrerer Verteidigungsschichten und Partitionierung

Die Kombination von den Konzepten Defense-in-depth und Partitionierung erhöht ebenfalls, aufgrund der Mehrfachverteidigung, die Sicherheit eines Systems. Der Angreifer muss dadurch viel mehr Aufwand betreiben, um im System Fuß fassen zu können. [98, p. 106] Bei der Sicherheitsstrategie Defense-in-depth werden mehrere Mechanismen aufgebaut, um eine Reihe von Barrieren zu schaffen. Das Committee on National Security Systems (CNSS) beschreibt die Strategie folgendermaßen [102, p. 47]: *„Integration von Mitarbeitern, Technologie und Funktionen zur Errichtung variabler Barrieren über mehrere Ebenen hinweg“*. Sollte es ein Angreifer durch eine Barriere schaffen, kann er sich nur so weit fortbewegen, bis er auf die nächste Barriere stößt. Durch das Partitionieren - das Teilen von Ressourcensätzen in effektiv getrennte Systeme mit gesteuerten Schnittstellen [103] - kann die Bewegungsfreiheit des Gegners weiter eingeschränkt werden.

Diversity im Systemdesign

Durch den Einsatz unterschiedlicher Programmierer soll das System sicherer werden. Jeder bringt dabei seine „Handschrift“ zur Verbesserung der Systemstabilität ein. [98, p. 112] Dadurch soll das Risiko der Systemhomogenität, bei der sich ein Angriff auf eine Komponente auch auf alle anderen ähnlichen Komponenten ausbreiten kann, verringert werden. Ein heterogenes System bietet außerdem den Vorteil, dass sich Fehler nicht durch das gesamte System ziehen können. Diversität im Systemdesign kann aber auch problematisch sein [89, p. 22]: Erstens kann die Angriffsoberfläche vergrößert werden, indem ein Angriff auf alle Komponenten des Systems abzielt und den Weg des geringsten Widerstandes sucht, um im System Fuß zu fassen. Zweitens könnte ein erhöhter Aufwand für Entwickler, Administratoren, Wartungspersonal und Benutzer entstehen, indem sie gezwungen werden, sich mit mehreren Schnittstellen

zu äquivalenten Komponenten zu befassen.

Redundanz pflegen und beibehalten

Redundanz ist der Schlüssel für viele Strategien, um resiliente Systeme zu schaffen, da es die Verfügbarkeit von beispielsweise kritischen Funktionen erhöht. Sollte eine Verbindung gekappt werden, gibt es einen zweiten Weg, um ans Ziel zu gelangen. [89, p. 23] Da sich Malware über homogene Ressourcen leichter verbreiten kann, muss die Redundanz im Zusammenhang mit Diversity angewandt und über mehrere Ebenen der Architektur berücksichtigt werden. [104, p. 1-3] Wie auch schon bei der Etablierung von Diversity erhöht sich bei der Redundanz der Aufwand, der betrieben werden muss, um sie zu warten, zu überwachen und aktuell zu halten.

Ressourcen ortsunabhängig machen

Eine Ressource, die an einen einzelnen Ort gebunden ist kann zu einem Single Point of Failure [105, p. 31] werden. Wenn diese Ressource ausfällt, steht das gesamte System dahinter. Für Angreifer ist dieser Punkt ein sich lohnendes Ziel, denn dort kann ein großer Schaden angerichtet werden. Um dieses Problem zu lösen, werden standortunabhängige Ressourcen empfohlen, die verlagert und wiederhergestellt werden können. [89, p.24] Dafür gibt es unterschiedliche Ansätze, die verwendet werden können, um ortsunabhängige Ressourcen zu ermöglichen: Virtualisierung, Replikation und Verteilung von Funktionen oder gespeicherten Daten. Bei der Datenvirtualisierung können Anwendungen Daten abrufen und verwenden, ohne den genauen Speicherort zu kennen. Dadurch verringert sich die Wahrscheinlichkeit, dass Daten lokal angesammelt werden. [106] Die Replikation ist ein Ansatz, bei dem dieselben Daten meist an mehreren verschiedenen Standorten gespeichert werden. Ein Vorteil dieses Ansatzes ist, dass die Daten synchronisiert werden. Sollten sie auf einem Standort fehlen oder beschädigt sein, werden sie mit den anderen Daten abgeglichen und aktualisiert. [107]

Health- und Statusdaten nutzen

Fast jede Systemkomponente stellt Health- und Statusdaten bereit, um beispielsweise die Verfügbarkeit anzuzeigen. Sie können zur Erkennung potenzieller Probleme dienen, ermöglichen aber auch eine Leistungsüberwachung. Sollten die Health- und Statusdaten einen Grenzwert überschreiten, könnten beispielsweise Warnungen per Mail verschickt werden.[89, p. 25-26]

Situationsbewusstsein aufrechterhalten

Auch im Cyberbereich wird das Situationsbewusstsein immer wichtiger. Das Wahrnehmen und Verstehen gewisser Situationen ist unabdingbar. Helfen soll dabei ein umfangreiches Lagebild über den aktuellen Stand der eigenen Infrastruktur, inklusive aktuellen Cyber-Vorfällen oder -Ereignissen. Der Vorteil ist, eine verbesserte Kommunikation und höhere Vernetzung der Stakeholder im Cyber-Bereich vorzufinden. [108, p. 1-5]

Persistenz minimieren - Vergänglichkeit maximieren

Die Strategie der Persistenzminimierung verfolgt das Ziel, die Angriffsoberfläche zu reduzieren. Gelingen soll dies mit Hilfe von Virtualisierungstechnologien, die Hard- und Software simulieren, wo selbst wieder Software ausgeführt wird. Dies ermöglicht eine vorübergehende Verwendung von Prozessen, Diensten und Anwendungen. Dadurch kommt es zur Verringerung von gespeicherten Daten auf lokalen persistenten Datenspeichern. Sollte eine virtualisierte Oberfläche kompromittiert werden, kann diese einfach gelöscht oder auf einen vorherigen Punkt zurückgesetzt werden. [89, p. 29]

Integrität laufend überprüfen

Eine regelmäßige Überprüfung der Integrität von Daten und Systemkomponenten ist ebenfalls zu empfehlen. Dadurch soll gewährleistet sein, dass die vorhandenen Daten nicht modifiziert wurden. Sollte es einem Angreifer beispielsweise gelingen, den Inhalt einer Datei zu manipulieren, würde es bei einer Überprüfung erkannt werden. Je öfters solche Überprüfungen durchgeführt werden, desto schneller können inkonsistente Daten erkannt werden und desto geringer sind die Auswirkungen. [89, p. 30]

Angriffsoberfläche verändern und den Gegner täuschen

Die meisten Informations- und Kommunikationssysteme verwenden eine statische Sicherheitskonfiguration, die über einen längeren Zeitraum gültig ist. Angreifer haben dadurch die Möglichkeit, das System in Ruhe auszukundschaften und sich gezielte Angriffe zu überlegen. Mit Hilfe von Konzepten, die laufend Veränderungen in der Konfiguration durchführen, soll auch die Angriffsoberfläche laufend verändert werden. [89, p. 33] Ein Konzept dazu ist „Moving Target Defense (MTD)“ [109, p. 85-86]. Ziel ist es, den Angreifer auf eine falsche Fährte zu locken. Die Angriffsoberfläche wird dabei verschoben und soll vom eigentlichen System ablenken. Die Täuschung soll dabei so echt wie möglich aussehen, damit der Angreifer seine Ressourcen daran verschwendet.

3.5 Eigenschaften einer cyber-resilienten Organisation

Damit eine Organisation, nach BSI Standard 31111 [69], als resilient gilt, sollten folgende Fähigkeiten vorhanden sein:

- eine starke Führung, die ausreichend Ressourcen zur Verfügung stellt, um die Cyber-Resilienz zu gewährleisten.
- Verpflichtung zu anerkannten Sicherheits- und Risikomanagement-Frameworks, wie beispielsweise der ISO/IEC 27000-Reihe [85] oder dem NIST Cybersecurity Framework [110]
- die Fähigkeit, Informationen über Bedrohungen zu sammeln, zu verstehen und zu teilen, um sicherzustellen, dass das Unternehmen und berechtigte Dritte fortlaufend darüber informiert werden
- Das Cyber-Risiko und die Cyber-Resilienz sind fest im Veränderungsmanagement[6] verankert.
- Das Cyber-Risikomanagement umfasst die gesamte Supply-Chain, damit sichergestellt werden kann, dass die Anzahl an Bedrohungen sowohl innerhalb als auch außerhalb des Unternehmens minimiert wird.
- Einsatz eines kontinuierlich gepflegten Cyber-Security Portfolio.
- Zugewiesene Ressourcen sind angemessen im Verhältnis zu den Cyber-Risiken.
- Für den Fall eines Ereignisses sind Vorkehrungen im Incident Management getroffen.
- Das Business Continuity Management deckt Cyber-Risiken ab, einschließlich der Kommunikation bei einem Vorfall, die beispielsweise über ein CSIRT[7] erfolgen kann.
- Fähigkeit, bei sich ändernden Situationen aus Erfahrung zum Lernen.

3.6 Komplexe Systeme und die Notwendigkeit der Resilienz

Die Digitalisierung schreitet mit großen Schritten voran - unsere Welt wird immer vernetzter. Der Sammelbegriff „Internet-of-things“ beschreibt die zunehmende Vernetzung von Gegenständen mit dem Internet, so dass die Gegenstände selbstständig über das Internet kommunizieren. [113, p. 3-4] Immer mehr Haushalte mutieren zu „Smart Homes“ wo Haustechnik, Haushaltsgeräte und Unterhaltungselektronik fortschreitend vernetzt werden. Im Jahr 2018 gab es mehr als 23 Milliarden vernetzte Geräte und laut dem Online-Portal für Statistik Statista [114] werden es 2023 mehr als doppelt so viele sein.

[6] Das Veränderungsmanagement verfolgt ein festes Ziel, das mittels planvoller Initiierung, Umsetzung und Kontrolle der Veränderungsprozesse erreicht werden soll. [111]

[7] Das Computer Security Incident Response Team besteht aus Fachpersonen der IT-Security, die Informationen über Sicherheitsvorfälle sammeln, Analysen durchführen und bei konkrekten IT-Sicherheitsvorfällen behilflich sind. [112, p. 4-5]

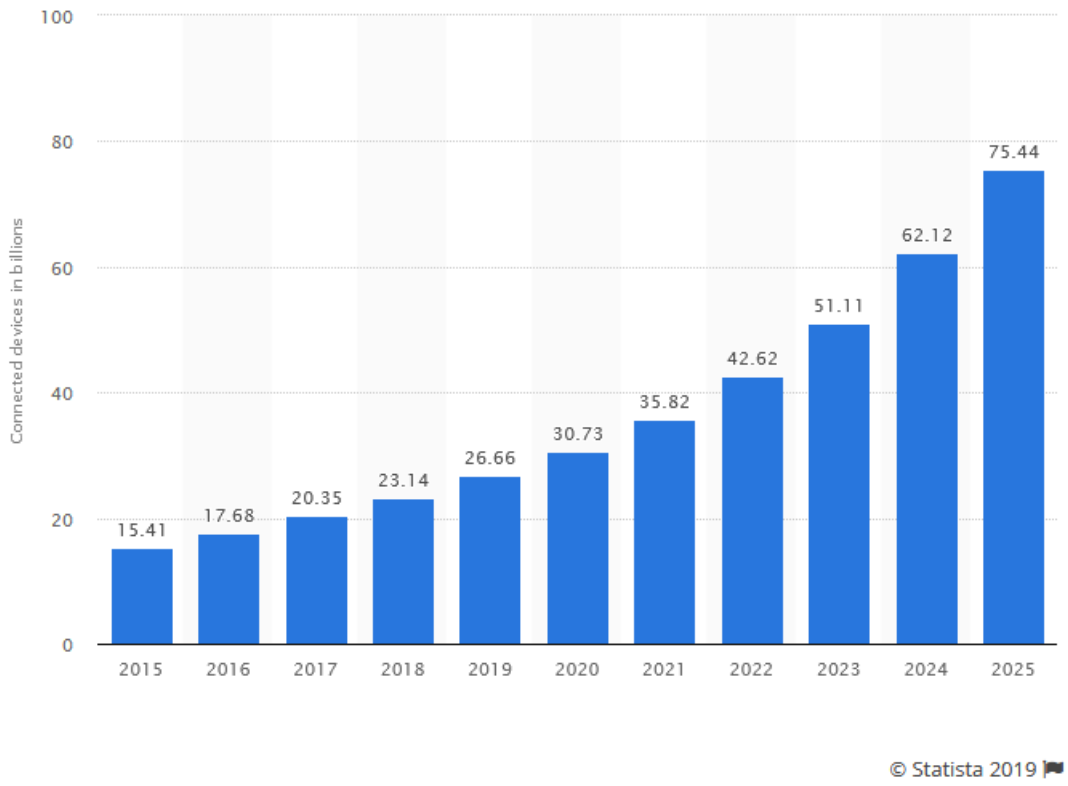

Abbildung 3.6: Anzahl vernetzter Devices weltweit von 2015 bis 2025 (Prognose) [114]

Die stark steigende Vernetzung lässt die Komplexität in Systemen sowie die wechselseitigen Abhängigkeiten steigen. Ausfälle können dann sehr weitreichende und unerwartete Konsequenzen mit sich bringen. Dies stellt eine bisher kaum bekannte Risikoqualität dar, die mit bisherigen Risikobewertungsmöglichkeiten kaum erfassbar ist. Besonders im Cybersicherheitsbereich, wo alle Syteme miteinander vernetzt sind, nehmen die Auswirkungen bei Sicherheitsvorfällen neue Dimensionen an. [7]

3.6.1 Komplexität und komplexe Systeme

Der Begriff Komplexität wird häufig im Zusammenhang mit intuitiv undurchsichtigen, komplizierten, vielschichtigen oder unerklärlichen Phänomenen und Situationen in Verbindung gebracht. [7] Der Duden beschreibt die Komplexität mit Vielschichtigkeit beziehungsweise dem Ineinander vieler Merkmale. [115] Komplexe Systeme bestehen aus einer Vielzahl von miteinander verbundenen Elementen, die mit ihrer Umwelt interagieren. Komplexe Systeme dürfen nicht mit komplizierten Systemen vertauscht werden. So gibt es im technischen Bereich Maschinen mit großer Anzahl von Elementen, die jedoch nur in einer determinierten Umgebung funktionieren. Zur Analyse können diese in ihre Einzelteile zerlegt und wieder zusammengebaut werden. Dabei handelt es sich um komplizierte Systeme oder auch tote Systeme. Komplexe Syteme können zu analytische Zwecke nicht einfach auseinander- und wieder zusam-

mengebaut werden. Sie werden auch lebendige Systeme genannt, die ein völlig anderes Systemverhalten aufweisen können, als die bisherigen toten Systeme. [7]

Kennzeichen von komplexen Systemen

Damit die Abgrenzung zwischen toten und lebendigen Systemen deutlicher wird, charakterisierte Saurugg folgende Punkte als Anzeichen für ein komplexes System: [7]

- Dynamik
- Emergenz
- Nicht-Linearität
- zeitverzögerte Wirkungen
- exponentielle Veränderungen
- kleine Ursachen mit großer Wirkung

Aufgrund der Vernetzung kommt es oft zu Rückkopplungen, die zu einer schwer durchschaubaren Eigendynamik führen. Ursache-Wirkungszusammenhänge sind damit nicht mehr durchschaubar und die Steuerbarkeit wird fast unmöglich. Eingriffe in das System wirken sich dabei oft zeitverzögert aus und selbst kleine Eingriffe können zu großen Wirkungen führen. [7] Eine Vereinfachung der komplexen Systeme ist jedoch kontraproduktiv. Um komplexe Systeme besser zu verstehen, werden diese in Teilabschnitte zerlegt, was in Folge oft nur zu einer Einzeloptimierung führt. Ein System besteht allerdings aus mehreren Teilabschnitten; es ist ein Konstrukt aus untereinander vielfach verknüpften Bausteinen mit unterschiedlichen Zusammenhängen. Komplexe Herausforderungen verlangen daher auch ein neues „vernetztes Denken“. [7] Herbert Saurugg versteht unter diesem Begriff: *„Die Erfassung von Mustern, Beziehungen, Zusammenhängen und (Wechsel-) Wirkungen zwischen Systemelementen.“* [9] Dadurch sollen „unsichtbare Fäden“ erkannt werden, was eine immer größere Herausforderung aufgrund der steigenden Vernetzung wird. Eine hohe Komplexität überfordert unser menschliches Gehirn, daher sind Hilfsmittel wie beispielsweise die Visualisierung von Zusammenhängen notwendig. Mit Hilfe der „unsichtbaren Fäden“ [9] soll zum Ausdruck gebracht werden, dass es bei Systemen besonders auf die Beziehung untereinander ankommt, anstatt auf die einzelnen Elemente selbst.

3.6.2 Lebensfähiges Systemdesign als Grundlage der Resilienz

Die Natur ist als Gesamtes ein offenes, komplexes System, von dem wir lernen können. In der Evolution haben sich drei wesentliche Systemdesignmerkmale für lebensfähige Systeme herauskristallisiert, die für

eine evolutionäre Weiterentwicklung ausschlaggebend waren. Auch technische Systeme profitieren von diesen Merkmalen und können sich zu robusten und resilienten Systemen entwickeln. [7]

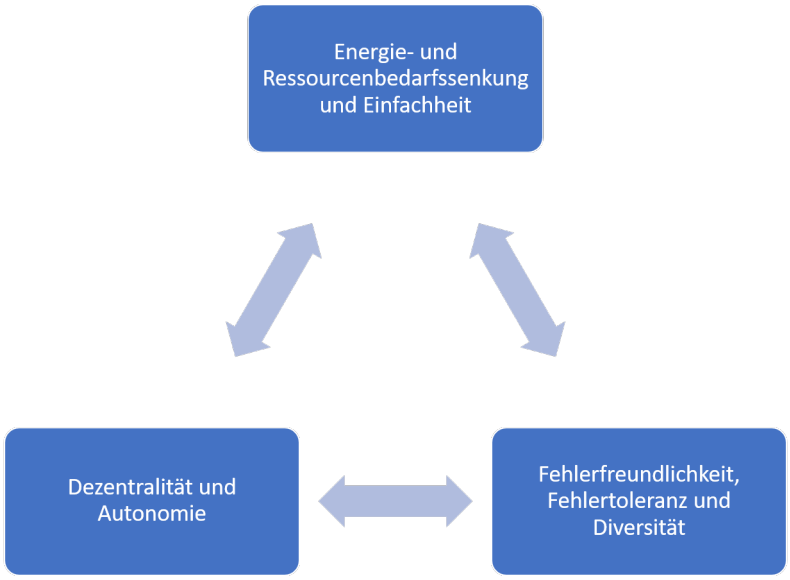

Abbildung 3.7: Systemdesignmerkmale für lebensfähige Systeme [7]

Energie- und Ressourcenbedarfssenkung, Einfachheit

Je weniger Ressourcen benötigt werden, desto unabhängiger - und in Folge auch lebensfähiger und robuster - ist ein System. Hier ist die Abkehr vom bisherigen Immer-mehr-und-größer-Denken gefragt, denn jedes System stößt irgendwann an seine Belastungsgrenzen. Werden die Belastungsgrenzen überschritten, kommt es zum Kollaps (schnell erfolgte Zusammenbrüche) oder auch Seneca-Effekt. [7] Ugo Bardi beschreibt in seinem Buch „Der Seneca-Effekt“ [116], warum Systeme kollabieren und wie wir damit umgehen können. Der Effekt beschreibt dabei ein Phänomen von komplexen Systemen, die zum Kollaps neigen. Dem Kollaps geht dabei meistens eine lange Aufbauphase voran. [117]

Dezentralität und Autonomie

Komplexe Systeme und eine zentrale Steuerung passen nicht zusammen, denn bei komplexen Systemen sind viele Akteure im Einsatz, die selbständig handeln und gleichzeitig miteinander verbunden sind. Hierarchische und zentralisierte Strukturen, die in der bisherigen Industriegesellschaft erfolgreich waren, stoßen in der Netzwerkgesellschaft zunehmend an ihre Grenzen beziehungsweise scheitern an der Bewältigung neuer Herausforderungen. Dezentrale Systeme sind autonome Strukturen, die miteinander vernetzt sind und die Ausbreitung von Störungen begrenzen beziehungsweise eine Rückfallebene nach einer Störung einnehmen. [7]

Fehlerfreundlichkeit, Fehlertoleranz und Diversität

Störungen sollten nicht vollständig ausgeschaltet werden, sondern in den Verlauf miteingebunden werden. Herbert Saurugg attestiert, dass im technischen Bereich häufig das Gegenteil passiert. Es wird versucht Menschen an die Technik anzupassen und nicht umgekehrt. [7]
Gerade im Umgang mit Neuem ist eine gewisse Risikobereitschaft notwendig. Die Fehlerfreundlichkeit ist dabei eine wesentliche Voraussetzung, denn Innovationen können nur entstehen, wenn Scheitern möglich ist.

