Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)077

Fragenkatalog, hier: Antwort des BSI

Öffentliche 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?**

Es kann insgesamt festgestellt werden, dass große Abhängigkeiten von den USA (besonders im Softwarebereich) und von China (besonders im Hardwarebereich) in Deutschland und Europa bestehen. Betroffen sind alle Bereiche der Gesellschaft, auch z.B. kritische Infrastrukturen. Einige Schlüsselindustrien für IT-Produkte sind in Europa nur noch in äußerst eingeschränktem Maße vorhanden. Bezüglich fast aller strategisch wichtigen IT-Komponenten, wie z.B. Prozessortechnologien, leistungsfähigen IT-Netzkomponenten, Mobilfunkgeräten/Smartphones ist Europa von Zulieferern außerhalb der EU abhängig.

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?**

Ziel auf nationaler und EU-Ebene aus Sicht des BSI sollte sein, durch hersteller-unabhängige technische Analyse, den Stand der Technik kontinuierlich nach hohen qualitativ-technischen Vorgaben zu analysieren und bei Bedarf anzuheben. Dafür sind entsprechende regulative Vorgaben oder Empfehlungen zu schaffen, die die digitale Sicherheit von öffentlichen Einrichtungen, kritischen Infrastrukturen, Unternehmen und Verbrauchern in einem schnelllebigen Markt gewährleisten. Das BSI ermittelt kontinuierlich den aktuellen „Stand der Technik“ und kann über verschiedene Maßnahmen, insbesondere unabhängige technische Analyse, Zertifizierung und Technische Richtlinien den Stand der Technik mitprägen.

Bezüglich Zertifizierung erfolgte ein wichtiger Schritt auf EU-Ebene durch das Inkrafttreten des Rechtsakts zur Cybersicherheit [Verordnung (EU) 2019/881), engl. Cybersecurity Act (CSA)] am 27. Juni 2019. Das BSI ist in den hierdurch neu geschaffenen Gremien vertreten (European Cybersecurity Certification Group, ECCG) und bringt dort in Zusammenarbeit mit den europäischen Partnern die hohen Standards und Vorgaben, die bereits auf nationaler Ebene geschaffen wurden, bei der Erstellung von neuen Schemata leitend ein.

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?**

Prävention, Detektion und Reaktion sind die wesentlichen Eckpfeiler einer Sicherheitsstrategie zum Schutz vor IT-Angriffen. Das BSI steht in der Bundesrepublik prominent für diese drei Eckpfeiler.

IT-Sicherheit erfordert Produkte und Dienstleistungen, die sowohl die notwendigen Sicherheitsfunktionen aufweisen als auch von den Anwendern so betrieben werden können, dass ein angemessener Schutz vor IT-gestützten Angriffen gewährleistet wird. Vor allem die Bereitstellung sicherer Soft- und Hardware, eine sichere Datenhaltung sowie die Dokumentation und Transparenz bei der Darstellung von Funktionen und Eigenschaften von Hard- und Software sollten dabei im Vordergrund stehen.

Aus Sicht des BSI sind deshalb auf europäischer Ebene geeignete Mindeststandards erforderlich, damit im Zuge der Digitalisierung keine inakzeptablen Risiken entstehen (Security by Design). Europäische Mindeststandards müssen dabei die durch die oftmals weltweiten Lieferketten erzeugten Risiken berücksichtigen und auf ein noch akzeptables Maß bringen (Supply Chain Security).

Sicherheitslücken können auch durch fehlerhaften Einsatz beim Anwender entstehen. Wichtig ist deshalb, dass bereits die herstellerseitige Auslieferung eines Produktes in einem sicheren Zustand („Security by Default“) erfolgt.

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

Handlungsbedarf wird grundsätzlich bei der vertrauenswürdigen Herstellung sowie beim Betrieb aller IT-Komponenten gesehen. Im Allgemeinen ist die Vulnerabilität dort besonders groß,

- wo einzelne Anbieter eine Monopolstellung innehaben (Bedrohung der Verfügbarkeit durch Vendor lock-in) oder
- wo Nutzdaten unverschlüsselt vorliegen (Bedrohung von Vertraulichkeit und Integrität durch Datenabfluss/-manipulation) sowie
- wo das Entdeckungsrisiko am geringsten ist und
- wo Analysen schwierig sind.

Aber auch verschlüsselte Daten sind auf lange Sicht durch den zuletzt beachtlichen Fortschritt bei der Entwicklung von Quantencomputern bedroht, weswegen das BSI dem Einsatz und der Entwicklung von quantencomputerresistenten krytografischen Lösungen eine hohe Priorität einräumt und in diesem Bereich sehr aktiv ist.

Verbraucherinnen und Verbrauchern kann nur ein Minimum an Verantwortung für die Sicherheit von IT-Komponenten zugemutet werden. Der größte Teil der Verantwortung muss den Herstellern und Anbietern zugewiesen werden.

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?

Neben dem bereits genannten Einsatz von Produkten der Microsoft-Windows- und Microsoft-Office-Familien gibt es weitere Produktbereiche, die ein hohes Maß an Vendor-Lock-In aufweisen. Beispielsweise können auch Datenbankprodukte in der Praxis oft nur durch groß angelegte und