Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 24. Januar 2023

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Fragekatalog auf Ausschussdrucksache SB20(23)14
zur öffentlichen Anhörung des Ausschuss für Digitales des Deutschen Bundestages
am Mittwoch, 25. Januar 2023, 14:00 – 16:00 Uhr,

zum Thema „Cybersicherheit
- Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Vorbemerkung

Als Bundesbeauftragter für den Datenschutz und die Informationsfreiheit habe ich ein massives Interesse an einer starken und vertrauenswürdigen Stelle, die das Thema IT-Sicherheit in Deutschland vertreten kann, denn effektiver Datenschutz ist ohne funktionierende IT-Sicherheit unmöglich. Sichere digitale Infrastrukturen und Dienste sind eine zentrale Voraussetzung für eine funktionierende Digitalisierung, denn nur funktionierende IT-Sicherheit kann das notwendige Vertrauen schaffen, ohne das Bürgerinnen und Bürger digitale Dienste nicht nutzen werden.

Fragenkatalog

1. *Im Koalitionsvertrag haben die Regierungsparteien vereinbart, dass sie „einen strukturellen Umbau der IT-Sicherheitsarchitektur" einleiten und das „Bundesamt für Sicherheit in der Informationstechnik (BSI) unabhängiger" aufbauen und es als „zentrale Stelle im Bereich IT-Sicherheit" ausbauen wollen. Wie sollte die Cybersicherheitsarchitektur auf nationaler und europäischer Ebene ausgestaltet werden, um effektiver, wirksamer und widerspruchsfreier aufgestellt zu sein und wo bedarf es einer Neuordnung oder auch Bündelung der Kompetenzen zwischen Bund, Ländern und der Europäischen Union und bedarf es auch angesichts der aktuellen Herausforderungen einer Diskussion über innere und äußere Sicherheit und der diesbezüglichen Kompetenzen und Grenzen? Welche anderen Akteure neben dem BSI (also etwa Cyber-Abwehrzentrum, Nationaler Cyber-Sicherheitsrat, ZITiS), die in Deutschland für Cybersicherheit zuständig sind, sollten reformiert werden und wie?*

   Diese Frage liegt außerhalb der Zuständigkeit des BfDI. Wichtig wäre das Vertrauen von Bürgerinnen und Bürgern, Institutionen und Unternehmen in die Arbeit der für die Cybersicherheit verantwortlichen Stelle oder Stellen. Dazu gehört auch die weitmöglichste Vermeidung der Vermischung von Aufgaben der Cybersicherheit und der Unterstützung von Strafverfolgungsbehörden.

2. *Wie kann das Ziel, das BSI unabhängiger aufstellen zu wollen, konkret erreicht werden und wo bedarf es neben der Rechtsaufsicht seitens des BMI auch einer Fachaufsicht – oder anders herum gefragt: wo sind die bestehenden Abhängigkeiten das größte Hemmnis mit Blick auf die Akzeptanz und das Vertrauen in das BSI und welche Möglichkeiten sehen Sie, diese abzubauen?*

   Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

3. *Könnten Sie bitte den Begriff der aktiven Cyberabwehr und die unterschiedlichen Stufen und Möglichkeiten der aktiven Cyberabwehr (auch vor dem Hintergrund einer allein defensiv ausgerichteten bzw. einer offensiv ausgerichteten Cyberabwehr) definieren und wo sehen Sie konkrete Defizite im geltenden Recht und in den geltenden Kompetenzen, die einer wirksamen Cyberabwehr entgegenstehen?*

Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

4. *Weitere Instrumente, die der Koalitionsvertrag adressiert, sind etwa auch*
   - *das Recht auf Verschlüsselung,*
   - *ein Schwachstellenmanagement und die Pflicht, Sicherheitslücken zu melden,*
   - *die Stärkung der digitalen Souveränität und die Beachtung der Vertrauenswürdigkeit von Unternehmen,*
   - *die Vorgaben „security-by-design/default" als Standard,*
   - *Stärkung der Produkthaftung und der IT-Sicherheitsforschung,*
   - *das Recht auf Interoperabilität und Portabilität sowie das Setzen auf offene Standards, Open Source und europäische Ökosysteme, etwa bei 5G oder KI.*

   Welche dieser Maßnahmen sollten mit welcher Priorität ungesetzt werden, wo besteht aus Ihrer Sicht darüber hinausgehender Handlungsbedarf und wo bestehen insbesondere Defizite?

