Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)076

CISPA | Stuhlsatzenhaus 5 | D-66123 Saarbrücken

Ausschuss Digitale Agenda
z. H. Cornelia Schultz
Sekretariat PA 23

Deutscher Bundestag
Platz der Republik 1
11011 Berlin

Ninja Marnau
Senior Researcher

CISPA Helmholtz Center for Information Security
Stuhlsatzenhaus 5, 66123 Saarbrücken | Germany

TEL +49 681 302-71943
FAX +46 681 302-71942
E-MAIL marnau@cispa.saarland
WEB www.cispa.saarland

Saarbrücken, 05.12.19

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

Sehr geehrte Mitglieder des Ausschusses Digitale Agenda,

ich bedanke mich herzlich für die Einladung zur Anhörung und beantworte Ihnen im Folgenden die übersandten Fragen.
Meine Antworten und Vorschläge beruhen teilweise auf Erkenntnissen aus dem noch laufenden Forschungsprojekt „IT-Sicherheitsregulierung” im Auftrag des BSI, dass ich gemeinsam mit Prof. Dirk Heckmann (TU München) und Prof. Thomas Riehm (Universität Passau) durchführe.

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?*

Sowohl Deutschland als auch die EU sind schlecht aufgestellt im Hinblick auf die Digitale Souveränität. Verwaltung und Industrie sind zum Großteil abhängig von Soft- und Hardware aus dem Nicht-EU-Ausland. Europa und Deutschland haben kaum noch eigene international konkurrenzfähige Soft- und Hardwareproduzenten für IT-Systeme. Die Verbesserung der digitalen Souveränität muss ein vorrangiges strategisches Ziel sein. Die Abhängigkeit von IT, der man mangels Überprüf- und Kontrollierbarkeit blind vertrauen muss, muss reduziert und das vorhandene Potenzial in Deutschland und Europa für Forschung und Entwicklung muss besser genutzt werden. Auch im Bereich der digitalen Bildung für die Bürger bestehen erhebliche Defizite.

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?

Der Gesetzgeber muss die Voraussetzungen schaffen, dass er die eingesetzte IT in ausreichendem Maße kontrollieren kann. Wichtig ist, tatsächlich regulativ sektorübergreifende Mindestanforderung an die IT-Sicherheit von Software und Hardware zu stellen, die in der EU bzw. In Deutschland vertrieben und eingesetzt werden.
Sinnvoll ist, diese generelle Anforderung durch ein EU IT-Sicherheitsgesetz (eine IT-Security Regulation in Ergänzung zum Cybersecurity Act) zu regeln. Zwar ist der deutsche Gesetzgeber nicht grundsätzlich daran gehindert, im Bereich der IT-Sicherheit nationale Regelungen als solche zu erlassen. Allerdings darf er sich nur in dem durch die EU-Rechtssetzung gesteckten Rahmen bewegen, unter Beachtung der Sperrwirkung, die von bestehender oder bevorstehender EU-Gesetzgebung ausgeht. Insofern eignet sich der Spielraum der nationalen Gesetzgebung eher dazu, ergänzende sektorale Anforderungen zu erlassen und vor allem auch IT-Sicherheit durch gezielte finanzielle Förderung und Bildungsinitiativen zu incentivieren. Nicht zu unterschätzen ist auch der Einfluss, den der Staat durch die eigene Vergabepraxis im Hinblick auf IT-Sicherheit ausüben kann.
Bürgerinnen und Bürger würden am ehesten durch zwei Aspekte in ihrer eigenen digitalen Souveränität unterstützt:

- Zum Ersten durch ein umfassendes Bildungsangebot im Hinblick auf informatisches Verständnis und IT-Kompetenz (von der Schule bis zur Erwachsenenbildung).
- Zum Zweiten durch verlässliche regulativ vorgegebene Mindestanforderungen für alle auf dem Markt erhältlichen IT-Produkte.