3.7 Kennzahlen zur Bewertung von Verbesserungen

Mit der Notwendigkeit, Cyber Resilienz zu gewährleisten, steigt auch das Interesse, diese zu bewerten. Mit Hilfe von Metriken sollen Fortschritte in der Cyber Resilienz verglichen und gemessen werden können. Metriken dienen aber nicht nur zur Entscheidungsunterstützung, sondern auch dazu, das Verständnis zu verbessern. Der Begriff Metrik stammt aus dem Griechischen und bedeutet „Messung“. [118] Nach allgemeinem Verständnis handelt es sich um ein System von Kennzahlen oder um Verfahren zur Messung von quantifizierbaren Werten.

Wie können Metriken nun ermittelt und charakterisiert werden? Die Schwierigkeit besteht darin, dass Entscheidungen oft von mehreren Interessensgruppen getroffen werden müssen, die mit Kennzahlen arbeiten, um unterschiedliche Ziele zu erreichen. Während bei Leitern von Geschäftsbereichen die Effektivität im Vordergrund steht, interessiert sich der Chief Information Security Officer für andere Ziele. Sein primäres Ziel ist, das Geschäft risikoorientiert zu ermöglichen und dabei ein angemessenes Schutzniveau bezüglich Informationen und Technologien zu gewährleisten. [119] Bei der Ermittlung von Kennzahlen sollte somit ein breites Netz abgebildet werden, um eine repräsentative Menge zu erhalten: [120, p. 1-2]

- Metriken um operative oder technische Entscheidungen zu unterstützen
- Metriken, die auf verschiedene Architekturschichten oder Ressourcenklassen anwendbar sind
- Metriken, die unterschiedliche Eigenschaften widerspiegeln
- Metriken in quantitativer, qualitativer und semi-quantitativer Form
- Metriken aus anderen technischen Bereichen, wie beispielsweise Security, wiederverwenden

Eine repräsentative Menge von Metriken beinhaltet somit Metriken mit unterschiedlichem Grad an Genauigkeit, die auf unterschiedliche Bereiche abzielen. Ein Set von Metriken, das nur auf einen einzigen

Bereich abzielt, könnte nicht mehreren Interessensgruppen dienen und wäre nicht effektiv nutzbar. Darüber hinaus sollten Bewertungen bei der Cyber Resilienz immer in realen Umgebungen durchgeführt werden.

3.7.1 Klassifizierungsmodell nach ENISA

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) arbeitet an einheitlichen Metriken und an einem Framework zur Messung von Resilienz in Netzwerken und Services. Das Ziel ist, eine einheitliche Taxonomie verschiedener Metriken und deren Eigenschaften zu schaffen. Die Stakeholder wünschten sich, dass ein gemeinsames Verständnis und Verfahren oder ein gemeinsamer Standard für Resilienzmetriken aufgebaut wird. [121]

Die ENISA veröffentlichte dazu ein zweidimensionales und flexibles Klassifizierungsmodell für Metriken zu resilienten Systemen. Auf der einen Seite nimmt das Modell die **ereignisbasierte Ansicht** der Klassifizierung von Resilienz-Metriken ein. Zeitlich reicht die Spannweite von vor dem Zwischenfall über den Zwischenfall selbst bis hin zur Wiederherstellung des normalen Betriebs. Auf der anderen Seite basiert die zweite Dimension auf den Teilen verschiedener Disziplinen, die als Domainen gruppiert werden und zusammen den Begriff Resilienz bilden. Sie wird **domainbasierte Ansicht** genannt. [8, p. 30]

Ereignisbasierte Ansicht

In der ereignisbasierten Ansicht wird die Resilienz in drei verschiedene Zeitphasen unterteilt: der Vorbereitungsphase, der Service-Bereitstellungsphase und der Wiederherstellungsphase. [8, p. 30]

Phase	Beschreibung
Vorbereitungsphase	Die Resilienz-Maßnahmen werden implementiert, um das System auf die Bewältigung von Störungen vorzubereiten. Metriken in dieser Dimension messen, wie gut Systeme und Dienste auf Störungen vorbereitet sind. Eine hoher Wert weist dabei auf eine verringerte Ausfallwahrscheinlichkeit hin. [8, p. 30]
Service-Bereitstellungsphase	Das resiliente Netzwerk ist betriebsbereit und erkennt das Auftreten von Störungen. Metriken in dieser Dimension messen den Unterschied im Servicelevel vor, während und nach einer Störung. Ein niedriger Wert (hoher Unterschied im Servicelevel) bedeutet, dass die Folgen einer Störung im Netzwerk reduziert werden. [8, p. 30]
Wiederherstellungsphase	Wenn sich das System auf einem nicht mehr akzeptablen Servicelevel befindet, wird die Wiederherstellung eingeleitet, um den normalen Betrieb wiederherzustellen. Metriken in dieser Dimension messen, wie schnell sich ein System von einer Störung erholen kann. Ein niedriger Wert zeigt an, dass sich das System schnell von einer Störung erholt und wieder auf die normale Funktionalitätsebene zurückkommt. [8, p. 30]

Tabelle 3.1: Zeitphasen der ereignisbasierten Ansicht [8, p. 30-32]

Die Klassifizierung in dieser Ansicht konzentriert sich auf den Gedanken der Bereitstellung und Wartbarkeit eines akzeptablen Serviceniveaus. Im Falle einer Störung wäre der Servicelevel beeinträchtigt. [8, p. 31] Während der Vorbereitungsphase befindet sich das System in einem stabilen Zustand. Hier werden die Maßnahmen ergriffen, um eine Störung zu verhindern oder diese auf ein Mindestmaß zu reduzieren. Die Vorsorgemaßnahmen kann man sich als Schild über das gesamte System vorstellen, das auch während einer Störung voll funktionsfähig ist. [8, p. 32]

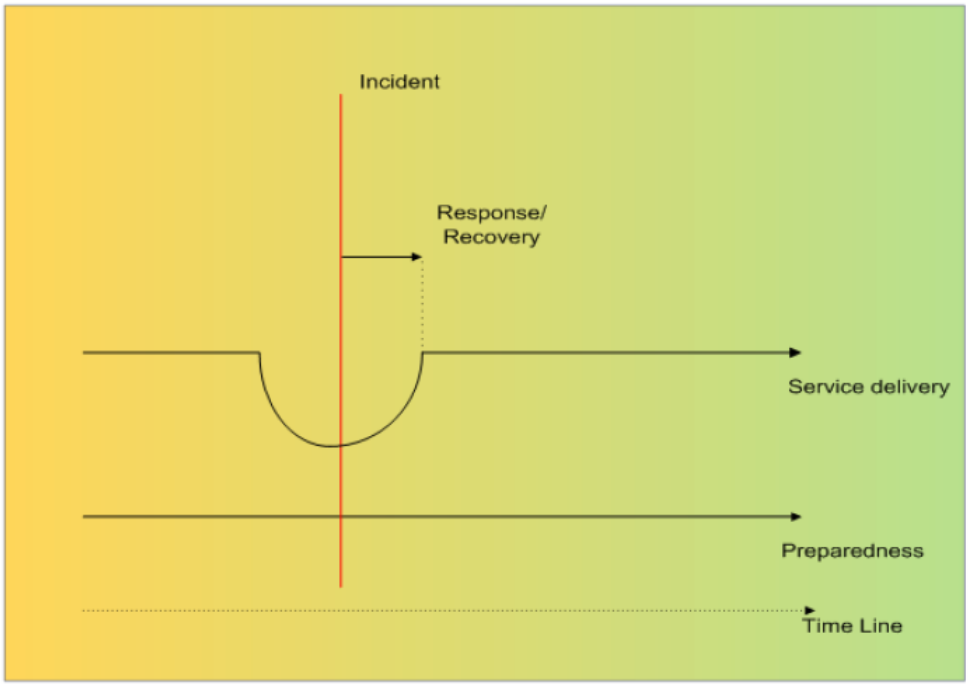

Abbildung 3.8: Grafische Darstellung der Zeitphasen der ereignisbasierten Ansicht [8, p. 32]

Nach einem Störfall versucht das System, den vorherigen Zustand wiederherzustellen. Die Wiederherstellungsphase reicht dabei vom Auftreten des Vorfalls bis zur vollständigen Wiederherstellung des Systems auf das vorherige Niveau der Servicebereitstellung. Ohne einer Störung findet diese Phase nicht statt. [8, p. 32] Während der Systemüberwachung treten immer wieder unterschiedliche Ereignisse auf. Sicherheitsereignisse sind Aktionen, die eine Störung verursachen und müssen folgende Eigenschaften aufweisen, damit sie gemessen werden können: [8, p. 33]

- hat leichte oder schwere Auswirkungen
- haben eine Laufzeit
- können entdeckt und beseitigt werden

Eine Störung kann dadurch als leicht oder schwer eingestuft werden. Sollte der Servicelevel unter ein zuvor definiertes „Mindestsicherheitsniveau“ fallen, könnte er automatisch als schwerwiegend eingestuft werden. Die Effizienz der Schutzmechanismen eines Systems ergeben sich aus der Anzahl von Störungen/Anzahl der Ereignisse gesamt. [8, p. 33]

Domainbasierte Ansicht

Die Domainen können auf unterschiedlichen Detail- und Abstraktionsebenen definiert werden, die sich an den gewünschten Unternehmensbereich richten. [8, p. 30] Eine Metrikdomain ist somit eine Gruppe

von Metriken, die verschiedene Aspekte derselben Ausfallsicherheitseigenschaft messen.

Die ENISA bringt mit dem Begriff „Sicherheit“ ein mögliches High-Level-Domain-Beispiel. Als Gegenstück dazu würde das „Patch-Management“ eine feinere Abstraktionsebene darstellen. Metriken wären hier: welche Systeme aktualisiert werden müssen oder wie oft diese gepatcht werden sollen. [8, p. 34]

Für die domainbasierte Klassifikation gibt es kein einheitliches Allheilmittel, denn die Domainen werden selbst für die eigene Organisation definiert und angepasst. Die ResiliNets-Forschungsinitiative [122] hat ein domainbasiertes Klassifizierungsmodell definiert, das als Vorlage dienen kann. Dort werden drei Domainen klassifiziert: [8, p. 38]

- Systemstabilität
- Security
- Durchführbarkeit

Die Systemstabilität beinhaltet Metriken, wie die Verfügbarkeit (Fähigkeit, ein System oder Dienst zu verwenden), Zuverlässigkeit (kontinuierlicher Betrieb eines Systems oder Dienstes) sowie der Integrität, Wartbarkeit und Sicherheit. Die Security ist die Eigeschaft eines Systems, Maßnahmen zu ergreifen, um sich vor unbefugten Zugriffen oder Änderungen zu schützen. Darunter fallen Metriken wie die Prüfbarkeit, Autorisierung, Authentizität und Vertraulichkeit. Mit der Systemstabilität teilt es sich zudem die Metriken Zuverlässigkeit und Integrität. Die Durchführbarkeit ist die Eigenschaft eines Systems, die geforderte Leistung zu liefern, wie beispielsweise Quality of Service (QoS). [8, p. 38]

Zweidimensionale Taxonomie

Die beiden Dimensionen (domainbasierte und ereignisbasierte Ansicht) können nun als Klassifikation betrachtet werden. Die ENISA stellt dies in Form einer zweidimensionalen Grafik dar: [8, p. 31]

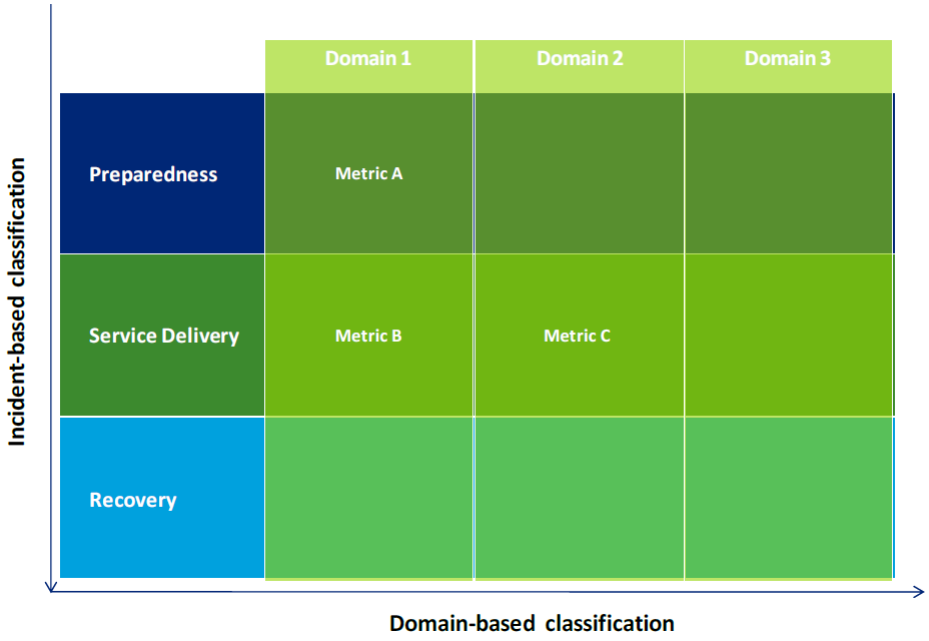

Abbildung 3.9: Zweidimensionale Taxonomie nach ENISA [8, p. 31]

Die Metrik A ist Teil der Domain 1 und befindet sich in der Vorbereitungsphase. Metrik B ist Teil der selben Domain, gehört aber zur Service-Bereitstellungsphase und ist somit in einer anderen ereignisbasierten Dimension. Metrik C gehört ebenfalls zur Service-Bereitstellungsphase, misst aber eine andere Resilienzeigenschaft im Vergleich zur Metrik B. [8, p. 31]

3.7.2 Cyber-Resilienz-Metriken

Der Basler Ausschuss für Bankenaufsicht hat in seiner Publikation „Cyber-resilience: Range of practices“ ein umfassendes Set an Resilienz-Metriken herausgegeben. [123] Er orientiert sich an dem Klassifizierungsmodell [8] der Agentur der Europäischen Union für Cybersicherheit (ENISA) und teilt die Metriken in die drei Phasen der ereignisbasierten Ansicht, sowie in 2 Domainen: Events und Methoden/ Verfahren. [123, p. 45]

Metriken nach Events

Phase	Cyber-Resilienz-Metriken
Vorbereitungsphase	
	• Anzahl der blockierten Verbindungen externer Scans
	• Anzahl aufgehaltener Malware
	• Anzahl bekannter Phishingseiten, die unserem Unternehmen „angeboten“ wurden
	• Schwachstellen pro Codezeile
	• Anzahl erkannter Sicherheitsereignisse
Service-Bereitstellungsphase	
	• Anzahl erkannter Endpoints mit schädlicher Software
	• Anzahl erkannter Server mit schädlicher Software
	• Anzahl von Vorfallarten (Denial-of-service-Attacke, Social engineering, . . .)
Wiederherstellungsphase	
	• Anzahl erkannter Advanced Persistent Threats (APTs)
	• Anzahl blockierter Verbindungen zu infizierten Webseiten
	• Anzahl erkannter Datenlecks mit personenbezogenen Daten
	• Höhe des finanziellen Schadens
	• Kundenverlust

Tabelle 3.2: Cyber-Resilienz-Metriken in der Domain Events [123, p. 45]

Metriken nach Methoden

Phase	Cyber-Resilienz-Metriken
Vorbereitungsphase	• Anzahl an durchgeführten Penetration Tests und gefundenen Bedrohungen • Anzahl der geschützten Systeme durch Identity Access Management (IAM) • Anzahl selbst entwickelter Systeme, welche keine Updates mehr erfahren • Anzahl der Systeme ohne Anti-Malware Schutz • Anzahl nicht-konformer Geräte im eigenen Netz • Einhaltung des Security Configuration Managements (Durchschnitt in Prozent) • Anzahl absolvierter Awarenessschulungen (in Prozent aller Mitarbeiter)
Service-Bereitstellungsphase	• Anzahl von Wiederherstellungsplänen und deren Abdeckungsgrad über das gesamte System • Anzahl und Qualität von Vorfällen aus Übungen
Wiederherstellungsphase	• veröffentlichte Vorfallberichte (Anzahl und Qualität)

Tabelle 3.3: Cyber-Resilienz-Metriken in der Domain Methoden [123, p. 45]

3.8 Too big to fail als Gegenstück zur Resilienz?

Als „too big to fail“ oder systemrelevant werden Unternehmen oder Organisationen bezeichnet, deren Wegfall nicht hingenommen werden kann. Sie spielen eine derart wichtige Rolle, dass beispielsweise öffentliche Mittel zum Verhindern eines androhenden Ausfalles aufgewendet werden. Speziell im Banken- und Versicherungsbereich ist die „too big to fail“- Problematik von besonderer Relevanz. Ein Scheitern dieser würde die Stabilität des gesamten Finanzsystems bedrohen. [9] Bereits im Jahr 1914 kam das „too big to fail“- Konzept das erste Mal zum Einsatz. Zu Beginn des ersten Weltkrieges war die Stadt New York zum Großteil in britischen Pfund verschuldet. Kurz vor ihrer Insolvenz ist das US-Finanzministerium eingesprungen und sorgte für die Rückzahlung der Devisen. Die Amerikaner waren der Auffassung, dass die amerikanische Volkswirtschaft durch eine Insolvenz stärker belastet wäre, als durch die Unterstützung der Stadt mit Steuergeld. [124, p. 2-4] Der Stadt New York, als „too big to fail“-Konstruktion, musste eben geholfen werden, denn eine Insolvenz hätte noch viel gravierendere Auswirkungen auf die Gesamtwirtschaft gehabt.

