VERBAND DER INTERNETWIRTSCHAFT E.V.

Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)079

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

Berlin, 10.12.2019

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?*

   Unter digitaler Souveränität versteht eco die Fähigkeit, unabhängige Entscheidungen im digitalen Raum zu treffen und selbstbestimmt handeln zu können[1]. Für Deutschland und Europa kann festgestellt werden, dass Bürgerinnen und Bürgern ein breites, marktgetriebenes Angebot an Diensten und Produkten zur Verfügung und Auswahl steht. Bestehende Gesetzgebung und Rechtsprechung stärkt zudem ihre Bürger- und Verbraucherrechte. Grundlegender regulatorischer Handlungsbedarf kann hier nicht festgestellt werden.

   Gleichzeitig sollte betont werden, dass jeder Einzelne für die Ausübung und den Aufbau seiner digitalen Souveränität, ebenfalls Verantwortung trägt. In den Teilbereichen „Umgang mit relevanten Sicherheitsaspekten“ sowie „Wahrnehmung möglicher Risiken“, welche beide Voraussetzungen digitaler Souveränität sind, besteht derzeit bei der Bevölkerung ein erkennbares Defizit. Die Herausforderung besteht daher insbesondere darin, ein Bewusstsein für die Konsequenzen des Einsatzes digitaler Technologien zu stärken. Hierbei können gezielte Programme helfen, welche auch und insbesondere ältere Bevölkerungsgruppen erreichen (Beispiel Südkorea, Internetschulung für alle).

   Für Regierungen und die Wirtschaft kann darüber hinaus festgehalten werden, dass diese auch im Rahmen der Vertragsfreiheit ausreichend Möglichkeit haben, digital mündig zu entscheiden und souverän zu agieren.

[1] Vgl. https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p2-digitale-souveraenitaet-plattformbasierter-oekosysteme.pdf?__blob=publicationFile&v=4

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?*

   Für eco sind die Hoheit über Daten und deren Standortbestimmung sowie faire Wettbewerbsbedingungen in der EU, aber auch Wissen um den Umgang mit und für die Entwicklung von digitalen Technologien zentrale Elemente zur Förderung der digitalen Souveränität. In Europa wird die digitale Souveränität der Bevölkerung nur erhalten, wenn hohe Summen in Bildung, Ausbildung und Forschung investiert werden (kreativ: Entwickler, Programmierer, Ingenieure und nutzend/konsumierend: wissend um Einsatzmöglichkeiten und Konsequenzen). Aber auch auf nationaler Ebene besteht weiterer Bedarf für die Ausgestaltung von Bildungs- und Förderprogrammen.

   Im Bereich Datenhoheit und Wettbewerbsbedingungen ist der nationale Spielraum hingegen im Bereich der Anreize und der Förderung eher größer als in der inhaltlichen Themensetzung, die stark europäisch geprägt ist. Im Hinblick auf die Verwirklichung eines digitalen europäischen Binnenmarkts ist dies auch sinnvoll.

   Bei diesen Vorhaben ist ein offener, technologieneutraler Ansatz erstrebenswert, um Innovation, Vielfalt und marktgetriebene Entwicklung zu fördern und der Abhängigkeit von einzelnen Systemen oder Technologien entgegenzuwirken. Offene Standards, wie sie beispielsweise auch im Rahmen des GAIA-X Projekts diskutiert werden, können hierbei eine zentrale Rolle spielen. Geschaffene Standards sollten zumindest EU-weit gelten, idealerweise darüber hinaus auch international.

   Anreize für eine Stärkung der Digitalwirtschaft als Grundlage digitaler Souveränität können die Verbesserung der Standort- und Wettbewerbsbedingungen sein, um die Attraktivität des Standorts Deutschland zu erhöhen. Beispielsweise die Förderung neuer Nutzungsmöglichkeiten der Abwärme von Rechenzentren, steuerliche Begünstigungen von energiesparenden Servern mit Flüssigkeitskühlung, die Befreiung/Senkung von EEG-Umlage usw. sein.

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?*

   Ein wirksames Mittel gegen IT-Angriffe und -Kriminalität ist die Ende-zu-Ende-Verschlüsselung auf hohem Niveau sowie die Speicherung in verschlüsselter Form auf dem Zieldatenträger bzw. Server.

   Der dringendste Handlungsbedarf besteht hier bei staatlichen Akteuren dahingehend, dass keine Softwarelücken oder andere systematischen Schwachstellen und Angriffsmöglichkeiten nach deren Entdeckung bewusst offengehalten werden, um Ermittlungen oder Überwachungsmaßnahmen gegen Einzelne durchführen zu können. Denn dies geht zwangsläufig mit erheblichen Gefahren für Gesellschaft, Wirtschaft und den Staat selbst einher. Insbesondere ausländische Geheimdienste und die Organisierte Kriminalität könnten sich solche Lücken ebenfalls zu Nutze machen, wenn sie davon Kenntnis erlangen.

   Die digitale Souveränität im Hinblick auf eine freie und offene Netzarchitektur lässt sich am besten dadurch behaupten, dass man sein Technologieportfolio diversifiziert, Redundanzen bei der Datensicherung und Bereitstellung herstellt, und individuell geeignete Sicherheitsprozesse einführt und kontinuierlich fortentwickelt. Im Bereich der Betreiber stellen nachvollziehbare Sicherheitskonzepte und ein Zusammenwirken mit den Aufsichtsbehörden, insbesondere der BNetzA und dem BSI, geeignete Maßnahmen dar.

   Die Aufsichtsbehörden stehen in der Pflicht, effektiv bei der Schließung von Sicherheitslücken mitzuarbeiten, bestehende und Ihnen bekannt werdende Sicherheitslücken zu kommunizieren und ggf. im Rahmen ihrer Aufsichtspflicht tätig zu werden.

