carmasec

security. done. right.

Wie man Krankenhäuser und Kliniken vor Hackerangriffen schützt

30.03.2021, online

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, Banken/ Versicherungen, Gesundheitswesen, Energie, 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

Wie man Krankenhäuser und Kliniken vor Hackerangriffen schützt

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

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

Wie man Krankenhäuser und Kliniken vor Hackerangriffen schützt

Anforderungen an die IT-Sicherheit

carmasec

Neue gesetzliche Vorgaben zum Management der IT-Sicherheit im Gesundheitswesen, veröffentlicht am 18.01.2021, in Kraft getreten am 01.02.2021:

- §75b SGB V: Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung

  Umsetzungsfristen: teilweise bis 01.04.2021

- §75c SGB V: IT-Sicherheit in Krankenhäusern

  Umsetzungsfristen: im Regelfall bis 01.01.2022

Sanktionsmöglichkeiten im 5. Sozialgesetzbuch (§394-§397 SGB V)

- Bei Ordnungswidrigkeiten: Bußgelder bis zu 300.000,- Euro

Wie man Krankenhäuser und Kliniken vor Hackerangriffen schützt

Anforderungen an die IT-Sicherheit

carmasec

	Praxistyp 1	Praxistyp 2	Praxistyp 3
Praxistyp laut IT-Sicherheitsrichtlinie	Praxis	Mittlere Praxis	Große Praxis
Ständig mit der DV betraute Personen	1-5	6-20	ab 21
Sonstige Kriterien			Hohes Datenvolumen (Labore, klinik-ähnliche MVZ)

WAS BEDEUTET „STÄNDIG MIT DER DATENVERARBEITUNG BETRAUT“?

Unter dem Begriff „Datenverarbeitung“ werden Tätigkeiten zusammengefasst wie Erheben und Abfragen, Ordnen, Speichern, Anpassen und Ändern, Auslesen und Weiterleiten, Löschen und Vernichten der Daten. In den Praxen beginnt dieser Prozess quasi bei der Terminvereinbarung am Telefon oder dem Einlesen der elektronischen Gesundheitskarte.

Anforderungen an die IT-Sicherheit

carmasec

Basisanforderungen für alle Praxen, Frist bis 01.04.2021:

- Verwendung sicherer Apps, Verhinderung von Datenabfluss, Schutz vertraulicher Informationen, Kryptographische Sicherung vertraulicher Daten, Sperren von Geräten, Einsatz von Virenschutzprogrammen, Zugriffsschutz, Dokumentation des Netzwerks, Verhinderung von unautorisierten Zugriffen auf Microphone/Kameras, Update von Mobiltelefonen

Basisanforderungen für alle Praxen, Frist bis 01.01.2022:

- Sichere Speicherung lokaler App-Daten, Firewalls, Schutz vor unerlaubter automatischer Nutzung von Webanwendungen, regelmäßige Datensicherung, Sperrmaßnahmen bei Verlust eines Mobiltelefons, Schutz vor Schadsoftware, zeitnahes Installieren verfügbarer Aktualisierungen, sicheres Aufbewahren von Administratordaten

Anforderungen an die IT-Sicherheit

carmasec

Für mittlere und große Praxen **ergänzend**:

- Bis 01.04.2021:
  - Minimierung und Kontrolle von App-Berechtigungen
- Bis 01.01.2022:
  - Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung
- Bis 01.07.2022:
  - Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten
  - Regelung zur Mitnahme von Wechseldatenträgern

Anforderungen an die IT-Sicherheit

carmasec

Für große Praxen **ergänzend**:

- Bis 01.01.2022:
  - Festlegung einer Richtlinie für den Einsatz von Smartphones/Tablets
- Bis 01.07.2022:
  - Auswahl und Freigabe von Apps

Anforderungen an die IT-Sicherheit

carmasec

Für alle Praxen mit medizinischen Großgeräten **ergänzend**:

- Bis 01.07.2021:
  - Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen
  - Nutzung sicherer Protokolle für die Konfiguration und Wartung
- Bis 01.01.2022:
  - Netzsegmentierung

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

Wie man Krankenhäuser und Kliniken vor Hackerangriffen schützt

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.