Diese Mindestanforderungen müssen dementsprechend auf die Mängelgewährleistungs- und Haftungspflichten der Hersteller und Verkäufer ausstrahlen und auch behördlich durchgesetzt werden können.

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?*

Die Verteidigung gegen staatliche Angreifer oder Angreifer mit vergleichbaren Ressourcen wie staatliche Angreifer ist extrem schwierig und technisch eine offene Forschungsfrage. Abschottung bis hin zur Netzabschaltung ist hier für einen demokratischen Rechtsstaat keine sinnvolle oder gangbare Lösung.

Eine sinnvolle proaktive Maßnahme für mehr digitale Souveränität in einer freien Netzarchitektur ist ein stärkeres Engagement Deutschlands im Thema Internet Governance. Einer der kritischsten Angriffspunkte der Internetinfrastruktur ist das Leiten von Datenverkehrs, konkret das BGP (Border Gateway Protocol). BGP-basierte Angriffe (BGP Hijacking, IP-Spoofing für Denial of Service-Angriffe, etc.) haben in den vergangen Jahren stark zugenommen und werden auch durch staatliche Akteure zur Manipulation des Internetverkehrs genutzt. Auch wenn die 2014 diskutierte Idee eines Schengen-Internets bereits infrastrukturell (aufgrund der Lage von Glasfaserkabeln, Knoten, etc.) nicht möglich ist, könnten Deutschland und die EU auf andere Weise darauf hinwirken, innerhalb der EU die Sicherheit des Routing-Systems zu erhöhen. Sie könnten europäische Netzbetreiber insbesondere darauf verpflichten, manipulationssicherere Verfahren des Routings wie BGPsec und Best Practice Empfehlungen gegen das Spoofing von IP-Adressen zu implementieren.

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

Die Vulnerabilität von Komponenten hängt nicht nur von ihrer eigenen Angriffsoberfläche ab, sondern auch von der Vernetzung. In komplexen vernetzten Systemen kann daher jede Komponente die Vulnerabilität aller anderen Komponenten beeinflussen. Im Hinblick auf den konkreten Handlungsbedarf verweise ich auf die Antworten zu Fragen 1. und 3.

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

/

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

Das Scheitern von Projekten zur Einführung von Open Source Produkten ist multikausal. Probleme ergeben sich im Hinblick auf:

- ein Unterschätzen der Kosten für die dauerhafte Anpassung und Support der Produkte;
- Fehlende Benutzbarkeit (Usability) und Komfort, den die Nutzer erwarten;
- Fehlende Kompatibilität mit anderen Produkten und dem umgebenden IT-Ökosystem.

Diese Problemfelder müssen von Beginn des Projekts an berücksichtigt und zusätzliche finanzielle und personelle Mittel eingesetzt werden. Darüber hinaus sollten Vergaberichtlinien und -verfahren so gestaltet werden, dass sie auch die gleichwertige Berücksichtigung von Open Source Software oder die Open Source Veröffentlichung öffentlich finanzierter IT-Produkte ermöglichen.
Auch im Hinblick auf eine Verwendung im Rahmen von Bundeswehr/BMVg ist es nicht der Fall, dass proprietäre Software generell mehr Sicherheit bieten würde. Gerade in diesem Bereich könnte die staatliche digitale Souveränität von der besseren Überprüfbarkeit und Kontrollierbarkeit quelloffener Software profitieren. In Einzelfällen kann es sinnvoll sein, die Nutzung von Open Source Software nicht transparent zu machen oder von einer Offenlegung des Codes abzusehen. Neben Aspekten der nationalen Sicherheit kommt als Grund auch der Schutz von geistigem Eigentum und Innovation in Betracht.

