**Antwort der CDU auf die Nachfrage der DISQU GmbH zur Landtagswahl Sachsen 2024**

---

vielen Dank für Ihre Anfrage. Gerne beantworten wir Ihnen die Fragen wie folgt:

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:
*Digitale Souveränität ist eine wesentliche Bedingung für Cyber-Resilienz. Derzeit besteht sicherlich sowohl in sächsischen Unternehmen, aber auch in der öffentlichen Verwaltung eine Abhängigkeit zu Technologieanbietern. Insbesondere die Verwaltung, der Bürgerinnen und Bürger regelmäßig sensible Daten zur Verfügung stellen, hat hier eine besondere Verantwortung. Die Schaffung und Stärkung widerstandsfähiger und souveräner Strukturen ist daher eine längst grundlegende und in ihrer Bedeutung wachsende Aufgabe, der sich sowohl die Wirtschaft als auch die öffentliche Verwaltung stellen muss. Aus unserer Sicht braucht es dafür zuvorderst einen kulturellen-strategischen Wandel weg von konventionellen Ansätzen hin zu einem ganzheitlichen Zero-Trust-Ansatz. Dieser „Kulturwandel" kann aber nicht staatlich oder politisch „von oben" verordnet werden, sondern muss durch die Unternehmen selbst erfolgen.*

*Das Thema digitaler Souveränität scheint uns allerdings grundsätzlich in den Behörden und sächsischen Unternehmen durchaus angekommen zu sein, auch ein Problembewusstsein für Abhängigkeiten ist vorhanden. Nun braucht es noch eine flächendeckende und tiefgreifende Verankerung dieses Themenfelds im Denken und Handeln der jeweiligen Akteure.*

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

Antwort:
*Wie bereits dargelegt, ist ein grundlegender strategischer Wandel die Grundbedingung, um tatsächliche digitale Souveränität zu erreichen. Davon unabhängig wollen wir als CDU mit dem Aufbau eines sächsischen Cyber-Resilienz-Zentrums ein Koordinierungszentrum schaffen, das nicht nur die wesentlichen Akteure miteinander vernetzt, sondern auch als Ansprechpartner fungiert.*

*Zudem haben wir mit dem 2019 von der Koalition verabschiedeten Sächsischen Informationssicherheitsgesetz (SächsISichG) erweiterte Maßnahmen zur Gefahrenabwehr implementiert, um das gesamte Verwaltungsnetz – das im Falle eines Angriffes auf ein Verwaltungssystem in seiner Gesamtheit betroffen ist – krisenfester zu machen. In den*

*Verbund aus Sächsischem Verwaltungsnetz (SVN) und Kommunalem Datennetz (KDN) werden beständig erhebliche finanzielle Mittel investiert, um eine leistungsfähige und sichere Kommunikationsinfrastruktur und wichtige zentrale Dienste für die sächsischen Verwaltungen zur Verfügung zu stellen. Mit dem Sicherheitsnotfallteam von SAX.CERT steht den Behörden der sächsischen Landesverwaltung außerdem ein fachkundiger Ansprechpartner zur Seite. Durch einen Ausbau der Zusammenarbeit mit dem Bund, anderen Bundesländern und weiteren Akteuren insbesondere aus Wirtschaft und Wissenschaft wollen wir nicht nur die Sicherheitsarchitektur vor Ort verbessern, sondern auch Schulungsangebote auf Basis von Know-How und Best Practices schaffen, die wiederum einen Grundstein für den erwähnten Kulturwandel bilden können.*

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

Antwort:
*Wir haben die Sächsische Staatsverwaltung in ihrer Open-Source-Strategie unterstützt. Diese wurde am 30.06.2023 herausgegeben.*

*Sächsischen Unternehmen muss es selbst obliegen können, inwiefern sie standardisierte bzw. offene Datenformate unterstützen und nutzen.*

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:
*Mit der zunehmenden Digitalisierung aller Lebensbereiche steigt auch die Bedeutung von Informations- und Kommunikationstechnologie (IKT). Die Bereitstellung von Open-Source-Ansätzen kann ein wichtiger Schritt sein, um digitale Souveränität herzustellen und zu erhalten. Weitere Bausteine digitaler Souveränität (Hard-Ware, Kompetenzen) gründen dann auf diesen Open-Source-Ansätzen. Aus diesem Grund hat der Freistaat seine Open-Source-Strategie erarbeitet und arbeitet an deren Umsetzung.*

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

Antwort:
*Als CDU stehen wir für möglichst unbürokratische Verfahren und achten die Prinzipien der kommunalen Selbstverwaltung.Zudem ist festzuhalten, dass sich bereits seit den Anfängen einer Entwicklung von „E-Government“ im Freistaat Sachsen der Freistaat und die Kommunen darauf verständigt haben, bestimmte, häufig verwendete IKT-Funktionen, -Dienste und -systeme zentral zu entwickeln, gemeinsam zu finanzieren und allen Bedarfsträgern zur Verfügung zu stellen.*

*Die Aufnahme zusätzlicher gesetzlich vorgeschriebener Auswahlkriterien ist aus unserer Sicht möglichst zu vermeiden. Open Source Software kann bereits heute jederzeit in Ausschreibungen aufgenommen werden, sofern der Ausschreibende das wünscht. Als CDU setzen wir hier auf Freiwilligkeit. Hohe Priorität haben für uns dabei die Kriterien der Zuverlässigkeit, Stabilität und Nutzerfreundlichkeit.*

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

Antwort:
*Als CDU setzen wir hier auf Freiwilligkeit und lehnen die Aufnahme weiterer verpflichtender Aufnahmekriterien für Vergaben der öffentlichen Hand ab.*

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

Antwort:
*Ja, diese Risiken sehen wir durchaus. Insbesondere Russland und China versuchen, durch gezielte Cyberkampagnen unsere digitale Infrastruktur anzugreifen. Gesteuerte Desinformationskampagnen tun ihr Übriges. Für die Herstellung und Umsetzung einer für die gesamte Sicherheitsarchitektur geltenden Cyber-Resilienz ist es daher aus unserer Sicht unabdingbar, auf europäische Anbieter zu setzen.*