

Cybersecurity in der Digitalen Transformation

Wolfgang Kiener

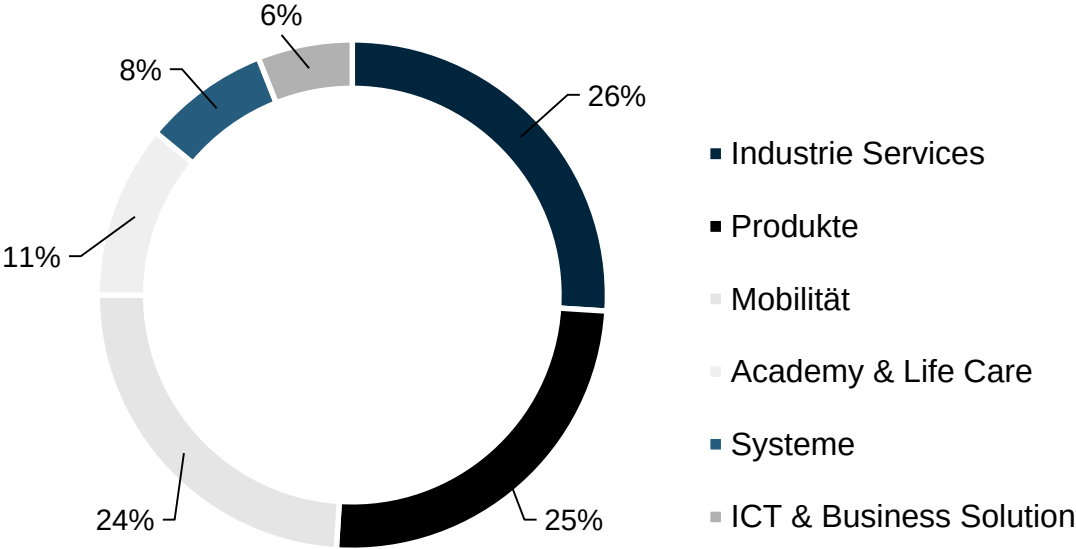
Business Development Manager – Cybersecurity
TÜV Rheinland



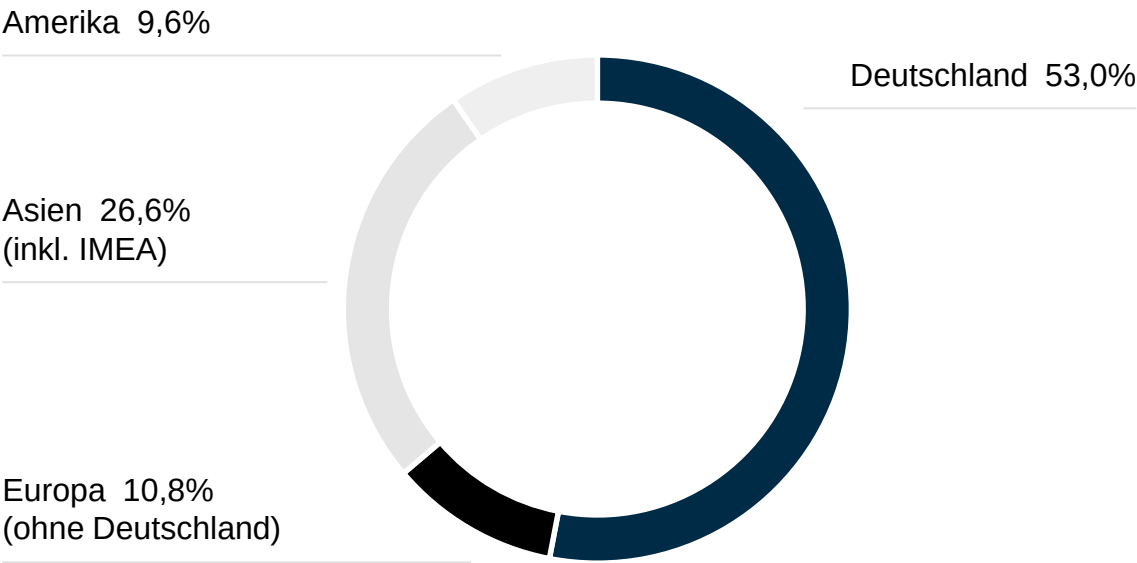
Zahlen 2016.

1.918 Mio. € Umsatz

Umsatz nach Geschäftsbereichen



Umsatz nach Regionen





ICT & Business Solutions

Von der strategischen Beratung über Konzeption und Prozessoptimierung bis zu Implementierung, Betrieb oder Zertifizierung der Systeme

ICT & Business Solutions.

Eckdaten

131 Mio. € Umsatz

6% des Gesamtumsatzes

600 Spezialisten

Geschäftsfelder

- IT-Services & Cyber Security
- Telco Solutions & Consulting

Schwerpunktbranchen

- Wir verfügen über ein breites Erfahrungsspektrum in Schlüsselbranchen
 - Telekommunikation
 - Finanzdienstleistungen
 - Energie
 - Handel
 - Gesundheit
 - Fertigung
 - Mobilität, Logistik, Automobil
 - Luft- und Raumfahrt

Wissenswertes

- Seit 2014 sind wir am deutschen Markt der führende unabhängige Anbieter von IT- und Internetsicherheitsleistungen und gehören weltweit zu den führenden Akteuren
- Wir beraten Netzbetreiber bei der Planung, beim Aufbau und bei der Pflege ihrer Telekommunikationsinfrastrukturen
 - kompetent
 - technologieorientiert
 - kosteneffizient

TÜV Rheinland i-sec. Informations- und IT-Sicherheit.

- Führender unabhängiger Dienstleister für Informationssicherheit in Deutschland
- Beratungs- und Lösungskompetenz in ganzheitlicher Informationssicherheit – von der Steuerungsebene bis ins Rechenzentrum inkl. betriebsunterstützender Leistungen
- Exzellente Technologie-Expertise, umfassendes Branchen-Know-how, Partnerschaften mit Marktführern
- International zählen wir im Verbund mit unseren Schwestergesellschaften OpenSky und 2MC zu den wichtigsten unabhängigen Anbietern
- Zertifiziert nach ISO 27001 und ISO 9001



TÜV Rheinland i-sec GmbH. Fakten und Zahlen.

Standorte Deutschland

- Köln (HQ)
- München
- Gelnhausen
- Saarbrücken
- Hannover
- Hamburg

Fachliches Kompetenzteam

- 15 × Sales
- 20 × Security Engineering
- 60 × Management Beratung
- 45 × Professional Service
und Betrieb

Kernbranchen und Sitz unserer Kunden

- Finanzen
- Automobil
- Energiewirtschaft
- Chemie/Pharma
- Telekommunikation
- Int. Mischkonzerne
- Transport/Logistik
- Öffentlicher Dienst
- Handel



Projekteinsatz an 25.000 Tagen in 2016.

Digital Enterprise. Protected.

Ein umfassendes, globales Serviceportfolio zum Schutz digitaler Unternehmen.