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?*

Zentralisierung und Bündelung ist im Hinblick auf die IT-Sicherheit ein zweischneidiges Schwert. Zwar lassen sich zentralisierte Systeme leichter warten, überwachen (im Sinne von Monitoring) und updaten, aber homogene und wenig diversifizierte Infrastrukturen erhöhen auch das Risiko dafür, dass immer das Gesamtsystem von Verwundbarkeiten und Ausfällen betroffen ist.
Um europäische Eigenlösungen für Schlüsseltechnologien (beispielsweise Herstellung von Hardwarekomponenten, ein europäisches Betriebssystem oder Browser) eine vergleichbare Wettbewerbsfähigkeit zu geben, bräuchte es tatsächlich eine mit der Gründung von Airbus vergleichbare finanzielle und politische Anstrengung.
Wichtiger ist aber die bereits verfügbaren Lösungen und existierende Technologien für IT-Sicherheit tatsächlich zum Einsatz zu bringen. Hier ist insbesondere die Gestaltung der Vergabe und die Projektbegleitung bei der IT-Konsolidierung sowie die Schulung der Mitarbeiter ausschlaggebend.

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?*

Zentral ist zunächst überhaupt generelle regulative Anforderungen an die IT-Sicherheit zu stellen. Derzeit ist die einzige generelle sektorübergreifende IT-Sicherheitsnorm der Art. 32 DSGVO, der aber eine andere Zielrichtung als IT-Sicherheit hat und auch nicht die Hersteller von IT-Komponenten verpflichtet. Durch eine Verpflichtung zu risikoadäquaten IT-Sicherheitsvorkehrungen könnten auch spezielle Risiken der Lieferkette adressiert werden. Unter den Zulieferen können einzelne Länder sein, die hinsichtlich Zusicherungen oder rechtlichen Bedingungen inadequäte Risiken implizieren. In Bereichen, in denen die Risiken als zu hoch eingeschätzt werden, wäre der EU-Hersteller oder Importeur dann verpflichtet, auf alternative und geeignete Quellen zuzugreifen oder andere Ausgleichsmaßnahmen zu treffen.
Diese qualitativen Anforderungen entfalten dann Wirksamkeit, wenn sie ins Mängelgewährleistungs-, Haftungs- und insbesondere Produkthaftungsrecht ausstrahlen. Auf dieses Weise können sie sowohl vertraglich, verbraucherrechtlich, wettbewerbsrechtlich als auch durch Aufsichtsbehörden durchgesetzt werden.
Zur Formalisierung der Risikoabschätzung und Unterstützung bei der Auswahl von IT-Sicherheitsmaßnahmen eignen sich Instrumente und Maßnahmen der Selbstregulierung. Um gezielt Lücken oder Qualitätsmängeln in der technischen Standardisierung zu begegnen sollte der Gesetzgeber gezielte Aufträge an Standardisierungsorganisationen vergeben (dieses Verfahren wird im EU-Produktsicherheitsrecht bereits seit Jahrzehnten eingesetzt). Die Beteiligung nationaler Unternehmen, Wissenschaftler und Vertreter der Zivilgesellschaft in den entsprechenden Standardisierungsgremien könnte durch finanzielle Förderung und Anforderungen in Forschungs- und Entwicklungsprojekten incentiviert werden.
Derartige EU-weite Marktzugangshürden für alle Anbieter auf dem EU-Binnenmarkt erscheinen erfolgversprechender als internationale Vereinbarungen.

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?*

Die Sicherheit, die eine No-Spy-Klausel bietet, ist nur begrenzt. Es ist eine vertraglich abgesicherte Absichtserklärung. Bei einer entdeckten Verletzung ergeben sich vertragliche Ansprüche, die dann noch international durchesetzt werden müssten.
Eine Konformitätsprüfung kann für komplexe Systeme selbst mit Hilfe von Testing und Analysetools nur stichprobenartig stattfinden. Auch Testierung, Zertifizierungen und Audits sind nur begrenzt aussagekräftig, abhängig von Prüfintervall und Prüfintensität. Unter Berücksichtigung der Kritikalität und Risikoeinschätzung kann der Ausschluss von Komponentenanbietern, bei denen ein signifikantes Spionagerisiko besteht, notwendig werden. Eine Trennung von Kern- und Zusatzkomponenten kritischer Infrastruktur kann abhängig vom Grad der Vernetzung (sie Antwort zu Frage 4) das Risiko nur bedingt mindern.

