carmasec

security. done. right.

Herausforderungen der Digitalisierung: Cybersicherheit und IT-Risiken professionell managen

IT-TRENDS 2020/2021: DIGITAL & SICHER (Online)

Carsten Marmulla, 10.02.2021

Cybersicherheit und IT-Risiken professionell managen

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.

Cybersicherheit und IT-Risiken professionell managen

Vorstellung Referent

Carsten Marmulla
Managing Partner &
Senior Trusted Advisor
Standort Essen
Geboren 1974
+49 151 150 500 59
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

Agenda

- ✓ Einblick: Herausforderungen der Digitalisierung
- ✓ Überblick: Digitalisierungsrisiken & Bedrohungslage
- ✓ Durchblick: Management von Cybersicherheit und IT-Risiken
- ✓ Ausblick: Lösungsansätze und Handlungsempfehlungen

Digitale Transformation: Warum eigentlich?

carmasec

- Unternehmen unterliegen globalem Wettbewerbsdruck
- Innovative Technologieansätze im Rahmen der Digitalen Transformation versprechen...
  - Effizienzgewinne,
  - höhere Umsetzungsgeschwindigkeit,
  - Kostenreduktion,
  - neue (datengetriebene) Geschäftsmodelle.

Digitale Transformation: Warum eigentlich?

carmasec

- In erster Linie:
  - Gesamtheitlicher Veränderungsprozess (Change Management)
- Primär zu definieren:
  - Zweck (Motivation) und
  - Ziel (Erwartung)
- **Nicht ausschließlich Technologiewandel!**

Beispiele für Anwendungsfälle (technologisch)

carmasec

- Nutzung von Cloud-Dienstleistungen, Outsourcing
- Industrie 4.0, Smart Factory, Smart Grid & Smart Metering
- Smart Home, Vernetztes Auto, Connected Services
- Prozessautomatisierung, Robotic Process Automation (RPA)
- Smart Data, Big Data (Vorhersagen und Erkenntnisse)
- Internet-of-Things (IoT), Machine-2-Machine, „Smart Everything“
- 5G-Mobilfunk
- ...

Exkurs: VUCA

VUCA ist ein Akronym für die englischen Begriffe

- *Volatility* ‚Volatilität' (Unbeständigkeit),
- *Uncertainty* ‚Unsicherheit',
- *Complexity* ‚Komplexität' und
- *Ambiguity* ‚Mehrdeutigkeit'.

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.

carmasec

„If everything seems under control, you're not going fast enough.”

—

Mario Andretti

Digitale Transformation vs. Cybersicherheit?

carmasec

INNOVATION

Beispiele: Was kann schief laufen?

carmasec

- Cyberangriffe durch Erpressungstrojaner (Ransomware)
- Ausspähen von Geschäftsgeheimnissen oder geschäftskritischen Daten
- Kompromittierung von geschäftskritischen Daten
- Einschränkungen im Geschäftsbetrieb wegen Nichtverfügbarkeit von IT-Systemen und Anwendungen
- Gefährliche Eingriffe in Steuerung geschäftskritischer Systeme (Produktionssteuerung, Leitstände, kritische Infrastrukturen, ...)
- Verstöße gegen gesetzliche Anforderungen bspw. Datenschutz (DS-GVO, BDSG)
- ...

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

Cybersicherheit und IT-Risiken professionell managen

Cyber-Bedrohungslage & Angreifertypologie

carmasec

	Typ 1: „Skript-Kid“	Typ 2: „Hacktivist“	Typ 3: „Cybercrime“	Typ 4: „Nachrichtendienste“
Beispiele	• Verunstalten von Internetseiten • Meldungen von Schwachstellen in Webseiten an die Presse • ...	• DDoS gegen Banken, die Wikileaks Konten gesperrt hatten • Anonymous-Angriffe gegen Unternehmen • ...	• APTs • Phishing-E-Mails • DDoS auf Online-shops/Onlinewetten • SPAM • ...	• Stuxnet (Iranisches Atomprogramm) • Red October (Regierungen im Ostblock) • ...
Aufwand Prävention/ Abwehr	Niedrig bis mittel	Mittel	Hoch	Sehr Hoch
Wirksamkeit	Hoch	Hoch bis mittel	Hoch bis mittel	Mittel bis niedrig

Primärer Fokus

Sekundärer Fokus

„Alles, was vernetzt werden kann,
wird vernetzt werden.”

„Alles was automatisiert werden kann,
wird automatisiert werden.”

