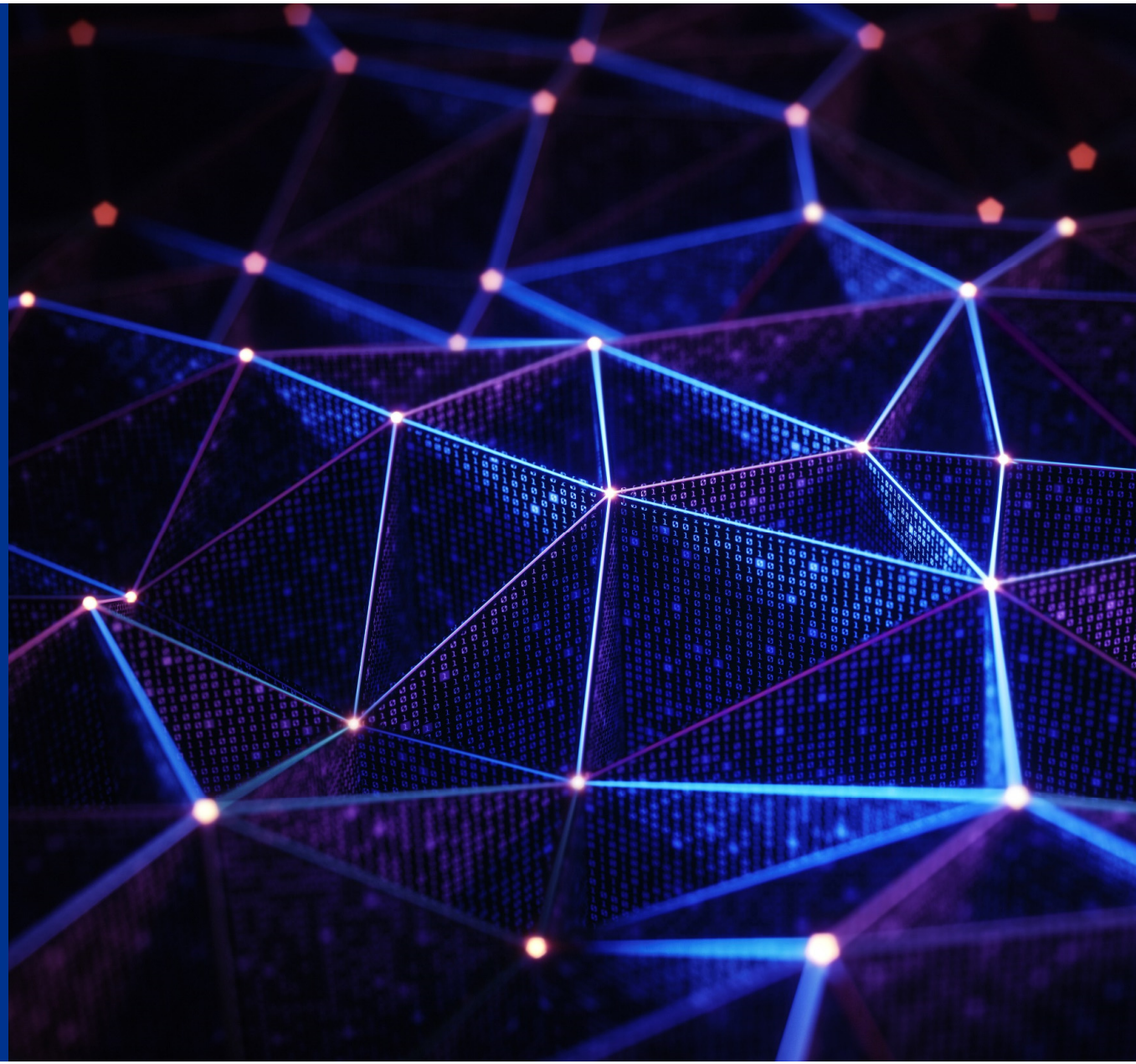
Lieferkette: Wie Cyber-Security von adäquater Zusammenarbeit abhängt

Nur durch eine sehr gute Zusammenarbeit in der IT-Lieferkette ist Null-Fehler-Sicherheit möglich

Hans-Peter Fischer, Dr. Frank Damm

-

18.03.2022



1 **Die Lieferketten – Stand der Dinge**

2 **Die Beteiligten und ihr Zusammenwirken in der Lieferkette**

3 **Ziel: Null-Fehler-Sicherheit**

1 **Die Lieferketten – Stand der Dinge**

2 Die Beteiligten und ihr Zusammenwirken in der Lieferkette

3 Ziel: Null-Fehler-Sicherheit

Die Lieferketten – Stand der Dinge

Cyber Security erfordert Konsistenz

Unternehmen A
- Eigene Interessen
- Eigener Sicherheitsbedarf
- Eigenes ISMS
- Eigene Policies
- Eigene Governance Schemata
- Eigene Ziele

Unternehmen B
- Eigene Ziele
- Eigene Interessen
- Eigener Sicherheitsbedarf
- Eigenes ISMS
- Eigene Policies
- Eigene Governance Schemata

Unternehmen C
- Eigene Ziele
- Eigene Interessen
- Eigener Sicherheitsbedarf
- Eigenes ISMS
- Eigene Policies
- Eigene Governance Schemata

Unternehmen D
- Eigene Ziele
- Eigene Interessen
- Eigener Sicherheitsbedarf
- Eigenes ISMS
- Eigene Policies
- Eigene Governance Schemata