Bisher sprach man besonders im Banken- und Finanzwesen über dieses Phänomen, dabei spielt das „too big to fail“- Konzept auch in anderen Bereichen eine entscheidende Rolle. Untersee-Kabel werden als die Arterien der globalen Kommunikation bezeichnet. [125] Diese „unsichtbaren“ Leitungen verbinden Kontinente; über sie fließt der Großteil des weltweiten Internet-Traffics. Seit Anfang 2019 sind mehr als 378 dieser Kabel im Einsatz, wobei diese eine beachtliche Länge erreichen können, wie man am Asia-America Gateway (AAG) Cable System, das 20.000 km Kabel umfasst, erkennen kann. [126] Diese kritische Infrastruktur ist aber auch sehr verletzlich, denn mit niedrigem Aufwand kann ein hoher Schaden verursacht werden, indem wichtige Untersee-Kabel durchtrennt werden. [125] Dies kann sogar so weit gehen, dass einzelne Länder überhaupt keine Internetanbindung an die restliche Welt mehr haben, wie das Beispiel von vier gekappten Internet-Seekabeln in der arabischen Welt [127] im Jahr 2008 zeigt. Indien musste die Hälfte der Bandbreite einbüßen, Ägypten sogar 70 Prozent ihrer Netz-Kapazität. Im Iran reagierte ein Router der Universität Teheran nicht mehr, was zu Totalverlusten der Internet-Konnektivität im Iran führte. [128] Auch wenn redundante Strukturen die Ausfälle abfedern, können gezielte Attacken einen hohen Schaden verursachen. [125]

Nassim Taleb beschreibt in seinem Werk „Anti-Fragilität“ eine Geschichte aus der rabbinischen Tradition. [24, p. 366] Der König war über das Verhalten seines Sohnes erbost und wollte diesen mit einem Felsbrocken zermalmen. Nachdem er sich beruhigt hatte, stand er vor einem Problem: Einerseits möchte er seinen Sohn nicht töten andererseits darf er seinen Eid nicht brechen, da er dann als Herrscher ange-

zweifelt wird. Mit Hilfe seines Ratgebers konnte er die Situation lösen. Er zerschlug den Stein in kleine Kieselsteinchen und bewarf ihn damit. Diese Geschichte kann auch umgekehrt betrachtet werden: Der Ausfall vieler kleiner Einheiten ist weniger schädlich als der Ausfall von einer großen Einheit. [9]

Im Jahr 2015 kam es zu einer Mega-Fusion in der Chipbranche, indem Avago Technologies den Wettbewerber Broadcom für 37 Millionen Dollar übernahm. [129] Aufgrund der Nachfrage nach günstigeren Chips kam es in diesem Industriezweig zu einer Übernahmewelle, um in Zukunft effizienter und billiger produzieren zu können. Dadurch entstand aber ein Monopol, das zu einer Abnahme der lebenswichtigen Diversität führt. Die Störanfälligkeit ist gestiegen - kommt es zu einem Problem, steigt die Gefahr von Dominoeffekten rapide an. [9] Nassim Taleb stellte dieses Problem bildlich dar:

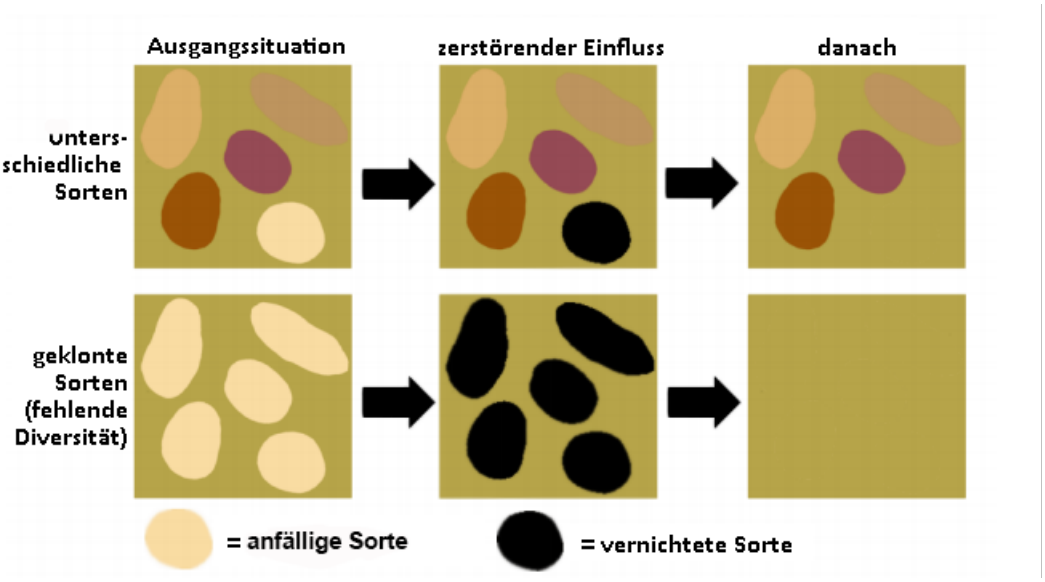

Abbildung 3.10: Bildliche Darstellung der Folgen von fehlender Diversität [9]

Damit Antibiotika billig bleiben, werden die Wirkstoffe bei Pharmaherstellern in China und Indien bestellt. *„Bis in die neunziger Jahre kamen etwa 80 Prozent aller Wirkstoffe aus Europa und den USA und wurden von den Pharmaherstellern selbst weiterverarbeitet“*, schätzt Thomas Rudolph, Analyst für Entwicklungen auf dem Arzneimittelmarkt für die Unternehmensberatung McKinsey. [130] Der ständige Sparzwang führte jedoch zu einer Konzentration auf wenige Anbieter, die großteils in Asien angesiedelt sind. Dies führt zu ungewollten Nebenwirkungen, wie Lieferengpässen und Resistenzen. [9] Die Wochenzeitung „Die Zeit“ veröffentlichte 2014 einen Artikel über „Gefährliche Lieferungen im Pharmabereich“ und beschrieb dort das Problem, dass ein Arzneimittelhersteller kein Penicillin mehr hat. Das gibt es fast ausschließlich nur noch in China zu erwerben und wird großteils für Mastanlagen von Schweinen und Hühnern benötigt. Sollte nun eines der großen Werke ausfallen, kann kurzfristig kein

Konkurrent mehr einspringen. Die Einhaltung der europäischen Qualitätsstandards ist ebenfalls ein Problem, denn Pharmaunternehmen wissen oft nicht woher die „Einzelteile“ ihrer Mittel kommen. [130]

Ein weiteres Beispiel für das „too big to fail“- Konzept ist der weltgrößte Rohstoff-Händler Glencore. 2015 lief dieser Gefahr zu crashen, da die Aktie enorm abstürzte. Der Rohstoff-Schock in der Weltwirtschaft zeichnete sich schon seit Monaten ab: Die Preise fallen bei fast allen wichtigen Rohstoffen. Beginnend mit dem Verfall des Ölpreises, wirkte sich das auch auf andere Rohstoffe aus und es entstand eine Spirale mit viel gravierenderen Folgen als die bisherig bekannten Faktoren, die die Märkte destabilisieren. [131] China fällt beispielsweise als Käufer und Verkäufer von Industrie-Metallen zurück. Folglich versiegt das Kapital in anderen Produzenten-Ländern und die einstigen „Hoffnungsträger“ rutschen in die Rezession. [132]

An diesem Beispiel kann das hohe Schadenspotenzial von „too big to fail“- Konstruktionen erkannt werden. So lange stabile Verhältnisse bestehen, läuft auch in der Regel alles gut. Bei Änderungen der Rahmenbedingungen tun sich große Organisationen oft schwer, flexibel und agil darauf zu reagieren. [9] Die Toleranz gegenüber Fehlern ist daher niedrig und die Fähigkeit zur Wiederherstellung ist nur schwer und langwierig zu bewältigen. „Too big to fail“- Konstruktionen sind daher kaum resilient. Oft scheitert es nicht an verfügbaren Informationen, sondern an der Verknüpfung der „unsichtbaren Fäden“, wie das Beispiel der Pharmaunternehmen zeigt. [9] Es wird versucht, das System in beherrschbare Teilabschnitte zu zerlegen, ohne die entscheidenden Vernetzungen und damit verbundenen Wechselwirkungen ausreichend zu berücksichtigen. [7]

Auch im Cyber-Raum gibt es solche Konstruktionen. Die öffentliche Verwaltung in Deutschland beispielsweise verwendet zum Großteil Produkte von Microsoft. Dies bringt eine Reihe von Sicherheitsbedenken mit sich, wie aktuelle Berichte zeigen. [133] [134] [135] [136] Im Fachjargon spricht man bei dieser Monokultur, also der Verwendung und resultierenden Abhängigkeit, vom „Microsoft-Dilemma“ [137] Entstanden ist der Begriff anhand einer TV-Reportage des ARD [138] im Jahr 2018. Sie zeigt auf, wie sich staatliche Behörden von einzelnen Global Playern abhängig machen – in diesem Fall Microsoft. Diese Abhängigkeit ist einerseits teuer, andererseits auch gefährlich, denn Windows und die Office Produkte von Microsoft sind beliebte Ziele für Angriffe, wie beispielsweise Ransomware bei veralteten Betriebssystemen von Microsoft Windows. Ein weiterer wesentlicher Punkt ist der Datenschutz, denn bei Verwendung von Microsoft Produkten müssen deren Lizenzbedingungen akzeptiert werden, die sich nicht immer mit den Sicherheitsstandards von Behörden oder Unternehmen decken. [139]

Nicht nur Angriffe bedrohen die „too big to fail“- Konstruktion - auch Sofwarefehler oder Ausfälle können weitreichende Folgen haben. [9] Hier spricht man von einem, nach Nassim Taleb definiertem Begriff des „Schwarzen Schwanes“[8] und vom „Verletzlichkeitsparadoxon“[9].

[8] Ein schwarzer Schwan ist ein Ereignis, das selten und höchst unwahrscheinlich ist (Ausreißer) - sollte es aber eintreten, ist häufig mit extremen Konsequenzen zu rechnen und wir versuchen im Nachhinein Erklärungen für sein Eintreten zu finden, um es erklärbar und vorhersehbar zu machen. [140, p. 19-20]

[9] Je besser etwas funktioniert, desto gravierender ist es, wenn es ausfällt. [141] Diese Definition kann auf alle möglichen Bereiche umgewälzt werden. So definiert sie das deutsche Bundesinnenministerium wie folgt: *„Je sicherer eine digitale Infrastruktur ist, desto verheerender kann sich ein doch einmal auftretender seltener Ausfall auswirken.“* [142, p. 90]

4 Anti-Fragilität

Die Anti-Fragilität wird als eine Eigenschaft von Systemen verstanden, die eine gesteigerte Leistungsfähigkeit als Folge von Stressoren, Fehlern, Angriffen oder Ausfällen aufweist. Professor Nassim Nicholas Taleb entwickelte in seinem Buch „Anti-Fragilität - Anleitung für eine Welt, die wir nicht verstehen“ ein Konzept dazu. [24, p. 579]

Fragilität kann als Beschleunigung der Empfindlichkeit gegenüber einem schädlichen Stressor definiert werden: Die Reaktion wird als konkave Kurve dargestellt und gipfelt mathematisch in mehr Schaden als Nutzen bei zufälligen Ereignissen. Im Gegensatz dazu führt die Anti-Fragilität zu einer konvexen Reaktion, die schließlich zu mehr Nutzen als Schaden führt. [143] Nassim Nicholas Taleb sieht in konkav und konvex die beiden Ausprägungen der Nichtlinearität. Die konvexe Ausprägung repräsentiert dabei die Anti-Fragilität, die konkave Ausprägung dagegen die Fragilität. [24, p. 365] Nichtlinearität deshalb, weil die Reaktionen regressiv sind: Eine doppelte Dosis hat sehr viel mehr oder sehr viel weniger als den doppelten Effekt. Die Geschichte des Sohnes mit unrühmlichem Verhalten aus dem Kapitel 3.8 macht dies deutlich: Ein zehn Pfund schwerer Stein verursacht einen mehr als doppelt so großen Schaden als ein fünf Pfund schwerer Stein. [24, p. 366]

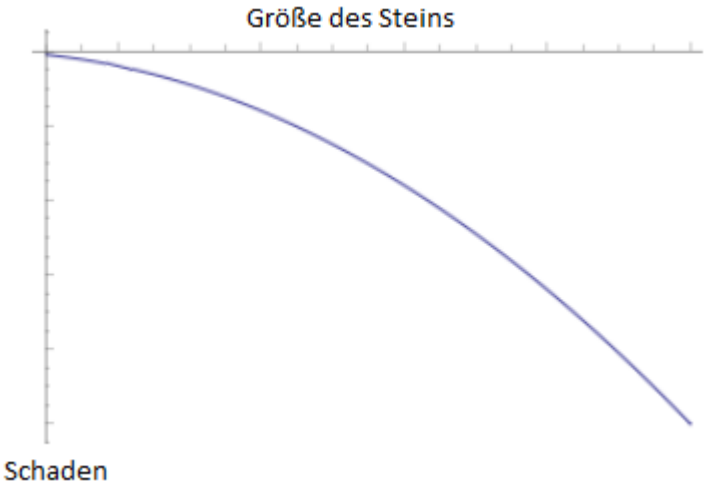

Abbildung 4.1: Nichtlinearität: Je größer der Stein - desto größer der Schaden bei fragilen Objekten [24, p. 367]; dargestellt mittels einer konkaven Kurve

Nach dem derzeitigen Stand der Technik sind Autos fragil. Bei einem Aufprall mit 80 Stundenkilometern entsteht ein größerer Schaden, als wenn man zehn mal mit 8 Stundenkilometern gegen das gleiche Hindernis, wie auf das mit 80 Stundenkilometern, fährt. [24, p. 367] Auch anti-fragile Objekte beruhen auf Nichtlinearität; für sie sind Schocks jedoch bis zu einer gewissen Grenze nützlich. Die Abbildung 4.2 verdeutlicht mit Hilfe einer konvexen Kurve, dass sich unerwartete Ereignisse positiv auf Objekte auswirken können.

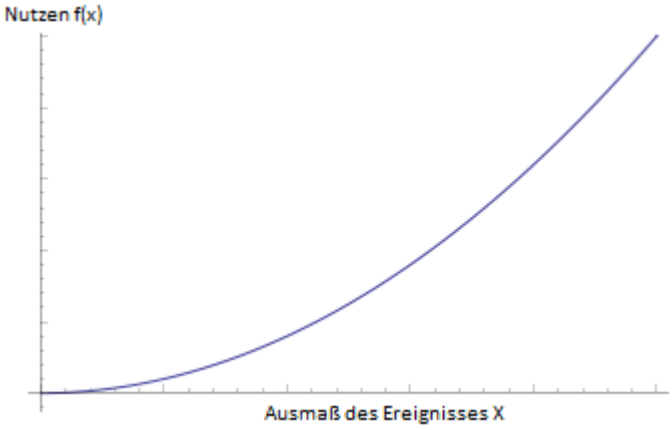

Abbildung 4.2: Nichtlinearität: Anti-fragile Objekte profitieren von Schocks; dargestellt mittels einer konvexen Kurve. [24, p. 367]

In einem Brief an die Fachzeitschrift „Nature“ beschrieb Nassim Nicholas Taleb die „Anti-Fragilität“ wie folgt: *„Anti-Fragilität ist definiert als eine konvexe Reaktion auf einen Stressor oder eine Schadensquelle (für eine gewisse Spannweite), die zu einer positiven Empfindlichkeit gegenüber einer Erhöhung der Volatilität*[1] *führt. Die „Fragilität“ wird als eine konkave Reaktion gegenüber Stressfaktoren definiert und zu einer negativen Empfindlichkeit gegenüber einer Erhöhung der Volatilität führt. Die Beziehung zwischen der Fragilität, Konvexität und Störungsempfindlichkeit ist mathematisch und wird durch ein Theorem erhalten, das nicht aus empirischem Data Mining oder aus historischen Erzählungen abgeleitet ist. Es ist somit a priori.“* [146]

Um die „Fragilität“ oder „Anti-Fragilität“ messen zu können, muss die Geschichte oder Statistik eines

[1] Die Volatilität ist in der Statstik ein Maß für Schwankung über einen Zeitverlauf, das angibt, wie weit die Werte vom Mittelwert entfernt sind. [144]

Heute wird der Begriff mit dem Finanzwesen assoziiert und bedeutet: *„Ausmaß der Schwankung von Preisen, Aktien- und Devisenkursen, Zinssätzen oder auch ganzen Märkten innerhalb einer kurzen Zeitspanne.“* [145]

In dieser Arbeit werden damit ein oder mehrere Mitglieder der „Chaosfamilie“, wie sie Nassim Taleb bezeichnet, [24, p. 35] die sich aus der Unsicherheit, Variabilität, unvollständigem Wissen, Risiko, Chaos, Unbeständigkeit, Unordnung, Entropie, Zeit, dem Unbekannten, Zufälligkeit, Unruhen, Stressoren, Irrtum, Streuung der Ergebnisse und Unwissen zusammensetzt.

Objekts nicht bekannt sein. Es reicht aus, wenn man beurteilen kann, ob sich das Objekt, wenn es der Volatilität oder Zufälligkeit ausgesetzt wird, in Richtung Schaden oder Nutzen beschleunigt.

4.1 Das Anti-fragile

Einige Dinge profitieren davon, instabilen, vom Zufall geprägten und ungeordneten Bedingungen ausgesetzt zu sein. Sie lieben das Abenteuer, das Risiko und die Ungewissheit und wachsen daran. Nassim Nicholas Taleb zufolge steckt dieses Prinzip hinter allem, was sich im Laufe der Zeit verändert hat. Damit gemeint sind beispielsweise: [24, p. 21-22]

- Evolution
- Kultur
- politische Systeme
- technische Innovationen
- wirtschaftliche Erfolge
- menschliche Spezies auf diesem Planeten

Anti-Fragile Gegenstände sind damit mehr als nur resilient. Sie widerstehen nicht nur Störungen und erholen sich von diesen, sie werden dadurch sogar noch besser. [24, p. 21-22]

Die Grenze zwischen Lebend (organisch) und Unbelebt (irgendein Objekt) soll durch die „Anti-Fragilität“ markiert werden. Die „Anti-Fragilität“ steht der Zufälligkeit und Ungewissheit positiv gegenüber und bietet die einzigartige Eigenschaft, mit dem Unbekannten erfolgreich umzugehen, ohne es zu verstehen. Auf der anderen Seite lässt uns die „Anti-Fragilität“ die „Fragilität“ besser verstehen. So können wir beispielsweise nicht unsere Gesundheit verbessern, ohne Krankheiten zu dezimieren. Auch der Reichtum kann nicht gesteigert werden, ohne zuvor die Verluste zu verringern. [24, p. 21-22]

Nassim Taleb gibt die Empfehlung ab, die heute übliche Vorgehensweisen im Bereich Risikomanagement neu zu überdenken. Er schlägt für alle Bereich auf der Welt Regeln vor, mit denen man sich vom „Fragilen“ weg- und auf das „Anti-fragile“ zubewegen kann. Gelingen soll dies einerseits durch die Reduktion der „Fragilität“ und andererseits durch die Nutzbarmachung von „Anti-fragilität“. Mit Hilfe eines einfachen Asymmetrietests soll überprüft werden können, ob etwas anti-fragil ist. Alles, was von zufälligen Ereignissen mehr profitiert, als es darunter leidet, ist anti-fragil. [24, p. 23]

Von einem anderen Blickwinkel aus betrachtet, stellt sich die Frage, wie Systeme, die Anti-Fragilität als Eigenschaft haben, reagieren, wenn sie Volatilität, Zufälligkeit und anderen Stressoren nicht mehr ausgesetzt sind. Theoretisch müssten diese schwächer werden beziehungsweise überhaupt absterben. Wenn der Mensch nach einem Unfall für ein Monat an das Bett „gefesselt“ wird, leidet der Körper unter Muskelschwund - der Körper wird somit geschwächt. Ähnlich verhält es sich bei Systemen, wenn sie keinen Stressoren mehr ausgetzt sind. Nassim Taleb findet, dass uns Top-Down-Strategien in vielen Bereichen geschadet haben, da sie genau diesen Effekt haben: Sie sind eine Kränkung der Anti-Fragilität von Systemen. Er geht davon aus, dass diese Strategie die Fragilität erhöht und Anti-Fragilität blockiert, während Bottom-Up-Strategien von Stress und Unordnung profitieren. [24, p. 23]

4.1.1 Motivation zur Erforschung der Anti-Fragilität

Nassim Taleb fiel eines Tages auf, dass die „(Anti-)Fragilität“ ein bisher nicht wissenschaftlich definierter Begriff war und er nur mit der „Unfähigkeit oder Unbeständigkeit zu vertragen“ beschrieben werden konnte. Dinge, die als „fragil“ bezeichnet werden, wie beispielsweise das Geschirr in der Vitrine, möchte zwangsläufig in Ruhe gelassen werden, damit die Verhältnisse um sie herum ordentlich und vorhersehbar bleiben. Sie würden von Stressoren nicht profitieren; im Gegenteil: mit unvorhersehbaren Gefahren, wie es ein Erdbeben ist, würden sie nicht gut fertig werden. [24, p. 33]

Die „Anti-Fragilität“ entwickelt sich aus der Definition der „Fragilität“. Alle kritischen Verhältnisse mit denen die fragilen Objekte nicht gut fertig werden, sind eine Chance für anti-fragile Objekte. Sie kommen mit allen Formen der Unsicherheit, wie Stressoren, Gefahren, Chaos, abruptem Wechsel, Unordnung und dem Vergehen von Zeit gut zurecht. [24, p. 34]

Die Tatsache, dass alle fragilen Objekte die Unbeständigkeit verachten und umgekehrt, ist dem wissenschaftlichen Diskurs bis dahin entgangen. [24, p. 34] Nassim Taleb nahm dies zum Anlass und erforschte den Begriff „Anti-Fragilität“, um seine Beobachtungen und Erkenntnisse über unvorhersehbare Ereignisse auf unterschiedliche Lebensbereiche, wie Politik, Wirtschaft, technische Innovationen und vielen mehr, zu erweitern. [24, p. 21-22]

4.1.2 Anti-Fragilität auf Kosten der Fragilität anderer

Manche Menschen werden auf Kosten anderer anti-fragil. So generieren sie Vorteile (beispielsweise einen Gewinn) von volatilen, schwankenden, ungeordneten Verhältnissen, indem sie andere Menschen Nachteilen aussetzen. Als Beispiel dafür gibt Taleb die Finanzkrise 2008 an: [24, p. 24-25] Aufgrund der

ständig zunehmenden Komplexität moderner Institutionen und politischer Vorgänge wurden die explosiven Risiken auf Kosten anderer verschleiert. Die Macht konzentriert sich dabei bei wenigen Menschen, die persönlich nicht exponiert sind und von Nassim Taleb als invertierte Helden der neuen Zeit bezeichnet werden. [24, p. 24-25]