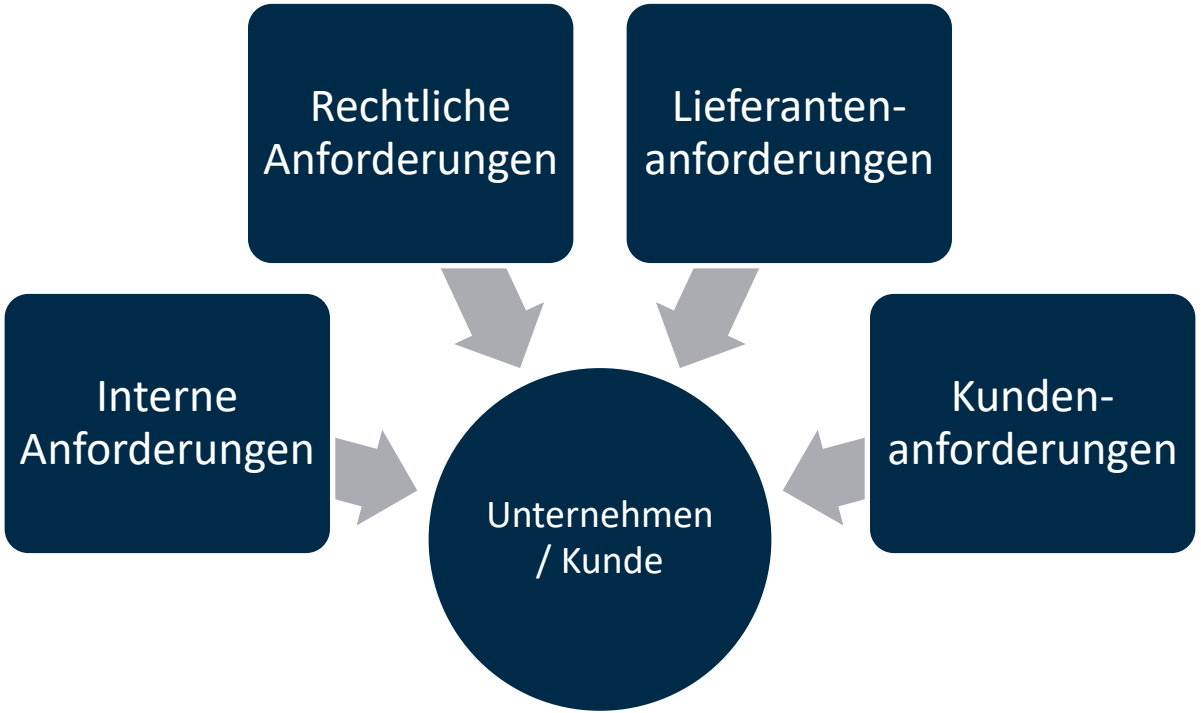
„Alles, was vernetzt werden kann, wird vernetzt werden.”

„Alles was automatisiert werden kann, wird automatisiert werden.”

„Alles, was gehackt werden kann, wird gehackt werden.“

Motivation zum Risikomanagement

carmasec



Terminologie: Einordnung der Begriffe

carmasec

Governance
Risk Management
Compliance

Informations-Sicherheit	Datenschutz	IT-Security
Schutz von geschäftskritischen Daten	Schutz von personenbezogenen Daten	Schutz von Applikationen, Systemen und Netzen

Terminologie: Definition eines Risikos

carmasec

Ein **Risiko** ist nicht dasselbe wir ein **Problem**.

