Karlsruher Thesen zur

Digitalen Souveränität Europas

Prof. Dr. Jörn Müller-Quade
Professor am KIT, Sprecher von KASTEL

Prof. Dr. Ralf Reussner
Professor am KIT, Vorstand FZI

Prof. Dr. Jürgen Beyerer
Professor am KIT, Direktor Fraunhofer IOSB

Mit Beiträgen von

Prof. Dr. Bernhard Beckert, KIT
Prof. Dr. Hannes Hartenstein, KIT
Luise Kranich, FZI
Jan Wiesenberger, FZI

Motivation

Das Karlsruher Institut für Technologie, das FZI Forschungszentrum Informatik und das Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung stehen als Forschungseinrichtungen mit vielen IT-Anwenderinstitutionen, wie öffentlichen Verwaltungen, kleinen und mittelständischen Unternehmen und Großkonzernen, in ständigem Austausch. Ebenso sind sie mit internationalen Wissenschaftsgemeinschaften eng vernetzt. Das Erreichen einer Digitalen Souveränität in Europa kommt dabei häufig zur Sprache.

I Wünsche für eine Digitale Souveränität

1. Wir müssen unsere Gesetze und Wertvorstellungen gegenüber Internet-Giganten durchsetzen können.
2. Wir wünschen uns die Kontrolle über Daten, auch wenn sie in der Cloud gespeichert oder verarbeitet werden.
3. Wir wünschen uns eine staatliche Kontrolle der Löschung von personenbezogenen Daten.
4. Wir wünschen uns flexible Geschäftsbedingungen von Internetservices, bei denen Anwender selbst entscheiden, inwieweit sie mit ihren Daten oder mit Geld bezahlen.
5. Wir wünschen uns, dass Internet-Seiten auf Basis nachvollziehbarer Suchmaschinen-Algorithmen gefunden werden.
6. Wir möchten den Komfort neuer sprachgesteuerter, internetbasierter Assistenzsysteme nutzen können und dabei wissen, was mit unseren Daten geschieht.
7. Wir brauchen die Kontrolle über die Hardware und Software, auf denen unsere Sicherheitsarchitekturen aufsetzen.
8. Wir brauchen Betriebssysteme auf Mobiltelefonen, Computern und Netzwerkinfrastrukturen, denen wir vertrauen können.
9. Wir brauchen software- und internetbasierte Infrastrukturen der Zukunft, wie Energieversorgung, Gesundheitswesen oder Mobilitätssysteme, unter der Kontrolle der europäischen Regierungen.
10. Wir brauchen IT-Systeme, die wirksamen Schutz gegen professionelle, staatlich unterstützte Industriespionage bieten.
11. Wir brauchen ein Internet, in dem Cyber-Kriminalität zurückverfolgt werden kann.

II Erreichen Digitaler Souveränität

Man erkennt an den obigen Aussagen, wie vielschichtig das Thema „Digitale Souveränität“ ist. Zum einen gibt es die verschiedenen Perspektiven von Bürgern, Unternehmen und Staaten. Zum anderen muss man den Begriff der Digitalen Souveränität genauer in verschiedene Aspekte unterteilen, um Lösungen aufzuzeigen.

A. *Infrastruktursouveränität* bezeichnet die Fähigkeit, technische Infrastrukturen vertrauenswürdig herzustellen, oder ihre Vertrauenswürdigkeit zu prüfen und sie so zu betreiben, dass darauf angebotene Dienste vertrauenswürdig sein können. Wir erreichen Infrastruktursouveränität durch:

- vertrauenswürdige Hardware. Dies umfasst Server, Telekommunikations-Hardware und Endgeräte.
- Verfahren zur Übertragung der Vertrauenswürdigkeit von Hardware-Vertrauensankern auf die Software.
- die Möglichkeit, ein abgesichertes Netz im Internet aufzubauen, in dem man garantiert anonym ist. Aber eine juristische Strafverfolgung darf und kann garantiert diese Anonymität aufdecken.
- ein reguliertes, verpflichtendes Zulassungsverfahren für vertrauenswürdige Hardware- und Internet-Dienste. Dazu gehört die Pflicht zur Offenlegung von Implementierungen gegenüber vertrauenswürdigen Prüfstellen, wissenschaftlich abgesicherte Prüfverfahren sowie Prüfsiegel mit für Endkunden nachvollziehbaren Bedeutungen.
- Rahmenbedingungen für Investitionen in Rechenzentren in Europa und deren wirtschaftlichen Betrieb.

