carmasec

security. done. right.

Whitepaper 09/2020

Reifegradmodelle für die Cybersicherheit Ihres Unternehmens:

Referenzrahmen für Handlungs-, Planungs- und Budgetsicherheit

Über das Whitepaper

Cybersicherheit ist eine der wichtigsten ständigen Herausforderungen für Unternehmen. Es stellt sich die Frage, ob die eingesetzten Maßnahmen immer zielführend sind. Auch können Erfolg und betriebswirtschaftliche Rendite dieser Maßnahmen nicht gemessen werden. Es fehlt ein Referenzrahmen, der den Entscheidern transparent und begründet darlegt, in welcher Ausgangssituation sich die Cybersicherheit befindet, um das Unternehmen vor Risiken und Gefahren zu schützen.

Solche Referenzrahmen stellen Reifegradmodelle dar. Ein Reifegrad ist ein Maß für Unternehmen zur kontinuierlichen Verbesserung in einer spezifischen Disziplin. Er trägt zur Standortbestimmung des Unternehmens bei und zeigt dessen Handlungsoptionen auf. Reifegradmodelle gewinnen in der Unternehmensführung und -steuerung zunehmend an Bedeutung, weil sie Mess-, Prüf- und Vergleichbarkeit zulassen.

Obwohl sie auch in der Softwareentwicklung existieren, gibt es bisher kein Reifegradmodell für Cybersicherheit. Dies gilt im besonderen für Deutschland, denn im angelsächsischen Raum werden solche Ansätze beispielsweise mit dem Cybersecurity Maturity Model (CMM) bereits eingesetzt. Doch diese können nicht zwangsläufig auf deutsche Unternehmen übertragen werden. Sie erfordern eine kritische Überprüfung.

In diesem Whitepaper diskutieren wir ausgewählte Reifegradmodelle für die Cybersicherheit und stellen ein eigenes Reifegradmodell vor, das in deutschen Unternehmen angewendet werden kann. Details des carmasec-Cybersicherheits Reifegradmodells (CS2RM) werden in einer Infografik veranschaulicht. Es baut auf dem Community Cyber Security Mature Model (CCCMM) auf.

Inhalt

Warum Reifegradmodelle wichtig sind	Seite 3
Vorteile von Reifegradmodellen	Seite 4
Welche Vorteile für Cybersicherheit existieren?	Seite 4
CCSMM - ideal für deutsche Unternehmen?	Seite 5
Fazit	Seite 8

ZUM AUTOR

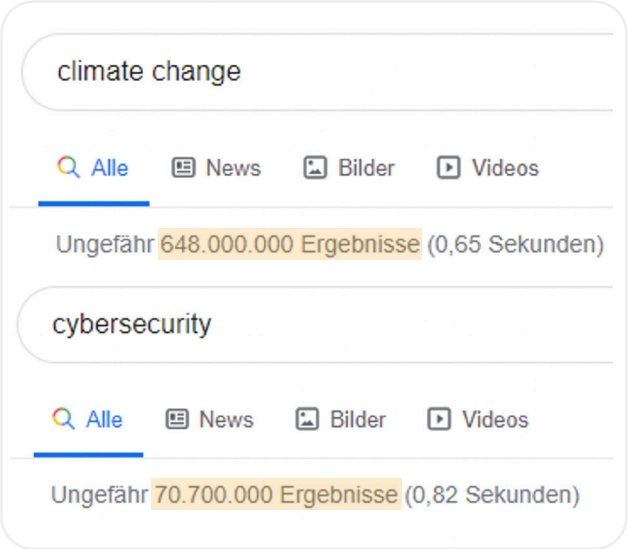
Carsten Marmulla ist Managing Partner der auf Cybersicherheit spezialisierten Beratungsboutique carmasec GmbH & Co. KG mit Hauptsitz in Essen. Als „Trusted Advisor“ ist er seit mehr als 20 Jahren Ansprechpartner für den Themenkomplex Cybersicherheit sowohl für viele mittelständische Unternehmen als auch 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

Warum Reifegradmodelle wichtig sind

Laut der Allianz-Studie "Risikobarometer" aus 2019 gehörte die Cybersicherheit bereits vor der Corona-Krise zu den wichtigsten Herausforderungen für Unternehmen. Cyberattacken lagen in der Risikobewertung des Versicherers auf Platz eins der möglichen Bedrohungen. Dicht gefolgt von Gefahren durch Betriebsunterbrechungen wegen rechtlicher Veränderungen wie Handelskonflikten, Zöllen, Sanktionen oder des Brexit. Der Klimawandel hingegen, der in der Öffentlichkeit spätestens durch die "Fridays For Future"-Bewegung eine globale Öffentlichkeit mobilisierte, belegte in der Studie nur den siebten Platz.

