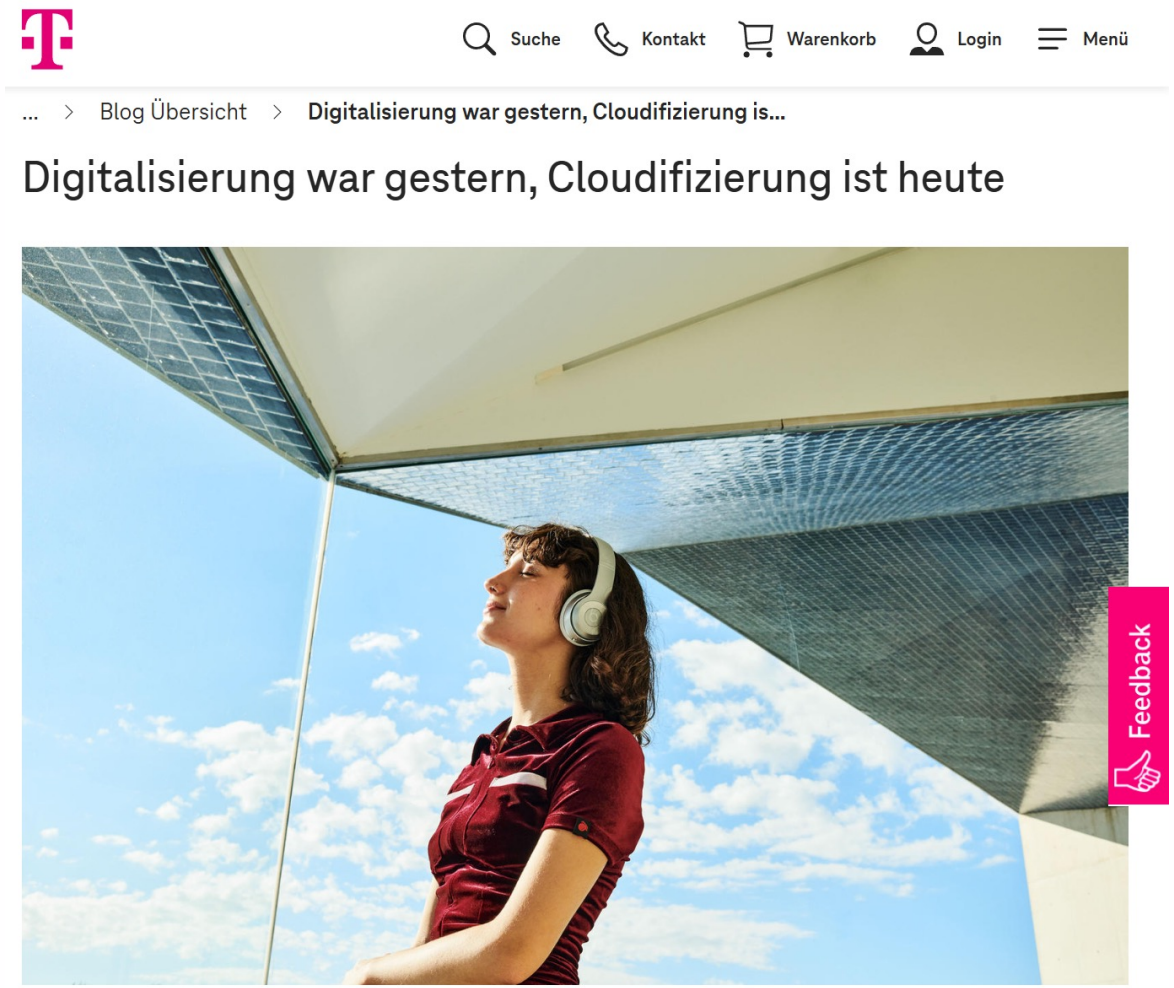
CYBER INTELLIGENCE
.Institute

Warum Security by Design ein Mehrwert für alle ist!

