carmasec

security. done. right.

Mehr Industrie 4.0 - Security durch Zero-Trust-Konzepte

deutsche ict + medienakademie, 13.01.2021

Carsten Marmulla

Agenda

carmasec

- Vorstellung Referent & Unternehmen
- Anwendungsfälle
- Bedrohungslage
- Bestehende Sicherheitsansätze
- Zero Trust Konzept
- Ausblick CARTA & Co.

Mehr Industrie 4.0 - Security durch Zero-Trust-Konzept

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.

Mehr Industrie 4.0 - Security durch Zero-Trust-Konzept

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

„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.“

Anwendungsfälle

carmasec

- Anwendungsfälle IoT / Smart-Everything
- Industrie-/Produktionsanlagen, Windparks, etc.
- Smart Grid & Smart Metering
- Smart Home, Vernetztes Auto, Connected Services

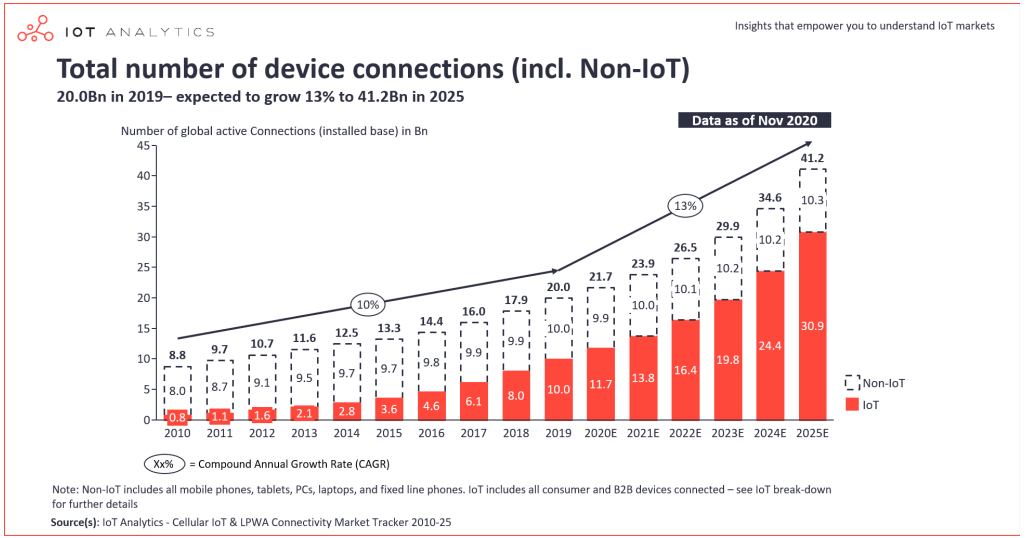
Ausgangs- & Bedrohungslage

carmasec

Zwei Angriffskategorien im Kontext von Industrie 4.0:

1. Attacken **auf** IoT-Geräte

2. Attacken **durch** IoT-Geräte



Bestehende Sicherheitsansätze

carmasec

- Perimeterschutz
- Netzsegmentierung
- Schutz vor Malware
- Authentifizierung/Autorisierung
- Patch Management
- Reaktive Maßnahmen bei Sicherheitsvorfällen

Bestehende Sicherheitsansätze

carmasec

- Perimeterschutz
- Netzsegmentierung
- Schutz vor Malware
- Authentifizierung/Autorisierung
- Patch Management
- Reaktive Maßnahmen bei Sicherheitsvorfällen

Beispielhafte Fragestellungen & Defizite:

- **Wo verläuft der Perimeter beim Einsatz von Cloud-Services?**
- **Wie segmentiere ich dezentrale Infrastrukturen?**
- **Wie binde ich Dienstleister und Zulieferer ein?**
- **Wie gehe ich mit unternehmensfremden Geräten um?**
- **Wie kann ich Sicherheit proaktiv steuern?**