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?*

Ich befürworte die Bemühungen um die „Bundes-Cloud“ und „GAIA-X“. Beide Projekte zielen darauf ab, in Bereichen zentraler kritischer Infrastrukturen nationale bzw. Europäische Alternativangebote zu schaffen. Insbesondere im Hinblick auf Gaia-X ist die Entwicklung von Modellen für Maschinelles Lernen auf einer europäischen KI-Plattform essentiell, um auch bei KI-Systemen eine Chance auf deren Verankerung in unserem europäischen Werte- und Rechtssystem zu erreichen.
Für reine Cloud-Dienste und Kommunikationsdienste existieren bereits eine Vielzahl erprobter Sicherheitslösungen, die hier zum Einsatz kommen können und sollten. Kooperative Datennutzungsinfrastrukturen mit dem Ziel von Data Science und maschinellem Lernen stellen hingegen zahlreiche neue Herausforderungen. Ein Projekt wie Gaia-X sollte daher mit Forschung begleitet werden zu Lösungen für

- den Schutzes von geistigem Eigentum sowohl im zentralen Datentreuhändermodell als auch für dezentrales verteiltes Lernen;
- das Anonymisieren multidimensionaler Daten (bei Personenbezug) und Erzeugen systhetischer Daten;
- datenschutzfreundliches maschinelles Lernen;
- die Manipulationssicherheit bei kooperativer Datennutzung.

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

Aus meiner Sicht sind diese Aspekte zentral, um ein höheres IT-Sicherheitsniveau des Gesamtmarkts zu erreichen. Ich befürworte eine technologieneutrale Generalanforderung für die IT-Sicherheit aller IT-Produkte, die sich an Zielvorgaben orientiert. Um umfassende IT-Sicherheitsgewährleistung zu erzielen, sollten die Norm sowohl Betreiber als auch Hersteller adressieren. Als Vorbild für eine solche Regelung kann Art. 32 DSGVO dienen. Welche IT-Sicherheitsmaßnahmen im konkreten Einzelfall zu ergreifen sind, sollte risikoabhängig am Stand der Technik orientiert vom Normadressaten bestimmt werden können. Hierfür sollte die gesetzliche Regulierung unbedingt harmonisch mit technischen Standards zusammen wirken. Ich verweise ergänzend auf meine Antworten zu der Frage 8.
Synergien und eine Erhöhung der IT-Sicherheit können erzielt werden, wenn nicht nur die Vergabe und Beschaffung den Einsatz von Open Source und Open Hardware anregen, sondern dies begleitet wird durch die staatliche finanzielle Förderung von Open Source Bug Bounty Programmen und Open Source Code Audits nach dem Vorbild von EU FOSSA. Der Erfolg des Programms zeigt, dass auf diesem Weg tatsächlich eine Erhöhung der IT-Sicherheit der Open Source Software erreicht werden kann.

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?