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

Ein vulnerabilitätsbasierter Ansatz für die Bestimmung von Sicherheit in IT-Systemen ist nur bedingt hilfreich, da die Größe oder Heftigkeit von Angriffen bedingt durch die unterschiedliche Kritikalität der Komponenten nicht zwingend mit den Auswirkungen korrelieren. Ein risikobasierter Ansatz erscheint aus Sicht der meisten IT-Sicherheitsakteure sinnvoller und wird im Rahmen der bestehenden Sicherheitskonzepte daher regelmäßig gewählt.

Zur Frage: Das niedrigste Schutzniveau ist in der Regel bei Endgeräten von privaten Nutzern, sowie deren Peripherie (Router, Connected Devices) anzutreffen. Diese sind meist am schwächsten geschützt, werden oft nicht aktualisiert und bestehende Sicherheitsrisiken bspw. in Form von Virusinfektionen werden gezielt für diese Geräte entwickelt, dort jedoch nicht behoben oder durch den Nutzer gar nicht bemerkt. Gleichzeitig sind diese Komponenten jedoch in der Regel am wenigsten kritisch für die Infrastruktur. Problematisch werden sie meist erst dann, wenn sie zu Botnetzen zusammengeschaltet werden, um größere Angriffe auf Netze und Infrastrukturen durchzuführen.

Sinnvoll wäre es daher, für diese Geräteklasse Sicherheitsanforderungen zu definieren, die nicht nur die Hersteller, sondern insbesondere auch deren Betreiber und Nutzer einhalten müssen. Hierbei sollte ein dialogorientierter Ansatz zwischen allen Beteiligten verfolgt werden und der jeweilige Markt- und Regulierungsrahmen berücksichtigt werden, um Akzeptanzprobleme und konkurrierende Standards, wie sie bspw. im Rahmen der Diskussion um die TR-Router zutage getreten sind, zu vermeiden.

Für Geräte im Einflussbereich der Netzbetreiber sowie im Einsatzbereich der kritischen Infrastrukturen bestehen bereits jetzt Regelungen, welche geeignete Sicherheits- und Betriebskonzepte vorsehen. Diese Regelungen werden regelmäßig an die aktuelle Rechtslage angepasst, so beispielweise nach Einführung der DSGVO oder aktuell durch eine Anpassung der aus §109 TKG folgenden Regelungen.

Sinnvoll für eine Erhöhung der IT-Sicherheit wäre die derzeit nicht normierte Einbeziehung von Herstellern und Inverkehrbringern von Geräten in die Verantwortung für die IT-Sicherheit.

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?*

   Die unmittelbare digitale Souveränität Deutschlands ist – wie in den Antworten zu 1 und 2 beschrieben – nicht zwingend durch den Betrieb von Software von Herstellern aus anderen Staaten gefährdet. Ein markt- bzw. wettbewerbsgetriebener Ansatz für die Wahrung der digitalen Souveränität sollte weiterverfolgt werden, anstatt auf Regulierung zu setzen.

   Maßgeblich für die Gestaltung der digitalen Souveränität des Bundes ist der stringente Einsatz offener, von einer Vielzahl von Anbietern unterstützter oder zumindest unterstützbarer Standards in der Verwaltung, die Stärkung der Vielfalt digitaler Infrastrukturen in Deutschland sowie die Förderung und Beschaffung interoperabler Systeme und Software (z.B. Browserlauffähig), um einseitige Abhängigkeiten zu vermeiden.

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?*

   Zu den Gründen des Scheiterns von Open Source IT-Projekten in der öffentlichen Verwaltung liegen keine ausreichenden Erkenntnisse vor. Eine Extrapolation aus den von Unternehmen und Einzelpersonen genannten Herausforderungen lässt jedoch auf eine mangelnde Interoperabilität mit Anwendungen anderer Teilbereiche der Verwaltung schließen, welche proprietäre Standards nutzen. Insofern erscheint nicht die eingesetzte Open-Source Software als ursächlich, sondern die Resilienz bestehender proprietärer Systeme gegen Integration, Anpassung und Veränderung.

Berichte über derartige Probleme haben jedoch in den letzten Jahren signifikant abgenommen und dürften bei einer geeigneten Umsetzung heute als weitestgehend überholt betrachtet werden.

Spezifischen Sicherheitsrisiken für bestimmte Systeme – darunter auch die der Bundeswehr – kann durch Einbeziehung in den KRITIS-Verbund und ggf. durch zusätzliche Auditierungs- und Zertifizierungsmaßnahmen Rechnung getragen werden. Zentral wäre dabei eine vertragliche Verankerung der Möglichkeit, jederzeit Source-Code Audits der eingesetzten Komponenten zumindest vornehmen zu können, um bestehende Sicherheitsrisiken zu erkennen und zu beheben oder bei aufkommenden Verdachtsmomenten und Hinweisen im Einzelfall in der Lage zu sein diesen nachgehen zu können.

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?*

   Grundsätzlich ist die Konsolidierung der IT-Systeme des Bundes vor dem Hintergrund des bestehenden Fachkräftemangels bei IT-Personal nachvollziehbar. Gleichzeitig gilt zu berücksichtigen, dass durch die Vereinheitlichung der Dienste die Abhängigkeit von einem einzelnen Dienst / Produkt zunimmt. Ähnliches gilt für die Zentralisierung von Rechenzentren. Hier ist für Redundanz zu sorgen, damit bei einer Störung nicht große Teile der gesamten IT-Infrastruktur des Bundes betroffen und gestört sind sowie deren Funktions- und Ausfallsicherheit gewährleistet wird.

8. *Wie wettbewerbsfähig sind dabei europäische und nationale Eigenlösungen gegenüber den Fertiglösungen der weltweit agierenden IT-Konzerne? 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 Frage einer Wettbewerbsfähigkeit ist nicht pauschal zu beantworten und stark abhängig von der konkreten Fallgestaltung, welche bspw. wieder von der Kritikalität des Dienstes, der Sensibilität der zugehörigen Daten und des Schutzbedarfs und ähnlichem abhängt.