Portfolio Kategorien:

Service Typen:

Mastering Risk & Compliance	Governance & Strategy	Business Continuity Management	Consulting Services 	Testing Services 	Managed Services 
	Risk & Compliance Management	Data Privacy			
	Information Security Management Systems				
Advanced Cyber Defenses	Identity & Access Management	IoT Security			
	Network Security	OT Security			
	Application Security	Security Analytics & Detection			
	Endpoint Security	Incident Response			
	Data Protection				
Secure Cloud Adoption	Cloud Security				
	Enterprise Cloud Adoption				
	Hybrid Infrastructure				

Referent



WOLFGANG KIENER

Business Development Manager
TÜV Rheinland i-sec GmbH
Wolfgang.Kiener@i-sec.tuv.com

1

Thema

Sichere Digitale
Transformation



2

Zielsetzung

Wissens-
austausch

Agenda

1 TÜV Rheinland. Eine weitere industrielle Revolution?

2 Was versteht man unter Digitaler Transformation?

3 Cyber Risk in der Digitalen Transformation.

4 Cybersecurity in der Digitalen Transformation.

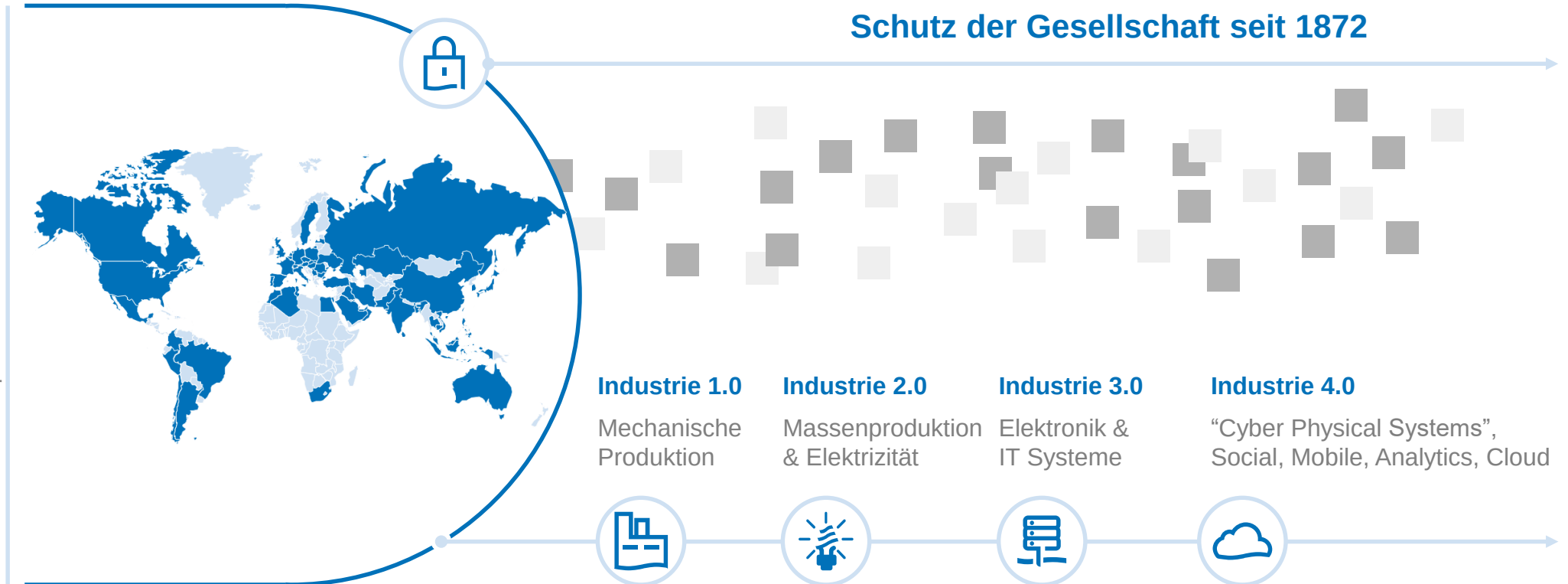
5 Zusammenfassung. Kernpunkte.

TÜV Rheinland. Eine weitere industrielle Revolution?



Precisely Right.

- \$2.3 Milliarden
- 144 Jahre
- 500 Standorte
- 69 Länder
- 19,320 Mitarbeiter



! Die 4. industrielle Revolution wird definiert durch den Einsatz von "Cyber Physical Systems".

TÜV Rheinland. Eine weitere industrielle Revolution?

Von einem einfachen Produkt zu einem “Cyber Physical System” und IoT.

Cyber Physical Systems (CPS)

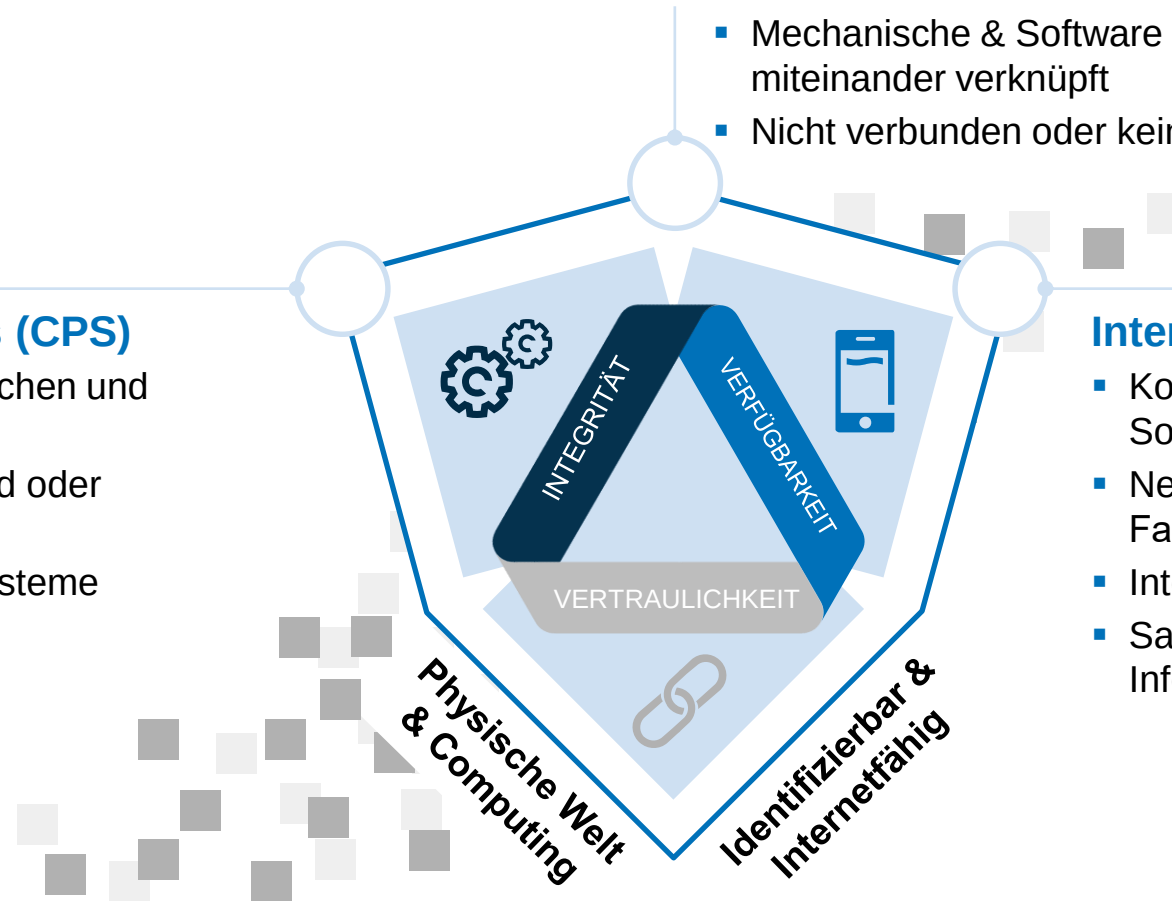
- Kombination von mechanischen und Software Komponenten
- Verbundene Systeme (wired oder wireless)
- Intelligente eingebettete Systeme

Produkte

- Mechanische & Software Komponenten sind nicht tiefgehend miteinander verknüpft
- Nicht verbunden oder keine Intelligenz

Internet of Things (IoT)

- Kombination von mechanischen und Software Komponenten
- Netzwerk aus physischen Endgeräten, Fahrzeugen...
- Intelligente eingebettete Systeme
- Sammlung und Austausch von Informationen



TÜV Rheinland. Eine weitere industrielle Revolution?

Cybersecurity als Grundlage für Sicherheit und Datenschutz.

