carmasec

security. done. right.

Dossier

Cyber-Resilienz: Ganzheitlicher Ansatz zur Krisenbewältigung in einer dynamischen Welt

Management Summary

Das Konzept der Resilienz hat seinen Ursprung in der Materialforschung, wurde aber seit den 1950er-Jahren von weiteren Disziplinen wie Psychologie, Ökologie und Wirtschaftswissenschaften adaptiert. In jüngster Zeit haben Akteure der Cybersicherheit den Resilienz-Begriff für sich entdeckt. Sie knüpfen dabei an die bereits etablierten Definitionen an, diese sind allerdings nicht vollständig und zeitgemäß. Vor allem wird die Rolle des Menschen als Problemlöser kaum oder gar nicht beachtet. In einem von der International Organization for Standardization (ISO) erstellten Richtlinienheft für organisatorische Resilienz nimmt der Mensch zwar eine herausragende Rolle ein, aber die Cybersicherheit findet dort nur marginal Beachtung.

Die Begriffsbestimmung der Cyber-Resilienz in diesem Dossier rückt Mensch, Prozesse und Technologien als die drei Säulen der Cybersicherheit in den Mittelpunkt. Sie knüpft an die Leitsätze der Agilität an, denn: Der Mensch ist in der Cybersicherheit die wichtigste Ressource, um Cyber-Resilienz anzuwenden. Diese Humanzentrierung, ohne die Ablehnung von Technologien und Prozessen, findet sich in der Agilität wieder.

Das Dossier verfolgt das Ziel, eine für die Unternehmenssteuerung und das IT-Management anwendbare Definition für Cyber-Resilienz zu entwickeln.

Inhalt

ZUM AUTOR

Carsten Marmulla ist Managing Partner der auf Cybersicherheit spezialisierten Beratungsboutique carmasec GmbH & Co. KG mit Hauptsitz in Essen. Als „Trusted Advisor“ ist er seit mehr als 20 Jahren Ansprechpartner für den Themenkomplex Cybersicherheit sowohl für viele mittelständische Unternehmen als auch DAX-Konzerne. Seine Branchenexpertise weist hierbei ein breites Spektrum auf. Er hat bislang Mandate in der Telekommunikation, im Bereich Medien/Entertainment, der chemischen und pharmazeutischen Industrie, in der Gesundheitsbranche, der Logistik und der Finanzdienstleistung wahrgenommen.

Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

Motivation und Aufbau des Dossiers

Unter dem Eindruck von Wirtschafts- und Finanzkrisen, geplatzten Immobilienblasen und Pandemien stehen Unternehmensführungen und -steuerungen vor der Herausforderung, geeignete ganzheitliche Handlungskonzepte zu erproben und zu installieren. Ganzheitlich, weil die eingetretenen Krisen entweder globalen Ausmaßes oder die Folgen der Krisen tiefgreifend sind. Vor diesem Hintergrund findet seit einigen Jahren das Konzept der **Resilienz als Handlungsstrategie** in einer unberechenbaren, mehrdeutigen und komplexen Welt immer mehr Aufmerksamkeit.

Resilienz ist Gegenstand verschiedener Disziplinen, die von der Psychologie über Biologie bis zu Wirtschafts- und Sozialwissenschaften reichen. Herausforderungen an die Cybersicherheit in Bezug auf Krisenbewältigung unterscheiden sich allerdings gravierend von anderen Disziplinen. Die Cybersicherheit stellt eine Basiskompetenz dar, kritische Infrastrukturen sind heute ohne IT-Systeme undenkbar. In Krisen muss Cybersicherheit mit einer anderen Geschwindigkeit agieren, da sich Bedrohungslagen im raschen Wechsel ändern und Angreifer sich immer schneller neue Technologien und Kompetenzen aneignen, um Schwächen in IT-Systemen von Unternehmen sowie kritische Infrastrukturen auszunutzen.

Im ersten Teil des Dossiers werden die Resilienz-Definitionen anderer Disziplinen vorgestellt. Dabei wird ihre generische Entwicklung und die Veränderung des Begriffs im Laufe der Jahrzehnte beschrieben.