Nimmt man die aktuellen IT-Lösungen von Großkonzernen als Vorbild werden z. B. unkritische Massenfunktionen gerne auf die Cloud-Angebote der weltweit agierenden IT Unternehmen ausgelagert, während für kritische oder unter einem besonders starken Datenschutz zu erbringende Funktionen in Eigenleistung erbracht und in gesonderten Datencentern vorgehalten werden. Ebenso relevant ist die Frage, inwieweit ein Dienst überhaupt sinnvoll als Clouddienst erbracht werden kann oder ob etwa im Rahmen einer aktuellen Entwicklung bereits eine moderne, verteilte Stack-Lösung (d.h. eine teils in Public Cloud, teils in Private Cloud, teils lokal in mehreren Instanzen lauffähige Softwarelösung) realisiert werden kann.

Um Risiken besser verteilen und streuen zu können sind wie in Frage 7 bereits aufgeworfen divers aufgebaute Netze im Sinne von Komponenten verschiedener Hersteller zu verwenden, ausreichende Redundanzen herzustellen und Monokulturen zu vermeiden. In TK-Netzen mit Luftschnittstelle (OTA) ist die Transportverschlüsselung ein geeignetes Mittel, um bessere Sicherheit der Kommunikation zu gewährleisten und in Deutschland durchweg gängige Praxis. Für Anbieter von Telemediendiensten bietet sich zudem eine Ende-zu-Ende Verschlüsselung zumindest zwischen Kunden und Anbieter an, zumindest in den Fällen, bei denen keine vollständige Ende-zu-Ende Verschlüsselung sinnvoll ist.

Sinnvoll im Bezug auf ein Haftungsregime könnte sein, wenn sich Hersteller bereit erklärten, über eine ihrer europäischen Niederlassungen einen Vertrag mit dem Netzbetreiber abzuschließen. Die Effektivität von Zertifizierungen ist eher kritisch zu bewerten, da auch durch diese nicht ausgeschlossen werden kann, dass die eingesetzten Systeme Sicherheitslücken oder Fehler aufweisen. Auch besteht die Möglichkeit, dass auch bei der Zertifizierung eine bewusst

implementierte Backdoor, unabhängig vom wem, im Zweifelsfall nicht erkannt oder im Extremfall einem nützlichen Dienst zugeordnet würde (Dual Use). Die Zertifizierung sämtlicher Updates und Ergänzungen stellt zudem einen enormen organisatorischen Aufwand dar, der die Implementierung obstruiert und sowohl für die Zertifizierungsstellen und staatlichen Behörden als auch für die Betreiber der Systeme einen enormen organisatorischen Aufwand darstellt. Entsprechende Maßgaben sollten daher nur in einem eng begrenzten Bereich verfolgt und deren Praktikabilität evaluiert werden.

Insbesondere vor dem Hintergrund, dass ein erheblicher Datenabfluss aus den Netzen der Telekommunikationsanbieter in der Regel durch diese erkenn- und feststellbar ist und nur mit Duldung des Anbieters über einen längeren Zeitraum Bestand haben wird, ist die Frage einer erzwungenen Kooperation eines Herstellers zur Ausleitung von Daten aus Netzen Dritter eher theoretischer Natur. Das Konzept einer unbemerkten, massenhaften Ausleitung von Inhaltsdaten durch Softwarelücken fußt insofern auf keiner realistischen Annahme der Gegebenheiten im Netzbetrieb.

Derartige Ausleitungen erfolgen zumeist auf Basis von Ausleitungsanordnungen der Behörden über spezielle Schnittstellen. International sind diese durch MLATs oder Instrumente wir die EIO im Gebiet der EU normiert. Eine heimliche Nutzung und Missbrauch dieser Funktionen sollte bereits heute durch ein geeignetes IDS-System des Betreibers in der Praxis ausgeschlossen 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 sind NoSpy-Abkommen für die Förderung des gegenseitigen Vertrauens auf politischer und diplomatischer Ebene sinnvoll. Ihre Wirksamkeit ist jedoch aufgrund der Natur geheim- bzw. nachrichtendienstlicher Aktivitäten und der Volatilität politischer Strukturen kritisch zu beleuchten.

   Fraglich bleibt jedenfalls, inwiefern zwischenstaatliche Verträge oder Verträge zwischen einem Hersteller und einem Staat tatsächlich

praktische Auswirkungen auf die Sicherheit eines TK-Netzes eines heute zumeist multinational aufgestellten Betreibers im konkreten Einzelfall haben können. Insbesondere für den privaten Sektor sind Konformitätsprüfungen bzgl. der Vertrauenswürdigkeit von Zulieferern sowie eine Prüfung der Lösungen auf Sicherheitsverletzung jedenfalls weiterhin notwendig und sinnvoll.

Insbesondere bei einer sehr niedrigen Anzahl und Auswahl potentieller Zulieferer von Lösungen führt eine Abschottung im Sinne des Ausschlusses eines einzelnen oder gar mehrerer Hersteller zu einer höheren Berechenbarkeit des Netzaufbaus und - ähnlich wie bei einer Monokultur - schlägt sich ein Fehler in Komponenten eines Herstellers gravierender nieder, je mehr Komponenten von ihm verbaut sind. Dies gilt für alle Hersteller unabhängig von ihrem Sitzland.

Zudem ist der Ausschluss eines einzelnen Herstellers derzeit auch aus kartellrechtlicher Sicht problematisch. Hier bedürfte es konkreter Nachweise über tatsächliche Sicherheitsrisiken oder einer Verwicklung des Herstellers in rechtswidrige oder nachrichten- bzw. geheimdienstliche Operationen für eine „fremde Macht“ analog zu §§94ff StGB. Die bloße Unterstellung einer möglichen Kooperation dürfte hier keinen Bestand haben.