4.1.3 Anti-Fragilität in der Natur

Die Wahrscheinlichkeit seltener Ereignisse ist schwerer zu berechnen als die von öfters stattfindenden Ereignissen. So wissen wir weniger über ein Jahrhunderthochwasser als über ein Jahrfünfthochwasser, denn mit abnehmbarer Wahrscheinlichkeit vergrößern sich die Modellfehlerwerte. Daraus folgt die Erkenntnis: *„Je seltener ein Ereignis ist, desto weniger handhabbar ist es, und desto weniger können wir wissen, wie häufig es auftritt.“* [24, p. 27] Ein Experte für seltene Ereignisse ist die Natur. Dank ihrer „Anti-Fragilität“ hat sie es geschafft, Jahrmilliarden fortzubestehen und seltene, höchst unwahrscheinliche Ereignisse abzuwehren. Erkennen kann man die Anti-Fragilität in der Natur daran, dass sie nicht nur sicher ist, sondern auch zerstört, austauscht, selektiert und neu ordnet, um sich an die vorherrschenden Gegebenheiten anzupassen. Wenn diese Flexibilität nicht gegeben wäre, müsste die Natur eine absolute Robustheit aufweisen, damit ein, für die Natur negatives Ereignis nicht zur Zerstörung des gesamten Systems führt. Da dies sehr unwahrscheinlich ist, muss es einen Mechanismus geben, welcher aus Volatilität und Stressoren lernt, anstatt an ihnen zu zerbrechen. Die „Anti-Fragilität“ kann im weiteren Sinne als Gegenmittel zu seltenen und höchst unwahrscheinlichen Ereignissen gesehen werden. [24, p. 27-28]

4.1.4 Die Messbarkeit

Im Gegensatz zu Risiken, speziell jene, die mit seltenen Ereignissen zusammenhängen, lässt sich die „Fragilität“ vergleichsweise gut messen. Nassim Taleb schreibt, dass niemand in der Lage ist, zukünftige und seltene Ereignisse im Risikomanagement messen zu können - auch wenn dies von einigen Wirtschaftswissenschaftlern behauptet wird. Die „Fragilität“ und „Anti-Fragilität“ hingegen sind Eigenschaften eines Objektes, die aufgespürt, gesehen und sogar gemessen werden können. Mit Objekten, die diese Eigenschaften aufweisen, lassen sich Vergleiche hinsichtlich der „Fragilität“ des einen oder anderen Objekts anstellen, während Risikovergleiche nicht zuverlässig sind. So kann nicht behauptet werden, dass ein bestimmtes abseitiges Ereignis wahrscheinlicher sei als ein anderes abseitiges Ereignis. Beispiele für die Vergleichbarkeit von fragilen Objekten müssen nicht von weit herbeigeholt werden: Die Großmutter ist beispielsweise im Bezug auf Temperaturschwankungen fragiler als ihr Enkel oder gewisse Militärdiktaturen sind im Fall von politischen Umschwüngen fragiler als beispielsweise der demokratische Staat Schweiz. Zusammenfassend kann man mit großer Gewissheit vorhersagen, welches von den jeweils bei-

den (weniger) fragiler ist. [24, p. 28-29]

4.2 Die drei Arten der Belastbarkeit

Scheinbar weit auseinander liegende Elemente sollen mit Hilfe eines Dreierschemas in Beziehung gebracht werden. Nassim Taleb behauptet sogar, dass sich jedes Thema, jeder Begriff, jede Strategie in dieses Dreierschema einordnen lässt. Es gilt jedoch herauszufinden in welche Kategorie eingeordnet werden muss und was man gegebenenfalls tun kann, um seine Bedingungen zu verbessern. [24, p. 46] Das Schema besteht aus den drei Arten der Belastbarkeit: Fragil, Robust und Anti-Fragil. Fragile Elemente sind dabei auf die Störungsfreiheit angewiesen, während das Anti-Fragile an der Unordnung wächst. Für robuste Elemente spielt weder das eine noch das andere eine Rolle. In der Fragilitäts-Kategorie sind Fehler seltener, dafür aber umso gravierender und unumkehrbar. Bei der Anti-Fragilität sind Fehler klein, harmlos und aufschlussreich. [24, p. 44-46] Um anti-fragil zu werden, muss man sich das Attribut „Fehler schätzen“ aneignen. Man darf viele kleine, relativ unschädliche Fehler machen, und sollte im besten Fall daraus lernen. Um die drei Arten der Belastbarkeit besser verstehen zu können, folgen nun einige Beispiele. Dabei gilt es festzuhalten, dass fragil und anti-fragil relative Begriffe sind und keine absoluten Eigenschaften. So bedeutet die Positionierung eines Eintrages auf der anti-fragilen Seite lediglich, dass er anti-fragiler ist als das Gegenstück auf der Seite Fragil. [24, p. 47]

	Fragil	**Robust**	**Anti-Fragil**
Mythologie (Griechenland)	Schwert des Damokles	Phönix	Hydra
Beschreibung	Damokles hatte ein Schwert über seinem Kopf hängen, das nur mit einem Rosshaar befestigt ist. Er hofft dass nichts passiert - etwas Gutes kann jedoch nicht passieren. [147]	Am Ende seines Lebens verbrennt der Phönix zu Asche. Man kann sich jedoch sicher sein, dass er wieder - gleich stark - aus seiner Asche auferstehen wird. [147]	Wenn der Hydra ein Kopf abgeschlagen wird, wachsen an dieser Stelle zwei Köpfe nach. Sie wächst somit an Stressoren und wird durch diese stärker. [148]

Tabelle 4.1: Auszug aus der Tabelle „Die zentrale Triade: Drei Arten von Belastbarkeit“ für den Bereich „griechische Mythologie“ [24, p. 48]

	Fragil	**Robust**	**Anti-Fragil**
Menschlicher Körper	Verweichlichung, Muskelabbau	Mithridatisation	Hormesis, Hypertrophie
Beschreibung	Der Körper muss immer wieder neu entscheiden, für welche Aktion es sich lohnt, Energie aufzuwenden. Sobald der Körper merkt, dass gewisse Muskeln nicht genutzt werden, versucht er sie zu reduzieren und plündert deren Energiespeicher. Damit kommt der Körper einige Zeit durch; so lange bis die Energiereserven aufgebraucht sind.	**Mithridatisation** beschreibt das Konsumieren von Giften einer nicht tödlichen Menge zum Selbstschutz. Nach einiger Zeit verträgt man die Mehrfache Menge der üblichen tödlichen Dosis an Gift. [149, p. 198-200] Impfungen und Allergietherapien funktionieren heutzutage nach diesem Prinzip. Der Körper wird durch das verabreichen einer kleinen Menge Gift robust dagegen gemacht.	**Hormesis** ist eine Hypothese von Paracelsus, die behauptet, dass geringe Dosen schädlicher Substanzen eine positive Wirkung auf Organismen haben können. [150, p. 357] **Hypertrophie** bezeichnet eine, unabhängig vom normalen Wachstum, Vergrößerung eines Organs oder Gewebes beispielsweise durch vermehrte Beanspruchung wie beim Muskelwachstum. Die Muskeln werden gezielt beansprucht und „zerstört“, damit sie danach stärker nachwachsen können. [151]

Tabelle 4.2: Auszug aus der Tabelle „Die zentrale Triade: Drei Arten von Belastbarkeit“ für den Bereich „Menschlicher Körper“ [24, p. 49]

4.3 Anti-Fragilität in der Cyber-Security

Die Natur vollzog viele Experimente - mit der Schaffung von vielen Arten und Unterarten. Dies erhöht die Chance, dass einige Experimente erfolgreich sein werden. Durch die Vielfalt von Pflanzen und Tieren erhöht sich die Überlebensfähigkeit, da sich einige Arten an die sich ändernden Bedingungen besser anpassen als andere. Die Natur kennt die Bedingungen nicht im Voraus, aber sie bietet genügend Vielfalt, dass einige Pflanzen und Tiere überleben werden. Die natürliche Evolutionsstrategie ist somit anti-fragil. [152] Die Anti-Fragilität eines Systems hängt also davon ab, ob Teile davon zerbrechlich sein können. In der Wirtschaft kann man dieses Modell mit Risikokapitalgebern beschreiben. Diese investieren in junge Unternehmen (Start-ups), ohne im Voraus zu wissen, welche Ideen erfolgreich sein werden. Daher investieren sie in eine große Anzahl von Start-ups, mit dem Wissen, dass die meisten davon scheitern werden. Einige wenige werden jedoch so erfolgreich sein, dass die Gewinne die Verluste bei den erfolglosen Unternehmen überwiegt. [152]

Die Gesellschaft kann somit von vielen kleinen Fehlern profitieren. Sie sind der Weg zur Anpassung und teilen uns mit, was nicht funktioniert. Sie teilen uns aber nicht unbedingt mit, warum gewisse Strategien funktionieren. [152]

4.4 Chaos Engineering

Nun stellt sich die Frage, wie das Konzept der Anti-Fragilität in anderen Bereichen angewandt werden kann. Für die Sicherheit in Informationstechnologien könnte die Umsetzung des Konzeptes mittels Chaos Engineering erfolgen. Das Thema Chaos Engineering, als mögliche Umsetzung der Anti-Fragilität, gewinnt immer mehr an Bedeutung, obwohl dabei etwas absichtlich „kaputt“ gemacht wird. Entwickler haben als oberstes Ziel, ihre Software fehlerfrei, stabil und sicher zu entwickeln. Um dies zu ermöglichen, schreiben sie Unit[2]- und Integrationtests[3]. In heutigen Architekturen gibt es jedoch oft Komponente, die diese nicht erfüllen. Die Systeme müssen hochverfügbar sein und werden immer komplexer und sind auf den ersten Blick nicht zu verstehen. Infolgedessen kommt es immer wieder zu Ausfällen im Gesamtsystem. Um dies zu vermeiden, dürfen temporäre Ausfälle in einem neuen Deployment nicht zum Ausfall der gesamten Applikation führen. Sie muss mit einzelnen Störungen umgehen können und passend dar-

[2] Unittests kommen in der Softwareentwicklung zum Einsatz, um funktionale Einzelteile von Softwareprogrammen auf ihre Funktionalität zu testen. [153]

[3] Nach erfolgreichen Unit-Tests werden Integrationtests angewandt. Sie testen eine aufeinander abgestimmte Reihe von Softwaretests. Ziel ist es, die verschiedenen voneinander abhängigen Kompenenten eines komplexen Systems im Hinblick auf deren Zusammenarbeit zu testen. [154, p. 301-302]

auf reagieren. [155]

Beim Chaos Engineering muss der Kunde immer im Fokus stehen, denn dieser muss die Sicherheit haben, dass das System in einem stabilen Zustand ist. Einzelne Ausfälle können möglicherweise schon zu Umsatzverlusten oder Rufschädigung führen. Chaos Engineering soll auch nicht zur Diffamierung von Kollegen, anlässlich gemachter Fehler oder falsch getroffenen Entscheidungen verwendet werden. Das Ziel ist nicht, etwas zu zerstören, sondern Software zu verbessern, um den Kunden den bestmöglichen Service anbieten zu können. [155]

4.4.1 Teststufen

In der Softwareentwicklung sichert man die Implementierung durch Tests in unterschiedlichen Ausprägungen ab, anhand der Entwicklungsstufe vom Projekt. Entwickler greifen dabei gerne auf die Testpyramide zurück, die veranschaulicht, welche Testart, in welchem Umfang geschrieben werden sollte. [155]

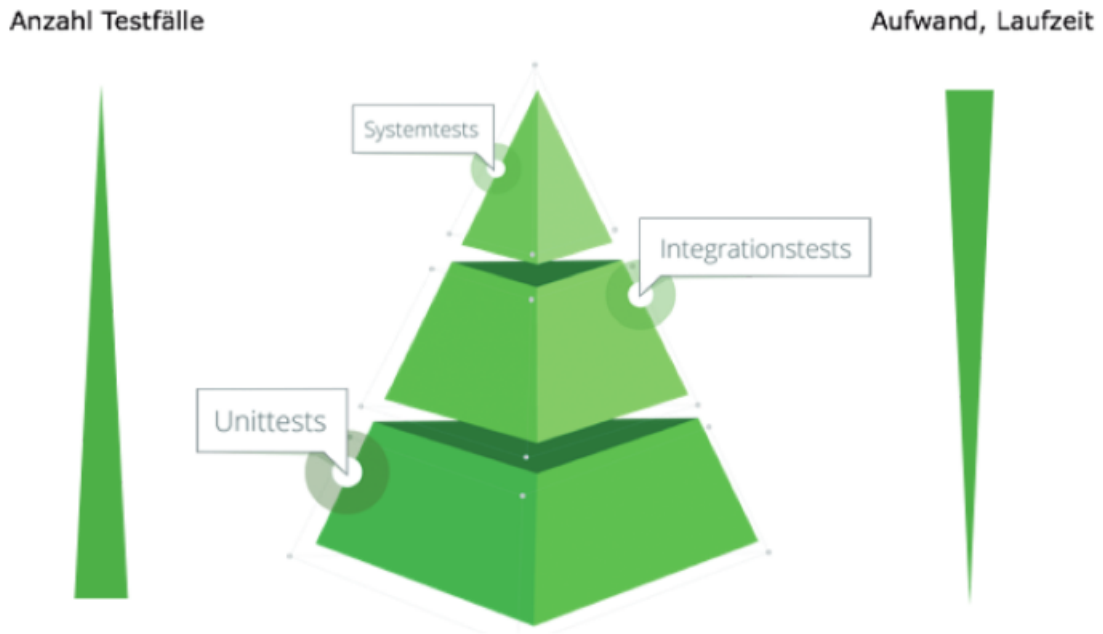

Abbildung 4.3: Teststufen in der Softwareentwicklung [156, p. 4]

Die Testpyramide der Abbildung 4.3 offenbart dabei auch ein Dilemma: Auf der Ebene der Unit-Tests finden sich viele Tests, die schnell und mit geringer Komplexität ausgeführt werden können. Je integrativer es jedoch wird, desto komplexer wird das Test-Setup und das bedeutet mehr Aufwand, Zeit und Kosten. Die höheren Schichten bauen auf den niederen Schichten auf, wobei man sich auf den höheren

Schichten auf möglichst wenige aussagekräftige Tests beschränken sollte. [156, p. 4]

Unittests

Beim Unittest, auch Modultest oder Komponententest genannt, handelt es sich um einen Test auf der Ebene der einzelnen Module der Software. Testgegenstand ist die Prüfung der korrekten Funktionalität innerhalb einzelner und bestimmter Codeabschnitten. Eine Funktion kann dabei mehrere Tests haben, um Ausnahmefälle oder Verzweigungen im Code zu erfassen. Unittest können nicht die gesamte Funktionalität eines Systems verifizieren, sondern stellen sicher, dass die einzelnen untereinander unabhängigen Komponenten funktionieren. [157, p. 371-373]

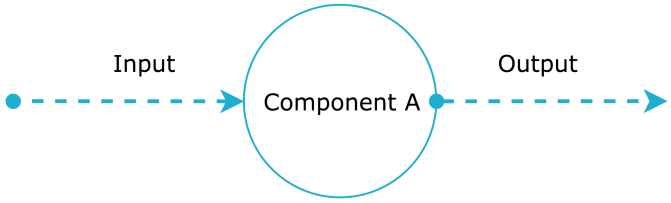

Abbildung 4.4: Schematische Darstellung eines Unittests [155]

Unittests können keine Fehlerfreiheit garantieren, sondern lediglich unterstützend wirken. Sollte der Autor von Unittests und den zu testenden Komponenten ident sein, können Denkfehler auch in der Implementierung des Tests vorkommen. Die Softwarekomponente würde dann auf „grün“ getestet werden, obwohl sich ein Fehler eingeschlichen haben kann. Abhilfe würde hierbei Extreme Programming schaffen, indem sich Entwickler beim Schreiben der Tests und Komponenten abwechseln. [158]

Integrationtests

Nach erfolgreicher Absolvierung der Unittests folgen Integrationtests. Diese überprüfen das Zusammenspiel der einzelnen Komponenten. Idealerweise laufen diese automatisiert ab und haben eine hohe Testabdeckung, um einen stabilen Zustand der Anwendung zu erreichen. Wichtig ist, unter realen Bedingungen zu testen, da nur so erkannt wird, wie sich die einzelnen Bausteine in der Gesamtarchitektur verhalten. [155] Aufgrund der hohen Komplexität und dem geringen Grad an Abhängigkeiten der Komponenten untereinander, sind Integrationtests wichtiger als je zuvor. Fehler in der einen Komponente können Probleme in anderen Komponenten verursachen. [159]

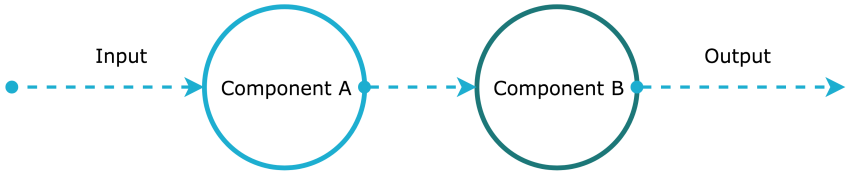

Abbildung 4.5: Schematische Darstellung eines Integrationtests [155]

Systemtests

In Zeiten von Softwarearchitekturen mit Microservices und loser Kopplung erreicht man schnell ein verteiltes System. Dies hat den Vorteil, dass einzelne Funktionen und Services unabhängig und schnell implementiert werden können. Weiterführend bedeutet dies, dass Services ohne Beeinflussung der anderen Services funktionieren (oder auch nicht). [159] Der Systemtest ist dazu da, ein vollständig integriertes System zu testen, um sicherzustellen, dass das System die Anforderungen erfüllt. [157, p. 371]

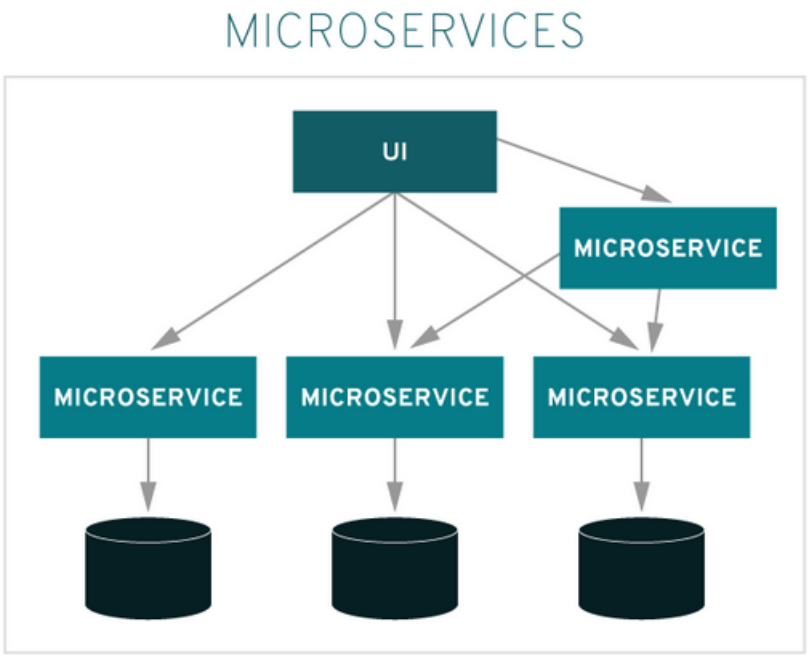

Abbildung 4.6: Beispiel einer Microserverarchitektur [159]

Um eine robuste Anwendung mit guter Performance zu betreiben, sind unzählige Komponente notwendig. [155] Die IT-Stakeholder müssen sich nun anders verhalten und sich entsprechend anpassen. Die ruhige, starre und kontrollierte Zeit ist damit vorbei.