Im zweiten Teil werden die bisherigen Definitionen um den organisatorischen Resilienz-Begriff ergänzt. Dieser rückt den Menschen ins Zentrum, während die sonstigen Definitionen Systeme betrachten, in denen der Mensch nur Verursacher oder Opfer einer Krise ist, aber keine gestaltende und bestimmende Instanz darstellt.

Im dritten Teil wird die Definition von Cyber-Resilienz erarbeitet.

Das Dossier verfolgt folgende Nutzenziele: Es möchte ein nachhaltiges, weil praktikables, Verständnis für das Konzept der Resilienz vermitteln und stellt deshalb eine für die Unternehmenssteuerung und das IT-Management anwendbare Definition für Cyber-Resilienz in den Mittelpunkt. Die Handlungsfähigkeit von Unternehmen in krisenhaften Ausnahmesituationen soll verbessert und so erweitert werden, dass aufkommende Probleme vermieden oder zumindest abgemildert werden können.

Ist Resilienz überhaupt wirksam?

Vor der Definition von Resilienz ist es zweckdienlich zu klären, ob sich dahinter ein wirksames Konzept verbirgt oder es sich nur um ein sogenanntes “Buzzword” handelt. Gerade in der Wirtschaftswelt werden Buzzwords viral über soziale Netzwerke verbreitet. Damit soll die Aufmerksamkeit auf ein Thema gelenkt werden, ohne belastbare Inhalte zu bieten. Mitunter sind Buzzwords hilfreich, denn sie vereinfachen komplizierte Sachverhalte, indem sie diese auf ein Wort oder ein Bild reduzieren. Sie erleichtern es den Entscheidern in Unternehmen, den Zugang zu Themen zu finden, die sonst stark erklärungsbedürftig sind. Digitalisierung oder Künstliche Intelligenz sind zwei solcher Beispiele. Anders ist es bei Resilienz. Dieser Begriff ist heute etabliert und hat Eingang in verschiedene wirtschafts-, sozial-, natur-, human- und ingenieurswissenschaftliche Disziplinen gefunden, wie im folgenden Abschnitt aufgezeigt wird. Durch Forschung, beispielsweise am renommierten Leibniz-Institut für Resilienzforschung in Mainz, ist sie eine eigenständige Disziplin geworden.

Ein weiterer wichtiger Aspekt zeigt die Wirksamkeit von Resilienz: Sie ist messbar. Voraussetzung für die Messbarkeit jedes Phänomens ist, dass sie beobachtet werden kann. Vor allem in der Psychologie existieren eine Reihe von Skalen, wie beispielsweise die Connor-Davidson Resilience Scale (CD-RISC) oder die Resilience Scale for Adults (RSA).

Auch für Resilienzbegriffe aus anderen Disziplinen existieren Skalen. Der "SRI-LSE Macroeconomic Resilience Index" ist eine von einem Versicherungsunternehmen aus der Schweiz entwickelte Skala. In der Ökologie wird die Bodenresilienz gemessen. In der Regionenforschung wurde gemessen, wie gut Regionen ökonomische Schocks wie die Wirtschaftskrise aus 2008 überstanden haben.

Die Eingangsfrage, ob Resilienz überhaupt wirksam ist, kann aus den Forschungsergebnissen heraus eindeutig bejaht werden. Allerdings ist vorwegzunehmen, dass in der Cyber-Resilienz eine Messbarkeit bisher nicht existiert. Diesem Umstand entgegnen die Autoren dieses Dossiers mit dem **carmasec-Cybersicherheit Reifegradmodell (CS2RM)**. Seine Stärke ist, dass das Konzept der Resilienz in der Praxis der Cybersicherheit anwendbar ist. So ist die Grundlage für eine quasi-Messbarkeit der Cyber-Resilienz gelegt, da jeder Reifegradstufe bewährte Methoden und Werkzeuge zugewiesen sind.