Sicherheit

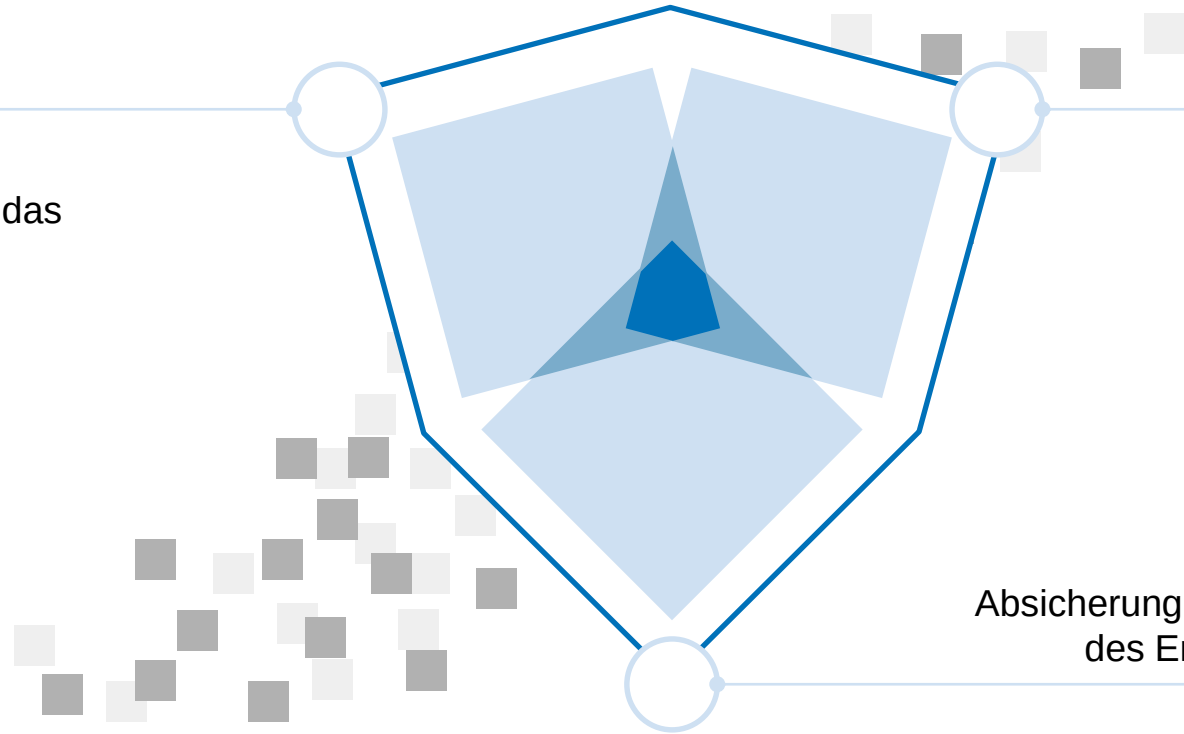
Schutz der Umgebung gegen das IoT Produkt

Cybersecurity

Schutz des IoT Produkt gegen Cyberkriminalität

Datenschutz

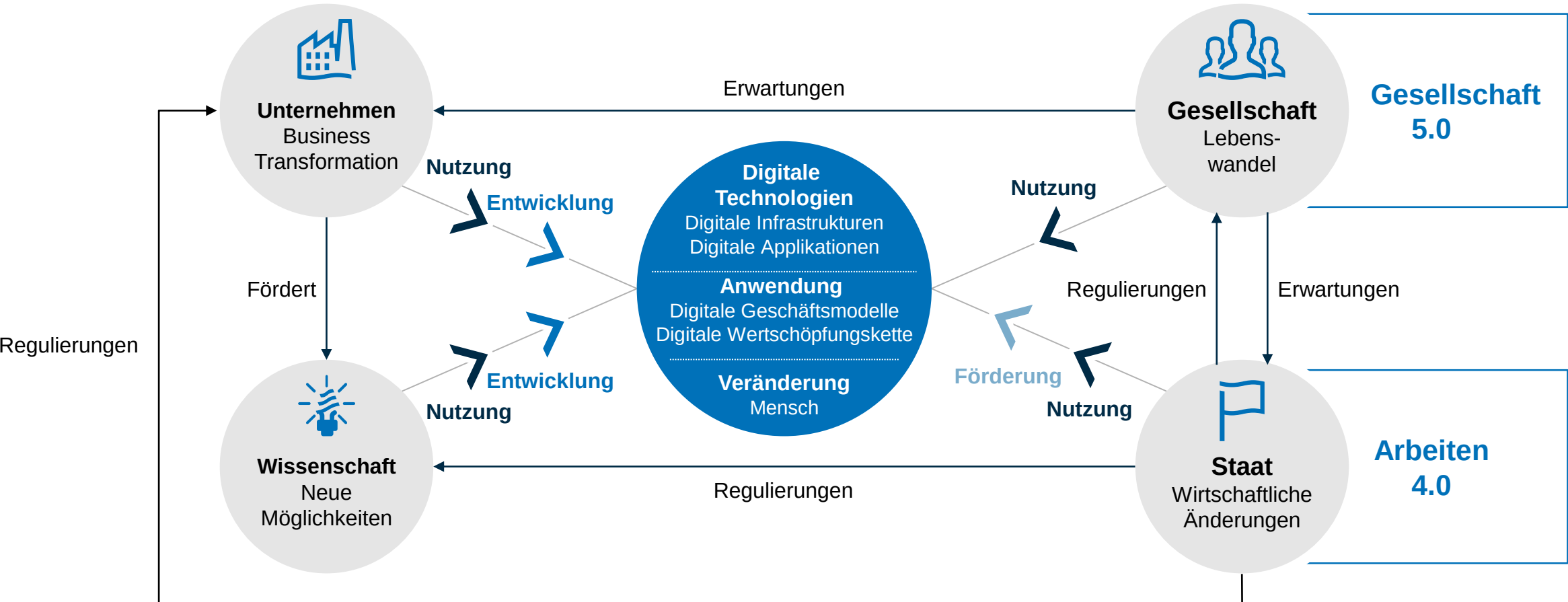
Absicherung der informationellen Selbstbestimmung des Endkunden und Schutz der Kundendaten



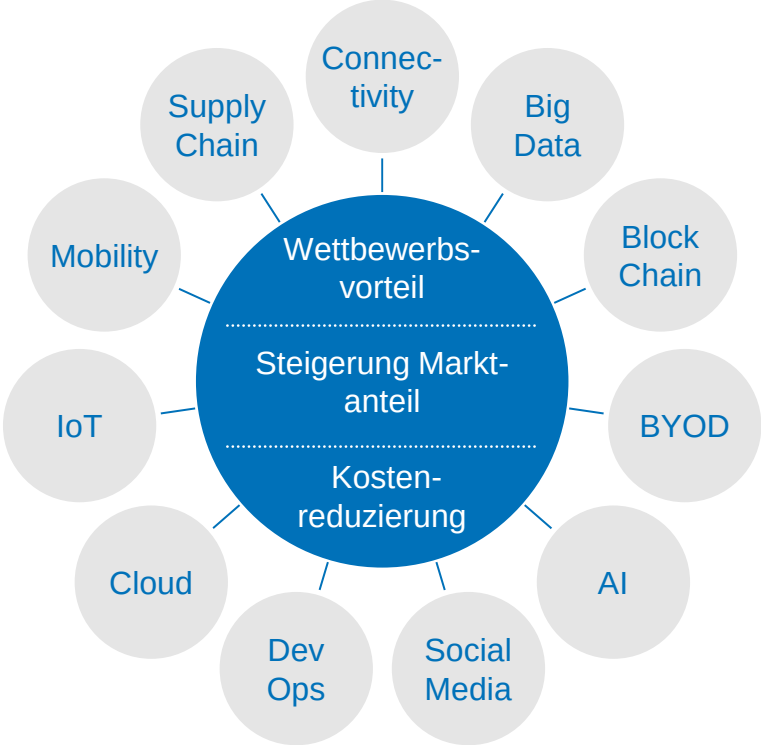
Das Testen von IoT Produkten und Systemen erfordert ein umfassendes und vielfältiges Wissen.