Beispiele für Vorgehensweisen

O-ESA

SABSA

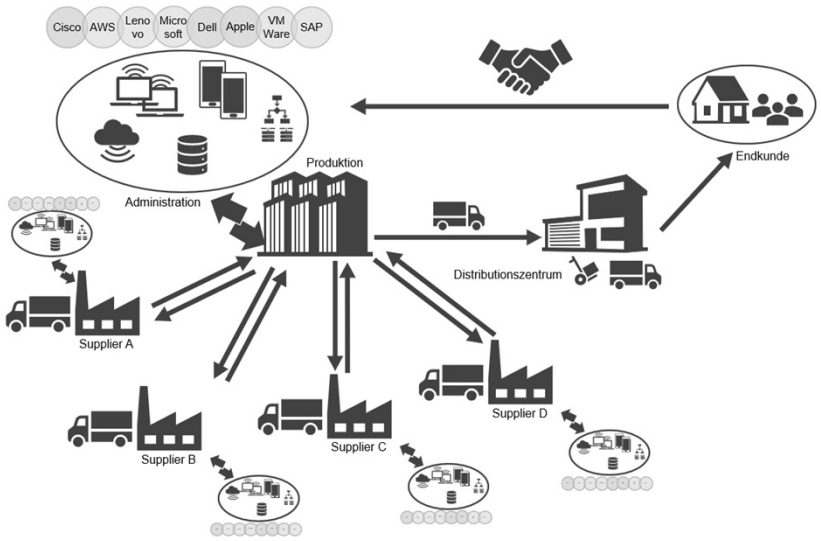
Problem:
Ein unternehmensübergreifend einheitlicher Sicherheitsstandard lässt sich so nicht abbilden.

Die Lieferketten – Stand der Dinge

In einem mittelgroßen Unternehmen finden wir in der IT-Lieferkette leicht 50 bis 100 Beteiligte.

Um die heutige Komplexität der IT-Lieferkette zu veranschaulichen, betrachten wir beispielhaft ein mittelgroßes produzierendes Unternehmen mit Fertigungsstätten in drei Ländern.

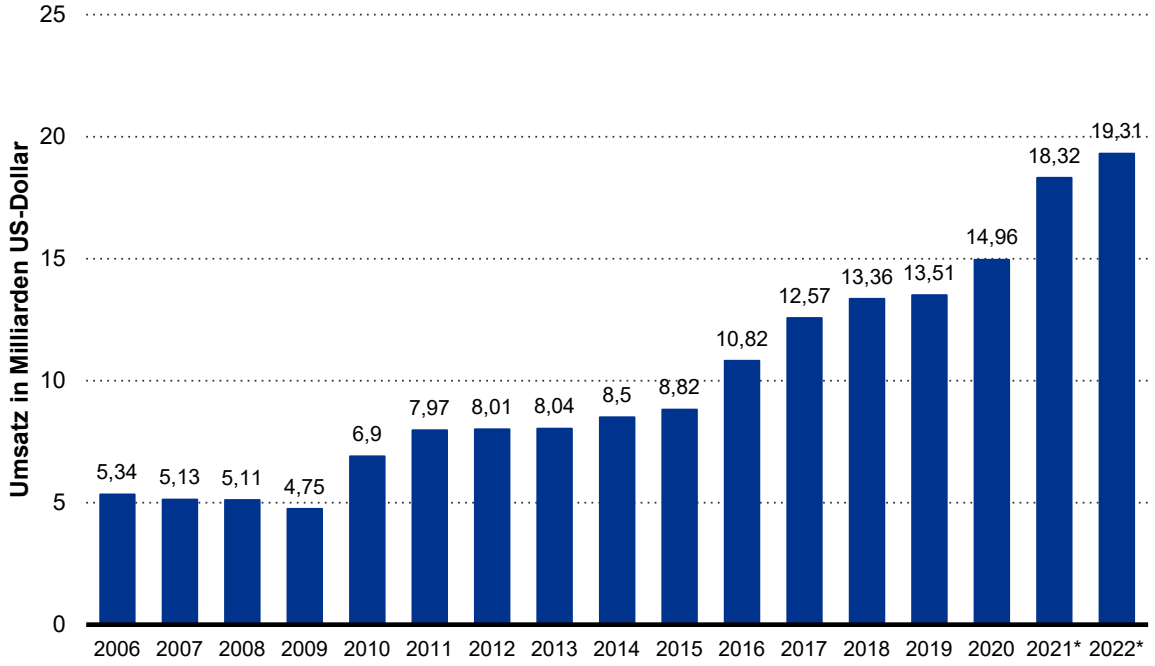
Tatsächlich brauchen Unternehmen für verschiedene Zwecke jeweils mehrere IT-Komponenten und so häuft sich auch die Anzahl der involvierten IT-Hersteller:



IT-Komponenten für:	Anzahl der IT-Hersteller
5 Produktionslinien und je 2 IT-Hersteller (Fertigung)	10
Standardsoftwarepakete	5
Selbstentwickelte Individualsoftware	1
Clients und Server	2
Betriebssystem, Middleware, Standardanwendungen	3
Switches und Router	2
Notebooks und Smartphones	9
Virtualisierungsschicht	1
SaaS in der Cloud des Herstellers	4
SaaS innerhalb der eigenen Cloud	1
SaaS in der public Cloud (Hyperscaler)	2
Summe IT-Hersteller im eigenen Unternehmen	**40**
IT-Hersteller bei Lieferanten und Kunden	**10 bis 60**

Letzte Woche ist die IT-Lieferkette wahrscheinlich verändert worden.

