carmasec

security. done. right.

Wie Sie erfolgreich und sicher Digitalisierungsrisiken vermeiden können

Carsten Marmulla

Digital Futurecongress, Messe Essen, 05.11.2019

Workshop-Agenda

carmasec

- Kurzvorstellung Referent
- Vorstellungsrunde / Erwartungshaltung Teilnehmer
- Themeneinführung
- Studienergebnisse
- Diskussion, Fragen & Antworten
- Lösungansätze

Kurzvorstellung Referent

Kurzvorstellung 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

Kurzvorstellung Referent / Unternehmen

carmasec

Gegründet im Jahr 2018 mit umfassender Expertise aus **über 30 Jahren Beratererfahrung** und **über 100 erfolgreichen Projektabschlüssen**.

Fokus:

- **Cyber Security**
  Advisory, Consulting & Research

Portfolio:

- IT-Risikomanagement, Cyber Risk
- Cyber- und IT-Sicherheit
- Informationssicherheitsmanagement
- Datenschutz und IT-Compliance
- Information Lifecycle Management, IT-Governance

Standorte:

- Essen und Köln
- Deutschlandweite Projekteinsätze

Branchenkenntnisse:

- Telekommunikation
- Logistik/Transport
- Finanzdienstleistungen
- Energieversorgung
- Gesundheitswesen
- Informationstechnologie

carmasec

Vorstellungsrunde & Erwartungshaltung der Teilnehmer

Kurzvorstellung Teilnehmer

carmasec

Stellen Sie sich bitte kurz:

- Ihr Name, Unternehmen, Position in Unternehmen

Leitfragen zur Erwartungshaltung:

- Haben Sie bereits Digitalisierungsprojekte im Unternehmen?
- Sind Sie im Rahmen der Umsetzung auf Schwierigkeiten gestoßen? Auf welche?
- Haben Sie im Rahmen des Projekts strukturiert und gezielt eine Risikoanalyse durch geführt?
- Haben Sie konkrete Problemfälle, die Sie zur Diskussion stellen möchten?

Themeneinführung

Digitalisierung – 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

Typische Anwendungsfälle (technologisch)

carmasec

- Nutzung von Cloud-Dienstleistungen, Outsourcing
- Modernisierung von IT-Landschaften
- Industrie 4.0, Smart Factory
- Prozessautomatisierung, RPA
- Smart Data, Big Data (Vorhersagen und Erkenntnisse)
- Internet-of-Things (IoT), Machine-2-Machine
- ...

carmasec

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

—

Mario Andretti

Digitale Transformation vs. Cybersicherheit?