Was bedeutet Resilienz? - Eine interdisziplinäre Begriffsbestimmung

Resilienz hat spätestens im Zuge der Corona-Pandemie an Bedeutung gewonnen (vgl. Google Trends). Hierunter wird im Allgemeinen die Widerstandskraft von Menschen und Unternehmen bei der Bewältigung von Krisensituationen verstanden. Der Ursprung des Begriffs liegt in der physikalischen Materialforschung. Als resilient werden dabei Materialien bezeichnet, die nach extremer Spannung wieder in den **ursprünglichen Zustand** zurückkehren. Weitere Definitionen bauen auf der lateinischen Wortherkunft resilire auf. Übersetzt bedeutet diese "zurückspringen" oder "abprallen". Ein solcher Zugang zum Thema greift zu kurz, da das Konzept der Resilienz im Fokus verschiedener Disziplinen im Laufe der Jahre weiter entwickelt wurde.

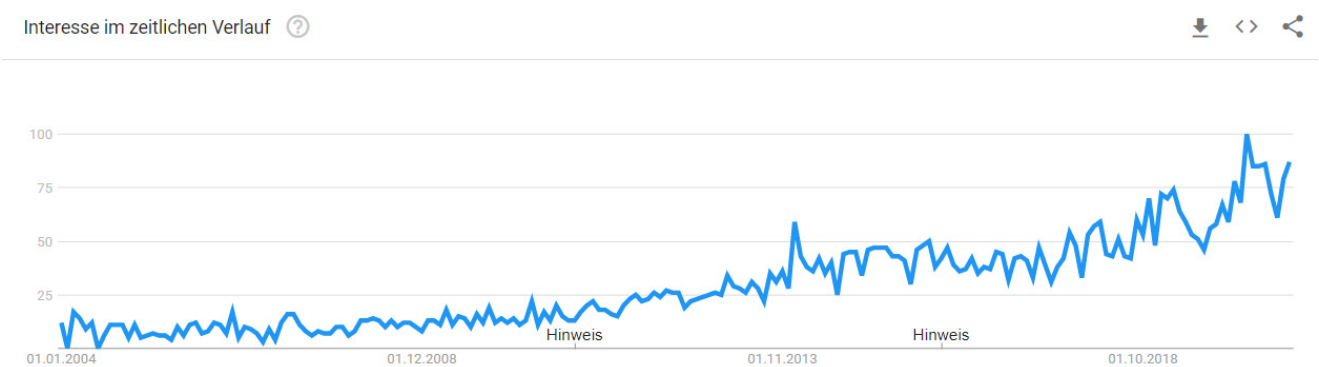
Psychologischer Resilienz-Begriff

Im Zentrum dieser Betrachtung steht das Individuum, das einschneidende Lebensereignisse, Krisen oder Traumata bewältigt muss. Resilienz ist die Fähigkeit, sich von Krisensituationen ohne anhaltende Beeinträchtigungen zu erholen und eine neue Lebensqualität zu erlangen. Nicht die Wiederherstellung eines vorherigen Zustandes steht im Vordergrund, sondern der Erhalt der **Handlungsfähigkeit**.

Ökologischer Resilienz-Begriff

Hier stehen die **Selbstheilungskräfte** eines ökologischen Systems im Vordergrund. In den 1970er-Jahren untersuchten Wissenschaftler in ersten empirischen Studien, ab welcher maximalen Störung ein ökologisches System, wie beispielsweise ein Wald, endgültig destabilisiert wird. Die Untersuchungen wiesen auf, dass sich diese Systeme beispielsweise nach einem Brand oder nach einer Umweltverschmutzung selbst regenerieren können.

An diese Überlegungen schließt auch die aktuelle Klimaforschung an, allerdings mit einem fundamentalen Unterschied: Hier wird davon ausgegangen, dass die



Herausgeber und Urheber:
carmasec GmbH & Co. KG | Ruhrallee 185 | 45136 Essen

Folgen des Klimawandels zu **unumkehrbaren Veränderungen** führen. Dabei wird eine kritische Schwelle ("Tipping Point") angenommen, die zu irreversiblen Folgen führt, wenn sie einmal überschritten wird.

Sozioökonomischer Resilienz-Begriff

Im Mittelpunkt des sozioökonomischen Resilienz-Begriffs stehen kritische Versorgungs- und Infrastrukturen einer Gesellschaft. Fallen sie aus, hat das katastrophale Folgen auf die Stabilität einer Gemeinschaft. Hier wird der bisherige Resilienz-Begriff um drei Aspekte erweitert:

- Ohne Vulnerabilität keine Resilienz. Vulnerabilität kann als Verletzlichkeit übersetzt werden. Sie sagt aus, dass moderne, vernetzte Gesellschaften grundsätzlich anfällig für Störungen und Ausfälle sind. Bedeutet: Das Versagen von Infrastrukturen ist kein außergewöhnliches Ereignis, sondern die Regel, von der immer ausgegangen wird.

