BAM
Bundesanstalt für Materialforschung und -prüfung

Sicherheit in Technik und Chemie

09.04.2019

# CYBERSICHERHEIT ALS EINE VORAUSSETZUNG FÜR SICHERE PRODUKTE, DIENSTLEISTUNGEN UND PROZESSE:

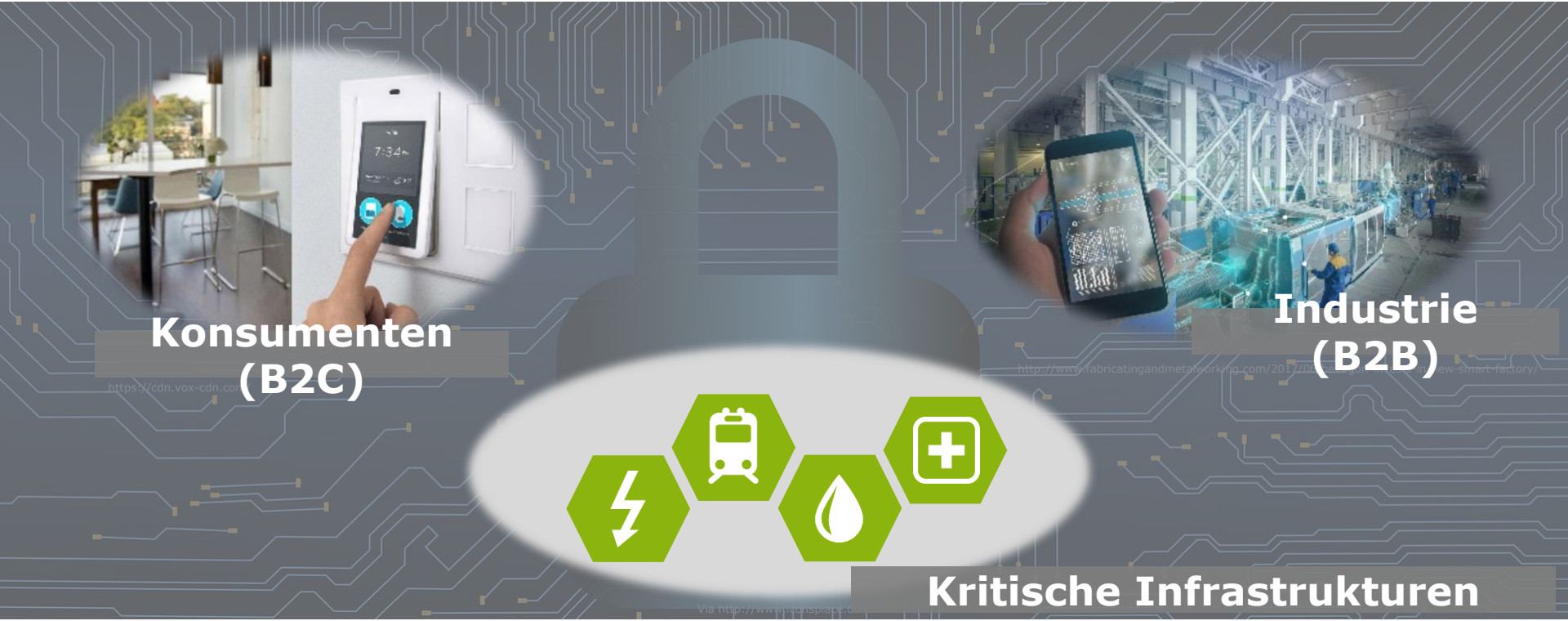
## DER NEUE EUROPÄISCHE RECHTSAKT ZUR CYBERSICHERHEIT

Mona Mirtsch

# Agenda

- Bedeutung von Cybersicherheit für die Konformitätsbewertung
- Vorstellung Rechtsakt zur Cybersicherheit [COM(2017)477] vom 13.9.2017 bzw. letzter Entwurf vom 12.3.2019
- Ergebnisse einer Analyse der Reaktionen von interessierten Kreisen
- Kurzvorstellung ausgewählter Normen im Bereich Cybersicherheit

# Cybersicherheit betrifft viele Bereiche in einer “smarten” Welt



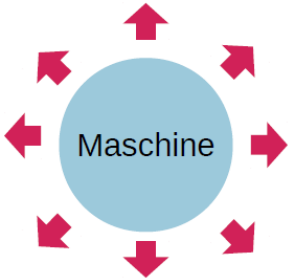

https://pixabay.com/de/hacken-cyber-kriminalit%C3%A4t-3112539/

# Wie unterscheiden sich Security und Safety?

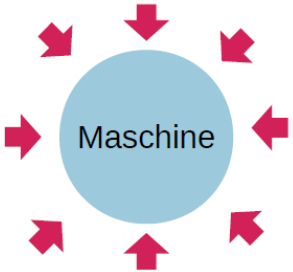
## Unfallvermeidung versus Kriminalprävention

***Safety*: im Zusammenhang mit zufälligen Risiken → Ziel ist es, Unfall zu verhindern**

***Security: im Zusammenhang mit beabsichtigten Risiken → Ziel ist es, kriminelle oder unbeabsichtigte Handlungen zu verhindern***



