Institut für
Nachhaltiges
Projektmanagement

SCHRIFTENREIHE
Jenseits der Begrenztheit – Projekte anders denken, Horizonte erweitern

BAND 6
Beatrix Palt, Michael Dost, Andreas Stemick & Team[1]

Expertisebildung heißt es wahrhaben wollen – nationale Software-Autonomie bis 2029 als Teil der nationalen Souveränität. Ein Denkanstoß

INP – Institut für Nachhaltiges Projektmanagement / Beatrix Palt (Hrsg.)

[1] Die Namen des Teams von Andreas Stemick sind an entscheidender Stelle bekannt.

Inhalt

Abstract

Dieser Beitrag beschreibt „es nicht wahrhaben wollen“ als Ursache für die bislang ausbleibende Verbindung von innerer und äußerer Sicherheit als Grundlage für nationale (digitale) Souveränität.

Aus politischer und gesellschaftlicher Perspektive wird staatsräsonal begründet und aus dem Koalitionsvertrag abgeleitet, die vertikale (Bund, Länder bis hinunter zu jeder einzelnen Person) und horizontale (Ministerien für Digitales, Inneres, Äußeres, Finanzen und Verteidigung) Verbindung von innerer und äußerer Sicherheit als politische, technologische und gesamtgesellschaftliche Aufgabe beschrieben.

Als Argumentationsgrundlage wird Artikel 1 des Grundgesetzes der Bundesrepublik Deutschland herangezogen: „Die Würde des Menschen ist unantastbar“, der Menschenbild und Menschenrechtsverständnis definiert und Leitfaden für politisches, gesellschaftliches und technologisches Handeln ist. Die Verankerung der Menschenwürde in Art. 1 GG und das darauf basierende Grundrecht auf informationelle Selbstbestimmung begründet eine staatliche Schutzpflicht, digitale Lebensgrundlagen resilient zu gestalten und so die Integrität innerer wie äußerer Sicherheit zu sichern.

Angesichts der politischen und ideologischen Auseinandersetzung der Systeme wird darauf verwiesen, dass selbst innerhalb von Demokratien unterschiedliche Menschenbilder und Menschenrechtsverständnisse zu beobachten sind (z. B. libertär). Unterschiedliche Menschenbilder und Menschenrechtsverständnisse „nicht wahrhaben wollen“ wird damit zum Grundproblem.

Zur Wahrung unserer freiheitlich demokratischen Grundordnung sind Autonomie und Selbstbestimmung wesentliche Faktoren. In Bezug auf das Erreichen einer nationalen Software-Autonomie bis 2029 wird darauf basierend eine Open-Source-Strategie beschrieben, die über deutsche Patente national und auf Europa ausgerollt werden kann.

Dazu werden bestehende Open-Source-Produkte auf nationaler Ebene weiterentwickelt und zertifiziert. Ein risikobasierter Ansatz zur Priorisierung der Umsetzung wird vorgestellt, der kurz-, mittel- und langfristige Maßnahmen umfasst.

Langfristig wird der Aufbau einer Open Source GmbH in Deutschland vorgeschlagen, die unter der operativen Koordination des Bundesamts für Sicherheit in der Informationstechnik (BSI) steht. Diese soll die Zusammenarbeit zwischen Bund und Ländern bündeln und die technologische Unabhängigkeit sicherstellen.

Das Dokument betont die Bedeutung einer sicheren und souveränen IT-Infrastruktur „made in, made by Germany and made for Germany“ für die nationale Sicherheit und die Notwendigkeit, technologische Abhängigkeiten zu minimieren.

Das hier vorgelegte Papier ist ein Denkanstoß.

Einleitung: Die Verbindung von innerer und äußerer Sicherheit

Kontext und Ausgangslage: Wir springen zu kurz

Es springt zu kurz, die derzeitigen Auseinandersetzungen der Systeme auf politischer und wirtschaftlicher Ebene international, national, auf der Ebene der föderalen Bundesländer bis hinunter zur einzelnen Person auf die Auseinandersetzung zwischen autoritären und demokratischen Systemen und Konstruktionen (NATO, EU etc.) zu reduzieren und sie ideologisch und politisch Parteien zuzuordnen, die dann wiederum um die Deutungshoheit in der Gesellschaft ringen. Es geht vielmehr um das Menschenbild und das Menschenrechtsverständnis, das unverbrüchlich in Artikel 1 im Grundgesetz der Bundesrepublik Deutschland verankert ist: „Die Würde des Menschen ist unantastbar." Denn allein aus diesem leitet sich unser gesellschaftlicher Anspruch und unser politisches Handeln ab, das dann in Maßnahmen mündet. Allein das ist unsere gesellschaftliche und politische Legitimation. Das ist unser Menschenbild und Menschenrechtsverständnis, zentraler Wert unserer Gesellschaft, unserer freiheitlichen Demokratie. Dies ist Grundlage, Leitbild und Leitlinie für alles, was wir im Bereich der inneren und äußeren Sicherheit tun, für alles, was wir verteidigen. Die Verankerung der Menschenwürde in Art. 1 GG und das darauf basierende Grundrecht auf informationelle Selbstbestimmung begründen eine staatliche Schutzpflicht, digitale Lebensgrundlagen resilient zu gestalten und so die Integrität innerer wie äußerer Sicherheit zu sichern. Daraus leitet sich staatsräsonales Verhalten der Regierung auch im Sinne der nationalen (digitalen) Souveränität und Sicherheit ab. Der gilt Digitales als „Machtpolitik".[2]
Der Gesetzgeber in Form der jetzt regierenden Parteien hat im Koalitionsvertrag den politischen Rahmen gesetzt und innere und äußere Sicherheit Bund-Länder-übergreifend verknüpft und über den Bundessicherheitsrat unter der Überschrift „Kohärenz im Außenhandeln" klar implementiert:
„Wir entwickeln den Bundessicherheitsrat, im Rahmen des Ressortprinzips, zu einem Nationalen Sicherheitsrat im Bundeskanzleramt weiter. Er soll die wesentlichen Fragen einer integrierten Sicherheitspolitik koordinieren, Strategieentwicklung und strategische Vorausschau leisten, eine gemeinsame Lagebewertung vornehmen und somit das Gremium der gemeinsamen politischen Willensbildung sein.
Für eine ganzheitliche Bewältigung von Krisen braucht Deutschland einen Bund-Länder- und ressortübergreifenden Nationalen Krisenstab der Bundesregierung und ein Nationales Lagezentrum im Bundeskanzleramt, in dem ressortübergreifend ein Gesamtlagebild zusammengefügt wird."[3]
Übersetzt auf „Digitales" heißt das unter der Rubrik „Deutschland – Digital. Souverän. Ambitioniert:

[2] https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf Abruf am 18.07.2025. S. 66.
[3] Ebda., S. 126.

