Antwort von Die Linke auf die Nachfrage der DISQU GmbH zur Landtagswahl Sachsen 2024

---

1. Sehen Sie eine mangelnde Digitale Souveränität in a) sächsischen Unternehmen und b) der öffentlichen Verwaltung Sachsens als Herausforderung? Wie hoch schätzen Sie das Risikobewusstsein ein?

Antwort:
a) Die Abhängigkeit von Produkten der großen IT-Monopolisten ist mutmaßlich in den sächsischen Unternehmen sehr hoch, denn die meisten sind kleine und Kleinstunternehmen, die oft das nutzen, was sie gewohnt sind. Deshalb ist es wichtig, bereits in Schulen und Ausbildungszentren keine Monopollösungen zu nutzen, sondern die Menschen in den notwendigen Bereichen der IT zu bilden. Kurz: Hin zu IT-Wissen, weg von Marken-Wissen.
Außerdem müssen Förderangebote für kleine Unternehmen und Solo-Selbstständige ausgebaut werden. Auch nach der Schul- und Berufsbildung müssen alle Menschen weiterhin Zugang zu kostenfreien und niedrigschwelligen Weiterbildungsangeboten, sowie kostenfreien Digitalisierungsberatungen haben.

b) Dass es überhaupt eine Open Source Strategie für den Freistaat Sachsen gebraucht hat, zeigt: Die Verwendung von Open Source Software und das Bewusstsein für Digitale Souveränität in der sächsischen Verwaltung ist ausbaufähig. Wie aus der Antwort auf die Frage unseres digitalpolitischen Sprechers Nico Brünler nach den Erfolgen der Open Source Strategie hervorgeht, ist dort noch Luft nach oben: Zwar steigt die Anzahl der Open Source Projekte, allerdings bleibt im Unklaren, ob damit kleine Werkzeuge oder komplexe IT-Lösungen gemeint sind. Außerdem sind die Ausgaben für proprietäre Lösungen immer noch immens, was gegen eine großflächige Nutzung von Open Source Produkten spricht.
Das immer noch zu geringe Risikobewusstsein zeigt sich zudem bei einem ähnlichen Thema in der Antwort zur Kleinen Anfrage zur Pseudonymisierung von Datensätzen die in der DSGVO vorgegeben ist. Hier erklärt die Staatsregierung im Wesentlichen, dass sie Datensätze nicht pseudonymisiert und dies auch nicht geplant ist. Leider werden auch in einer dritten Antwort auf eine Kleine Anfrage vollkommen an der Realität vorbei Überwachungs- und Leak-Gefahren seitens der Staatsregierung klein geredet.

2. Welche politischen Maßnahmen zur Steigerung der digitalen Souveränität wurden bereits durchgeführt und welche sind in der Planung? (Nennen Sie gerne auch Beispiele)

Antwort:
Die Verabschiedung der Open Source Strategie war ein wichtiger Schritt. Sie muss jetzt mit Leben gefüllt werden. Wichtige Grundvoraussetzung für die Erlangung von Digitaler Souveränität ist das Vorhandensein von IT-Fachpersonal in den öffentlichen

Beschaffungsstellen. Hierzu braucht es bessere Arbeitsbedingungen: Dazu zählen zuvorderst schlankere und agilere Strukturen; ein höheres Gehalt kann eine Rolle spielen. Notwendig sind zudem in allen Staatsministerien und Fachbehörden einheitliche Hard- und Software sowie IT-Sicherheitsstandards. Bereits vorhandene behördenspezifische Insellösungen müssen nach Möglichkeit wieder abgeschafft werden. Dabei setzen wir vorrangig auf Open-Source-Lösungen. Open Source muss daher unserer Meinung nach eine Bedingung in Ausschreibungen der öffentlichen Verwaltung sein. Wir setzen darauf, dass aus diesen Maßnahmen auch Impulse für die hiesige IT-Unternehmenslandschaft ausgehen.