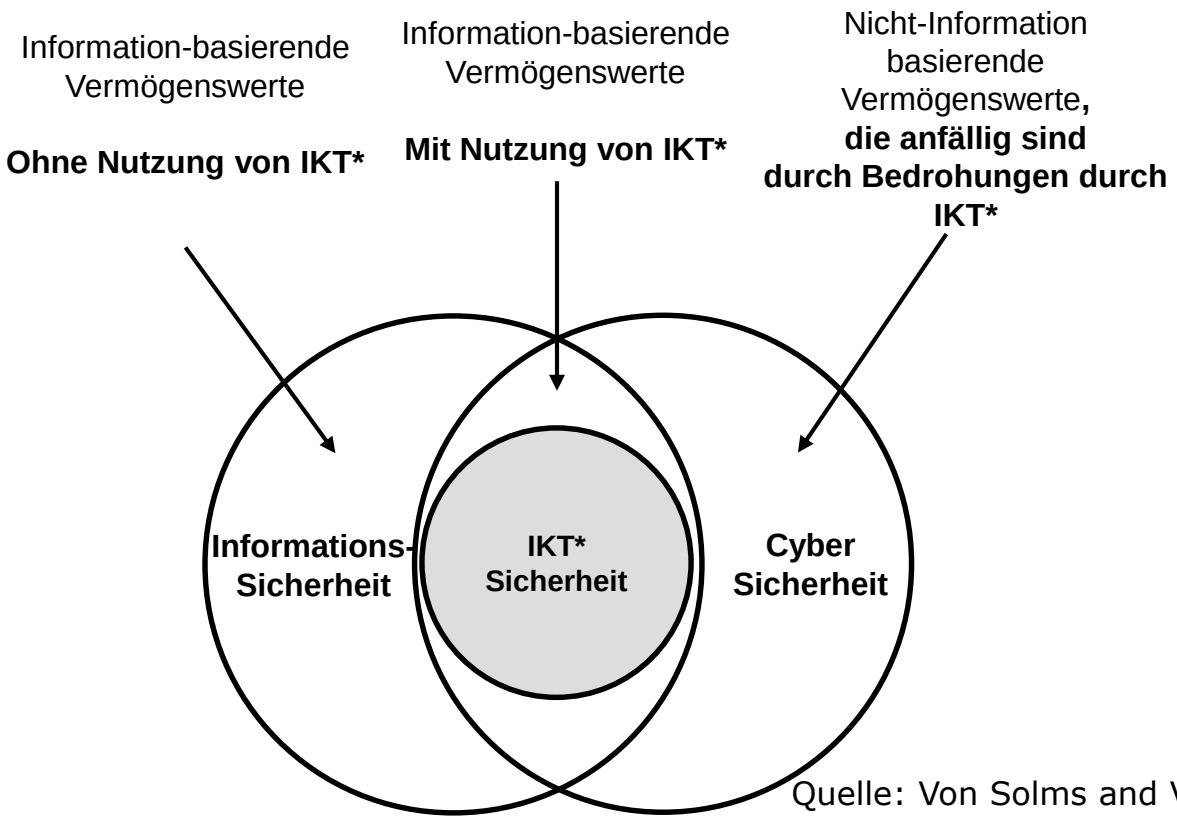

Safety:
Schutz vor Gefahr
für Mensch und Umwelt
von der Maschine




Security:
Schutz vor Gefahr
für Maschine
von Menschen

Quelle: BSI, 2019

# Wie grenzt sich Cybersicherheit von anderen Konzepten ab?




* Informations- und Kommunikationstechnik

Quelle: Von Solms and Van Niekerk, 2013

# Informations-Sicherheit: Die CIA- Ziele

Informationssicherheit beschreibt die „Aufrechterhaltung der Vertraulichkeit […], Integrität […] und Verfügbarkeit […] von Informationen“ (ISO/IEC 27000:2018)

Priorität Bürowelt (IT)

- **Vertraulichkeit** (*confidentiality*): Eigenschaft, dass Information unbefugten Personen, Entitäten oder Prozessen nicht verfügbar gemacht oder offengelegt wird
- **Integrität** (*integrity*): Eigenschaft der Richtigkeit und Vollständigkeit
- **Verfügbarkeit** (*availability*): Eigenschaft zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat

Priorität Produktions-welt (OT)

# Wieso gibt es nun einen Handlungsbedarf?

## Die Anzahl der Cyberangriffe nimmt zu…

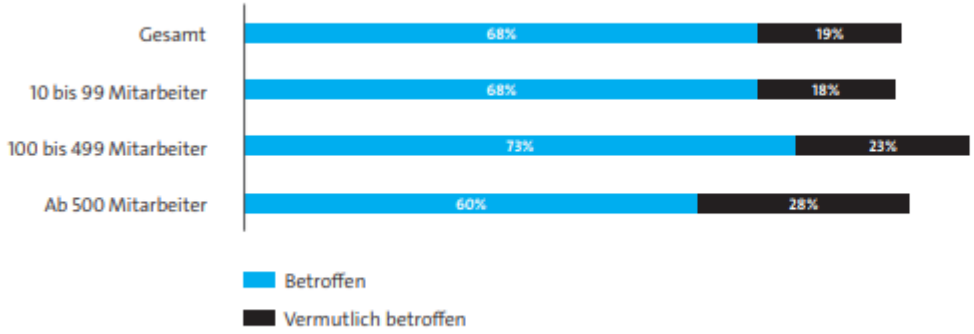



**Abbildung 3: Betroffene Unternehmen nach Betriebsgrößenklasse**

War Ihr Unternehmen innerhalb der letzten 2 Jahre von Datendiebstahl, Industriespionage oder Sabotage betroffen bzw. vermutlich betroffen?