- Perspektivwechsel von Problemlösung zur Problemprävention. Prävention nimmt im sozioökonomischen Resilienz-Begriff eine herausragende Rolle ein. Der Anspruch ist nicht mehr, ein aufgetretenes Problem zu lösen, sondern es erst gar nicht entstehen zu lassen.

- Jede Krise verbessert die Resilienzfähigkeit. Da ein Versagen von Versorgungs- und Infrastrukturen nicht komplett ausgeschlossen werden kann, stellt jede Krisensituation einen Testfall dar, um die Resilienz kontinuierlich zu verbessern. Mit dem Ziel, den nächsten Krisenfall idealerweise zu vermeiden, oder aber zumindest seine Folgen zu minimieren.

Ökonomischer Resilienz-Begriff

Aus ökonomischer Sicht wird es nicht als sinnvoll erachtet, wenn beispielsweise Unternehmen nach der Überwindung einer Wirtschaftskrise in ihren Ursprungszustand zurückkehren. Vielmehr sind sie als Marktteilnehmer gefordert, sich an den Wandel und Innovationsdruck anzupassen. Damit ist Transformation ein weiteres konstitutives Merkmal, das auch in der Definition der Cyber-Resilienz beachtet werden muss. Allerdings ist hier anzuführen, dass Resilienz dem ökonomischen Prinzip der effizienten Ressourcenallokation widerspricht. Sie erfordert die redundante Bereitstellung von knappen Ressourcen - für einen Krisenfall, der unter bestimmten Wahrscheinlichkeiten eintritt.

Zwischenfazit: Resilienz ist ein Maß für Überlebensfähigkeit

Die bisherigen Definitionsansätze nehmen eine systemische Perspektive ein, in der das Gleichgewicht eines Systems im Mittelpunkt steht.

Die folgenden Faktoren sind demnach für Resilienz relevant:

- Wiederherstellung des ursprünglichen Zustands
- Selbstheilung / Selbstorganisation
- Prävention
- Transformation

Zusammengenommen kann Resilienz als "ein Maß für die Überlebensfähigkeit" definiert werden. In dieser systemischen Betrachtung nimmt der Mensch allerdings keine zentrale Rolle ein. Daher ist es erforderlich, die bisherigen Begriffsbestimmungen um die organisatorische Resilienz zu ergänzen.

Organisatorischer Resilienz-Begriff

Ein wichtiger Grund, organisatorische Resilienz explizit in die Betrachtung einzubeziehen, ist die Veröffentlichung der **ISO-Norm ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes** durch die International Organization for Standardization (ISO) im Jahr 2017. Diese enthält folgende Richtlinien für Unternehmen, um die organisatorische Resilienz nachhaltig zu installieren:

- Gemeinsame **Vision** und Klarheit über den Unternehmenszweck
- Verständnis und Einflussnahme auf den internen und externen **Kontext**

- Wirkungsvolle und kraftvolle **Führung**
- Schaffung einer **Kultur** zur Unterstützung organisationaler Resilienz
- **Austausch** von Informationen und Wissen
- Bereitstellung von **Ressourcen**
- **Entwicklung und Koordination von Management-Disziplinen**
- Unterstützung der **kontinuierlichen Verbesserung**
- **Fähigkeit zur Antizipation und Umsetzung** von Veränderungen

Die von der ISO aufgestellten Anforderungen an eine resiliente Organisation zeigen auf, dass Resilienz folgendes voraussetzt:

- Fähigkeiten (z.B. Management, qualifiziertes Personal, Kompetenzen, Markt- und Gesellschaftsbeobachtung)
- Ressourcen (z.B. Technologie, Informationen, veränderungsaffine Organisationskultur, Finanzen)
- Strukturen (z.B. kontinuierliches Verbesserungsmanagement, transparente Informationspolitik)

Die ISO-Norm weist **Cybersicherheit, Informationssicherheit und Business Continuity Management als für Resilienz erforderliche Management-Disziplinen** aus.