Eine Abschottung gegenüber einzelnen Komponenten bzw. deren Lieferanten wäre außerdem nur begrenzt wirksam. In einem solchen Szenario wäre eine Verbesserung der Sicherheit nur im Falle einer vollständigen Kontrolle über alle Komponenten und Infrastrukturelemente des vollständigen Übertragungsweges (Privates Netz) zu erreichen. Für alle anderen Fälle – d.h. auch für die Nutzung öffentlicher Netze – sollte unter Sicherheitsaspekten theoretisch von einem potentiell kompromittierten Übertragungsweg als Szenario ausgegangen werden und ein Schutz der übertragenen Daten durch geeignete Ende-zu-Ende-Verschlüsselungsmethoden sicherzustellen. Dies wird als Schutz gegen „Man in the Middle“-Attacken bezeichnet.

Dieses Szenario ist aber keineswegs neu. Es wurde beispielsweise historisch auch bei Nutzung des Analog-, ISDN- oder Datex-Netzes der Deutschen Bundespost erwartet. Die Annahme, das Netz sei unsicher, ist eine grundlegende, notwendige Annahme für jegliches Lösungsdesign im ITK-Bereich und regelmäßig geübte Praxis in jeweiligen Unternehmensbereichen.

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 USCloud-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?*

    Das Projekt GAIA-X zeigt einen möglichen Weg auf, vertrauenswürdige Infrastrukturen auf Basis gemeinsamer Standards zu schaffen. eco unterstützt daher das Konzept von GAIA-X. Der durch GAIA-X verfolgte föderierte Ansatz ermöglicht dezentrale Datenvorhaltung, was den Effekt eines für einen Datenzugriff durch außereuropäische Behörden schwieriger gestaltet. Die zentrale Herausforderung bei der weiteren Entwicklung und Ausgestaltung von GAIA-X ist dabei weniger der Umgang mit amerikanischen Anbietern und deren rechtlichen Rahmenbedingungen, sondern insbesondere auch die europäische Politik, die momentan durch die Europäische Kommission und den Rat mit dem e-Evidence-Entwurf und den Beratungen des Europarats im Rahmen der „Budapest Convention on Cybercrime“ aufzeigt, das das Thema des „grenzübergreifenden Datenzugriffs“ ohne ausreichende Gewährleistung von Bürgerrechten und Sicherheitsstandards kein solitär amerikanisches Problem ist.

    Für die Betreiber ist die Situation derzeit paradox: Besteht die Möglichkeit einer Kompromittierbarkeit durch staatliche Akteure einer fremden Macht sollen diese „Lücken“ geschlossen werden, oder Garantien dafür abgegeben werden, dass sie nicht bestehen. Sind die Produkte hingegen sicher, sollen Zugriffsmöglichkeiten auf die Rohdaten der Kommunikation unter Umgehung aller Schutzmaßnahmen für staatliche Akteure geschaffen werden, welche dann aufgrund der Vielzahl von Ersuchen ohne die rechtsstaatlich gebotene Kontrolle des Ziellandes genutzt werden sollen.

    Das in der Realität bereits bestehende Problem eines sanktionierten unkontrollierten Datenabflusses an Drittstaaten wie beispielsweise im Rahmen von E-Evidence, Cloud Act oder Budapest Convention vorgesehen, übertrifft in seiner Quantität signifikant den durch etwaige Kooperationsvereinbarungen hypothetisch angenommenen.

Zur Sicherung von Daten in Kommunikationsnetzen wird auf die Antworten zu den Fragen 8 und 9 verwiesen.

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

    Mindeststandards mit Konformitätskennzeichnung können dabei unterstützen, grundlegende Sicherheitsfunktionen in IT-Systemen zu implementieren und das Bewusstsein auf Anwender-, Hersteller- und Entwicklerseite für Anforderungen an IT-Sicherheit zu sensibilisieren.

    Eine Dynamisierung von Mindeststandards sollte jedoch mit Bedacht betrieben und diese Standards weiterhin klar definiert werden, da sie andernfalls auf eine Stand-der-Technik-Regelung hinauslaufen könnte, die sich unter Umständen negativ auf das Angebot und den Betrieb von IT-Systemen auswirken könnte.

    Offene Standards erleichtern den Austausch von Daten und verbessern deren Lesbarkeit. Dies mag bei der Zusammenarbeit von Behörden oder der Interaktion von Staat und Bürger durchaus sinnvoll sein, erleichtert aber umgekehrt unbefugten Dritten ebenfalls die Ausleitung und Analyse dieser Daten. Open Source und Open Hardware sind daher in diesem Kontext ebenfalls als ambivalent zu betrachten: Ein offener Quellcode bzw. öffentlich bekannte Schaltpläne können einen Beitrag liefern, Sicherheitslücken zu entdecken und schnell zu schließen. Allerdings könnten sie – abhängig vom Entdecker – eben auch missbraucht werden. Grundsätzlich davon auszugehen, dass die Vorteile von Open Source und Open Hardware die Nachteile langfristig überwiegen.

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?*

    Ein IT-Gütesiegel im Sinne einer Konformitätskennzeichnung mit bestimmten Sicherheitsstandards kann Nutzern bei der Orientierung im

Markt helfen. Derartige Gütesiegel müssten jedoch einen zeitlichen Faktor beinhalten, um dem Nutzer nicht das trügerischen Gefühl einer dauerhaften Sicherheit zu vermitteln (beispielsweise im Stil einer Prüfplakette mit Ablaufdatum „TÜV-Plakette“).

Insgesamt bedarf es hier allerdings eines Bewusstseins für die Konsequenzen und Maßgaben für eine sichere Nutzung und den Einsatz von IT. Dies erscheint zumindest momentan sowohl bei der Bevölkerung als auch bei den Unternehmen noch nicht in ausreichendem Maße vorhanden und ausbaufähig zu sein. Es stellt sich zudem die Frage, inwieweit eine (hoheitliche) Zertifizierung von IT-Produkten insbesondere in einer servicegetriebenen IT-Landschaft (SaaS / PaaS) überhaupt sinnvoll gestaltbar ist (vgl. Antwort auf Frage 8).