Basis: Alle befragten Industrieunternehmen (n=503) | zu 100 Prozent fehlende Prozente entfallen auf »Nicht betroffen« & »Weiß nicht / keine Angabe«
Quelle: Bitkom Research

Quelle: Bitkom, 2018

# Wieso gibt es nun einen Handlungsbedarf?

**…und Cybersicherheit ist derzeit unzureichend reguliert:**

Da die geltende Richtlinie 2001/95/EG zur Produktsicherheit von einer „vernünftigerweise vorhersehbaren Verwendung“ ausgeht, deckt sie den möglichen Missbrauch verbundener IoT Geräte im Cyberraum möglicherweise nicht ab (VdTÜV, 2017).

Daher gäbe es nun einen Bedarf, die grundlegenden Anforderungen an Produkte und Dienstleistungen zu überarbeiten.

Quelle: VdTÜV, 2017

# Europäische Initiativen: Die NIS-Richtline:
## IT-Schutz kritischer Infrastrukturen und digitaler Anbieter

- Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

- Bis Mai 2018 war Überführung in nationale Gesetze Pflicht (Deutschland: IT Sicherheitsgesetz)

Quelle: BSI, 2019

# Europäische Initiativen: Vorschlag eines Rechtsakts zur Cybersicherheit (Cybersecurity Act)

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik

("Rechtsakt zur Cybersicherheit") COM(2017)

# Neuer europäischer Rechtsakt zur Cybersicherheit

- Vorgestellt von der europäischen Kommission am 13.9.2017

- Angenommen in angepasster Form am 12.3.2019 von dem Europäischen Parlament

- Ausstehend: Annahme durch den Europäischen Rat, bevor der Rechtsakt 20 Tage nach Publikation als Verordnung europaweit in Kraft tritt.

Quelle: Europäisches Parlament (2019)

# Cybersecurity Act: Schaffung eines EU-Zertifizierungsrahmen für Cybersicherheit

## z. Zt.

Schwer zu unterscheiden zwischen mehr oder weniger sicheren Produkten/ Dienstleistungen

## In der Zukunft..

Informationen zu den Sicherheitseigenschaften von Produkten/Dienstleistungen vor dem Kauf liegen vor

Erhöhung der Sicherheit und des Vertrauens von IKT-Produkten und-Dienstleistungen

Das Zusammenleben von parallelen Programmen erschwert den Vergleich...und macht es teuer für Unternehmen

... Endnutzer verzichten auf den Kauf zertifizierter Produkte/Dienstleistungen

Mehr Anreiz für Konsumenten, zertifizierte Produkte/Dienstleistungen zu kaufen

Unternehmen nutzen die Möglichkeit der One-Stop-Zertifizierung

Verringerung der aktuellen europäischen Marktfragmentierung

Quelle: Europäische Kommission, 2018

# Inhalte des Veordnungsvorschlages

# Neuer europäischer Rechtsakt zur Cybersicherheit

## Begriffe

Artikel 2(1):

„Cybersicherheit" bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;

Quelle: Europäisches Parlament, 2019

# Neuer europäischer Rechtsakt zur Cybersicherheit

## Zertifizierungsrahmen und europäische Schemata

Artikel 46 (2):

Der europäische Zertifizierungsrahmen für die Cybersicherheit legt einen Mechanismus fest, mit dem europäische Schemata für die Cybersicherheitszertifizierung geschaffen werden

und mit dem bescheinigt wird, dass die nach einem solchen Schema bewerteten IKT-Produkte, -Dienste und -Prozesse den festgelegten Sicherheitsanforderungen genügen, um die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus zu schützen

→ CIA Ziele über den ganzen Lebenszyklus für Produkte/DL und Prozesse

Quelle: Europäisches Parlament, 2019

# Neuer europäischer Rechtsakt zur Cybersicherheit

## Ausarbeitung der europäischen Schemata

Artikel 48 (1)

Die Kommission kann die ENISA* damit beauftragen, ein mögliches Schema auszuarbeiten oder ein bestehendes europäisches Schema für die Cybersicherheitszertifizierung auf der Grundlage des fortlaufenden Arbeitsprogramm der Union zu überarbeiten.