Staatliche Zertifizierung und Systemtests sind auf mehreren Ebenen limitiert: Es fehlt an geeignetem Fachpersonal, die Menge an Produkten auf dem Markt ist unüberschaubar und die Aussagekraft von Zertifizierung und Tests ist begrenzt, da Verwundbarkeiten beispielsweise erst durch eingebundenen externen Code oder durch Updates entstehen können.
Dennoch können Zertifizierung und Systemtests gezielt eingesetzt zur Erhöhung der IT-Sicherheit beitragen. Es müssen aber Kriterien für die Auswahl der zu untersuchenden IT zu entwickelt werden, die den verfassungsrechtlichen Anforderungen von Art. 3 Abs. 1 und 14 Abs. 1 GG genügen. Weder darf die Auswahl willkürlich sein noch den Wettbewerb verzerren. Solche Kriterien können etwa die Kritikalität (bereits angelegt bei der Regulierung kritischer Infrastrukturen) oder ein hochrelevantes Informationsbedürfnis der Verbraucher sein. Außerdem muss eine Konkurrenz zu privaten Testern vermieden werden.
Sinnvoll ist die Ergänzung staatlicher Zertifizierungen und Tests um die in Antwort 11 genannten Open Source Code Audits und Bug Bounty Programme.

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

Der staatliche Umgang mit IT-Sicherheitslücken hat signifikante und messbare Auswirkungen auf die globale IT-Sicherheit. Von staatlicher Seite zurück gehaltene und verwendete Sicherheitslücken bleiben durchschnittlich für 7 Jahre ungepatcht durch den Hersteller. Währenddessen können sie genauso durch Kriminelle und antidemokratische Staaten gefunden oder gekauft werden. Darüber hinaus sind diese Sicherheitlücken bei staatlichen Stellen ein lohnendes Ziel für Angreifer. Die Hacker-Gruppe The Shadow Brokers hat in den letzten Jahren mehrfach geheime Angriffswerkzeuge der NSA, darunter auch hochkritische 0day-Angriffe, veröffentlicht. Eine dieser und so bekannt gewordenen Sicherheitslücken wurde später für die weltweite WannaCry-Attacke ausgenutzt.
Dennoch kann ein legitimes rechtsstaatliches Interesse bestehen, im absoluten Ausnahmefall Sicherheitslücken für Strafverfolgungszwecke zu nutzen, beispielsweise im Rahmen der Quellen-TKÜ wenn alle anderen Erkenntnismöglichkeiten ausgeschöpft sind. Insbesondere da das gezielte Angreifen von einzelnen Endgeräten weniger invasiv ist als das Installieren von Backdoors in Verschlüsselungverfahren für alle Nutzer.
Ich befürworte daher einen nationalen Vulnerabilities Equities Process (VEP), vergleichbar zu dem der Vereinigten Staaten. Dies ist ein definierter Prozess mit transparenten Kritierien, nach welchem von Fall zu Fall bestimmt werden kann, wie mit Sicherheitslücken verfahren werden soll: Ob diese zu Strafverfolgungszwecken eingesetzt werden sollen oder gegenüber dem Hersteller oder sogar der Öffentlichkeit offen gelegt werden müssen.

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?

Aus dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erwächst eine staatliche Schutzpflicht. Sie verbietet es dem Gesetzgeber im Hinblick auf die IT-Sicherheitsgewährleistung untätig zu bleiben oder gänzlich ungeeignete oder völlig unzureichende Maßnahmen zu ergreifen (das sog. Untermaßverbot). In Anbetracht der defizitären IT-Sicherheitslage kann und sollte der Gesetzgeber im Rahmen seiner Gewährleistungspflicht geeignete regulative Maßnahmen ergreifen (siehe Antwort 1).

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?

Dies technisch in Einklang zu bringen ist extrem schwierig und kann nur mit Abstrichen auf beiden Seiten, der individuellen IT-Sicherheit und der Reichweite von Strafverfolgungsinstrumenten erreicht werden. In jedem Fall ist, sofern alle anderen Erkenntnismittel ausgeschöpft sind, die Schwächung der IT-Sicherheit auf Basis individueller Endgeräte (Quellen-TKÜ) gegenüber einer generellen Schwächung von Kryptographie vorzuziehen. Dies erfordert einen sorgfältigen und verantwortlichen Umgang mit IT-Sicherheitslücken, die diesen Zugriff auf Endgeräte ermöglichen können (siehe Antwort 13).

