carmasec

security. done. right.

Pragmatische Reifegrad-Messung der Cyber-Resilienz in Ihrer Unternehmens-IT

16.06.2021, Carsten Marmulla
IT-Trends Digital & Sicher (networker NRW)

Agenda

carmasec

- Vorstellung Referent
- Status Quo:
  - Cyber-Bedrohungslage in der Pandemie, Exkurs: VUCA-Welt, Sonstige Herausforderungen
- Cyber-Resilienz
  - Definition, Grundprämissen
- Reifegradmodelle
  - Sinn & Zweck, Übersicht & Einordnung
- Reifegradmodelle zur Cybersicherheit
- Fazit

Vorstellung Carsten Marmulla

Carsten Marmulla
Managing Partner &
Senior Trusted Advisor

c.marmulla@carmasec.com
www.carmasec.com

Herr Marmulla ist ein erfahrener Managementberater mit den langjähriger Berufs- und Projekterfahrung in den Themenschwerpunkten Informationssicherheits-, und IT-Risikomanagement, IT-Compliance (u.a. Datenschutz), IT-Sicherheit und IT-Governance.

Er zeichnet sich durch sein exzellentes, aktuelles und praxiserprobtes Fachwissen sowie seine strukturierte und analytische Denk- sowie seine eigenständige Arbeitsweise aus.

Diese Fähigkeiten hat er in zahlreichen Projekten mit unterschiedlichen Aufgabenstellungen erfolgreich einsetzen können. Er übernimmt sowohl strategische, konzeptionelle sowie implementierende Aufgaben als auch Projektleitungs- und Ergebnisverantwortung.

Er ist als interner Auditor für ISO 27001, als ISIS12-Berater sowie gemäß der Standards ITIL v3, COBIT 4.1 und PRINCE2 zertifiziert.

Skills und Themenschwerpunkte:

- 20 Jahre IT-Branchenerfahrung (Projektmanagement- und IT-Beratungserfahrung)
- Informationssicherheitsmanagement (ISO 27001, BSI IT-Grundschutz), IT-Service-management gemäß ITIL v3
- IT-GRC: IT-Governance, IT-Risikomanagement, IT-Compliance (inkl. Datenschutz)
- Zertifizierungen: Certified Information Security Manager (CISM), ITIL v3, ISO 27001 Auditor (ISMS), ISIS12, COBIT-Practitioner, PRINCE2-Practitioner

Projekterfahrung (Auszug):

- Erstellung von Sicherheitskonzepten; Informationssicherheitsrichtlinien, Schutzbedarfsfeststellungen; Festlegung, Einführung und Kontrolle der Sicherheitspolitik und Sicherheitsstrategie
- Organisatorische Reifegradermittlung; Durchführung von Schwachstellen-/ Risiko- und Business Impact Analysen (BIA); Identifizierung und Steuerung der Maßnahmen
- Konzeption, Aufbau und Einführung von Managementsystemen für Informationssicherheit gemäß ISO 27001 und Zertifizierungsvorbereitung; Konzeption und Implementierung von Kennzahlensystemen (KPI)
- Optimierung der IT-Wertschöpfung im Rahmen der IT-Governance (COBIT); Überprüfung der Einhaltung der IT-Compliance und der Datenschutzanforderungen

Referenzkunden (Auszug):

- Deutsche Post AG
- Postbank Systems AG
- Vodafone Group Services GmbH
- Deutsche Telekom AG
- Fresenius Netcare GmbH
- Uniper IT GmbH

Vorstellung carmasec GmbH & Co. KG

Gegründet im Jahr 2018 mit umfassender Expertise aus **über 30 Jahren einschlägiger Beratererfahrung** und **über 100 erfolgreichen Projekt-abschlüssen**.

Leistungsbereiche:
Managementberatung, **Projektmanagement**, **Technologieberatung** in den Themenfeldern Cybersicherheit, Cyber-Resilienz & IT-GRC

Standorte:
Essen und **Köln**, deutschlandweite Projekteinsätze

Branchenkenntnisse (Auszug):
Telekommunikation, Logistik/Transport. Finanzdienst-leistungen, Energieversorgung. Gesundheitswesen, Informationstechnologie, u.a.

