Deutscher Bundestag **Drucksache 20/8103**

20. Wahlperiode 23.08.2023

Kleine Anfrage

der Fraktion der CDU/CSU

Digitale Souveränität in der Bundesverwaltung – Entwicklung, Beschaffung und Einsatz von IT-Sicherheitsprodukten

Die Bundesverwaltung ist vom einwandfreien Funktionieren und der uneingeschränkten Verfügbarkeit von IT-Systemen abhängig (www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheiskriterien/it-sicherheiskriterien_node.html; www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Grundsaetzliche-Aussagen/grundsaetzliche-aussagen_node.html).

Deshalb hat unter anderem das Bundesamt für Sicherheit in der Informationstechnik (BSI) einerseits nach dem BSI-Gesetz (BSIG) und der BSI-Zertifizierungs- und Anerkennungsverordnung die Aufgabe, Zertifizierungen informationstechnischer Produkte oder Komponenten sowie informationstechnischer Systeme durchzuführen. Zertifikate des BSI sind ein unabhängiger Konformitätsnachweis dahin gehend, dass ein IT-Sicherheitsprodukt definierten Sicherheitsanforderungen entspricht. In einigen Bereichen ist eine Zertifizierung durch Gesetz, Verordnung, Richtlinie oder Standard verbindlich vorgeschrieben. Für die Produktzertifizierung empfiehlt das BSI eine Zertifizierung nach den international anerkannten Sicherheitskriterien der Common Criteria (CC). Die CC sind ein etablierter und international anerkannter Kriterienkatalog für das Design, die Implementierung, Auslieferung und Wartung der Sicherheitsfunktionen von IT-Sicherheitsprodukten. Für die Zertifizierung nach den CC wurde international die gegenseitige Anerkennung von IT-Sicherheitszertifikaten unter gewissen Bedingungen vereinbart, um die Mehrfach-Zertifizierung des gleichen Produkts in verschiedenen Staaten zu vermeiden. Mit einem CC-Zertifikat bestätigt das BSI die Korrektheit und Effektivität der vom Produkt angebotenen Sicherheitsfunktionen. Eine Zertifizierung kann auch nach einer Technischen Richtlinie (TR) erfolgen. Ein wesentlicher Bestandteil davon ist die Konformitätsprüfung, in der untersucht wird, ob ein Produkt die in der jeweiligen TR festgelegten Vorgaben und Anforderungen erfüllt. Das Ziel einer TR des BSI ist die Verbreitung von angemessenen IT-Sicherheitsstandards. Ihre Verbindlichkeit entsteht erst durch individuelle Vorgabe des Bedarfsträgers. Die europäisch anerkannten ITSEC-Sicherheitskriterien (ITSEC = Information Technology Security Evaluation Criteria) können einerseits für eine Produktzertifizierung im BSI-Zertifizierungsschema nur noch in begründeten Ausnahmefällen angewandt werden (www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/zertifizierung-und-anerkennung_node.html; www.bsi.bund.de/DE/Themen/Unternehmen-und-Orga

nisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/zertifizierung-nach-cc_node.html; www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/itsicherheitszert.html?nn=127290; www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/CC-Produkte.pdf?__blob=publicationFile&v=10; Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen (bund.de); www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Zertifizierte-IT-Sicherheit.pdf?__blob=publicationFile&v=1).