4.4.2 Regeln des Chaos Engineering

Um das Verhalten komplexer und hochverfügbarer Systeme besser zu verstehen, verfolgt man den neuen Ansatz Chaos Engineering. Durch Chaos Engineering sollen Ausfälle kontinuierlich und kontrolliert stattfinden, um Schwächen eines verteilten Systems zu finden und aus ihnen zu lernen. Damit Chaos Engineering stattfinden kann, gibt es zentrale Regeln: [155]

- geplante Chaos-Experimente mit allen Beteiligten absprechen
- Wenn die Konsequenz bereits im Vorhinein bekannt ist, lohnt sich das Experiment nicht
- Chaos Engineering soll Hypothesen beweisen oder widerlegen und nicht für Überraschungen sorgen
- Verteilte Systeme sollen durch Chaos Engineering besser verstanden werden
- Radius des Experiments sollte begrenzt sein
- Während des Experiments sollte man immer die Kontrolle über das Chaos-Experiment haben

Ohne ihnen würde Chaos Engineering nur zu weiterem Chaos - ohne Verbesserungen - führen. [155]

4.4.3 Phasen des Chaos Engineering

Das Ziel des Chaos Engineering ist, das vorhandene Chaos und dessen Folgen aktiv zu bekämpfen. Damit dies nicht zu weiterem Chaos führt, muss es unter kontrollierten Bedingungen stattfinden. Chaos Engineering bietet dafür ein erprobtes und stabiles Vorgehen, das allen Beteiligten bekannt sein muss. [155]

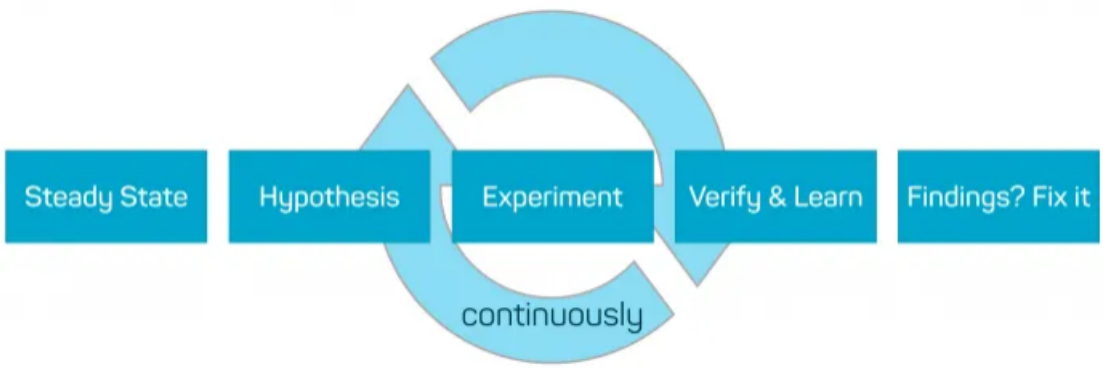

Abbildung 4.7: Die Phasen des Chaos Engineering [155]

Steady State

Bevor Chaos Engineering betrieben werden kann, ist es wichtig, Metriken zum Gesamtzustand des Systems zu definieren und kontinuierlich zu überwachen. Sie sind so zu wählen, dass mit einem Blick erkennbar ist, ob es sich um eine Anomalie im System handelt, die einen Abbruch des Experiments erfordert. Die Metriken können dabei sowohl technischer als auch fachlicher Natur sein. Derzeit überwiegen noch technische Metriken beim Betrieb der Systeme, wie beispielsweise die CPU-Auslastung oder die Auslastung des Arbeitsspeichers. Diese Metriken alleine vermitteln aber nicht, ob das Gesamtsystem korrekt arbeitet. Besser wäre eine Kombination mit den fachlichen Metriken, wie beispielsweise die Anzahl der erfolgreichen Bestellungen in einem Onlineshop, um zu erkennen, dass sich das System in einem Normalzustand befindet. [155]

Hypothese über das Experiment

Was kann beim Experiment passieren und welchen Nutzen hat es, die Behauptung unter Beweis zu stellen? Diese Frage sollte man sich im Vorhinein stellen. Um das Experiment kontrolliert zu testen, sollte man sich auch die Frage, welche Fehler in einer realen Anwendung auf einem System eintreten können, stellen. [155]

Das Experiment und der Blast-Radius

Um während des Experiments jederzeit die Kontrolle zu behalten, müssen auf der Entwicklerseite klare Grenzen gesetzt werden. Dies wird „Blast-Radius“ genannt. Dadurch lässt sich steuern, welche Komponenten ein Experiment beeinflussen und welche Services betroffen sind. Sollte bei dem Experiment eine Komponente ein verändertes Verhalten außerhalb des definierten Blast-Radius aufweisen, muss es gestoppt und analysiert werden. [155]

Verify & Learn - Findings? Fix it!

Nach dem Abbruch eines Experiments müssen die resultierenden Funde an die Verantwortlichen weitergegeben werden. Dabei gilt es, die Fehler zu eliminieren und das Experiment von neuem zu beginnen. Nach einer erfolgreichen Iteration kann der Blast-Radius erweitert werden und ein neues Experiment beginnt. Ein einmaliges Experiment würde nicht ausreichen. Chaos Engineering muss kontinuierlich stattfinden, da sich Systeme ständig verändern, neue Versionen eingespielt werden, neue Hardware verbaut wird oder Änderungen in der Konfiguration (Firewall,...) vorgenommen wurden. [155]

4.5 Chaos Monkey als Chaos Engineering Vorreiter

Während der Migration von Netflix in die Cloud im Jahr 2011 entstand die Idee eines Tools, das zu Ausfällen in der von Netflix-Kunden verwendeten Produktionsumgebung führt, um dem Mangel an ausreichenden Ausfallsicherheitstests entgegen zu wirken. Das Streaming-Portal Netflix hat das Thema Chaos Engineering vorangetrieben und entwickelte das Tool Chaos Monkey. Durch absichtliches und regelmäßiges Zerstören von zufälligen Diensten war es möglich, eine redundante Architektur zu testen, um sicherzustellen, dass ein Serverausfall keine spürbaren Auswirkungen auf Kunden hat. [160] Der Name Chaos Monkey wird im Buch Chaos Monkeys von Antonio Gargica Martinez wie folgt erklärt: *„Stellen Sie sich vor ein Affe betritt ein Rechenzentrum mit Farmen von Servern, die alle notwendigen Funktionen der Online-Aktivität eines Unternehmens ausführen. Der Affe wütet herum und zerstört Server und Kabel nach dem Zufallsprinzip. Nun liegt die Herausforderung bei der IT, eine Architektur zu erschaffen, die mit dem Problem fertig wird.“* [161].

Chaos Monkey hat die Aufgabe, laufende Amazon AWS-EC2-Instanzen und Dienste per Zufall zu zerstören, um zu überprüfen, ob sie redundant sind. [155] Zu viele Unternehmen implementieren Systeme ohne einer durchdachten Redundanzstrategie - sei es auf einer VMWare-Plattform oder in der Cloud - es gibt fast immer Fehlerstellen, die schnell übersehen werden. In der realen Welt kann es jederzeit und ohne Vorwarnung zu Chaos Monkeys kommen. Damit ist das Tool nicht nur ein Hilfsprogramm, sondern die Realität, der man sich stellen muss. [162]

Netflix brachte das Tool Chaos Monkey als Open-Sorce-Version heraus und gab dabei an, dass das Tool ein Jahr lang ausgeführt wurde und 65.000 Instanzen nach dem Zufallsprinzip beendet hat. Erstaunlicherweise bemerkte es der Endkunde kaum, aber das System lernt noch immer aus den Überraschungen, die Chaos Monkey mit sich bringt. [162] Während eines Experiments überwacht Netflix die Anzahl der erfolgreichen Klicks, ein Video zu starten. Das ist die fachliche Kernmetrik von Chaos Monkey, denn wenn für die Kunden keine Videos mehr zur Verfügung stehen, geht die Kundenzufriedenheit hinunter. [155]

Mittlerweile ist Chaos Monkey ein Teil der großen Tool-Suite Simian Army, mit der Reaktionen auf verschiedene Systemfehler und Randfälle getestet werden können. Darin enthalten sind beispielsweise noch der Latency Monkey, der absichtlich Delays in der Kommunikation simuliert, um eine Verschlechterung der Netzwerke abzubilden. Ein weiteres Tool ist der Chaos Gorilla. Er legt eine vollständige „Verfügbarkeitszone“ lahm, um zu überprüfen, dass andere Zonen mit der Mehrlast umgehen können. [160]

4.6 Cyber Red Teaming

Ein weiterer Ansatz, um das Konzept der Anti-Fragilität bei Informations- und Kommunikationssystemen umzusetzen, könnte Cyber Red Teaming (CRT) sein. Der Begriff Cyber Red Teaming wird häufig als Synonym für Penetrationstests verwendet. [163, p. 8] Penetrationstests gibt es in unterschiedlichen Arten, die als individuelle Aktivitäten durchgeführt werden. Wenn diese Tests kombiniert werden, beginnt die Idee des Cyber Red Teamings. Dabei handelt es sich um ein Team aus Angreifern, die alles in ihrer Macht stehende tun, um ein System zu kompromittieren. Das Team nutzt dafür die gesamte Bandbreite virtueller, physischer und sozialer Angriffe aus, um motivierte und hartnäckige Angreifer zu imitieren. [164] Während die Ergebnisse von Penetrationstests die gleichen praktischen Auswirkungen auf ein System haben wie bei Cyber Red Teaming, sind die Angriffsvektoren bei Penetrationstests sehr eng umfasst und sagen oft nicht viel über das System insgesamt aus. [163, p. 8]

Cyber Red Teaming ist somit eine wichtige Verteidigungsmaßnahme für Unternehmen und Organisationen mit großer Infrastruktur bei Informations- und Kommunikationstechnologien, denn aufgrund ihrer Größe können sie schnell zu Zielen für kriminelle Organisationen, Gruppierungen mit gemeinsamen Interesse oder für fremde Regierungen werden. [163, p. 1]

Mit Hilfe von Cyber Red Teaming soll bewertet werden können, wie anfällig eine Infrastruktur, Geschäftsprozesse oder Mitarbeiter für Angriffe sind und zeigen auf, wo Verbesserungen notwendig sind. Cyber Red Teaming umfasst die Erstellung von Angriffsvektoren, der Ausführung selbst und der Analyse der Auswirkungen. Die Ergebnisse werden dann zur Entwicklung von Mitigationsstrategien genutzt. [163, p. 3] Da Cyber Red Teaming-Übungen über einen längeren Zeitraum gehen und etliche Ressourcen binden, ist eine Automatisierung der Übung zu empfehlen. Die eingesparten Ressourcen könnten dann beispielsweise in die Etablierung von Abschwächungs- und Gegenmaßnahmen gesteckt werden. [163, p. 7]

4.6.1 Das Welt-Modell

Im Cyber Red Teaming haben sich unterschiedliche Begriffe entwickelt. Das Gesamtsystem, für das ein Red Teaming durchgeführt wird, bezeichnet man als Weltmodell. [165, p. 31-55] [166, p. 1] Welt-Modell deshalb, weil Cybersysteme große, komplexe digitale Ökosysteme sind, in denen viele intelligente Einheiten gemeinsame Ressourcen nutzen und verbrauchen. Dabei gibt es zwei Seiten: Auf der einen Seite agiert der Gegner, der auf die andere Seite, die Umgebung abzielt.

Der Gegner

Nicht alle Angreifer folgen dem gleichen Muster. Jeder Gegner hat eine Reihe spezifischer Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures - TTPs). Manche sind einfallsreicher und mit besseren Mitteln ausgestattet, andere haben wiederum ganz bestimmte Ziele, wenn sie beispielsweise gezielt eine Organisation angreifen.

Beim Aufbau eines Red Teaming-Angreifers stellen sich somit folgende Fragen: [163, p. 8-9]

- Welches Ziel verfolgt der Angreifer beziehungsweise was sucht er?
- Welche Fähigkeiten besitzt der Angreifer? Hat er beispielsweise genügend Ressourcen, um komplexe TTPs einzusetzen?
- Welche Einschränkungen (begrenztes Zeitfenster, Anonymität) hat er?
- Welches Verhaltensmuster des Gegners ist zu erkennen? Hat er schon einmal angegriffen? (Frühere Angriffsmuster könnten auf zukünftige Muster und Ziele hinweisen.)

Die Zielumgebung

Ein Computernetzwerk für Organisationen, wie beispielsweise bei Ministerien, ist im Allgemeinen sehr groß, dynamisch und komplex. [167, p. 11] Das genaue Modellieren und Simulieren eines solchen Netzwerks für Cyber Red Teaming erfordert möglicherweise das Anwenden von Abstraktionen oder Annahmen. Folgende Leitfragen können beim Aufbau eines problemspezifischen Welt-Modells helfen: [163, p. 9]

- Welche Entitäten gibt es im Weltmodell?
- Wie ist die Beziehung zwischen den Entitäten?
- Wie dynamisch ist die Welt?
- Welche Teile der Welt sind relevant?
- Welche Teile der Welt sind von außen sichtbar?

4.6.2 Erstellung eines Angriffsplanes

Bei einer CRT-Übung sind zahlreiche mögliche Angriffspläne geplant. Das rote Team (Übungsläufer, die die Rolle eines Gegners spielen) wählt anhand einer oder mehrerer der unten angeführten Faktoren aus, welche dieser Angriffe zuerst ausgeführt werden sollen. Einige Angriffe können auch von bestimmten Antworten des Zielcomputers oder -benutzers abhängen. Durch Simulation kann die Schadensbewertung und Schadensbegrenzungsplanung basierend auf den Angriffseffekten geschätzt werden. [163, p. 9-10]

- anliegenbasiert (Priorisierungder Angriffe, welche am wichtigsten sind)
- erfolgsbasiert (Priorisierung der Angriffe, deren Erfolg am wahrscheinlichsten sind)
- kostenbasiert (Priorisierung der Angriffe, die am wenigsten Ressourcen verbrauchen)
- impactbasiert (Priorisierung der Angriffe, deren Auswirkungen am größten sind)
- gelegenheitsbasiert (Priorisierung der Angriffe, die für bestimmte Situationen relevant sind)
- überprüfungsbasiert (Priorisierung der Angriffe, die zuvor behandelt wurden. Dient dazu, um sicherzustellen, dass die bereits getroffenen Schutzmaßnahmen wie erwartet funktionieren.)

4.6.3 Probleme und Herausforderungen

Bei der Planung und Durchführung einer Cyber Red Teaming-Übung kann man mit einer Reihe von Herausforderungen konfrontiert sein. Ein wesentlicher Punkt sind die vorhandenen (limitierten) Ressourcen. Oft ist der Zeit- und Rechenaufwand für die Durchführung einer Übung zu hoch und unrealisierbar. Eine weitere Herausforderung ist die asymmetrische Bedrohung, denn Gegner verfügen zum Teil über TTPs, die über die eigenen Fähigkeiten im Unternehmen hinausgehen, wodurch solche Angriffe nur schwer erkennbar sind und verteidigt werden können. Darüber hinaus muss die Situationsbewertung fast in Echtzeit stattfinden, da einige Cyber-Angriffe innerhalb von Millisekunden wieder abgeschlossen sind. Zum Schluss darf nicht vergessen werden, dass nicht bekannte Schwachstellen nicht impliziert, dass keine Schwachstellen vorhanden sind. [163, p. 10] Um den Zeit- und Ressourcenaufwand gering zu halten, sowie unterschiedliche Bedrohungsszenarien zu bespielen, empfiehlt es sich, das Cyber Red Teaming automatisiert zu betreiben.

4.6.4 Automatisiertes Cyber Red Teaming

Eine automatisierte Planung, mit Hilfe von künstlicher Intelligenz, wird bereits bei Computerspiel-Engines verwendet. Das Verhalten von Nicht-Spieler-Charakteren (NPCs) wird, besonders wenn sie die gegnerische Rolle spielen, automatisch geskriptet. Dabei hat sich gezeigt, dass NPCs, die automatisierte Planer einsetzen, taktisch und strategisch bessere Entscheidungen mit besseren Ergebnissen treffen, als erfahrene menschliche Spieler. [168] Diese Fähigkeit würde sich gut für automatisierte Cyber Red Teaming-Übungen eignen, da diese ebenfalls gezielte und intelligente Angriffe simulieren sollen.

Das erste klassische Spiel, in dem ein Computer gegen einen Menschen gewann, ist Tic-Tac-Toe. Der Algorithmus dazu wurde bereits in den 1950er Jahren, als Doktorarbeit von Alexander Sandy Douglas programmiert. Die Steuerung des Spielers erfolgte über die Telefonwählscheibe, wobei die Zahlen eins bis neun für je ein Kästchen standen. [169, p. 1-3] Ein weiterer berühmter Computer, der gegen einen

Menschen gewann, ist der Schachcomputer „Deep Blue“ von der International Business Machines Corporation (IBM). 1997 gewann dieser einen Wettkampf gegen den damaligen Schachweltmeister Garri Kasparow unter realistischen Turnierbedingungen. [170] IBM war es, die auch das Computerprogramm „Watson“ entwickelte. Dieses Programm soll mit Hilfe der künstlichen Intelligenz Fragen analysieren und Antworten auf Fragen geben können. [171] In der Quizshow „Jeopardy!“, die aus den USA stammt, gelang dem Computerprogramm der Sieg gegenüber zwei Gegenspielern, die zuvor Rekordsummen gewonnen hatten. [172] Wie fast alles im Leben hat auch die künstliche Intelligenz ihre Schattenseite. In Japan beispielsweise ersetzte ein Versicherungsunternehmen mehr als 30 Mitarbeiter mit dem Computerprogramm Explorer. Dieses wird künftig automatisch Krankenhausakten einlesen, um mögliche Auszahlungen zu berechnen. [173]

Auch im Cyber Red Teaming greift man auf die künstliche Intelligenz zurück, um Cyber Red Teaming zu automatisieren. Ein Planungswerkzeug dafür ist beispielsweise „PbP2“ von der Universität Brescia. PbP2 ist ein Multiplaner-System, das automatisch die effizientesten Planer für eine Domaine auswählt und kombiniert. [174] Zusätzlich erstellt das PbP2 für jeden Plan unterschiedliche Makros mit automatischen Parametereinstellungen und einer zielgerichteten Konfiguration. [163, p. 19]

4.7 Fuzzing

Fuzzing ist eine automatisierte Technik, um Software auf Sicherheitslücken zu testen, indem das Programm an mehreren Eingabeschnittstellen mit zufälligen Daten befeuert wird. Entwickelt wurde diese Technik an der Universität von Wisconsin-Madison bereits im Jahr 1988 und zeigt, dass selbst moderne Betriebssysteme für einfaches Fuzzing anfällig sind. [175]

Beim Fuzzing versucht ein Angreifer unterschiedliche Kombinationen von Zahlen, Zeichen, Metadaten (wie beispielsweise Benutzereingabetexte) oder reine binäre Sequenzen, die sowohl gültig als auch ungültig sind, zu injizieren. [176] Das Ziel eines Fuzzers ist es, Eingaben zu erstellen, die dazu führen, dass Programme beliebige Programmpfade ausführen, die zu interessante Programmzustände führen. [177, p. 2] Der große Vorteil von Fuzzing ist das einfache Testdesign, das frei von Vorurteilen gegenüber dem Systemverhalten ist. Dieser Ansatz ermöglicht es, Fehler zu finden, die von Menschen oft übersehen worden wären. [176]

Ein bekannter Vertreter, der die Fuzzing-Technologie verwendet, ist Google. Mit Hilfe von Fuzzing konnten hunderte von Fehlern in Google’s Code gefunden werden, einschließlich Komponente von Googles

Webbrowser Chrome. [178]

4.7.1 Fuzzing Typen

Im Laufe der Zeit enwickelten sich beim Fuzzing unterschiedliche Ansätze. Das traditionelle Fuzzing, also das Erzeugen von völlig zufälligen Inputs, mit denen das Programm gefüttert wird, wird als „naives Fuzzing“ bezeichnet. [177, p. 2] Naives Fuzzing ist zwar einfach zu implementieren, die Wahrscheinlichkeit einen interessanten Programmzustand in einem gewissen Zeitrahmen zu erreichen, ist jedoch sehr gering. Deshalb bildeten sich in Folge drei weitere Typen beim Fuzzing: Mutation-based Fuzzing, Generation-based Fuzzing und Evolutionäres Fuzzing. [177, p. 2]

Mutation-based Fuzzing

Bei mutation-based Fuzzing werden die bereitgestellten Eingabewerte blind manipuliert oder verändert und dann in das Programm eingespeist. Um Mutation-based Fuzzing zu betreiben, benötigt man oft Kenntnisse zu möglichen Eingabewerten, um effektive Eingaben innerhalb eines Eingabekorpus zu generieren. Gültige Anfangseingaben führen zu tieferen Programmzuständen. [177, p. 2] Dies können beispielsweise erwartete Eingaben für einen TLS-Handshake sein. [179]
Ein Vertreter dieses Types von Fuzzing ist der Peach Fuzzer von der US-amerikanischen Firma PeachTech. [180]

Generation-based Fuzzing

Beim generation-based Fuzzing werden zuerst die Spezifikationen vom verwendeten Protokoll beziehungsweise Informationen über das erwartete Eingabeformat eingeholt. Die Eingaben werden dann anhand dieser Informationen generiert. Beim generation-based Fuzzing werden in der Regel tiefere Programmzustände und eine höhere Code-Abdeckung als beim mutation-based Fuzzing erreicht. Der Nachteil ist jedoch, dass man genaue Programmeingangsspezifikationen benötigt, um den Fuzzer einzurichten. Dies erfordert mehr Zeit als die einfache Erzeugung eines Eingabekorpus. [177, p. 2]
Generation-based Fuzzing wird beispielsweise durch das Open-Source-Tool Sulley unterstützt. [181]

Evolutionäres Fuzzing

Die neueste Art, Fuzzing zu betreiben, ist das evolutionäre Fuzzing. Dieser Typ von Fuzzing baut auf dem mutation-based Fuzzing auf, indem die Eingabewerte zuvor bekannt sind und die Eingänge für die manipulierten Daten zuvor ausgewählt werden. Es wird bewertet, was jede Eingabe im Programm

veranlasst. Basierend auf dieser Bewertung werden die zu überprüfenden Eingänge dann ausgewählt und mit manipulierten Werten innerhalb des Eingabekorpus befeuert. [177, p. 2]
Evolutionäres Fuzzing kann unter anderem durch das Open-Source-Tool honggfuzz durchgeführt werden. [182]

4.7.2 Fuzzing basierend auf maschinellem Lernen

Um eine hohe Code-Abdeckung zu gewährleisten, müssen viele dynamische Prozesse untersucht werden. Das erfordert einerseits viel Zeit und andererseits Intelligenz, um die Prozesse zu verstehen und ein sinnvolles Voranrücken in den Prozessschritten zu garantieren. Außerdem können kleine Änderungen und nicht automatisierte Abläufe den gesamten Workflow durcheinander bringen und die laufende Analyse verfälschen. Die wirkliche Situation wird dadurch nicht mehr abgebildet. Die Überprüfung der Eingangsschnittstellen, um Sicherheitslücken zu finden, sollte dauerhaft, somit während des Betriebes, stattfinden und sich den Begebenheiten anpassen, um das System laufend verstärken zu können. Gelingen kann das, indem Fuzzing maschinelles Lernen zur Unterstützung zur Verfügung gestellt wird.

