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

aufwändige Migrationsprojekte durch Produkte anderer Hersteller ersetzt werden. Bestimmte Programmiersprachen können ebenfalls eine Festlegung auf einen bestimmten Anbieter begünstigen. Ein weiteres Risiko in diesem Bereich stellt die Nutzung von Cloud-Services ohne geeignete Exit-Strategie dar.

Gefahren durch Abhängigkeiten von IT-Produkten bestehen aus Sicht des BSI grundsätzlich produktkategorie-übergreifend. Beispielsweise bestehen Abhängigkeiten bezüglich Office, Datenbanken, Hypervisoren / Virtualisierungslösungen / Prozessorttechnologien und weiteren Halbleiterkomponenten. Die Entwicklung, Pflege und Weiterentwicklung von Funktionalitäten, Formaten und Schnittstellen erfolgt hier nicht selbst-bestimmt (durch die Nutzer), sondern fremd-bestimmt (durch die Hersteller).

Grundsätzlich kann Abhängigkeiten langfristig nur mit der Möglichkeit von eigener Einflussnahme (oder der Schaffung, Pflege und Balance wechselseitiger Abhängigkeiten) entgegengewirkt werden.

Konkret gibt es aktuell verschiedene Möglichkeiten, bestehende die Auswirkung von bestehenden Abhängigkeiten zu reduzieren:

- durch vertragliche Vereinbarungen mit den Herstellern zu langfristiger Format- und Schnittstellenkompatibilität sowie Möglichkeiten langfristiger kundenseitiger Einflussnahme auf die Pflege und Weiterentwicklung von IT-Produkten ergeben.
- dem Prinzip der Risikostreuung folgend, durch Diversifikation hinsichtlich IT-Produkt-Herstellern
- durch die Schaffung/Vereinbarung von Nutzungsmöglichkeit des Quelltextes von Software-Produkten, die eine nutzer-koordinierte/-kontrollierte Weiterentwicklung und -pflege von Software-Produkten ermöglicht
- durch eine möglichst durchgängige Nutzung offener und international anerkannter Standards, Schnittstellen und Protokolle.

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?

Open Source ist heute aus der weltweiten IT-Landschaft nicht mehr wegzudenken.

Herkömmliche Arbeitsplatz-PC und Laptops sind eine der wenigen Domänen, in denen sich quelloffene Software bislang nicht durchsetzen konnte. Ein wesentlicher Grund hierfür ist das bekannte "Henne-Ei-Problem": Einerseits wird typische Software für Arbeitsplätze oft nur für Windows (und manchmal auch für MacOS) programmiert, weil dies die vorherrschenden Desktop-Betriebssysteme sind. Andererseits setzen Anwender auf Arbeitsplätzen meist auf Windows bzw. MacOS, eben weil typische Software für diese Betriebssysteme geschrieben wird. Bei den genutzten Office-Programmpaketen ist es ähnlich: Microsoft Office hat sich in der Industrie und in der Verwaltung als De-Facto-Standard etabliert.

Bisher handelte es sich bei Open-Source-Projekten zudem um Einzelprojekte. Diese haben im Verbund mit den marktgängigen Hardware- und Software-Projekten immer einen hohen Anpassungsbedarf. Daher sind für die Entwicklung der Basissoftware und der individuellen Lösungen sowie für die Entwicklung und Einhaltung der schutzbedarfsorientierten

Sicherheitsstandards sehr gut ausgebildete Mitarbeiter notwendig. Dies stellt für Open-Source-Projekte eine schwer erfüllbare Voraussetzung dar.

Besonderen Risiken muss aus Sicht des BSI dadurch begegnet werden, dass an den entscheidenden, sicherheitsrelevanten Punkten besonders gehärtete Spezialprodukte mit den notwendigen Sicherheitsfunktionen eingesetzt werden. Dies betrifft beispielsweise Produkte zur Verschlüsselung bei der Übertragung staatlicher Verschlusssachen. Die Instrumente der Zulassung von Produkten und der Freigabe von Systemen, wie sie durch das BSI eingesetzt werden, haben sich hierzu bewährt.

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?**

Die IT-Konsolidierung Bund führt zu einer gewollten Vereinheitlichung der IT-Infrastruktur und der eingesetzten Softwareprodukte. Damit bieten sich Chancen zur Professionalisierung der IT, entstehen aber auch erhöhte Risiken durch die Abhängigkeit von einzelnen IT-Produkten bzw. IT-Herstellern.
Die IT-Konsolidierung Bund hat die Gewährung der Informationssicherheit und die Sicherstellung der Handlungsfähigkeit der Bundesverwaltung als Ziel. Der Erfolg der IT-Konsolidierung ist hinsichtlich dieses Ziels derzeit aus den folgenden Gründen gefährdet:

1. Es fehlt eine Verankerung des Informationssicherheitsmanagements in der Governance der IT-Konsolidierung Bund. Insbesondere ist kein Informationssicherheitsbeauftragter der IT-Konsolidierung installiert und es fehlt ein IT-Risikomanagement mit Berichtsweg an den IT-Rat. Das BSI stünde hierfür zur Verfügung.
2. Das BSI ist heute nur eingeschränkt in der Lage, über das Informationssicherheitsniveau des gesamten IT-Verbunds der konsolidierten IT Auskunft zu geben. Es fehlen dem BSI Prüfungsrechte gegenüber zentralen IT-Dienstleistern, Netzdienstleistern und den die IT-Konsolidierung nutzenden Bundesbehörden (Kunden).

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?