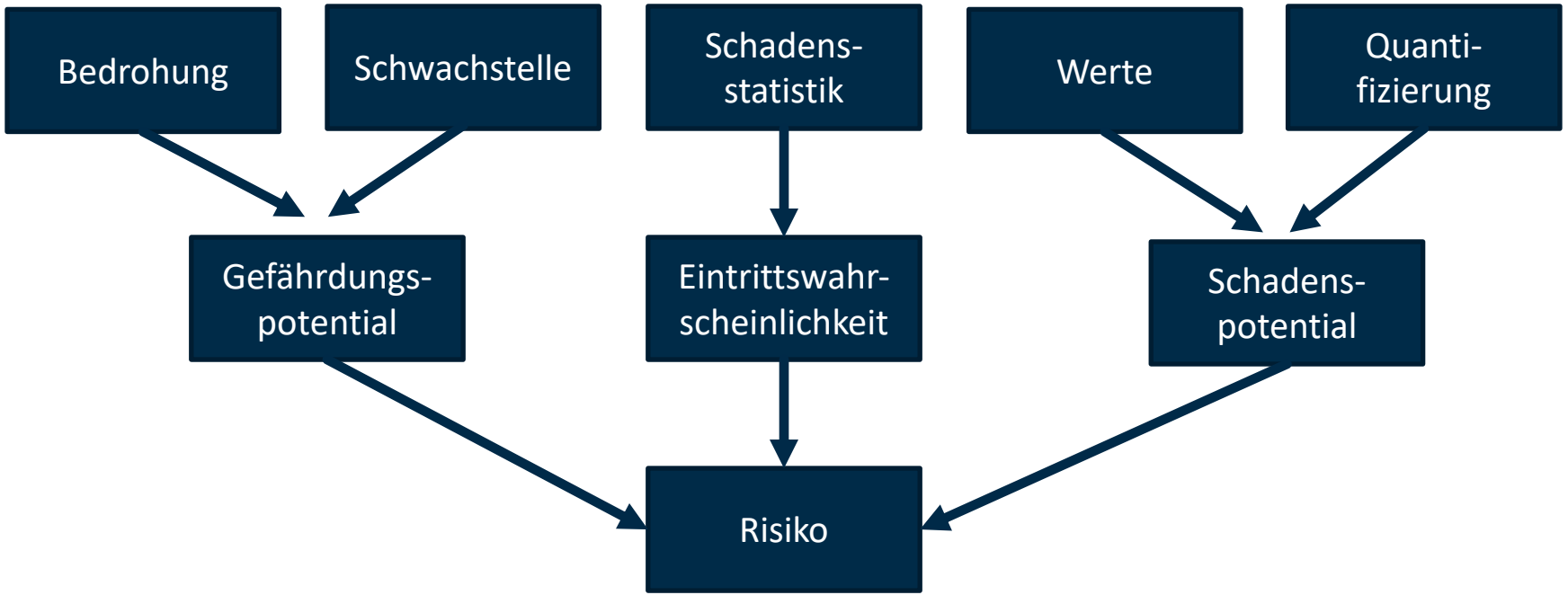
Ein **Problem** ist eine fragliche Angelegenheit
oder ein **Konflikt**: Probleme sind bereits vorhanden.

Im Gegensatz dazu ist ein Risiko noch nicht eingetreten
und wird es vielleicht auch nicht.

Risiken, die eintreten, werden typischerweise zu Problemen.

Terminologie: Definition eines Risikos

carmasec



Mindestanforderungen Cybersicherheit

carmasec

- **Einhaltung der grundsätzlichen rechtlichen Rahmenbedingungen**, zzgl. branchenspezifischer Anforderungen nach dem **Stand der Technik** und orientiert an internationalen Standards (ISO 27001 ff., ISO/IEC 22301, ...)
- Umsetzung von (technischen) **Maßnahmen gemäß „Stand der Technik“**
- Aufbau und Betrieb eines **Managementsystems für Informations-sicherheit und Datenschutz** (ISMS, DSMS), erfordert auch **IT-Risiko-management**
- Aufbau eines **Meldewesen** und Beachtung von **Meldepflichten** (KRITIS)
- Etablierung eines „**Business Continuity Management**"

carmasec

„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

Cybersicherheit und IT-Risiken professionell managen

Management von Informationssicherheit (ISMS)

carmasec

Aufbau Informationssicherheitsmanagement

carmasec

- Wirkungsbereich (“Scope“) zu definieren
  - Interne und externe Belange berücksichtigen
  - Anforderungen von beteiligten Dritten
- “Management Commitment“
  - Unterstützung der Unternehmensführung bei Einführung und Weiterentwicklung des ISMS
  - Etablierung einer Informationssicherheitsrichtlinie (IS-RL)
- Etablierung eines IS-Risikomanagements
  - Orientiert an ISO 27005
  - Definition des Risikoappetits, (akzeptierte) Restrisiken

Aufbau Informationssicherheitsmanagement

carmasec

- Sicherheitsstrategie, Sicherheitsrichtlinien
- Sicherheitsorganisation
- Personalmanagement
- Management von Informationswerten („Assets“)
- Zugriffskontrollen
- Kryptographie
- Physische Sicherheit
- Sicherer IT-Betrieb (...)
- Kommunikationssicherheit
- Beschaffung / Entwicklung / Wartung von IT-Systemen
- Vertrags- / Dienstleister-management
- Informationssicherheitsvorfall-management (Incident Mgmt.)
- Business Continuity Management

Management von Risiken (gemäß ISO 27005)