*European Union Agency for Network and Information Security ("Europäische Cybersicherheitsagentur")

Quelle: Europäisches Parlament, 2019

# Neuer europäischer Rechtsakt zur Cybersicherheit

## Vertrauenswürdigkeitsstufen

Artikel 52 (1):

Ein europäisches Schema für die Cybersicherheitszertifizierung kann für IKT--Produkte, -Dienste und -Prozesse eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig", „mittel" und/oder „hoch" angeben

Die Vertrauenswürdigkeitsstufe muss in einem angemessenen Verhältnis zu dem mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses verbundenen Risiko im Hinblick auf die Wahrscheinlichkeit und die Auswirkungen eines Sicherheitsvorfalls stehen

Quelle: Europäisches Parlament, 2019

# Neuer europäischer Rechtsakt zur Cybersicherheit

## Umgang mit nationalen Schemata

Artikel 57:Nationale Cybersicherheitszertifizierungsschemata und Cybersicherheitszertifikate

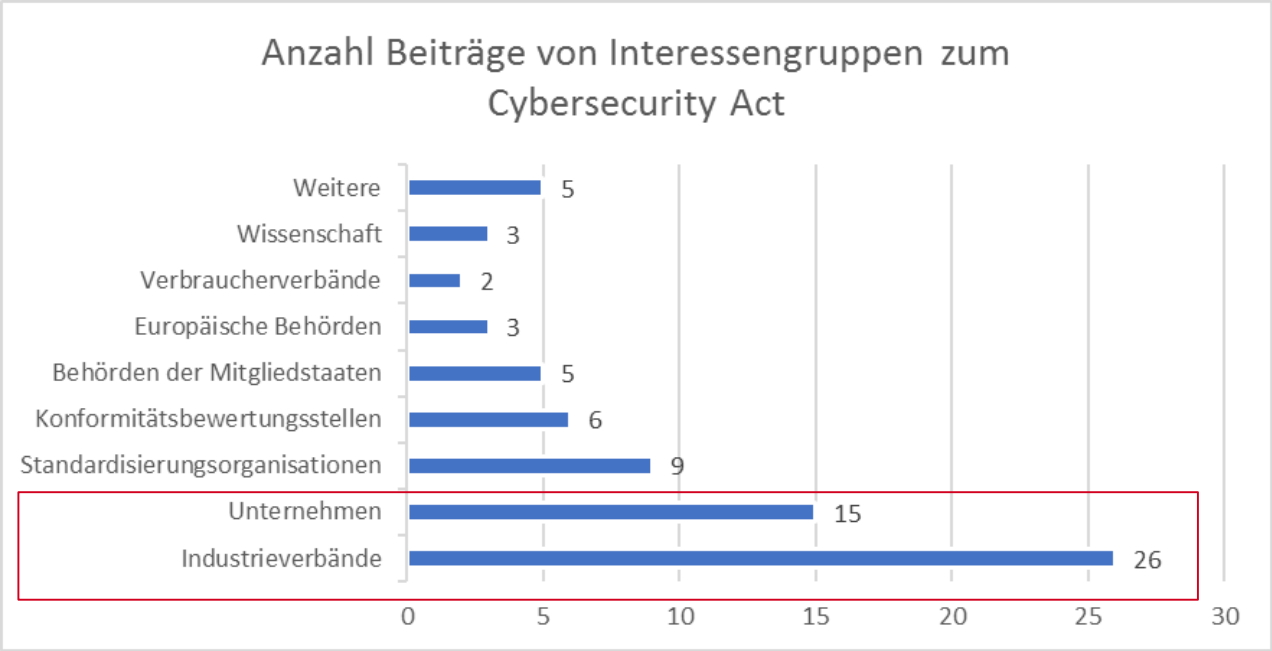
(1) Unbeschadet des Absatzes 3 dieses Artikels werden nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und -Prozesse , die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam, der in dem nach Artikel 49 Absatz 4 erlassenen Durchführungsrechtsakt festgelegt ist. Nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und-Prozesse , die nicht unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, bleiben bestehen.

Quelle: Europäisches Parlament, 2019

# Kritische Diskussion zum vorliegenden Verordnungsvorschlag mit Hilfe einer Analyse der Aussagen interessierter Kreise

# (Zeitraum September 2017-März 2018)

# Vorgehen: Aus 74 Dokumenten wurden insgesamt 343 Aussagen identifiziert…..

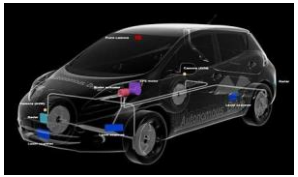


# …und zu übergreifenden 7 Themen zusammengefasst

1. Anwendungsbereich des Zertifizierungsrahmens
2. Freiwilligkeit der Konformitätsbewertung (freiwillig oder verpflichtend)
3. Art der Konformitätsbewertung (Herstellerklärung erlaubt?)
4. Entwicklung der Zertifizierungsprogramme
5. Einsatz von Labeln und Kennzeichnungen
6. Die Rolle von Standards
7. Wie passt der Cybersecurity Act in den bestehenden neuen Rechtsrahmen (NLF)

# 1. Anwendungsbereich des Zertifzierungsrahmens

- Allgemein: IKT-Produkte, Dienste und Prozesse
- Speziell genannt:
  - Vernetzte und automatisierte Fahrzeuge
  - elektronische medizinische Geräte
  - automatische Steuerungssysteme der Industrie und intelligente Netze



**Eine Klassifikationen (z.B. nach Produkten/Sektoren/Risikobereichen..) ist notwendig**

# 2. Freiwilligkeit der Konformitätsbewertung (freiwillig oder verpflichtend)

Artikel 56

(2) Sofern im Unionsrecht oder im Recht der Mitgliedstaaten nicht anders bestimmt, ist die Cybersicherheitszertifizierung freiwillig.