Die Vertrauenswürdigkeit und Integrität des Herstellers ist insbesondere bei IT-Sicherheitsprodukten von zentraler Bedeutung. Um Abhängigkeiten von einzelnen Herstellern zu vermeiden, muss ein breites Fundament an IT-Sicherheitsprodukten in Verbindung mit einer Multi-Vendor-Strategie etabliert werden. Zur Steigerung der Vertrauenswürdigkeit eines Herstellers können bestimmte Anforderungen vertraglich vereinbart werden:

- No-Spy-Klausel,
- Offenlegung von technischer Dokumentation, die die Anwendung von Sensorik zur

Anomaliedetektion und Stichprobenkontrollen ermöglicht,
- Sourcecode-Hinterlegung.

Obwohl durch Zertifizierung nach Common Criteria das Sicherheitsniveau signifikant gesteigert werden kann, ist es unrealistisch, ein komplexes Produkt wie einen Hochleistungsprozessor zu zertifizieren. Die Dauer einer Zertifizierung steigt exponentiell mit der Komplexität des zu zertifizierenden Produktes. Daher sind Zertifizierungen nur für kleine, klar abgegrenzte Komponenten wie insbesondere Sicherheitselemente sinnvoll.

Der aktuelle Entwurf des Kataloges von Sicherheitsanforderungen nach TKG §109 enthält in Anlage 2 (Punkt 8) Forderungen in Bezug auf die Sicherstellung einer ausreichenden Diversität sowohl im Kern-Netz als auch Funkzugangsnetz durch die TK-Anbieter. Es wird gefordert, dass Komponenten / Systeme von zwei unterschiedlichen Herstellern verwendet werden und dass die Komponenten eines Herstellers maximal zwei Drittel aller Komponenten ausmachen sollen. Vorteile einer Multi-Vendor-Strategie liegen in der Verringerung der Abhängigkeiten von einzelnen Herstellern. Darüber hinaus sinkt das Bedrohungspotential durch Schwachstellen in einzelnen Produkten (vgl. Zwei-Browser-Strategie). Als Nachteile kommen insbesondere höhere Kosten für Beschaffung, Einführung und Pflege gegenüber einer IT-Monokultur / homogenen IT-Landschaft zum Tragen. Außerdem muss dann mehreren Herstellern vertraut werden.

Ein Haftungsregime kann die Durchsetzung der o.g. Anforderungen bekräftigen. Die derzeit existierenden gesetzlichen Haftungsgrundlagen in Deutschland sind dabei aus Sicht des BSI grundsätzlich geeignet, zur Durchsetzung eines angemessenen IT-Sicherheitsniveaus beizutragen. Als durchaus problematischer erweist sich im Einzelfall allerdings eine Rechtsdurchsetzung gegenüber Herstellern oder Diensteanbietern im Ausland, da diese in der Regel mit Zeitverzug, finanziellem Aufwand und einer fremden Rechtsordnung einhergeht, die ggf. deutlich von der Deutschen abweicht.

Die Rolle (unabhängiger) wirksamer Aufsichtsstrukturen ist für ein Vertrauen in sichere IT-Infrastruktur fundamental. Dies ist vor allem im Bereich der Sicherheitszertifizierung im IT-Bereich zu erkennen (vgl. Erwägungsgrund 65 der VO (EU) 2019/881 (Cyber Security Act - CSA)).

Mit dem Cyber Security Act ist auf europäischer Ebene ein Regelwerk in Kraft getreten, das vor allem Vertrauen in ITK-Produkte und Sicherheitsinfrastruktur adressiert. In der Verordnung werden darüber hinaus Aufsichtsverantwortlichkeiten klar benannt, zugeordnet und die notwendigen Mittel bereitgehalten, die Vorgaben der Verordnung durchzusetzen. Dabei ist besonders zu betonen, dass die Verordnung klar die Unabhängigkeit der Zertifizierungsstellen von den Überwachungs- und Aufsichtsbehörden voraussetzt (insb. Art. 58 Abs. 3 und 4 CSA). Auch soll über die ENISA das Zusammenwirken auf internationaler Ebene im Bereich der Cyberabwehr und dem Vertrauen in ITK-Produkte gesteigert werden. Insbesondere sollte so die Zusammenarbeit mit Organisationen wie der OECD, der OSZE und der NATO gestärkt werden.

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?

Grundsätzlich entfaltet jeder geschlossene Vertrag, unabhängig ob zwischenstaatlich oder privatrechtlich, eine sog. Bindungswirkung, d.h. die Parteien sind mit dem Vertragsabschluss an den Vertrag gebunden. Es ist daher möglich, ein zwischenstaatliches Abkommen als Mittel zum Schutz vor Abhörmaßnahmen zu nutzen.
Es ist grundsätzlich ein wirksames Mittel, No-Spy-Vereinbarungen zu schließen bzw. No-Spy-

Klauseln in Verträge einzubinden. Sofern ein schuldhafter Verstoß gegen diese Vereinbarung/Klausel nachgewiesen werden kann, hat der Gläubiger u.a. die Möglichkeit Schadenersatz zu verlangen und/oder das Vertragsverhältnis zu beenden.
Die Wirksamkeit impliziert jedoch nicht die Effektivität. Um eine Effektivität in der Umsetzung zu gewährleisten, muss initial ggf. sogar fortwährend überprüft werden, ob tatsächlich keinerlei Überwachungs- bzw. Abhörmaßnahmen vorgenommen werden.
Bei einer Beurteilung der Durchführbarkeit solcher Tests, ist die Unterscheidung zwischen Hard- und Softwarekomponenten geboten.
Eine praktische Durchführbarkeit von Konformitätstest an Hardwarekomponenten steht in Anhängigkeit zu der Menge an Hardware und der tatsächlichen Zugänglichkeit zum jeweiligen Hardwareprodukt. Je mehr Hardwarekomponenten geprüft werden müssen, desto schwieriger wird eine personelle Umsetzung, so dass nur noch Stichproben möglich sind.

