Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Neue Herausforderungen für die Cybersicherheit

Dr. Günther Welsch, Abteilungsleiter Krypto-Technik und IT-Management, BSI

24. Oktober 2022

Kennzeichen der modernen Digitalisierung

1. Technische (R)Evolutionen und Leistungssprünge halten an (Moore´s Law)
2. Game Changer: Cloud Computing: **„X as a Service“ und Künstliche Intelligenz**
3. Nutzung offener Kommunikationssysteme – Abschied vom Burgwall Perimeterschutz
4. Globale digitale Geschäftsmodelle treiben alle volkswirtschaftlichen Bereiche
5. Usability zum Nutzer – Superlineares Komplexitätswachstum in den Technologien
6. Effizienzgetriebene Geschäftsmodelle ohne Resilienz und Fokussierung auf Sicherheit
7. Regulative Vermeidungsstrategien: Unterschiedliche Rechts- und Regulierungsräume
8. Industrialisierte, organisierte Kriminalität und Save Harbors ohne Verfolgungsdruck
9. Medienkompetenz in Bezug auf „Click“ nicht die dahinterliegende Technologie
10. Digitale Enthaltsamkeit ist keine Option!

Digitalisierung und Volkswirtschaft

- Gross Domestic Product (GDP) in USA 2020: **21.180 Mrd US $**
  - Anteil Informationstechnik an GDP **11 %**: **2.450 Mrd US $**
  - Anstieg seit 2011 von **3,4 %**
  - Informationstechnik ist in der US Volkswirtschaft 7 mal schneller pro Jahr gewachsen!

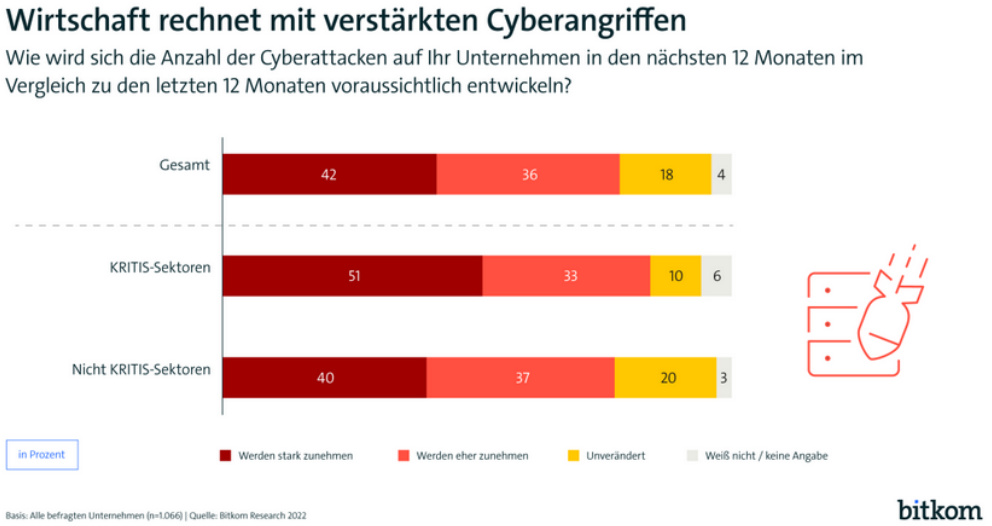
- Vergleich EU 2019: **3,8 %** Anteil an GDP
  - Randnotiz: EU hängt in digitalen Services deutlich hinter den USA zurück

- Bezogen auf Deutschland 2021:
  - BIP: **3.600 Mrd €**
  - Anteil Informationstechnik (ca. **4 %**): **145 Mrd €**

- Konsequenzen:
  - Digitalisierung wird noch stark voranschreiten
  - **Quellen des Wohlstands liegen in erfolgreicher Digitalisierung**
  - Allerdings: Attraktivität für Cyber-Kriminalität steigt gleichermaßen!