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

Die mehrfach erwähnte generelle Anforderungen an die IT-Sicherheit sollte aus meiner Sicht eher auf EU-Ebene reguliert werden.
Für die Reform des nationalen IT-Sicherheitsgesetzes möchte ich folgende drei Aspekte anregen:

- Die Ergänzung staatlicher Produkttests auf IT-Sicherheit mit Open Source Code Audits und Bug Bounty Programmen (siehe Antworten 11 und 12).
- Eine Konsolidierung des nationalen IT- und Computerstrafrechts: Die Vorfeldverlagerung und Unbestimmtheit vieler Strafnormen kriminalisiert unbeabsichtigt sozialadäquates Verhalten und insbesondere legitime IT-Sicherheitsforschung. Die Beseitigung dieser „Chilling Effects“ beim Einsatz bestimmter Verfahren (beispielsweise Reverse Engineering), Technologien (Dual Use) oder im Responsible Disclosure Verfahren könnte zu einer verbesserten internationalen Wettbewerbsfähigkeit der deutschen IT-Sicherheitsforschung beitragen. Denkbar ist auch ein strafrechtlicher Rechtfertigungstatbestand für IT-Sicherheitsforschung.

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?

Der Umfang der Aufgaben des BSI führt potentiell zu Interessenkonflikten. Die Herauslösung der Aufgaben, die nicht die IT-Sicherheit staatlicher Stellen zum Ziel haben, sondern Beratung und Verbraucherschutz könnte diesen Interessenkonflikt beheben. Eine Unabhängigkeit ist anders als beim Datenschutz nicht geboten. Für diese Aufgaben böte sich die Fach- und Rechtsaufsicht des Bundesministeriums der Justiz und für Verbraucherschutz an.

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

/

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

Die Stufen 1-3 der vorgeschlagenen aktiven Cyberabwehr enthalten teilweise sinnvolle eher defensive und forensische Maßnahmen, die unter bestimmten Voraussetzungen zu einer Erhöhung der nationalen Verteidigungsfähigkeit beitragen können. Die Stufen 4 und 5, die unter anderem den Hackback oder staatliche Denial of Service-Angriffe umfassen, halte ich aufgrund des Risikos von fehlerhafter Attributierung, Kollateralschäden und völkerrechtlichen Konsequenzen für äußerst problematisch. Im Bereich der Forensik und Attributierung besteht zwar weiterhin Forschungsbedarf, allerdings werden wir in diesem Bereich immer mit einer großen Unsicherheit umgehen müssen.
Backdoors stellen eine umfassende und jeden Nutzer treffende Schwächung kryptographischer Sicherheitsgarantien unverhältnismäßig. Bei der Debatte um eine mögliche Frontdoor ist entscheidend, dass hier nicht bloß eine Umbenennung der Backdoor mit allen begleitenden Problemen geschieht. Zielführender ist der Vorschlag über eine gesetzliche Verpflichtung der Hersteller zu diskutieren, auf richterliche Anordnung eine manipulierte Version der Kommunikationssoftware auf dem Endgerät zu installieren, die den Zugriff auf die Kommunikation erlaubt. In diesem Fall findet aber gerade keine Ende-zu-Ende verschlüsselte Kommunikation mehr statt.

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

/

21. *Investieren Deutschland und Europa genug in Forschung und Entwicklung für IT-Sicherheit? Wo sehen Sie Defizite und wo dringenden Handlungsbedarf?*

Welche Forschungsaktivitäten im IT-Sicherheitsbereich in Deutschland werden sowohl durch EU-Mitgliedsstaaten als auch durch Nicht-EU-Staaten finanziell gefördert?