Prof. Dr. Dennis-Kenji Kipker

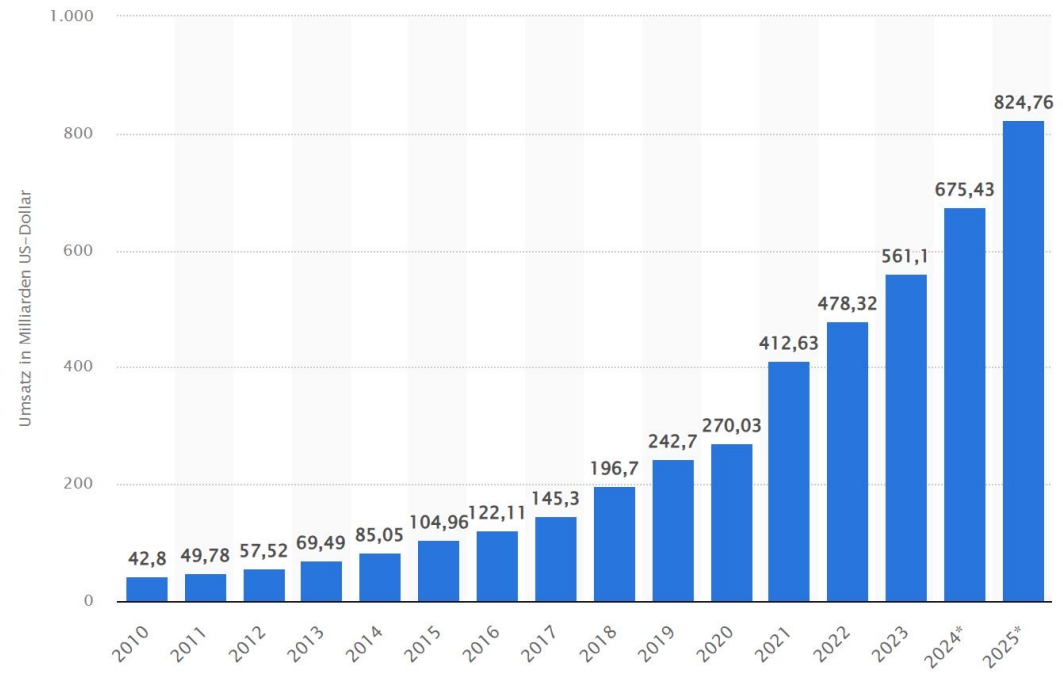
“Digitalisierung war gestern, Cloudifizierung ist heute”



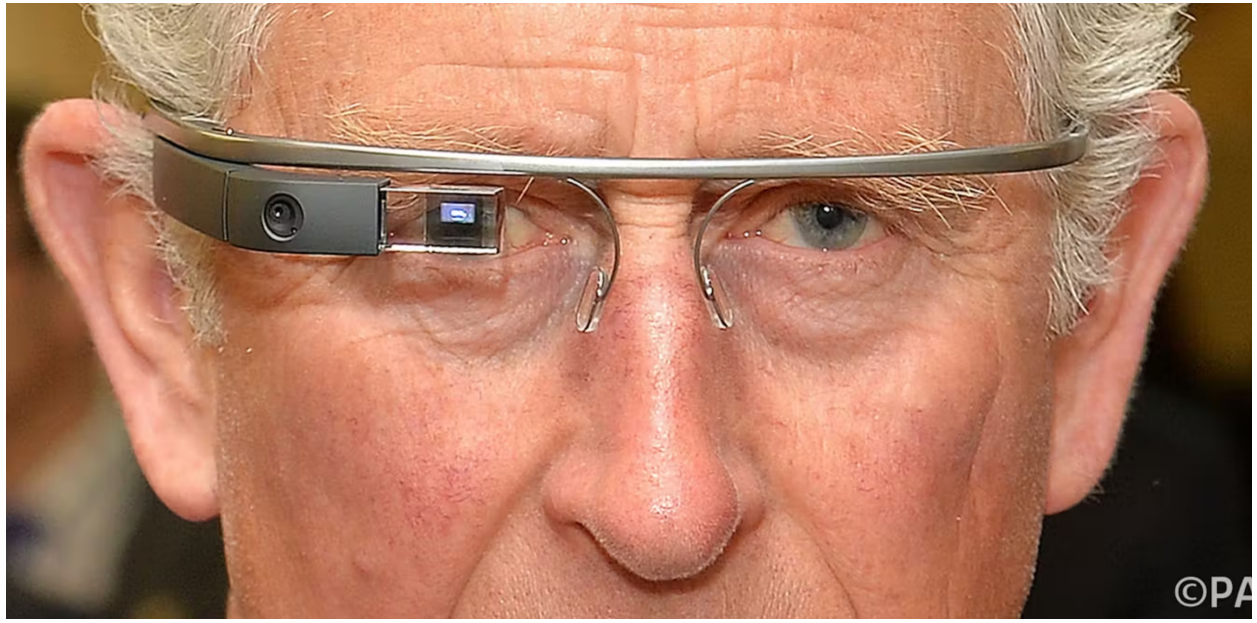
“Digitalisierung war gestern, Cloudifizierung ist heute”