Eine Überprüfbarkeit auf Schwachstellen und Backdoors ist bei IT-Systemen grundsätzlich nicht vollständig leistbar. Das liegt in der Natur des für Menschen nicht nachvollziehbaren Maschinencodes, einer fehlenden Beweisbarkeit vieler Algorithmen sowie der Co-Abhängigkeit von Softwarelösungen untereinander. Daher wäre eine durchgängige, volle Kontrolle von Systemen durch sämtliche Aspekte der Lieferkette nach heutigem Kenntnisstand realistisch nicht möglich.

Am ehesten hätten die Anbieter der entsprechenden Systeme oder Produkte einen Überblick darüber, welche Komponenten von Ihnen angeboten werden und es ist davon auszugehen, dass sie auch am ehesten die von ihnen betriebenen bzw. angebotenen Systeme am besten kennen. Externe oder staatliche Auditoren müssten sich in diese Systeme und Produkte und deren komplexes Zusammenspiel in den unterschiedlichsten Anwendungsszenarien zunächst eingehend einarbeiten, um auch nur ansatzweise eine rudimentäre Einschätzung und Bewertung vornehmen zu können. Auf Grund dieses komplexen Zusammenspiels, dass Tests von Komponenten außerhalb des Netzes, in dem sie verwendet werden soll, auch nur sehr bedingte Aussagekraft haben.

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

Grundsätzlich sind Sicherheitslücken bzw. deren umgehende Beseitigung von großer Relevanz und elementar für die IT-Sicherheit. Der Handel mit Sicherheitslücken wirkt sich ebenfalls auf die IT-Sicherheit aus, muss jedoch differenzierter betrachtet werden, da damit sowohl positive als auch negative Auswirkungen und Effekte verbunden sind.

Der Handel mit Sicherheitslücken bzw. im eigentlichen Sinne der Ankauf kann sich für Anbieter von IT als sinnvoll darstellen, wenn bspw. Hersteller mit sog. Bug-Bounty-Programmen Prämien für eine Meldung von Sicherheitslücken ausloben und damit den Herstellern eine Erkennung bislang nicht bekannter und umgehende Beseitigung ermöglichen.

Darüber hinaus ist der Handel mit Sicherheitslücken gleichzeitig auch ein Risiko für die Anbieter von IT-Produkten wenn, wie derzeit gegeben, durch einen Verkauf neu entdeckter Sicherheitslücken an staatliche Stellen, an Anbieter von „dual use“ Software oder gar ein Angebot auf dem Grau- oder Schwarzmarkt für derartige Informationen ein Vielfaches der Erträge aus Bug Bounty Programmen erzielt werden kann und Sicherheitslücken in Folge nicht oder nicht zeitnah gemeldet werden. Eine umgehende Beseitigung von Sicherheitslücken wird dadurch erschwert und verhindert.

In diesem Kontext möchten wir auf einen weiteren kritisch zu beurteilenden Aspekt bei der Veröffentlichung von Sicherheitslücken hinweisen. Teilweise wird von Unternehmen versucht, durch rechtliche Maßnahmen die Veröffentlichung von Sicherheitslücken in ihren Produkten zu verhindern, ohne dass zugleich unternehmensseitig geeignete Maßnahmen ergriffen werden um diese Schwachstellen selbst zu zuschließen oder zu beseitigen. Dieses rigorose Vorgehen veranlasst selbst renommierte Sicherheitsforscher regelmäßig dazu, aus Angst vor juristischen Auseinandersetzungen und drakonischen Forderungen von einer Veröffentlichung von Sicherheitslücken Abstand zu nehmen.

Eine Meldepflicht für staatliche Stellen, die Sicherheitslücken den Anbietern oder Betreibern mitteilen müssen, ist sinnvoll und erforderlich. Hierdurch wird das Vertrauen sowohl in den Staat als auch in digitale Technologien gefördert. Für die digitalisierte Gesellschaft ist es zwingend notwendig, dass alle bekannten Sicherheitslücken unmittelbar und ohne zeitliche Verzögerung geschlossen werden. Jede Stelle – sei

sie staatlich oder privat – welche Sicherheitslücken bewusst zu Förderung eigener Interessen zurückhält und nicht zu einer unmittelbaren Schließung derselben beiträgt, gefährdet die Sicherheit aller.

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 IT-Grundrecht ist in seiner vorliegenden Fassung mit entsprechender Gesetzgebung abgesichert und konkretisiert. Zusätzlich bestehende Rechtsprechung gibt weitere Orientierung dahingehend, wie das Recht auf informationelle Selbstbestimmung, nach dem sich das IT-Grundrecht richtet, ausgelegt werden sollte und in welchem Verhältnis es zu anderen zentralen Grundrechten steht. Aus dem Grundrecht und der daraus abgeleiteten Gesetzgebung ergeben sich die bestehenden Sorgfaltspflichten, wie sie bspw. im IT-Sicherheitsgesetz niedergelegt sind.

Zu Diskutieren wäre eine aus dem IT-Grundrecht und dem IT-Sicherheitsgesetz abgeleitete Pflicht zur Nachbesserung von Software bei bekannt werden von Sicherheitslücken.

Hierbei sollte auch erörtert werden, inwieweit die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auch eine Verpflichtung zum Betrieb sicherer IT-Systeme für den Einzelnen abgeleitet werden kann bzw. abgeleitet werden muss. Mit dem Recht auf diese Gewährleistung geht aber auch Pflicht des Einzelnen einher, selbst auch etwas dafür zu tun.

Daneben sollte auch debattiert werden, inwieweit der Staat zukünftig seine aus dem IT-Grundrecht erwachsenden Schutzpflichten stärker bei seinen gesetzgeberischen Aktivitäten berücksichtigen sollte und inwieweit die Schutzziele für Bürger und Wirtschaft durch gegenläufige sicherheitspolitische Aktivitäten und Maßnahmen (z. B. Bundestrojaner, Vorratsdatenspeicherung, BKA-Gesetz, etc.) konterkariert werden.