Der deutsche Gesetzgeber hat in den letzten Jahren die IT-Sicherheitsforschung in großem Umfang finanziell gefördert. Die Kompetenzzentren für IT-Sicherheitsforschung wurden ausgebaut und letztendlich mit Unterstützung des Bundes und der Länder auch verstetigt. Dank dieser Förderung ist es dem CISPA gelungen innerhalb von knapp 7 Jahren zum wissenschaftlich erfolgreichsten Standort Europas in der IT-Sicherheitsforschung zu werden.
Die deutschen IT-Sicherheitsforscher unterhalten zahlreiche und langjährige Forschungskooperationen mit Nicht-EU-Staaten. Die wichtigsten sind institutionalisierte Kooperationen mit den USA, Israel und Japan.
Handlungsbedarf sehe ich bei den regulativen Rahmenbedingungen für IT-Sicherheitsforschung, um Chilling Effekte zu beseitigen und die internationale Wettbewerbsfähigkeit der nationalen Forschung zu erhalten (siehe Antwort 16).

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 Bildung für den Umgang mit der digitalen Lebenswirklichkeit insbesondere auch IT-Sicherheit ist eine zentrale Schlüsselkompetenz für die gesamte Gesellschaft. Sie sollte bereits in der Schule vermittelt werden durch ein Schulfach nach dem Vorbild des “Computing” in England, das ein umfassendes Verständnis und Kompetenz für algorithmische Entscheidungsfindung, Problemlösung, Medienkompetenz und souveränen, selbstbestimmten und kreativen Umgang mit IT zum Ziel hat. Diese Schulbildung muss begleitet werden durch auf IT-Sicherheit spezialisierte Studienangebote und Fort- und Weiterbildungsangebote in der Erwachsenenbildung. Die Universität des Saarlandes hat in den vergangen Jahren nicht nur einen Bachelor Cybersicherheit etabliert, sondern beispielsweise auch einen rechtswissenschaftlichen Master “Informationstechnik und Recht”. Dies könnte als Vorbild für weitere interdisziplinäre Studienangebote dienen.
Die größte Herausforderung für diese Vision ist die Ausbildung der Lehrkräfte und Ausstattung der Schulen. Hier muss durch die Länder und soweit möglich unterstützt durch den Bund entsprechende Schwerpunkte in der Lehrerausbildung gesetzt werden beispielsweise mit fachspezifischen Lehrstühlen und Unterrichtsmaterialien für “Didaktik des Computing”.

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?

Aktuelle kryptographische Forschung berücksichtigt bereits Quantencomputing als Angriffsszenario zur Bewertung der Garantien von neuen kryptographischen Verfahren. Insofern ist Post-Quanten-Kryptographie bereits seit einigen Jahren ein Gegenstand der aktuellen Forschung mit rapidem Erkenntnisfortschritt. Die Herausforderung wird sein, diese Erkenntnisse in die Praxis zu überführen. Bereits Verschlüsselung nach dem heutigen Stand der Technik wird häufig gar nicht eingesetzt oder falsch installiert. Dies ist auf mangelnde Awareness der Nutzer und fehlende Benutz- und Bedienbarkeit der Verfahren zurückzuführen. Benutzbare und komfortable Produkte zur langzeitsicheren Verschlüsselung herzustellen wird daher die zentrale Herausforderung darstellen.

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

Eine gesetzliche Verpflichtung erscheint nicht notwendig. Der Großteil der Verbraucherinnen und Verbraucher hat keinen direkten Vorteil oder Vertrauensgewinn aus der Offenlegung von Quellcode. Ohne eine aktive Community ist auch keine Sicherheitsgewinn zu erwarten.
Vielversprechender ist eine (verpflichtende) Kennzeichnung von Verbraucherprodukten beim Verkauf im Hinblick auf ihre Sicherheitseigenschaften und die Dauer für die Updates bereit gestellt werden. Ein solches standardisiertes Sicherheits-Infoblatt könnte eine leichtere Vergleichbarkeit für Verbraucher erzielen und IT-Sicherheit als Wettbewerbsfaktor stärken.

*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?*

/

Mit freundlichen Grüßen
Ninja Marnau