Unsere Digitalpolitik ist ausgerichtet auf Souveränität, Innovation und gesellschaftlichen Fortschritt. Digitalpolitik ist Machtpolitik. Wir wollen ein digital souveränes Deutschland[4]. Dazu werden wir digitale Abhängigkeiten[5] abbauen, indem wir Schlüsseltechnologien entwickeln, Standards sichern, digitale Infrastrukturen schützen und ausbauen. Wir schaffen europäisch integrierte und resiliente Wertschöpfungsketten für Schlüsselindustrien, von Rohstoffen, über Chips bis zu Hard- und Software"[6].

Staatsräson gilt für die (digitale) Verbindung von innerer und äußerer Sicherheit gesamtstaatlich horizontal und vertikal verknüpft, betrifft also zusammenfassend die Ministerien für Inneres, Äußeres, Verteidigung – und als Klammer über alle hinweg – Digitales, von der Bundesregierung über die Bundesländer und Kommunen bis hin zu jeder einzelnen Person – als durchgängiges, allseits verbindliches System und Wirkprinzip.[7]

Somit hat der Koalitionsvertrag Implikationen auf mehreren Ebenen:

- Erstens bedeutet das, dass in Folge staatsräsonal begründete Lösungen notwendig sind, die ans Kanzleramt gebunden und von dort ausgehend vertikal über alle Ebenen und horizontal für die betroffenen Ministerien gleichermaßen bindend sind und unterhalb dieser Ebene, der nationalen Weisung folgend, umzusetzen sind.[8]
- Und zwar, weil zweitens zur Kenntnis genommen und bewertet werden muss, dass es selbst innerhalb dessen, was als freiheitliche Demokratien bezeichnet wird, unterschiedliche Ausprägungen von Demokratieverständnissen gibt, denen unterschiedliche Menschenbilder und unterschiedliche Menschenrechtsverständnisse zugrunde liegen. Daher wäre es berechtigt, selbst bei den Unternehmen, die sich als deutsch bezeichnen und dies auch sind, hinter die Kulissen zu schauen, welche Partnerschaften und internationalen Verpflichtungen sie eingegangen sind und ob sich

---

[4] Siehe auch: Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, IT-Planungsrat Januar 2021; mit Gesetzesänderung zur vorrangigen Nutzung von Open Source Software im Bund. Mit dem OZG-Änderungsgesetz (OZGÄndG) trat am 24.07.2024 auch eine Anpassung des E-Government-Gesetzes (EGovG) in Kraft, welche die vorrangige Nutzung von Open Source Software in der Bundesverwaltung regelt.

[5] Mit BSI-IT-Sicherheitshinweis vom 21.07.2025 in der Kritikalität 3 / Orange (Maßnahmen müssen unverzüglich ergriffen werden. Massive Beeinträchtigung des Regelbetriebs möglich) wird die gravierende Ausnutzung einer Zero-Day Schwachstelle beschrieben. Das außerordentlich Kritische hierbei ist der Tatsache geschuldet, dass „Patches nicht direkt verfügbar waren und Angreifer durch systematische Ausnutzung kryptografischer Schlüssel … Machine Keys entwenden und somit persistenten Zugang auch nach dem Patchen erlangen konnten". Alleinig die Sicherheitsupdates bzw. Patches aufzuspielen, ist somit völlig unzureichend. Es müssen zwingend neue Schlüssel von Microsoft entsprechend den Ratschlägen von Microsoft eingetauscht werden. Ebenso pikant dabei ist der Umstand, dass „zum aktuellen Zeitpunkt ausschließlich von Organisationen in Eigenregie betriebene On-Premise SharePoint Server" verwundbar sind. Eben diese On-Premise-Lösungen werden oftmals als die einzig verfügbare Lösung aus einer lizenz- oder patentrechtlichen Abhängigkeitslage von Drittstaaten genannt, obwohl man, wie dieser Sicherheitshinweis eindrucksvoll beschreibt, noch nicht einmal über eigene nationale digitale Schlüssel dafür verfügt. De facto digitale Unsicherheit, da angreifbar, im Einklang mit einer direkten Abhängigkeit bei digitalen Schlüsseln von Nicht-EU-Tech-Giganten. Siehe: BITS-H # 2025-262781-1032 | Version 1.0 vom 21.07.2025

[6] https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf Abruf am 18.07.2025. S. 66f.

[7] Bereits Anfang des Jahres wurden in den Veröffentlichungen von Palt & Team und Palt (beides 2025, vgl. https://inp-hamburg.com/inp-wissenschaft/, Abruf 22.07.2025) immanente Systemfehler aufgezeigt. Der hier vorliegende Denkanstoß zeigt, wie Systemfehler sich über die Zeit und seit der Veröffentlichung aufaddieren.

[8] Was ggf. bedeutet, Projekte (sicherheitspolitisch und haushalterisch) neu oder noch einmal auf den Prüfstand zu bringen.

hinter diesen libertäre, egalitäre oder anthroposophische Menschenbilder und Menschenrechtsverständnisse – offen oder verdeckt – verbergen, die unseren im Grundgesetz verbrieften entgegenlaufen. Wozu auch die Frage gehört, welchem Menschenbild und Menschenrechtsverständnis die hinter diesen Partnerschaften stehenden Investoren zugeneigt sind.