Dieser Vergleich zeigt im Umgang mit der Dringlichkeit von Zukunftsaufgaben einen interessanten Aspekt: würden die Ergebnisse einer Internet-Suche als Maßstab für Bedrohungen herangezogen werden, dann müsste auf Platz eins der Klimawandel und erst in den hinteren Rängen Cybersicherheit liegen. Unbestritten gehört der Klimawandel zu den wichtigsten Zukunftsaufgaben. Dieses Beispiel führt allerdings vor, dass vor allem angstgetriebene Zukunftsthemen eine hohe Aufmerksamkeit erzeugen. Die Risikobewertung der Allianz-Studie zeigt aber, dass solche Themen immer einer sachlichen Prüfung unterzogen werden müssen. Nach dem Motto: wo Rauch zu sehen ist, muss nicht immer Feuer sein.



Auch Medienartikel über Cybersicherheit sind häufig angstgetrieben und unterstellen mittelständischen Unternehmen generell, die Bedrohung durch Cyberangriffe zu unterschätzen. Sie treffen pauschale Aussagen über alle Unternehmen und sind damit oftmals wenig konstruktiv. Sie gehen nicht differenziert darauf ein, wo ein Unternehmen in Bezug auf Cybersicherheit aktuell steht, über welche Ressourcen es verfügt oder welche Maßnahmen naheliegend sind, um seine Fähigkeit in der Cybersicherheit schrittweise zu steigern. Sie erzeugen damit überflüssigerweise zusätzlichen Druck auf Unternehmen, der ohnehin bereits vorhanden ist. Tatsächlich benötigen Unternehmen fassbare Instrumente und Methoden der langfristigen Planung, die iterativ und berechenbar umgesetzt werden können. Dafür ist die Aneignung von spezifischen Fähigkeiten erforderlich:

- **Anpassungsfähigkeit** des IT-Managements und der betrieblichen Infrastruktur, um kommenden Bedrohungsszenarien wie Pandemien, Naturkatastrophen, politischen Konflikten usw. so zu begegnen, dass der Geschäftsbetrieb aufrecht erhalten werden kann;

- **Widerstandsfähigkeit** durch Entwicklung eines Maßnahmenplans, um schnell und angemessen zu reagieren, wenn Bedrohungssituationen eintreten;

- **Handlungsfähigkeit** des IT-Managements und der IT-Infrastruktur, um komplexen Bedrohungsszenarien proaktiv zu begegnen und Risiken zu minimieren;

- **Wiederherstellungsfähigkeit** des Geschäftsbetriebs mithilfe von Notfallplänen und eines wirksamen Disaster Recovery Managements;

- **Lernfähigkeit**, um die Erfahrungsbasis des Managements im Umgang mit Krisen sowie die Prozesse zur Abwehr von Bedrohungsszenarien und Wiederherstellung des Geschäftsbetriebs kontinuierlich auszubauen.

Vorteile von Reifegradmodellen

Eigentlich postulieren diese Ausführungen die **Cyber-Resilienz**. Diese ist allerdings keine Methode, sondern fasst einen Katalog von Aspekten, Methoden und Instrumenten ganzheitlich zusammen. Diese Methoden und Instrumente sind nicht a priori festgelegt, sondern müssen je nach Ausstattung des Unternehmens, der Erfahrungsbasis des Managements, der vorliegenden Marktsituation und den strategischen Zielen des Unternehmens individuell zusammengestellt werden. Vor diesem Hintergrund ist das Cybersecurity Maturity Model (CMM) von besonderem Wert. Das Reifegradmodell hilft einem Unternehmen, seine gegenwärtigen Fähigkeiten, Ressourcen und seine vorhandene Infrastruktur zu evaluieren. So weiß es anschließend, auf welcher Stufe des Reifegrades es aktuell steht und kann auf dieser Grundlage einen Maßnahmenplan entwickeln, um die nächste Stufe des Reifegradmodells zu erreichen. Damit ist eine Reihe von Vorteilen verbunden: Das Unternehmen weiß, welche Aufgaben als nächstes anstehen und kann seine Ressourcen und die Investitionsbedarfe entsprechend planen. Das Cybersecurity Maturity Model hilft bei der Sicherstellung der Produktivität und Qualität des Unternehmens sowie der Einhaltung der Budget- und Zeitplanungen.