Digitalisierung und Informationssicherheit (Cyber-Sicherheit)

- BITKOM Studie zur Cybersicherheit:
  - Volkswirtschaftliche Schäden 2021: **ca. 223 Mrd €**
  - Cyber-Spionage und Cyber-Sabotage wird erwartet
  - IT-Attacken aus russischen und chinesischen Regionen
  - KRITIS noch stärker betroffen als die Gesamtwirtschaft
  - 45 % der Unternehmen fürchten um Ihre Existenz
  - Anteil IT-Sicherheit an IT-Budget in Unternehmen **9 %**

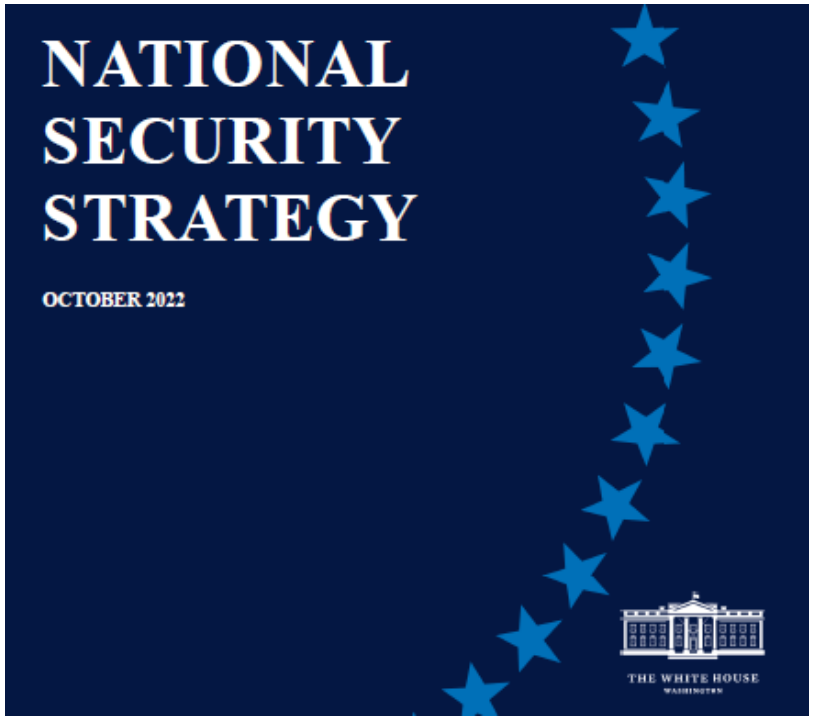


„Von der Politik wünschen sich **98 Prozent mehr Einsatz für eine verstärkte EU-weite Zusammenarbeit** bei Cybersicherheit. 97 Prozent fordern, dass die Politik stärker gegen Cyberattacken aus dem Ausland vorgehen soll. Und drei Viertel **(77 Prozent) meinen, die Politik solle die Ermittlungsbefugnisse erweitern, damit Cyberangriffe aufgeklärt** werden können. Zugleich beklagen 77 Prozent, dass der bürokratische Aufwand bei der Meldung von Vorfällen zu hoch ist.“

https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022#item-16368-close

Digitalisierung und Geopolitischer Rahmen

- **Geopolitische Risiken nehmen rapide zu**
- Größten Herausforderungen (u.a. aus Perspektive USA):
  - Wettbewerb zwischen Demokratien und Autokratien
  - Klimawandel und Energiesicherheit
  - Pandemien und Abwehr von Biogefahren
  - Nahrungsmittelunsicherheiten
  - Verteilungskämpfe um die verfügbare Biosphäre
  - Handel und Ökonomie
  - **Sicherer Cyber-Raum**



www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

- Digitalisierung ist essentieller Teil unserer Welt und der Geopolitik
  - Sicheres Handeln und sichere Technik sind erfolgskritisch auf globaler und regionaler Ebene
  - Hybride Risiken sind zukünftig mitzudenken!