(3) Die Kommission bewertet regelmäßig die Effizienz und Nutzung […], um ein angemessenes Maß an Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen in der Union sicherzustellen und das Funktionieren des Binnenmarktes zu verbessern. Die erste Bewertung findet bis spätestens 31. Dezember 2023 statt und danach nachfolgende Bewertungen finden mindestens alle zwei Jahre statt. Die Kommission stellt auf der Grundlage der Ergebnisse der Bewertung fest, welche IKT-Produkte, -Dienste und -Prozesse, die unter ein bestehendes Zertifizierungsschema fallen, unter ein verpflichtendes Zertifizierungsschema fallen müssen.

Quelle: Europäisches Parlament, 2019

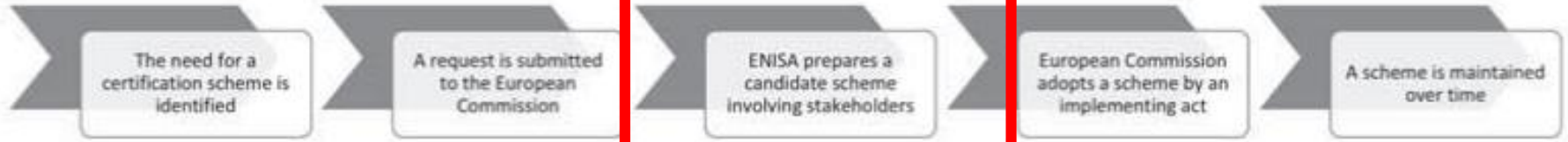
# 3. Art der Konformitätsbewertung (Herstellerklärung erlaubt?)

Artikel 53
(1) Ein europäisches Schema für die Cybersicherheitszertifizierung kann die Durchführung einer Selbstbewertung der Konformität unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen zulassen.

Die Selbstbewertung der Konformität ist nur für IKT-Produkte, -Dienste und -Prozesse mit niedrigem Risiko erlaubt, die der Vertrauenswürdigkeitsstufe „niedrig" entsprechen.

Quelle: Europäisches Parlament, 2019

# 4. Wer initiiert bzw. entwickelt die Konformitätsbewertungsprogramme?




Die Entwicklung erfolgt durch ENISA **unter Konsultation** der interessierten Kreise

Quelle: Mitrakas, 2018

**Eine Konsultation wird als nicht ausreichend erachtet: aktive Einbeziehung der interessierten Kreise gefordert**

*European Union Agency for Network and Information Security ("Europäische Cybersicherheitsagentur")

# 4. Wer initiiert bzw. entwickelt die Konformitätsbewertungsprogramme?

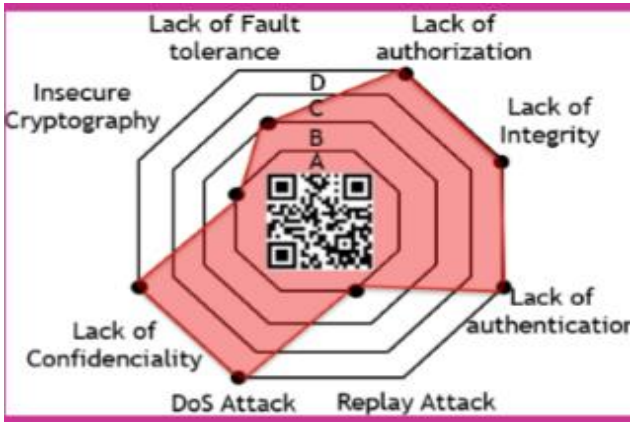
Artikel 49

(3) Bei der Ausarbeitung der möglichen Schemata konsultiert die ENISA* alle in Frage kommenden Interessenträger im Wege eines förmlichen, offenen, transparenten und inklusiven Konsultationsprozesses.

Quelle: Europäisches Parlament, 2019

*European Union Agency for Network and Information Security ("Europäische Cybersicherheitsagentur")

