European Society for Digital Sovereignty e.V.

Digitale Souveränität in Deutschland

European Society for Digital Sovereignty e.V.
Email: info@esfds.org

Deutschland plant in den Koalitionsverhandlungen zur neuen Bundesregierung eine Digitalisierungsoffensive. Das ist sehr begrüßenswert. Jedoch darf eine solche Offensive nicht zu Einschränkungen des Bürgers und zu Datenpannen führen, sondern Datenschutz und digitale Selbstbestimmung müssen gleichzeitig gestärkt werden. Ein wesentlicher Faktor ist die Digitale Souveränität. Wir, die European Society for Digital Sovereignty, möchten den Koalitionsverhandlungen folgende Empfehlungen mitgeben:

I. Unabhängigkeit in der Öffentlichen Verwaltung

Die öffentliche Verwaltung soll digitaler und agiler werden. Sie darf sich dabei aber nicht von einem „Big Champion“ in eine Abhängigkeit begeben. Der Staat muss flexibel und handlungsfähig bleiben. Das bedeutet, dass Digitalisierung auf viele Schultern und viele Produkte gestützt werden muss. Es ist stets der Einsatz von Open Source Software zu prüfen und vorzuziehen, insbesondere in sicherheitsrelevanten Umgebungen. Verlässliche IT-Sicherheit ist in den allermeisten Fällen nur durch Open Source Produkte möglich. Insbesondere bei dem Aufbau einer Bundescloud ist darauf zu achten. Gaia-X und Phönix setzen hier schon auf die richtige Strategie, diese sollte weiter verfolgt werden und keine proprietären Anbieter zugelassen werden, wenn man Digitale Souveränität erhalten möchte. Allerdings ist Gaia-X seit langer Zeit ein Stillstandprojekt und droht in der Bedeutungslosigkeit zu verschwinden. Das kann die Bundesregierung mit den europäischen Partnern lösen. Die Förderung europäischer Produkte sollte grundsätzlich im Mittelpunkt stehen. Wir haben in der Vergangenheit gesehen, wie sich eine Abhängigkeit durch Software eines einzelnen Unternehmens aus den USA und der Abhängigkeit bei der Hardwareproduktion in China auswirkt. Unsere führenden deutschen Unternehmen haben existenzbedrohende Einbußen durch den Lieferengpass von Mikrochips, ein Softwarehersteller aus den USA diktiert der öffentlichen Verwaltung die Arbeitsweise und schreibt den Aufbau der Infrastruktur vor und verleitet auch Behörden zur Datenspeicherung auf amerikanischen Cloudservern. Laut einer Studie im Auftrag des BMI stellte PWC fest, dass Microsoft die digitale Souveränität des Staates gefährdet. Das bedeutet nicht, dass grundsätzlich keine proprietäre Software eingesetzt werden kann, sie darf aber nicht zur Abhängigkeit führen.

Die IT-Sicherheit des Bundes, Europa und der Nato muss verstärkt werden. Die Bundesregierung sollte die Digitale Souveränität stärken, um Integrität multilateraler Kommunikation sicherzustellen. Im Kontext der Europäischen Union und des NATO-Verbundes sollte die Entwicklung einer einheitlichen Kommunikations-Plattform vorangetrieben werden. In Deutschland gibt es bereits Produkte, die eine Grundlage dafür bieten (z.B. VS-K der Auslands IT).

II. Europäischer Kontext

Europa und die Bündnispartner handeln bisher häufig nicht mit einer Stimme im Umgang mit den Herausforderungen technischer Innovationen, wie der Zeitpunkt und Verlauf der KI-Verordnung zeigt. Digitale Diplomatie muss frühzeitig technische Entwicklungen aufgreifen und eine abgestimmte Regulierung auf Basis gemeinsamer Werte finden (z.B. Open Source first) - die Verzahnung der technologischen und der diplomatischen Expertise muss dazu gestärkt werden. Das erste Themenfeld muss die Regulierung von Robotic sein. Initiativen zur Regulierung digitaler Themenstellungen werden zukünftig immer auf europäische Auswirkungen und gegenwärtige Initiativen geprüft sowie die Einbindung von Praktikern in der operativen Umsetzung berücksichtigt. Hierfür sollte ein Beirat Digitale Exzellenz gegründet werden. Dieser muss Experten aus innovativen Themenfeldern und CIOs der Ressorts gleichermaßen einbinden, um die Machbarkeit von Normen und Vorgaben sicherstellen.