Die praktische Durchführbarkeit von Konformitätstest an Softwareprodukten stellt sich als wesentlich komplexer dar. Diese kann effektiv nur erfolgen, wenn der gesamte Quellcode offengelegt würde und dieser komplett überprüft werden könnte.
Eine Alternative zur Herausgabe des Quellcodes und damit Preisgabe des wichtigsten Geschäftsgeheimnisses wäre ein Quellcodehinterlegungsvertrag ähnlich eines Escrow Agreements, welcher zur Offenlegung in begründeten Verdachtsfällen berechtigen würde.
Quellcodehinterlegungsverträge (Escrow Agreement) sollen einer besonderen Gefahr, die mit der Softwareerstellung verbunden ist, vorbeugen.

Ein genereller Marktausschluss von Komponenten-Anbietern wäre dann ein effektives Mittel zum Schutz der Vertrauenswürdigkeit und Hardware-/Software-Integrität, wenn sichergestellt wäre, dass dieser Ausschluss alle potenziell gefährlichen Anbieter umfassen würde.
Dies wirft allerdings die Frage auf, wie eine solche potentielle Gefährlichkeit festgestellt werden sollte. Würde dies einen Vorabtest der Hard- oder Software bedeuten, müsste er unter den oben bereits beschriebenen Kriterien erfolgen.
Eine Abschottung der Märkte bzw. ein Ausschluss von Komponenten-Anbietern auf dem Markt würde einen schwerwiegenden Eingriff in die freie Marktwirtschaft bedeuten, welche nur wenig staatliche Kontrolle oder Marktregulierung duldet. Ein derartig schwerer Eingriff wäre nur dann angemessen, wenn das zu schützende Gut nicht außer Verhältnis zum verfolgten Zweck stünde.

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?**

Die Bundescloud bietet dem Bund große Gestaltungsmöglichkeiten, hohe Flexibilität und ein hohes Maß an Kontrolle, vor allem für Daten und Prozesse, für die dies notwendig ist (z. B. Verschlusssachen). Zum Schutz von Daten in Kommunikationsnetzen vor dem Zugriff Dritter sind umfangreiche IT-Sicherheitsmaßnahmen erforderlich, beispielsweise eine wirksame physische oder gleichwertige Trennung von Kommunikationsnetzen von anderen Kommunikationsnetzen. Sollte die Bundescloud alleine nicht sämtliche Bedürfnisse aller Bundesbehörden decken können, kann das Angebot ggf. durch weitere Clouds ergänzt werden (z. B. Angebote des Bundes für Bürger, Spezialanwendungen). Es ist wichtig und sinnvoll, den Aufbau der Bundescloud als Basisinfrastruktur für die Bundesverwaltung weiter voranzutreiben, technische Expertise bei den Mitarbeitern des Bundes aufzubauen und für kritische Vorgänge ein möglichst hohes Maß an Kontrolle und Stabilität zu erhalten.

GAIA-X ist ein wertvoller Ansatz und sollte mit Nachdruck verfolgt werden. Der Erfolg des Modells wird davon abhängen, ob es gelingt, interessante und wirtschaftlich relevante Angebote auf der Plattform bereitzustellen (z. B. im Bereich Office/Groupware). Hierzu werden starke Partner benötigt. Das Projekt kann auch nur dann erfolgreich sein, wenn strenge Anforderungen an die IT-Sicherheit gestellt und diese für den Nutzer transparent nachgewiesen werden.

Der sogenannte CLOUD-Act (Clarifying Lawful Overseas Use of Data Act) regelt den Zugriff auf Daten von US-Kommunikationsanbietern, die im Ausland gespeichert sind, durch US-Strafverfolgungs-Behörden durch eine gerichtliche Anordnung. Bei der Auswahl von Cloud-Diensten sind solche Regulierungen durchaus relevant: Beispielsweise sind Behörden rechtlich verpflichtet, Privat- und Dienstgeheimnisse zu wahren und diese vor unbefugtem Zugriff zu schützen, haben aber selbst keine Möglichkeit Widerspruch gegen eine solche US-gerichtliche Anordnung einzulegen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat sich in seinem 27. Tätigkeitsbericht ähnlich geäußert, und angeführt, dass die Vorgaben für eine Auftragsverarbeitung von personenbezogenen Daten nach § 62 BDSG von Anbietern, die dem CLOUD-Act unterliegen, nicht eingehalten werden können.

Zum Schutz vor dem Zugriff auf Daten durch unberechtigte Dritte in Kommunikationsnetzen können Maßnahmen ergriffen werden: Daten in Bewegung können über eine Transportverschlüsselung nach Stand der Technik geschützt werden (vgl. Publikation "Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden"). Eine Verschlüsselung der Daten selbst erhöht die Sicherheit nochmals, in Fällen wo dies möglich ist. Um technische Sicherheitsanforderungen oder -mechanismen an vertrauenswürdige Intermediäre zur kooperativen Datennutzung zu formulieren, müssen zunächst die genauen Rahmenbedingungen und die Zielsetzung des Szenarios spezifiziert und dann analysiert werden. Die Überprüfung der Umsetzung von entsprechenden Sicherheitsanforderungen kann ggf. durch externe Audits im Rahmen einer Zertifizierung erfolgen.