Umsatz mit Cloud Computing weltweit von 2010 bis 2023 und Prognose bis 2025**

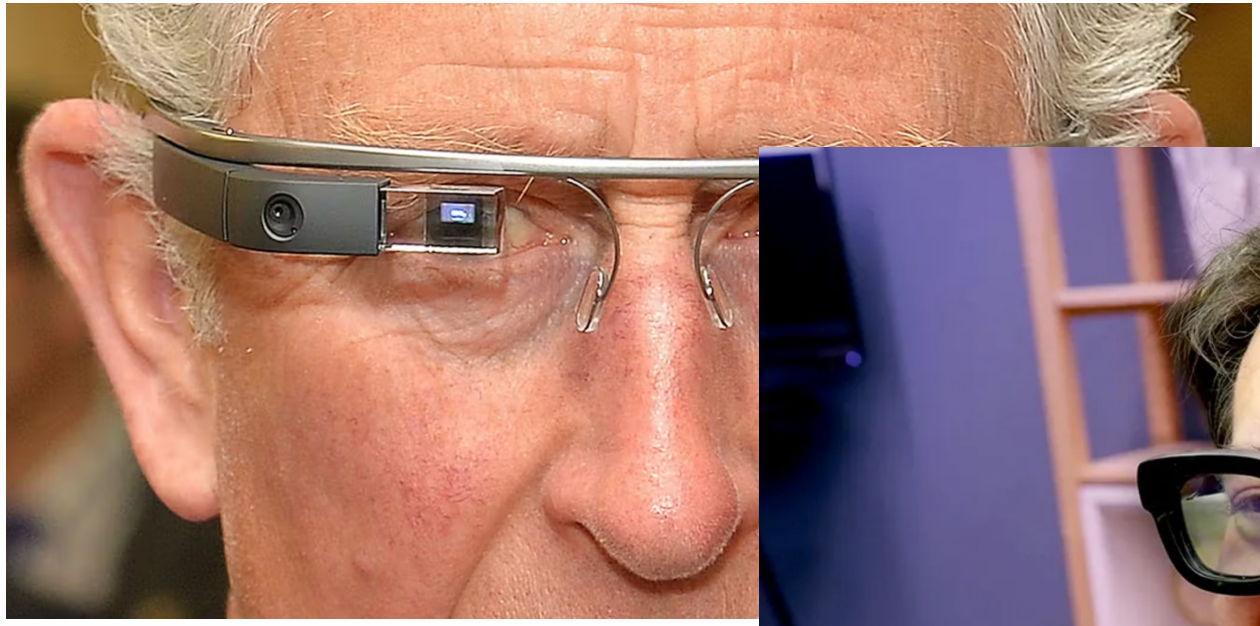
(in Milliarden US-Dollar)



“Digitalisierung war gestern, Cloudifizierung ist heute”



“Digitalisierung war gestern, Cloudifizierung ist heute”



Digitale Lieferkette jenseits technischer Spielereien

Rechtliche Einheiten[1] mit Bezug kostenpflichtiger IT-Dienste als Cloud Services
Insgesamt
und zwar für folgende Zwecke
E-Mail
Office-Anwendungen (Textverarbeitung, Tabellenkallkulation und so weiter)
Betrieb von Unternehmensdatenbanken
Speicherung von Daten
Softwareanwendungen im Finanz- oder Rechnungswesen
CRM-Software
Rechenkapazität zur Ausführung
Enterprise Resource Planning (ERP)-Software
Sicherheitssoftware
Computerplattformen

Digitale Lieferkette jenseits technischer Spielereien

Rechtliche Einheiten[1] mit Bezug kostenpflichtiger IT-Dienste als Cloud Services
Insgesamt
und zwar für folgende Zwecke
E-Mail
Office-Anwendungen (Textverarbeitung, Tabellenkallkulation und so weiter)
Betrieb von Unternehmensdatenbanken
Speicherung von Daten
Softwareanwendungen im Finanz- oder Rechnungswesen
CRM-Software
Rechenkapazität zur Ausführung
Enterprise Resource Planning (ERP)-Software
Sicherheitssoftware
Computerplattformen

Niedersachsen. Klar.