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

—

William H. Webster
(Former Director, FBI)

carmasec

Vielen Dank für Ihre Aufmerksamkeit!

Wir freuen uns auf die weitere Diskussion mit Ihnen.

Weiterführende Informationen

Links & Quellen:

- carmasec.com – Sichere IT-Infrastruktur: https://www.carmasec.com/de/sichere-infrastruktur/
- TeleTrust – Stand der Technik: https://www.stand-der-technik-security.de/startseite/
- KBV – Infohub zur IT-Sicherheitsrichtlinie: https://hub.kbv.de/site/its
- KBV – Praxiswissen IT-Sicherheit: https://www.kbv.de/media/sp/PraxisWissen_IT-Sicherheit.pdf
- BSI – Leitfaden zur Basisabsicherung nach IT-Grundschutz: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3
- Allianz für Cybersicherheit – Basismaßnahmen v2.0: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_006.html

Wie man Krankenhäuser und Kliniken vor Hackerangriffen schützt

Anforderungen an die IT-Sicherheit

carmasec

§ 75b SGB V Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung

(1) Die Kassenärztlichen Bundesvereinigungen legen bis zum 30. Juni 2020 in einer Richtlinie die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung fest. Die Richtlinie umfasst auch Anforderungen an die sichere Installation und Wartung von Komponenten und Diensten der Telematikinfrastruktur, die in der vertragsärztlichen und vertragszahnärztlichen Versorgung genutzt werden.

(2) Die in der Richtlinie festzulegenden Anforderungen müssen geeignet sein, abgestuft im Verhältnis zum Gefährdungspotential und dem Schutzbedarf der verarbeiteten Informationen, Störungen der informationstechnischen Systeme, Komponenten oder Prozesse der vertragsärztlichen Leistungserbringer in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele zu vermeiden.

(3) Die in der Richtlinie festzulegenden Anforderungen müssen dem Stand der Technik entsprechen und sind jährlich an den Stand der Technik und an das Gefährdungspotential anzupassen. Die in der Richtlinie festzulegenden Anforderungen sowie deren Anpassungen erfolgen im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik sowie im Benehmen mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der Bundesärztekammer, der Bundeszahnärztekammer, der Deutschen Krankenhausgesellschaft und den für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen. Die Anforderungen nach Absatz 1 Satz 2 legen die Kassenärztlichen Bundesvereinigungen zusätzlich im Benehmen mit der Gesellschaft für Telematik fest.

[...]

Anforderungen an die IT-Sicherheit

carmasec

§ 75b SGB V Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung (Fortsetzung)

[...]

(4) Die Richtlinie ist für die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer verbindlich. Die Richtlinie ist nicht anzuwenden für die vertragsärztliche und vertragszahnärztliche Versorgung im Krankenhaus, soweit dort bereits angemessene Vorkehrungen getroffen werden. Angemessene Vorkehrungen im Sinne von Satz 2 gelten als getroffen, wenn die organisatorischen und technischen Vorkehrungen nach § 8a Absatz 1 des BSI-Gesetzes oder entsprechende branchenspezifische Sicherheitsstandards umgesetzt wurden.

(5) Die Kassenärztlichen Bundesvereinigungen müssen ab dem 30. Juni 2020 die Mitarbeiterinnen und Mitarbeiter der Anbieter im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik auf deren Antrag zertifizieren, wenn diese Personen über die notwendige Eignung verfügen, um die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer bei der Umsetzung der Richtlinie sowie deren Anpassungen zu unterstützen. Die Vorgaben für die Zertifizierung werden von den Kassenärztlichen Bundesvereinigungen im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik sowie im Benehmen mit den für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen bis zum 31. März 2020 erstellt. In Bezug auf die Anforderungen nach Absatz 1 Satz 2 legen die Kassenärztlichen Bundesvereinigungen die Vorgaben für die Zertifizierung der Mitarbeiterinnen und Mitarbeiter der Anbieter nach Satz 1 im Benehmen mit der Gesellschaft für Telematik fest.

Anforderungen an die IT-Sicherheit

carmasec

§ 75c SGB V IT-Sicherheit in Krankenhäusern

(1) Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.

(2) Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

(3) Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.

Ihr Ansprechpartner: Carsten Marmulla

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

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