- In Konsequenz leitet sich drittens daraus die Forderung ab, Parteipolitik und -interessen sowie ideologische Strömungen innerhalb der Parteien dem staatsräsonalen Interesse und den daraus abgeleiteten Vorgaben ebenso unterzuordnen wie die wirtschaftlichen Interessen der Unternehmen, die in Gänze oder mit dem Staat als Anteilseigner mit Sperrminorität unterwegs sind.[9]

Problembeschreibung: Kill Switch und Datenabfluss

Im zuvor beschriebenen Kontext sind die nun folgenden Ausführungen als Denkanstoß zu sehen, wie das Thema angegangen werden kann:
Für die europäische Union ist es schwierig, das EU-Recht so anzupassen, dass eine vertrauenswürdige Nutzung der US-Clouds für Behörden und Organisationen mit Sicherheitsaufgaben umsetzbar ist. Zeitgleich ist es schwierig, einen fremdstaatlichen Zugriff technisch und organisatorisch zu erkennen und zu verhindern. Damit stehen die Sicherheitsziele Vertraulichkeit und Verfügbarkeit im Zentrum dieses Papiers.[10] Sollten die USA den drei großen Cloud-Dienstanbietern Google Cloud, Microsoft Azure und Amazon Web Services (alle US-amerikanisch) eine Zusammenarbeit mit Europa oder gezielt Deutschland untersagen, wären gravierende Störungen (auch für On-Premise-Anteile) dieser Anbieter unvermeidbar – unabhängig von deren Hardware. Ein noch größeres Risiko für die Vertraulichkeit der deutschen/europäischen Daten ergäbe sich, wenn die USA den drei großen Cloud-Anbietern und anderen Dienstleistern die Pflicht auferlegte, die Daten aus diesen Clouds der US-Regierung zu übergeben. Ein weiterer, bisher oft unterschätzter Risikofaktor

[9] Ebenso gilt es, andere Schieflagen gerade zu ziehen, wie sich an folgendem Statement von Timotheus Höttges, dem Vorstandsvorsitzenden des einzigen deutschen Providers mit dem Staat als Anteilseigner mit Sperrminorität verdeutlichen lässt, der sich auf „langwierige Genehmigungsverfahren, aber auch die mangelnde Nachfrage des Staates“ bezog: „Wenn die Bundesregierung ‚Souveränität‘ sagt, aber dann ihre ganze Datenstruktur an amerikanische Hyperscaler auslagert, dann wird da kein Schuh draus“ (zitiert aus: Kerkmann, Scheuer, Bomke & Schimrosik. Cloud Anbieter: So soll Deutschland unabhängig von US-Digitalkonzernen werden. https://www.handelsblatt.com/technik/it-internet/cloud-anbieter-so-soll-deutschland-unabhaengig-von-us-digitalkonzernen-werden/100120584.html, Abruf am 20.07.2025).
Das Selbstverständnis des BMVG besteht darin, digitale Sicherheit als eine Angelegenheit zwischen den Sicherheitsbehörden, deren IT- und Telekommunikationsdienstleistern, der Bundeswehr und der BWI zu betrachten. An der Stelle schließt sich der Kreis zum Hinweis auf den Koalitionsvertrag – und zur veröffentlichten Projektskizze (vgl. Palt & Team, 2025) und zur vorab veröffentlichten Rede zum Marine-Workshop der DWT e. V. (Palt, 2025), https://inp-hamburg.com/inp-wissenschaft/, Abruf am 22.07.2025.

[10] Bereits 2018 hatte die Trump-Regierung mit dem ‚Cloud Act‘ alle US-Cloud-Anbieter verpflichtet, auch für den Fall, dass Daten ihrer Nutzer sich außerhalb der USA befinden, diese auf Anfrage an US-Behörden herauszugeben. Daher ist es kaum verwunderlich, dass nicht nur deutsche Aufsichtsbehörden hinter verschlossenen Türen ihre tiefgreifende Sorge darüber äußern, ob US-amerikanische Cloud-Dienste innerhalb der EU auch Datenschutz-Grundverordnungs-konform genutzt werden können. Diesbezüglich halbherzig der EU angebotene vertrauensbildende Maßnahmen der Biden-Administration konnten nicht ernsthaft Abhilfe schaffen.

besteht in der möglichen Existenz technischer „Backdoors“ in proprietärer Software und sogar in Firmware bzw. Hardwarekomponenten. Diese könnten – gewollt oder ungewollt – externen Akteuren Zugriff auf kritische Systeme ermöglichen. Da die Prüfung und Verifikation proprietärer Systeme nur eingeschränkt möglich sind, entsteht eine schwer kontrollierbare Blackbox-Infrastruktur, die das Prinzip der Vertrauenswürdigkeit infrage stellt.
Damit stehen Vertraulichkeit und Verfügbarkeit von IT-Systemen in der Verwaltung, auch mit Blick auf Wartung, Zugriffsrechte und Weiterentwicklung, substanziell infrage. Der potenzielle Verlust der Integrität und Verfügbarkeit relevanter Daten stellt Wirtschaft, Verteidigung und unsere gesamtgesellschaftlichen systemrelevanten Sicherungssysteme (Energie, Gesundheit, Logistik etc.) vor signifikante Herausforderungen.