Welche Reifegradmodelle für Cybersicherheit existieren?

Der Ursprung der Cybersecurity Management Modelle liegt im amerikanischen Verteidigungsministerium: Das Pentagon kündigte im Mai 2019 an, dass Lieferantenbetriebe und Dienstleister des Department of Defense für die Beteiligung an Ausschreibungen die Qualifizierung ihrer Cybersicherheit dokumentieren und nachweisen müssen. Hierfür setzte das Ministerium das Zertifizierungs- und Auditierungsprogramm "Cybersecurity Maturity Model Certification (CMMC)" auf. Damit wurde das Ziel verbunden, diese Unternehmen einer Risikoqualifizierung zu unterziehen und sie gleichzeitig in der Weiterentwicklung ihrer Cybersicherheit zu fördern. Je höher der Reifegrad der Cybersicherheit, den ein Unternehmen erreicht, umso höher die Chance, an Ausschreibungen teilzunehmen. Das Verteidigungsministerium hat insgesamt fünf Reifegradstufen unterschieden:

- Level 1: Basic Cyber Hygiene
- Level 2: Intermediate Cyber Hygiene
- Level 3: Good Cyber Hygiene
- Level 4: Proactive
- Level 5: Advanced/Progressive

Diese Unterteilung der Reifegradstufen ist vor dem Hintergrund der zuvor vorgestellten Cyber-Resilienz und der Definition von Reifegraden wenig hilfreich. Das CMMC des amerikanischen Verteidigungsministeriums zielt auf einen spezifischen Zweck, um in erster Linie eigene Interessen sicherzustellen. Die schrittweise Verbesserung der Cybersicherheit der Unternehmen hat eine nachgelagerte Priorität. Es ist zweifelhaft, ob diese von einer ausländischen Behörde aufgestellten Stufen so auf ein Unternehmen in Deutschland übertragen werden können.

SIND REIFEGRADMODELLE WIRKSAM?

Obwohl Reifegradmodelle in unterschiedlichen Funktionsbereichen von Unternehmen eingesetzt werden, gibt es nur wenige wissenschaftliche Untersuchungen hinsichtlich ihrer Wirksamkeit. In einer fundierten Studie von Wissenschaftlerinnen und Wissenschaftlern aus Großbritannien und Italien, "Value of maturity models in performance measurement", fassen Ümit S. Bititcia, Patrizia Garengob, Aylin Atescand und Sai S. Nudurupat ihre Untersuchung zur Wirksamkeit in zwölf Fertigungsbetrieben zusammen. Sie gelangen zu der Erkenntnis, dass organisatorisches Lernen und die Managementfähigkeiten durch Planung, Einführung und Evaluation mithilfe von Reifegradmodellen verbessert werden.

Quelle: Umit S. Bititci, Patrizia Garengo, Aylin Ates & Sai S. Nudurupati (2015) Value of maturity models in performance measurement, International Journal of Production Research

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

Auch das amerikanische Energieministerium hat mit dem Cybersecurity Capability Maturity Model (C2M2) einen etablierten Ansatz entwickelt. Dieser baut auf dem Cybersecurity Framework des National Institute of Standard and Technology (NIST CSF) auf. NIST selbst legt großen Wert darauf, dass das entwickelte Framework in unterschiedlichen Bereichen zum Einsatz kommt. Außerdem wird es in einigen Ländern wie Japan, Israel, Italien oder Großbritannien genutzt. Beide Modelle unterscheiden folgende fünf Reifegradstufen:

- Level 1: Identifizieren
- Level 2: Schützen
- Level 3: Erkennen
- Level 4: Reagieren
- Level 5: Genesen

CCSMM - ideal für deutsche Unternehmen?