Cyber-Resilienz - Warum eine eigene Definition wichtig ist

In Anbetracht der vielfältigen Resilienz-Begriffe stellt sich die Frage, ob eine auf Cybersicherheit ausgelegte Resilienz-Definition möglich, ja sogar notwendig ist. Schließlich sind die bestehenden Definitionen bereits sehr weitreichend. Sie bieten daher für die spezifischen Anforderungen der Cybersicherheit an die Resilienz eine breite Anschlussfähigkeit: IT-Systeme sind vulnerabel, wie jede andere Infrastruktur, die Gegenstand des sozioökonomischen Resilienz-Begriffs ist. Allein aufgrund des technologischen Innovationszyklusses ist die Cybersicherheit gefordert, sich einem stetigen Wandel anzupassen. Das Business Continuity Management weist eine große Überschneidung zur “Wiederherstellung des ursprünglichen Zustands“ auf. Bei der “Selbstorganisation“ und “Prävention“ knüpfen Konzepte wie CARTA (Continuous Adaptive Risk and Trust Assessment) von Gartner an. Dabei sollen Angriffe auf IT-Systeme kontinuierlich überwacht, vermieden und automatisch beseitigt werden.

Aus Sicht der Autoren dieses Dossiers gibt es mehrere Gründe, die einen eigenen Resilienz-Begriff für Cybersicherheit erforderlich machen:

1. **VUCA-Welt:** Die Welt ist unsicherer und komplexer geworden. Dies wirkt sich unmittelbar auf die Unternehmensführung und -steuerung aus. Unternehmen müssen ihre Sicherheitslage kontinuierlich bewerten und anpassen. Das setzt eine passende Sicherheitskultur voraus.

2. **Endgültigkeit:** Der Verlust von Daten kann unwiederbringlich sein, während dagegen eine durch Naturkatastrophen zerstörte Infrastruktur wieder aufgebaut und in Betrieb genommen werden kann. Um dies zu vermeiden, ist der Aufwand für die Datensicherheit vielfach höher.

3. **Basistechnologie:** IT-Systeme bilden eine Basistechnologie, ohne welche der Betrieb einer Infrastruktur undenkbar ist. Ihre Verfügbarkeit ist notwendig, damit die Anlagen zuverlässig funktionieren. Nicht zuletzt nimmt die Vernetzung der Infrastrukturen untereinander zu. Damit nimmt die Cybersicherheit eine herausragende Rolle ein.

4. **Geschwindigkeit:** Das Bedrohungsumfeld hat sich dynamisiert und Angriffsvektoren verändern sich in immer kürzeren Zeitabständen. Angreifer und Kriminelle eignen sich schnell neue Technologien und Methoden an, um ihre Ziele zu erreichen. Nicht in Tagen, sondern binnen Sekunden müssen Gefahrenlagen erkannt und abgewehrt werden.

5. **Empowerment:** Nach der oben vorgestellten ISO-Norm stellt der Mensch eine Ressource dar, um Resilienz zu entwickeln, zu praktizieren und zu verbessern. Er ist also nicht nur Verursacher und Opfer von Krisen.

Definition von Cyber-Resilienz nach carmasec

Cybersicherheit benötigt einen eigenen Resilienz-Begriff, da sie eine enge Verknüpfung von Menschen und Technologien voraussetzt. Aus der systemischen Perspektive findet der Mensch kaum oder gar keine Beachtung. In der Definition von ISO wird zwar der Mensch in den Mittelpunkt gerückt, dafür nimmt Cybersicherheit aber eine untergeordnete Rolle ein. Daraus ergibt sich eine Lücke in der Begriffsbestimmung von Cyber-Resilienz, die in Anlehnung an das **Agile Manifest** (Manifest for Agile Software) gefüllt werden kann. Seine vier Leitsätze lauten:

- Individuen und Interaktionen sind wichtiger als Prozesse und Werkzeuge.
- Funktionierende Software ist wichtiger als umfassende Dokumentation.
- Zusammenarbeit mit dem Auftraggeber ist wichtiger als Vertragsverhandlung.
- Reagieren auf Veränderung ist wichtiger als das Befolgen eines Plans.