Umsatz der Halbleiterindustrie weltweit im Bereich Sensoren



Hinweis(e): Weltweit; 2006 bis 2020, * Prognose

Quelle(n): WSTS(2021): Prognose zum Umsatz der Halbleiterindustrie weltweit im Bereich Sensoren in den Jahren 2006 bis 2022*(in Milliarden US-Dollar)*. Statista. Statista GmbH. https://de.statista.com/statistik/daten/studie/150945/umfrage/umsatz-der-halbleiterindustrie-im-bereich-sensoren-aktuatoren/bzw. WSTS; ID 150945

Zunehmende Verbreitung und Vernetzung von IoT-Sensoren

— An den Sensoren entstehen sehr schnell sehr viele Daten.

Parallel dazu:

— Evergreen (wöchentliche und kleine Aktualisierung von Systemen statt jährliche und große Aktualisierung),

— DevOps (verbesserte Softwareentwicklungsprozesse durch enge Zusammenarbeit mit dem IT-Betrieb) und

— agile Organisationen setzen sich immer stärker durch.

Die zunehmende Verbreitung von IT und die Geschwindigkeit der Entwicklung führen dazu, dass die Lieferkette immer häufiger verändert wird.

KPMG

Benutzer spielen eine entschei-dende Rolle für die Cyber-Security

Fehlbedienung führt zu Stillstand

KPMG

Benutzer spielen eine entschei-dende Rolle für die Cyber-Security

Unbefugte Zugriffe und Mitnahme führen zu Datenkompromittierung

KPMG

Benutzer spielen eine entschei-dende Rolle für die Cyber-Security

Durch interne und externe Mitarbeiter

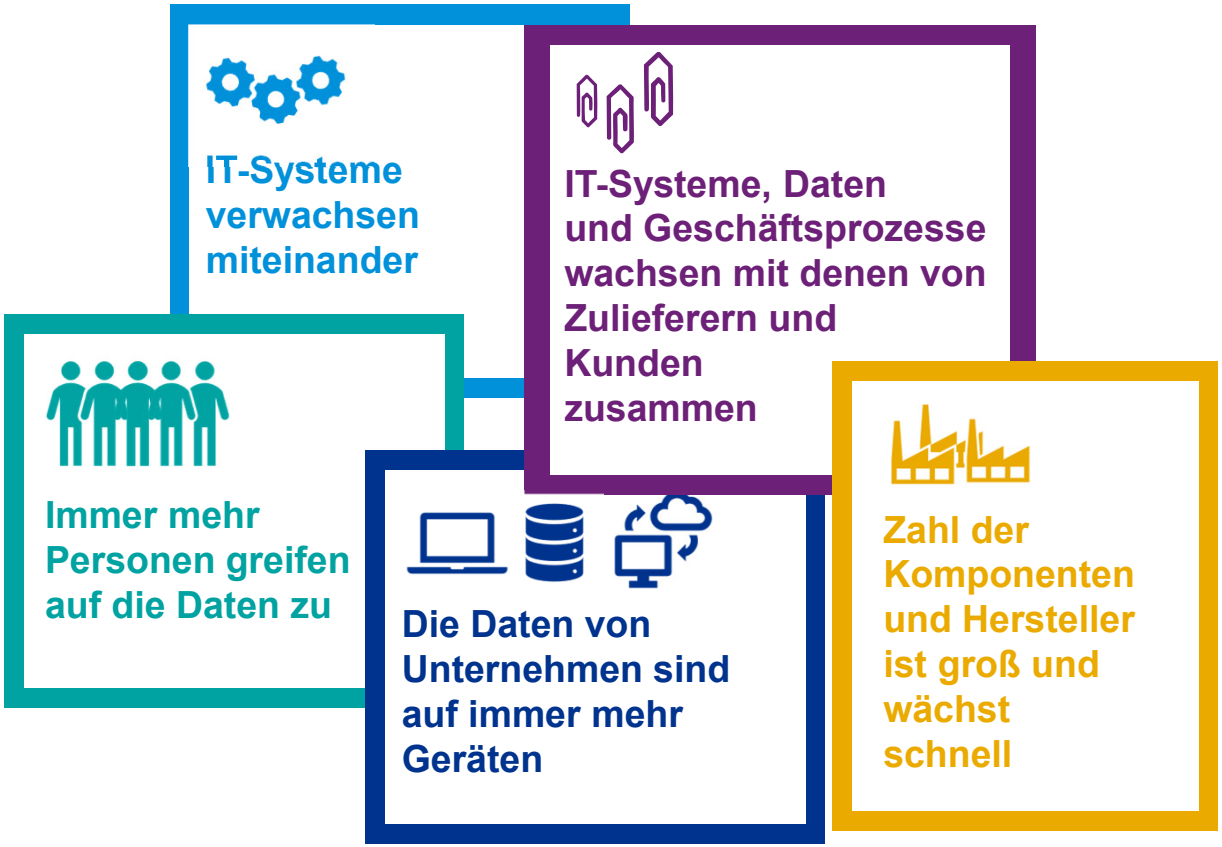
KPMG

Benutzer spielen eine entschei-dende Rolle für die Cyber-Security

Vor Ort oder aus der Ferne

Die Lieferketten – Stand der Dinge

Die Komplexität der IT-Lieferkette steigt durch mehrere Treiber



1 Die Lieferketten – Stand der Dinge

2 **Die Beteiligten und ihr Zusammenwirken in der Lieferkette**

3 Ziel: Null-Fehler-Sicherheit

Die Beteiligten und ihr Zusammenwirken in der Lieferkette

Cyber Security erfordert Zusammenarbeit in der IT-Lieferkette – in jedem Moment des Lebenszyklus