Niedersachsen wird Vorreiter bei der Nutzung von Microsoft Teams in der Landesverwaltung

INNENSTAATSSEKRETÄR MANKE: „DIE ERGEBNISSE DER INTENSIVEN VERHANDLUNGEN DES LANDES MIT MICROSOFT DIENEN ALS BLAUPAUSE FÜR DIE NUTZUNG VON TEAMS IN DER ÖFFENTLICHEN VERWALTUNG“

Der CIO des Landes Niedersachsen, Dr. Horst Baier, hat die Ressorts der Niedersächsischen Landesregierung in dieser Woche (17. KW) über den erfolgreichen Abschluss einer datenschu
enger Abs
kritische ,
umfangre
Datensch

Betriebskosten von Rechenzentren zu erwarten. Der Fachkräftemangel fordert darüber hinaus, dass wir uns mit unseren Mitarbeiterinnen und Mitarbeitern auf die fachlichen Aufgaben konzentrieren. IT aus der Steckdose soll so weit wie möglich eingekauft werden.“

die datenschutzkonforme Umsetzung war die Entwicklung einer auf das Land bezogenen Datenschutzfolgeabschätzung mit einer Risikoabschätzung und diversen umzusetzenden technischen und organisatorischen Maßnahmen. Maßgeblich für die DSGVO-Konformität von Teams war die Entscheidung von Microsoft, die Daten in Europa zu speichern und zu verarbeiten („EU-Boundary“). Alle wesentlichen geforderten Punkte des Landes Niedersachsen wurden berücksichtigt.

Die Abhängigkeiten wachsen – und damit auch die Cybersicherheitsanforderungen?

zdfheute

"Einerseits umfassend Cloudisierung von IT: Das heißt, dass sehr, sehr viele große Konzerne, kritische Infrastrukturen, staatliche Einrichtungen, Finanzinfrastrukturen umfassend auf Microsoft Cloud gesetzt haben, um eben auch Verwaltungsaufwände zu reduzieren." Zusätzlich hätten sie sich ein Tool ins Haus geholt, das auch Cyber Security-Überwachung, Cyber Security-Management unterstütze. Und da sehe man:

> **Allein schon aufgrund dieser großen Zahl an betroffenen IT-Systemen, betroffenen Unternehmen, kann man durchaus sagen, es ist wirklich der absolute Super-GAU, den wir hier im Bereich Cyber Security bislang in den letzten Jahren hatten.**
>
> Dennis-Kenji Kipker, Universität Bremen

Er beschäftige sich jetzt schon viele Jahre mit dem Thema, "und ich habe bislang nichts vergleichbar Schwerwiegendes feststellen können."

Die Abhängigkeiten wachsen – und damit auch die Cybersicherheitsanforderungen?

zdfheute

"Einerseits umfassend Cloudisierung von IT: Das hei
Konzerne, kritische Infrastrukturen, staatliche Einrich
umfassend auf Microsoft Cloud gesetzt haben, um e
zu reduzieren." Zusätzlich hätten sie sich ein Tool ins
Security-Überwachung, Cyber Security-Management

> **Allein schon aufgrund dieser gro
> betroffenen IT-Systemen, betroff
> kann man durchaus sagen, es ist
> Super-GAU, den wir hier im Berei
> bislang in den letzten Jahren hat**
>
> Dennis-Kenji Kipker, Universität Bremen

Er beschäftige sich jetzt schon viele Jahre mit dem T
nichts vergleichbar Schwerwiegendes feststellen kör

COMPUTERWOCHE

News
18 August 2024 • 5 Minuten

Sicherheit

Der Update-Supergau geht in die nächste Runde. CrowdStrike will nicht allein für die Flugausfälle verantwortlich sein und nennt Deltas Vorwürfe „irreführend".

MUSSTE AM BODEN BLEIBEN. DOCH WER SOLL DAFÜR ZAHLEN?

