



TeleTrust @ it-sa 365 Launch Days

Digitale Plattform it-sa 365, 06.10.2020

Technologische Souveränität in einer zunehmend komplexeren Welt-Wirtschaftslage

Prof. Dr. (TU NN) Norbert Pohlmann,

Vorstandsvorsitzender des Bundesverband IT-Sicherheit e.V. (TeleTrust)

Professor für Informationssicherheit

Leiter des Instituts für Internet-Sicherheit - if(is)

Warum ist die technologische Souveränität wichtig?

- Die Digitalisierung ist der **Motor und die Basis** für das Wohlergehen unserer Gesellschaft.
- Die Digitalisierung ist global und kann von **globalen Herstellern** und **Diensteanbietern** beeinflusst werden.
- **Und wir müssen realisieren**, dass die **geopolitische Lage** im Moment sehr schwierig ist und daher spielen technologische Abhängigkeiten zurzeit eine wichtige Rolle.
- **Technologische Souveränität** trägt dazu bei, eigenständig, selbstbestimmt und unabhängig **Wirtschaft** und **Gesellschaft** zu gestalten, um unseren **Wohlstand** aufrecht zu erhalten.
- Da in Zukunft **in allen Branchen** der **Wertschöpfungsanteil der IT immer größer** wird, werden in der Zukunft auch alle Branchen abhängiger **von der IT** sein.



Technologische Souveränität

→ erhöhen und bewahren (2/2)



Wir müssen aber auch realisieren, dass eine vollständige technologische Souveränität finanziell nicht umgesetzt werden kann, aber wir sollten zumindest **wichtige Schlüsseltechnologien** beherrschen und weiterentwickeln können.

Randbedingungen

- Der **Digitalisierungsprozess** wird immer schneller,
- die **technologischen Innovationszyklen** werden immer kürzer,
- das bedeutet auch, wir können **rascher neue Technologien einführen** und
- damit **schneller eine höhere technologische Souveränität** umsetzen.

Handlungsempfehlungen für mehr technologische Souveränität:



Handlungsempfehlungen

→ Künstliche Intelligenz (KI)



- **Künstliche Intelligenz (KI) ist eine Schlüsseltechnologie** für das **zukünftige Wirtschaftswachstum** in allen Branchen.
- **Daher** müssen wir die **Verfügbarkeit unserer Daten durch die Speicherung in DE, in der EU sicherstellen**, um Abhängigkeit zu reduzieren.
- **Wir müssen leistungsstarke eigene KI-Infrastruktur aufbauen**, um souverän das Wirtschaftswachstum in allen Branchen zu ermöglichen.
- **Unterstützung des Mittelstands**, damit dieser KI optimal, qualitativ und souverän nutzen kann, um den zukünftigen Erfolg zu garantieren.
- Die **Selbstbestimmung und Autonomie** der Nutzer sollten berücksichtigt werden, damit die KI eine **hohe Akzeptanz bei den Nutzern** erzielt.



Handlungsempfehlungen

→ Cloud-Dienste fördern und aufbauen



- Es ist keine Frage von **"ob in die Cloud"** sondern lediglich, **"wann"** und **"wie"**.
- Die Corona-Krise hat uns gezeigt, wie wichtig solche Internet-Infrastrukturen sind und in der Zukunft weiter an Bedeutung zunehmen werden.
- Daher sollten wir eigene Cloud-Dienste fördern, die unsere **Sicherheits- und Wertestandards** berücksichtigen.
- Das Projekt GAIA-X ist der richtige Ansatz, weil hier in Europa **mit europäischen Anbietern** eine Alternative bzw. eine Ergänzung zu den **Hyperscalern** der außereuropäischen Marktführer geschaffen wird.



Handlungsempfehlungen

→ Cyber-Sicherheit fördern und ausbauen



- Die Cyber-Sicherheitsherausforderungen sind groß und werden mit der zunehmenden Digitalisierung immer größer.
- **IT-Sicherheitsinfrastrukturen und deren Dienste** wie zum Beispiel für ***Verschlüsselung, elektronische Identitäten, Domänenzertifikate*** usw. sollten hinsichtlich der Herkunft von Technologien und Produkten in **europäischer Verantwortung** liegen und den **Stand der Technik** erfüllen.
- Im Bereich der **Anzahl der Cyber-Sicherheitsexperten** spielt Deutschland an der Spitze mit und hat ideale Voraussetzungen, sich erfolgreich international zu positionieren.
- Wir sollten „**IT Security made in Germany**“ oder „**IT Security made in EU**“ noch stärker zum Qualitätssiegel machen!



Handlungsempfehlungen

→ Open-Source-Software



- Das können wir auch **international mit vielen Partnern gemeinsam tun.**
- **Ein Großteil unserer Gesellschaft** funktioniert zurzeit mit und dank Open-Source-Software.
- Die **Entwicklungsparadigmen "Security by Design", "Privacy by Design"** sowie **nachvollziehbare Qualitätssicherung** müssen für alle IT-Lösungen bedingungslos definiert und umgesetzt werden.
- Offene Systeme erlauben es, **Sicherheit und Vertrauenswürdigkeit zu überprüfen** und **den Stand der Technik** in alle IT-Systeme **standardisiert** und **flächendeckend** zur Verfügung zu stellen.