„There are only two types of companies:
those, that have been hacked,
and those, who don’t know,
they have been hacked.“

John T. Chambers

Cyber-Bedrohungslage in der Pandemie

carmasec

Sicherheitsrisiko Home-Office / Telearbeit:

- Fehlende Sensibilisierung/Awareness, Social Engineering
- Phishing-Attacken, CEO-Fraud, Chefbetrug
- Malware, Ransomware (bspw. Emotet)
- Mangelhafter Perimeterschutz (Clients)
- Datenleaks & Datenschutzverstöße
- Kritische Sicherheitslücken in Softwareprodukten
- DDoS-Attacken

Vgl. Lagebericht IT-Sicherheit in Deutschland des BSI,
https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

Exkurs: VUCA

VUCA ist ein Akronym für die englischen Begriffe

- *volatility* ‚Volatilität' (Unbeständigkeit),
- *uncertainty* ‚Unsicherheit',
- *complexity* ‚Komplexität' und
- *ambiguity* ‚Uneindeutigkeit'.

Es beschreibt schwierige Rahmenbedingungen der Unternehmensführung. Der Begriff entstand in den 1990er Jahren am *United States Army War College* (USAWC) und diente zunächst dazu, die multilaterale Welt nach dem Ende des Kalten Krieges zu beschreiben. Später breitete der Begriff sich auch in andere Bereiche strategischer Führung und auf andere Arten von Organisationen aus, vom Bildungsbereich bis in die Wirtschaft.

Exkurs: VUCA

carmasec

VOLATILITY

Volatilität. Flüchtigkeit. Wir leben in einer Welt, die sich ständig verändert, instabiler wird und in der kleine oder gravierende Veränderungen unvorhersehbarer werden – und zwar immer drastischer und immer schneller. Ereignisse verlaufen völlig unerwartet und Verstehen von Ursache und Wirkung wird mitunter unmöglich.

Exkurs: VUCA

carmasec

UNCERTAINTY

Ungewissheit. Unsicherheit. Vorhersehbarkeit und Berechenbarkeit von Ereignissen nehmen rapide ab, Prognosen und Erfahrungen aus der Vergangenheit als Grundlage für die Gestaltung von Zukunft verlieren ihre Gültigkeit und Relevanz. Planung von Investitionen, Entwicklungen und Wachstum wird fast unmöglich. Immer weniger ist klar, wohin die Reise geht.

Exkurs: VUCA

carmasec

COMPLEXITY

Komplexität. Unsere Welt ist komplexer denn je. Was ist die Ursache? Was die Wirkung? – Probleme und deren Auswirkungen werden vielschichtiger und schwerer zu verstehen. Es vermischen sich die verschiedenen Ebenen und machen Zusammenhänge unübersichtlicher. Entscheidungen werden zu einem nicht mehr steuerbaren Geflecht aus Reaktion und Gegenreaktion. Die Entscheidung für den einen richtigen Weg ist kaum möglich.

Exkurs: VUCA

carmasec

AMBIGUITY

Uneindeutigkeit. „One fits all“ und „best practice“ war gestern – selten ist etwas ganz eindeutig oder ganz exakt bestimmbar. Nicht nur schwarz und weiß, sondern auch bunt ist eine Option. Die Anforderungen an Organisationen und Führung von heute sind widersprüchlicher und paradoxer denn je und stellen das persönliche Wertesystem komplett auf die Probe. Das „Was?“ tritt hinter dem „Warum?“ und dem „Wie? zurück. Entscheidungen fordern Mut, Bewusstheit und Fehlerfreudigkeit.

Sonstige Herausforderungen

carmasec

- Kommunikationsbarriere zwischen Fach- und Führungsebene(n):
  „IT und Business sprechen nicht die gleiche Sprache!“
- Schwierigkeit ein angemessenes Vorgehen zu definieren: „Rote Laterne vs. Branchenprimus“
- Cybersecurity wird als komplex und umfangreich wahrgenommen, es fehlt Orientierung
- Spannungsfeld zwischen Digitalisierungsvorhaben und Risikomanagement
- Erfolge der Cybersecurity können nur eingeschränkt ans Management kommuniziert werden
- Budgetrestriktionen schränken eine schnellle aber notwendige Maßnahmenumsetzung ein

Cyber-Resilienz: Definition

Cyber-Resilienz

ist ein **systemischer, ganzheitlicher, strategischer und interdisziplinärer Ansatz,**

um **Sicherheitsvorfälle zu vermeiden**

sowie deren **Auswirkungen auf den Geschäftsbetrieb zu minimieren** und die **Werte des Unternehmens zu bewahren**.