Eine dritte Variante, das "Community Cyber Security Maturity Model" (CCSMM) ist für uns interessant. Im Mittelpunkt dieses Ansatzes steht die lokale Gemeinschaft (Community). Sie besteht neben Einzelpersonen aus einer Verwaltung, Zivilgesellschaft und Wirtschaftsbetrieben. Das Modell rückt Menschen stärker in den Mittelpunkt als die anderen Varianten. Dies zeigen die Reifegradstufen, die unten vorgestellt sind. Vor dem Hintergrund, dass der Mensch den wichtigsten Angriffsvektor für Cyberkriminelle darstellt, gewinnt dieser Ansatz zusätzlich an Bedeutung. Für die Messbarkeit zur qualitativen und quantitativen Standortbestimmung eines Unternehmens bietet CCSMM eine Vielzahl an Messgrößen. Diese Metriken beziehen sich allerdings auf die Gesamtheit einer Gemeinschaft. Unternehmen sind davon nur eine Teilmenge. Dies macht eine spezifische Ausarbeitung der Metriken, die die Unternehmen in den Fokus der Betrachtung rückt, erforderlich.

Dieses Reifegradmodell unterscheidet folgende fünf Stufen:

- **Level 1: Security Awareness**
  (Sicherheitsbewusstsein): In dieser Stufe gilt es insbesondere bei den Organisationsmitgliedern ein hohes Maß an Bewusstsein für Cybersicherheit zu fördern.

- **Level 2: Process Development**
  (Prozessentwicklung): In dieser Stufe stehen die Prozesse und Richtlinien im Vordergrund. Diese gewährleisten, dass Cybersicherheit im Betrieb funktioniert.

- **Level 3: Information Enabled**
  (Informationspolitik): Voraussetzung für diese Stufe ist, dass die Organisationsmitglieder das erforderliche Sicherheitsbewusstsein besitzen und in der Organisation entsprechende Prozesse existieren, damit Informationen wirksam fließen können, um Bedrohungen zügig zu erkennen und zu beseitigen.

- **Level 4: Tactics Development**
  (Taktikentwicklung): In dieser Stufe verfügt das Unternehmen bereits über die Fähigkeit (und die dazugehörigen Pläne), um Bedrohungsszenarien proaktiv zu erkennen und zu beseitigen. Prävention spielt an diesem Punkt eine wichtige Rolle.

- **Level 5: Full Security Operational Capability**
  (Volle Betriebsfähigkeit in Cybersicherheit): In dieser Reifegradstufe erfüllt das Unternehmen nicht nur alle zuvor genannten Voraussetzungen. Zusätzlich wirken die Prozesse und Mechanismen durchgehend im gesamten Unternehmen. Darüber hinaus kann es sich mit anderen relevanten Unternehmen und Institutionen vernetzen, um auf ein komplexes Bedrohungsszenario zu reagieren.

Übersicht ausgewählter Reifegradmodelle im Vergleich

Bedrohungslage	**unstrukturiert**		**strukturiert**		**hochgradig- strukturiert**
Reifegradstufe CMMC C2M2	**Level 1** Basic Cyber Hygiene Identifizieren	**Level 2** Intermediate Cyber Hygiene Schützen	**Level 3** Good Cyber Hygiene Erkennen	**Level 4** Proactive Reagieren	**Level 5** Advanced/Progressive Genesen
CCSMM	Sicherheitsbewusstsein *(Security Awareness)*	Prozessentwicklung *(Process Development)*	Informationspolitik *(Information Enabled)*	Taktikentwicklung *(Tactics Development)*	Volle Betriebsfähigkeit in Cybersicherheit *(Full Security Operational Capability)*
Beschreibung	In dieser Stufe gilt es insbesondere bei Organisationsmitgliedern ein hohes Maß an Bewusstsein für Anliegen der Cybersicherheit zu fördern.	In dieser Stufe stehen die Prozesse und Richtlinien im Vordergrund. Diese gewährleisten, dass Cybersicherheit im Betrieb funktioniert.	Voraussetzung für diese Stufe ist, dass die Organisationsmitglieder über das erforderliche Sicherheitsbewusstsein verfügen und in der Organisation entsprechende Prozesse existieren, damit Informationen wirksam fließen können, um zügig Bedrohungen zu erkennen und zu beseitigen.	In dieser Stufe verfügt das Unternehmen bereits über die Fähigkeit (und Pläne), um Bedrohungsszenarien proaktiv zu erkennen und zu beseitigen. Prävention spielt an diesem Punkt eine wichtige Rolle.	In dieser Reifegradstufe erfüllt das Unternehmen nicht nur alle zuvor genannten Voraussetzungen. Die Prozesse und Mechanismen wirken im gesamten Unternehmen durchgehend. Darüber hinaus kann es sich mit relevanten Unternehmen und Institutionen vernetzen, um auf ein komplexes Bedrohungsszenario zu reagieren.