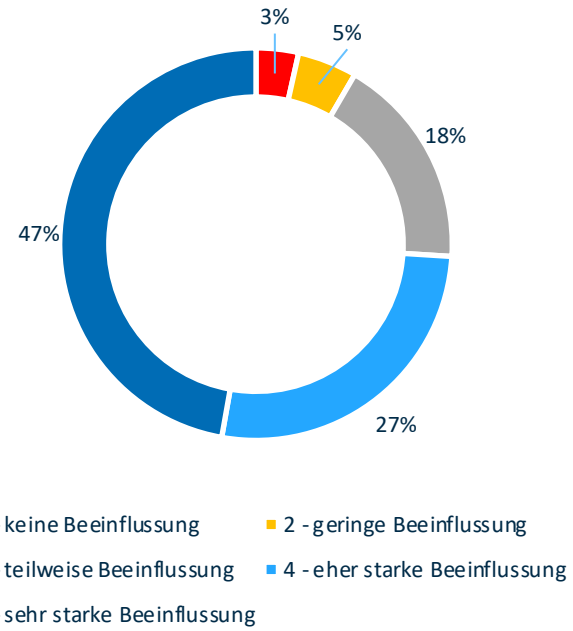
carmasec

INNOVATION

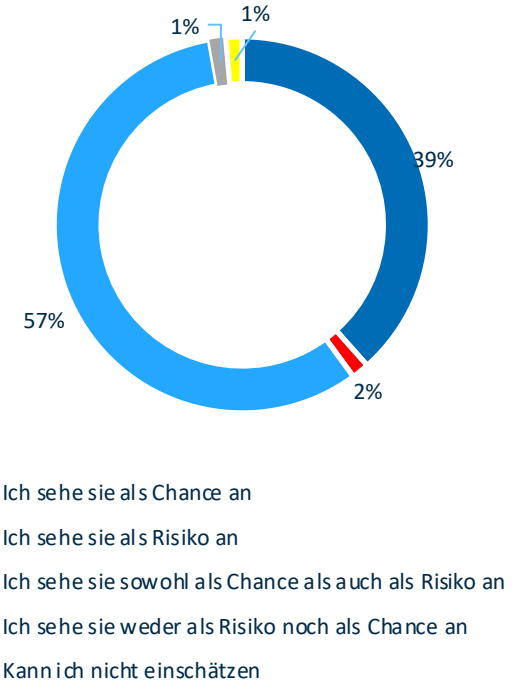
Studienergebnisse

Studienergebnisse (Auszug)

Wie stark beeinflusst die Digitalisierung Ihr Geschäftsmodell?

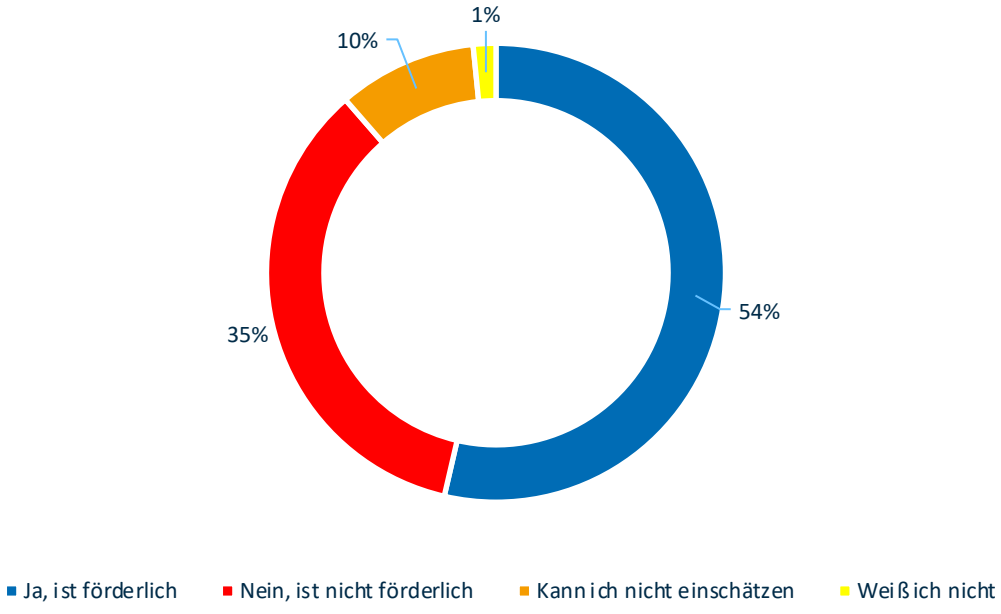


Digitalisierung eher Chance oder Risiko?



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”.

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

Beispiele: Was kann schief laufen?

carmasec

- Cyberangriffe durch Erpressungstrojaner
- 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)
- ...