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

Standards internationaler, offener, konsensualer und freiwilliger Standardisierungsorganisationen wie ISO/IEC, CEN/Cenelec oder DIN/DKE gewährleisten durch die breite Beteiligung der Fachöffentlichkeit ein hohes Maß an Transparenz und Ausgewogenheit der technischen Anforderungen. Durch die hohe Anzahl der beteiligten Experten - wie z. B. des BSI - und dem offenen Zugang zu den Dokumenten ist für eine hohe Qualität der sicherheitstechnischen Anforderungen gesorgt.
Mit Hilfe von Produktzertifizierungen lassen sich die Produkte verschiedenster Hersteller durch unabhängige Zertifizierungsstellen prüfen und dahingehend bestätigen, dass sie die an sie gestellten Sicherheitsanforderungen der jeweiligen Standards erfüllen. Für den Kunden wird somit leicht nachvollziehbar, welche Produkte die an sie gestellten Sicherheitsanforderungen erfüllen.

Allerdings können auch zertifizierte Produkte „Hintertüren“ enthalten – entweder durch eine nicht ausreichende Prüftiefe, oder die „Hintertüren“ werden nach der Zertifizierung eingebaut.

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 dieGrenzen der Überprüfbarkeit?

Eine (hoheitliche) Zertifizierung von IT-Produkten mit dem Ziel der Gewährleistung und Stärkung des Nutzervertrauens und der IT-Sicherheit erfordert eine Regulierung, die die Anbieter und Hersteller von IT-Produkten verpflichtet, die erforderliche Sicherheitszertifizierung zu erlangen. Die zuständigen Prüf- und Zertifizierungsstellen müssen über die notwendige Fachkompetenz und die Prozesse zur Durchführung der Prüfverfahren verfügen und gegenüber einer zuständigen nationalen Aufsichtsstelle nachweisen.
Aufgrund der Komplexität der Sachlage und der ständigen Fortentwicklung der Technologie muss der Prüfrahmen, die Prüftiefe sowie Art und Umfang der Überwachung der Zertifikate angemessen, z.B. im Kontext spezifischer Anwendungssektoren festgelegt werden, idealerweise durch nationale oder internationale Standards und gesetzliche Regularien. Der neue EU Cyber Security Act wird im Bereich der Sicherheitszertifizierung von IT-Produkten einen EU-weiten Rahmen spannen.

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

Das BSI als die Cyber-Sicherheitsbehörde des Bundes wirkt gemäß seines gesetzlichen Auftrags zur Förderung der Sicherheit in der Informationstechnik (§ 3 (1) BSIG) darauf hin, sämtliche Sicherheitslücken umgehend und im vertrauensvollen Austausch mit den Technologieherstellern zu schließen. Das BSI bewertet ein Offenhalten und den Handel von Schwachstellen als schädlich für die Informationssicherheit in der Digitalisierung. Es schadet sowohl der wirtschaftlichen Prosperität Deutschlands als auch dem Vertrauen der Bürgerinnen und Bürger in Technologie.

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?

Das sog. IT-Grundrecht ist eine vom Verfassungsgericht festgestellte Ausprägung des allgemeinen Persönlichkeitsrechtes, um den aus Art. 2 Abs. 1 i.V.m. Art.1 Abs. 1 GG abgeleiteten individuellen Persönlichkeitsschutz vor den neuartigen Gefährdungen durch technischen Fortschritt und den Wandel der Lebensverhältnisse (vgl. BVerfG - 1 BvR 370/07, C I. 1. a. Rn. 168 f.) zu gewährleisten.
Für den Schutz der persönlichen IT-Systeme, den Schutz der Vertraulichkeit der Kommunikation und den Schutz digitaler Infrastrukturen heißt das, dass es als extensives Auffanggrundrecht gegen einen ungerechtfertigten staatlichen Zugriff schützt, soweit dieser potentiell persönlichkeitsrechtsgefährdend ist:
Das Grundrecht erlaubt somit in der Praxis Hacking, Trojaner und vergleichbare Zugriffe ohne Einwilligung auf quasi alle Computersysteme, Netzwerke, Telefone, Mobilgeräte, IoT-Geräte und sonstige IT-Systeme mit Personenbezug nur noch unter der Voraussetzung, dass ein allgemeines beschränkendes Gesetz vorliegt und der Eingriff verhältnismäßig ist (C I. 2. Rn. 207).
Aufgrund der Bindungswirkung der genannten Entscheidung und des rechtsstaatlichen Grundsatzes des Vorrangs des Gesetzes ist jede staatliche Stelle daran gebunden. Regulatorisch erfordert dies die besonnene Zurückhaltung bei der Schaffung von Notwendigkeiten für eine breite staatliche Überwachung und durch die Schaffung klar begrenzter, sich des besonderen Eingriffs bewusster Ermächtigungsgrundlagen für Ausnahmefälle.

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?

Die Souveränität des Einzelnen sowie der rechtskonforme Zugriff des Staates bedürfen einer sorgfältigen Abwägung unter Beachtung des Angemessenheitsgrundsatzes.
Wichtig ist aus Sicht des BSI vor allem, dass staatliche Zugriffe so ausgestaltet werden, dass dadurch keine Schwächung des Sicherheitsniveaus gegenüber Angriffen Dritter erfolgt. Das bedeutet, dass der täterseitige Missbrauch von Zugriffsmöglichkeiten, die der Staat aus berechtigten Interessen geschaffen hat, mit hoher Zuverlässigkeit ausgeschlossen werden muss. Dies schließt insbesondere eine bewusste Schwächung von Verschlüsselungsverfahren und das künstliche Offenhalten von Schwachstellen in IT-Produkten und IT-Dienstleistungen aus, denn solche 'Hintertüren' können auch von Angreifern missbraucht werden.
Wo staatliche Zugriffsmöglichkeiten geschaffen werden, muss deshalb immer eine zuverlässige Authentisierung der berechtigten Stellen erfolgen und eine Überprüfbarkeit des Zugriffs sichergestellt sein.