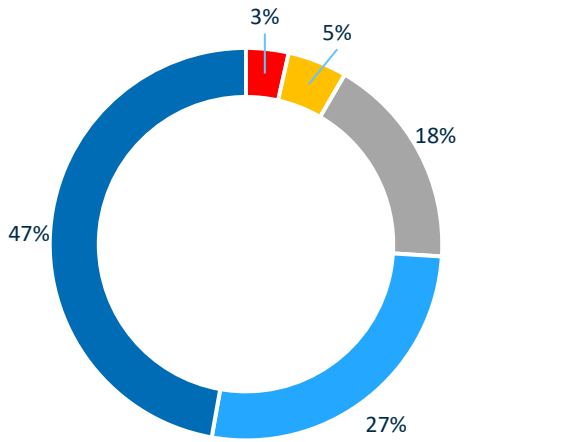
carmasec

- **Risikovermeidung:**
  Ein identifiziertes Risiko wird durch eine technische und/oder organisatorische Maßnahme vollständig vermieden, so dass kein Restrisiko nach Durchführung der Maßnahme verbleibt.
  (Beispiele: Abschaltung einer Applikation, Datenlöschung)
- **Risikominderung:**
  Ein identifiziertes Risiko wird beispielsweise durch eine technische und/oder organisatorische Maßnahme gemindert und auf ein definiertes akzeptables Niveau reduziert. Es verbleibt ein Restrisiko unterhalb der zuvor definierten Risikotoleranzgrenze.
  (Beispiele: Einsatz von Firewalls, Implementierung von Verschlüsselungslösungen, Verschärfung von Zugriffskontrollen)
- **Risikoverlagerung:**
  Das identifizierte Risiko wird an einen Dritten übergeben.
  (Beispiele: Abschluss einer Risikoversicherung, Übergabe der Applikationsverantwortung im Rahmen von „Managed Services“ oder Gewerken)
- **Risikoakzeptanz:**
  Das identifizierte Risiko liegt unterhalb der zuvor definierten Risikotoleranzgrenze.
  (Beispiele: Ausnahmegenehmigung, dokumentierte Risikoübernahme durch die Fachseite)

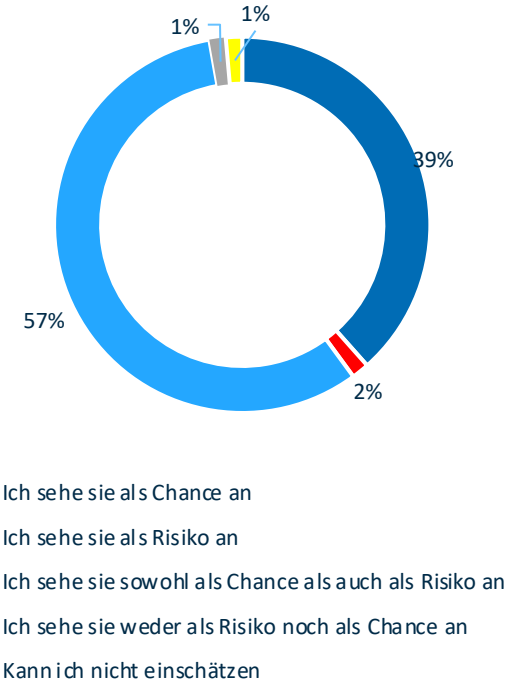
Cybersicherheit und IT-Risiken professionell managen

Studienergebnisse (Auszug)

Wie stark beeinflusst die Digitalisierung Ihr Geschäftsmodell?

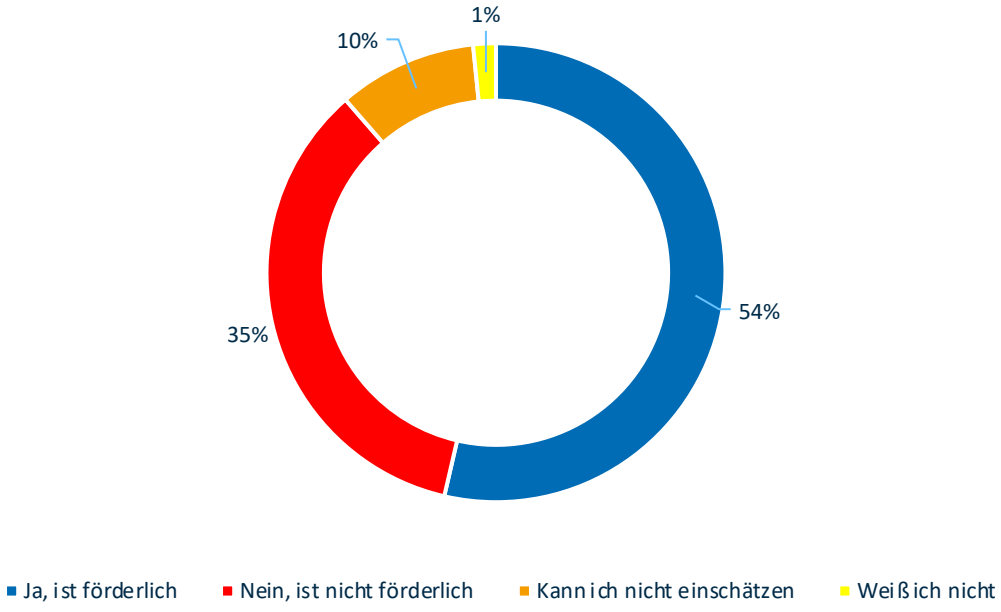


Digitalisierung eher Chance oder Risiko?