Die Abhängigkeiten wachsen – und damit auch die Cybersicherheitsanforderungen?

zdfheute

"Einerseits umfassend Cloudisierung von IT: Das hei
Konzerne, kritische Infrastrukturen, staatliche Einrich
umfassend auf Microsoft Cloud gesetzt haben, um e
zu reduzieren." Zusätzlich hätten sie sich ein Tool ins
Security-Überwachung, Cyber Security-Management

**Allein schon aufgrund dieser gro
betroffenen IT-Systemen, betroff
kann man durchaus sagen, es ist
Super-GAU, den wir hier im Berei
bislang in den letzten Jahren hat**

Dennis-Kenji Kipker, Universität Bremen

Er beschäftige sich jetzt schon viele Jahre mit dem T
nichts vergleichbar Schwerwiegendes feststellen kör

COMPUTERWOCHE

News
18 August 2024 • 5 Minuten

Sicherheit

Der Update-Supergau geht in die nächste Runde. CrowdStrike will n
für die Flugausfälle verantwortlich sein und nennt Deltas Vorwürfe
„irreführend".

MUSSTE AM BODEN BLEIBEN. DOCH WER SOLL DAFÜR ZAHLEN?

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCS – CLOUD SERVICES SCHEME

EUCS, a candidate cybersecurity certification scheme for cloud services

DECEMBER 2020

Warum wir Security by Design brauchen – und was das bedeutet

Secure by design

7 languages

Article Talk | Read Edit View history Tools

From Wikipedia, the free encyclopedia

> This article **contains instructions, advice, or how-to content**. Please help rewrite the content so that it is more encyclopedic or move it to Wikiversity, Wikibooks, or Wikivoyage. *(June 2022)*

Secure by design, in software engineering, means that software products and capabilities have been designed to be foundationally secure.

Alternate security strategies, tactics and patterns are considered at the beginning of a software design, and the best are selected and enforced by the architecture, and they are used as guiding principles for developers.[1] It is also encouraged to use strategic design patterns that have beneficial effects on security, even though those design patterns were not originally devised with security in mind.[2]

Secure by Design is increasingly becoming the mainstream development approach to ensure security and privacy of software systems. In this approach, security is considered and built into the system at every layer and starts with a robust architecture design.

Warum wir Security by Design brauchen – und was das bedeutet

Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Handreichung "Security by Design"

Leitfaden für die Entscheidungsebene

2 Grundverständnis "Security by Design"

"Security by Design" ist ein Prinzip, das sicherstellt, dass Sicherheitsanforderungen bereits zu Beginn des Entwicklungsprozesses systematisch ermittelt und berücksichtigt werden, um spätere Aufwände zur Behebung von Sicherheitslücken zu verhindern oder zu minimieren.

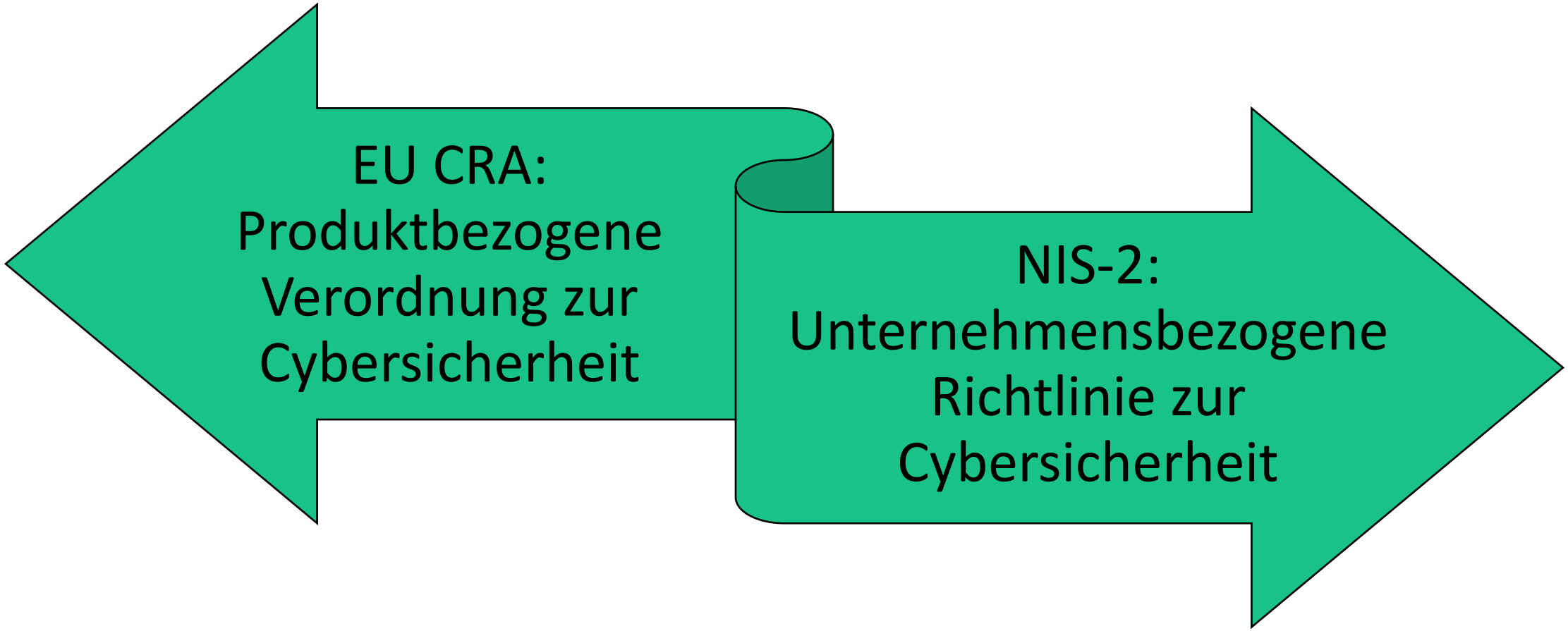
Das "Security by Design"-Prinzip ist nicht neu und im Grunde genommen eine Anleitung zum Bau und Betrieb sicherer Systeme. Es wird seit etlichen Jahren bereits von führenden Unternehmen wie Apple, Microsoft, Google, Adobe, Oracle etc. praktiziert. Es kann und sollte komplementär mit anderen Prinzipien (z.B. "Privacy by Design") umgesetzt werden.