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

Aus Sicht des BSI müssen die folgenden Themen zwingend Eingang in die Weiterentwicklung des IT-Sicherheitsgesetzes finden:

- Digitaler Verbraucherschutz, auch als neue Aufgabe im Koalitionsvertrag verankert (§ 3 Absatz 1 Satz 2 Nr. 14a BSIG-E) & freiwilliges IT-Sicherheitskennzeichen (§ 9a BSIG-E)
- Aktive Suche nach Sicherheitslücken – sogenannte „Scan-Befugnis“, §§ 7b BSIG-E, § 7c BSIG-E
- Schutz der Kommunikationstechnik des Bundes, § 5 und § 5a BSIG-E sowie Definition in § 2 Absatz 3 BSIG-E
- TKG - Präventive Informationspflicht der Provider (§ 109a TKG-E), Anordnungsbefugnis des BSI bzgl. Maßnahmen (nach § 109a Absatz 4 bis 6 TKG-E), Bereinigen von Systemen
- Kontrolle der Kommunikationstechnik des Bundes, § 4a BSIG-E
- KRITIS-Erweiterung und neue „Infrastrukturen in besonderem öffentlichen Interesse“
    - Neue Regelungen zu „KRITIS Kernkomponenten“, §§ 2 Absatz 13, 8a Absatz 6 BSIG-E– Absicherung der Lieferkette
    - KRITIS-Betreiber-Pflicht zum Einsatz von Systemen zur Angriffserkennung, § 8a BSIG-E

17. Ist 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?

Das BSI im Geschäftsbereich des BMI wird durch dieses in seinen Aufgaben unterstützt. Bis dato lag der Fokus der Tätigkeit des BSI im Bereich der Informationssicherheit. Durch Festlegungen im Koalitionsvertrag sowie neue gesetzliche Grundlagen erhält das BSI stetig weitergehende Aufgaben mit dem Ziel, die Sicherheit in der Digitalisierung für Deutschland zu gestalten. Exemplarisch seien hier die Beispiele e-Health, autonomes Fahren sowie der digitale Verbraucherschutz genannt. Das BSI gestaltet damit als zentrale Kompetenzstelle des Bundes die Digitalisierung ressortübergreifend. Die integrierte Wertschöpfungskette der Cyber-Sicherheit aus Prävention, Detektion und Reaktion unter einem Dach ist ein weltweites Alleinstellungsmerkmal des BSI. Im Übrigen handelt es sich um eine politische Fragestellung.

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?

Als Cyber-Sicherheitsbehörde des Bundes kommt das BSI seinen gesetzlichen Aufgaben nach und erhöht die Cybersicherheit, indem es Empfehlungen gibt, Anwender berät, Vorgaben macht und die Umsetzung prüft. Die Rolle des BSI sollte weiter gestärkt werden und das BSI im Sinne von "Security by Design" bei allen wichtigen Digitalisierungsvorhaben des Bundes bereits zu Beginn verpflichtend eingebunden werden.
Im Bereich der nationalen und internationalen Zusammenarbeit sollte das Ziel sein, eine komplementäre und auf Kooperation ausgerichtete Cybersicherheitsarchitektur zu schaffen. Die Kompetenz des BSI in aktuellen Themen der Digitalisierung sollte hierdurch den nationalen und internationalen Partnern zur Verfügung gestellt und die Kooperationen verstärkt werden. Wo erforderlich, sollten hierfür weitere Rechtsgrundlagen geschaffen werden.

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?**

Die öffentliche Diskussion zum Themenkomplex "proaktive Cyberabwehr" sollte aus Sicht des BSI differenziert geführt werden. Systeme der Angreifer enthalten oft wertvolle Informationen darüber, welche Opfer bereits betroffen sind, welche Ziele zukünftig angegriffen werden sollen oder welche Daten entwendet wurden. Es wäre wünschenswert, dass sich deutsche Sicherheitsbehörden unter strengen Rahmenbedingungen auf solche Systeme einloggen dürfen, um diese Informationen zu gewinnen und für die Abwehr bzw. für die Schadensbegrenzung zu nutzen. Dabei muss sorgfältig darauf geachtet werden, dass durch diesen Zugriff keine inakzeptablen Seiteneffekte entstehen, etwa eine Beeinträchtigung unbeteiligter IT-Systeme oder IT-Anwendungen. Auch dürfen solche Maßnahmen nur dann ergriffen werden, wenn weniger invasive Maßnahmen nicht zum Ziel führen. Auch der Grundsatz der Angemessenheit muss jederzeit beachtet werden.

Die Attribution von Cyber-Angriffen ist ein kontinuierlicher Analyse-Prozess auf verschiedenen Ebenen, u.a. technischer Ebene, nachrichtendienstlicher Ebene und politischer Ebene.

Ob eine Attribution gelingt, ist maßgeblich von der Datenlage des zuzuordnenden Vorfalls sowie von Informationen über vergangene Vorfälle abhängig. Attribution ist daher weniger eine Frage der Forschung, als der tatsächlich durchgeführten kontinuierlichen Analyse von Angriffen aus unterschiedlichen Perspektiven. Das BSI fokussiert sich aktuell auf die technische Attribution einzelner Angriffe auf der Ebene von Angreifer-Gruppen.

Das BSI spricht sich uneingeschränkt gegen jede Form der Schwächung von Sicherheitsvorkehrungen aus. Hardware und Software weisen trotz aller Bemühungen immer noch so viele ungewollte Schwachstellen auf, dass kein Bedarf besteht, Schwachstellen bewusst offen zu halten.