Andererseits hat das BSI auch die vertrauensbildende gesetzliche Aufgabe, IT-Produkte für die Sicherheit in der IT zu prüfen und eine verbindliche Aussage zum Sicherheitswert zu machen. Betroffen sind IT-Produkte, die zudem für die Übertragung und Verarbeitung von amtlich geheim gehaltenen Informationen im Geheimschutz und in Verschlusssachen (VS) im Bereich des Bundes und der Länder oder bei Unternehmen im Rahmen von Aufträgen des Bundes oder der Länder eingesetzt werden. Derartige Produkte benötigen eine Zulassung durch das BSI. Das BSI legt überdies fest, welche IT-Sicherheitsprodukte über eine Zulassung verfügen müssen. Diese IT-Sicherheitsprodukte im Bereich der Informationstechnik zur Handhabung von Verschlusssachen einschließlich deren Übertragung (VS-IT) übernehmen IT-Sicherheitsfunktionen zum Schutz elektronischer VS. Der Antrag auf Zulassung eines solchen IT-Produkts kann grundsätzlich nur von einem behördlichen Anwender gestellt werden. Sind keine zugelassenen IT-Sicherheitsprodukte für VS-IT vorhanden oder kann eine Bereitstellung nicht zeitgerecht veranlasst werden, kann beim BSI eine Einsatzerlaubnis für andere IT-Sicherheitsprodukte beantragt werden. Das BSI kann diese Einsatzerlaubnis zeitlich befristen sowie besondere Auflagen und Einschränkungen hinsichtlich der Einsatz- und Betriebsbedingungen erteilen. Von der Zulassungsregelung sind begrenzt auch solche IT-Sicherheitsprodukte betroffen, die für sensitive, aber nicht eingestufte Informationen im Behördenbereich eingesetzt werden können. Grundsätzlich gilt eine solche Zulassungsregelung für den Bereich der sensitiven, aber nicht eingestuften Informationen aber nicht (Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz [Verschlusssachenanweisung – VSA] vom 13. März 2023, § 5 Absatz 1 Nummer 5 und 6 sowie § 51 Absatz 1 und 5 VSA; www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zulassung/Hinweise-zur-Liste-der-zugelassenen-IT-Sicherheitsprodukte-und-systeme/hinweise-zur-liste-der-zugelassenen-it-sicherheitsprodukte-und-systeme.html; www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/FAQ-Zertifizierung-und-Anerkennung/faq-zertifizierung-und-anerkennung_node.html).

Zudem unterscheidet das BSI in IT-Sicherheitsprodukte, die vom BSI zugelassen sein müssen, und IT-Sicherheitsprodukte, die zugelassen sein sollen. Letztere lassen Ausnahmen zu, falls keine geeigneten zugelassenen Produkte zur Verfügung stehen. In der Regel kommen dabei IT-Sicherheitsprodukte zum Einsatz, die durch das BSI mit nationalem Schutzprofil CC-zertifiziert wurden (www.bsi.bund.de/DE/Service-Navi/FAQ/EvaluierungundZulassung/faq_evaluierung-zulassung_node.html).

Die VSA listet zudem IT-Sicherheitsfunktionen innerhalb von VS-IT, die Gegenstand einer Zulassungsaussage des BSI sein können. Das BSI hat einen auf diesen IT-Sicherheitsfunktionen und den sich hieraus ableitenden Produktklassen und Produkttypen basierenden Katalog veröffentlicht (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zulassung/VS-Produktkatalog_BSI.pdf?__blob=publicationFile&v=13). Der Katalog der Produktklassen und Produkttypen definiert insbesondere, ob eine Zulassungsaussage für einen Produkttyp erforder-

lich ist und welche Sicherheitsfunktionen in einem Zulassungsverfahren für einzelne Produkttypen gelten (§ 52 VSA).

Im Übrigen unterstützen und beraten die IT-Sicherheitsbeauftragten die Geheimschutzbeauftragten in der Verwaltung in allen Fragen des Einsatzes von VS-IT (§ 9 VSA).

Neben den IT-Sicherheitsprodukten für VS-IT darf aber nicht unerwähnt bleiben, dass selbstverständlich auch solche IT-Sicherheitsprodukte, die nicht im Bereich der Verschlusssachen eingesetzt werden, Relevanz für die ganzheitliche digitale Souveränität der Bundesverwaltung haben. Denn häufig bekommen Dienstleister auch mit diesen IT-Sicherheitsprodukten Einblicke in den Daten- und Netzverkehr. Dies kann z. B. bei Schutzlösungen für die sogenannten Layer 3, 4 und 7 oder den E-Mail-Verkehr der Fall sein. Diese IT-Sicherheitsprodukte sind daher auch von Interesse für die Fragesteller in der vorliegenden Kleinen Anfrage.