Studienergebnisse (Auszug)

Ist die DS-GVO förderlich für die Digitalisierung Ihres Unternehmens?



Mehr als die Hälfte der Probanden sieht die DS-GVO als förderlich für die Digitalisierung ihres Unternehmens an (53,65%). Immerhin mehr als ein Drittel der Befragten empfindet die DS-GVO nicht als förderlich für die Digitalisierung des Unternehmens.

Festzustellen ist, dass die DS-GVO über eine große Bekanntheit verfügt, nur 10% der Probanden geben an, die Förderlichkeit der DS-GVO auf die Digitalisierung ihres Unternehmens nicht einschätzen zu können. Nur 1.6% der Befragten geben an “weiß ich nicht”.

Cybersicherheit und IT-Risiken professionell managen

Lösungsansätze & Handlungsoptionen

carmasec

- Ermittlung des individuellen organisatorischen Risikoprofils
- Klassifizierung von Daten in Verarbeitungsprozessen
- Ermittlung von geschäftskritischen Prozessen, Systemen, Anwendungen
- Dokumentation der Ergebnisse und Prozesse zur Vermeidung von grober Fahrlässigkeit
- Definition einer gesamtheitlichen Cybersicherheitsstrategie, Vermeidung von isolierten Einzelmaßnahmen
- Risikobasierter Ansatz bei Maßnahmendefinition, kein „Fort Knox“
- Dauerhaftes & überprüfbares Management der Cybersicherheitsstrategie

Lösungsansätze & Handlungsoptionen

carmasec

Best Practices: z.B. **Basismaßnahmen** zur Cyber-Sicherheit vom BSI

- Absicherung von Netzübergängen
- Abwehr von Schadprogrammen (z.B. „Virenscanner“)
- Inventarisierung der IT-Systeme
- Vermeidung von offenen Sicherheitslücken (z.B. Softwareaktualisierung)
- Logdatenerfassung und -auswertung
- Sicherstellung eines aktuellen Informationsstandes (CERT, Lagebild)
- Bewältigung von Sicherheitsvorfällen (CSIRT)
- ...

Quelle: BSI Basismaßnahmen der Cyber-Sicherheit v2.0:
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_006.html

Lösungsansätze & Handlungsoptionen

carmasec

Best Practices: z.B. **Basismaßnahmen** zur Cyber-Sicherheit vom BSI

- ...
- Sichere Authentisierung
- Sichere Interaktion mit dem Internet
- Sichere (oder keine) Nutzung sozialer Netze
- Gewährleistung der Verfügbarkeit notwendiger Ressourcen
- Durchführung nutzerorientierter Maßnahmen (“Awareness“-Schulungen)
- Regelmäßige Durchführung von technischen Sicherheitsüberprüfungen

Quelle: BSI Basismaßnahmen der Cyber-Sicherheit v2.0:
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_006.html

Exkurs: Definition von Cyber-Resilienz

carmasec

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**.

Exkurs: Definition von Cyber-Resilienz

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

Exkurs: Definition von Cyber-Resilienz

Dies bedingt die Entwicklung folgender Fähigkeiten innerhalb der Organisation:

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

Exkurs: Definition von Cyber-Resilienz

carmasec

Grundprämisse

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

Exkurs: Reifegradmodelle in der Cybersicherheit

carmasec

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

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

—

William H. Webster
(Former Director, FBI)

Fazit & Empfehlungen

carmasec

1. **IT-Risikomanagement:**
   - Definition des individuellen Risikoprofils (Risikoanalyse)
   - Etablierung eines Managementsystems für Informationssicherheit und Datenschutz
2. **Cybersicherheit:**
   - Thematisches Bewusstsein (und Verständnis) über Informationssicherheit
   - Definition und Umsetzung von **technischen und organisatorischen Maßnahmen** („TOMs“)

3. **DAS WICHTIGSTE: KEINE ZEIT VERLIEREN UND HEUTE STARTEN**

carmasec

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns auf die weitere Diskussion mit Ihnen.

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