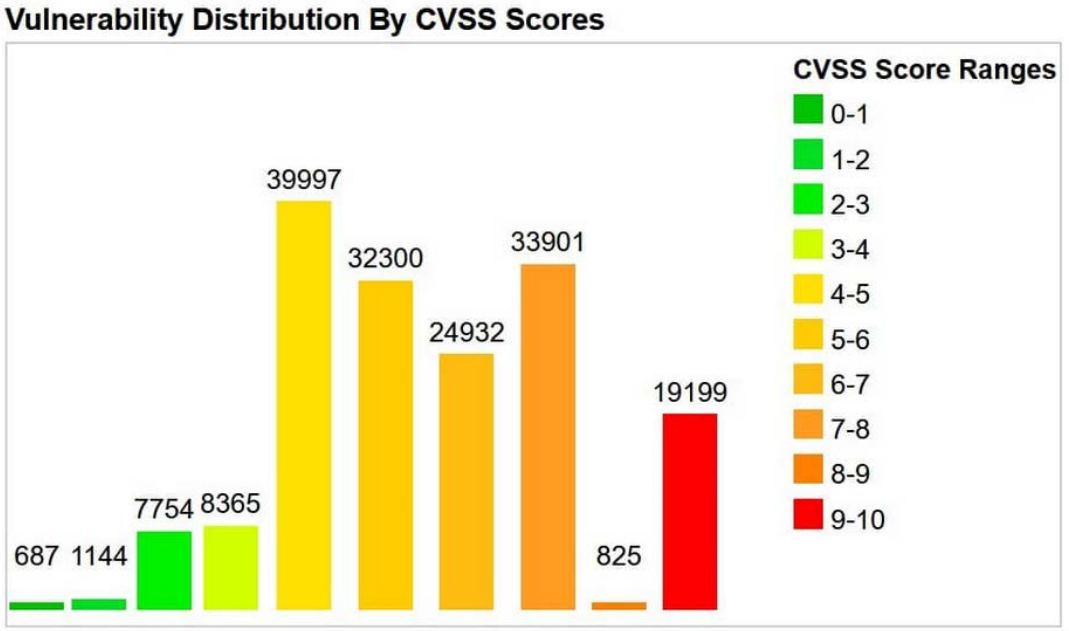
Wachstum von IT-Gefährdungen

Eigenschaften der globalen Informationstechnik

- Vielseitigkeit, Veränderungsgeschwindigkeit, Vernetzung und Komplexität von IT sehr hoch
- Funktionalität und Time-2-Market für IT-Produkten entscheidend – nicht Security!

Konsequenzen:

- Wachstum erkannter IT-Schwachstellen (CWE) ca. 20.000 p.a.
- Gelistete Verwundbarkeiten (CVE) ca. 176.000
- Mehr als 11 % der Verwundbarkeiten sind extrem kritisch
- Mittlere Zeitdauer zur Eindämmung ca. 60 Tage in Bezug auf internetausnutzbare Verwundbarkeiten



https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/
https://cve.mitre.org/

Bedrohung durch Cyber-Kriminalität

- Derzeit: Größte Bedrohung durch **Ransomware**
- Wirtschaftsmodell mit Arbeitsteilung: Cybercrime-as-a-Service
- „Big Game Hunting“: Gezielte Angriffe auf Organisationen
- Zunehmende Qualität und Quantität, große Angriffslast
- Maximierung des Erpressungsdrucks:
  - Verschlüsselung der Daten
  - Daten-Leaks trotz Lösegeldzahlung
  - Kontaktaufnahme zu Kunden & Partnern
  - Anzeige bei Aufsichtsbehörden
- Wiederherstellungsdauer der Arbeitsfähigkeit im Durchschnitt: **23 Tage**

ZEIT ONLINE

Suche

Politik Gesellschaft Wirtschaft Kultur ▾ Wissen Gesundheit ▾ Digital Campus ▾ Sinn Arbeit ZEITmagazin ▾

Cyberattacken

Mehr als 500 Millionen Dollar mit Ransomware in den USA erpresst

Mehr als eine halbe Milliarde Euro haben US-Firmen allein im ersten Halbjahr 2021 nach Angriffen mit Erpressungstrojanern gezahlt. Die Attacken werden immer häufiger.