B. *Datensouveränität* bezeichnet die Fähigkeit, informiert und selbstbestimmt zu entscheiden, wie und von wem Informationen über die eigene Person oder Institution, eigene Handlungen oder Produkte erhoben, verarbeitet und weitergegeben werden. Wir erreichen Datensouveränität durch:

- Dienste, die nachvollziehbar aufzeigen, wie sie mit Anwender-Daten umgehen und welche Absicherung der Daten sie bieten. Damit können Anwender entscheiden, welche Dienste sie nutzen. Dadurch werden neue Märkte für vertrauenswürdige Services ermöglicht.
- konfigurierbare Dienste, sodass Anwender selbst die Entscheidung treffen können, welcher Art der Datennutzung sie zustimmen und welcher nicht.
- öffentliche Sensibilisierung für Datenschutzfragen, spezifisch auch für die Nutzung moderner IT-Dienste.

C. *Entscheidungssouveränität* bezeichnet die Möglichkeit, Ursprünge und Begründungen für Entscheidungen und Handlungsempfehlungen autonomer Systeme und Assistenten nachzuvollziehen und diese gegebenenfalls durch menschliches Eingreifen zu beeinflussen. Wir erreichen Entscheidungssouveränität durch:

- die Offenlegung der Daten, ihrer Herkunft und Güte, die in Berechnungen eingehen, sowie die Offenlegung der Berechnungsvorschrift selbst gegenüber Anwendern oder vertrauenswürdigen Dritten. So können sie nachvollziehen, wie ein Ergebnis berechnet wurde.
- Gütesiegel, die Dienste auszeichnen, die Daten aus offenen, nachvollziehbaren Quellen in einer geprüften Art verarbeiten.
- öffentliche Einrichtungen als Vorreiter, Vorbilder und Beispiele für den Einsatz vertrauenswürdiger Dienste.

D. *Plattformsouveränität* entsteht dann, wenn auch die Marktmacht großer Akteure in einer Plattformökonomie durch Regulierung und bewusste Kundenentscheidungen auf ein Maß beschränkt wird, in dem ein fairer Wettbewerb möglich bleibt. Wir erreichen Plattformsouveränität durch:

- gesetzliche Rahmenbedingungen, die zu einem ausgewogenen Machtverhältnis führen zwischen staatlicher Einflussnahme – beispielsweise zum Schutz kritischer Infrastrukturen, sozialer und ökologischer Nachhaltigkeit sowie Verbraucherschutz –, den Interessen der Nutzer und wirtschaftlichen Interessen der Betreiber zu Investitionen und Innovationen, die den Grundwerten einer Gesellschaft dienen.
- eine nachhaltige Gründer-Unterstützung, die auch das langwierige Etablieren von Plattformen unterstützt.

III Forschen für Digitale Souveränität

Die Realisierung der oben genannten Thesen benötigt Forschung zur Digitalen Souveränität, um die Lücke zwischen dem heutigen methodischen Kenntnisstand und den Anforderungen zum Erreichen der Digitalen Souveränität zu schließen.

1. Wir müssen verstehen, wie man die Vertrauenswürdigkeit von Hardware effizient und verlässlich prüfen kann.
2. Wir müssen verstehen, wie man die Vertrauenswürdigkeit von Hardware bei der Entwicklung auf das ganze System übertragen oder nachträglich durch Analysen nachweisen kann.
3. Wir müssen verstehen, wie man die algorithmische Verarbeitung von Daten für Computer nachvollziehbar auch für Menschen beschreibt und wie man absichert, dass beide Beschreibungen einander entsprechen.
4. Wir müssen verstehen, wie Sicherheit bestimmt werden kann, sodass Anwender die Sicherheit von Diensten vergleichen und Unternehmen Sicherheit als Risikofaktor berücksichtigen können.
5. Wir müssen verstehen, wie wir Systeme analysieren und bewerten, deren Eigenschaften sich während des Betriebs durch Lernverfahren verändern.
6. Wir müssen verstehen, unter welchen Rahmenbedingungen Plattformen genossenschaftlich betrieben werden können.
7. Wir müssen verstehen, welche gesetzlichen Rahmenbedingungen bewirken, dass Plattformen sich öffnen und vernetzen, Monopole wirksam verhindert werden und Plattformen betrieben werden können, ohne Kunden unnötigerweise fest zu binden.

Digitale Souveränität und verlässliche Systeme für Informations- und Kommunikationssysteme sind eine Grundvoraussetzung für eine freiheitliche Gesellschaft, für eine funktionierende Wirtschaft und für einen unabhängigen Staat. Es bedarf jetzt einer großen Anstrengung, um Digitale Souveränität zu erreichen. Dazu ist eine große konzertierte Aktion von Forschung, Wirtschaft und Politik nötig. Die Handlungsfelder umfassen Hardware, Software, Prüf- und Zertifizierungsverfahren, aber auch staatliche Regulierung und neue Geschäftsmodelle für Internetdienste, sowie Aufklärung, Bildung und gesellschaftlichen Diskurs. Nur eine Bündelung der notwendigen Kompetenzen und ein enger Austausch in Form eines interdisziplinären Ansatzes mit Technik, Jura, Wirtschaftswissenschaften und Technikfolgenabschätzung kann diese umfassende Herausforderung angehen.