Darüber hinaus existieren in der Wirtschaft Einrichtungen, deren Beeinträchtigung Gefahren für das Leben oder die Gesundheit der Bevölkerung, für die öffentliche Sicherheit oder Ordnung sowie die Verteidigungsbereitschaft des Landes hervorrufen können. Eine besondere Gefahr kann dabei immer von Personen ausgehen, die in diesen Einrichtungen tätig sind. Durch die Geheimschutzbetreuung der Firmen beispielsweise in Form von Sicherheitsüberprüfungen der VS-befassten Mitarbeiterinnen und Mitarbeiter, und durch den vorbeugenden Sabotageschutz, etwa in Form von Sicherheitsüberprüfungen von Mitarbeitern, die an sicherheitsempfindlichen Stellen eingesetzt werden sollen, begegnen die zuständigen Geschäftsbereiche der Bundesregierung basierend auf den gesetzlichen Regelungen des Sicherheitsüberprüfungsgesetzes (SÜG) diesen Gefahren (www.bmwk.de/Redaktion/DE/Artikel/Wirtschaft/sicherheit-in-der-wirtschaft.html).

In der Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (BMI) vom Juli 2022 wird betont, dass die Stärkung der Cyber-Resilienz von Bundesbehörden keinen weiteren Aufschub duldet. Unter anderem fordert es, dass Bundesbehörden mit weiterentwickelten IT-Produkten ausgestattet werden sollen (www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4, S. 5, S. 10.). In ihrer Digitalstrategie erhebt die Bundesregierung zudem den Anspruch, die Erforschung, Anwendung und Einführung von Schlüsseltechnologien als Grundlage für digitale Souveränität konsequent voranzutreiben. In diesem Zusammenhang beabsichtigt die Bundesregierung, unter anderem die Kompetenzen in der Cybersicherheit auszubauen und ganzheitlich das dazugehörende Ökosystem zu stärken (Digitalstrategie, S. 33 f., abrufbar unter: digitalstrategie-deutschland.de/static/fcf23bbf9736d543d02b79ccad34b729/Digitalstrategie_Aktualisierung_25.04.2023.pdf). Darüber hinaus vertritt die Bundesregierung in ihrer kürzlich veröffentlichten Nationalen Sicherheitsstrategie den Anspruch, im Zusammenhang mit einer Weiterentwicklung der Cybersicherheitsstrategie auch die Cybersicherheit der Bundesverwaltung umfassend zu stärken (Nationale Sicherheitsstrategie der Bundesregierung, Bundestagsdrucksache 20/7220, S. 59, S. 61). Auch adressiert sie in der Nationalen Sicherheitsstrategie wichtige Fragen zur Beschaffung von Sicherheitstechnologien als Schlüssel-technologien an prominenter Stelle. So heißt es unter anderem, dass es „[…] eines gezielten Auswahlprozesses, der Wissensentwicklung und -verbreitung, der Rahmensetzung, der Ressourcenmobilisierung und Marktentwicklung für strategische Technologielinien [bedürfe]“ (Nationale Sicherheitsstrategie der Bundesregierung, Bundestagsdrucksache 20/7220, S. 57) und die Bundesregierung werde „[…] überprüfen, bei welchen Schlüsseltechnologien nationale und europäische Fähigkeiten zum Schutz unserer technologischen und digitalen Souveränität nötig sind [und] gezielt Anbieter

kritischer Schlüsseltechnologien mit geeigneten Maßnahmen, z. B. durch staatliche Ankeraufträge, unterstützen, um eigene Fähigkeiten zu Forschung und Entwicklung in kritischen Technologien zu erhalten und weiterzuentwickeln“ (Nationale Sicherheitsstrategie der Bundesregierung, Bundestagsdrucksache 20/7220, S. 58).

Unter dem Eindruck der obigen Ausführungen rund um Zertifizierung, Zulassung und Sicherheitsüberprüfungen im gesamten Bereich von IT-Sicherheitsprodukten – also denen für den Einsatz im Bereich von VS-IT als auch denen für den Einsatz abseits von Verschlusssachen – und den dargestellten Ansprüchen der Bundesregierung in der Cybersicherheit und zur digitalen Souveränität ergeben sich für die Fraktion der CDU/CSU Fragen zur Beschaffung und zum Einsatz von IT-Sicherheitsprodukten für die Bundesverwaltung (Hinweis: Bei den folgenden Fragen mit Bezug zur Bundesverwaltung sind die Nachrichtendienste des Bundes auszunehmen.).