# 5. Einsatz von Labeln und Kennzeichnungen



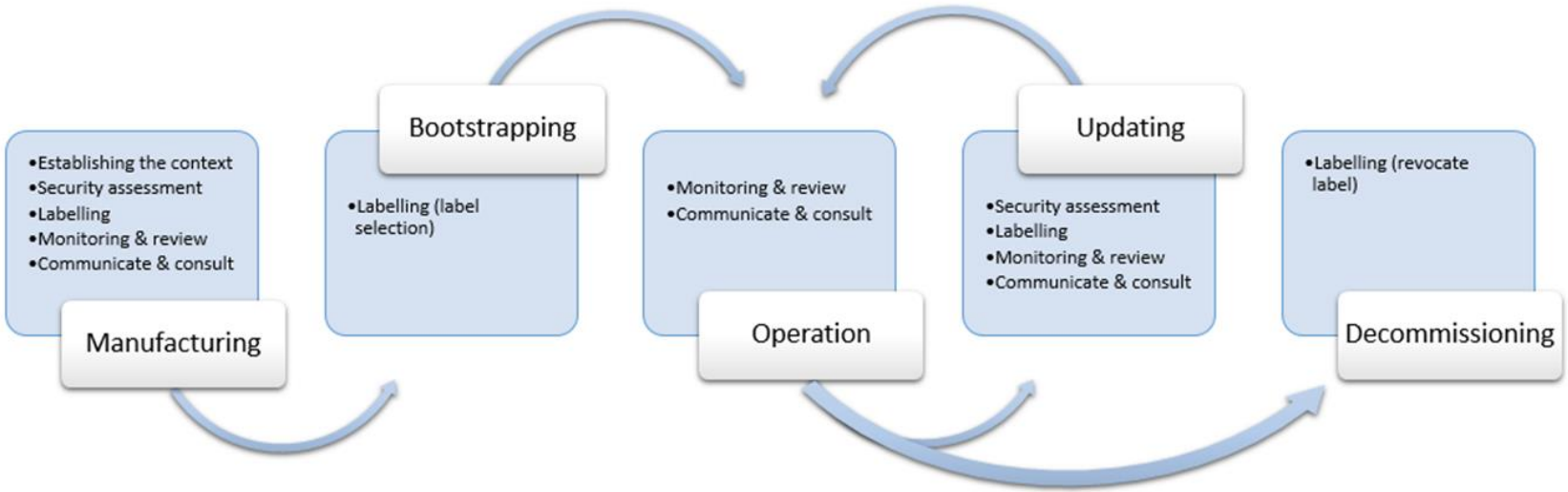

Visuelle Kennzeichnung als Ergebnis der Auswertung, die dem Nutzer angemessen kommuniziert werden muss.

Mehr Fläche = mehr Risiko

**Ein Label ähnlich der Energieverbrauchskennzeichnung wird als schwierig erachtet..**

Quelle: Joint Research Centre, 2018

# 5. Einsatz von Labeln und Kennzeichnungen




**… auch vor dem Hintergrund der verschiedenen Phasen im Lebenszyklus der IoT Geräte**

Quelle: Joint Research Centre, 2018

# 6. Die Rolle von Standards
# Ausgewählte Normen im Bereich Cybersicherheit

- **ISO 27000er Reihe:** Anforderungen an ein Informationssicherheits**managementsystem** (ISMS)
- **IEC 62443:** „Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme

Anforderung an den Gegenstand der Konformitätsbewertung **(was wird getestet?)**

- **ISO/IEC 15408:** Evaluationskriterien (Common Criteria) → Behördliche Abkommen

Anforderung an die Prüfmethoden der Konformitätsbewertung **(wie wird getestet?)**