Am erfolgreichsten ist das Zusammenspiel zwischen Fuzzing und maschinellem Lernen in der Phase, wo der Input generiert wird. [177, p. 6] Für die Inputgenerierung werden meistens „genetische Algorithmen[4]“ verwendet, da diese die Fähigkeit besitzen, auf früheren erfolgreichen Eingaben aufzubauen. [177, p. 6] Genetische Algorithmen folgen immer einer iterativen Abfolge von Rekombination, Mutation und Selektion [183, p. 6] und sind unter gewissen Voraussetzungen in der Lage, komplexe Optimierungsprobleme zu behandeln. Sie können aus einer sehr großen Zahl von möglichen Lösungen ein Set aus den besten Lösungen beziehungsweise die beste Lösung ermitteln. Diese dienen dann als Grundlage für die Erzeugung neuer Lösungen, mit der Erwartung an noch bessere Lösungen zu gelangen. [184]

Interessante Programmzustände, die beim Fuzzing erzeugt worden sind, wurden bisher manuell analysiert. Mit Hilfe von maschinellem Lernen soll dieser Schritt automatisch erfolgen, indem Abstürze vorselektiert und Programmfehler mittels Ursachenanalyse kategorisiert werden. [177, p. 8-10] Einen Nachteil hat Fuzzing mit Hilfe von maschinellem Lernen allerdings auch: Cyber-Kriminelle können diese Technik nutzen, um automatisiertes Fuzzing zu betreiben und Zero-Day-Schwachstellen[5] schneller zu

[4] Genetische Algorithmen sind eine Gruppe von Methoden zur Bewältigung von Optimierungsproblemen und basieren auf dem Vorbild der natürlichen Evolution, denn dort entwickelten sich Populationen nach dem Prinzip „Überleben des Stärkeren“ [183, p. 6]

[5] Die Zero-Day-Schwachstelle beschreibt eine bisher unbekannte Sicherheitslücke, die von Angreifern ausgenutzt wird, bevor das Opfer dieses überhaupt als Sicherheitslücke erkennt und darauf reagieren kann. [185]

erkennen.

In der Studie „Automatic Patch Generation by Learning Correct Code“ [186] wird das Tool Prophet vorgestellt, das sowohl die Hauptursachen für Fehler identifiziert als auch Patches dagegen generiert - und das mit Hilfe von Algorithmen für maschinelles Lernen. In Kombination mit Fuzzing könnte diese Konstruktion somit Sicherheitslücken lokalisieren und mit Patches beseitigen. Dies wäre ein weiteres Modell in Richtung Anti-Fragilität.

5 Der Vergleich

5.1 Resilienz vs. Anti-Fragilität

„Anti-Fragilität geht über die Resilienz und Robstheit hinaus. Das Resiliente, das Widerstandsfähige widersteht Schocks und bleibt sich gleich; Das Anti-Fragile wird besser.“, so Nassim Nicholas Taleb in seinem Buch Anti-Fragilität - Anleitung für eine Welt, die wir nicht verstehen. [24, p. 21]

Ein offensichtliches Beispiel für etwas, das sich durch Stress verbessert, ist der menschliche Körper. Er wird durch Bewegung stärker, fitter und weniger anfällig für Krankheiten. Wir lernen, Stress ist gut - aber nicht zu viel davon! Ein Zement-LKW, der über einen drüber fährt, ist zu viel Stress. [152] Das Gleiche gilt für die menschliche Psyche. Fernsehprogramme harmloser Art, wo nichts in Frage gestellt wird, werden den Verstand nicht schärfen. Schwierige Herausforderungen im Leben oder in der Mathematik, die eine sorgfältige und langwierige Problemlösung erfordern, können dies aber sehr wohl. Probleme im Leben, die zu psychischen Zusammenbrüchen führen, sind aber wieder zu viel und nicht gut für uns. [152]

5.1.1 Worin unterscheiden sich die Begriffe

„Anti-Fragil“ ist ein Begriff, der bisher nicht im Wörterbuch gefunden werden konnte. Nassim Taleb prägte das Wort, da er über die weltweiten Sprachen hinaus keinen Begriff finden konnte, der diese Fähigkeit beschreibt. Nämlich sich durch Stress zu verbessern, anstatt nur widerstandsfähig zu sein, wie es die Resilienz impliziert. Der Begriff „Resilienz“ ist im Unterschied zur Anti-Fragilität leicht im Wörterbuch zu finden. [152] Im Random House Kernerman Webster’s College Dictionary [187] gibt es dazu folgende Definition: *„Die Kraft oder Fähigkeit, in die ursprüngliche Form oder Position zurückzukehren, nachdem etwas gebogen, zusammengedrückt oder gedehnt wurde.“* Dies scheint eine gute Sache zu sein - bis zu einem gewissen Grad ist es das auch. Resiliente Systeme, Menschen und Gesellschaften sind gut darin, ihren derzeitigen Betrieb aufrechtzuerhalten oder bei Störungen zu ihrem vorherigen Zustand zurückzukehren. [152]

Genau hier steckt der Grund, warum die Anti-Fragilität ein besserer Ansatz ist, als die Resilienz. Die Resilienz hängt zum Teil davon ab, mit welcher Art von Belastung sie konfrontiert ist, um dagegen Abwehrkräfte aufzubauen. Für die Anti-Fragilität ist es nicht erforderlich, im Voraus zu wissen, wie hoch die Belastungen sein werden und um welche Art von Belastung es sich handelt, da man davon ausgeht, verstärkt aus der Sache hinauszugehen. [152] Wobei einschränkend klargestellt werden muss, dass auch hier ein zu enormer Stress das anti-fragile System - ebenso wie ein resilientes System - auslöschen wird.

Daraus ergeben sich für das anti-fragile Konzept zwei Vorteile:

- Nicht alle Stresssituationen (Störungen) müssen vorhergesagt und vorbereitet werden.
- Belastungen werden als Chance gesehen, von denen man profitieren kann.

5.2 Cyber-Resilienz vs. Anti-Fragilität

Eine der grundlegeden Fragen, wenn man das erste Mal etwas von Cyber-Resilienz hört, ist: Wie unterscheidet sich die Cyber-Resilienz von der Cyber-Security und warum ist sie besser? Die Resilienz wurde in den letzten Jahren als einer der wichtigsten Überlebensmechanismen von Systemen hervorgehoben. Einen deutlichen Unterschied zur Cyber-Security gibt es jedoch nicht. Vielmehr ist es ein neuer Begriff, um über bestehende Ideen und Sicherheitsmaßnahmen zu reden. Angesichts der Komplexität und des rasanten Fortschrittes der Informations- und Kommunikationstechnologien sind Volatilität, Unsicherheit und Unordnung eine Konstante in unserem täglichen Leben geworden. Die Resilienz muss daher zwingend verbessert und angepasst werden, um die Effizienz der Systeme aufrechtzuerhalten. Die Systeme müssen eine bessere Anpassungsfähigkeit besitzen, die es ihnen nicht nur ermöglicht, resilient gegen Angriffe zu sein, sondern es ihnen auch erlaubt, im Angesicht des Chaos' sich zu entwickeln. Eine Rückkehr zur ursprünglichen Form reicht nicht mehr aus; vielmehr müssen Kompetenzen zur Verbesserung vorhanden sein, um zukünftigen Stressoren entgegenzuwirken. [188, p. 1-3]

Bei Systemen mit hoher Komplexität sind Gleichgewicht und Stabilität kaum vorhanden und auch nicht nützlich, da sie dem System keinen Anreiz zur Verbesserung geben. Im Gegensatz dazu wird der Zustand „Am Rande des Chaos" als Verstärker der Wachstumskapazität und Entwicklung der Systeme hervorgehoben. [188, p. 1-3] In diesem Zusammenhang gewinnt der Begriff der Stigmergie zunehmend an Bedeutung. Durch die Einbeziehung von Selbstorganisations- und Lernmechanismen sowie Lernfähigkeit wird Systemen die Fähigkeit gegeben, sich anzupassen und weiterzuentwickeln. [189, p. 34] Der französische Zoologe beschreibt die Stigmergie als einen Koordinationsmechanismus, der bei Insekten

auftritt. Insekten hinterlassen in der Natur Spuren, die die spätere Arbeit derselben oder anderen Insekten beeinflussen, ohne dass es zu irgendeiner Form der Planung, Kontrolle oder direkten Interaktion kommt. [190, p. 1]

Stigmergie = Selbstorganisation + Lernfähigkeit + Anpassungsfähigkeit [191, p. 1-3]

Ein Eingriff in den natürlichen Verlauf von Systemen würde den Selbstorganisationsmechanismus hindern und das System eher schwächen als stärken. [188, p. 2] Außerdem sollten wir nicht versuchen, die Zukunft auf Grundlage vergangener Daten vorherzusagen, denn angesichts ständiger Veränderungen ist diese unvorhersehbar. Besser wäre es die Unsicherheit zu akzeptieren und die Anpassungsfähigkeit sowie die Lernfähigkeit verbessern, um mit dem Unbekannten in der Zukunft zurechtzukommen. [192, p. 765-779]

Der neue Mechanismus für Systeme zum Überleben und Entwickeln wird von Nassim Nicholas Taleb als Anti-Fragilität bezeichnet. [24, p. 21-22] Er schreibt, dass die Anti-Fragilität mehr als Resilienz oder Robustheit ist. Während resiliente Systeme Schocks widerstehen und gleich bleiben, verbessert sich das anti-fragile System. Im Industriesektor beschreibt Vicenzo De Florio [191] die Anti-Fragilität als fortschrittlichen Mechanismus der Resilienz, der die Aspekte Elastizität und maschinelles Lernen miteinbezieht:

Anti-Fragilität = Resilienz + Elastizität + maschinelles Lernen

De Florio präsentiert dabei zwei sich ergänzende Modelle, die je einen unabhängigen „Snapshot“ des Systems betrachten. Das algebraische Modell betrachtet das System als eine vordefinierte und unveränderliche Einheit. Die Schlüsselstrategie dieses Modells ist die Elastizität: Ungünstige Veränderungen und Fehler sollen durch Vorkehrungen, die keine intensive Neukonfiguration des Systems erfordern, verschleiert oder ausgeglichen werden. [191, p. 2-4]

Das zweite Modell ist verhaltensbezogen und konzentriert sich auf die Dynamik des Systems. Es umfasst komplexe Fähigkeiten wie beispielsweise die reaktive und proaktive Planung. Ereignisse, welche die Qualität gefährden, werden eher toleriert statt verschleiert. Im besten Fall sollen diese Ereignisse aktiv genutzt werden, um die Qualität zu optimieren. [191, p. 4-7]

Die beiden Modelle werden durch maschinelles Lernen unterstützt, damit das System eine Form von „Klugheit“ aufgrund erlangtem Wissen erwerben kann. De Florio [191, p. 2] beschreibt, dass alle drei

Aspekte zusammen einen vorbereitenden Schritt für die Entwicklung von anti-fragilen Systemen bilden.

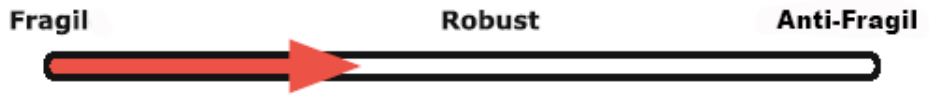

Abbildung 5.1: Der Weg zur Anti-Fragilität [193, p. 7]

Die Idee von De Florio, dass Anti-Fragilität eine erweiterte Form der Resilienz ist, wird auch von Hole [193] verteidigt. Er erklärt die Fragilität, Resilienz und Anti-Fragilität anhand von Stufen in einem Spektrum, in dem die Anti-Fragilität einen höheren Grad der Resilienz darstellt. Weiters gibt er an, dass Systeme zuerst robust beziehungsweise resilient sein müssen, bevor sie anti-fragil sein können, siehe Abbildung 5.1. Kein System kann jedoch gegen alle möglichen Arten von Impacts anti-fragil sein. [193, p. 7]

5.3 Unterschiedliche Konzepte und Definitionen

In der Tabelle 5.1 werden die unterschiedlichen Konzepte und Definitionen von (Cyber)-Resilienz, Robustheit und Anti-Fragilität miteinander verglichen. Dabei soll demonstriert werden, dass die Anti-Fragilität eine Art der (Cyber)-Resilienz in der fortschrittlichsten Form ist.

Resilienz	**Robustheit**	**Anti-Fragil**
gekennzeichnet durch geringe Störanfälligkeit Ist die *„Fähigkeit von Systemen, Änderungen von Zustandsvariablen, Steuerungsvariablen und Parametern zu absorbieren und das System zu erhalten.“* [57, p. 1-23]	Robustheit ist eine Eigenschaft bei einfach oder auch komplizierten Systemen, die sich durch vorhersagbares Verhalten auszeichnet und es dem System ermöglicht, nach einer Störung wieder in seinen Normalzustand zurückzukehren. [194, p. 541-557]	

Fortsetzung auf der nächsten Seite

Tabelle 5.1 – *Fortsetzung von der vorigen Seite*

Resilienz	**Robustheit**	**Anti-Fragil**
dynamischer Prozess mit positiver Anpassung im Kontext signifikanter Widrigkeiten [195, p. 543-562]		*„wird mit jedem Schock besser“* [196, p. 4]
„Resilienz erfordert ein ständiges Gefühl des Unbehagens, das Selbstzufriedenheit verhindert.“ [197, p. 355-356]		*„Die Robustheit oder Resilienz wird durch Volatilität und Unordnung weder beeinträchtigt noch verbessert, während die Anti-Fragilität davon profitiert und dieser positiv gegenübersteht.“* [24, p. 31]
Es ist die Fähigkeit, auf Unsicherheit ausreichend zu reagieren, zusammen mit einem Prozess des Lernens und des Aufbaus eines Wissensspeichers aus vergangenen negativen Erfahrungen. [198, p. 738-757]		*„Systeme, die lernen können, während sie dynamische und resiliente Strategien anwenden“* [191, p. 8]
„Fähigkeit eines Systems, mögliche Gefahren vorzubeugen und ihnen zu widerstehen und zum normalen Betrieb zurückzukehren“ [199, p. 43-60]		*„Anti-Fragilität geht über die Resilienz und Robustheit hinaus. Das Resiliente, das Widerstandsfähige widersteht Schocks und bleibt sich gleich; Das Anti-Fragile wird besser.“* [24, p. 21]

Tabelle 5.1: Vergleich unterschiedlicher Definitionen zu Resilienz, Robustheit und Anti-Fragilität

5.4 Die neue Resilienz

Nach der Gegenüberstellung einiger aktuellen Definitionen zur Resilienz und Anti-Fragilität, liegt die Vermutung nahe, dass die beiden Begriffe mehr miteinander zu tun haben als zuvor angenommen. In der Studie „From Resilience to the Design of Antifragility“ [188, p. 3] wird nach der Gegenüberstellung unterschiedlicher Definitionen von Resilienz und Anti-Fragilität sogar davon gesprochen, dass die Anti-Fragilität ein Synonym für die fortgeschrittenste Form der Resilienz (die „neue“ Resilienz) ist.

Als Beweis dafür wird auf die Idee von De Florio [191] zurückgegriffen und diese mit der Resilienz und Stigmergie verglichen, welche die „neue“ Resilienz abbilden soll. Die Elastizität kann dabei direkt mit der Idee der Anpassungsfähigkeit und das maschinelle Lernen mit der Lernfähigkeit und Selbstorganisation verglichen werden.

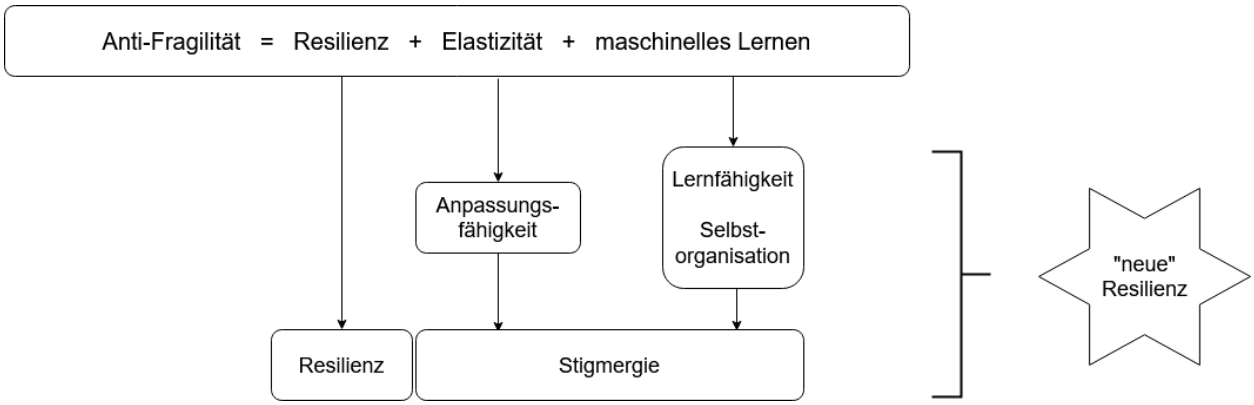

Abbildung 5.2: Die Evolution der Resilienz [188, p. 3]

Die Studie [188] kommt zum Ergebnis, dass die beiden Ideen übereinstimmen und sich die Resilienz, als „neue“ Resilienz, zur Anti-Fragilität weiterentwickelt hat.

Anti-Fragilität = „neue“ Resilienz

6 Conclusion

Resiliente Systeme, Menschen und Gesellschaften sind gut darin, ihren derzeitigen Betrieb aufrechtzuerhalten oder bei Störungen zu ihrem vorherigen Zustand zurückzukehren. Nassim Nicholas Taleb porträtierte die Resilienz mit der Figur des Phönix-Vogels [147], der niemals ausgelöscht wird sondern nach dem Tod aus der Asche aufersteht. Das demonstriert die absolute Robustheit gegen Schocks, ohne Verbesserung. Wenn dem schlangenähnlichen Ungeheuer Hydra aus der griechischen Mythologie jedoch der Kopf abgeschlagen wird, wachsen zwei Köpfe nach. Sie lernt sozusagen aus der Stresssituation, indem doppelt so viel Köpfe nachwachsen wie abgeschlagen werden und ist damit anti-fragil. [148]

Auch Informations- und Kommunikationstechnologien mit komplexen Strukturen benötigen einen Mechanismus, der aus Stresssituationen lernt, um die Effizienz der Systeme aufrecht erhalten zu können. Gerade sie sind anfällig für „schwarze Schwäne“ [140] und den daraus resultierenden, unerwarteten und enormen Auswirkungen. [193, p. 137] Gelingen kann dies mittels der Anti-Fragilität, die als fortschrittlicher Mechanismus der Resilienz gilt und die Aspekte Elastizität und maschinelles Lernen miteinbezieht. [191, p. 1-3]

Als Vorreiter gilt das Tool Chaos Monkey vom Streaming-Portal Netflix. Die Idee dazu entstand während der Migration des eben genannten Portals in die Cloud und der Feststellung, dass sich das System nun in einer komplexen Umgebung befindet. Bei diesem Tool werden laufend AWS-Instanzen per Zufall mutwillig zerstört, um das System aus Fehlern lernen zu lassen. Dadurch konnte man die redundante Architektur testen und sicherstellen, dass ein Serverausfall keine spürbaren Auswirkungen für die Kunden hat. [160]

Auch Fuzzing mit maschinellem Lernen kann helfen, komplexe Systeme sicherer zu machen. Die automatisierte Technik erzeugt Zufallsdaten, die mit Hilfe von maschinellem Lernen qualitativ hochwertiger sind, um Sicherheitslücken aufzuspüren. [200] Intelligente automatische Patchtools können dann die zuvor entdeckten Sicherheitslücken schließen. [186]

Mit Hilfe eines roten und blauen Teams soll ebenfalls die Anpassung an komplexe Systeme und den sich ständig verändernden Herausforderungen gelingen. Beim Cyber Red Teaming tritt das rote Team als Gegner auf, um Sicherheitslücken aufzuspüren. [201, p. 1] Im Gegensatz zu herkömmlichen Angreifern hat das rote Team nicht die Absicht, Profit zu erzielen, Spionage zu betreiben oder ideologische Ziele durchzusetzen. Vielmehr geht es darum, die Sicherheitslücken zu entdecken, damit das blaue Team sie schließen kann. Dieses Verfahren kostet viele Ressourcen, härtet jedoch das System, indem laufend Schwachstellen gefunden und ausgebessert werden.