Was versteht man unter der Digitalen Transformation?

Es geht weiter als Industrie 4.0.



Was versteht man unter Business Transformation?



TREIBER ODER NOTWENDIG

Neue Technologie
& Innovation

Anhaltender
Wandel

Neue Kunden und
Interaktionen

Digitale Prozesse

Organisatorischer
Wandel

Neue Partner und
Interaktion

Datengetrieben

Arbeitsweise

Kultureller Wandel



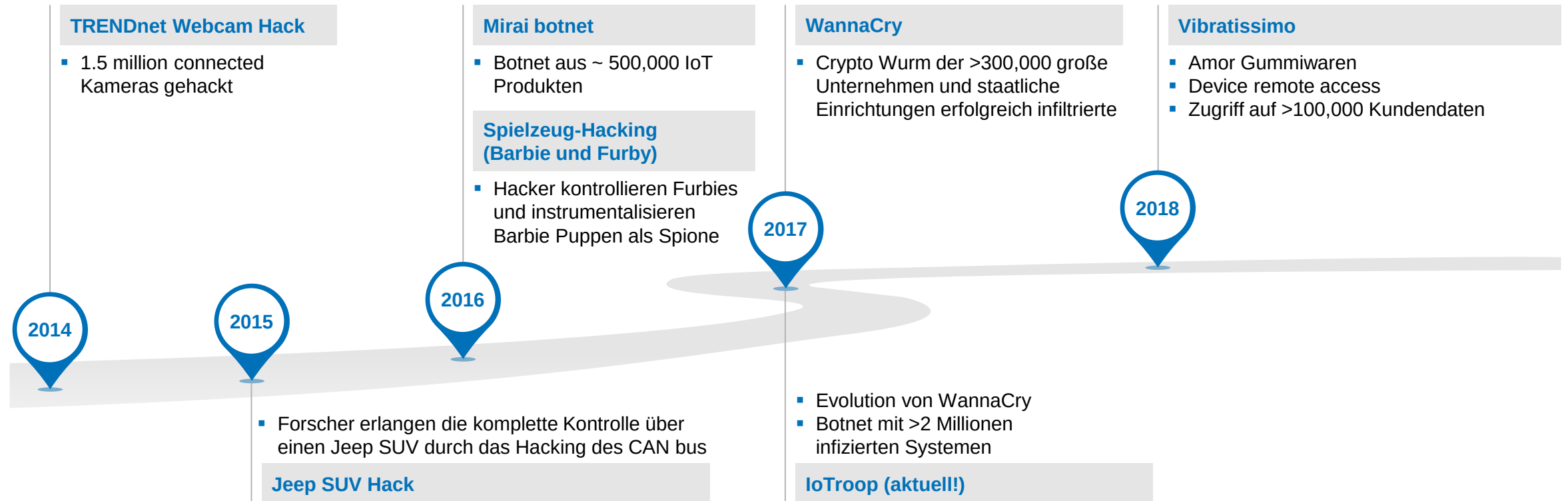
Digitale Transformation heißt vor allem kontinuierlicher Wandel – heute und in der Zukunft!

Cyber Risk in der Digitalen Transformation.



Zusammenfassung kürzlicher Attacken.

Einige Beispiele...



Beispiel: Wie macht man es richtig?

Großstörung bei der Telekom: Die Telekom prüft Hinweise auf Hackerangriff **UPDATE**

28.11.2016 10:52 Uhr – Jürgen Kuri

vorlesen



(Bild: dpa, Martin Gerten)

"Wir haben erste Hinweise darauf, dass wir möglicherweise Opfer eines Hacker-Angriffs geworden sind", hieß es von der Telekom. Seit Sonntagnachmittag haben viele Kunden Probleme mit Internet-Zugang, VoIP und IPTV.

Source: heise.de, 2016

Magenta Security Kongress: Software-Update gegen Telekom-Großstörung im Eiltempo, kein Router gekapert

29.11.2016 14:19 Uhr – Torsten Kleinz

vorlesen



Großstörung bei der Telekom: Was wirklich geschah

30.11.2016 14:12 Uhr – Jürgen Schmidt

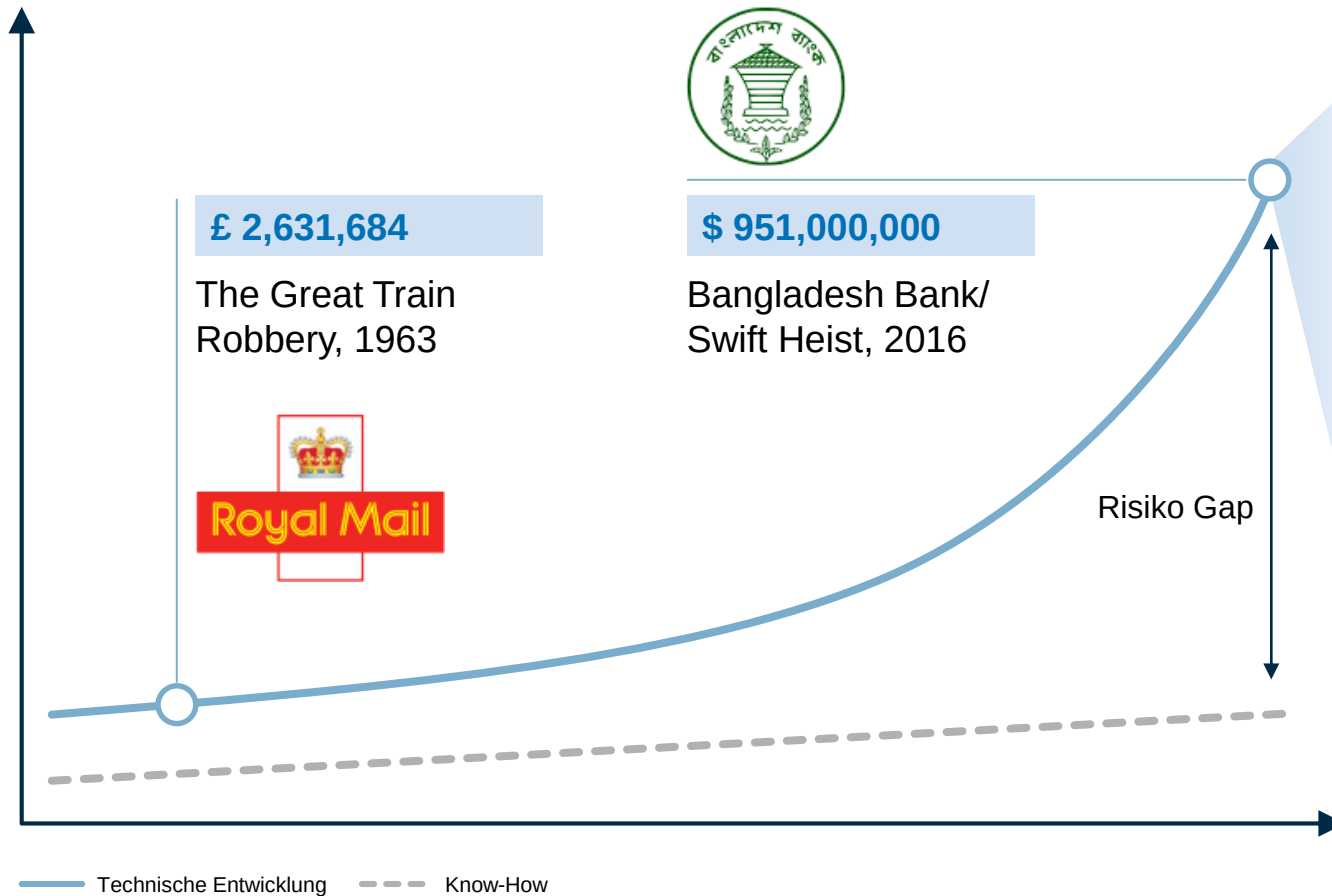
vorlesen



Es ist wichtig, ein System aus einem unsicheren Status zurück in einen sicheren Status zu bringen.