Aus Sicht des Datenschutzes sind alle diese Instrumente wichtig. Am grundlegendsten ist hier sicher das Recht auf Verschlüsselung, denn Bürgerinnen und Bürger müssen sich darauf verlassen können, dass ihre private Kommunikation auch privat bleibt. Verlieren die Bürgerinnen und Bürger das Vertrauen in digitale Dienste und Infrastruktur, wird Digitalisierung nicht funktionieren.

Aus dem gleichen Grund ist es aber auch wichtig, dass es eine Pflicht gibt, Sicherheitslücken zu melden, denn jede Sicherheitslücke, die nicht geschlossen werden kann, weil sie jemand (aus welchem Grund auch immer) nicht an den Hersteller gemeldet hat, gefährdet fundamental die Sicherheit digitaler Dienste und Infrastrukturen und untergräbt so das Vertrauen in diese. Hier kann eine vertrauenswürdige unabhängige Stelle hilfreich sein, die Schwachstellenmeldungen sammelt, und gezielt an die Hersteller weiterleitet, aber auch gegebenenfalls die Öffentlichkeit, insbesondere Firmen und Institutionen, informiert, die Software einsetzen, die von Schwachstellen betroffen ist.

Auch digitale Souveränität ist ein wichtiger Bestandteil funktionierender Digitalisierung und Voraussetzung für einen effektiven Datenschutz. Wenn digitale

Dienste und Infrastrukturen von Komponenten und anderen Diensten abhängen, deren Eigenschaften und Vertrauenswürdigkeit nur teilweise bekannt sind und die sich auf Grund ihrer Marktmacht oder weil sie in einer gänzlich anderen Jurisdiktion angesiedelt, sich einer Kontrolle gegebenenfalls entziehen können, dann wird es sowohl für die Digitalisierung der öffentlichen Verwaltung als auch für digitale Angebote in der Wirtschaft sehr schwer nachzuweisen sein, dass diese Dienste und Angebote den gesetzlichen Anforderungen entsprechen.

An dieser Stelle mache ich darauf aufmerksam, dass der Begriff der digitalen Souveränität in der öffentlichen Debatte unterschiedlich verwandt und verstanden wird. Zum Teil werden Bezüge zu einem aus Datenschutzsicht abzulehnenden Dateneigentum hergestellt. Für eine fundierte und verlässliche Befassung wird eine eindeutige Definition des Begriffs der digitalen Souveränität und ein daraus hervorgehendes einheitliches Verständnis für essentiell betrachtet und sollte geschaffen werden. Digitale Souveränität wird ausgehend von der Fragestellung nicht mit der Begrifflichkeit des Dateneigentums verbunden.

Analog zu dem Grundsatz „Data Protection by Design and by Default“, der in Artikel 25 der Datenschutz-Grundverordnung gesetzlich verankert ist, sollte für die Entwicklung von Geräten, Software und Diensten auch der Grundsatz „Security by Design and by Default“ etabliert werden, denn genau wie der Datenschutz muss auch Sicherheit von Anfang an mitgedacht und in Produkte und Dienste integriert werden. Die Betrachtung der Sicherheit erst einmal hintan zu stellen wird am Ende immer schwieriger und teurer werden, als sie von Anfang an zu berücksichtigen. Genau wie beim Grundsatz „Data Protection by Design and by Default“ braucht aber natürlich auch die Anforderung „Security by Design and by Default“ nicht unbedingt „absolut“ gestellt werden, sondern sie kann ebenfalls in Abhängigkeit von Faktoren wie den involvierten Risiken, dem Stand der Technik und auch den Implementierungskosten betrachtet werden.

Wenn man den Grundsatz „Security by Design and by Default” erst einmal etabliert hat, dann wird es nur folgerichtig sein, die Beachtung dieses Grundsatzes über entsprechende Vorschriften zur Produkthaftung von den Herstellern, Entwicklern und Betreibern auch einzufordern. Die Stärkung der Sicherheitsforschung kann in diesem Zusammenhang ebenfalls ein passendes Instrument sein, da sie einerseits die Grundlagen dafür legen kann, dass Sicherheit effektiv und effizient in Produkte und Dienste integriert werden kann, aber andererseits auch einen Beitrag dazu leisten kann, dass gegebenenfalls Sicherheitsmängel aufgedeckt (und im zweiten Schritt dann hoffentlich behoben) werden.

Wichtig ist in diesem Zusammenhang vor allem, dass der Staat diesen Grundsatz bei seinen datenbasierten Diensten und Produkten als selbstverständliche Verpflichtung berücksichtigt und Verstöße unter allen Umständen vermeidet.