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

Attraktiv an diesem Reifegradmodell ist, dass zwischen unterschiedlichen Bedrohungssituationen unterschieden wird:

- **Unstrukturierte Bedrohungen:** Sie sind am häufigsten. Die Kriminellen verfolgen dabei kurzfristige Effekte, ohne die gesamte Betriebsfähigkeit gefährden zu wollen. Typische Angriffe sind beispielsweise CEO Frauds, um die schnelle Überweisung von Geldern zu erwirken.

- **Strukturierte Bedrohungen:** Hinter den Angriffen steckt oft eine organisierte Gruppe. Denn diese sind geplant und die Verantwortlichen gehen methodisch vor. Ihr Ziel ist nicht, sich zu bereichern, sondern an sensible Informationen zu gelangen oder die Betriebsfähigkeit zu beeinträchtigen. Neben Kriminellen gehören zur Tätergruppe auch (politische) Aktivisten, so genannte "Hacktivisten".

- **Hochgradig organisierte Bedrohungen:** Angriffe auf diesem Niveau haben das Ziel, die Betriebsfähigkeit zu beeinträchtigen. Zu den Zielen der Angreifer zählt nicht nur die Informationsgewinnung, sondern auch die Vernichtung von Informationen. Die Gruppe ist in der Regel hochgradig organisiert, verfügt über ein großzügiges Budget und greift auf multidisziplinäre Kompetenzen zurück. Die Angriffe finden oft in Kombination mit physischen und psychischen Bedrohungen statt.

Damit wird deutlich, dass nicht jedes Unternehmen die höchste Reifegradstufe erreichen muss, um vor Bedrohungen geschützt zu sein. Die angestrebte Reifegradstufe wird vielmehr von der Bedrohungssituation bestimmt. Diese Betrachtung hilft, Ressourcen und Investitionen optimal einzusetzen. Das bedeutet aber auch: strebt ein Unternehmen Wachstum an, geht dies einher mit Änderungen der Wertschöpfungskette, des Geschäftsmodells und der Märkte, wodurch sich die Bedrohungslage verändert. Mit Hilfe des Cybersecurity Maturity Models kann das Unternehmen Ressourcen und Finanzmittel für die geeignete Reifegradstudie der Cybersicherheit vorausplanen.

Fazit

Reifegradmodelle gewinnen in Deutschland zunehmend an Bedeutung und kommen im Marketing, der Digitalisierung, der Softwareentwicklung, der Logistik oder im Projektmanagement vermehrt zum Einsatz. In der Cybersicherheit stellen sie einen sehr jungen Ansatz dar. Im angelsächsischen Raum existiert sowohl Anwendungswissen als auch Erfahrung, das für deutsche Unternehmen nützlich ist, aber nicht unkritisch übernommen werden sollte. Daher wurden bestehende Reifegradmodelle miteinander verglichen und mit dem Ziel bewertet, einen für deutsche Unternehmen anwendbaren Ansatz zu entwickeln. Das zu diesem Zweck von *carmasec* entworfene Cybersicherheit-Reifegradmodell (CS2RM) baut auf dem Community Cyber Security Maturity Model (CCSMM) auf. Die wichtigste Herausforderung für das CS2RM bestand darin, CCSMM auf die spezifische Situation von Unternehmen auszurichten. Wie in den Ausführungen oben dargelegt, bezieht sich die Messbarkeit des Modells auf eine ganze Gemeinschaft (Community). Für seine Anwendbarkeit sieht CS2RM einen Assessment-Prozess vor, in dem ein Unternehmen zum Beginn auditiert wird. Die Infografik veranschaulicht die Details des Modells.

Durch Zuweisung bewährter Instrumente und Methoden zu jeder Reifegradstufe, ist der carmasec-Ansatz operabel und anwendungsfreundlich: 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, das ist abhängig von der Geschäftsstrategie.