Ziel und Aufbau

Das hier vorgelegt Papier ist ausdrücklich keine wissenschaftliche Arbeit. Verfolgt wird das Ziel, Denkanstöße in zwei Richtungen zu geben:

1. Erstens wird die politische und gesellschaftliche Herausforderung adressiert, die darin besteht, aus staatsräsonalen Gründen innere und äußere Sicherheit mit horizontalem (von der Bundesregierung über die Bundesländer und Kommunen bis zu jeder einzelnen Person) und vertikalem (Digitales, Inneres, Äußeres, Verteidigung) Durchgriffsrecht, aufgehangen beim Bundeskanzleramt umzusetzen.[11] Was auch beinhaltet, Parteipolitik und ideologische Ausrichtungen innerhalb der Parteien sowie den Business Case der Unternehmen, die vollständig oder mit Sperrminorität den Staat als Anteilseigner haben, hinsichtlich ihrer (bislang vorrangig wirtschaftlichen Interessen und Vorgaben) auf eine andere Spur zu bringen.
2. Zweitens wird ein technologischer Ansatz inklusive Umsetzungsvorschlag und konkretem Zeitplan ins Spiel gebracht. Mit Blick auf grundsätzliche Risiken in der Informationssicherheit (Vertraulichkeit/Verfügbarkeit) erscheint als sinnvoller Lösungsansatz, den urheberrechtlichen, lizenzrechtlichen sowie patentrechtlichen Abhängigkeiten sofort nachzugehen (IPA FREE): valide, schonungslose, ehrliche Diagnostiken zur Implementierung durchsetzungsfähiger De-Risking-Strategien gegenüber systemischen Rivalen (China, Russland) und wirtschaftlichen Konkurrenten.

Der bereits erfolgten Beschreibung von Kontext und Ausgangslage sowie Problembeschreibung folgen der Lösungsansatz und die Beschreibung von Mehrwert und Machbarkeit. Das Papier endet mit einem kurzen Fazit.

Die Autoren treibt die Überlegung an, dass zeitkritische einsatzrelevante militärische Dienste unserer gesamtstaatlichen Verteidigung nicht einmal ansatzweise softwareseitig durch Abhängigkeiten von Drittstaaten demaskiert, offengelegt, infiltriert und/oder durch

[11] Nicht zu verkennen ist dabei, dass aufgrund beispielsweise des hohen Energiebedarfs von KI, des Schutzes kritischer Infrastrukturen und der Finanzierbarkeit der Lösungen auch weitere Ministerien betroffen sind.

ausländische Androhungen politischer wie auch technischer Kill-Switches infrage gestellt werden können sollten.

Lösungsansatz

Die im Papier diskutierte softwareseitige Lösung einer Open-Source-Strategie, blendet die Abhängigkeit von Hardware-Komponenten aus, die ebenfalls als signifikantes Risiko hinsichtlich der diskutierten Schutzziele betrachtet werden sollte.[12] Die softwareseitige Lösung besteht in der stringenten Umsetzung einer Open-Source-Strategie.[13] Bestehende Open-Source-Produkte müssen nicht zeitraubend und kostenintensiv neu entwickelt werden. Die Kosten für Implementierung und Betrieb bleiben allerdings weiterhin bestehen. Die Bundesregierung trifft die Entscheidung zur Gründung der Open Source GmbH und erteilt den Auftrag an die dann gegründete Open Source GmbH, mit einem ressourcenminimalistischen Einsatz gezielt ihre bestehende Expertise dafür einzusetzen, digitale Instrumente der Open Source Community zu übernehmen, zu begleiten, zu zertifizieren und weiterzuentwickeln, indem bestehende dislozierte Expertise-Kapazitäten national gebündelt, gefördert und ausgebaut werden.
Ein risikobasierter Ansatz zur Priorisierung der Umsetzung könnte folgendermaßen aussehen:

- **Kurzfristig:** Nutzung von US-Clouds mit maximaler Kontrolle, technischen Verschlüsselungs-Gateways und rechtskonformen Verträgen
- **Mittelfristig**: Aufbau europäischer Infrastruktur, Förderung von Open-Source-Clouds (z. B. Sovereign Kubernetes)
- **Langfristig:** Analyse aller intellectual property dependencies (IPA), Aufbau eines „digitalen Katastrophenschutzplans“ für strategische Notfälle[14]

[12] Auf hardwareseitige Implikationen sei dennoch in diesem Papier hingewiesen.
[13] Folgende Herausforderungen werden gesehen:
1. Die technologische Rückständigkeit Europas/Deutschlands:
So sehr es wünschenswert wäre – Europa hat bisher kein konkurrenzfähiges Hyperscale-Cloud-Angebot hervorgebracht. Gaia-X ist fragmentiert, Sovereign Clouds wie T-Systems oder OVHcloud sind Nischenlösungen. KI-Lösungen, insbesondere leistungsstarke LLMs, sind nicht vorhanden.
2. Die Gefahr eines digitalen Protektionismus:
Ein radikales De-Risking kann zur Abschottung führen – mit wirtschaftlichen Kollateralschäden. Was passiert mit der Innovationskraft europäischer Unternehmen, wenn ihnen der Zugang zu weltweit führender KI-Infrastruktur (z. B. Azure OpenAI, AWS SageMaker) genommen wird?
Diese Herausforderungen sind in einer mittel- und langfristigen Strategie zu verorten und sowohl mit Expertise als auch mit den notwendigen Ressourcen auszustatten.
[14] Backdoors in US-Anbietern (NSA & Co.): Dual_EC_DRBG in Juniper ScreenOS: 2015 entdeckte Juniper Networks in seinem ScreenOS-Code nicht nur einen Hardcoded-Master-Passwort-Backdoor, sondern auch heimlich eingeführte NSA-kompromittierte Zufallszahlengeneratoren (Dual_EC_DRBG). Diese erlaubten es, verschlüsselte VPN-Sitzungen zu entschlüsseln und administrative Kontrolle zu erlangen (vgl. wired.com).
Wissenschaftliche Analyse bestätigt Manipulation: Eine unabhängige Studie zeigte, dass die angeblichen Gegenmaßnahmen von Juniper gegen Dual_EC nie ausgeführt wurden und die Hintertür schon in einer ScreenOS-Version von 2008 steckte (vgl. eprint.iacr.org).