Für die Akteure im Bereich der IT-Sicherheitsforschung muss ein ausreichender, geeigneter und rechtssicherer Handlungsrahmen vorhanden sein bzw. kurzfristig geschaffen werden. Insbesondere müssen für diese Forschungszwecke gesetzliche Regelungen vorliegen, welche erforderliche Rechtseingriffe durch die Verarbeitung von personenbezogenen Daten normenklar und ausdrücklich hinsichtlich Anlässe, Zwecke und Grenzen der Eingriffe legitimieren.

5. *Vor dem Hintergrund des hybriden Angriffskrieges Russlands gegen die Ukraine sind erneut Forderungen nach Instrumenten der sogenannten offensiven Cyberabwehr laut geworden. Wie beurteilen Sie diese Forderungen und die Argumentation, offensive Instrumente vermeintlich unterhalb der Schwelle von Hackbacks einzusetzen, im Hinblick auf ihre Recht-und Zweckmäßigkeit?*

Unabhängig von den Ereignissen des vergangenen Jahres und außerhalb meiner Zuständigkeit möchte ich zu bedenken geben, dass alleine der Begriff der „offensiven Abwehr" bereits problematisch - da in sich widersprüchlich - ist. Ein grundlegendes Problem bei allen „offensiven Abwehrmaßnahmen" stellt die Attribution dar, denn es ist insbesondere bei Cyberangriffen in der Regel sehr schwierig bis unmöglich, einen Angriff einem bestimmten Angreifer mit hinreichender Sicherheit zuzuordnen, zumal Angreifer in vielen Fällen Systeme oder Netze Dritter für ihre Aktionen missbrauchen. Bereits aus diesem Grund sehe ich erhebliche Zweifel bei der Frage der Rechtmäßigkeit. Gerade dieser Umstand impliziert auch erhebliche Zweifel zur Frage der Zweckmäßigkeit, da „offensive Abwehrmaßnahmen" hier auch erhebliche und kaum abschätzbare Kollateralschäden verursachen können.

6. *Was kann die Bundesrepublik Deutschland in ihrer nationalen und internationalen Cybersicherheitspolitik von anderen Ländern und internationalen Best Practices konkret lernen, insbesondere im Hinblick auf staatliche Stellen, Governance, verfügbare Instrumente, Fokus und Kapazitäten?*

Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

7. *Welche politischen und rechtlichen Herausforderungen stellen sich bei der Schaffung eines Regelwerks für eine Meldepflicht für Sicherheitslücken (zero days) und einen gesetzlich strukturierten Umgang mit Schwachstellen („wirksames Schwachstellenmanagement, mit dem Ziel Sicherheitslücken zu schließen")?*

   Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

8. *Die Bundesregierung hat Eckpunkte eines KRITIS-Dachgesetzes verabschiedet und will dabei insbesondere eine bessere Verschränkung des Schutzes digitaler und physischer Infrastruktur erreichen: Welche organisatorischen und rechtsdogmatischen Ansatzpunkte sind denkbar, um physische und digitale Komponenten kritischer Infrastruktur gemeinsam und kohärent zu regulieren und inwiefern kann der Gesetzgeber hier insbesondere auf geltendem Recht und Regulierungsvorschlägen aus der Vergangenheit (etwa rund um das IT-Sicherheitsgesetz 2.0) aufsetzen?*

   Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

9. *Mit Blick auf Redundanzen in der Kommunikationsinfrastruktur der Deutschen Bahn könnte das Netzwerkprotokoll TCP/IP als Rückfallebene bei etwaigen Sabotageakten verwendet werden. TCP/IP müsste dabei aber nicht über Mobilnetze, sondern kabelgebunden verwendet werden. Dafür müsste die DB-Netze ein kleines Matrix-Netz an den Knoten aufbauen, das bspw. mit der Kabelinfrastruktur einzelner Netzbetreiber verbunden ist. Dann läuft das System weiter, auch wenn die Infrastruktur punktuell beschädigt, oder zerstört würde. Was könnten Gründe dafür sein, dass ein solches Matrix-Netz nicht bereits existiert?*

   Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

10. *Wenn in Deutschland entscheidende Bestandteile für kritische Infrastrukturen (KRITIS) beschafft werden – etwa für Telekommunikationsnetzwerke –, dann können Produzenten unter bestimmten Bedingungen davon ausgeschlossen werden. Die Hürden hierfür sind jedoch hoch. So kann dies erst nach wiederholten Verstößen gegen die Vertrauenswürdigkeit geschehen (bspw. wenn ein Hersteller falsche Angaben gemacht hat, Sicherheitsüberprüfungen nicht unterstützt oder IT-Schwachstellen nicht unverzüglich meldet und beseitigt). Sehen Sie in Anbetracht der sog. „Zeitenwende"*

Anlässe den geltenden Rechtsrahmen zu verschärfen (etwa in einem IT-Sicherheitsgesetz 3.0) und, falls ja, wie?

Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

11. *Wie bewerten Sie die Lage von IT-Fachkräften – insbesondere für Cybersicherheit – auf dem Arbeitsmarkt und was müssten staatliche (Sicherheits)-Behörden verbessern, um noch mehr kompetente IT-Fachkräfte zu gewinnen?*

    Aus den eigenen Erfahrungen in meiner Dienststelle kann ich bestätigen, dass es für staatliche Stellen aktuell sehr schwierig ist, kompetente IT-Fachkräfte zu gewinnen. Neben Maßnahmen zur Erhöhung der eigenen Ausbildungskapazitäten des Bundes über Ausbildung, Studium und Stipendien sollten auch Veränderungen im Dienstrecht in Betracht gezogen werden. Insbesondere sollte der Zugang zum gehobenen und höheren Dienst bzw. entsprechende Einstufungen von Tarifbeschäftigten an die real vorhandenen Lebensläufe von IT-Fachkräften angepasst werden. Nachdenken sollte man auch über Fachkarrieren von besonders herausgehobenen Fachkräfte, ohne in höhere Laufbahngruppen einsteigen oder Personalverantwortung übernehmen zu müssen.

12. *Wie könnte die Ausbildung von IT-Cyberfachkräften sowohl in quantitativer als auch in qualitativer Hinsicht in Deutschland weiter verbessert werden?*

    Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

13. *Wie bewerten Sie die vorhandenen technischen Fähigkeiten in Deutschland für eine wirksame Cyberabwehr – auch mit aktiven Cyberabwehr-Instrumenten?*

    Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

14. *Welche Rolle spielen private Cybersicherheits-Unternehmen für eine effektive staatliche Cyberabwehr im internationalen Vergleich?*

Diese Frage liegt außerhalb der Zuständigkeit des BfDI.

15. *Inwieweit sind aus technischer Sicht sog. Software-Schwachstellen (nicht gemeint sind spezifische IT-Schnittstellen für Sicherheitsbehörden, wie sie z. B. derzeit im Rahmen des 3GPP-Gremiums für den künftigen 6G-Mobilfunkstandard unter Beteiligung von ZITiS und Cyberagentur entwickelt werden) erforderlich, um Sicherheitsbehörden Zugriff auf Kommunikationsendgeräte im Rahmen von Strafermittlungen zu verschaffen oder gibt es mittlerweile hinreichend wirksame Technologien, wie z. B. kryptographische Verfahren, die weniger Kollateralschäden aufweisen und inwieweit ist diese Schwachstellen-Diskussion auf mittlere Sicht hinfällig, wenn wir an Entwicklungen wie Quantenkommunikation denken?*

Aus technischer Sicht sind Software-Schwachstellen nicht erforderlich, um Sicherheits- und Strafverfolgungsbehörden Zugriff auf Kommunikationsendgeräte zu geben, denn für den Zugriff von Sicherheits- und Strafverfolgungsbehörden stehen die erwähnten spezifischen IT-Schnittstellen zur Verfügung, die einen regulierten Zugriff erlauben.

Ein unregulierter Zugriff über Schwachstellen hingegen wird immer Kollateralschäden verursachen und schadet dem Vertrauen der Bürgerinnen und Bürger in digitale Infrastrukturen und Dienste.

Jede gezielte Schwächung einer Sicherheitsfunktion oder Sicherheitseigenschaft schwächt zudem das betroffene Produkt oder den betroffenen Dienst für alle Nutzerinnen und Nutzer und nicht nur für diejenigen, gegen die sich ein solcher Eingriff richtet.

In meiner Stellungnahme im Verfassungsbeschwerdeverfahren – 1 BvR 1552/19 – gegen § 15b und § 15c des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018 habe ich deutlich gemacht, dass die Schaffung von Befugnissen, mit denen die Behörden Sicherheitslücken ausnutzen dürfen, im Widerspruch zu dem eigenen Schutzkonzept zur IT-Sicherheit stehen würde, das im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) zum Ausdruck kommt.