**International, anerkannte Normen durchweg gewünscht/ Ausnahme: Bereich der inneren Sicherheit**

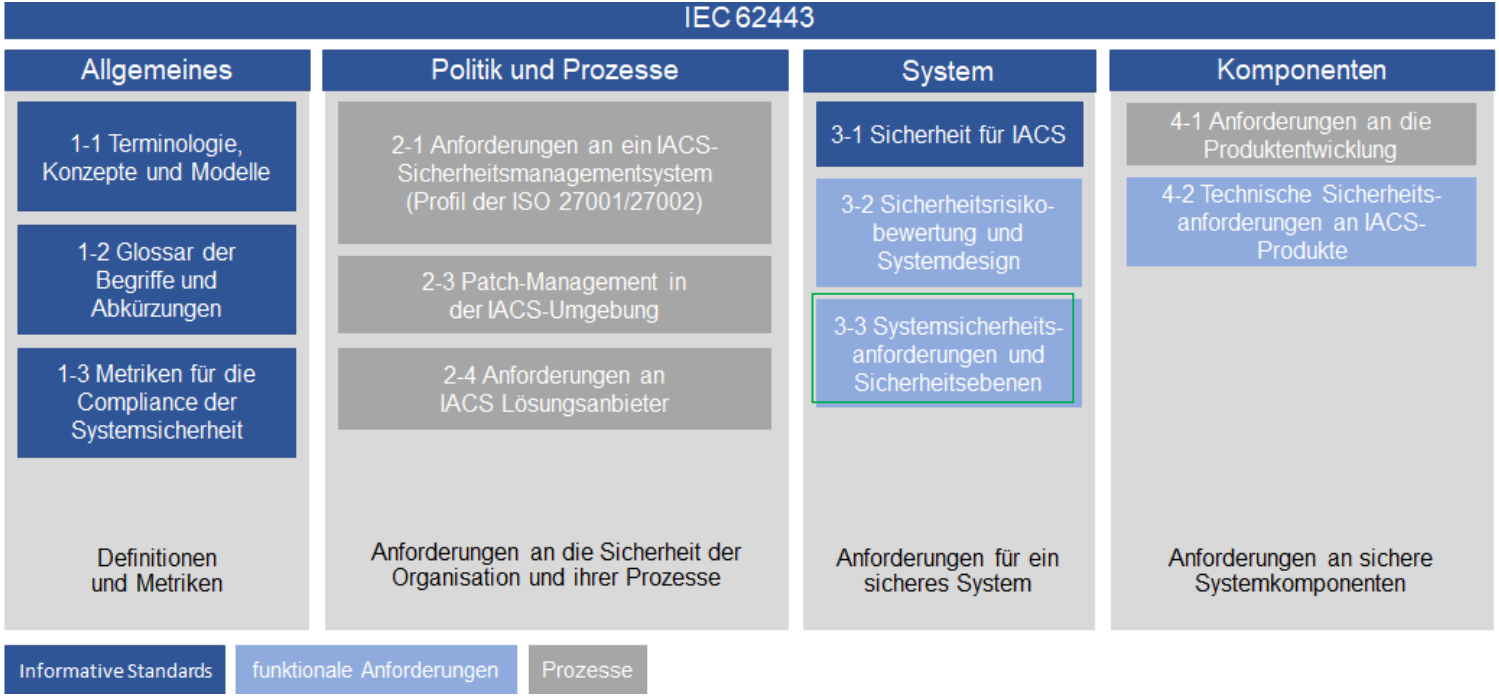
# ISO/IEC 27000er Reihe

- legt die Anforderungen an Aufstellen, Umsetzen, Betrieb, Überwachung, Bewertung, Wartung und Verbesserung von dokumentierten **Informationssicherheit-Managementsystemen** in Bezug auf die allgemeinen Geschäftsrisiken einer Organisation fest.

→ **Diese Norm ist für alle Organisationsarten (zum Beispiel Handelsunternehmen, Regierungsstellen, gemeinnützige Gesellschaften) anwendbar.**

→ **Die ISO 27000er Reihe umfasst Begriffe (ISO/IEC 27000), Informationssicherheitsmaßnahmen (ISO/IEC 27002), … branchenspezifisch für Telekommunikationsunternehmen, (ISO/IEC 27011), ..für Cloud-Computing Dienste Anbieter (ISO/IEC 27017), …Anforderungen an Energieversorgungsunternehmen (ISO/IEC 27019).., Guidelines für Cyber Insurances (ISO/IEC CD 27102)**

# IEC 62443 “Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme”




Quelle: TÜV Nord, 2017

# 7. Wie passt der Cybersecurity Act in den bestehenden neuen Rechtsrahmen (NLF)

CCA [Cybersecurity Act] has to be part of the NLF and it fit's fully in!! (TÜV Süd, 2018)

"It should therefore be stated clearly that the certification framework should not apply for mandatory requirements in existing or future Union acts. Should there be mandatory requirements in Union acts, the NLF should apply."
(ETSI, 2018)

The proposal unfortunately disregards the use of the tried and tested single market infrastructure of the 'New Legislative Framework' ('NLF') (VDMA, 2018)
)

**Uneinigkeit, ob der Cybersecurit Act in den NLF passt oder nicht…**

# Aktueller Vorschlag vom ZVEI: Horizontale Produktregulierung für Cybersicherheit

| | |
|---|---|
| **1. Schritt** | **Cybersecurity Act:** Rahmen für die freiwillige Cybersicherheit-Zertifizierung von Produkten, Diensten und Prozessen |
| **2. Schritt** | **NLF:** Grundlage für verbindliche öffentlich-rechtliche Produktanforderungen an die Cybersicherheit auf dem EU-Binnenmarkt |

Quelle: ZVEI (2018)