Wir fragen die Bundesregierung:

1. In welchen Bereichen ist eine Zertifizierung von IT-Sicherheitsprodukten durch Gesetz, Verordnung, Richtlinie oder Standard verbindlich vorgeschrieben?
2. Von welchem Zeitraum genau geht die Bundesregierung bei einer nicht „zeitgerechten“ Veranlassung von zugelassenen IT-Sicherheitsprodukten für VS-IT und einer daraus gegebenenfalls notwendig werdenden Beantragung einer Einsatzerlaubnis für andere IT-Sicherheitsprodukte als die zugelassenen IT-Sicherheitsprodukte für VS-IT aus?
3. Welche genauen Produkttypen von IT-Sicherheitsprodukten, die für sensitive, aber nicht eingestufte Informationen im Behördenbereich eingesetzt werden können, sind in welchen Bereichen begrenzt von der Zulassungsregelung betroffen?
4. Welche Produkttypen von IT-Sicherheitsprodukten umfasst für welche Bereiche gemäß der Unterscheidung des BSI bei IT-Sicherheitsprodukten solche IT-Sicherheitsprodukte, die vom BSI zugelassen sein sollen, und um welche Ausnahmen genau handelt es sich, falls keine geeigneten zugelassenen Produkte zur Verfügung stehen?
5. Ist das Amt des IT-Sicherheitsbeauftragten einer Bundesverwaltung oder einer Bundesbehörde bei der Auswahl eines zu beschaffenden IT-Sicherheitsprodukts beteiligt, und wenn ja, wie genau ist es daran beteiligt, und bei welchen Bundesverwaltungen und Bundesbehörden ist das regelmäßig der Fall (bitte auflisten)?
6. Plant die Bundesregierung, für den vom Bundesinnenministerium in seiner Cybersicherheitsagenda vorgeschlagenen CISO Bund (CISO = Chief Information Security Officer) Kompetenzen (siehe Cybersicherheitsagenda des BMI, S. 10) im Bereich der Beschaffung von IT-Sicherheitsprodukten für die Bundesverwaltung zu verankern, und wenn ja, welche?
7. Unter welchen Umständen und Bedingungen hinsichtlich Erfüllung von CC, Reputation, Inhaberstruktur und Firmensitz des Herstellers darf eine Bundesbehörde eine produktscharfe Ausschreibung für ein IT-Sicherheitsprodukt an einen Hersteller mit Sitz außerhalb der Europäischen Union (EU) vornehmen?
8. Gelten für IT-Sicherheitsprodukte von Herstellern mit Sitz außerhalb der EU dieselben Zertifizierungs- und Zulassungsregularien des BSI wie für Hersteller von IT-Sicherheitsprodukten mit Sitz innerhalb der EU?

9. Für welche IT-Sicherheitsprodukte wurden seit März 2022 Zertifizierungen für den Einsatz in der Bundesverwaltung nach welchem Zertifizierungsschema beim BSI beantragt, bei welchen davon wurde eine positive Zertifizierungsaussage getroffen, und bei welchen davon befand sich der Hauptsitz des Herstellers des IT-Sicherheitsprodukts außerhalb der EU (bitte nach Produktname, Art der beantragten Zertifizierung, Zertifizierungsaussage, Hersteller, Hauptsitz des Herstellers aufschlüsseln) für

   a) IT-Sicherheitsprodukte des Produkttyps Firewall,

   b) IT-Sicherheitsprodukte des Produkttyps Datendiode,

   c) IT-Sicherheitsprodukte des Produkttyps VS Guard,

   d) IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung,

   e) IT-Sicherheitsprodukte des Produkttyps Hypervisor,

   f) IT-Sicherheitsprodukte des Produkttyps Separation Kernel,

   g) IT-Sicherheitsprodukte des Produkttyps Mobile Device Management,

   h) IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement,

   i) IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente,

   j) IT-Sicherheitsprodukte des Produkttyps Key-Management-Software,

   k) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme,

   l) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme,

   m) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen,

   n) IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung,

   o) IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung,

   p) IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger,

   q) IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung,

   r) IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung,

   s) IT-Sicherheitsprodukte des Produkttyps Funkgeräte,

   t) IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung,

   u) IT-Sicherheitsprodukte des Produkttyps VPN-Client,

   v) IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung,

   w) IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger,

   x) IT-Sicherheitsprodukte des Produkttyps VPN-Gateway,

   y) IT-Sicherheitsprodukte des Produkttyps Datenschleusen (optional auch mit Datenwäschekomponente),