Implementierung der IT-Lieferkette in Geschäftsprozesse

— Mit vielen Beteiligten (Herstellern) müssen Prüf- und Abnahmeverfahren für die IT Komponenten vereinbart werden.
— Im Beispielunternehmen erfordert dies Kommunikation mit bis zu 100 Herstellern!
— Regelmäßiger Austausch über Sicherheitskomponenten ist nötig
— Test & Inbetriebnahme der Komponenten erfordert Kommunikation
— Der Schutz von Daten (Vertraulichkeit & Integrität) erfordert Kommunikation

Betrieb

— Während des Betriebs soll die Zusammenarbeit automatisch erfolgen.
— Das erfordert Performance Messungen & Qualitätskontrolle bei ständig wechselnden Einzelkomponenten.
— Eine standardisierte und änderungsstabile Qualitätskontrolle ist notwendig!

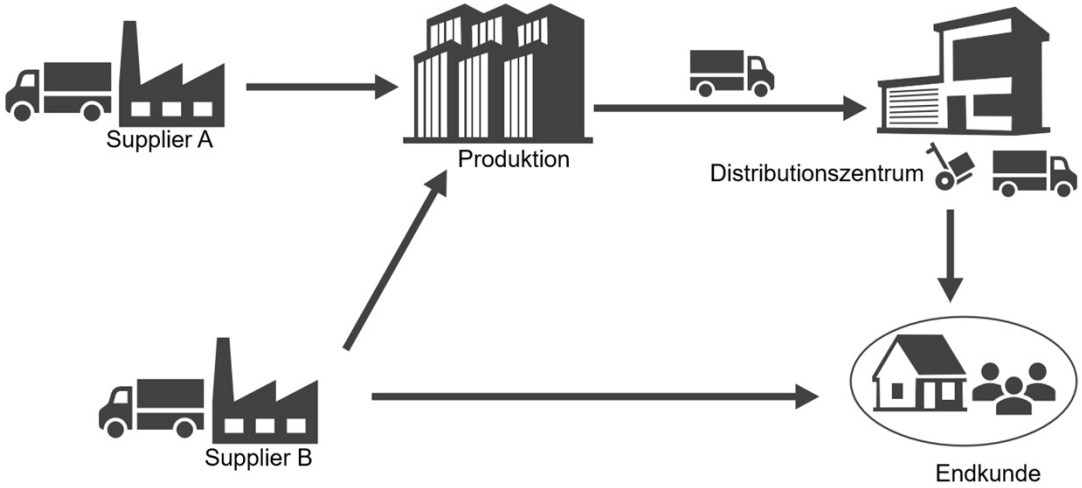
Wartung & Weiterentwicklung

— Viele Beteiligte und die Notwendigkeit von Zusammenarbeit und Kommunikation
  - Schwachstellen von IT-Komponenten ausbessern
  - Agile Software Entwicklung
  - Mehr Komponenten & Hersteller bedeuten auch mehr Risiko

Die Beteiligten und ihr Zusammenwirken in der Lieferkette

Lieferketten sind ständig im Wandel - Jedes Glied hat eigene Interessen

- Die Lieferketten wachsen in kleinen Schritten
- Permanente Wartung & Weiterentwicklung durch neue Glieder bzw. Supplier
- Belastbarkeit trotz wechselnder Glieder benötigt



Die Beteiligten in der Lieferkette haben verschiedene Interessen.
Der Dienstleister in einer Lieferkette kann der Wettbewerber in einer anderen Lieferkette sein.

Die Beteiligten und ihr Zusammenwirken in der Lieferkette

Störung ist nicht gleich Störung.

Die Störung für den Unternehmer

Die Störung für die IT-Abteilung

Die Störung wird sehr unterschiedlich wahrgenommen, was weitere Kommunikation erfordert und Zeit kostet.

Die Beteiligten und ihr Zusammenwirken in der Lieferkette

Störung ist nicht gleich Störung.

Die Störung für den Unternehmer

Frage: Welche Auswirkung hat die Störung auf welchen Geschäftsprozess oder welche Daten?