Cyber-Resilienz: Definition

carmasec

Maßnahmen der Cyber-Resilienz verfolgen die 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

Cyber-Resilienz: Definition

carmasec

Dies bedingt die Entwicklung folgender Fähigkeiten innerhalb der Organisation:

- **Anpassungsfähigkeit** an sich wandelnde Bedrohungsszenarien und Umfeldbedingungen
- **Lernfähigkeit** aus Ereignissen und Erarbeitung neuer **Handlungsoptionen**

Cyber-Resilienz: Definition

carmasec

Grundprämisse

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

Cyber-Resilienz: Einordnung

carmasec

Cyber-Resilienz

- Cyber-sicherheit
- Business Continuity
- Desaster Recovery

Reifegradmodelle & Reifegradmessung

carmasec

- 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.

Übersicht bekannter Reifegradmodelle

carmasec

Allgemeine Reifegradmodelle:

- Capability Maturity Model Integration (CMMI)
- Software Assurance Maturity Model (openSAMM)
- Quality Management Maturity Grid (QMMG)
- Test Maturity Model (TMM)
- ...

Für Informations-, Cybersicherheit & Cyberresilienz:

- Open Information Security Management Maturity Model (O-ISM3)
- COBIT Maturity for Information Security
- NIST Cybersecurity Framework
- ISACA CMMI Cybermaturity Platform
- Cybersecurity Maturity Model Certification (CMMC), Department of Defence (DoD)
- Community Cyber Security Maturity Model (CCSMM), Center for Infrastructure Assurance and Security (CIAS)
- Cybersecurity Capability Maturity Model (C2M2), U.S. Department of Energy
- ...

Vorteile und Nutzung von Reifegradmessungen

carmasec

- Evaluierung von gegenwärtigen Fähigkeiten, Ressourcen und Infrastruktur
- Objektivierte Stand- und Statusermittlung des Reifegrads
- Vergleichbarkeit zu anderen Marktteilnehmern
- Planungsgrundlage für Maßnahmenplan zur Erreichung der nächsten Stufe
- Sicherstellung der Produktivität und Qualität (sowie Aufrechterhaltung) der Geschäftsprozesse eines Unternehmens
- Planung und Einhaltung von Budget- und Zeitplanungen
- Klare Kommunikation innerhalb und außerhalb des Unternehmens in einheitlicher Sprache

Wirksamkeit von Reifegradmodellen

carmasec

- 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.

Reifegradmodelle im Vergleich

carmasec

Bedrohungslage	**unstrukturiert**		**strukturiert**		**hochgradig- strukturiert**
Reifegradstufe	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
CMMC	Basic Cyber Hygiene	Intermediate Cyber Hygiene	Good Cyber Hygiene	Proactive	Advanced/Progressive
C2M2	Identifizieren	Schützen	Erkennen	Reagieren	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.

Reifegradmodelle in der Cybersicherheit

carmasec Cybersicherheits-Reifegradmodell:
„Best of Breed“-Ansatz mit Adaption für deutsche und europäische Anwenderunternehmen

Reifegradmodelle in der Cybersicherheit

carmasec

Level 1:	**Sicherheitsbewusstsein**
Beschreibung:	In dieser Stufe gilt es insbesondere bei den Organisationsmitgliedern ein hohes Maß an Bewusstsein für Anliegen der Cybersicherheit zu fördern.
Methoden & Instrumente:	• Management-Attention und Management-Commitment (Grundlagen GRC und Cybersicherheit., Workshops, etc.) • Mitarbeitersensibilisierung (Awareness, Schulungen) • Isolierte Adhoc-Maßnahmen (TOMs) • Einzelne Sicherheitsüberprüfungen, Penetrationstests