Hersteller von digitalisierten Produkten, Prozessen und Dienstleistungen werden mit "Security by Design" in die Lage versetzt, gesetzliche und regulatorische Vorgaben zur IT-Sicherheit sowie diesbezügliche marktübliche und kundenspezifische Anforderungen einzuhalten und ggf. entsprechende Zertifizierungen zu erhalten.

"Security by Design" ist ebenso eine unabdingbare Voraussetzung, um Gefährdungen der Betriebssicherheit (functional safety) von Produkten und Diensten durch Sicherheitslücken abzuwehren. Ebenso ist die Einhaltung von "Security by Design"-Prinzipien, die Grundvoraussetzungen für die Gewährleistung von "Privacy by Design"-Prinzipien, die zum Schutz der Privatsphäre bei Verarbeitung personenbezogener Daten von der EU-DSGVO gefordert werden.

"Security by Design" ist für Unternehmen kein "nice to have", sondern zwingendes "Muss", um mit Produkten, Prozessen und Dienstleistungen erfolgreich in den Markt einzutreten, am Markt agieren und bestehen zu können. Der Erfolg des herstellenden bzw. anbietenden und/oder betreibenden Unternehmens hängt essenziell davon ab, dass die "Security by Design"-Prinzipien über den gesamten Lebenszyklus aktiv und konsequent angewandt werden.

NIS-2 und CRA als normative Anknüpfungspunkte für Security by Design



Security by Design nach NIS-2

Risikomanagementmaßn

(1) Besonders wichtig
eignete, verhältnismäßige u
nach Absatz 2 konkretisiert
tät und Vertraulichkeit der i
die sie für die Erbringung i
cherheitsvorfällen möglichs
der Maßnahmen nach Satz
richtung, die Umsetzungsk
cherheitsvorfällen sowie ihr
rücksichtigen. Die Einhaltu
dokumentieren.

(2) Maßnahmen nach
gigen europäischen und in
gefahrenübergreifenden An
umfassen:

1. Konzepte in Bezug au
technik,

2. Bewältigung von Siche

3. Aufrechterhaltung des
einem Notfall, und Kris

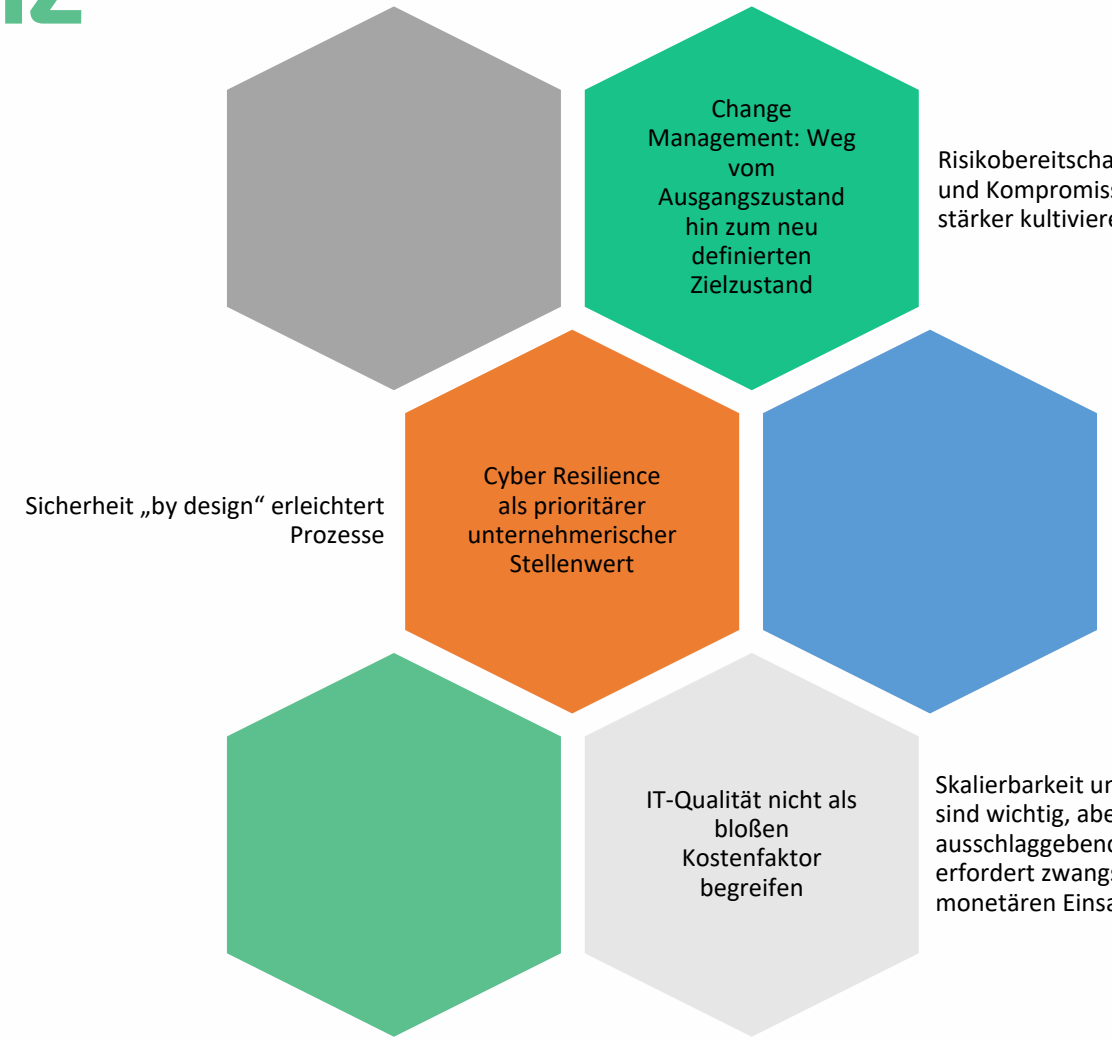
Risikomanagementmaßnahmen-Bereiche
1. Leitungsorgane
2. Sicherheitsrichtlinien
3. Risikomanagement
4. Verwaltung von Vermögenswerten
5. Personalwesen
6. Grundlegende Cyberhygienemaßnahmen und Cybersicherheitsschulungen
7. Sicherheit von Lieferketten
8. Zugangssteuerung
9. Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung
10. Kryptographie
11. Umgang mit Cybersicherheitsvorfällen
12. Betriebskontinuitäts- und Krisenmanagement
13. Umgebungsbezogene und physische Sicherheit

Stand von Wissenschaft und Technik

Security by Design nach CRA

1.	2.	3.	4.	5.
Produkte mit digitalen Elementen (Hardware/Software)	„Security by Design“ als Lebenszyklus-anforderung (EoL)	Risikobewertung und Dokumentations-pflichten	Schutz der Lieferkette unter Einbeziehung von Produkten aus Drittstaaten	Pflicht zu Sicherheits-aktualisierungen „by default“

Security by Design als zentrales Element der digitalen Resilienz



Vielen Dank!

Prof. Dr. Dennis-Kenji Kipker

cyberintelligence.institute
Research Director

MesseTurm
Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.
GERMANY

dennis.kipker@cyberintelligence.institute