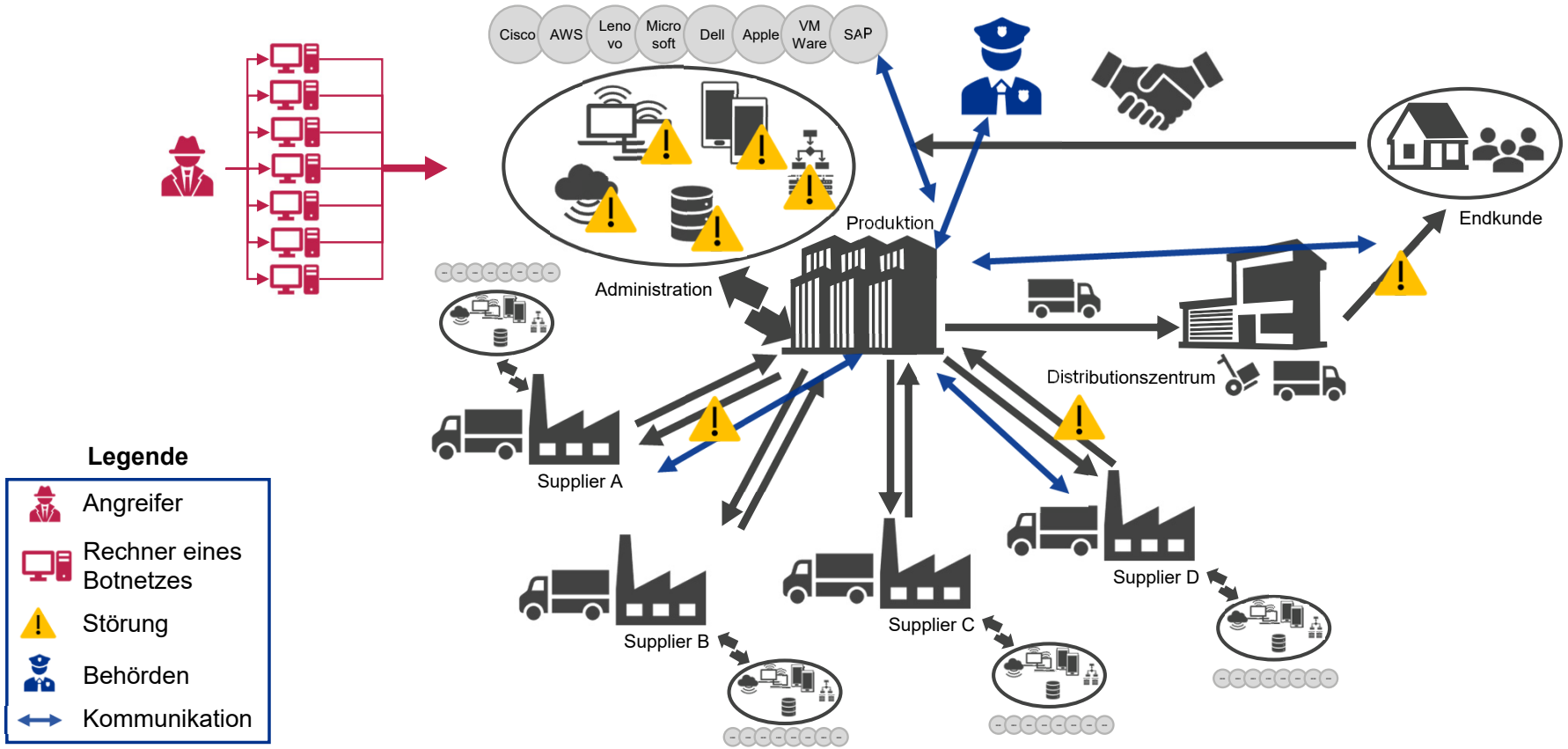
Die Störung für die IT-Abteilung

Frage: Von welcher Technologie wird die Störung verursacht?

Die Störung wird sehr unterschiedlich wahrgenommen, was weitere Kommunikation erfordert und Zeit kostet.

Die Beteiligten und ihr Zusammenwirken in der Lieferkette

Die Bewältigung eines Angriffs auf die Verfügbarkeit erfordert Zusammenarbeit in der IT-Lieferkette



Die Beteiligten und ihr Zusammenwirken in der Lieferkette

Mit der Zahl der IT-Komponenten steigt das Risiko

Was tun, wenn Sicherheitsanforderungen nicht erfüllt werden können, weil:

— eine Komponente fehlerhaft hergestellt wurde

— eine Sicherheitsanforderung dem Hersteller der Komponente nicht bekannt war

— sie zwar richtig hergestellt, aber vom Betreiber falsch eingerichtet oder bedient wurde

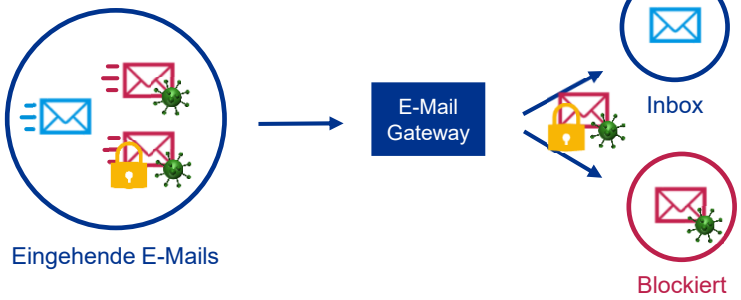
— jede Komponente für sich die Sicherheitsanforderungen erfüllt, aber ihre Komposition nicht mehr?

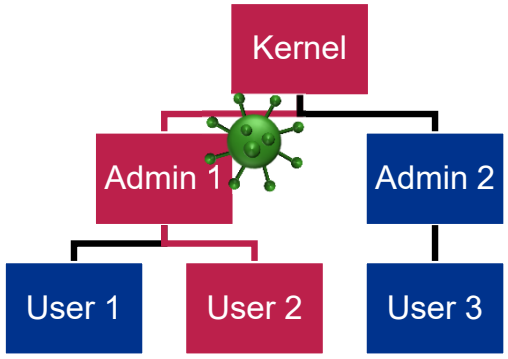
Wechselwirkungen zwischen IT-Komponenten

Komponenten Hersteller

Komponenten Hersteller: Nr.	1	2	3	4	5	...
1			x			
2	x		x		x	
3				x		
4	x		x			
5	x			x		
⋮					x	

x = Cyber Security Herausforderung





Anzahl der Komponenten Hersteller	Anzahl der Möglichkeiten für Sicherheitsrisiken
3	9
4	16
5	25
⋮	⋮
10	100
⋮	⋮
40	1.600
⋮	⋮
100	10.000

Die Beteiligten und ihr Zusammenwirken in der Lieferkette

Das IT-Sicherheitsgesetz berücksichtigt die IT entlang der Lieferkette(a)