Diese Leitsätze der Agilität, deren Ursprung in der Software-Entwicklung liegt, demonstrieren, dass in dessen Mittelpunkt der Mensch steht ohne die Technologie zu verdrängen.

Das wechselseitige Zusammenwirken von Technologien, Prozessen und Menschen in einem Unternehmen - als soziotechnisches System - bildet somit das Fundament der Cyber-Resilienz in jedem Unternehmen. Der Mensch ist dabei die wichtigste Ressource, um Störungen zu beheben, Krisen zu bewältigen und Anpassungen vorzunehmen. Jedes Störereignis verbessert die Lernfähigkeit des Unternehmens, nachhaltige Strategien und Handlungsoptionen für die nächste Störung zu entwickeln.

Hieraus ergibt sich für Cyber-Resilienz folgende Definition nach carmasec:

Cyber-Resilienz ist ein systemischer, ganzheitlicher, strategischer und interdisziplinärer Ansatz, um Sicherheitsvorfälle zu vermeiden sowie deren Auswirkungen auf den Geschäftsbetrieb zu minimieren und Werte des Unternehmens zu bewahren.

Maßnahmen der Cyber-Resilienz verfolgen folgende Zielsetzungen für die gesamte Organisation:

Handlungsfähigkeit auch in Krisensituationen zu bewahren

Widerstandsfähigkeit auf Basis eigener Stärken und Ressourcen aufzubauen

Wiederherstellungsfähigkeit zu gewährleisten, um sich von Krisensituationen ohne anhaltende Beeinträchtigungen zu erholen

Dies bedingt die Entwicklung folgender Fähigkeiten innerhalb der Organisation:

Anpassungsfähigkeit an sich wandelnde Bedrohungsszenarien und Umfeldbedingungen

Lernfähigkeit aus Ereignissen und Erarbeitung neuer Handlungsoptionen

Grundprämisse ist die Akzeptanz von permanenten und schnellen Veränderungen der Welt und von Bedrohungsszenarien sowie der Wille zur steten Weiterentwicklung.

Weitere Informationen zur Cyber-Resilienz finden Sie auf unserer Sonderwebsite:
https://www.cyber-resilienz.info

Das carmasec-Reifegradmodell zur Cybersicherheit als Messinstrument in der Cyber-Resilienz

Reifegradmodelle korrespondieren stark mit dem Konzept der Resilienz. Ein Reifegradmodell hilft einem Unternehmen, seine gegenwärtigen Fähigkeiten, Ressourcen und seine vorhandene Infrastruktur zu evaluieren. Dies bietet den Vorteil, über potenzielle Bedrohungslagen und Risiken hinaus die nächsten zielgerichteten Maßnahmen zu planen. Das Resultat: Anpassungsfähigkeit, Widerstandsfähigkeit, Handlungsfähigkeit, Wiederherstellungsfähigkeit und Lernfähigkeit. Alle Fähigkeiten, die auch in den verschiedenen Resilienz-Begriffen enthalten sind.