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

Das BSI fordert seit jeher die Verschlüsselung von Datenverkehr zur Erhöhung der Sicherheit im Hinblick auf das Schutzziel Vertraulichkeit. Die Interoperabilität verschlüsselt kommunizierender Messenger würde die Sicherheit und den Schutz im Netz fördern. Applikations- und herstellerübergreifend sicher kommunizieren zu können, verbessert die Digitalisierung von Verwaltung, Wirtschaft und Gesellschaft. Standardisierung bildet die Rahmenbedingung für sichere Verfahren zur verschlüsselten Kommunikation. Vertrauenswürdige IT-Systeme und Anbieter auf Basis global nutzbarer technischer Architekturen helfen, die digitale Resilienz zu stärken. Gängige Standards wie PGP/SMIME bei der E-Mail-Kommunikation zeigen, dass nutzerfreundliche und handhabbare Lösungen interoperabel bereitgestellt werden können. Die Verbreitung sicherer Produkte („Security by Design“) wird durch angemessene und einheitliche IT-Sicherheitsstandards unterstützt und durch quelloffene Implementierungen nachvollziehbar umgesetzt.

Zwei Effekte sollten bei der Forderung nach Interoperabilität von verschlüsselten Messengern berücksichtigt werden. Während der Lock-in-Effekt eine starke Bindung des Anwenders an einen einmal gewählten Messenger bewirkt, ist der Netzwerkeffekt maßgeblich für eine Bevorzugung eines Messengers mit der größten Nutzerzahl seiner Kommunikationspartner.

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?

IT-Sicherheitsforschung ist ein wichtiger Baustein, um auf neuen Entwicklungen basierende innovative IT-Sicherheitsverfahren auszuarbeiten. IT-Sicherheitsforschung trägt dazu bei, das Sicherheitsniveau in Deutschland zu erhöhen, Bürgerinnen und Bürger sowie Unternehmen und den Staat vor Angriffen präventiv und nachhaltig zu schützen und die Wettbewerbsfähigkeit des Standorts Deutschland zu stärken.

Deutschland verfügt im Bereich IT-Sicherheit über eine exzellente Forschungslandschaft aus international hoch anerkannten Gesellschaften, Instituten und Forschungsclustern der Hochschulen. Dennoch besteht eine Gefahr, dass wir im internationalen Vergleich abgehängt werden. Hauptgrund ist die immer schnellere Verbreitung der Digitalisierung in allen Lebensbereichen und die damit einhergehenden wachsenden Schutzbedarfe und zunehmenden Risiken. So wie die Bedrohungen im Cyberraum zunehmen, muss auch noch stärker in IT-Sicherheitsforschung und -entwicklung investiert werden.
Notwendig ist eine frühzeitige Einbindung der IT-Sicherheit als integraler Bestandteil in Technologieentwicklungen, wodurch Rahmenbedingungen zur Herstellung vertrauenswürdiger Technologien geschaffen und gleichzeitig nationale technologische Kompetenzen gestärkt werden. Schlussendlich muss der Transfer in die nationale Wirtschaft gewährleistet sein, um die Wertschöpfungskette für die geförderten Technologien durch die Bereitstellung marktfähiger Produkte hoher Vertrauenswürdigkeit zu erweitern. Dies wird beispielsweise durch einen kooperativen Ansatz mit investitionsfreudigen deutschen Unternehmen – ggf. auch im europäischen Verbund – sowie durch eine gezielte Förderung der Gründung von Startups im Bereich der Digitalisierung und insbesondere der Cybersicherheit unterstützt.

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?

Das BSI sieht die Vermittlung von IT-Qualifikationen im Bereich der Bildung als wesentlichen Beitrag zur sicheren Gestaltung der Digitalisierung. Durch Wissen über die Herausforderungen und Chancen der Informationstechnik werden Endverbraucher wie Fachkräfte in die Lage versetzt, Risiken einschätzen und bewerten zu können, effektive Prävention zu betreiben und letztendlich auch im Falle einer Betroffenheit richtig zu reagieren.

Das BSI begrüßt die Initiativen verschiedener Hochschulen und Universitäten (z.B. Hochschule des Bundes, Universität Bonn, Hochschule Bonn-Rhein-Sieg), eigenständige Studiengänge mit dem Schwerpunkt "IT-Sicherheit" anzubieten. Darüber hinaus hat es sich beim BSI bewährt, beispielsweise durch Praktika und die Betreuung von Abschlussarbeiten Studierende in ihrer fachlichen Entwicklung zu unterstützen und den Einstieg in das Thema IT-Sicherheit zu vereinfachen.

Des Weiteren liegt großes Potential in der Steigerung des Frauenanteils in der Informationstechnik und den zugehörigen Studiengängen. Das BSI begrüßt aus diesem Grund Initiativen wie "Komm, mach MINT" oder des Bitkom e.V., welche sich dieser Thematik annehmen.

Zusätzlich wird es notwendig sein, die in der Bildung und Ausbildung tätigen Lehrkräfte zu befähigen, Inhalte der Informationstechnik und Informationssicherheit vermitteln zu können.
Das BSI versteht sich unter anderem mit seinem Informations- und Beratungsangebot "BSI für Bürger" als kompetente Anlaufstelle zu Fragen der IT-, Internet- und Cyber-Sicherheit für Privatanwender/innen. Dieses Angebot wird aktuell für diverse Subzielgruppen ausgebaut, unter anderem für Eltern und Kinder sowie Senior/innen. Mit einer „BSI im Dialog“-Veranstaltung am 29. November 2019 startete das BSI die Arbeit zur Stärkung der Cyber-Sicherheit für die Zielgruppe Schule.

Mit Blick auf das eigene Personal sieht das BSI große Herausforderungen in der schnelllebigen Weiterentwicklung der Anforderungen an die Beschäftigten. Die „Halbwertszeit“ des Wissens gestaltet sich in der IT- und IT-Sicherheitsbranche besonders kurz.

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?