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?*

    Bei den bekannten Maßnahmen wie Bundestrojaner, Vorratsdatenspeicherung, Ausleitung bzw. Abschöpfen von Kommunikation/ Ghost Receiver findet immer ein Eingriff in die digitale Souveränität des Bürgers und weiterer an der Kommunikation Beteiligter statt. Dieser Umstand lässt sich durch keine bekannte Technologie beseitigen.

    Zugriffe auf solche Daten erfolgen nicht zwingend immer via IT. Es gibt vergleichbare Fälle der Einschränkung persönlicher Freiheitsrechte durch staatliche Stellen (zum Beispiel: Unverletzlichkeit der Wohnung, Bankgeheimnis, etc.). Diese sind umfassend rechtstattlich normiert und einer richterlichen Kontrolle unterworfen und wirken in die Zukunft. Staatliche Eingriffe in die digitale Souveränität, die sich in diesem Rahmen bewegen, sind daher in der Regel vertretbar.

    Sehr problematisch sind jedoch staatliche Ansätze wie die heimliche Ausleitung gespeicherter Daten (z.B. Clouddaten, Festplatten, Bilddatenbanken, etc.), Ausleitungen an Drittstaaten ohne geeignete rechtliche Abwehrmaßnahmen für Bürgerinnen und Bürger. Für diese Eingriffe gibt es derzeit auch kein Pendant, da sie, anders als bspw. Durchsuchungen ohne Kenntnis der Zielpersonen oder weiterer Betroffener durchgeführt werden. Darüber hinaus sind alle staatlichen Maßnahmen und Anordnungen, welche in die Vergangenheit wirken (VDS) oder eine Ermittlung erst auslösen (automatische Weitergabe von Verdachtsmomenten, Meldepflichten etc.), äußerst problematisch.

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

    Die Verantwortung des Bundes für die Gewährleistung von IT-Sicherheit muss dringend gestärkt werden. Eine Meldepflicht von entdeckten IT-Sicherheitslücken an die Hersteller und Entwickler ist unabdingbar, ebenso wie eine (anonymisierte) Weitergabe erkannter Lücken an

betroffene Betreiber. Darüber hinaus sollte das Verhältnis von ZITIS und BSI klargestellt werden.

Wünschenswert wäre zumindest eine abstrakte Verpflichtung aller Akteure auf eine stringente, systematische Erhöhung der IT-Sicherheit und somit auch der digitalen Souveränität von Bürgern, Unternehmen und Staat. Eine derartige Verpflichtung sollte sich zudem nicht alleine auf die Betreiber kritischer Infrastrukturen erstrecken, sondern vielmehr – analog zum Straßenverkehr - alle Teilnehmer auf ein Mindestmaß an Regeln und den Betrieb sicherer Systeme verpflichten.

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?*

Die derzeitige Einordnung des BSI unter die Fach- und Rechtsaufsicht des BMI ist aufgrund der weiteren Aufgaben des BMI (BfV, BKA, ZITIS) und deren entsprechend anders gelagerten Interessen nicht unproblematisch.

Die Unabhängigkeit des BSI ähnlich wie die des BfDI hätte den Vorteil, dass das Amt über jeden bestehenden Zweifel erhaben als die Institution für die Stärkung der IT-Sicherheit gesehen werden könnte. Dies gilt auch im Kontext der Verhältnisse bei der Zusammenarbeit im Nationalem Cyberabwehr-Zentrum NCAZ im Verbund mit dem BfV.

Inwieweit sich eine Unabhängigkeit des BSI als problematisch darstellen könnte, kann aus unserer Perspektive nicht beurteilt werden.

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?*

Je weniger komplex, konsistent und normenklar sowohl eine umfassende IT-Sicherheitsarchitektur ist und vor allem die IT-

Sicherheitsregulierung ist, desto einfacher haben es Unternehmen, sich rechtskonform im europäischen digitalen Binnenmarkt zu bewegen.

Daher sollten harmonisierten europäischen Vorgaben und Strukturen immer Vorrang vor nationalen gegeben werden. Darüber hinaus bergen nationale Alleingänge und Regulierung das Risiko der Isolierung in sich – ein Umstand, der eine Herausforderung für Unternehmen darstellt und sich nachteilig auf IT-Unternehmen auswirken kann, wenn sie ihre Dienste und Produkte in verschiedenen und entsprechend unterschiedlich regulierten Märkten rechtskonform anbieten wollen.

Die Kompetenzen nationaler Behörden oder jene der Bundesländer sollten dementsprechend im Einklang mit europäischer Regulierung mandatiert sein.

Allerdings bleibt festzustellen, dass die Zuständigkeiten und Aufgaben im Rahmen der deutschen Cyber-Sicherheitsarchitektur derzeit gerade nicht klar dargelegt sind und sich die Aufgaben und Verantwortungsbereiche der Akteure zu einer unüberschaubaren Vielzahl komplexer Verbindungen entwickelt hat.

Aktuell wurde diese Komplexität in einer Arbeit von Dr. Sven Herpig und Kira Messing der Stiftung neue Verantwortung aus November 2019 dargestellt, welche die Akteure und Zuständigkeiten in der deutschen Cybersicherheitspolitik untersucht haben. Es bedarf keiner weiteren Erläuterung, dass allein bedingt durch die Anzahl der Akteure, deren Zuständigkeiten und Aufgabenbereiche ein effizientes Arbeiten nahezu unmöglich wird. Eine deutliche Verschlankung der Architektur mit klar definierten Zuständigkeiten und Ansprechpartnern für die Akteure aus der Wirtschaft erscheint daher dringend erforderlich.

Darüber hinausgehende Vorschläge zur Verbesserungen für die Arbeit des BSI können über die in Antwort 16 und 17 getroffenen Aussagen hinaus aus unserer Perspektive nicht vorgeschlagen 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?

