carmasec

security. done. right.

carmasec

security. done. right.

Digitale Krankheitserreger & Prävention: Impfen Sie sich gegen Cyber-Bedrohungen

Carsten Marmulla

Wümek-Kongress, Würzburg, 08.05.2019

Agenda

carmasec

- Vorstellung
- Ausgangssituation:
  - Digitale Transformation / Gesundheitswesen
- Bedrohungslage
- Behandlungsempfehlung
- Mindestanforderungen zur Cybersicherheit
- Fazit

Vorstellung Referent

Carsten Marmulla

Managing Partner &
Senior Trusted Advisor

Skills und Themenschwerpunkte:

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

Projekterfahrungen (Auszug):

- Aufbau und Optimierung von IT-Servicemanagementprozessen
- Erstellung von Sicherheitskonzepten; Schutzbedarfsfeststellungen; Organisatorische Reifegradermittlung; Durchführung von Schwachstellen-/ Risiko- und Business Impact Analysen (BIA); Identifizierung und Steuerung der Maßnahmen
- Definition von Prozessen für Informations-, IT-Sicherheit sowie Datenschutz, Erstellung von Informationssicherheitsrichtlinien, Festlegung, Einführung und Kontrolle der Sicherheitspolitik und Sicherheitsstrategie
- 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
- Vodafone D2 GmbH
- DeTeAccounting GmbH
- Fresenius Netcare GmbH
- TÜV Rheinland AG
- OXEA GmbH
- Grünenthal GmbH
- ProActiv Service GmbH (Talanx)
- Hochtief Concessions GmbH

Vorstellung Unternehmen

carmasec

- Gegründet **2018,** Standorte: **Essen** und **Köln**
- Fokus: Cyber Security **Advisory**, **Consulting** und **Research**
- Zielgruppe: Gehobener Mittelstand, KMU
- Branchenerfahrung: **Gesundheitswesen**, **Informationstechnologie**, Telekommunikation, Logistik, Finanzdienstleistungen, Energie, u.a.
- Kooperationsnetzwerke: Allianz für Cybersicherheit (BSI), TeleTrust, Cyber Security Cluster Bonn, eco - Verband der Internetwirtschaft, Eurocloud, networker.nrw, BVMW, ...

Dienstleistungsübersicht

carmasec

Information Security Management
Wegweisende Konzepte auf Basis langjähriger Expertise und Best-Practise.

Security Automation
Automatisierte Lösungen für das Security Management in agilen Entwicklungsprozessen und im Incident Response.

Data Privacy Protection
Evaluation relevanter Datenschutzvorgaben und Sicherstellung der Compliance (z.B. BDSG und DSGVO).

Governance, Risk, Compliance
Beratung des Managements im GRC Kontext auf Basis der spezifischen Anforderungen.

Agile Security
Integration des agilen Software Development Lifecycle in das vorhandene Security Management (Secure SDLC).

Cyber Resilience
Schutz vor Cyber Attacken und Steigerung der Widerstandskraft gegen Angriffe auf die Informationssicherheit.

Business Continuity
Aufrechterhaltung und Wiederherstellung des Geschäftsbetriebs nach Security Incidents.

DevSecOps
Transformation zu DevSecOps durch geräuschlose Integration von Security Controls in die DevOps und CI/CD Pipeline.

Security Research
Evaluation aktueller Security Entwicklungen und neuartiger Angriffsszenarien sowie Ableitung von Abwehrstrategien.

„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

Digitale Transformation (Allgemein)

carmasec

- Unternehmen unterliegen globalem Wettbewerbsdruck
- Innovative Technologieansätze versprechen...
  - Effizienzgewinne,
  - höhere Umsetzungsgeschwindigkeit,
  - Kostenreduktion,
  - neue (datengetriebene) Geschäftsmodelle.

Digitale Transformation (Allgemein)

carmasec

- In erster Linie:

  Gesamtheitlicher Veränderungsprozess (Change Management)

- Primär zu definieren:
  - Zweck (Motivation) und
  - Ziel (Erwartung)
- Nicht ausschließlich Technologiewandel

Digitale Transformation (Gesundheitswesen)

carmasec

- Telemedizin
- eHealth
- Krankenhausinformationssysteme
- Patientenmanagementsysteme
- Vernetzer OP, Konvergenz zwischen OT und IT
- Elektronische Gesundheitskarte
- Digitale Patientenakte
- „Quantified Me“ / Wearables
- ...

Digitale Transformation vs. Cybersicherheit

carmasec

INNOVATION

Beispiele: Was kann schief laufen?

carmasec

- Angriff auf Lukas Krankenhaus Neuss, „Locky“ (Ransomware)
- Kompromittierung von medizinischen Daten
- Verstöße gegen Datenschutzanforderungen (DS-GVO, BDSG)
- Einschränkungen im Geschäftsbetrieb wegen Nichtverfügbarkeit von IT-Systemen und Anwendungen
- Gefährliche Eingriffe in Steuerung medizinischer Geräte (bspw. Herzschrittmacher, Insulinpumpen, OP-Geräte, ...)
- ...