§ 2 Abs. 14 Nr. 2 BSIG

(14) Unternehmen im besonderen öffentlichen Interesse sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind und

1. […]
2. die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind **oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind** oder
3. […]

Die Unternehmen im besonderen öffentlichen Interesse […] werden durch die **Rechtsverordnung** […] bestimmt, in der festgelegt wird, welche wirtschaftlichen Kennzahlen maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland […] gehört und **welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für solche Unternehmen von wesentlicher Bedeutung sind.**

§ 8f BSIG

(1) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 sind verpflichtet, […] **alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit** beim Bundesamt vorzulegen, aus der hervorgeht,

[…] welche **Zertifizierungen** […], sonstigen **Sicherheitsaudits** oder […], **welche Prüfgrundlage und welcher Geltungsbereich** hierfür festgelegt wurden oder […], und ob dabei der **Stand der Technik eingehalten** wird.

[…]

(7) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 haben […], die folgenden **Störungen unverzüglich** […] zu **melden**:

1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen **Beeinträchtigung der Erbringung der Wertschöpfung** geführt haben,
2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung führen können.

[…]

Anm.: (a) für bestimmte Unternehmen und bestimmte Zulieferer (siehe §2(14) Nr.2 und §8f BSIG)

Die Beteiligten und ihr Zusammenwirken in der Lieferkette

Beteiligte und ihr Zusammenwirken im Überblick

1 Die Lieferketten – Stand der Dinge

2 Die Beteiligten und ihr Zusammenwirken in der Lieferkette

3 **Ziel: Null-Fehler-Sicherheit**

Ziel: Null-Fehler-Sicherheit

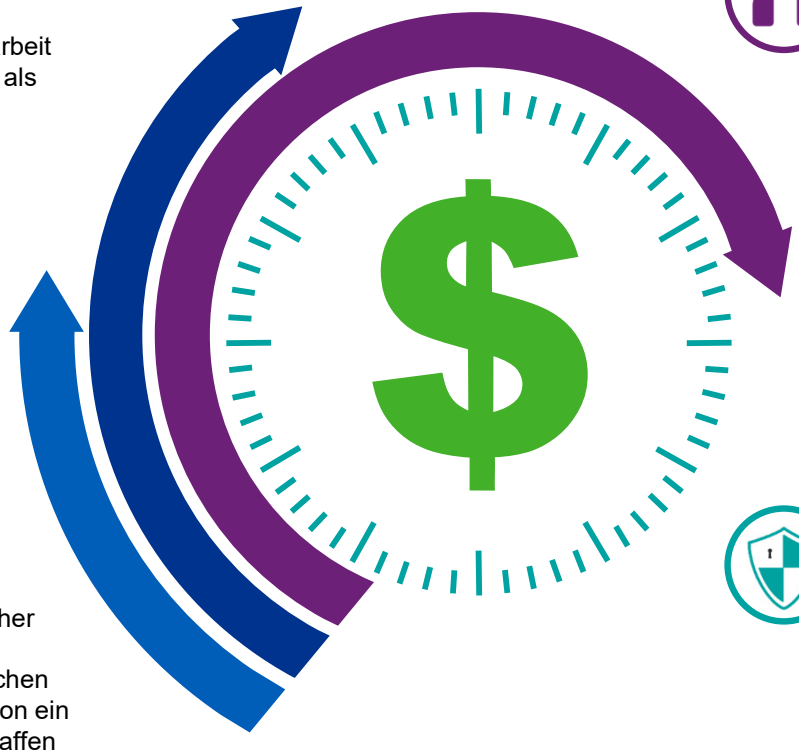
Null-Fehler-Sicherheit – Ein fortlaufender Prozess

Zusammenarbeit

Kommunikation und Zusammenarbeit deutlich vereinfachen und soweit als möglich standardisieren

Sichtweise

Traditionelle Sichtweisen der Lieferkette und des eigenen Unternehmens als Innenwelt und der bedrohenden Außenwelt an die tatsächlich heute gegebene Situation anpassen



Bewusstsein

Negative Konsequenzen schwacher Cyber-Security allen Beteiligten sichtbar und nachvollziehbar machen und zur Verbesserung der Situation ein einheitliches Bewusstsein zu schaffen

Null-Fehler-Sicherheit

Das Zusammenspiel aller drei Komponenten bringt uns der Null-Fehler-Sicherheit näher. Der Weg dort hin ist jedoch ein fortlaufender Prozess.

Ziel: Null-Fehler-Sicherheit

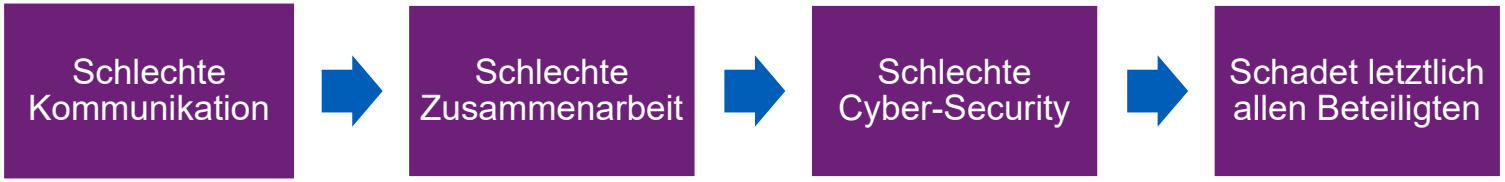
Bewußtsein: Sicherheit als Qualitätsaspekt der Lieferkette

Cyber-Security ist sichtbar, wirtschaftlich spürbar und erfordert ein hohes **Bewusstsein**.