III. Big Data

Der Bürger muss über die Brisanz seiner Daten informiert sein. Awareness ist hier das Stichwort. Wir empfehlen eine groß angelegte Aufklärungskampagne zum Thema Umgang mit persönlichen Daten und der Möglichkeiten sowie Gefahren von Big Data. Der Satz „Ich hab ja nichts zu verbergen“ ist weit verbreitet und zeigt die Unwissenheit über die Gefahren von der Kombination gesammelter Daten. Wenn es eine Bundeszentrale für gesundheitliche Aufklärung gibt, ist eine Bundeszentrale für digitale Aufklärung von mindestens gleicher Wichtigkeit.

IV. IT-Sicherheitsgesetz 2.0

Das IT-Sicherheitsgesetz sollte von der neuen Bundesregierung ernsthaft und wissenschaftlich evaluiert werden, unter Einbeziehung der Wissenschaft und Forschung, als auch der Zivilgesellschaft. Hier gilt der Grundsatz: Was der Staat kann, können organisierte Kriminelle schon lange. Durch Hintertüren, Exploits und Staatstrojaner wird die Sicherheit für digitale und kritische Infrastrukturen nicht verbessert. Wo Sicherheitsbehörden und Nachrichtendienste Zugang zur Überwachung haben, können Angreifer diese offene Tür nutzen und werden dies auch vornehmen. Dabei muss davon ausgegangen werden, dass ein Angreifer größeres Wissen und Motivation mitbringt, als die Sicherheitsbehörden. Das hat auch eine Signalwirkung auf schützenswürdige Bevölkerungsgruppen, die eine Verfolgung damit auch in Deutschland befürchten müssen, da diese Schwächen auch von demokratiefeindlichen Autoritäten genutzt werden. Solche Praktiken dürfen nicht die Souveränität und die Sicherheit digitaler und kritischer Infrastrukturen schwächen. Stattdessen sollte die Bundesregierung eine strikt defensive Cybersicherheitsstrategie fahren, um die Resilienz dieser Infrastrukturen nachhaltig zu erhöhen. Das BSI sollte unabhängig nach wissenschaftlichem Stand der Technik agieren und Entscheidungen politisch nicht beeinflusst und weisungsungebunden kommunizieren.

V. Datenschutz

Datenschutz ist eine der größten Aufgaben im Zeitalter der Digitalisierung. Eine Speicherung von Daten ist für eine funktionierende digitale Welt unerlässlich, aber die informationelle Selbstbestimmung ebenso. Es ist stets eine Gradwanderung zwischen Datenschutz und Datenspeicherung. Daher sollte die Bundesregierung jedem Bürger ermöglichen, jederzeit, wo Daten der Person gespeichert sind, eine Kontrollmöglichkeit zu haben, ob und wie Daten abgefragt und verwendet worden sind. Ein Verstoß gegen den Datenschutz muss unkompliziert und digital angezeigt werden können und auch verfolgt werden. Eine Möglichkeit wäre, jegliche Verwendung von gespeicherten Daten über ein Logging dem Nutzer nach Authentifizierung, z.B. durch den digitalen Personalausweis, zur Verfügung zu stellen. Vorstellbar ist ein zentrales Register, dass jegliche Datenverwendung dem Bürger zugänglich macht.

VI. Schutzziele

Vertraulichkeit, Verfügbarkeit und Integrität sind nicht verhandelbar. Die Auswirkungen der rasanten Weiterentwicklung der Quanten-Computer bringen Veränderungen und können die Vertraulichkeit durch gebrochene Chiffren gefährden. Die Bundesregierung sollte daher einen Schwerpunkt auf die Ausstattung der Forschung legen. Internet muss in ganz Deutschland in jedem Wald, in jedem Keller und an jedem Ort verfügbar sein. Daher ist der im Sondierungspapier angestrebte Gigabitausbau unerlässlich und muss umgehend umgesetzt werden. Fehl- und Desinformation ist ein weltweites High-Level Risiko für die Sicherheit und muss bekämpft werden.

VII. Umsetzung Digitaler Souveränität

Um die digitale Souveränität zu erreichen, gibt es erfolgversprechende Schlüsselstrategien wie zum Beispiel Open Source, Open Standards und Public Money - Public Code. Bei der Beschaffung von Softwaredienstleistungen muss der Staat prüfen, ob die Dienstleistung unter Einhaltung voller staatlicher Souveränität möglich ist. Wenn digitale Souveränität eines Produktes nicht gewährleistet werden kann, ist es Aufgabe des Staates eine quelloffene Alternative in eigenem Auftrag zu entwickeln. Aufgabe des Staates ist es Vergabeprozesse zielführend anzupassen und parallele Vergaben an mehrere Anbieter zu ermöglichen, um im praxisnahen mehrjährigen Probebetrieb die geeignetste Lösung zu identifizieren und gleichzeitig durch Entwicklung offener Interoperabilitätsstandards den freien Datenverkehr zu ermöglichen.