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

Terminologie

carmasec

Governance
Risk Management
Compliance

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

Behandlungsempfehlung

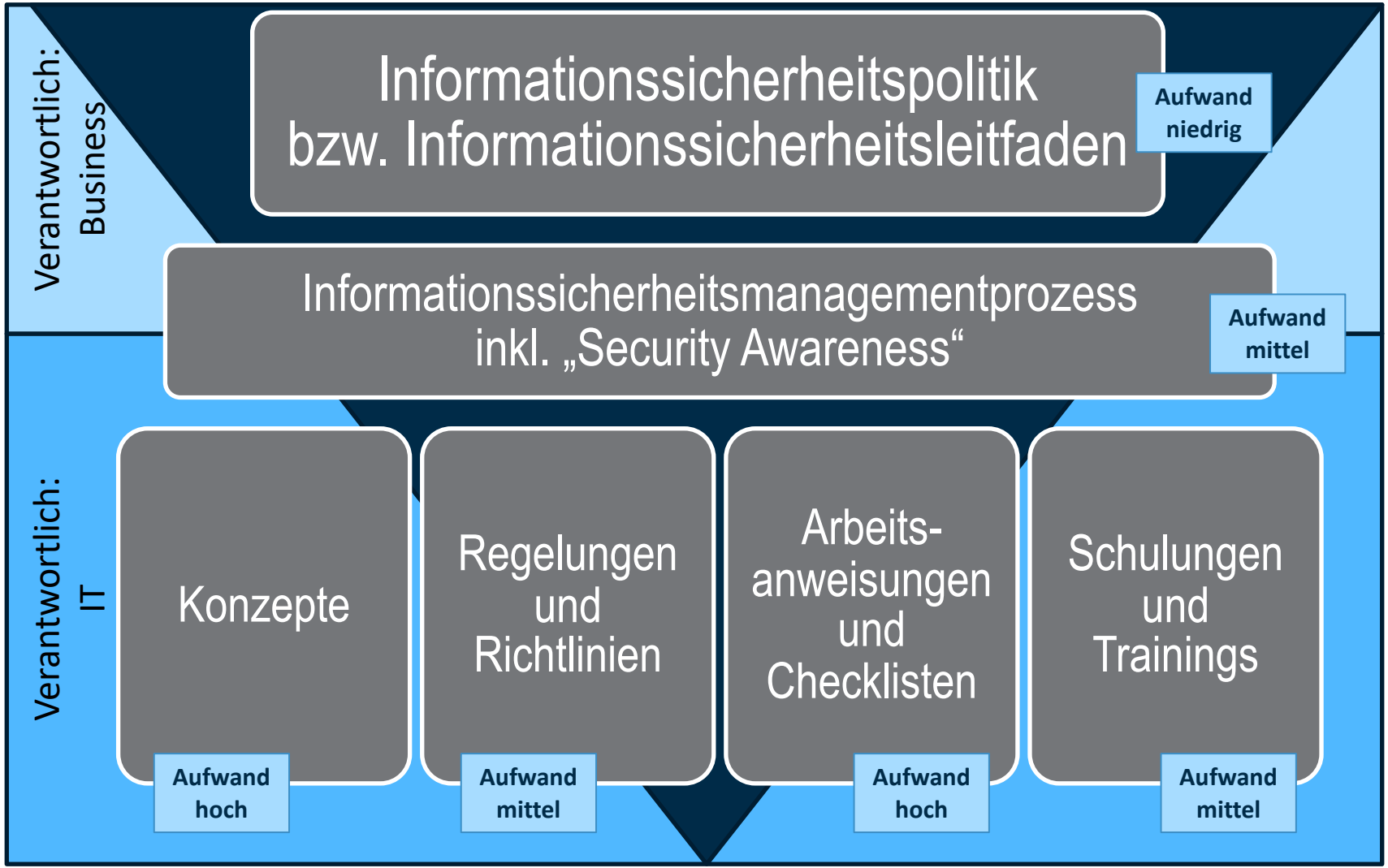
carmasec

- 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 und überprüfbares Management der Cybersicherheitsstrategie

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 Informationssicherheit und Datenschutz** (ISMS, DSMS), erfordert auch **IT-Risikomanagement**
- Aufbau eines **Meldewesen** und Beachtung von **Meldepflichten** (KRITIS)
- Etablierung eines „**Business Continuity Management**"


Verantwortlich: Business
Informationssicherheitspolitik bzw. Informationssicherheitsleitfaden
Aufwand niedrig
Informationssicherheitsmanagementprozess inkl. „Security Awareness“
Aufwand mittel
Verantwortlich: IT
Konzepte
Aufwand hoch
Regelungen und Richtlinien
Aufwand mittel
Arbeits-anweisungen und Checklisten
Aufwand hoch
Schulungen und Trainings
Aufwand mittel

Risikomanagement (gemäß ISO 27005)

- **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)

BSI – Basismaßnahmen zur Cyber-Sicherheit

carmasec

- 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

BSI – Basismaßnahmen zur Cyber-Sicherheit

carmasec

- ...
- 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

Fazit & Tipps

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

4. **<u>DAS WICHTIGSTE: KEINE ZEIT VERLIEREN UND HEUTE STARTEN</u>**

Herzlichen Dank für Ihre Aufmerksamkeit!

Umfrage: Digitalisierung vs. Rechtsrahmen

Link zur Umfrage: umfrage.carmasec.com

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

carmasec Limited & Co. KG
Ruhrallee 185
45136 Essen
Germany

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

Weiterführende Links & Quellen

carmasec

- Allianz für Cybersicherheit – BSI Basismaßnahmen der Cyber-Sicherheit v2.0: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_006.html
- Allianz für Cybersicherheit – BSI Cyber-Sicherheits-Exposition v2.0: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_013.html
- BSI Leitfaden Cyber-Sicherheits-Check: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden-Cyber-Sicherheits-Check.html
- BSI IT-Grundschutz auf Basis der ISO 27001: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- BSI Technische Richtlinien: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html