Ein solcher strategischer Ausbau nationaler Ressourcen und die Erweiterung des vorhandenen Know-hows wird signifikante Investitionen benötigen.[15] Eine zivilmilitärische lizenzrechtliche Adaption ist risikolos per sofort umsetzbar[16]: Ziel wäre die IT-technisch autonome Kriegstüchtigkeit für 2029. Voraussetzungen wären:

- Ausbildung und Training personeller Ressourcen,
- Software-Erprobungen sind bis Ende 2027 zu vertesten,
- eine Freigabe der Software durch die DEUMilSAA (Deutsche militärische Security Accreditation Authority),
- Readiness for Federated Mission Network, um mit anderen Nationen gemeinsam im Gefecht wirken zu können,
- Abschluss der Entwicklungen zwingend bis Ende 2026.

Was in 2025 nicht beschafft wird oder nicht bereits durch erste Erprobungen (Minimum Viable Product) seinen Nutzen unter Beweis stellen konnte, hat für eine Kriegstüchtigkeit 2029 keinen Nutzen – was bedeutet: Hier ist ein gesamtstaatlicher Ansatz gefragt, der nicht nur für das Verteidigungswesen gilt. Auch hierzu äußert sich der Koalitionsvertrag.[17] Daher muss die zentrale Sicherheits-Governance für eine souveräne, Open Source-basierte Plattformlösung entwickelt und beim Bundesamt für Sicherheit in der Informationstechnik (BSI) angesiedelt werden. Wer dann die Beschaffung auslöst, wird noch zu klären sein. Sicher ist: Ausschließlich das BSI gewährleistet als nationale Prüfinstanz, Koordinationsplattform und Sicherheitsanker nicht nur die Zertifizierungen[18], sondern auch die sicherheitspolitische Ad-hoc-Fähigkeit zur Übernahme, Stabilisierung und Weiterentwicklung im Krisenfall.

Ein potenzielles Risiko bei der Umsetzung einer solchen Open-Source-Strategie liegt in der fragmentierten politischen und organisatorischen Struktur Deutschlands. Frühere Initiativen, wie etwa Gaia-X, sind nicht zuletzt daran gescheitert, dass föderale Interessensgegensätze,

---

Technische Expertise deckt NSA-Eingriff auf: Sicherheitsexperten wiesen nach, dass Juniper beim Einbau des Dual_EC_DRBG seine eigenen Kontrollen unwirksam machte, was stark auf eine externe, bevollmächtigte Partei – etwa die NSA – hindeutet (vgl. csoonline.com).

[15] Demgegenüber belasten erhebliche finanzielle Aufwendungen durch Lizenzgebühren den Haushalt: „Alle Ressorts der Bundesregierung haben laut einer heise online vorliegenden Übersicht 2023 erstmals mehr als eine Milliarde Euro für die Nutzung von Lizenzen für Computerprogramme und IT-Services ausgegeben: Die einschlägigen Gebühren sind von rund 771 Millionen Euro im Jahr 2022 auf über 1,2 Milliarden in 2023 gestiegen. Das entspricht einer Zunahme von 441 Millionen Euro beziehungsweise rund 57 Prozent." Quelle: Bund: Lizenzkosten für Microsoft auf hohem Niveau, insgesamt neuer Rekord. heise online; Abruf am 01.06.2024.

[16] Die Sicherstellung der Investitionen in Ressourcen (Expertise und monetär) und in die oben in Schritten beschriebene Entwicklung ist jedoch notwendig.

[17] „Auch den IT-Einkauf des Bundes wollen wir zentral strategisch steuern, um Abhängigkeiten von monopolistischen Anbietern zu reduzieren und den Digitalstandort Deutschland zu stärken", https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf, S. 65, Abruf am 20.07.2025.

[18] Beispielsweise RHEL 9.0: VID 11379 (09.01.2024) – evaluiert nach Collaborative PP v4.3 + SSH & TLS, Eingetragen in NIAP-Produktliste, ebenfalls automatisch durch CCRA vom BSI anerkannt. RHEL ist derzeit in der Zulassung für eine Bare-Metal-Server-Lösung mit einer Open Source Kubernetes Platform für eingestufte Infrastruktur (wie z. B. VS-NfD durch eine Behörde des BSI). Ergänzend dazu: https://www.linkedin.com/posts/secunet-security-networks-ag_cloud-digitalesouveraeunitaeut-itsicherheit-activity-7353407454556160001-04Xx?utm_medium=ios_app&rcm=ACoAABa9FxcBZptQkvNvgvJKc7Bopyf-KMaNZaQ&utm_source=social_share_send&utm_campaign=mail , Abruf am 22.07.2025.

Ressortegoismen und fehlende zentrale Steuerungsbefugnisse zu einem Auseinanderdriften der Zielvorstellungen führten. Um dieser Gefahr zu begegnen, muss die Sicherheits-Governance zwingend beim Bundesamt für Sicherheit in der Informationstechnik (BSI) konzentriert werden, das über die Zertifizierung mit klaren regulatorischen Durchgriffsrechten ausgestattet ist. Nur so kann gewährleistet werden, dass das Vorhaben nicht im politischen Klein-Klein versandet, sondern aus einer einheitlichen sicherheitspolitischen Perspektive heraus koordiniert, zertifiziert und im Krisenfall souverän weiterentwickelt werden kann.
Ein weiteres Risiko liegt in der strukturellen Spannung zwischen dem notwendigen sicherheitspolitischen Zielhorizont einer souveränen Plattformarchitektur und den Erfordernissen agiler, innovativer Open-Source-Entwicklung. Ein zu stark zentralistisch durchgetakteter Rollout-Plan birgt die Gefahr, dass technologische Entwicklungen zu starr und zu spät auf neue Anforderungen oder Sicherheitslücken reagieren. Um dem entgegenzuwirken, ist eine staatlich getragene Open-Source-Governance zu etablieren, die einerseits verbindliche Roadmaps definiert, andererseits aber Freiräume für dezentrale Community-Innovation schafft. Dies erfordert die aktive Förderung eines nationalen Open-Source-Entwicklungsnetzwerks, das kontinuierlich in die Plattformpflege eingebunden ist und gemeinsam mit dem BSI an sicherheitsrelevanten Stable-Forks arbeitet. Auf diese Weise kann gewährleistet werden, dass die technologische Innovationskraft der Open-Source-Community nicht verloren geht, sondern zur operativen Stärke des Gesamtprojekts wird.