Zusammenfassend verhalten sich resiliente Systeme lediglich neutral gegenüber Erschütterungen, während anti-fragile Systeme aufblühen und daraus profitieren. [147] Ganz gleich, ob es sich um das Tool Chaos Monkey von Netflix, Cyber Red Teaming, Fuzzing oder andere ähnlichen Technologien handelt, lässt sich zusammenfassend sagen: Mit ihnen ist der erste Schritt in Richtung anti-fragiler komplexer Systeme, die einerseits besser werden und andererseits immer verfügbar sein sollen, getan.

6.1 Ausblick und weiterführende Arbeit

Abschließend ist festzuhalten, dass diese Arbeit als Grundlage für weitere Forschungen im Bereich Anti-Fragilität dienen soll. Wie Prognosen, anhand des Beispiels in der Abbildung 3.6, zeigen, wird der Einsatz von vernetzten Geräten weiter steigen. Dadurch werden die Komplexität in Systemen sowie die wechselseitigen Abhängigkeiten auch weiter steigen. Bisherige Methoden zur Erkennung und Behebung von Schwachstellen in Systemen, haben zwar den Grundstein für anti-fragile Systeme gelegt, müssen aber laufend verbessert werden.

Derzeitige Methoden arbeiten zum Teil schon mit der künstlichen Generierung von Wissen aus Erfahrungen, greifen aber noch etwas zu kurz, da komplexere Angriffsvektoren nicht beachtet werden können. Nicht-automatisierte Techniken könnten diese zwar beachten, würden aber zu viele Ressourcen benötigen, um ständig das System zu verbessern. In Zeiten von Big Data und Industrie 4.0 ist dies nicht mehr flächendeckend möglich.

Die Forschung sollte sich deshalb auf Methoden konzentrieren, die maschinell dazulernen und Aufgaben selbstständig bewältigen können. Wichtig ist dabei, das gesamte System abzudecken und dieses kontinuierlich, unter Einbeziehung komplexer und zielgerichteter Angriffsvektoren, wie sie bei Advanced Persistent Threats vorkommen, zu testen.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[1] Lexico.com, “cybersecurity,” https://www.lexico.com/en/definition/cybersecurity, Zugriffsdatum: 09.07.2019.

[2] A. DeNisco-Rayome, “Five emerging cybersecurity threats you should take very seriously in 2019,” https://www.zdnet.com/article/five-emerging-cybersecurity-threats-you-should-take-very-seriously-in-2019/, Zugriffsdatum: 25.07.2019.

[3] D. Presse-Agentur, “SSchwerwiegender Cyberangriffäuf österreichisches Außenministerium,” https://www.heise.de/newsticker/meldung/Schwerwiegender-Cyberangriff-auf-oesterreichisches-Aussenministerium-4628190.html, Zugriffsdatum: 27.01.2020.

[4] P. Muncaster, “Vietnamese Hackers Compromised BMW and Hyundai: Report,” https://www.infosecurity-magazine.com/news/vietnamese-hackers-compromised-bmw/, Zugriffsdatum: 27.01.2020.

[5] A. Kannenberg, “Geheimdienst hinter Angriff auf Bundestag vermutet,” https://www.heise.de/newsticker/meldung/Geheimdienst-hinter-Angriff-auf-Bundestag-vermutet-2660419.html, Zugriffsdatum: 27.01.2020.

[6] G. W. Michael Schirmbrand, Andreas Tomek, “Cyber Security in Österreich - Strategien österreichischer Unternehmen gegen Cyberkriminalität,” 2018. [Online]. Available: http://www.kpmg.at/NewsletterEvent/getFile.php?id=4792&hash=5afe88f0ad0ed1.34318628

[7] H. Saurugg, “Vernetzung und Komplexität,” https://www.saurugg.net/vernetzung-komplexitaet, Zugriffsdatum: 11.07.2019.

[8] T. E. U. A. for Cybersecurity (ENISA), “Measurement Frameworks and Metrics for Resilient Networks and Services - Technical report,” 2011. [Online]. Available: https://www.enisa.europa.eu/publications/metrics-tech-report/at_download/fullReport

[9] H. Saurugg, “Too-big-to-fail – eine Gefahr für die Systemsicherheit,” https://www.saurugg.net/hintergrundthemen, Zugriffsdatum: 17.07.2019.

[10] E. G. Amann, “Resilienz - Widerstandsfähigkeit im Beruf,” https://www.saurugg.net/strom-blackout/resilienz-und-anpassung, 2017.

[11] W. N. Adger, “Social and ecological resilience: are they related?” 2000. [Online]. Available: https://www.researchgate.net/profile/W_Adger/publication/235737390_Social_and_Ecological_Resilience_Are_They_Related/links/0c9605300fc07a35a6000000/Social-and-Ecological-Resilience-Are-They-Related.pdf?origin=publication_detail

[12] K. J. Fridolin Simon Brand, “Focusing the Meaning(s) of Resilience: Resilience as a Descriptive Concept and a Boundary Object,” https://www.ecologyandsociety.org/vol12/iss1/art23/, Zugriffsdatum: 13.11.2019.

[13] C. L. Heinz Ellenberg, “Vegetation Mitteleuropas mit den Alpen,” 2010.

[14] C. S. Ian de Terte, “Psychological Resilience of Workers in High-Risk Occupations,” 2014.

[15] J. S. J. Z. Fredrik Björck, Martin Henkel, “Cyber Resilience – Fundamentals for a Definition,” 2015.

[16] A. Securities and I. Commission, “REPORT 429: Cyber resilience: Health check,” 2015. [Online]. Available: https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf

[17] B. H. Daniel L. Elliott, Lawrence Susskind, “Just waiting for the next big bang: business continuity planning in the UK finance sector.” 1999.

[18] B. für Sicherheit in der Informationstechnik (BSI), “BSI-Standard 100-4: Notfallmanagement Version 1.0,” 2008. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2

[19] O. E. Dictionary, “resilience (n.),” https://www.itwissen.info/Metrik-metric.html, Zugriffsdatum: 01.07.2019.

[20] M. Dictionary, “resilient,” http://www.macmillandictionaryblog.com/resilient, Zugriffsdatum: 01.07.2019.

[21] E. G. Amann, “Resilienz - Widerstandsfähigkeit im Beruf,” 2012. [Online]. Available: https://www.uni-hamburg.de/career-center/angebot/fishingforcareeers/frueherevortraege/resilienzimberuf-amann/resilienzimberuf-vortrag-amann.pdf

[22] G. Kormann, “Resilienz – Was Kinder stärkt und in ihrer Entwicklung unterstützt,” 2007. [Online]. Available: www.kormann.de/downloads/DL06_Resilienz-Was_Kinder_staerkt.pdf

[23] S. Mauritz, “Salutogenese,” https://www.resilienz-akademie.com/salutogenese/, 2018, Zugriffsdatum: 23.05.2019.

[24] N. N. Taleb, “Anti-Fragilität - Anleitung für eine Welt, die wir nicht verstehen,” 2012.

[25] F. W. Nietzsche, “Götzen-Dämmerung oder Wie man mit dem Hammer philosophiert,” 1889.

[26] P. D. F. Petermann, “Vorhersagefaktoren kindlicher Resilienz,” 2018. [Online]. Available: https://www.psychologie.uzh.ch/dam/jcr:1f5f12f3-7662-4c58-ba8f-c96e218f9f1e/02_Vorhersagefaktoren%20kindlicher%20Resilienz%20-%20Ergebnisse%20deutscher%20und%20internationaler%20L%C3%A4ngsschnittstudien%20(Prof.%20Dr.%20Franz%20Petermann).pdf

[27] M. H. S. Manred Laucht, Günter Esser, “Längsschnittforschung zur Entwicklungsepidemiologie psychischer Störungen: Zielsetzung, Konzeption und zentrale Befunde der Mannheimer Risikokinderstudie ,” https://doi.org/10.1026//0084-5345.29.4.246, 2000, Zugriffsdatum: 27.05.2019.

[28] I. Wernicke, “Resilienz und Möglichkeiten von Resilienzförderung im Kontext von Kindertageseinrichtungen,” 2018. [Online]. Available: http://edoc.sub.uni-hamburg.de/haw/volltexte/2018/4452/pdf/Wernicke_Inga_BA_2018_11_27.pdf

[29] W. Stangl, “Stichwort: ’Resilienz’,” https://lexikon.stangl.eu/593/resilienz/, 2019, Zugriffsdatum: 24.04.2019.

[30] Wikipedia, “Resilienz (Psychologie),” https://de.wikipedia.org/wiki/Resilienz_(Psychologie), Zugriffsdatum: 27.04.2019.

[31] Duden, “Ingenieurwissenschaft, die,” https://www.duden.de/rechtschreibung/Ingenieurwissenschaft, Zugriffsdatum: 11.07.2019.

[32] T. R. Shift, “What is resilient infrastructure?” https://www.resilienceshift.org/work-with-us/faqs/, Zugriffsdatum: 13.11.2019.

[33] Wikipedia, “Resilienz (Ingenieurwissenschaften),” https://de.wikipedia.org/wiki/Resilienz_(Ingenieurwissenschaften), Zugriffsdatum: 11.07.2019.

[34] D. M. Schumann, “Verteilte Systeme: State of the Art,” 2003. [Online]. Available: http://webdoc.sub.gwdg.de/ebook/lm/arbeitsberichte/2003/01.pdf

[35] M. v. S. Andrew S. Tanenbaum, “Verteile Systeme, 2. Auflage,” 2008.

[36] D. K. Pohl, "Software Systems Engineering," https://sse.uni-due.de/forschung/schwerpunkte/adaptive-systeme, Zugriffsdatum: 11.07.2019.

[37] Wissen.de, "Schott," https://www.wissen.de/lexikon/schott-schifffahrt, Zugriffsdatum: 11.07.2019.

[38] H. Saurugg, "Das Energiesystem resilient gestalten," https://www.saurugg.net/2017/blog/strom-versorgung/das-energiesystem-resilient-gestalten, 2017, Zugriffsdatum: 28.05.2019.

[39] P. D. O. Renn, "Das Energiesystem resilient gestalten," 2017. [Online]. Available: https://www.akademienunion.de/fileadmin/redaktion/user_upload/Publikationen/Stellungnahmen/ESYS_Analyse_Das_Energiesystem_resilient_gestalten.pdf

[40] H. Saurugg, "Naht der Schwarze Schwan der Energiewirtschaft – Ein Black Out?" https://www.saurugg.net/2018/presse/naht-der-schwarze-schwan-der-energiewirtschaft-ein-black-out, Zugriffsdatum: 04.01.2020.

[41] ——, "Auswirkungen eines Blackouts," https://www.saurugg.net/strom-blackout/auswirkungen-eines-blackouts, Zugriffsdatum: 04.01.2020.

[42] T. u. n. M. e. V. Bundesverband Informationswirtschaft, "Ausfallsicherheit des Energieversorgungssystems – Von der Robustheit zur Resilienz," 2018. [Online]. Available: https://www.bitkom.org/sites/default/files/file/import/180530-Diskussionspapier-Resilienz-des-Energieversorgungssystems-online-final-2.pdf

[43] E. Philippines, "IMPLEMENTING SINGLE OUTAGECONTINGENCY (N-1) OPERATIONAL CRITERION," 2014. [Online]. Available: http://www.erc.gov.ph/Files/Render/media/N-1OperationalCriteria.pdf

[44] H. L. Willis, "Power Distribution Planning Reference Book," 2004.

[45] B. für Nachhaltigkeit und Tourismus, "Energie in Österreich 2018," 2018. [Online]. Available: https://www.bmnt.gv.at/dam/jcr:3db9b813-8c0f-49fd-b5ff-89e9600c3cd7/Energie_in_OE2018_Barrierefrei.pdf

[46] W. M. L. H. R. R. T. J. P. Anvari, Lohmann, "Short term fluctuations of wind and solar power systems," 2016. [Online]. Available: https://iopscience.iop.org/article/10.1088/1367-2630/18/6/063027/pdf

[47] H. Lund, "Smart energy and smart energy systems," 2017.

[48] N. K. GmbH, “Was ist ein Schwarzstart?” https://www.next-kraftwerke.de/wissen/schwarzstart, Zugriffsdatum: 13.11.2019.

[49] B. für Wirtschaft und Energie, “Was ist ein "Prosumer"?” https://www.bmwi-energiewende.de/EWD/Redaktion/Newsletter/2016/06/Meldung/direkt-erklaert.html, Zugriffsdatum: 07.06.2019.

[50] N. L. Stefan Luber, “Was ist Predictive Maintenance?” https://www.bigdata-insider.de/was-ist-predictive-maintenance-a-640755/, Zugriffsdatum: 07.06.2019.

[51] Bundesnetzagentur, “IT-Sicherheitskatalog für Strom- und Gasnetze,” https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/Netzbetreiber/IT_Netzbetreiber_node.html, Zugriffsdatum: 14.06.2019.

[52] R. des Bundes, “BGBl. I Nr. 111/2018,” https://www.ris.bka.gv.at/eli/bgbl/I/2018/111, Zugriffsdatum: 05.08.2019.

[53] ——, “Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG),” https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536, Zugriffsdatum: 05.08.2019.

[54] ——, “215. Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV),” https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2019_-II_215/BGBLA_2019_II_215.html, Zugriffsdatum: 05.08.2019.

[55] Spektrum.de, “Lexikon der Biologie - Ökosystemforschung,” https://www.spektrum.de/lexikon/biologie/oekosystemforschung/47500, Zugriffsdatum: 03.06.2019.

[56] F. Fischer, “Climate Crisis and the Democratic Prospect: Participatory Governance in Sustainable Communities,” 2017.

[57] C. S. Holling, “Resilience and Stability of Ecological Systems,” 1973.

[58] S. R. C. A. K. Brian Walker, C. S. Holling, “Resilience, Adaptability and Transformability in Social–ecological Systems,” https://www.ecologyandsociety.org/vol9/iss2/art5/, Zugriffsdatum: 04.06.2019.

[59] D. Tilman, “Global environmental impacts of agricultural expansion: The need for sustainable and efficient practices,” https://www.ncbi.nlm.nih.gov/pmc/articles/PMC34218/, Zugriffsdatum: 05.06.2019.

[60] Food and A. O. of the United Nations, “Definitions of forest change processes,” http://www.fao.org/3/ad665e/ad665e04.htm, Zugriffsdatum: 05.06.2019.

[61] W. W. F. F. N. (WWF), “overfishing,” https://www.worldwildlife.org/threats/overfishing, Zugriffsdatum: 06.06.2019.

[62] D. Johnston, “Overfishing,” https://ypte.org.uk/factsheets/overfishing/introduction, Zugriffsdatum: 13.11.2019.

[63] S. R. C. S. S. University, “About us,” https://www.stockholmresilience.org/about-us.html, Zugriffsdatum: 07.06.2019.

[64] I. der Vereinten Nationen (UNIS) Wien, “Ziele für nachhaltige Entwicklung,” http://www.unis.unvienna.org/unis/de/topics/sustainable_development_goals.html, Zugriffsdatum: 24.06.2019.

[65] H. Esser, “Soziologie: allgemeine Grundlagen,” 1999.

[66] K. Thoma, “Resilien-Tech: "Resilience-by-Design": Strategie für die technologischen Zukunftsthemen,” 2014.

[67] W. K. Peter Hupfer, “Witterung und Klima: Eine Einführung in die Meteorologie und Klimatologie,” 2013.

[68] B. W. F. M. L. Alexis Kwasinski, Joseph Trainor, “A Conceptual Framework for Assessing Resilience at the Community Scale,” 2016. [Online]. Available: dx.doi.org/10.6028/NIST.GCR.16-001

[69] BSI, “Cyber risk and resilience - guidance for the governing body and executive management,” British Standards Institution (BSI), Standard BS 31111:2018, 3 2018.

[70] D. C. J. Kaplan, A. Weinberg, “Risk and Responsibility in a Hyperconnected World,” 2012. [Online]. Available: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

[71] Duden, “cyber-, Cyber-,” https://www.duden.de/rechtschreibung/cyber_, 2019, Zugriffsdatum: 12.06.2019.

[72] S. Ebner, “Warum sprechen eigentlich alle von "Cyber"? ,” https://www.suedkurier.de/ueberregional/wissenschaft/Warum-sprechen-eigentlich-alle-von-Cyber-Wo-das-Wort-herkommt-und-was-es-bedeutet;art1350069,8854775, 2019, Zugriffsdatum: 13.06.2019.

[73] H. W. Karl-Heinz Dammer, Thomas Vogel, “Zur Aktualität der Kritischen Theorie für die Pädagogik,” 2015.

[74] M.-W. C. Dictionary, “cybersecurity,” https://www.merriam-webster.com/dictionary/cybersecurity?src=search-dict-hed, Zugriffsdatum: 09.07.2019.

[75] expert group formed by members of the ETSI/CEN/CENELEC Cybersecurity Coordination Group (CSCG) and ENISA, “Definition of Cybersecurity – Gaps and overlaps in standardisation,” 2015. [Online]. Available: https://www.enisa.europa.eu/publications/definition-of-cybersecurity

[76] B. für Sicherheit in der Informationstechnik, “Glossar und Begriffsdefinitionen,” https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html, 2013, Zugriffsdatum: 13.06.2019.

[77] T. M. Corporation, “Cyber Resiliency FAQ,” 2017. [Online]. Available: https://www.mitre.org/sites/default/files/PR_17-1434.pdf

[78] T. E. C. B. (ECB), “What is cyber resilience?” https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html, Zugriffsdatum: 09.07.2019.

[79] D. Dobrygowski, “Cyber resilience: everything you (really) need to know,” https://www.weforum.org/agenda/2016/07/cyber-resilience-what-to-know/, Zugriffsdatum: 19.06.2019.

[80] CVEdetails.com, “Security Vulnerabilities Published In 2017,” https://www.cvedetails.com/vulnerability-list/year-2017/vulnerabilities.html, Zugriffsdatum: 06.11.2019.

[81] M. Corporation, “About CVE,” https://cve.mitre.org/about/index.html, Zugriffsdatum: 06.11.2019.

[82] CVEdetails.com, “Security Vulnerabilities Published In 2018,” https://www.cvedetails.com/vulnerability-list/year-2018/vulnerabilities.html, Zugriffsdatum: 06.11.2019.

[83] C. R. Frederick Kempe, “Overcome by cyber risks? Economic benefits and costs of alternate cyber futures,” https://publications.atlanticcouncil.org/cyberrisks/, Zugriffsdatum: 19.06.2019.

[84] C. Veltsos, “Cyber Resilience Tools and Principles for Boards of Directors,” https://securityintelligence.com/cyber-resilience-tools-and-principles-for-boards-of-directors/, Zugriffsdatum: 10.07.2019.

[85] ISO/IEC, “Information technology — security techniques — information security management systems — overview and vocabulary,” International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), Standard ISO/IEC 27000:2018(en), 2018.

[86] ISO, “Risk management — guidelines,” International Organization for Standardization (ISO), Standard ISO 31000:2018(en), 2018.

[87] N. H. L. Solutions, “5 Tips for Building a Cyber Resilience Strategy,” https://blog.nhlearningsolutions.com/blog/5-tips-for-building-a-cyber-resilience-strategy, Zugriffsdatum: 10.07.2019.

[88] Encyclopedia.com, “Cascade Effect,” https://www.encyclopedia.com/science/dictionaries-thesauruses-pictures-and-press-releases/cascade-effect, Zugriffsdatum: 14.11.2019.

[89] R. G. Deborah Bodeau, “Cyber Resiliency Design Principles,” 2017. [Online]. Available: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf

[90] J. T. F. T. Initiative, “NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View,” 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[91] A. W. P. D. G. D. L. Marianne Swanson, Pauline Bowen, “NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems,” 2010. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[92] S. F. P. M. M. K. D. S. M. H. Thorsten Scheibel, Claudia Krüger, "BIA-Anwenderleitfaden," 2019. [Online]. Available: https://www.ibcrm.de/wp-content/uploads/2019/04/BIA-Anwenderleitfaden_08.04.2019.pdf

[93] D. of Defense, "Cybersecurity Test and Evaluation Guidebook," 2015. [Online]. Available: http://www.dote.osd.mil/docs/TempGuide3/Cybersecurity_TE_Guidebook_July1_2015_v1_0.pdf

[94] J. T. F. T. Initiative, "NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations," 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[95] C. T. Lopez, "Assume Networks Are Compromised, DOD Official Urges," https://www.defense.gov/explore/story/Article/1970167/assume-networks-are-compromised-dod-official-urges/, Zugriffsdatum: 28.11.2019.