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

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

carmasec

Diskussion
Fragen & Antworten

carmasec

Lösungsansätze

Behandlungsempfehlung

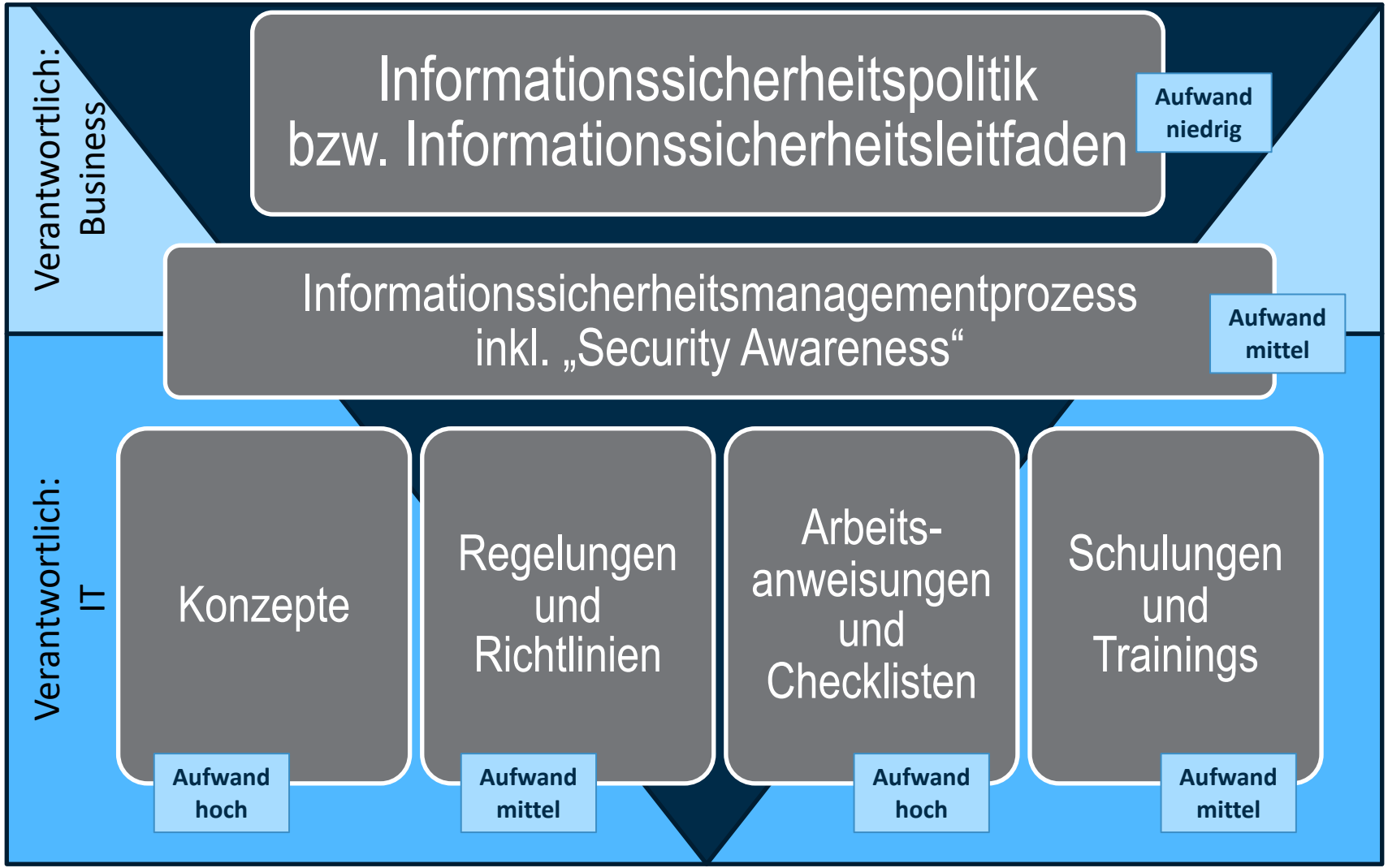
carmasec

- 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

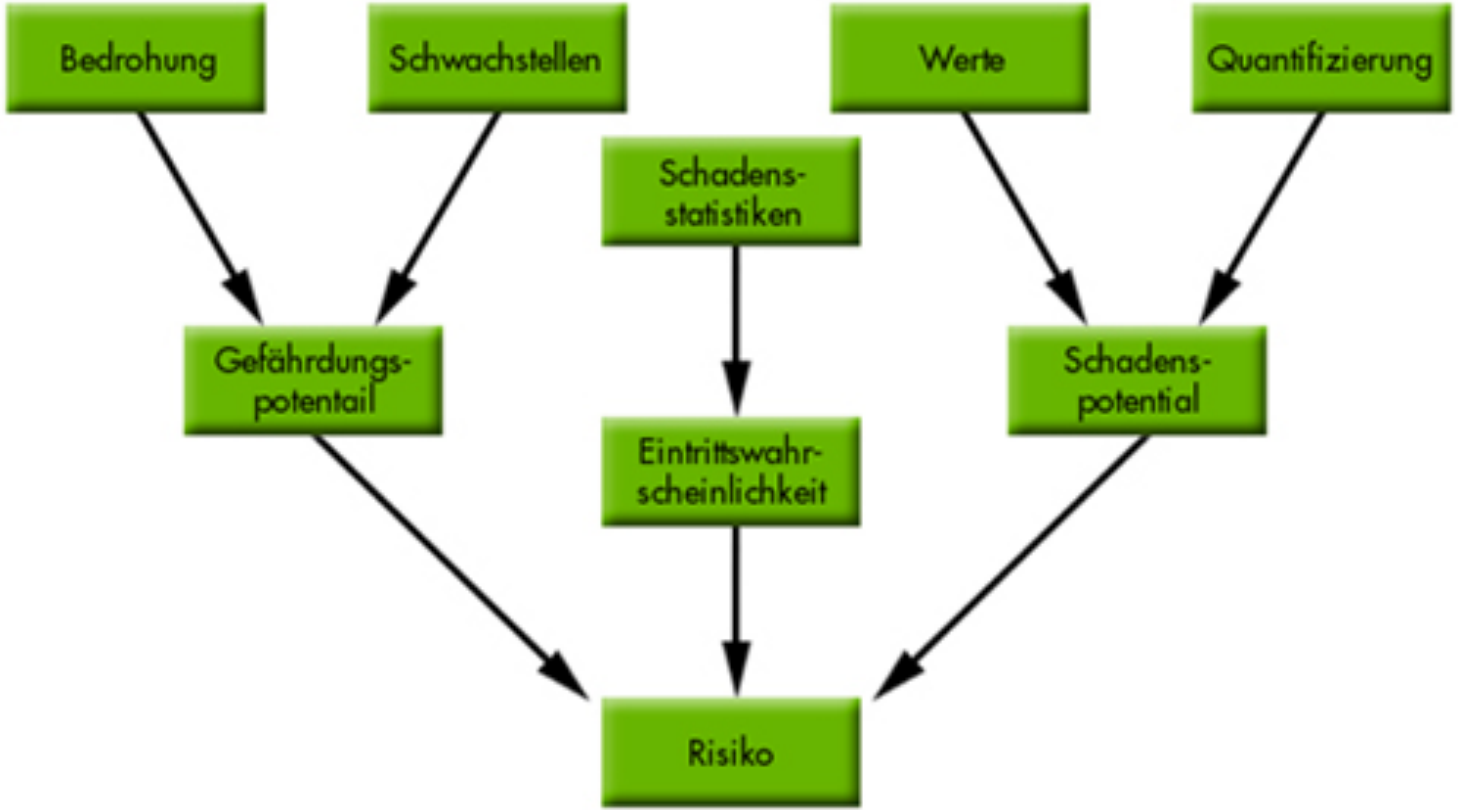
carmasec

- **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

Was ist eigentlich ein Risiko?

carmasec



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>**

carmasec

security. done. right.

Besuchen Sie uns am Stand A21 in Halle 8

carmasec Ltd. & 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

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