Zero Trust Konzept: Einführung

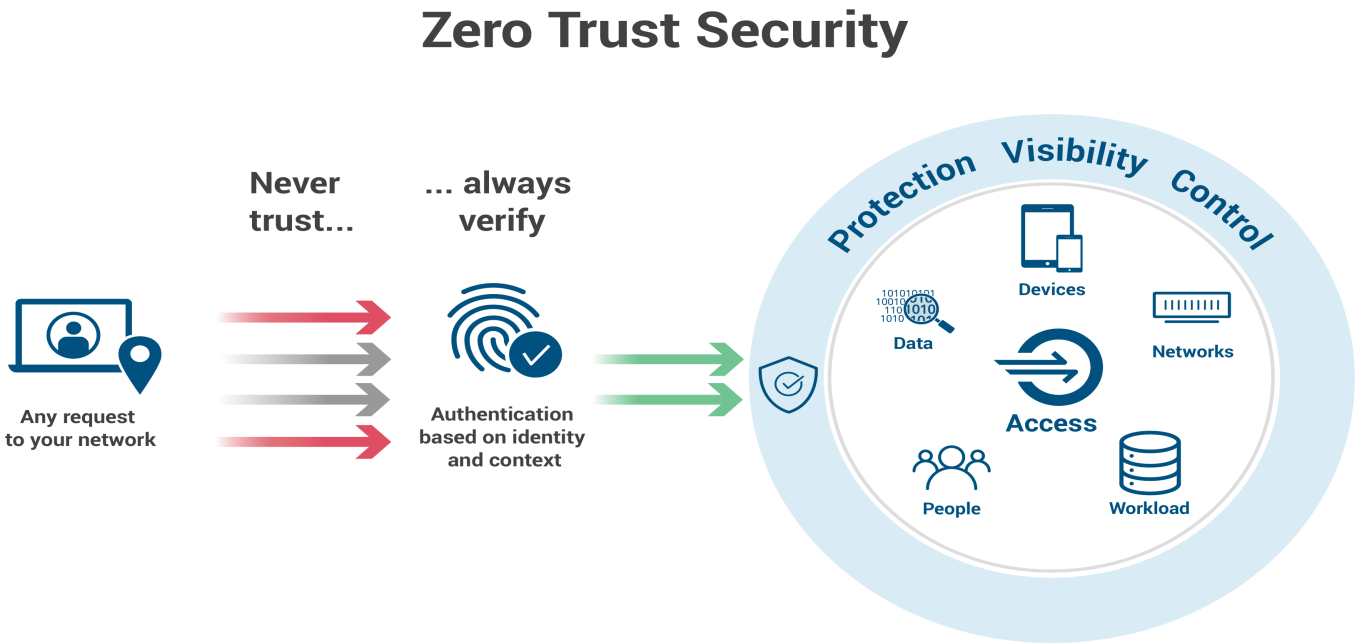
carmasec

„Never trust, always verify!“

- Methodik vor ca. 10 Jahren entwickelt, um komplexe Infrastrukturen besser zu schützen
- Keine pauschales Vertrauen für Geräte im Netzwerk („Zero Trust“)
- Fokussiert auf Benutzer, Assets & Ressourcen
- „Zero Trust Architecture“ dokumentiert in NIST SP 800-207 (August 2020)

Zero Trust Konzept: Kontrolle statt Vertrauen

carmasec



Zero Trust Konzept: Grundprinzipien

carmasec

1. Zentrale Quelle für Benutzeridentitäten
2. Authentifizierung der Benutzer
3. Authentifizierung der Geräte
4. Zusätzlicher Kontext: bspw. Richtlinien, Gerätezustände
5. Richtlinien zur Autorisierung
6. Richtlinien zur Zugriffskontrolle