Das BSI setzt sich seit 2017 intensiv mit dem Thema Blockchain auseinander. Der Veröffentlichung von Eckpunkten zur Sicherheit von Blockchain Anfang 2018 folgte 2019 eine umfangreiche Analyse des BSI („Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertungen“[1]), die unter Beteiligung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt wurde.
Diese Analyse hat ergeben, dass in vielen Praxisfällen noch Umsetzungsfragen wie Langzeitsicherheit und Behandlung der Virtuell-Real-Schnittstelle – also der Authentisierung von extern eingespeisten Daten – offen sind. Das Potential der Blockchain-Technologie für viele Anwendungen hängt auch von der Klärung dieser Fragen ab.
Das BSI hat das Forschungszentrum Informatik (FZI) in Karlsruhe mit einem Projekt zur „Sicherheitsuntersuchung ausgewählter Blockchain-Anwendungen“ beauftragt. Dabei wurde

[1] Download unter www.bsi.bund.de/blockchain

zunächst ein Marktüberblick geschaffen und danach eine Reihe von Produkten exemplarisch auf ihre Sicherheitseigenschaften untersucht.
Grob lassen sich die Ergebnisse wie folgt zusammenfassen:

- Der Anteil an Produkten und Anwendungen mit deutscher Herkunft ist recht gering.
- Marktdurchdringung und Reifegrad vieler Anwendungen sind gering.
- Existierende Angebote wurden bisher kaum öffentlichen Sicherheitsanalysen unterzogen.
- Zahlungsverkehr und Spiele sind die Hauptanwendungsfelder von existierenden Blockchain-Anwendungen.
- Viele Produkte kombinieren ungeprüft Software aus verschiedenen externen Quellen.

Datenschutz ist für den Einsatz der Blockchain-Technologie in der EU ein wesentlicher Gestaltungsfaktor, da die Anforderungen der DSGVO (wie „Recht auf Vergessenwerden“) direkte Auswirkungen auf die Umsetzung von Blockchains haben. Dies kann durchaus als Standortvorteil genutzt werden, schränkt aber auch die umsetzbare Funktionalität ein.
Grundsätzliche Vorteile gegenüber alternativen Technologien zur Datenhaltung sind vom Einsatz von Blockchains momentan allenfalls in Anwendungsfällen zu erwarten, an denen eine Vielzahl von Parteien beteiligt sind und keine vertrauenswürdige zentrale Stelle existiert, die die Anwendung kontrolliert.

Die Bundesregierung plant, in dieser Legislaturperiode 650 Millionen Euro in die Förderung von Quantentechnologien in Deutschland zu investieren. Im Rahmenprogramm „Quantentechnologien – von den Grundlagen zum Markt“ werden Ziele und Maßnahmen hierzu definiert. In diesem Rahmenprogramm werden auch Aktivitäten und Aufgaben des BSI beschrieben.
Quantentechnologien sind aus Sicht der IT-Sicherheit zuerst eine Bedrohung. Mit Existenz eines hinreichend großen universellen Quantencomputers wäre der heute eingesetzten Public-Key-Kryptografie die Grundlage entzogen. Um eine fundierte Einschätzung des aktuellen Entwicklungsstandes bzw. der potentiellen zukünftigen Verfügbarkeit eines Quantencomputers zu erhalten, wurde vom BSI die Studie „Entwicklungsstand Quantencomputer“ in Auftrag gegeben. Diese Studie[2] zeigt, dass aktuell eine enorme Anstrengung nötig wäre, um eine kryptografisch relevante Skalierung von Quantencomputer-Technologien vorzunehmen. Gleichzeitig wird deutlich, dass die Entwicklung durch starke Industrieakteure und große Forschungsprogramme schneller geworden ist und dass weitere kommerzielle Anwendungen diese noch beschleunigen könnten. Die Studie schätzt kurzfristige Entwicklungssprünge in Richtung kryptografisch relevanter Quantencomputer als eher unwahrscheinlich ein. Für kryptografische Anwendungen, die Informationen mit langen Geheimhaltungsfristen und hohem Schutzbedarf verarbeiten, ergibt sich dennoch akuter Handlungsbedarf. Hier besteht die Gefahr darin, dass Nachrichten zur Schlüsselaushandlung und die mit den ausgehandelten Schlüsseln verschlüsselten Daten auf Vorrat gesammelt und in der Zukunft mit Hilfe eines Quantencomputers entschlüsselt werden ("store now, decrypt later").

Zurzeit werden in einem – frühestens 2022/23 abgeschlossenen – Prozess des US-amerikanischen National Institute of Standards and Technology (NIST) kryptografische Verfahren standardisiert, die resistent gegen Angriffe mit Quantencomputern sein sollen (Post-Quanten-Kryptografie).
Das BSI begrüßt diese Aktivitäten. Dennoch sind die „neuen“ Verfahren noch nicht so gut erforscht wie die „klassischen“ Verfahren (wie RSA und ECC). Das BSI empfiehlt daher, Post-Quanten-Kryptografie möglichst nicht isoliert einzusetzen, sondern nur „hybrid“, d. h. in Kombination mit klassischen Algorithmen. Im Hochsicherheitsbereich wird vom BSI der Einsatz von hybriden Lösungen vorgesehen.
Neben der Entwicklung von quantencomputer-resistenten kryptografischen Verfahren ist auch die Anpassung von kryptografischen Protokollen an die neuen Verfahren eine große Herausforderung. Aus Sicht des BSI steht der Sicherheitsaspekt bei der Auswahl von neuen Algorithmen naturgemäß an erster Stelle. Als Verfahren für eine Schlüsseleinigung sind das gitterbasierte Verfahren