Reifegradmodelle in der Cybersicherheit

carmasec

Level 2:	Prozessentwicklung
Beschreibung:	In dieser Stufe stehen die Prozesse und Richtlinien im Vordergrund. Diese gewährleisten, dass Cybersicherheit im Betrieb funktioniert.
Methoden & Instrumente:	• Aufbau GRC-Organisation, Sicherheitsteam • Aufbau Managementsysteme, Leitlinien • Identifikation kritischer Werte, Klassifizierung von Werten, Definition der Schutzziele • Durchführung von Sicherheitsüberprüfungen • Erstellung von Sicherheitskonzepten • Blue-Teaming

Reifegradmodelle in der Cybersicherheit

carmasec

Level 3:	Informationspolitik
Beschreibung:	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.
Methoden & Instrumente:	• 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 Notfallplänen

Reifegradmodelle in der Cybersicherheit

carmasec

Level 4:	Verbesserungsmanagement
Beschreibung:	In dieser Stufe verfügt das Unternehmen bereits über die Fähigkeit (und Pläne), um Bedrohungsszenarien proaktiv zu erkennen und zu beseitigen. Prävention spielt hier eine wichtige Rolle.
Methoden & Instrumente:	• Erweiterung der Frühwarnsysteme, Szenario-basierte Risikosimulationen • Etablierung integrierter Sicherheitssysteme (SIEM, SOC, Threat Intelligence, …) • Etablierung/Umsetzung der gesamtheitlichen Cybersicherheits-strategie • Re-Evaluierung und Wirksamkeitsprüfung, Review, PDCA-Zyklus (Plan-Do-Check-Act/Deming-Kreis), KVP/CSI (Kontinuierlicher Verbesserungsprozess/Continuous Service Improvement), Kaizen

Reifegradmodelle in der Cybersicherheit

carmasec

Level 5:	Volle Betriebsfähigkeit in der Cybersicherheit
Beschreibung:	In dieser Reifegradstufe erfüllt das Unternehmen nicht nur alle zuvor genannten Voraussetzungen. Die Prozesse und Mechanismen wirken auch im gesamten Unternehmen durchgehend. Darüber hinaus kann es sich mit relevanten Unternehmen und Institutionen vernetzen, um auf ein komplexes Bedrohungsszenario zu reagieren.
Methoden & Instrumente:	• Durchführung von gesamtheitlichen szenario-basierten Notfallübungen und Sicherheitstest • Etablierung von Security Automation, Threat Intelligence, ML-/KI-basierte Ansätze • Integration von Partnern, Kunden, Zulieferern und Mitbewerbern in das Cybersecurity-Ökosystem

„Security is always too much,
until the day it is not enough.“

William H. Webster
(Former Director, FBI)

Fazit

carmasec

- Reifegradmodelle sind für viele Disziplinen verfügbar
- Im Bereich Cybersicherheit & Cyber-Resilienz kommen aktuelle Modelle ausschließlich aus dem US-amerikanischen Raum
- Reifegradmodelle scheinen ein wirksames Instrument für die Themensteuerung zu sein
- Sie helfen bei der objektiven Bewertung des Ist- und Sollzustands und ermöglichen eine Vergleichbarkeit zu anderen Anwendern

Weiterführende Informationen

- Whitepaper 09/2020, carmasec:
  „Reifegradmodelle für die Cybersicherheit Ihres Unternehmens: Referenzrahmen für Handlungs-, Planungs- und Budgetsicherheit“
  kostenfrei per Email

- Themenseite Cyber-Resilienz:
  “Der Ansatz zur Krisenbewältigung und für Cybersicherheit in einer dynamischen VUCA-Welt“
  http://cyber-resilienz.info

carmasec

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns auf die weitere Diskussion und Ihre Fragen.

Melden Sie sich für unseren Newsletter an: www.carmasec.com/newsletter

Hauptsitz:
carmasec GmbH & Co. KG
Ruhrallee 185
45136 Essen
Germany

Niederlassung:
carmasec GmbH & Co. KG
Im Mediapark 5
50670 Köln
Germany

Telefon: +49 (0) 201 426 385 900
Fax: +49 (0) 201 426 385 909
Web: www.carmasec.com
Email: contact@carmasec.com