Digitalisierung ist voranschreitend. Unaufhaltsam!

Risiken entwickeln sich auch exponentiell.



INDUSTRIE 4.0

- Automation
- Skalierbarkeit und Interkonnektivität
- AI und Machine Learning
- Agilität



CYBER RISK 4.0

- Automatisierte Attacken
- AI und Machine Learning
- Angreifer sind agil
- Komplexität erhöht Angriffsfläche
- Verwundbarkeit ist fast nicht zu vermeiden

Cyber Risk = Business Risk

Cyber Risk in der Digitalen Transformation

DIGITALE TRANSFORMATION

- Wandel
- Agilität
- Konnektivität
- Mobilität
- Erwartungen (Kunde, Mitarbeiter)
- Wettbewerbsvorteil
- Marktanteil erhalten
- Operationelle Effizienz

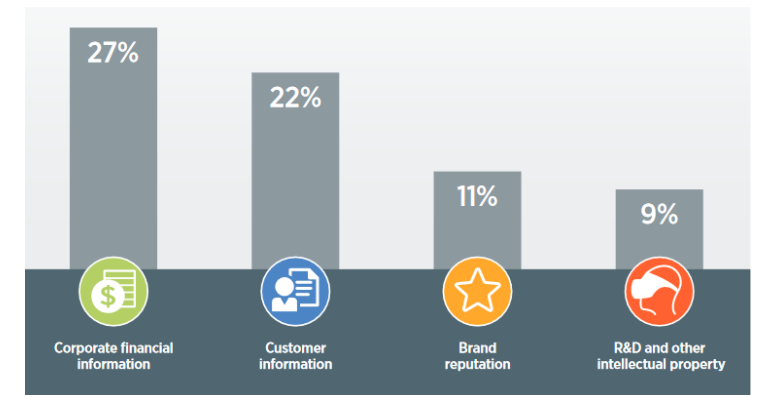


CYBERSECURITY VS. INNOVATION

- Mangel an Innovation
- Mangel an Fähigkeiten
- Wird zu spät involviert
- Beibehaltung der alten Strukturen
- Point Solutions
- Kostenfaktor anstelle von Investment



DIE WICHTIGSTEN ASSETS IM EINSATZ GEGEN EINE ANTACKE



Quelle: Enterprises re-engineer security in the age of digital transformation, Forbes, 2017

Source: Ponemon Institute

Ø Kosten
eines Angriffs

\$4.31M

Ø Kosten pro
gestohlenem
Eintrag

\$225

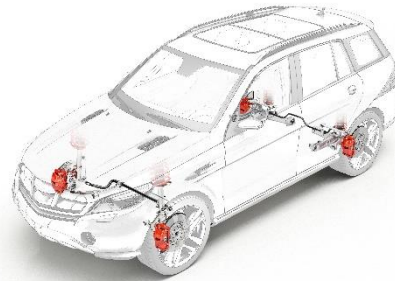
Kosten-
anstieg pro
Eintrag

25%

Cybersecurity in der Digitalen Transformation

Cybersecurity als Enabler und Innovator

Warum brauchen wir Bremsen?



Warum brauchen wir ABS, ESP, EBD, ...?

BUSINESS ENABLER

- Cybersecurity ist nicht nur Kosten und Risiken
- Cybersecurity ist mehr als ein Pflichtprogramm
- Cybersecurity steigert die Effizienz und Produktivität
- Cybersecurity unterstützt die Unternehmensziele
- Beispiel: Offene und hybride Infrastrukturen

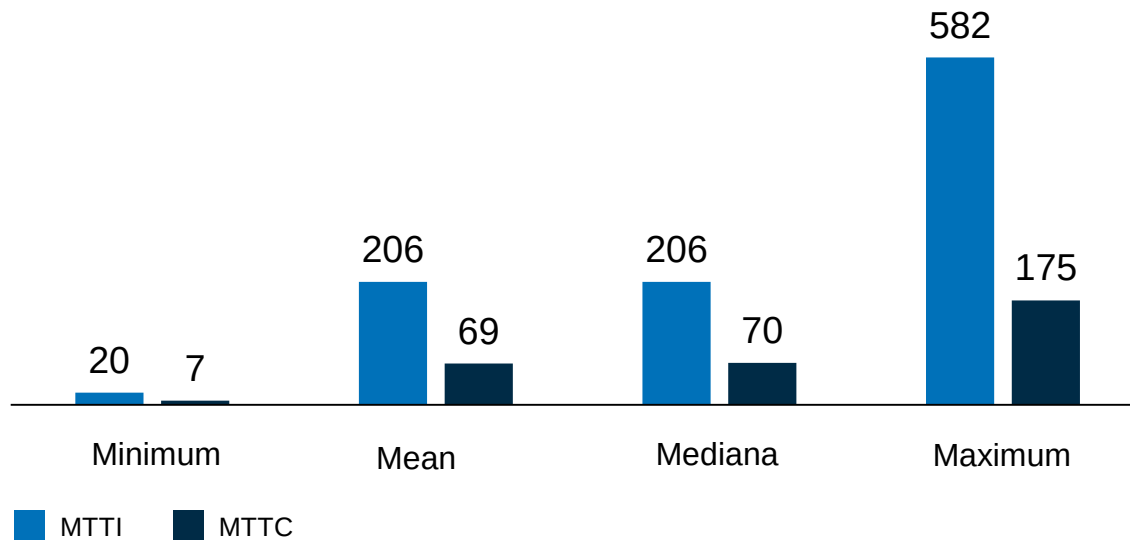
BUSINESS INNOVATOR

- Cybersecurity erfordert einen businessorientierten Wandel
- Cybersecurity kann mehr sein als ein Business Enabler
- Innovative Cybersecurity Kultur ermöglicht schnelleres Wachstum
- Unterstützung und Adaption von neuen Technologien wie bspw. Blockchain
- Beispiel: Sichere Digitale Identität