15. Oktober 2021, 19:51 Uhr / Quelle: ZEIT ONLINE, AFP, fa / 17 Kommentare /

Angriffe in 2021	Lösegeld (geschätzt)
Darkside Angriff auf Colonial Pipeline Corp.	4 Mio. $
Revil Angriff auf JBS	11 Mio $
Evil Corp Angriff auf CNA Financial	40 Mio $

Übergreifende Herausforderungen für die Cyber-Sicherheit

1. Missionskritische Abhängigkeiten von Digitalisierung (KRITIS)
2. Verlässlichkeit, Verfügbarkeit und Integrität von Supply Chains
3. Sicherheitsmanagement komplexer Infrastrukturen (Prävention, Health Status, Angriffserkennung, DC, BCM)
4. Überforderungen der Anwender und Digitale Sorglosigkeit
5. Daseinsvorsorge des Staates

Technische Herausforderungen für die Cyber-Sicherheit

1. Inhärent sichere IT-Architekturen (Verfügbarkeit, Vertraulichkeit, Integrität, Verlässlichkeit, Beherrschbarkeit)
2. Technische Eindämmung von Social Engineering
3. Patch- und Updatemanagement in komplexer IT
4. Quantencomputing und Post-Quantum Kryptografie
5. Dualität neuester IT und Legacy HW/SW

Vorschläge für multiwirksame und mehrschichtige Lösungsansätze

1. **Technische und logische Ansätze:**
   - Authentifizierung, SDN, Zero-Trust, Automatisierung, Künstliche Intelligenz, Kryptoagilität
   - Technische Robustheit und Resilienz
   - Prävention, Detektion
2. **Organisatorisch-soziale Ansätze**
   - Auditierungen, Testate, Zertifizierungen
   - „Assume the Breach“ – Vorbereitet auf den Ernstfall sein: Incidence Management, Disaster Recovery, BCM
   - „Human Firewall“, Digitalkompetenz vermitteln, Sensibilisierung, Compliance
   - Asymmetrien auflösen, Vernetzungen und Kooperationen, Managed Security Services
3. **Rechtliche-wirtschaftliche Ansätze**
   - In Märkten und Business Eco Systemen denken
   - Harmonisierte Regulierungsrahmen schaffen
   - Haftungstatbestände einführen
   - Kritische Infrastrukturbetreiber stärker verpflichten

Software Bill of Materials (SBOM)
Common Security Advisory Framework (CSAF)

Allianz für Cyber-Sicherheit

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Kleine Randnotiz:

Managed Security Services werden Commodity!

Organisatorisch-soziale Lösungsansätze

Vereinheitlichung der Informationsweitergabe innerhalb der Lieferkette

Software Bill of Materials (SBOM)

- Digitaler „Beipackzettel“ für alle verwendeten Softwarekomponenten
- Für Hersteller und OEMs

Common Security Advisory Framework (CSAF)

- Einheitliches Format für Informationen über Patches und Updates
- Fokus Endkunden
- Automatisierung Updates und Sicherheitsmanagement

CSAF

Politische Lösungsansätze in Deutschland

Koalitionsvertrag der Regierungsparteien

Rechtsetzung definiert den Rahmen – Ausgestaltung ist gemeinsame Aufgabe:

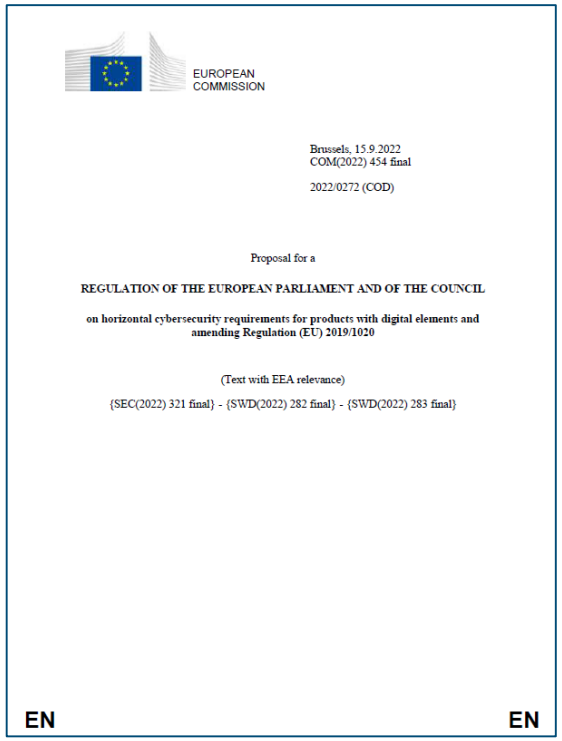
- Stärkung der Cybersicherheit als digitale Schlüsseltechnologie Deutschlands
- Verschlüsselung, Security by design & default, offene Standards sowie Interoperabilität
- Aufbau eines wirksamen Schwachstellenmanagements zur schnellstmöglichen Schließung von Sicherheitslücken
- Einsatz für Cyber-Normen zur Gewährleistung verantwortlichen Handelns von Staaten im Cyberraum
- Ausbau der Unterstützung der KMU in IT-Sicherheitsfragen

„Sichere Digitalisierung“ erwähnt in mehr als 60 Stellen des KoaV

Regulative europäische Lösungsansätze

Cyber-Resilience Act

- Entwurf der Europäischen Kommission vom 15. September 2022
- CRA regelt den Marktzugang in Form von horizontalen europäischen Cyber-Sicherheitsanforderungen für ein breites Spektrum digitaler Produkte und Dienste
- Anforderungen an Produkte über deren gesamten Lebenszyklus (Design, Entwicklungs- und Fertigungsprozesse, Einsatzphase, kostenlose Patches und Updates)
- Bei Incidences sind Hersteller zur Meldung an die EU-Cybersicherheitsbehörde ENISA verpflichtet



EUROPEAN COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

(Text with EEA relevance)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EN EN

Regulative europäische Lösungsansätze

NIS2: Wirtschaftsraum cyber-sicher gestalten

Stärkere Harmonisierung der Anforderungen
Sicherheitsmaßnahmen werden europaweit einheitlicher für Wirtschaft/Verwaltung geregelt; Überarbeitungen B3S ggf. erforderlich; mehr Anforderungen (supply chain)

Ausweitung der Aufsichts- und Durchgriffsrechte
BSI wird mehr Kompetenzen ggü. Wirtschaft erhalten/weitere Aufsichts- und Durchgriffsrechte für einen Großteil der Unternehmen aus mehr NIS-Sektoren

Einheitlichere Meldepflichten
Vorfallsmeldeverfahren werden europaweit einheitlicher für Wirtschaft/Verwaltung geregelt; 3-stufiges Verfahren; zeitliche Fristen

Erweiterte Informationspflichten
mehr Vorgaben bei Überlieferung von Unternehmensdaten an das BSI; ggf. Selbstidentifizierung; bei Vorfällen: Information der Kunden zu mögl. Maßnahmen

§

Einheitliche Vorgaben bei Sektorrechtsakten
Anwendung horizontaler und sektoraler Anforderungen werden grundsätzlich auf EU-Ebene geregelt; NIS2 immer als Mindestsicherheit auch bei „Doppelregulierungen“

€

Potentiell höhere Strafen & Verantwortung CEOs
Sanktionsregime wird erweitert; höherer Bußgeldrahmen; CEOs können bei Verstößen sanktioniert werden

Fazit

- Cyber-Sicherheit ist die Voraussetzung einer erfolgreichen Digitalisierung
- Digitalisierung ist aber auch gleichzeitig die Grundlage für höhere Cyber-Sicherheit!

- **Herausforderungen in der Cyber-Sicherheit sind drängend, Lösungsansätze stehen zur Verfügung**
- **IT-Security wächst als Business Eco-System und wird zunehmend Marktdifferenziator**

- Das BSI agiert als partnerschaftlicher Mitgestalter der Informationssicherheit in der Digitalisierung
- Sozialisierung ist ein Erfolgskriterium: Seien Sie bspw. Teilhaber der Allianz für Cyber-Sicherheit!