Umsetzung und strategischer Mehrwert

Bis 2029 kann davon ausgegangen werden, dass alle relevanten Open-Source-Kryptographie-Lösungen (OpenSSL und OpenSSH) Post-Quanten-Algorithmen verwenden können. Darüber hinaus werden die meisten Linux-Distributionen nicht nur softwareseitig quantensicher ausgerichtet, sondern man konzentriert sich neben der softwareseitigen Übertragung auch auf ein quantensicheres und damit zukunftssicheres Zusammenspiel der Applikationen auf Soft- und Hardwareebene[19].
Folgende Umsetzung bietet sich an:

1.) Unmittelbare querschnittliche Beteiligung an der Entwicklung der Open-Source-Enterprise-fähigen Produkte und Betriebssysteme[20] sowie der dazugehörigen noch auszuwählenden Softwareprodukte, um bestehende Expertise auszubauen und zu bündeln (fallen ausländische Programmierer weg, könnten Kernelemente jederzeit national aufrechterhalten werden und den eigenen Weiterbetrieb ermöglichen).

[19] https://www.ibm.com/quantum/assets/quantum-safe/IBM_Quantum_Safe_Roadmap.pdf

[20] Ein prominentes Beispiel für systemische Abhängigkeit ist der SAP-Technologiestack. SAP S/4HANA wird aktuell ausschließlich auf Red Hat Enterprise Linux unterstützt – einem US-Produkt, dessen Steuerung, Lizenzierung und Pflege nicht in europäischer Hand liegt. Es gibt keine patentrechtlichen Abhängigkeiten, nur eine Subscriptions- und Support-Lizenz für Unterstützung, Fehlerbehebung und der Nutzung, um jederzeit funktionale Weiterentwicklungen am Produkt zu erhalten. Das Produkt kann nach erstem Wartungsvertrag auch ohne Wartung genutzt werden. Dann obliegen alle Aufgaben dem Nutzer. Eine Organisation wie die Open Source GmbH könnte diese Aufgabe in Deutschland / der EU (mit der notwendigen und erforderlich Anzahl an Entwicklern) nicht nur für Notfalllagen übernehmen. Ebenfalls möglich wäre eine Unterstützung der SAP dahingehend, dass sie ihre Produkte auf anderen Plattformen zertifizierbar macht.

2.) Maßnahmen zum umfänglichen nationalen Erhalt aller Rechte an enterprisefähigen Open-Source-Produkten, um Weiterentwicklung und Support sicherzustellen. Hier empfiehlt es sich, sich mittels Open Source GmbH mit eigener Entwicklungs- und Support-Expertise in die Weiterentwicklungs-, Pflege- und Support-Wertschöpfungskette des Enterprise-Open-Source-Anbieters einzufügen, um vollumfängliche Expertise aufzubauen und die Fähigkeit für eigenständigen Support und Pflege zu erlangen.
3.) Implementierung eines nationalen Cloud-Dienstanbieters[21] durch die Deutsche Telekom als Konzern mit Staatsbeteiligung mit Sperrminorität: mit Nutzung der europäischen IaaS (Infrastructure as a Service) der Deutschen Telekom, um in unterschiedlichsten Krisenfällen nicht nur europaweit, sondern auch international handlungsfähig zu bleiben.
4.) Nutzung und Weiterentwicklung der bereits standardisierten quantenkryptographischen Verschlüsselungen, unter Einbindung der an der Entwicklung der Verschlüsselung beteiligten deutschen und europäischen Forscher, für nationale quantenkryptographische Verschlüsselungen, die auch international anerkannt werden (Stärkung der deutschen Industrie mit Schlüsseltechnologie), insbesondere unter Vermeidung einer Abhängigkeit von Microsoft.
5.) Aufbau einer Open Source GmbH in Deutschland. Das BSI übernimmt die Zertifizierung der Open Source GmbH durch ein eigenes Lenkungsgremium auf Abteilungsleitungsebene in Verbindung mit IPA-Kapazitäten. Nicht zuletzt dadurch wird auch querschnittlich und interdisziplinär die Zusammenarbeit zwischen Bund und Ländern auf dem Weg zur Cyberdominanz im Krisenmanagement innerhalb des Innenressorts als zentrale Aufgabe digitaler Souveränität nationaler Verteidigungsfähigkeit gebündelt.
6.) Die Open-Source-Plattformarchitektur wird in das nationale Cyber-Lagebild des Cyber-Abwehrzentrums (Cyber-AZ) eingebettet, um im Fall hybrider Angriffe unmittelbare operative Reaktionsfähigkeit sicherzustellen.
7.) Langfristiges Ziel muss auch die vollständige Ablösung proprietärer Hardware-Komponenten sein, um jede Hintertür zu eliminieren und maximale Transparenz, Auditierbarkeit und Kontrolle sicherzustellen. Dafür sollte parallel zur Softwaremigration ein modularer Fahrplan greifen, der auf offene, nachvollziehbare Designs setzt, die vom BSI geprüft, zertifiziert[22] und sukzessive in die nationale

[21] Gemäß der Projektskizze (vgl. Palt & Team, 2025) schlagen wir die Deutsche Telekom vor – als einzigem deutscher Provider mit dem Staat als Anteilseigner mit Sperrminorität.

[22] Auch hier müssen im Vorfeld systemische Unschärfen in der strukturellen Nähe zwischen sicherheitskritischen IT-Dienstleistern und Zertifizierungsinstanzen im staatlichen Bereich zwingend aufgelöst werden. Zwar nimmt die BWI selbst keine Zertifizierungsaufgaben wahr, doch als zentrale IT-Dienstleisterin der Bundeswehr ist sie vielfach für die Umsetzung, den Betrieb und die Integration von Systemen verantwortlich, die im militärischen Kontext über die Deutsche militärische Security Accreditation Authority (DEUmilSAA) zertifiziert bzw. akkreditiert werden. Damit ergibt sich ein komplexes Geflecht aus Dienstleistung, militärischer Zertifizierung und späterer Schnittstelle zu zivilen Behörden, insbesondere dort, wo die BWI auch Leistungen für zivile Bundesbehörden erbringt, etwa für das Bundesamt für Sicherheit in der Informationstechnik (BSI), das wiederum eigenständig als nationale Zertifizierungs- und

Supply-Chain integriert werden. So entsteht eine durchgehende Vertrauenskette von der Hardware über das Betriebssystem bis in die Container-Orchestrierung – für echte Unabhängigkeit bis in die Silizium-Ebene.