Cybersecurity in der Digitalen Transformation

Cybersecurity als Enabler und Innovator – Innovationslücke

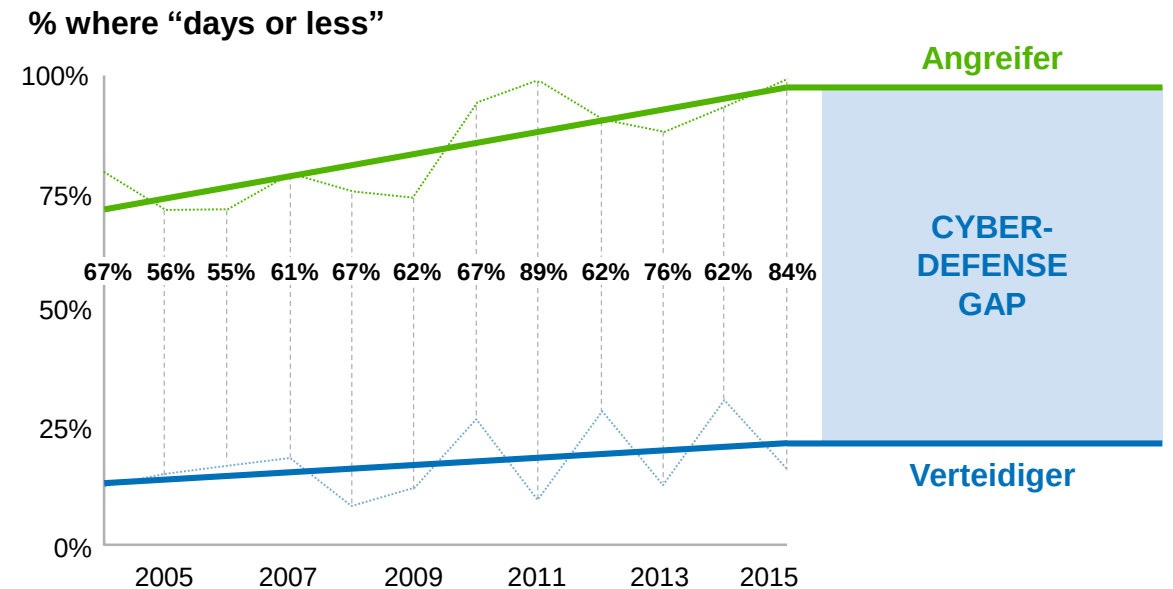
KOSTEN UND ZEIT FÜR SANIERUNG SIND HOCH UND STEIGEND²



2016: im Durchschnitt kostete es die Befragten **242 Tage zur Aufdeckung einer Attacke durch einen bösartigen Angreifer** und **weitere 99 Tage um sie einzudämmen**.

¹ Verizon DBIR | ² Ponemon Institute

VERTEIDIGER VERLIEREN DEN INNOVATIONS-KAMPF¹



Ø Kosten eines Angriffs

\$4.31M

Ø Kosten pro gestohlenem Eintrag

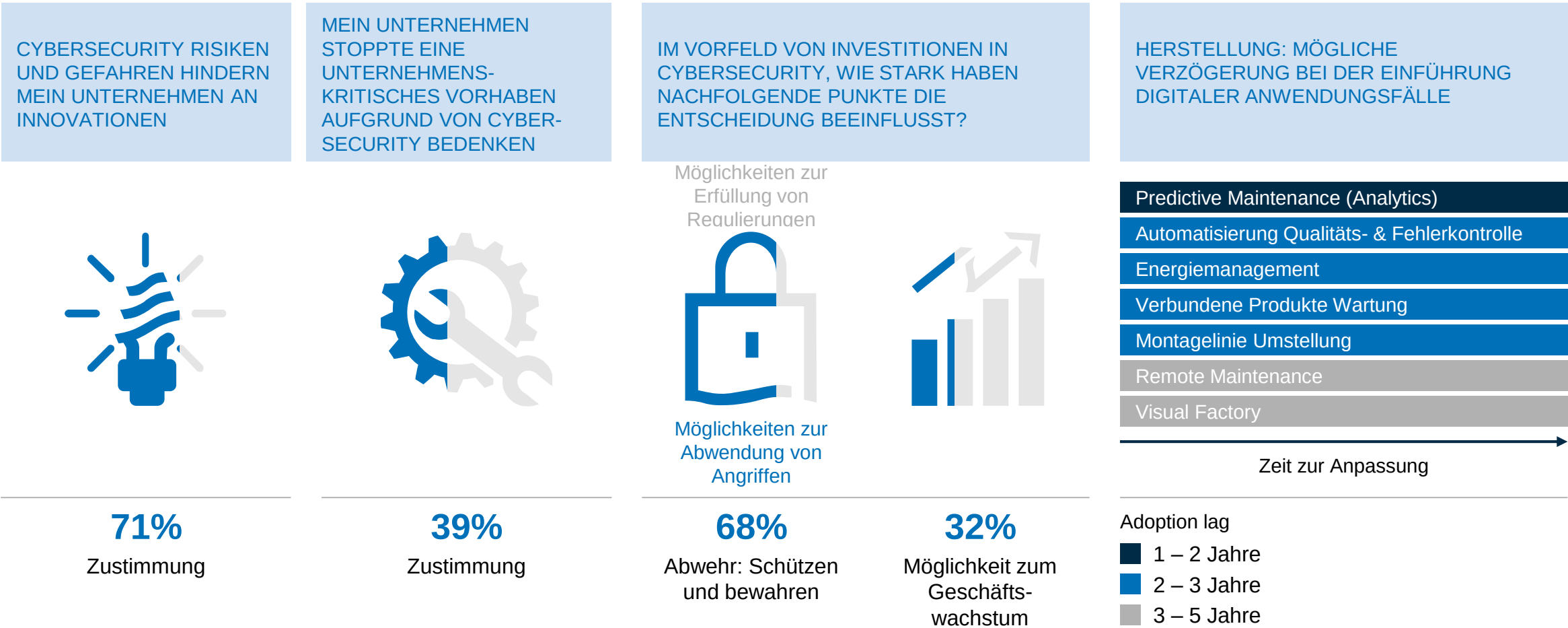
\$225

Kostenanstieg pro Eintrag

25%

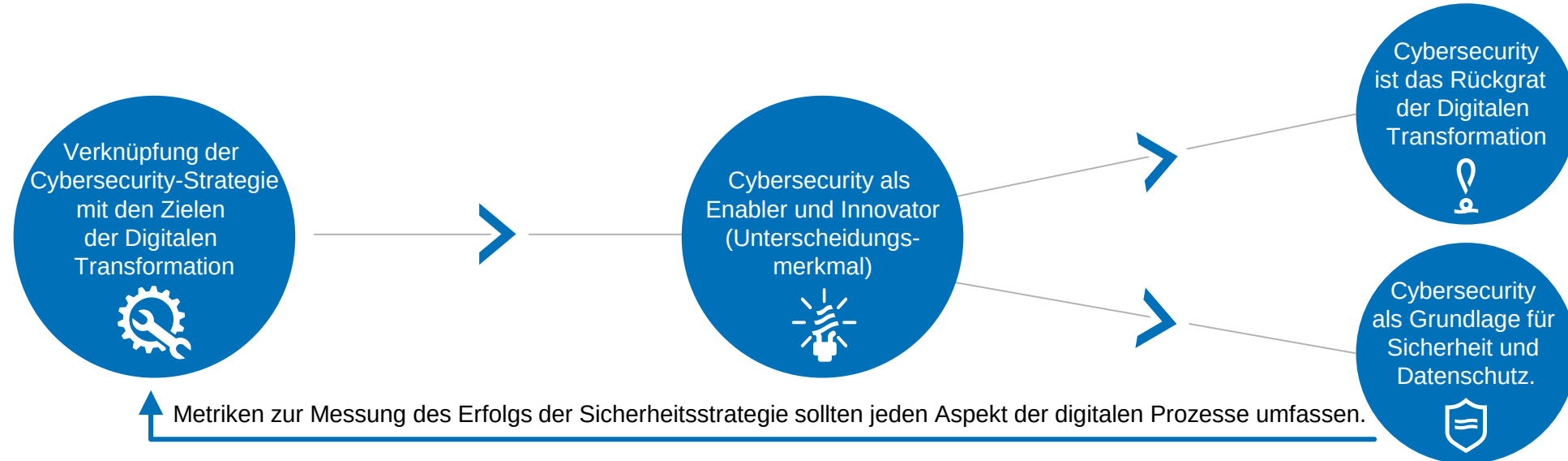
Cybersecurity in der Digitalen Transformation

Cybersecurity als Enabler und Innovator



Source: Cybersecurity as a growth advantage, Cisco, 2016

Cybersecurity in der Digitalen Transformation



Bis 2025 kann Europa 1,25 Billionen Euro industrielle Wertschöpfung erzielen. Cybersecurity macht mehr als ein Viertel aus (Quelle: BDI, Cisco).

Fähigkeit der Führungsebene, Risiken zu bewerten, ROI zu berechnen und artikulieren.

Die Digitale Transformation sollte von einer klaren und fokussierten Strategie bestimmt werden. Mit Cybersicherheit im Herzen von allem.