[96] C. Eilers, "Was ist ein Advanced Persistent Threat (APT)?" https://www.ceilers-news.de/serendipity/219-Was-ist-ein-Advanced-Persistent-Threat-APT.html, Zugriffsdatum: 28.11.2019.

[97] I. FireEye, "Anatomy of Advanced Persistent Threats," https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html, Zugriffsdatum: 28.11.2019.

[98] R. G. D. B. R. M. Ron Ross, Victoria Pillitteri, "NIST SP 800-160, Developing Cyber Resilient Systems," 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

[99] U. of Cape Town, "Information hiding," https://www.cs.uct.ac.za/mit_notes/software/htmls/ch07s07.html, Zugriffsdatum: 29.11.2019.

[100] SearchSoftwareQuality, "What is obfuscation (obfu)? - Definition from WhatIs.com," https://searchsoftwarequality.techtarget.com/definition/obfuscation, Zugriffsdatum: 29.11.2019.

[101] M. Rouse, "Analyse des Nutzerverhaltens oder User Behavior Analysis (UBA)," https://www.computerweekly.com/de/definition/Analyse-des-Nutzerverhaltens-oder-User-Behavior-Analysis-UBA, Zugriffsdatum: 29.11.2019.

[102] C. on National Security Systems, "Glossary," 2015. [Online]. Available: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[103] V. Joshi, "Parsing Through Partitions in a Distributed System," https://medium.com/baseds/parsing-through-partitions-in-a-distributed-system-3c1723fecc4e, Zugriffsdatum: 30.11.2019.

[104] E. K. C. A. J. J. P. R. M. S. P. S. James P.G. Sterbenz, David Hutchison, "Redundancy, Diversity, and Connectivity to Achieve MultilevelNetwork Resilience, Survivability, and Disruption Tolerance," 2012. [Online]. Available: http://www.ittc.ku.edu/resilinets/papers/Sterbenz-Hutchison-Cetinkaya-Jabbar-Rohrer-Scholler-Smith-2012.pdf

[105] K. Dooley, "Designing Large Scale Lans: Help for Network Designers," 2002.

[106] M. Rouse, "data virtualization," https://searchdatamanagement.techtarget.com/definition/data-virtualization, Zugriffsdatum: 02.12.2019.

[107] techopedia.com, "Replication," https://www.techopedia.com/definition/1236/replication, Zugriffsdatum: 02.12.2019.

[108] F. S. Maria Leitner, Timea Pahi, "Das Konzept von Situationsbewusstsein und Cyber-Lagebildern," 2018.

[109] B. Noglik, "Moving Target Defense," 2015. [Online]. Available: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2015-03-1/NET-2015-03-1_12.pdf

[110] N. I. of Standards and T. (NIST), "Cybersecurity Framework," https://www.nist.gov/cyberframework, Zugriffsdatum: 03.12.2019.

[111] G. U. of Technology, "Veränderungsmanagement," https://www.tugraz.at/tu-graz/universitaet/leitziele-und-schwerpunkte/veraenderungsmanagement/veraenderungsmanagement/, Zugriffsdatum: 19.06.2019.

[112] D. S. Y.M. Wara, "A Guide to Establishing Computer Security Incident Response Team (CSIRT)," 2015. [Online]. Available: https://www.bitkom.org/sites/default/files/file/import/180530-Diskussionspapier-Resilienz-des-Energieversorgungssystems-online-final-2.pdf

[113] D. C. Steinhoff, "Aktueller Begriff - Industrie 4.0," 2013. [Online]. Available: https://www.dieterstier.de/cms/wp-content/uploads/2013/06/industrie-4-0-data.pdf

[114] Statista, " Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)," https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, Zugriffsdatum: 11.07.2019.

[115] Duden, “Komplexität, die,” https://www.duden.de/rechtschreibung/Komplexitaet, Zugriffsdatum: 12.07.2019.

[116] U. Bardi, “Der Seneca-Effekt: Warum Systeme kollabieren und wie wir damit umgehen können,” 2017, Zugriffsdatum: 16.07.2019.

[117] litteratur.ch, “Ugo Bardi: Der Seneca-Effekt,” https://blog.litteratur.ch/WordPress/?p=8990, Zugriffsdatum: 16.07.2019.

[118] I. D. B. GmbH, “Metrik,” https://www.itwissen.info/Metrik-metric.html, Zugriffsdatum: 24.06.2019.

[119] M. Gehri, “CISO – eine Investition mit ROI,” https://www.infoguard.ch/de/blog/ciso-eine-investition-mit-roi, Zugriffsdatum: 17.08.2019.

[120] L. L. P. K. A. R. J. B. Deb Bodeau, Rich Graubart, “Cyber Resiliency Metrics,” 2012. [Online]. Available: https://register.mitre.org/sr/12_2226.pdf

[121] T. E. U. A. for Cybersecurity (ENISA), “Resilience Metrics,” https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/internet-infrastructure/metrics, Zugriffsdatum: 19.07.2019.

[122] T. W. I. A. T. A. C. I. Brian Bates, Karen M. Goertzel, “Measuring Cyber Security and Information Assurance: A State-of-the Art Report,” 2009.

[123] B. C. B. Supervision, “Cyber-resilience: Range of practices,” 2018. [Online]. Available: https://www.bis.org/bcbs/publ/d454.pdf

[124] W. L. Silber, “The Great Financial Crisis of 1914: What Can We Learn from Aldrich-Vreeland Emergency Currency?” 2007. [Online]. Available: https://archive.nyu.edu/bitstream/2451/26369/2/FIN-06-009.pdf

[125] F. Patalong, “Die fragilen Lebensadern des Internets,” https://www.spiegel.de/netzwelt/web/unterseekabel-die-fragilen-lebensadern-des-internets-a-1015809.html, Zugriffsdatum: 20.08.2019.

[126] TeleGeography, “Submarine Cable Frequently Asked Questions,” https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions, Zugriffsdatum: 20.08.2019.

[127] C. Stöcker, "Vierter Netzausfall nährt Verschwörungs-Theorien," https://www.spiegel.de/netzwelt/tech/internet-seekabel-vierter-netzausfall-naehrt-verschwoerungs-theorien-a-533040.html, Zugriffsdatum: 20.08.2019.

[128] LiveLeak.com, "THIRD Internet Cable cut - TEHRAN 100% Outage," https://web.archive.org/web/20080209163116/http://www.liveleak.com/view?i=15a_1201978059, Zugriffsdatum: 20.08.2019.

[129] Reuters, "37-Milliarden-Dollar-Übernahme rüttelt Chipbranche auf," https://de.reuters.com/article/chipbranche-fusion-idDEKBN0OD1ME20150528, Zugriffsdatum: 17.07.2019.

[130] E. Grabar, "Antibiotika: Gefährliche Lieferungen," https://www.zeit.de/wissen/gesundheit/2014-11/antibiotika-penicillin-lieferung-engpass, Zugriffsdatum: 17.07.2019.

[131] D. W. Nachrichten, "Glencore: Crash-Gefahr beim größten Rohstoff-Händler der Welt," https://deutsche-wirtschafts-nachrichten.de/2015/09/28/crash-gefahr-beim-groessten-rohstoff-haendler-der-welt/, Zugriffsdatum: 18.07.2019.

[132] ——, "Rohstoff-Schock: Gefährliche Spirale, die kaum zu stoppen ist," https://deutsche-wirtschafts-nachrichten.de/2015/08/07/rohstoff-schock-gefaehrliche-spirale-die-kaum-zu-stoppen-ist/, Zugriffsdatum: 18.07.2019.

[133] S. Krempl, "Marktanalyse: Microsoft-Abhängigkeit führt zu SSchmerzpunkten"beim Bund," https://www.heise.de/newsticker/meldung/Marktanalyse-Microsoft-Abhaengigkeit-fuehrt-zu-Schmerzpunkten-beim-Bund-4533951.html, Zugriffsdatum: 15.10.2019.

[134] D. Schirrmacher, "Patchday Microsoft: Windows für wurmartige Attacken anfällig," https://www.heise.de/security/meldung/Patchday-Microsoft-Windows-fuer-wurmartige-Attacken-anfaellig-4496244.html, Zugriffsdatum: 21.08.2019.

[135] ——, "Patchday: Angreifer attackieren Windows und Windows Server," https://www.heise.de/security/meldung/Patchday-Angreifer-attackieren-Windows-und-Windows-Server-4466722.html, Zugriffsdatum: 21.08.2019.

[136] H. Böck, "Windows-Texteingabesystem bietet viele Angriffsmöglichkeiten," https://www.golem.de/news/project-zero-windows-texteingabesystem-bietet-viele-angriffsmoeglichkeiten-1908-143199.html, Zugriffsdatum: 21.08.2019.

[137] A. Freude, "Kommentar zum Bundeshack: Schluss mit Schlangenöl und Monokultur!" https://www.heise.de/newsticker/meldung/Kommentar-zum-Bundeshack-Schluss-mit-Schlangenoel-und-Monokultur-3985144.html, Zugriffsdatum: 21.08.2019.

[138] A. Barczok, "Das Microsoft-Dilemma: Windows 10 und Office in Behörden," https://www.heise.de/ct/artikel/Das-Microsoft-Dilemma-Windows-10-und-Office-in-Behoerden-3970996.html, Zugriffsdatum: 21.08.2019.

[139] M. Förster, "Sicherheitslücken und mangelnder Datenschutz: Microsoft patzt bei Office 365 ," https://www.heise.de/ix/meldung/Sicherheitsluecken-und-mangelnder-Datenschutz-Microsoft-patzt-bei-Office-365-4398584.html, Zugriffsdatum: 23.08.2019.

[140] N. N. Taleb, "Der Schwarze Schwan - Die Macht höchst unwahrscheinlicher Ereignisse," 2015.

[141] S. Zeitung, "Das Verletzlichkeitsparadox ," https://www.sueddeutsche.de/wissen/urbane-sicherheit-24-stunden-bis-zum-chaos-1.1341258-2, Zugriffsdatum: 18.07.2019.

[142] C. B. Roland Heuermann, Matthias Tomenendal, "Digitalisierung in Bund, Ländern und Gemeinden: IT-Organisation, Management und Empfehlungen," 2018.

[143] N. N. Taleb, "'Antifragility' as a mathematical idea," https://www.nature.com/articles/494430e, Zugriffsdatum: 04.07.2019.

[144] S. H. To, "Volatility in Statistics and Markets: Simple Definition, Calculation ," https://www.statisticshowto.datasciencecentral.com/volatility/, Zugriffsdatum: 15.11.2019.

[145] Duden, "Volatilität, die," https://www.duden.de/rechtschreibung/Volatilitaet, Zugriffsdatum: 05.07.2019.

[146] Nature, "Antifragility as a mathematical idea," 2013.

[147] U. Techt, "Antifragilität: Weshalb Systeme antifragil statt nur robust sein sollten," https://uwetecht.de/antifragilitaet-weshalb-systeme-antifragil-statt-nur-robust-sein-sollten/, Zugriffsdatum: 08.07.2019.

[148] D. Ogden, "Drakon: Dragon Myth and Serpent Cult in the Greek and Roman Worlds," 2013.

[149] R. Kotansky, "Greek Magical Amulets: The Inscribed Gold, Silver, Copper, and Bronze Lamellae," 2014.

[150] L. A. B. Edward J. Calabrese, "Hormesis as a Biological Hypothesis," 1998. [Online]. Available: https://ehp.niehs.nih.gov/doi/pdf/10.1289/ehp.98106s1357

[151] G. u. K. Bundesministerium für Arbeit, Soziales, "Hypertrophie," https://www.gesundheit.gv.at/lexikon/h/lexikon-hypertrophie, Zugriffsdatum: 08.07.2019.

[152] K. Cobb, "Is "antifragile" better than "resilient"?" https://www.resilience.org/stories/2013-11-24/is-antifragile-better-than-resilient/, Zugriffsdatum: 23.07.2019.

[153] S. T. Fundamentals, "Unit Testing," http://softwaretestingfundamentals.com/unit-testing/, Zugriffsdatum: 20.07.2019.

[154] A. R. G. Daniel Roy Greenfeld, "Two Scoops of Django: Best Practices For Django 1.8," 2015.

[155] B. Wilms, "Chaos Engineering: Für kontrollierte Unordnung sorgen," https://www.heise.de/developer/artikel/Chaos-Engineering-Fuer-kontrollierte-Unordnung-sorgen-4423501.html?seite=all, Zugriffsdatum: 20.07.2019.

[156] M. Y. Daniel Knapp, "Tools und Techniken in der Testpyramide: Wo eine Größe nicht allen passt," 2016. [Online]. Available: https://www.sigs-datacom.de/uploads/tx_dmjournals/knapp_yilmaz_OS_02_16_bmKo.pdf

[157] G. R. Ralph Stair, "Fundamentals of Information Systems," 2017.

[158] M. Fowler, "UnitTest," https://martinfowler.com/bliki/UnitTest.html, Zugriffsdatum: 18.11.2019.

[159] R. Hat, "Was sind Microservices?" https://www.redhat.com/de/topics/microservices/what-are-microservices, Zugriffsdatum: 22.07.2019.

[160] N. T. Blog, "The Netflix Simian Army," https://medium.com/netflix-techblog/the-netflix-simian-army-16e57fbab116, Zugriffsdatum: 18.11.2019.

[161] A. G. Martinez, "Chaos Monkeys: Obscene Fortune and Random Failure in Silicon Valley," 2017.

[162] O. Williams, "How your business could learn from Chaos Monkey," https://thenextweb.com/insider/2013/03/03/how-your-business-could-learn-from-chaos-monkey/, Zugriffsdatum: 22.07.2019.

[163] J. Yuen, "Automated Cyber Red Teaming," 2015. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.954.2682&rep=rep1&type=pdf

[164] J. Lorains, "Cyber Exercising, Red Teaming and Pentesting," https://medium.com/swlh/cyber-exercising-red-teaming-and-pentesting-5fc11296c4b0, Zugriffsdatum: 19.10.2019.

[165] Åke J. Holmgren, "A framework for vulnerability assessment of electric power systems," 2007.

[166] R. R. V. I. E. W. Glenn Taylor, Richard Frederiksen, "Agent-based Simulation of Geo-Political Conflict," 2004.

[167] D. of Defense (DoD), "Department of Defense IT Enterprise Strategy and Roadmap," 2011. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf

[168] H. H. E. K. G. R. J. S. Chris Fawcett, Malte Helmert, "Adaptive Game AI with Dynamic Scripting," 2005. [Online]. Available: https://www.spronck.net/pubs/DynamicScripting.pdf

[169] P. D. J. Koubek, "OXO, Spacewar!, Adventure – Ein handlungsorientierter Ausflug in die Geschichte der Computerspiele," 2009. [Online]. Available: https://medienwissenschaft.uni-bayreuth.de/wp-content/uploads/assets/Koubek/forschung/KoubekSpielegeschichte.pdf

[170] W. Saletan, "Chess Bump," https://slate.com/technology/2007/05/the-triumphant-teamwork-of-humans-and-computers.html, Zugriffsdatum: 09.11.2019.

[171] T. D. R. T. IBM, "Watson," https://researcher.watson.ibm.com/researcher/view_group.php?id=2099, Zugriffsdatum: 09.11.2019.

[172] J. Markoff, "Computer Wins on 'Jeopardy!': Trivial, It's Not," https://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html, Zugriffsdatum: 09.11.2019.

[173] P. Welter, "Versicherer ersetzt zahlreiche Mitarbeiter durch künstliche Intelligenz," https://www.faz.net/aktuell/wirtschaft/japan-versicherer-ersetzt-mitarbeiter-durch-ki-ibm-watson-14605854.html, Zugriffsdatum: 09.11.2019.

[174] S. A. Gerevini, Alfonso and M. Vallati, "PbP2: Automatic Configuration of a Portfolio based Multi Planner," 2011. [Online]. Available: http://eprints.hud.ac.uk/id/eprint/15381/1/gersaevalipc11.pdf

[175] B. Miller, "Operating System Utility Program Reliability - The Fuzz Generator," 1988. [Online]. Available: http://pages.cs.wisc.edu/~bart/fuzz/CS736-Projects-f1988.pdf

[176] O. Foundation, "Fuzzing," https://www.owasp.org/index.php/Fuzzing, Zugriffsdatum: 28.10.2019.

[177] D. M. D. P. W. K. Gary J Saavedra, Kathryn N Rodhouse, "A Review of Machine Learning Applications in Fuzzing," 2019. [Online]. Available: https://arxiv.org/pdf/1906.11133.pdf

[178] T. O. G. S. T. Chris Evans, Matt Moore, "Fuzzing at scale," https://security.googleblog.com/2011/08/fuzzing-at-scale.html, Zugriffsdatum: 04.11.2019.

[179] H. Böck, "How Heartbleed could've been found," https://blog.hboeck.de/archives/868-How-Heartbleed-couldve-been-found.html, Zugriffsdatum: 30.10.2019.

[180] P. Tech, "Peach Fuzzer," https://www.peach.tech/products/peach-fuzzer/, Zugriffsdatum: 30.10.2019.

[181] P. A. Ryan Sears, Aaron Portnoy, "sulley," https://github.com/OpenRCE/sulley, Zugriffsdatum: 30.10.2019.

[182] R. Swiecki, "honggfuzz," https://github.com/google/honggfuzz, Zugriffsdatum: 30.10.2019.

[183] J. Heistermann, "Genetische Algorithmen: Theorie und Praxis evolutionärer Optimierung," 2013.

[184] B. L. Maik Buttelmann, "Optimierung mit Genetischen Algorithmen und eine Anwendung zur Modellreduktion," 2004. [Online]. Available: https://www.rt.mw.tum.de/fileadmin/w00bhf/www/publikationen/2004_Buttelmann_at.pdf

[185] N. Inc., "Zero-day vulnerability: What it is, and how it works," https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html, Zugriffsdatum: 30.10.2019.

[186] M. R. Fan Long, "Automatic Patch Generation by Learning Correct Code," 2016. [Online]. Available: https://people.csail.mit.edu/fanl/papers/prophet-popl16.pdf

[187] R. H. K. W. C. Dictionary, "resilience," https://www.thefreedictionary.com/resilience, Zugriffsdatum: 23.07.2019.

[188] F. M. S. Danielle Sandler dos Passos, Helder Coelho, "From Resilience to the Design of Antifragility," 2018. [Online]. Available: https://www.thinkmind.org/download.php?articleid=pesaro_2018_2_10_60003

[189] F. Heylighen, "Stigmergy as a Universal Coordination Mechanism: components, varieties and applications," 2015. [Online]. Available: http://pespmc1.vub.ac.be/Papers/Stigmergy-Springer.pdf

[190] M. D. Aiden Dipple, Kerry Raymond, "General Theory of Stigmergy: Modelling Stigma Semantics," 2014.

[191] V. D. Florio, "Antifragility = Elasticity + Resilience + Machine Learning - Models and Algorithms for Open System Fidelity," 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050914006991/pdf?md5=4479b8cb70faca5c332bc328530db1ff&pid=1-s2.0-S1877050914006991-main.pdf

[192] J. M. A. N. A. Steve Carpenter, Brian Walker, "From Metaphor to Measurement: Resilience of What to What?" 2001.

[193] K. J. Hole, "Anti-fragile ICT Systems," 2016.

[194] R. Dahlberg, "Resilience and Complexity: Conjoining the Discourses of Two Contested Concepts," 2015.

[195] B. B. Suniya S. Luthar, Dante Cicchetti, "The Construct of Resilience: A Critical Evaluation and Guidelines for Future Work," 2000.

[196] S. B. T. K. Andreas Karadimas, Elias Hewig, "A Case Study of Black Swans and Antifragility," 2014. [Online]. Available: http://www.adaptivecycle.nl/images/AndreasKaradimasGroupMACaseStudyofBlackSwansandAntifragility.pdf

[197] E. Hollnagel, "Resilience: The challenge of the unstable," 2006.

[198] T. E. B. Cynthia A. Lengnick-Hall, "Adaptive Fit Versus Robust Transformation: How Organizations Respond to Environmental Change," 2005. [Online]. Available: https://doi.org/10.1177/0149206305279367

[199] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," 2014. [Online]. Available: https://doi.org/10.1016/j.ress.2013.06.040

[200] H. Bonn-Rhein-Sieg, "BMBF genehmigt das Projekt SoftSCheck," https://www.h-brs.de/de/pressemitteilung/bmbf-genehmigt-das-projekt-softscheck, Zugriffsdatum: 16.11.2019.

[201] B. Mulvaney, "Strengthening Through the Challenge," 2012. [Online]. Available: https://www.hqmc.marines.mil/Portals/138/Docs/PL/PLU/Mulvaney.pdf