Ein „Hackback“ ist politisch problematisch, da vor einer Ausführung der einzelnen Aktionen zumeist unklar bleibt, gegen welche Systeme sich die Attacken konkret richten und so unter Umständen nicht intendiert am Zielort relevante Infrastrukturen schädigen können. Die Abgrenzung entsprechender Maßnahmen von einem kriegerischen Akt ist dadurch problematisch. Zudem erhöht eine „Hackback“ Politik, bei der Server oder IT-Systeme in anderen Staaten ausgeschaltet werden, die Angreifbarkeit der eigenen Systeme und Infrastrukturen, da diese dadurch für angreifende Akteure oder Hackbackteams anderer Staaten sichtbarer und relevanter werden.

Völlig unklar bleibt auch, wie sich ein staatlicher Akteur gegenüber einer Zielperson oder einem Zielakteur konkret verhalten und offenbaren soll. Dies müsste zur Abgrenzung von Aktivitäten anderer Akteure, bspw. von Cyber-Kriminellen, und der Einhaltung des Rechtsweges erfolgen.

Vollständig abzulehnen sind Forderungen nach einem „privaten Anspruch auf Cyber-Verteidigung“, wie dies beispielsweise durch private Gruppen aus den USA gefordert wurde[2]. Hier werden – teils durch große Unternehmen – aktive Gegenmaßnahmen in Form von Hack-Backs als zulässige Reaktion auf Angriffe gegen eigene Infrastrukturen gesehen, der Sitz des potentiellen Angreifers spielt in dieser Betrachtung keine Rolle.

Ein derartiges Vorgehen auch nur zu tolerieren birgt in einem internationalen Medium wie dem Internet das Risiko unüberschaubarer Zustände, in welchen selbst die Rollen von Angreifern und Verteidigern endgültig nicht mehr zuzuordnen sind. Ein „privater Anspruch auf Cyberverteidigung“ ist daher – insbesondere international – strikt abzulehnen. Dies sollte daher auch eine klare Position der deutschen Cyber-Sicherheits- und Außenpolitik sein.

Was den Forschungsstand für die Attribution von komplexen IT-Angriffen anbetrifft, ist Deutschland grundsätzlich gut aufgestellt – sofern eine diesbezügliche Attribution überhaupt rechtssicher erfolgen kann, da

[2] **Siehe hierzu https://www.lawfareblog.com/hackback-back-assessing-active-cyber-defense-certainty-act**

eine Einschätzung in der Regel nur aus einem Vergleich mit bekannten Quellen erfolgen kann. Wem eher was zugeordnet/attribuiert wird, ist öffentlich bekannt. Dies wird auch gerne als Tarnung benutzt, vor kurzem wohl russische Hacker getarnt als iranische. Wichtig wäre es, entsprechendes Fachwissen z.B. durch Schulungen besser zu verbreiten, um im Falle einer Cyberattacke die notwendigen Beweismittel zu sichern, deren Analyse zu ermöglichen und nicht schlimmstenfalls alle Spuren der Angreifer durch überstürzte Maßnahmen zu vernichten. Hierzu gehört auch, das Angreifer nicht durch ungeeignete Maßnahmen über eingeleitete Untersuchungen alarmiert werden, ohne gleichzeitig die vollständige Kontrolle über das System bereits wiedererlangt zu haben. Mehr Forschungsmittel sind in diesem Bereich grundsätzlich sinnvoll.

Die Debatte um eingebaute Hintertüren (Backdoors), eine verdeckte Teilnahme an der Kommunikation (Ghost Protocol, Frontdoor) sowie generell über die Ausleitung unverschlüsselter Kommunikation an Quelle oder Ziel ist sehr problematisch. Allen Ansätzen gemeinsam ist die Schwächung der Sicherheit und Integrität der angebotenen Dienste. Dies schadet allen Anwendern und Nutzern, den Diensten und ihren Anbietern maßgeblich. Das Wissen über die Möglichkeit der Ausspähung privater Kommunikation durch Dritte höhlt das Vertrauen in digitale Technologien und den Staat als Garant für Sicherheit aus. Darüber hinaus sind sie im Vergleich zur gewünschten Eingriffstiefe absolut unverhältnismäßig.

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

Messengerdienste, die zur Interoperabilität verpflichtet werden, stehen vor der Herausforderung, ihre Angebote so zu gestalten, dass sie diensteübergreifend sicher sind und bspw. auch eine Verschlüsselung diensteübergreifend zuverlässig funktioniert.

In einem solchen Szenario wechselt die prinzipielle Herausforderung von einer sicheren Ende-zu-Ende Verschlüsselung zu der Kernfrage der sicheren, diensteübergreifenden Nutzerauthentifizierung und eines anbieterübergreifenden Schlüsselmanagements. Sofern diese Elemente nicht ebenfalls anbieterübergreifend gewährleistet werden können, ist eine Entschlüsselung an der Netzwerkgrenze für eine diensteübergreifende Interoperabilität zwingend erforderlich. Dies würde

eine signifikante Minderung der Sicherheit gegenüber dem derzeitigen Stand der Technik darstellen, welche nicht nachvollziehbar ist und nicht im Interesse der Verbraucher liegen kann.

Allgemein ist davon auszugehen, dass sich durch eine Verpflichtung zur Interoperabilität von Messengern die Verschlüsselungstechnologien sowie die Möglichkeiten zum Schlüsselaustausch konzentrieren, reduzieren und weniger innovativ sein werden. Die bestehende marktliche Dynamik bei der Entwicklung von entsprechend sicheren Technologien könnte damit konterkariert und ausgehebelt werden. Inwieweit sich überhaupt noch verschiedene Messenger und Dienste von unterschiedlichen Anbietern in einem solchen Szenario als sinnvoll darstellen, ist fraglich. Die Forderung nach einer Interoperabilität von verschlüsselten Messengerdiensten sollte vor diesem Hintergrund daher kritisch hinterfragt werden.