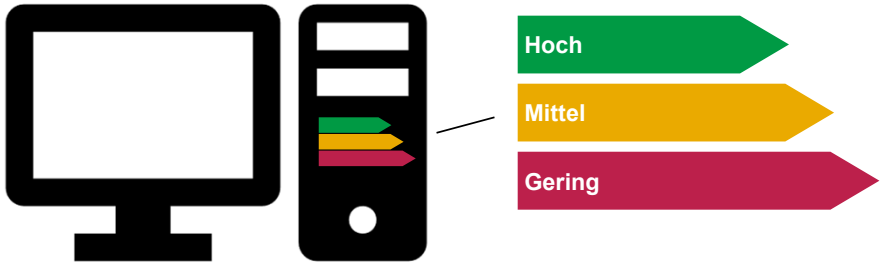
Qualität der Lieferkette,

— kostet kurzfristig mehr Geld,

— aber:



— Eine Security-Skala könnte helfen:



— Wichtig ist, dass alle mitziehen – auch der Endkunde.

Ziel: Null-Fehler-Sicherheit

Zielorientiert - Zusammenarbeit und Kommunikation

Zusammenarbeit und Kommunikation standardisieren?

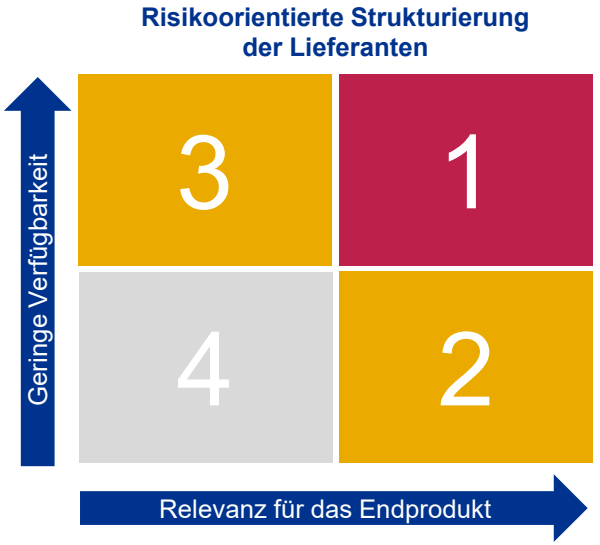
Allgemein gilt:

1. Nur das Unternehmen kennt die Kritikalität der Daten, der Lieferanten und des Geschäftsprozesses.
2. Es können sehr verschiedene Anforderungen an Sicherheit wie etwa Vertraulichkeit, Integrität und Verfügbarkeit bestehen.
3. Es gibt verschiedene Möglichkeiten, IT-Komponenten und Services miteinander zu verbinden.

Daher bedarf es:

— Einigung über notwendige Maßnahmen (Zero Outage Industry Standard)
— Gleiche Sprache und gleiche Struktur (ESARIS)
— Standardisierter Einkauf für alle Lieferanten und Abnehmer
— Risikoorientierte Strukturierung der Lieferanten

Methoden: SABSA, O-ESA, ISO 27000, Cobit und Best Practises des ISF



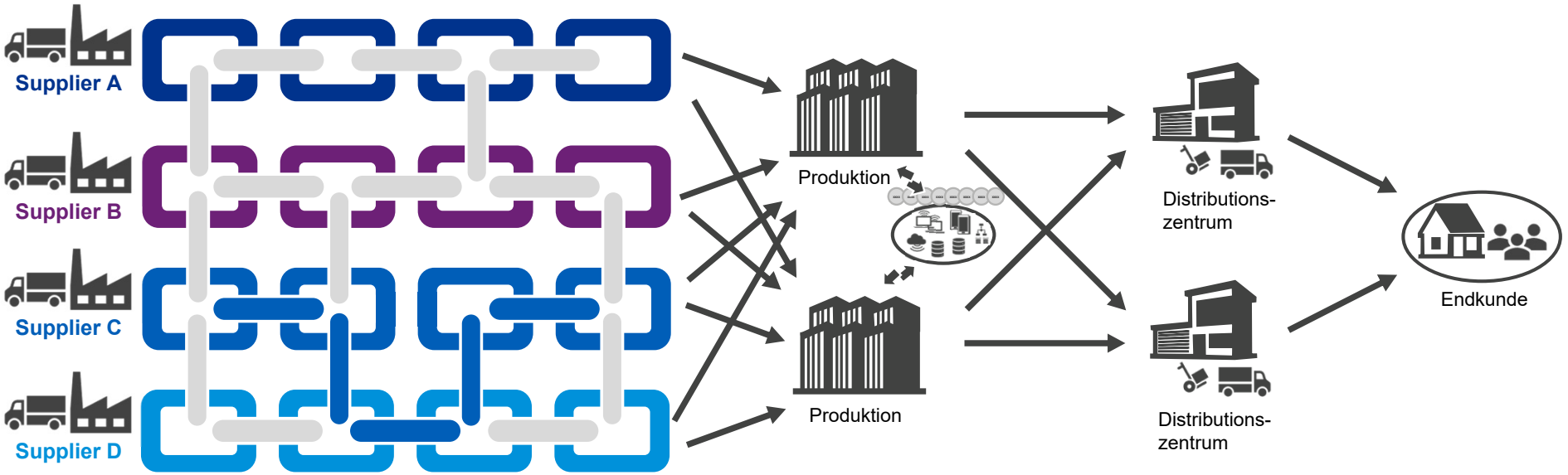
Beispiel: Aufbauen eines Continuous Assessment Process (CAP)