Die digitale Transformation hört nie auf, sich zu verändern. So auch nicht Cybersecurity.

Nur 21 Prozent der CISOs (Chief Information Security Officers) erstatten dem CEO oder Board Bericht.

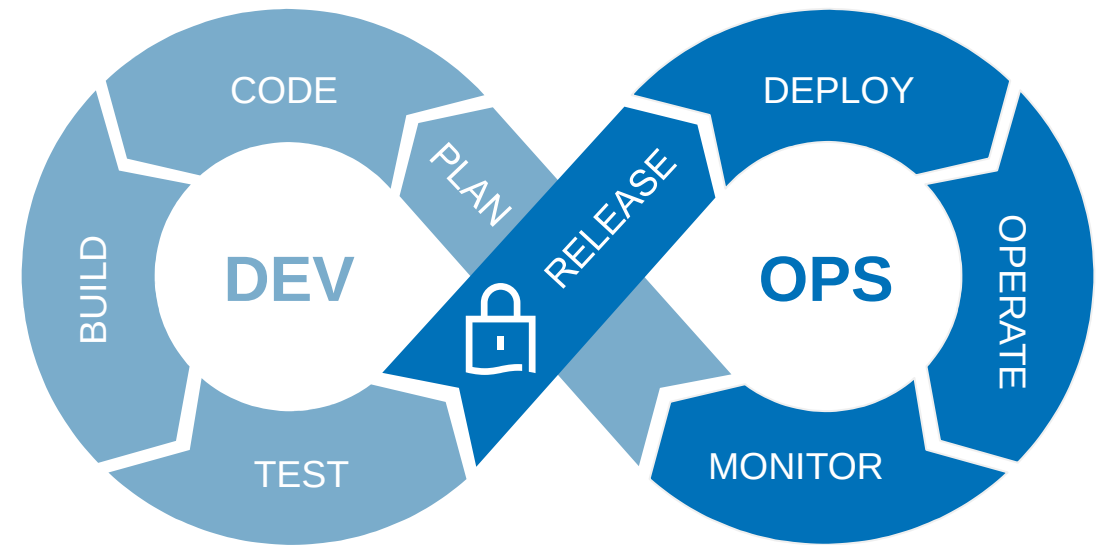
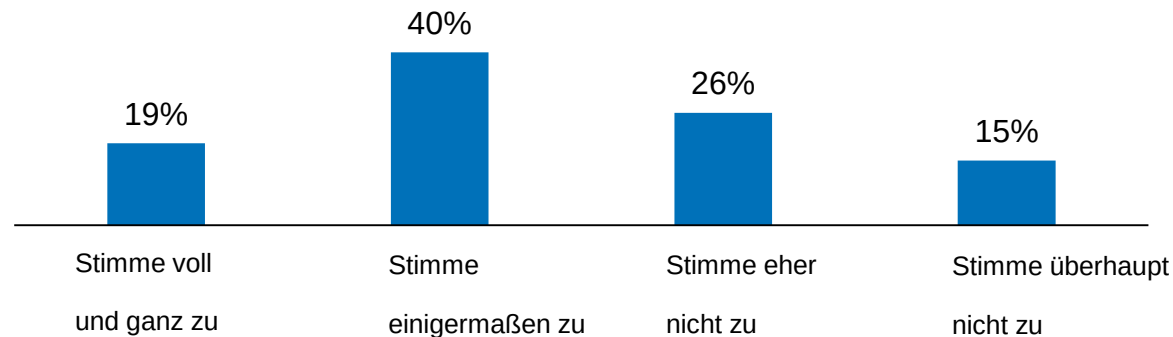
Cybersecurity-Profis müssen Risikoberater werden.

Cybersecurity in der Digitalen Transformation

Beispiel: DevSecOps

SICHERHEIT IST EIN HEMMNIS FÜR AGILITÄT

- Cybersecurity nach links verschieben
- Automatisieren Sie Sicherheitsbewertungen als Teil Ihres Workflows
- Automatisieren Sie alles z.B. automatisierte Sicherheitstests in Komponententests
- Sicherung der Produktinfrastruktur
- Sicherung DevOps Infrastruktur



Source: tripwire.com



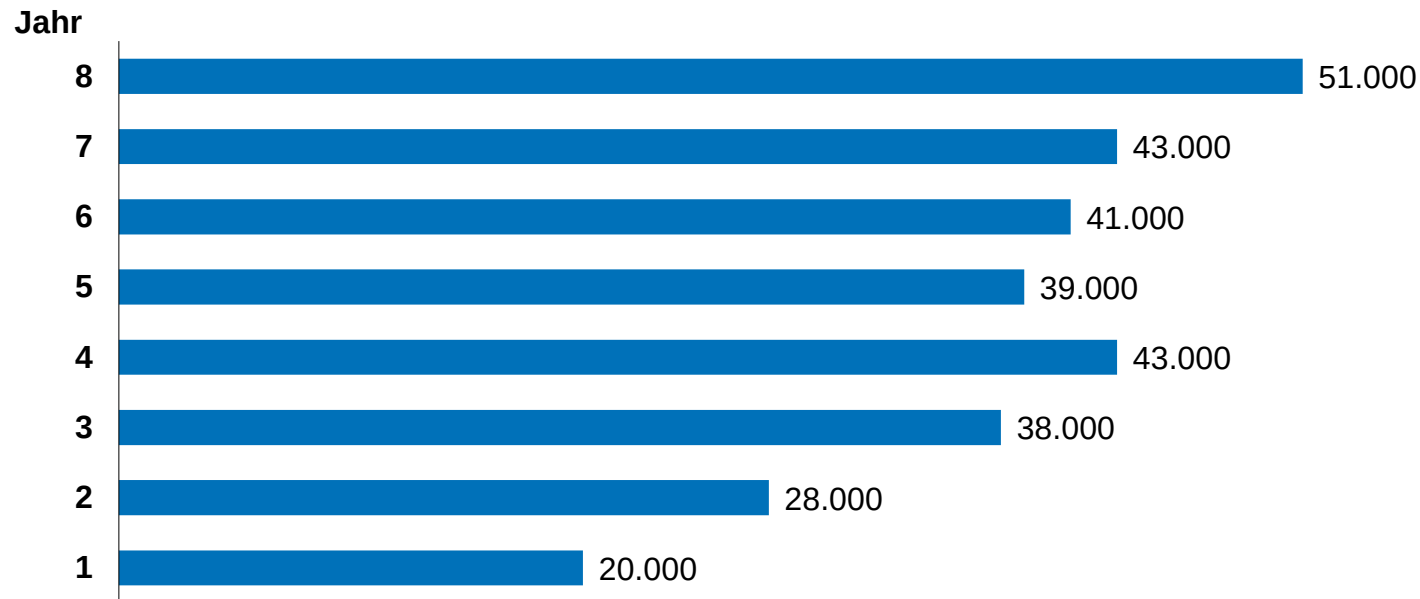
Zerlegen Sie Silos, um Effizienz, Sichtbarkeit, Compliance und Geschwindigkeit zu verbessern.

Source: 2017 DevSecOps Community Survey

Cyber Risk in der Digitalen Transformation

Die Ressourcenlücke in der Cybersicherheit nimmt zu

OFFENE IT-POSITIONEN IN DEUTSCHLAND



Quelle: Bitkom Research 2016

Eine Million Cybersecurity-Jobs ...
werden im Jahr 2016 geschaffen ...
bis zum Jahr 2019 wird ein
Defizit von 1,5 Millionen erwartet.

Quelle: Cisco and Symantec



Cybersecurity-Markt wächst
von 75 Milliarden US-Dollar
im Jahr 2015 auf 170 Milliarden
US-Dollar bis 2020.

Quelle: Gartner.Inc



Die Gehälter für "Cybersecurity"
für "Senior Engineers" liegen
2017 bei \$ 180.000 bis
\$ 220.000 (USA).