3. Wie unterstützen Sie die Verwendung standardisierter/offener Datenformate?

Antwort:
Als Die Linke fordern wir, dass bestehende Richtlinien, die Anforderungen an die Veröffentlichung von Daten stellen, umgesetzt werden. Insbesondere sollen statistischen Daten zugänglich gemacht werden. Zudem müssen diese offenen Daten unserer Ansicht nach maschinenlesbar, so vollständig wie möglich und aktuell sein. Außerdem sollen sie unter einer offenen Lizenz stehen. Wir sprechen uns gegen die Kommerzialisierung von öffentlichen Daten aus. Die Benutzerfreundlichkeit von Informationssystemen und Portalen hat dabei für uns eine hohe Priorität. Ebenso sollen die Prinzipen von Open Data und Open Source ein Kriterium in den Ausschreibungen von Aufträgen an externe Dienstleister sein. Denn offene Schnittstellen ermöglichen die Weiterverwendung der Informationen und die Entwicklung von angepassten Systemen. Gleichzeitig wird die Bindung an einzelne Firmen verhindert. Grundlegend ist für uns auch, dass Systeme in der öffentlichen Verwaltung so gebaut werden, dass offene Schnittstellenspezifikationen implementiert werden und somit die Daten unterschiedlicher Ressorts ohne Einschränkungen untereinander genutzt werden können.

4. Wie schätzen Sie die Rolle von Open Source Software zur Erlangung Digitaler Souveränität ein? Möchten Sie die Verwendung und/oder Entwicklung von Open Source Software fördern?

Antwort:
Der Einsatz von Open-Source-Software ist entscheidend für die Stärkung digitaler Souveränität. Wie bereits erwähnt, möchten wir die Entwicklung von Open-Source-Software aktiv fördern. Darüber hinaus unterstützen wir die Initiative „Public Money Public Code“ der Free Software Foundation Europe. Diese Initiative setzt sich dafür ein, dass Software, die mit öffentlichen Geldern finanziert wird, nicht durch Kommerzialisierung der Öffentlichkeit vorenthalten wird. Wir sind der Meinung, dass alle Software, die in Behörden und staatlichen Betrieben genutzt wird, freie Software sein sollte, nicht nur Open Source. Die Praxis zeigt den potenziellen Nutzen solcher Ansätze. Ein positives Beispiel ist die Weiterentwicklung der Corona-Warn-App, bei der Bürger:innen neben der staatlich finanzierten Entwicklung auch zur Lösung von Problemen beigetragen haben.

5. Sollte bei Ausschreibungen der öffentlichen Hand bevorzugt auf Open Source Software gesetzt werden?

Antwort:
Ja, wir unterstützen dieses Anliegen.

6. Sollte bei Ausschreibungen der öffentlichen Hand das Vorhandensein kompatibler Alternativprodukte (sowohl Soft- als auch Hardware) als verpflichtendes Wertungskriterium eingeführt werden?

Antwort:
Quelloffene Hard- und Software-Lösungen sollten aus unserer Sicht immer bevorzugt behandelt werden. Falls es keine vollständig passende offene Lösung gibt, muss geprüft werden, ob eine Bestehende angepasst werden kann. Auch das sollte Bestandteil des Ausschreibungsprozesses sein.

7. Sehen Sie Risiken bei der Verwendung (insbesondere von nicht-europäischen Anbietern) von Cloudservices hinsichtlich der Datensouveränität?

Antwort:
Im Rahmen des Datenflusses zu nicht-europäischen Anbietern gibt es Gefahren hinsichtlich des Datenschutzes: Es ist nicht immer gewährleistet, dass Daten die auf nicht-europäischen Servern liegen, auch vertraulich bleiben. Verschiedene Länder erlauben auch Praktiken, wie die Zusammenführung unterschiedlich erhobener Daten über Personen, wie sie nicht mit der DSGVO bzw. dem BDSG vereinbar sind.
Vorzugsweise sollten Lösungen zum Einsatz kommen, die innerhalb der öffentlichen Infrastruktur durch die Behörden selbst betrieben werden. Ist dieser Aufwand nicht zu rechtfertigen, sollten nur Datenschutz-konforme Dienstleistungen in Anspruch genommen werden.
Technisch lässt sich dies durch eine Verschlüsselung der Daten in einer Art, in der der Anbieter es nicht entschlüsseln kann, abbilden und ist bei vielen Anbietern auch schon gängige Praxis.