- Sichtung und Einteilung/Tagging aller Lieferanten
- Vor-Klassifizierung und priorisierte Zusatzbewertung
- Entwicklung Fragenkataloge und Pilot-Abfragen
- Priorisierte Lieferantenbefragung
- Auswertung, Feststellung von Quick Wins und Maßnahmen
- Überführung in ein Continuous Assessment Process (CAP)

Art und Häufigkeit der Maßnahmen zur Supply Chain in der Cyber-Security

Maßnahme / Risikoklasse	Häufigkeit des Assessments	Fragebogen	Assessment-Typ
Klasse 1	Quartalsweise	Detailliert	Vor-Ort-Begehung/ Interview vor Ort
Klasse 2 & 3	Monatlich	Detailliert	Automatisiertes Assessment
Klasse 4	Quartalsweise	Basis	Self-Assessment

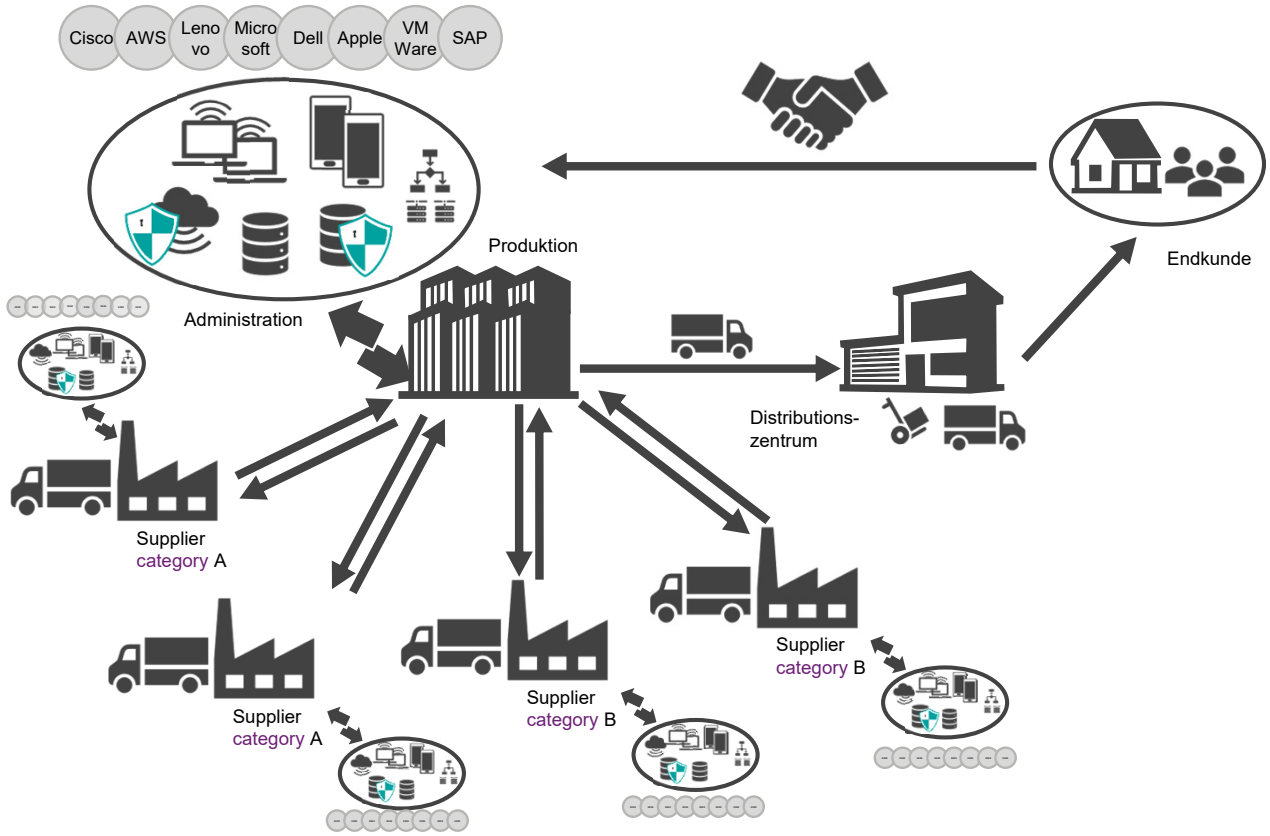
Moderne Sichtweise: Liefernetz statt Lieferkette



Die Erholung der Wirtschaft bei der Corona Pandemie zeigt, dass das Liefernetz hilft.

Ziel: Null-Fehler-Sicherheit

Moderne Sichtweise: Vertraulichkeit und Integrität durch Sicherheitszonen



Ziel: Null-Fehler-Sicherheit

Das Ziel der Null-Fehler-Sicherheit im Überblick

Wesentliche Take Aways

1 **Vergesst die Lieferkette – nutzt das Liefernetz.**

2 **Perimeterschutz ist gut. Zero Trust ist heute.**

3 **Cyber Security braucht sehr gute Kommunikation aller Beteiligten.
Vertrauensvoll. Einfach. Standardisiert. Schnell.**

Ihre Ansprechpartner

Hans-Peter Fischer
Partner
Consulting, Cyber Security
T +49 69 9587-2404
hpfischer@kpmg.com

Dr. Frank Damm
CISM
Senior Manager
Consulting, Cyber Security
T +49 221 2073-5728
fdamm@kpmg.com

www.kpmg.de/socialmedia

www.kpmg.de