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?*

Die Bereitstellung von Mitteln und die Ausweitung entsprechender Förderung für Forschung und Entwicklung für IT-Sicherheit ist sinnvoll, insbesondere wenn die Ergebnisse – anders als im Rahmen privater Forschung – von der Allgemeinheit zur Absicherung ihrer ITK-Systeme verwendet werden können. Grundsätzlich bleibt aber auch festzuhalten, dass die bestehenden Strukturen insbesondere in Deutschland durchaus positiv sind. Das jüngst im Bundestag verabschiedete Gesetz zur steuerlichen Förderung von Forschung und Entwicklung (Forschungszulagengesetz - FZulG) stärkt zudem die betriebliche Forschung – ein Faktor, der insbesondere im marktgetriebenen IT-Umfeld wichtig ist. Wichtig ist zudem, dass zu Querschnittstechnologien wie Künstlicher Intelligenz oder aufkommenden technologischen Herausforderungen wie Quantensicherheit bereits heute geforscht wird, und dass gemeinsame Standards von der Branche definiert werden – grenzübergreifend.

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?

Die Stärkung und Ausbildung von praktischem und akademischem Wissen über IT-Sicherheit ist zentral für die digitale Souveränität in Deutschland – auch über die Fachkräftedebatte hinaus. Erreicht werden kann dies am ehesten durch angemessene, altersgerechte und fachbezogene Ausbildung von IT-Kompetenzen in Schule, Ausbildung, Hochschule und durch Schulungen in Unternehmen. Das setzt natürlich entsprechende Kenntnisse der jeweiligen Lehrkräfte etc. voraus.

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?*

Blockchain als Querschnittstechnologie kann in bestimmten Bereichen helfen, Authentizität von Daten nachzuweisen. Vor diesem Hintergrund werden die Möglichkeiten der Blockchaintechnologie in allen Anwendungsbereichen als positiv gesehen, welche ein derartiges System verteilten Vertrauens benötigen oder durch eine verteilte, massiv redundante Architektur profitieren. Die langfristig datenschutzkonforme Umsetzung einer solchen Technologie hingegen ist durchaus eine Herausforderung, auch ist die Zukunftssicherheit der heute verwendeten Systeme mit Hinblick auf die Authentizität für längere Zeiträume kritisch zu evaluieren.

Auch Quantencomputing wird im Bereich der Verschlüsselung nichts an der grundlegenden Herausforderung ändern, sichere Schlüssel auf der einen Seite zu erzeugen, die auf der anderen Seite notfalls mittels einer Brute Force Attacke geknackt werden könnten. Wichtig ist jedoch, diese Herausforderung bereits heute perspektivisch auf sogenannte „quantensichere“ Verfahren zu erweitern, d.h. zu berücksichtigen,

welche auch durch Quantencomputer nicht auf einfache Operationen reduziert werden können. Hierbei ist der Zeithorizont elementar. Beispielsweise werden heutzutage amtliche Ausweise mit einer Laufzeit von 10 Jahren ausgegeben, welche nicht nachträglich nach Ausgabe um neue Verschlüsselungserfahren erweitert werden können und welche nicht quantensicher sind und bereits absehbar ist, dass mit einer Verfügbarkeit der entsprechenden Geräte innerhalb der nächsten 5-8 Jahre zu rechnen.

Gleiches gilt für Unternehmen und Verwaltungen: Unabhängig von der Laufzeit neuer Infrastruktur sollten bereits jetzt angesichts der zeitlichen Planungs- und Realisierungshorizonte alle Projekte das Aufkommen von Quantencomputern und die sich hieraus ergebenden Herausforderungen berücksichtigen.

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

    Wie bereits zuvor dargelegt, ist die Veröffentlichung von Quellcodes ambivalent. Eine Veröffentlichung kann hilfreich sein, allerdings auch Probleme mit sich bringen. Inwieweit Anwenderinnen und Nutzer von einer Veröffentlichung profitieren, hängt maßgeblich von deren Kenntnissen in der jeweiligen Programmiersprache ab.

    Für gewisse Klassen von Algorithmen, welche einen unmittelbaren Bezug zur IT-Sicherheit haben, sollte eine Veröffentlichung zur unabhängigen Evaluation – ggf. eingeschränkt auf Behörden oder neutrale Sachverständige - vorgesehen werden, die gilt insbesondere für kritische Aspekte wie z.B. Crypto Algorithmen und ähnliches.

    Grundsätzlich bedarf es allerdings einer breiten Diskussion darüber, für welche Produkte und Dienstleistungen es welche Schutz- und Auditierungsverfahren bedarf.

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?*

Die Problematik von Dual-Use-Funktionen im IT-Bereich ist, das oftmals einzelne Elemente zu einer Software verbaut werden, deren Einsatzzweck nicht dem von den Entwicklern intendierten Einsatzzweck entspricht. So können bspw. Screensharing-Programmen im E-Learning oder im Supportbereich sinnvoll sein, gleichzeitig aber auch zur Überwachung von Mitarbeitern eingesetzt werden. Dieses zentrale Problem kann auf Entwicklungsebene nicht behoben werden.

Andere Softwareprodukte, wie beispielsweise sogenannte Penetration Testing Software, sind für die Arbeit von Sicherheitsfachleuten elementar und notwendig. Diese können aber ebenfalls von Cyberkriminellen eingesetzt werden. Eine Haftung der Entwickler für diese zumeist als Open Source veröffentlichte Software würde zu einer Einstellung der Entwicklung in diesem Bereich führen und so mittelfristig der Verbesserung von IT Sicherheit schaden und das Testen der Sicherheit von Systemen und dem Auffinden von Schwachstellen erschweren.

Haftungsregeln für Anbieter von Software, welche sich explizit an staatliche Akteure wendet, sind sinnvoll um eine Kooperation im Bereich der Strafverfolgung zu ermöglichen. Für solche Bausteine sollten daher im Zweifel im Falle eines Exports an bestimmte Regierungen und politischen Regime eine Genehmigungspflicht gelten, und ein Haftungs- und/oder Erstattungsregelung greifen.

Über eco
eco - Verband der Internetwirtschaft e.V. ist Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit mehr als 1.100 Mitgliedsunternehmen. Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunter-nehmen. eco ist der größte nationale Internet-Service-Provider-Verband Europas.