Diese Maßnahmen bilden nicht nur das zukünftige Fundament eines national gesteuerten Enterprise-Supports, sondern sie etablieren auch den Grundstock

- zu verlässlichen Softwareprodukten und deren technologischer Weiterentwicklung
- zur Integration moderner Antivirendetektoren
- zur zukunftsfähigen Virtualisierung für die Reduzierung der VMware- Abhängigkeit
- zu sicheren generativen KI-Modellen zur Weiterentwicklung
- zur Projektanbieter-Unabhängigkeit
- zur Trennung (unabhängige Verträge) von Enterprise-Support-Anbieter und Projektanbieterleistung
- zur Sicherstellung der IP-Entwicklung für die Rückführung in Enterprise-Open-Source-Lösungen und
- der Supportfähigkeit der Entwicklungsanteile.

Unser besonderes Augenmerk gilt hierbei dem Aufbau einer Open Source GmbH in Deutschland mit zentraler Aufgabe einer Entwickler-Expertise-Bildung aus Deutschland / der EU. Aufgabe ist diese Expertise dauerhaft und redundant an sich zu binden, um letztendlich neben einem zuverlässigen unabhängigen Support auch die Weiterentwicklungsmöglichkeiten für den Enterprise-Open-Source-Anbieter mit folgenden strategischen Mehrwerten darzustellen:

Zukünftig dauerhaft sichere Open-Source-Lösungen mit zu entwickeln bedeutet, tiefen Inside-Code zu erhalten und eine Ad-hoc-Fähigkeit für eine sofortige Übernahme des Gesamtsupports und für die Weiterentwicklung im Krisenfall sowie die unmittelbare Nutzung aller verfügbaren Funktionen. Das bedeutet auch den begleitenden wissenschaftlichen Aufbau einer Forscher-/Entwickler-Community, auch um Open-Source-Lösungen auf Schadsoftware prüfen zu können und sichere Software zu zertifizieren.

Von ausgesprochen sicherheits- und verteidigungspolitischer Bedeutung wird die Bereitstellung von sicheren und supporteten Eigenentwicklungen im Rahmen deutsch-europäischer Partner-Lösungen sein, welche nicht als Enterprise-Open-Source für die Allgemeinheit verfügbar sein werden. Damit liegen zeitkritische, einsatzrelevante militärische Dienste weiterhin in nationaler und eigener Verantwortung der jeweiligen europäischen Partner und erfüllen einen lokalen Betrieb auch in einer zukunftsfähigen virtualisierten Infrastruktur (VMs und Container).

Bundesweit und im europäischen Rahmen werden kritische Infrastrukturen in ihrer Steuerung, der Logistik und Energieversorgung auf unabhängigen und sicheren digitalen Plattformen eingerichtet werden können. Ausländische (nicht europäische) KI in Anlagen und Fahrzeugen

Prüfinstanz agiert. Ein systematischer, ressortübergreifender Abgleich der jeweiligen Zertifizierungslogiken, militärisch wie zivil, wäre hier ein geeigneter nächster Schritt.

wird national ersetzt und verhindert den unkontrollierten Abfluss systemerhaltender Daten, angreifbarer Verbindungen und logistisch sensibler Routen.
Diese Open-Source-Governance unter BSI-Steuerung wird als Blaupause für europäische Partner dienen und zeigt einen gangbaren Weg zur technologischen Unabhängigkeit im Rahmen einer gemeinsamen sicherheits- und verteidigungspolitischen Architektur.

Fazit: Nicht wahrhaben wollen …

Der bislang eingeschlagene Weg zeichnet sich vor allem dadurch aus, dass folgende Prämissen nicht wahrgehabt werden (wollen):
Es gibt – und das ist nicht von der Hand zu weisen, gleichwohl kann man es nicht wahrhaben wollen – innerhalb von Demokratien unterschiedliche Menschenbilder und Menschenrechtsverständnisse, die unterschiedliche Zielvorstellungen zur Ausgestaltung von Demokratien nach sich ziehen und gezielt umsetzen wollen. Ignorieren wir diese und gehen – gewollt oder ungewollt, bewusst oder unbewusst – Partnerschaften mit Akteuren ein, die nicht unserem Menschenbild entsprechen, riskieren wir, politisch, technologisch und gesellschaftlich unterwandert und/oder ausgehebelt werden zu können. Mit unserer nationalen digitalen Souveränität laufen wir Gefahr, Deutungshoheit und Narrative abzugeben und damit das, was Basis und Ankerpunkt unseres Menschenbilds und Menschenrechtsverständnisses ist: Artikel 1 des Grundgesetzes der Bundesrepublik Deutschland: „Die Würde des Menschen ist unantastbar."
Indem in diesem Papier ein gemeinsamer gesamtgesellschaftlicher Steuerungskreis über die Ressorts vorgeschlagen wird, wird formal dem Koalitionsvertrag entsprochen und ein Finger in die Wunde gelegt, dass innere und äußere Sicherheit bislang nicht verbunden sind – auch nicht mit Blick auf eine nationale Software-Autonomie, die in diesem Papier beispielhaft durchgespielt wird. Dass der Schwenk auf eine Open-Source-Strategie nur eine Facette dessen ist, was eine gesamtstaatliche Steuerung erforderlich macht, wird anhand der Umpriorisierung (Sicherheit vor Business Case) der Unternehmen klargemacht, bei denen der Staat Anteilseigner ist. „Nicht wahrhaben wollen" scheint sich bei allen Beteiligten als roter Faden durchzuziehen.
Die Güteabwägung, die der Staat nun treffen muss, weil ein staatsräsonaler Ansatz mit Blick auf unser grundgesetzlich verbrieftes Menschenbild verstörend anmuten muss, verdeutlicht den Zielkonflikt: Wie sieht die Schrittfolge aus, wie die Balance, die auszutarieren ist, um unser Menschenbild und unser Menschenrechtsverständnis zu schützen und zu erhalten.
Das müssen wir nicht nur wahrhaben wollen. Das müssen wir dann auch tun.