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

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 dann die nächste Reifegradstufe anzustreben.

carmasec Cyber Security Maturity Modell

Das carmasec Cyber Security Maturity Model (CS2RM) baut auf dem Community Cyber Security Maturity Model (CCSMM) auf, das im Gegensatz zu anderen Reifegradmodellen den Menschen stärker in den Mittelpunkt rückt. Das carmasec Cyber Security Maturity Model ergänzt das CCSMM um etablierte und bewährte Methoden, so dass gezielt die Reifegradstufe bestimmt und zügig adäquate Maßnahmen eingeleitet werden können.

Level 1
Sicherheitsbewusstsein

- Management-Attention (Grundlagen GRC und Cybersicherheit, Workshops, etc.)
- Mitarbeiter-Sensibilisierung (Awareness, Schulungen)
- Isolierte Ad-Hoc-Maßnahmen (TOMs)
- Red-Teaming

Level 2
Prozessentwicklung

- Aufbau GRC-Organisation, Sicherheitsteam
- Aufbau Managementsysteme, Leitlinien
- Identifikation kritischer Werte, Klassifizierung von Werten, Definition der Schutzziele
- Durchführung von Sicherheitsüberprüfungen
- Erstellung von Sicherheitskonzepten
- Blue-Teaming

Level 3
Informationspolitik

- Aufbau Risikomanagement, Bedrohungsmodellierung
- Definition und Umsetzung von TOMs (Maßnahmen)
- Zertifizierung Managementsysteme
- Definition einer gesamtheitlichen Cybersicherheitsstrategie
- Business Impact Analysen für Geschäftsprozesse
- Aufbau von Business Continuity Management, Erstellung von Notfallpläne

Level 4
Taktikentwicklung

- Erweiterung der Frühwarnsysteme, Szenario-basierte Risikosimulationen
- Etablierung integrierter Sicherheitssysteme (SIEM, SOC, Threat Intelligence, …)
- Etablierung/Umsetzung der gesamtheitlichen Cybersicherheitsstrategie
- Re-Evaluierung und Wirksamkeitsprüfung, Review, PDCA-Zyklus (Plan-Do-Check-Act / Deming-Kreis), KVP/CSI (Kontinuierlicher Verbesserungsprozess/Continuous Service Improvement), Kaizen

Level 5
Volle Betriebsfähigkeit in Cybersicherheit

- Durchführung von gesamtheitlichen szenariobasierten Notfallübungen und Sicherheitstest
- Etablierung von Security Automation, Threat Intelligence, ML-/KI-basierte Ansätze
- Integration von Partnern, Kunden, Zulieferern und Mitbewerbern in das Cybersecurity-Ökosystem

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

carmasec

SO UNTERSTÜTZEN WIR SIE BEI DER STEIGERUNG IHRES REIFEGRADS

IT-Governance, -Risk & -Compliance

Damit Sie wissen, wo Sie stehen

Wir ermitteln, ob der Reifegrad Ihres Unternehmens zur aktuellen Bedrohungslage passt und erstellen einen validen Fahrplan für Ihre IT-Sicherheit.

Dabei messen und bewerten wir die Reifegradstufe für Ihre Transparenz.

Security Projektmanagement

Damit Sie Ihre Möglichkeiten kennen

Wir erstellen einen Maßnahmenplan, damit Sie die nächste Reifegradstufe konsequent erreichen, einschließlich Budgetsteuerung.

Dabei informieren wir Sie über den Stand der Maßnahmen Projekt on-Track.

Technische Security

Damit Sie die nächste Reifegradstufe erreichen

Wir setzen die geplanten und von Ihnen freigegebenen technischen Maßnahmen zügig, zuverlässig und fachgerecht um.

Dabei erhöhen wir den Reifegrad der Cybersicherheit in Ihrem Unternehmen.

SIE HABEN FRAGEN? SPRECHEN SIE UNS AN

Carsten Marmulla
Managing Partner & Senior Trusted Advisor

Schwerpunkt: IT-GRC

Jan Sudmeyer
Managing Partner & Senior Trusted Advisor

Schwerpunkt: Security Projektmanagement

Timm Börgers
Managing Partner & Senior Trusted Advisor

Schwerpunkt: Technische Security

UNSERE KONTAKTDATEN

www.carmasec.com
contact@carmasec.com
+49 (0) 201 426 385 900
xing.carmasec.com
twitter.carmasec.com
linkedin.carmasec.com

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

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