Deutscher Bundestag

Ausschuss Digitale Agenda

Ausschussdrucksache
SB19(23)11

Fragenkatalog für die Anhörung des Ausschusses Digitale Agenda zum Thema „IT-Sicherheit von Hard und Software als Voraussetzung für Digitale Souveränität“ am 11. Dezember 2019

1. Digitale Souveränität ist eine Grundvoraussetzung für die staatliche Souveränität Deutschlands. Wie sehen Sie Deutschland und Europa - hinsichtlich der Bürger, der Unternehmen, der Verwaltung -diesbezüglich aufgestellt und wo sehen Sie welchen regulativen Handlungsbedarf mit Blick auf die verschiedenen Akteure?

2. Wo besteht gesetzgeberischer Handlungsbedarf, um die digitale Souveränität auf nationaler und auf EU-Ebene langfristig zu sichern? Welche Spielräume hat der nationale Gesetzgeber und welche Vorgaben sollten zwingend auf EU-Ebene getroffen werden? Welche Aspekte, Technologien und Standards unterstützen am meisten die digitale Souveränität der Bürgerinnen und Bürger – und wie kann der Staat diese am besten fördern?

3. IT-Angriffe und -kriminalität, auch Tätigkeiten ausländischer Nachrichtendienste, sind eine große Herausforderung mit Blick auf IT-Sicherheit und Souveränität. Wo sehen Sie hier den dringendsten Handlungsbedarf? Wie kann eine digitale Souveränität erreicht werden, die nicht allein auf Abschottung setzt und sich sinnvoll mit einer offenen und freien Netzarchitektur verbindet?

4. Wie stufen sie die Vulnerabilität der unterschiedlichen Komponenten der IT-Architektur sowie der digitalen Infrastrukturen ein und wo sehen Sie welchen konkreten Handlungsbedarf?

5. Vor wenigen Wochen hat eine im Auftrag des BMI vorgelegte Studie bestätigt, dass der Bund „in hohem Maße“ abhängig von Microsoft sei. Diese Abhängigkeit könne „kritische Folgen“ haben, die „noch weiter zunehmen dürften“. Die Studie sieht dringenden Handlungsbedarf, um die „digitale Souveränität der Bundesverwaltung langfristig zu sichern“. Hinsichtlich welcher Elemente (Betriebssysteme / Office-Anwendungen / Cloud-Systeme / Hyperscaler / Hardwareverfügbarkeit etc.) bestehen welche Abhängigkeiten, durch ggf. die digitale Souveränität gefährdet wird? Wie kann es gelingen, bestehende Abhängigkeiten abzubauen?

6. Warum hat sich Open Source in der öffentlichen Verwaltung bislang noch nicht durchgesetzt und warum sind bisherige Projekte der Einführung von Open Source in der öffentlichen Verwaltung gescheitert? Welche Rolle spielen hierbei freie und offene Software sowie freie und offene Standards? Inwiefern kann spezifischen Sicherheitsrisiken für von Bundeswehr/ BMVg genutzten Systemen Geltung getragen werden?

7. Welche Bedeutung kommt - Stichwort IT-Konsolidierung des Bundes - der Vereinheitlichung und Bündelung von Diensten, Rechenzentren, Beschaffung und weiteren Dienstleistungen zu und welche Schwierigkeiten stehen solchen Prozessen entgegen? Wie wettbewerbsfähig sind dabei europäische und nationale Eigenlösungen gegenüber den Fertiglösungen der weltweit agierenden IT-Konzerne?

8. Trotz aller Sicherheitsvorkehrungen kann es eine absolute Sicherheit bezüglich eingesetzter Hard- und Software nicht geben. Daher stellt sich, unabhängig von einzelnen Unternehmen, die grundsätzliche Frage des Vertrauens in die Integrität der Hersteller und dem Rechtssystem im Herstellerland. Welche Möglichkeiten sehen Sie, um Risiken bestmöglich zu streuen, einseitige Abhängigkeiten zu vermeiden und die Frage der Vertrauenswürdigkeit – nicht im Sinne von Abschottung – als formalisiertes Merkmal von IT-Sicherheitskonzepten zu etablieren? Welche Bedeutung kommt Haftungsregimen zu? Wie wichtig sind verpflichtende Mindeststandards und Zertifizierungsverfahren? Welche Rolle sollten (unabhängige) Aufsichtsstrukturen spielen? Sind Vereinbarungen hierzu auch auf internationaler Ebene notwendig und realistisch – und wenn ja welche?

9. Wie bewerten Sie die Wirksamkeit vertraglicher Vereinbarungen, wie z.B. NoSpy-Abkommen, sei es auf zwischenstaatlicher Ebene oder im Rahmen privatrechtlicher Verträge? Halten Sie Konformitätsprüfungen in Bezug auf Vertrauenswürdigkeit und Hardware/Software Integrität für wirksam durchführbar oder wäre eine „Abschottung“ und Ausschluss von Komponenten-Anbietern wirksamer?

10. Um die digitale Souveränität zu erhöhen, werden derzeit u.a. vertrauenswürdige Speicherinfrastrukturen auf deutscher und europäischer Ebene diskutiert, insbesondere die sog. „Bundes-Cloud“ und „GAIA-X“. Wie bewerten Sie die derzeitigen Bemühungen? Welche Rolle spielt Regulierung in anderen Ländern, wie z.B. der US-Cloud-Act? Was ist ferner erforderlich, damit Daten dann auch in den Kommunikationsnetzen sicher vor dem Zugriff Dritter geschützt sind und für kooperative Datennutzungsmodelle vertrauenswürdige Intermediäre entstehen?