Es wäre widersprüchlich, wenn das BSI zur Erfüllung seiner Aufgaben gemäß § 7 BSIG die Öffentlichkeit und betroffene Kreise vor Sicherheitslücken und Schadprogrammen warnen kann, andere (Sicherheits-) Behörden dieselben Sicherheitsrisiken jedoch geheim halten dürften. In der von der Bundesregierung formulierten Cyber-Sicherheitsstrategie für Deutschland 2016 hieß es zu Recht: „Staat, Wirtschaft, Wissenschaft und Gesellschaft tragen für die Sicherheit des Cyber-Raums eine gemeinsame Verantwortung. Sie müssen daher auch aufeinander abgestimmte Antworten auf die jeweils aktuellen Herausforderungen geben“ (BT-Drucks. 18/10395, S. 4).

An dieser Einschätzung hat sich nichts geändert.

16. *Wie sollte ein Schwachstellen-Management technisch, personell und organisatorisch aufgesetzt werden, sind dafür z. B. Risiko Management-Standards als ein Vorbild denkbar und welche Ziele kann sich ein Schwachstellen-Management setzen, angesichts von über 20.000 Software-Schwachstellen, wie sie zuletzt der BSI-Lagebericht festgestellt hat und inwieweit ist für die Konzeptionierung und Implementierung eines solchen Schwachstellen-Managements tatsächlich ein unabhängiges BSI zwingend erforderlich?*

Beim Aufbau eines Schwachstellen-Managements gibt es viele Variablen. Aus meiner Sicht sollte aber zumindest als ein Ziel definiert werden, Schwachstellen so schnell wie möglich zu beseitigen. Nur so kann der bestmögliche Schutz der Rechte und Freiheiten der Bürgerinnen und Bürger erreicht werden, um so das Vertrauen in die Sicherheit digitaler Dienste und Infrastrukturen zu fördern.

Mit Blick auf die Prozesse zur Meldung von Schwachstellen sollte eine Möglichkeit geschaffen werden, dass Sicherheitsforscherinnen und –forscher (oder ganz allgemein Personen, die Schwachstellen in Produkten oder Diensten entdeckt haben) die entsprechenden Informationen an eine vertrauenswürdige Stelle weiterzugeben, ohne Repressalien befürchten zu müssen. Vermutlich wird dies nur dann möglich sein, wenn auch eine anonyme oder zumindest pseudonyme Meldung ermöglicht wird.

Dies impliziert, dass eine „Schwachstellen-Meldestelle“ ein hohes Maß an Unabhängigkeit erhalten muss und dass es keine Verpflichtung geben darf, entweder Informationen zu Schwachstellen zurückzuhalten oder andererseits Informationen zu den meldenden Personen herauszugeben, insbesondere nicht an die Hersteller oder Betreiber von Produkten oder Diensten, bei denen Schwachstellen entdeckt wurden.

17. *Anhand welcher Maßnahmen und/oder Methoden kann das Sicherheitsverständnis und -verhalten von IT-Nutzer*innen effektiv in den Mittelpunkt gerückt, eine höhere IT-Sicherheitskultur aufgebaut und das individuelle Vertrauen in die digitale Umgebung gestärkt werden?*

    Wie auch bei anderen Fragen einer digital literacy ist dieses Thema sehr weitgehend. Fundament muss die Bereitschaft der öffentlichen Hand sein, bei eigenen Projekten und bei selbst verwendeten Tools höchsten Wert auf die IT-Sicherheit zu legen und diese nicht als „überzogen" zu diskreditieren. Verzichtet werden muss auf alle Vorhaben, die die IT-Sicherheit digitaler Infrastruktur oder weit verbreiteter Geräte und Lösungen in irgendeiner Form schwächt, um so das Vertrauen der Bürgerinnen und Bürger dort zu stärken, wo dieses dann auch berechtigt ist.

18. *Wer bzw. was muss alles in den Blick genommen werden, wenn wir über Zuständigkeiten und Instrumente zur Verbesserung der IT-Sicherheit nachdenken, wo liegen die jeweiligen Defizite sowie Verbesserungsmöglichkeiten und wie bewerten Sie die Effektivität aktueller Informations- und (Weiter-)Bildungsmaßnahmen?*

    Diese Frage liegt z.T. außerhalb der Zuständigkeit des BfDI, ansonsten verweise ich auf die Antworten zu verwandten Fragen.