TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Staatskanzlei des Saarlandes | Dialog Cyber-Security

«Wachsende Bedrohung vor dem Hintergrund des Ukraine-Krieges?»

Online, 11.03.2022

Stellungnahme TeleTrusT: Resilienz stärken, hybriden Lagen begegnen

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Dr. André Kudra

Eine Premiere und ein Plädoyer dazu

- **Erstmalig in der Geschichte der Menschheit, dass hybride Auseinandersetzung in diesem Ausmaß stattfinden kann**
- **Transparenz in hybriden Lagen schaffen**

- TeleTrusT-Pressemeldung zum Thema

https://www.teletrust.de/startseite/pressemeldung/?tx_ttnews%5Btt_news%5D=1458&cHash=3322401aa266dc17f85dfdb07bae9bfb

„Jetzt handeln!“ muss die Maxime sein

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Digitale Souveränität ist aktuell eine Illusion
- Wir sind im Hintertreffen
- "Aufrüsten" in der IT-Sicherheit unabdingbar
- Resilienz steigern bzw. schaffen

➔ **TeleTrusT IT-Sicherheitsagenda 2029 betont dies**

TeleTrusT IT-Sicherheitsagenda 2029 – IT-Sicherheit in der Digitalisierung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Forderungen

1. Klares Bekenntnis zu unbeschränkter IT-Sicherheit

2. **Technologische Souveränität im Bereich IT-Sicherheit schaffen - für eine werteorientierte, sichere und vertrauenswürdige digitale Zukunft**

3. **Auf- und Ausbau von IT-Sicherheitsinfrastrukturen für Bürger, Unternehmen und Verwaltung fordern und fördern**

4. **Mehr IT-Sicherheitstechnologie "Made in Germany" in der Praxis**

5. Verbot der Kompromittierung von IT-Sicherheit, keine Backdoors, Staatstrojaner oder geschwächte Verschlüsselung

6. Europäische IT-Sicherheitsgesetze für eine erhöhte Rechts- und Investitionssicherheit - klar, konsolidiert und agil

Quelle: https://www.teletrust.de/teletrust-it-sicherheitsagenda

Situation im Grundsatz

- Perimeterschutz ist praktisch unmöglich geworden
- Unverständliche Komplexität von IT-Systemen dominiert
  - Komplexität ist der schlimmste Feind der IT-Sicherheit
- Keine relevanten physischen IT-Massenprodukte aus EU

Was kann man konkret tun? Sofort und perspektivisch.

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- **Zugriffsschutz erhöhen** – bspw. mit Multi-Faktor Authentifizierung (MFA)
- Volle **Transparenz schaffen**, was "verbaut" ist
- Stringentes **Patch- und Schwachstellenmanagement** leben
- **Komplexität** von IT-Systemen **reduzieren**
- **Abhängigkeiten** kennen und **verstehen**
- **Vertrauenswürdige IT-Produkte** einsetzen
- **Open Source konsequent** für mehr Transparenz
- **Auditieren** und **versiegeln** – Systeme und Fertigung
- Attraktive **Bug Bounty** – Incentivierung für Lückenfinden
- **Angriffe erkennen** – Monitoring (SIEM) & Security Operations Center (SOC) as a Service

Situation im Grundsatz und eine relevante Stoßrichtung

- Perimeterschutz ist praktisch unmöglich geworden
- Unverständliche Komplexität von IT-Systemen dominiert
  - Komplexität ist der schlimmste Feind der IT-Sicherheit
- Keine relevanten physischen IT-Massenprodukte aus EU

➔ **Zero Trust-Verständnis & -Architekturen als Zielbild**

Wo das Vertrauen anfängt und aufhört bei Zero Trust

- **Zero Trust heißt: Authentifizierung am IT-System**
  - Für menschlichen Zugriff
  - Für Maschine-zu-Maschine Interaktion
- Entscheidung für Zugriff am IT-Asset treffen

- **Irgendwo muss man auch bei Zero Trust vertrauen**
- Im "Inneren" muss man dem IT-Asset vertrauen können

Wir können es nicht (mehr) selbst und es dauert lange…

- **Hardware** wieder in **EU** entwickeln und bauen
  - Von Endnutzer:innen verwendete Hardware kann nur als unsicher betrachtet werden
  - Auch bei Serversystemen ist belastbare Sicherheit schwer erreichbar
  - Cloud-Infrastrukturen bestehen aus Servern UND kommen nicht aus EU

- **Konsequent umstellen** trotz massiven Aufwands

➔ **Es NICHT zu tun ist keine Option!**

Backup

- **Details zur TeleTrusT IT-Sicherheitsagenda 2029**

1. Klares Bekenntnis zu unbeschränkter IT-Sicherheit

- Die gewünschte digitale Transformation beschleunigt auf allen Ebenen
- IT-Sicherheitsprobleme werden jedes Jahr größer
- Heutige IT ist nicht sicher genug, um Angriffe intelligenter Hacker abzuwehren
- Unbeschränkte IT-Sicherheit ist Grundvoraussetzung für Erfolg
- Wir brauchen ein klares Bekenntnis

2. Technologische Souveränität im Bereich IT-Sicherheit schaffen - für eine werteorientierte, sichere und vertrauenswürdige digitale Zukunft

- Selbstbestimmt und unabhängig Wirtschaft und Gesellschaft gestalten
- Open Source für Schlüsseltechnologien / kritische Bereiche
- Schwerpunkt auf Softwarequalität, Sicherheit und Vertrauenswürdigkeit
- Investitionen in IT-Sicherheitsinfrastrukturen als Basis für die Digitalisierung
- IT-Sicherheit zum Schutz und Aufbau von Vertrauen, um Akzeptanz zu erzielen

3. Auf- und Ausbau von IT-Sicherheitsinfrastrukturen für Bürger, Unternehmen und Verwaltung fordern und fördern

- Bereitstellung von IT-Sicherheitsmechanismen ist eine Infrastrukturaufgabe
- eID-Initiativen bündeln, weiterführen, skalieren
- Mobiles Arbeiten durch Vertrauensdienste ergänzen
- Webseiten und E-Mail konsequent absichern
- Staat als Enabler

4. Mehr IT-Sicherheitstechnologie "Made in Germany" in der Praxis

- Vorhandene Technologieproduktionen ausbauen
- Sichere Plattformen mit "Airbus-artigem" Willen umsetzen
- Vergabe- und Förderrecht mittelstandsfreundlich gestalten
- Kleine, innovative Unternehmen in Normung bringen
- Investitionen in eigene IT-Sicherheit fördern

5. Verbot der Kompromittierung von IT-Sicherheit, keine Backdoors, Staatstrojaner oder geschwächte Verschlüsselung

- Staat hat digitale Grundrechte zu verteidigen
- Abkehr von Grundrechtseingriffen, die
  - rechtlich unangemessen sind
  - die IT-Sicherheit schwächen
  - das Vertrauen in Digitalisierung senken
  - das Vertrauen in IT-Sicherheitstechnologien beeinträchtigen

6. Europäische IT-Sicherheitsgesetze für eine erhöhte Rechts- und Investitionssicherheit - klar, konsolidiert und agil

- Europäische IT-Sicherheitsverordnung schaffen
- Anwendungsbereich des IT-Sicherheitsgesetzes angemessen auf KMU erweitern
- Qualität/Agilität der Gesetze erhöhen
- Vorgehen der Aufsichtsbehörden konsolidieren