Handlungsempfehlungen

→ Evaluierung und Zertifizierung



- Wir werden nicht in der Lage sein, alle wichtigen IT-Technologien souverän zu entwickeln, daher müssen Methoden eingeführt werden, die helfen, IT-Technologien **kontinuierlich analysieren** und **bewerten zu können**.
- Da die **Evaluierung und Zertifizierung** von IT-Technologien und -Diensten den **Level an Vertrauenswürdigkeit erhöht**, sollte diese für wichtige Bereiche vorgeschrieben werden.



Handlungsempfehlungen

→ international standardisieren



- Eine sehr gute Möglichkeit, neue Technologien mitgestalten zu können, ist das **Engagement** in den **wichtigsten internationalen Standardisierungsgremien**.
- Diese Notwendigkeit sollte deutlich mehr und intensiver umgesetzt werden.



Technologische Souveränität

→ Zusammenfassung



- Um eine passende technologische Souveränität für Deutschland zu erreichen, müssen alle **wichtigen und relevanten Stakeholder** zusammen:
 - **messbare Ziele formulieren**,
 - deren **Umsetzung beschließen** und
 - **mit vereinten Kräften** durchführen.

- Nur so werden wir in der Lage sein, die vorgeschlagenen **Handlungsempfehlungen** erfolgreich **zum Wohle unserer Gesellschaft** umzusetzen.



Technologische Souveränität

in einer zunehmend komplexeren Welt-Wirtschaftslage

Technologische Souveränität trägt dazu bei, eigenständig, selbstbestimmt und unabhängig Wirtschaft und Gesellschaft zu gestalten, um unseren Wohlstand aufrecht zu erhalten.

Prof. Dr. (TU NN) Norbert Pohlmann,
Vorstandsvorsitzender des Bundesverband IT-Sicherheit e.V. (TeleTrust)
Professor für Informationssicherheit
Leiter des Instituts für Internet-Sicherheit - if(is)



N. Pohlmann: "Künstliche Intelligenz und Cybersicherheit – Diskussionsgrundlage für den Digitalgipfel 2018"

<https://norbert-pohlmann.com/app/uploads/2018/12/Künstliche-Intelligenz-und-Cybersicherheit-Diskussionsgrundlage-für-den-Digitalgipfel-2018-Prof.-Norbert-Pohlmann.pdf>

N. Pohlmann: "Künstliche Intelligenz und Cybersicherheit - Unausgegoren aber notwendig", IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2019

<https://norbert-pohlmann.com/wp-content/uploads/2019/04/393-Künstliche-Intelligenz-und-Cybersicherheit-Unausgegoren-aber-notwendig-Prof.-Norbert-Pohlmann.pdf>

N. Pohlmann, A. Wehrhahn-Aklender: "Cloud unter (eigener) Kontrolle: Trusted Cloud Enklave - Vertrauen durch Sicherheit", IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 3/2018

<https://norbert-pohlmann.com/wp-content/uploads/2019/02/378-Cloud-unter-eigener-Kontrolle-Trusted-Cloud-Enklave-Vertrauen-durch-Sicherheit-Prof.-Norbert-Pohlmann.pdf>

N. Pohlmann: "Wertschöpfung der Digitalisierung sichern - Vier Cybersicherheitsstrategien für den erfolgreichen Wandel in der IT", IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT, 1/2020

<https://norbert-pohlmann.com/wp-content/uploads/2019/08/408-Wertschöpfung-der-Digitalisierung-sichern-Vier-Cybersicherheitsstrategien-für-den-erfolgreichen-Wandel-in-der-IT-Prof.-Norbert-Pohlmann.pdf>

M. Linnemann, N. Pohlmann: "Turaya - Die offene Trusted Computing Sicherheitsplattform", in "Open Source Jahrbuch 2007", Hrsg.: B. Lutterbeck, M. Bärwolff, R. Gehring, Lehmanns Media, Berlin, 2007

<https://norbert-pohlmann.com/wp-content/uploads/2015/08/193-Turaya-Die-offene-Trusted-Computing-Sicherheitsplattform.pdf>

N. Pohlmann: **Lehrbuch "Cyber-Sicherheit"**, Springer Vieweg Verlag, Wiesbaden 2019

ISBN 978-3-658-25397-4s

<https://norbert-pohlmann.com/cyber-sicherheit/>

Weitere Artikel siehe: <https://norbert-pohlmann.com/artikel/>

Bericht des Weisenrats für Cyber-Sicherheit (mit einem Kapitel zur "Technologische Souveränität"): <https://norbert-pohlmann.com/wp-content/uploads/2019/08/Jahresbericht-des-Weisenrates-für-Cyber-Sicherheit-2020-Prof.-Norbert-Pohlmann.pdf>



Wir empfehlen

- **Kostenlose App securityNews**



securityNews



- **7. Sinn im Internet (Cyberschutzraum)**

<https://www.youtube.com/cyberschutzraum>



- **Master Internet-Sicherheit**

<https://it-sicherheit.de/master-studieren/>



- **Cyber-Sicherheit**

Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von "Cyber-Sicherheitssystemen in der Digitalisierung", Springer Vieweg Verlag, Wiesbaden 2019

- <https://norbert-pohlmann.com/cyber-sicherheit/>



Besuchen und abonnieren Sie uns :-)

WWW

<https://www.internet-sicherheit.de>

Facebook

<https://www.facebook.com/Internet.Sicherheit.ifis>

Twitter

https://twitter.com/_ifis

YouTube

<https://www.youtube.com/user/InternetSicherheitDE/>

Prof. Norbert Pohlmann

<https://norbert-pohlmann.com/>



Quellen Bildmaterial

Eingebettete Piktogramme:

- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.

<https://www.it-sicherheit.de/>