11. Welchen Beitrag können dynamisch angepasste Minimalstandards und Zertifizierungen, offene Standards, Interoperabilität, Open Source, Open Hardware usw. zu mehr IT-Sicherheit leisten?

12. Welche Voraussetzungen wären erforderlich, um eine (hoheitliche) Zertifizierung von IT-Produkten zur Gewährleistung und Stärkung des Nutzervertrauens und der IT-Sicherheit (Schutz vor Datenabflüssen, Datensammlungen, Überwachung) zu errichten? Auch auf der Ebene der Hardware sind mögliche Hintertüren auch nur noch begrenzt erkennbar. Wer sollte/könnte die Überprüfung leisten? Wo liegen die Grenzen der Überprüfbarkeit?

13. Welche Rolle spielen Sicherheitslücken und der Handel mit ihnen für die IT-Sicherheit? Halten Sie eine Meldepflicht staatlicher Stellen für Sicherheitslücken für ratsam?

14. Das Bundesverfassungsgericht hat bereits 2008 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) festgeschrieben. Sollte der Gesetzgeber aus Ihrer Sicht konkrete Schritte unternehmen, um diesem nicht mehr ganz „neuen IT-Recht“ zum politischen Durchbruch zu verhelfen? Was bedeutet das Grundrecht für den Schutz der persönlichen IT-Systeme, den Schutz der Vertraulichkeit der Kommunikation und den Schutz digitaler Infrastrukturen?

15. Kann der rechtskonforme Zugriff des Staates auf individuelle Daten und Kommunikation technisch in Einklang gebracht werden mit der digitalen Souveränität des einzelnen Bürgers oder schließt sich dies grundsätzlich aus?

16. Was muss aus Ihrer Sicht zwingend Eingang in die Reform des IT-Sicherheitsgesetzes finden?

17. Sind aus Ihrer Sicht die Herstellung der Unabhängigkeit des BSI und ein Herauslösen aus der Fach- und Rechtsaufsicht des Bundesministeriums des Inneren, für Bauen und Heimat, notwendig und geboten? Welche Vor-, welche Nachteile sehen Sie hier?

18. Das Gefüge der europäischen, nationalen und länderbezogenen IT-Sicherheitsarchitektur ist mit dutzenden Behörden mit unterschiedlichen Rechtsgrundlagen und Befugnissen sehr komplex. Wie sollte dieses Gefüge in Zukunft aufgestellt werden? Welche Verbesserung auf Bundesebene bei Strukturen und Prozessen für Programm-, Projekt- und Architekturmanagement schlagen sie vor?

19. Wie bewerten Sie im Kontext IT-Sicherheit Forderungen nach einem „Hackback“ oder einer „proaktiven Cyberabwehr“? Wie beurteilen Sie Deutschlands Fähigkeit und den weiteren Forschungsbedarf bei der Attribution von Cyberangriffen im internationalen Vergleich? Wie bewerten Sie im Kontext der IT-Sicherheit Forderungen nach generellen Hintertüren in Messengerdiensten (Stichwort „cryptowars“) und in allen Geräten des „Internet der Dinge“? Wie bewerten Sie den Vorschlag von u.a. BKA-Präsident Münch, statt einer „Backdoor“- eine „Frontdoor-Debatte“ zu führen?

20. Welche Vor- und Nachteile sehen Sie in der Forderung nach Interoperabilität von verschlüsselten Messengern?

21. Investieren Deutschland und Europa genug in Forschung und Entwicklung für IT-Sicherheit? Wo sehen Sie Defizite und wo dringenden Handlungsbedarf?
Welche Forschungsaktivitäten im IT-Sicherheitsbereich in Deutschland werden sowohl durch EU-Mitgliedsstaaten als auch durch Nicht-EU-Staaten finanziell gefördert?

22. Welche Rolle spielen IT-Qualifikationsmöglichkeiten, z.B. an Schulen und Hochschulen, um das Ziel der digitalen Souveränität zu erreichen? Wie kann dem akuten und sich verstärkenden Mangel an geeignetem IT- Sicherheits- und IT-Fachpersonal begegnet werden? Welche Herausforderungen und konkreten Anforderungen sehen Sie für die Bereiche der Bildung und Ausbildung von IT-(Sicherheits)-Fachkräften, sowie für die Verankerung von IT-(Sicherheits-)Kenntnissen und Grundlagen, in Schule, Ausbildung und Hochschule?

23. Welche Potenziale sehen Sie in Technologien wie der Blockchain-Technologie, insbesondere mit Blick auf IT-Sicherheit und Datenschutz, auch als europäischer Standortvorteil? Wie bewerten Sie die Auswirkungen der Thematik des Quantencomputing für die IT-Sicherheit, beispielsweise im Hinblick auf Verschlüsselungstechnologien? Wie bewerten Sie den derzeitigen Entwicklungsstand der post-quanten-Kryptographie? Welche Sicherheitsrisiken drohen hier? Ist Deutschland wettbewerbsfähig aufgestellt?

24. Ist eine gesetzliche Verpflichtung zur Offenlegung des Quellcodes von Programmen und Algorithmen zur Stärkung des Nutzer*innen-Vertrauens und der Sicherheit sinnvoll/notwendig?

25. Inwieweit können Haftungsregelungen für Anbieter von Dual-Use-Gütern im IT-Bereich (NSO, Fin Fisher etc.) so gestaltet werden, dass diese im Falle des Einsatzes zum einen von öffentlicher Auftragsvergabe ausgeschlossen und zum anderen für die Verwendung ihrer Produkte bspw. gegen Dissident*innen, Journalist*innen etc. zur Verantwortung gezogen werden können?