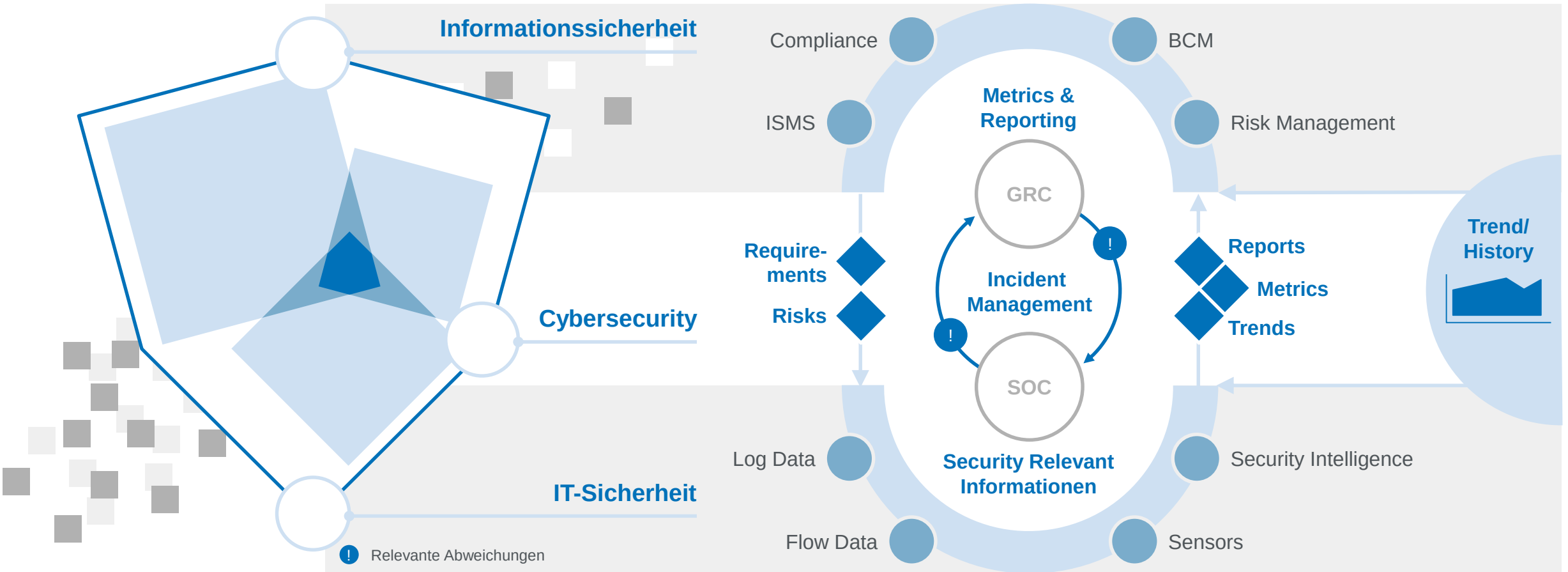
Quelle: CSOnline.com



Die Ressourcenlücke ist die größte Herausforderung in der Cybersecurity derzeit und in Zukunft.

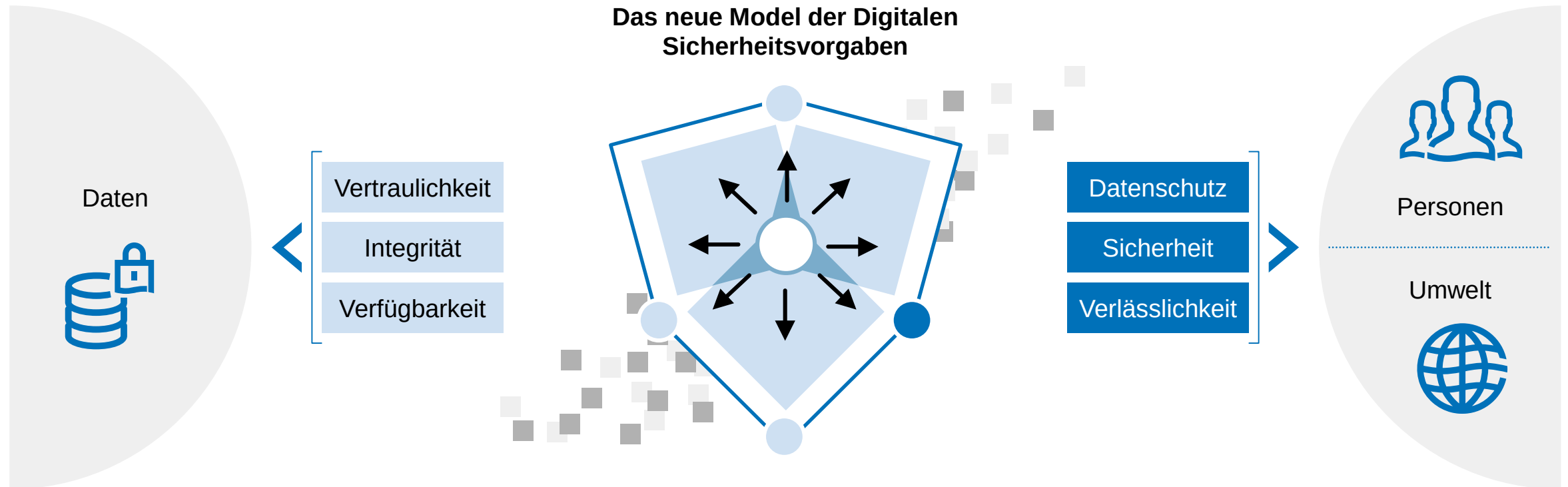
Cybersecurity in der Digitalen Transformation

Verknüpfung der Cybersecurity-Strategie mit den Zielen der Digitalen Transformation



Cybersecurity in der Digitalen Transformation

SICHERHEIT, ZUVERLÄSSIGKEIT UND DATENSCHUTZ: DIGITALE SICHERHEITSVORGABEN



Source: Gartner Security & Risk Management Summit: „Tutorial: Gartner Essentials: Top Cybersecurity Trends for 2016 – 2017“; Earl Perkins, 12 – 13 Sept. 2016

Zusammenfassung. Kernpunkte.



Die digitale Transformation hört nie auf, sich zu verändern. So auch nicht Cybersecurity.



Schließen Sie Cybersecurity in die Strategie zur Digitalen Transformation ein und fordern Sie das Commitment der Führung.



Denke darüber nach, schneller **und** sicherer zu sein als andere.



Hören Sie auf, über Sicherheit als einen verteidigungszentrierten Ansatz nachzudenken, der von Angst verkauft wird.



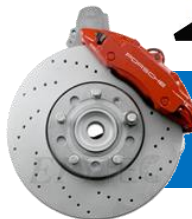
Stellen Sie sich Cybersecurity als Innovationserleichter vor und helfen Sie Ihrem Unternehmen dabei, Fortschritte zu machen.



Cybersecurity ist das Rückgrat der Digitalen Transformation.



Kultureller Wandel ist erforderlich, um Innovationen in der Cybersecurity zu ermöglichen.



Sie brauchen Bremsen, um schneller und sicherer zu fahren!

Vielen Dank für Ihre Aufmerksamkeit!

Wolfgang Kiener

Business Development Manager – Cybersecurity

TÜV Rheinland i-sec GmbH

Am Grauen Stein

51105 Köln



+49 174 1880217



wolfgang.kiener@i-sec.tuv.com

www.tuv.com/informationssicherheit

LEGAL DISCLAIMER

This document remains the property of TÜV Rheinland. It is supplied in confidence solely for information purposes for the recipient. Neither this document nor any information or data contained therein may be used for any other purposes, or duplicated or disclosed in whole or in part, to any third party, without the prior written authorization by TÜV Rheinland.

This document is not complete without a verbal explanation (presentation) of the content.

TÜV Rheinland AG