Anhang

Was ist Secure Boot?

Secure Boot ist eine Schutzfunktion des UEFI-Firmware-Standards, die dafür sorgt, dass beim Starten eines Rechners nur vertrauenswürdig signierte Software ausgeführt wird. So wird verhindert, dass Bootloader, Treiber oder Firmware-Module, die manipuliert wurden (z. B. Bootkits oder Rootkits), das System kompromittieren.
Erklärung Secure Boot
Auf der Erlaubnis-Liste (Allowed Signature Database, DB) steht, welche Firmen oder Programme (wie Microsoft) als „sichere Handwerker" gelten. Beim Einschalten schaut der Computer nach, ob der gerade geladene Boot-Teil (Bootloader, Treiber usw.) von einem dieser Einträge unterschrieben ist. Wenn ja, darf er starten – so weißt du, dass nichts Fremdes oder Gefährliches geladen wird.

Microsoft-Zertifikat

Dieses CA-Zertifikat steht auf der Allowed Database (DB) und erlaubt es, Firmware-Module, die von Microsoft signiert wurden (bspw. der „Shim"-Bootloader oder Windows-Bootloader), zu starten. Alles, was mit diesem Schlüssel signiert ist, gilt als vertrauenswürdig.
UEFI-Einstellungen „Allow Microsoft 3rd party UEFI CA" oder „Enable Microsoft UEFI CA key" – das ist genau dieses Zertifikat, das dafür sorgt, dass Windows, Linux-Shim und andere von Microsoft signierte Boot-Komponenten automatisch starten dürfen.
Die meisten PCs, Laptops, physikalischen Server und Hypervisor (z. B. VMWare) werden ab Werk mit UEFI-Firmware ausgeliefert, die nur den Microsoft-Root-CA-Schlüssel im Allowed Database (DB) enthält. Das heißt: Die Firmware vertraut nur Programmen, die mit diesem Microsoft-Schlüssel signiert sind.

Alternative Ansätze und die Abhängigkeit von Microsoft-Zertifikaten

Use-Your-Own/Shielded VMs bietet eine Möglichkeit, die Abhängigkeit von Microsoft-Zertifikaten zu reduzieren.

Wie funktioniert der automatische Umgang mit eigenen Zertifikaten?

Der Cloud-Anbieter stellt eine Infrastruktur bereit, bei der Kunden ihre eigenen Zertifikate (z. B. eigene Root-CA) einmalig hochladen können. Diese Zertifikate werden dann automatisch in die UEFI-Umgebung der VMs integriert. Es ist keine manuelle Interaktion durch den Endnutzer notwendig – der Cloud-Provider sorgt dafür, dass alle VM-Instanzen korrekt mit den eigenen Zertifikaten ausgestattet sind. Bei Bedarf können Kunden die Zertifikate regelmäßig erneuern, ohne dass es zu einem manuellen Eingriff in jede VM kommt. Die Verwaltung erfolgt zentral durch den Cloud-Anbieter.
Die Informationen zu Shielded VMs, wie sie beispielsweise bei Google Cloud verfügbar sind, zeigen, dass dort die Möglichkeit besteht, kundenspezifische Secure Boot-Zertifikate für benutzerdefinierte Images zu integrieren. Dies umfasst das Hochladen von Platform Keys (PK),

Key Exchange Keys (KEK) und anderen Zertifikaten, um Vertrauensbeziehungen zwischen Plattform, Firmware und Betriebssystem herzustellen.
Bei der Open Telekom Cloud fehlen jedoch konkrete Hinweise darauf, dass ein vergleichbarer Mechanismus für kundeneigene Secure-Boot-Zertifikate angeboten wird. Ob und wie solch ein Service durch die Deutsche Telekom bereitgestellt wird, muss angefragt werden.

(Un-)Abhängigkeit von Microsoft

Auch wenn eigene Zertifikate hochgeladen werden können, bleibt in der Regel der Microsoft-Shim ein wichtiger Bestandteil, um den Secure Boot zu ermöglichen.
Der Microsoft-Shim fungiert als Zwischenschicht, die die Integrität der Bootprozesse sicherstellt, indem es die Integrität der geladenen Software überprüft.
In diesem Szenario könnte der Microsoft-Shim mit dem eigenen Zertifikat kombiniert werden – das bedeutet, dass man vom Microsoft-Zertifikat unabhängig sein kann, jedoch nach wie vor auf den Microsoft-Shim als Initialisierer angewiesen ist. Das heißt, der Boot Loader müsste ersetzt werden.
Red Hat Enterprise Linux (RHEL) verwendet beispielsweise standardmäßig den Microsoft-Shim für Secure Boot. Es bietet jedoch umfassende Optionen zur Konfiguration des Secure-Boot-Prozesses, sodass der Microsoft-Shim durch benutzerdefinierte Lösungen ersetzt werden kann. Durch die Anpassung der Bootloader-Konfiguration, die Verwendung eigener Zertifikate und die Verwaltung von Secure Boot über UEFI ist es möglich, ein Shim-freies Setup zu realisieren.

Hamburg, Juli 2025

ISSN 1865-6137

Jenseits der Begrenztheit

Impressum:
INP – Institut für Nachhaltiges Projektmanagement
Direktorin & Inhaberin: Prof. Dr. Beatrix Palt
Waldring 12 | 21272 Egestorf
info@inp-hamburg.com | www.inp-hamburg.com