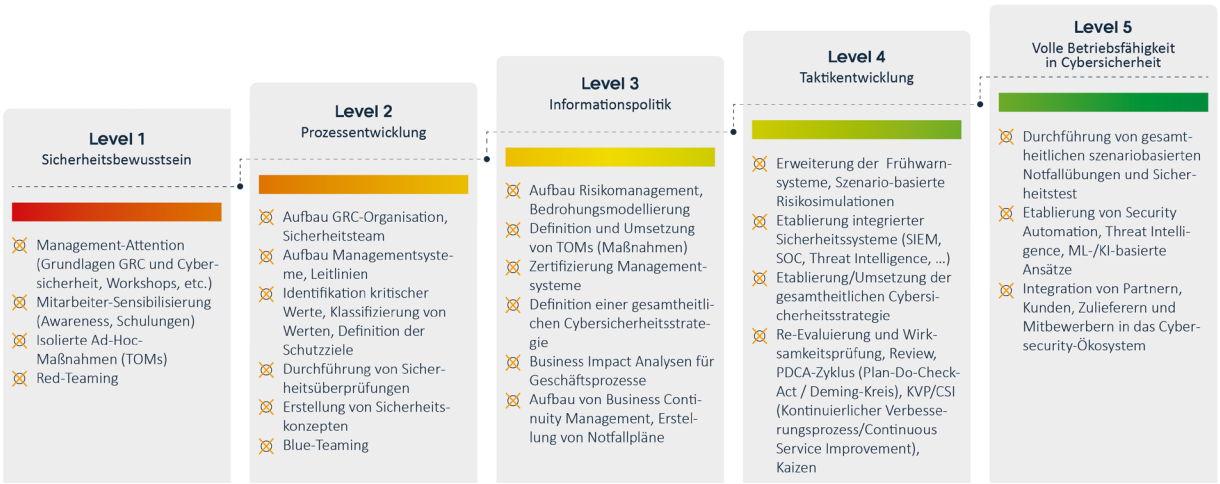
Für die Cybersicherheit haben die Autoren dieses Dossiers mit dem **carmasec-Cybersicherheit Reifegradmodell (CS2RM)** ein auf die Cybersicherheit zugeschnittenes Reifegradmodell entwickelt. Entsprechend der hier vorgelegten Definition von Cyber-Resilienz steht auch beim CS2RM der Mensch im Mittelpunkt.

- Am Anfang steht ein Assessment-Prozess, dann werden jeder Reifegradstufe bewährte Instrumente und Methoden zugewiesen (siehe Infografik zu CS2RM).
- Nach der Auditierung der gegenwärtigen Cybersicherheit (Architektur, Richtlinien, Kultur, Technologien usw.) erfolgt eine Standortbestimmung im Reifegradmodell. Sie stellt dabei eine Art Blaupause dar, mit der Handlungs- und Optimierungsbedarfe sichtbar gemacht werden.
- Auf dieser Grundlage werden ein Maßnahmenkatalog und ein Fahrplan entworfen, welche durch eine Investitions- und Budgetplanung ergänzt werden.
- Durch Monitoring und Evaluation der Maßnahmen wird der Fortschritt kontinuierlich bewertet und geprüft.
- Sind die Anforderungen der Reifegradstufe erfüllt, wird ferner entschieden, ob die nächste Reifegradstufe angestrebt werden soll.

Ein Unternehmen, das den CS2RM anwendet, kann zielgerichtete Handlungsmaßnahmen definieren, Budgets zuweisen, den Fortschritt kontinuierlich überwachen und entsprechend der Geschäftsstrategie einen sinnvollen Zeitplan festlegen, um die nächste Reifegradstufe anzustreben.

Zusammenfassend kann angeführt werden, dass Cybersicherheit einen eigenen Resilienz-Begriff benötigt. Das wechselseitige Zusammenwirken von Technologien, Prozessen und Menschen in einem Unternehmen findet in den übrigen Resilienz-Definitionen nicht genügend Beachtung. Die hier vorgestellte Definition von Cyber-Resilienz führt Menschen, Prozesse und Technologien zusammen.

Das carmasec-Cybersicherheit Reifegradmodell operationalisiert die Cyber-Resilienz, so dass sie in der Unternehmenssteuerung und im IT-Management angewendet werden kann.



carmasec
security. done. right.

ÜBER CARMASEC

carmasec ist eine im Jahr 2018 in Deutschland gegründete Beratungsboutique im Themenfeld Cybersicherheit und Datenschutz. Als „Trusted Advisor“ bieten wir unseren nationalen und internationalen Kunden professionelle Beratungsleistungen und Lösungen in den Bereichen DevSecOps, Secure SDLC, Automatisierung von Informationssicherheitsmanagement sowie IT-GRC (Governance, Risk, Compliance).

Unser fachkundiges Expertenteam verfügt über langjährige einschlägige Beratungserfahrung, mit der wir bereits über 100 Kundenprojekte in den Branchen Telekommunikation, Logistik, Finanzdienstleistungen, Gesundheitswesen und Energie erfolgreich umgesetzt haben.

UNSERE STANDORTE

Standort Essen

carmasec GmbH & Co. KG
Ruhrallee 185
45136 Essen

Standort Köln

carmasec GmbH & Co. KG
Im Mediapark 5
50670 Köln