[2] Verfügbar unter www.bsi.bund.de/qcstudie

FrodoKEM und das codebasierte Verfahren Classic McEliece die konservativste Wahl. Das BSI beabsichtigt, in der neuen Version der Technischen Richtlinie zu Algorithmen und Schlüssellängen[3] die beiden genannten Verfahren als grundsätzlich geeignet (in einer hybriden Lösung) zu empfehlen, wenn ein Hersteller oder Nutzer schon jetzt ein quantencomputer-resistentes Verfahren zur Schlüsseleinigung einsetzen möchte.
Neben der Lösung Post-Quantum-Kryptografie wird auch die Nutzung der sogenannten Quantenkryptografie vorgeschlagen, die Sicherheit auf Basis physikalischer Prinzipien garantieren soll. Das BSI unterstützt Projekte zur Quantenkryptografie beratend (Q.Link.X, QuNET) und beabsichtigt die Beauftragung eines Protection Profiles zur Prüfung von Geräten zur Quantum-Key-Distribution (QKD) nach den Common Criteria. Momentan stehen verschiedene Gründe dem alleinigen Einsatz von QKD entgegen.

Die Entwicklungen in der Post-Quanten-Kryptografie werden von der deutschen Industrie beachtet und einige Hersteller haben bereits quantencomputer-resistente Algorithmen implementiert oder bieten sogar schon Produkte an. An einer Reihe der Einreichungen zum NIST-Prozess waren deutsche Co-Autoren beteiligt. Das BMBF hat am 22. August 2018 eine "Richtlinie zur Förderung von Forschungsvorhaben zum Thema 'Post-Quanten-Kryptografie'" veröffentlicht. Themenschwerpunkte für die Förderung sind "Quantencomputer-resistente Verfahren und ihre Sicherheitseigenschaften", "Effiziente, sichere Soft- und Hardware für quantencomputer-resistente Verfahren" sowie "Lösungen für eine einfache Migration zu quantencomputer-resistenten Verfahren". Das BSI begrüßt das Förderprogramm des BMBF und war an der Begutachtung der Forschungsvorhaben beteiligt. Insofern erscheint Deutschland im Bereich der Post-Quanten-Kryptografie wettbewerbsfähig. Im Bereich der Quantenkryptografie gibt es eine starke deutsche Forschungslandschaft; hier gilt es, die Forschungsergebnisse in Produkte zu überführen.

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

Das Offenlegen von Quellcode allein erhöht noch nicht die Sicherheit, da er potentiellen Evaluatoren und potentiellen Angreifern gleichermaßen offengelegt wird. Das Auffinden etwaig vorhandener Schwachstellen erfordert dennoch oft erhebliche Aufwände. Im Vergleich zu Closed Source bietet Software mit offengelegtem Quellcode sowohl Vorteile (der Code kann geprüft werden) als auch Nachteile (er wird ggf. weder gründlich noch umfassend geprüft oder nur von Angreifern, die entdeckte Schwachstellen nicht mitteilen, sondern für Ihre Zwecke ausnutzen.)

Bei der Behebung von Schwachstellen bietet Open-Source-Software im Vergleich zu proprietärer Software oft Vorteile, da die Hersteller proprietärer Software nicht immer erreichbar, bereit oder in der Lage sind, geeignete Patches/Updates zur Korrektur des Problems zu liefern. Bei Open-Source-Software können entsprechende Updates/Patches notfalls auch durch andere fachkundige Mitglieder der Community herausgegeben werden. Dieser Vorteil von Open-Source-Software gilt nicht zwangsläufig auch für proprietäre Software, deren Quellcode lediglich zur Einsichtnahme offengelegt wird (sogenannte Shared-Source-Software)

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?

[3] BSI TR-02102-1: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“.

Das Wort „Einsatz“ wird so verstanden, dass davon der am Ende der Frage genannte Fall gemeint ist, wonach das Produkt gegen die dort genannten Gruppen eingesetzt wird.

Bei Haftungsregelungen muss grundsätzlich zwischen gesetzlichen und vertraglichen Haftungsregelungen unterschieden werden. In letzterem Fall ist es jedoch bereits fraglich, ob sich o. g. Anbieter bereitwillig einem vertraglichen Haftungsregime unterwerfen, welches sie für den aus deutscher Sicht unethischen oder rechtswidrigen Einsatz ihres Produktes zur Rechenschaft zieht.

Auf gesetzlicher Ebene ist es denkbar, Anbieter von der Auftragsvergabe auszuschließen, wenn ihre Produkte in Fällen eingesetzt werden, die die Fragestellung bereits darlegt oder die diesen vergleichbar sind. Problematisch bei diesem Ansatz, „*unredlichen*“ Anbietern den Marktzugang zu öffentlichen Auftraggebern zu verwehren, ist die Frage, bis zu welchem Punkt einem Anbieter der Einsatz seines Produktes zugerechnet werden kann.
Während ein Anbieter die Produktionskette, bis sie ihn erreicht, in einem gewissen Maß beeinflussen kann, ist der weitere Verlauf der Warenkette – abgesehen von seinem direkten Abnehmer – stärker seinem Einfluss entzogen. Der Anbieter, der regelmäßig Spyware an diktatorische Regimes zur Unterdrückung der politischen Opposition liefert, könnte sicherlich mittels einer gesetzlichen Bestimmung von Vergabeverfahren ausgeschlossen werden. Schwierig wird es, wenn durch Zwischenhändler oder einen lizenzwidrigen Einsatz dieser Spyware gegen Oppositionelle die Zurechnung zum Anbieter selbst nicht mehr klar erfolgen kann.

Ein möglicher Ansatzpunkt wäre, von Anbietern von Dual-Use-Gütern gesetzlich die Abgabe einer entsprechenden Eigenerklärung im Vergabeverfahren zu verlangen, in der der Anbieter ausführt, dass und wie er den ethisch korrekten Einsatz seines Produktes gewährleistet.