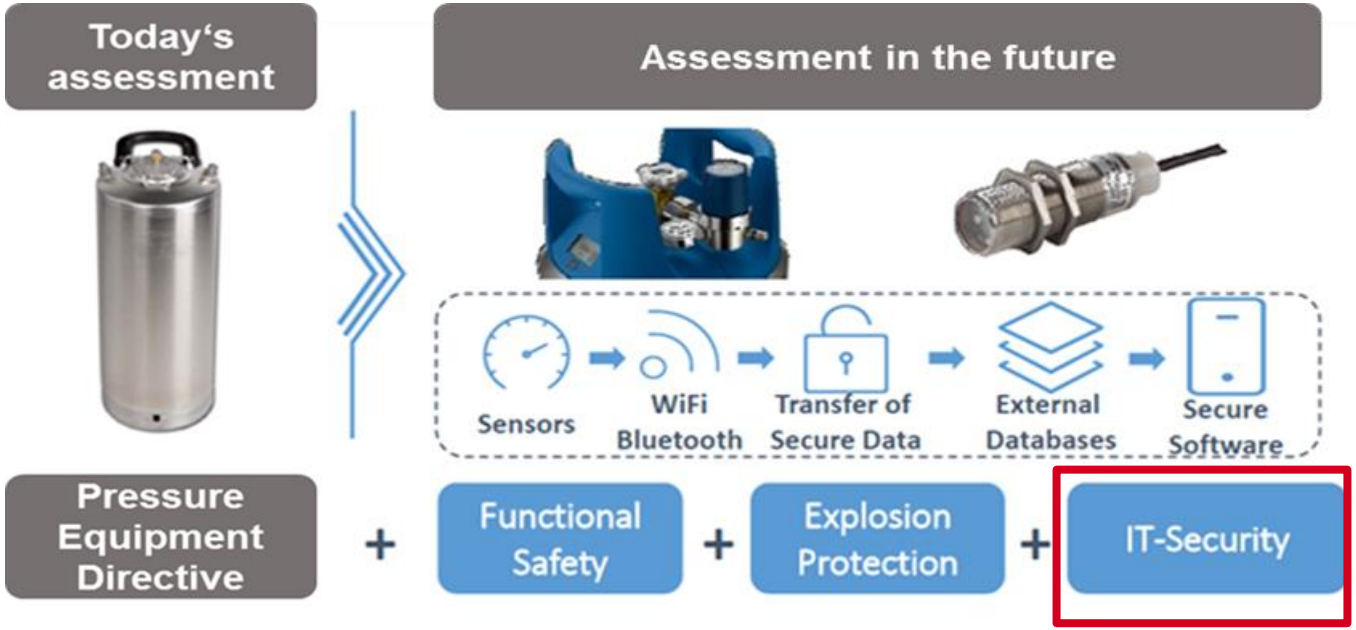
# Zusammenfassung

**Die meisten Beteiligten sind sich einig:**

- Es besteht Handlungsbedarf, um die Cybersicherheit zu erhöhen (vorzugsweise internationaler Ansatz)
- Eine Integration des Aspektes Cybersicherheit entweder durch Anpassung der jetzigen Verordnungen und Richtlinien oder Schaffung neuer Richtlinien bzw. Verordnungen wird allgemein befürwortet
- Die Zertifizierung von Cybersecurity kann dazu beitragen, das Vertrauen der Verbraucher in IKT-Produkte und-Dienstleistungen zu stärken, und ein europaweiter Zertifizierungs-Rahmen kann dazu beitragen, die Fragmentierung zu verringern

**Allerdings gibt es umfangreichen Klärungsbedarf, insbesondere zur Integration des Zertifzierungsrahmens in den bestehenden neuen Rechtsrahmen**

# Und wie kann sich das auf die Konformitätsbewertung auswirken?




Richtlinie 2014/68/EU über Druckgeräte

**"Security for Safety" Konzept**

Quelle: TÜV Süd, 2018

# Referenzen


- BSI (2019), Jens Mehrfeld, NASG Beirat, 24.2.2019
- Von Solms, R. and J. Van Niekerk (2013). "From information security to cyber security." Computers & Security 38: 97-102.
- VdTÜV. (2017a). VdTÜV-Position: Regulativer Nachbesserungsbedarf für sichere IoT-Produkte in Europa. Verfügbar unter: https://www.vdtuev.de/dok_view?oid=679604
- Bundesamt für Sicherheit in der Informationstechnik (2019). Schutz Kritischer Infrastrukturen. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf;jsessionid=76A9CE58B71DBE74E73ECEE50585DF75.2_cid360?__blob=publicationFile&v=7
- Bitkom Research (2018). Studienbericht 2018. Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Verfügbar unter: https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf
- Bundesrat (2017). Unterrichtung durch die Europäische Kommission: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit") COM(2017): 110.
- Europäische Kommission (2018). "Towards a reformed EU Cybersecurity Agency and reinforcing the cybersecurity single market in the EU..." Verfügbar unter: https://www.eesc.europa.eu/en/news-media/presentations/towards-reformed-eu-cybersecurity-agency-and-reinforcing-cybersecurity-single-market-eu

# Referenzen


- Europäisches Parlament (2019) Legislative Entschließung des Europäischen Parlaments vom 12. März 2019 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit") (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)) (Ordentliches Gesetzgebungsverfahren: erste Lesung) Verfügbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0151+0+DOC+XML+V0//DE

- Mitrakas, A. (2018). "The emerging EU framework on cybersecurity certification." Datenschutz und Datensicherheit-DuD **42**(7): 411-414

- Joint Research Centre (2018). "EU R&D in cybersecurity's certification." Verfügbar unter: https://www.eesc.europa.eu/sites/default/files/files/joint_research_centre.pptx

- TÜV Nord (2017). "Zertifizierung nach IEC 62443." Verfügbar unter https://www.tuev-nord.de/fileadmin/Content/TUEV_NORD_DE/pdf/PDB_Zertifizierung_nach_IEC_62443_DE_WEB.pdf

- ZVEI (2018). Whitepaper: Horizontale Produktregulierung für Cybersicherheit. Verfügbar unter: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2018/November/Horizontale_Produktregulierung_fuer_Cybersicherheit_Whitepaper/Horizontale-EU-Produktreglung-Cybersicherheit-Whitepaper.pdf

- TÜV Süd (2018). "CONFERENCE CCA –13.Feb. 2018 –Brussels-MariottCEN –CENELEC –ETSI -ENISA." Vortrag von Christian Priller. Verfügbar unter: ftp://ftp.cencenelec.eu/EN/News/Events/2018/Cybersecurity_ENISA_CEN_CL_ETSI_Presentations/Christian-PRILLER_TÜV-SÜD-AG.pdf

- VDMA (2018). "Cybersecurity – a strategic task for Europe." Verfügbar unter: https://euro.vdma.org/documents/106103/24584945/Cybersecurity%2520-%2520a%2520strategic%2520Task%2520for%2520Europe%2520%2520VDMA%2520on%2520Cybersecurity%2520Act%25202%25202018_1518594749524.pdf/b1270707-efa0-48b4-a867-c8121958bbbe

- ETSI (2018). "ETSI Position Paper on draft Regulation 2017/0225 ''Cybersecurity Act”." Verfügbar unter: http://www.etsi.org/images/files/ETSI_position_paper-CyberAct_20180206.pdf

Vielen Dank für die Aufmerksamkeit
und für Fragen!