Zero Trust Konzept: Grundprinzipien

carmasec

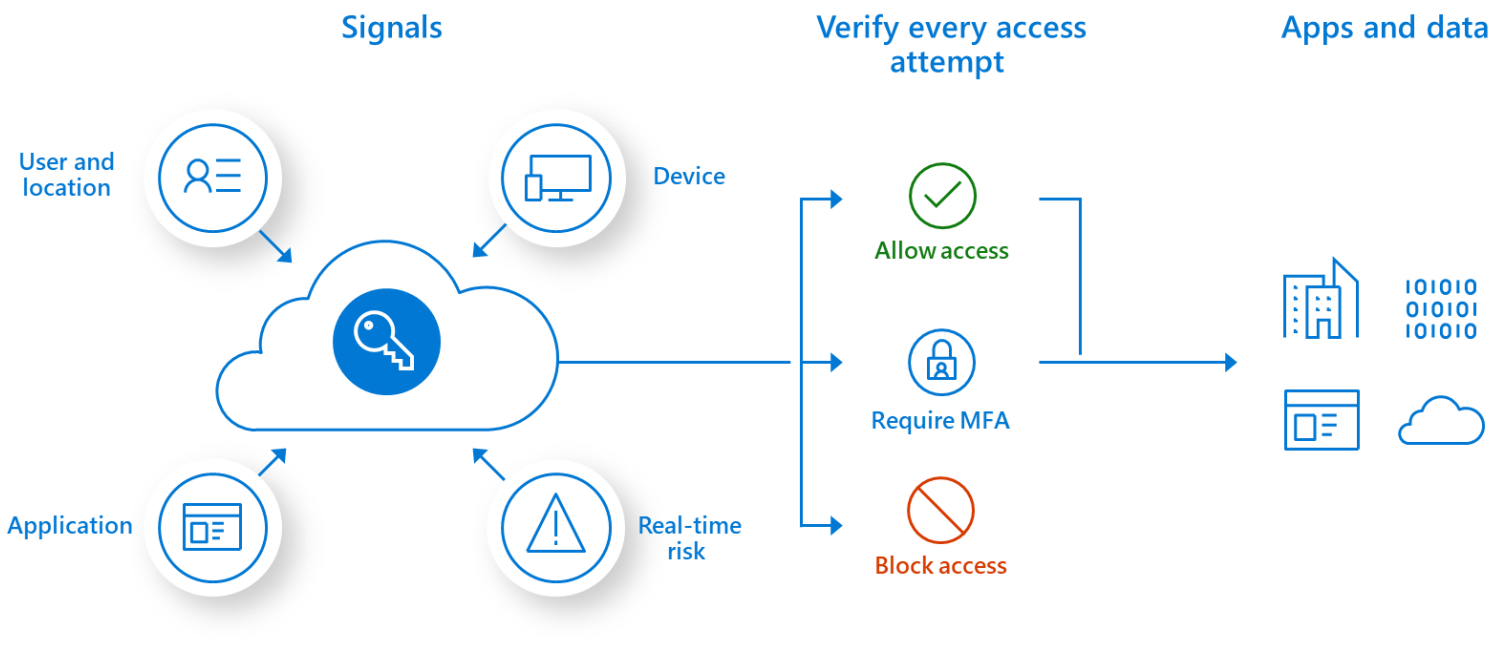
1. Zentrale Quelle für Benutzeridentitäten
2. Authentifizierung der Benutzer
3. Authentifizierung der Geräte
4. Zusätzlicher Kontext: bspw. Richtlinien, Gerätezustände
5. Richtlinien zur Autorisierung
6. Richtlinien zur Zugriffskontrolle

- Jeder Benutzer wird verifiziert!
- Jedes Gerät wird verifiziert!
- Begrenzter und ggf. bedingter Zugriff auf Assets & Ressourcen

- Regelmäßige Kontrolle und Nachjustierung

Zero Trust Konzept: Bedingter Zugriff

carmasec



Ausblick CARTA

- Methodik wurde bereits 2017 von Gartner entwickelt
- Inkludiert in weiten Teilen auch Zero Trust Ansätze
- Automatisierte Kontrolle & selbstlernende Analyse von system-/ prozessübergreifenden Transaktionen
- Korrelation von Ereignissen wird bewertet, um Angriffe & Sicherheitsvorfälle frühzeitig erkennen und vermeiden zu können
- Risikobasierter Ansatz

„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

carmasec

Vielen Dank für Ihre Aufmerksamkeit!

Quellen & weiterführende Links

carmasec

- https://www.carmasec.com/de/whitepaper-carta/
- https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF
- https://en.wikipedia.org/wiki/Zero_Trust_Networks
- https://www.ncsc.gov.uk/collection/mobile-device-guidance/infrastructure/network-architectures-for-remote-access
- https://www.nist.gov/publications/zero-trust-architecture
- https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify
- https://www.zscaler.com/blogs/product-insights/zero-trust-vs-gartner-carta-one-actually-part-other
- https://www.tec-bite.ch/wohin-die-it-security-reise-geht-teil1-carta/
- https://www.computerwoche.de/a/zero-trust-verstehen-und-umsetzen,3547307
- https://www.itsicherheit-online.com/news/vertraue-nichts-und-niemandem-zero-trust-ansatz-fuer-die-cloud
- https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx

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