   z) IT-Sicherheitsprodukte Verschlüsselung Layer 1,

   aa) IT-Sicherheitsprodukte Verschlüsselung Layer 2,

   bb) IT-Sicherheitsprodukte des Produkttyps Intrusion Detection System,

   cc) IT-Sicherheitsprodukte Threat Detection System?

10. Für welche IT-Sicherheitsprodukte wurden seit März 2022 Zulassungen für den Einsatz in der Bundesverwaltung durch welchen behördlichen Anwender beim BSI beantragt, bei welchen davon wurde eine positive Zulassungsaussage getroffen, und bei welchen davon befand sich der Hauptsitz des Herstellers des IT-Sicherheitsprodukts außerhalb der EU (bitte nach Produktname, beantragendem behördlichen Anwender samt des ihm zuzuordnenden Geschäftsbereichs der Bundesregierung, Zulassungsaussage, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln) für

    a) IT-Sicherheitsprodukte des Produkttyps Firewall,

    b) IT-Sicherheitsprodukte des Produkttyps Datendiode,

    c) IT-Sicherheitsprodukte des Produkttyps VS Guard,

    d) IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung,

    e) IT-Sicherheitsprodukte des Produkttyps Hypervisor,

    f) IT-Sicherheitsprodukte des Produkttyps Separation Kernel,

    g) IT-Sicherheitsprodukte des Produkttyps Mobile Device Management,

    h) IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement,

    i) IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente,

    j) IT-Sicherheitsprodukte des Produkttyps Key-Management-Software,

    k) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme,

    l) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme,

    m) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen,

    n) IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung,

    o) IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung,

    p) IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger,

    q) IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung,

    r) IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung,

    s) IT-Sicherheitsprodukte des Produkttyps Funkgeräte,

    t) IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung,

    u) IT-Sicherheitsprodukte des Produkttyps VPN-Client,

    v) IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung,

    w) IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger,

    x) IT-Sicherheitsprodukte des Produkttyps VPN-Gateway,

    y) IT-Sicherheitsprodukte des Produkttyps Datenschleusen (optional auch mit Datenwäschekomponente),

    z) IT-Sicherheitsprodukte Verschlüsselung Layer 1,

    aa) IT-Sicherheitsprodukte Verschlüsselung Layer 2,

    bb) IT-Sicherheitsprodukte des Produkttyps Intrusion Detection System,

    cc) IT-Sicherheitsprodukte Threat Detection System?

11. Für welche IT-Sicherheitsprodukte hat die Bundesverwaltung inklusive der IT-Dienstleister des Bundes für welchen behördlichen Anwender der Bundesverwaltung inklusive der IT-Dienstleister des Bundes seit März 2022 Verträge zur Beschaffung von IT-Sicherheitsprodukten geschlossen (bitte nach Produktname, Geschäftsbereich der vertragsschließenden Bundesbehörde, bedarfstragendem behördlichen Anwender, Art der Zertifizierung beziehungsweise Zulassungsaussage des beschafften IT-Sicherheitsprodukts, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln) für

    a) IT-Sicherheitsprodukte des Produkttyps Firewall,

    b) IT-Sicherheitsprodukte des Produkttyps Datendiode,

    c) IT-Sicherheitsprodukte des Produkttyps VS Guard,

    d) IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung und Abwehr,

    e) IT-Sicherheitsprodukte des Produkttyps Hypervisor,

    f) IT-Sicherheitsprodukte des Produkttyps Separation Kernel,

    g) IT-Sicherheitsprodukte des Produkttyps Mobile Device Management,

    h) IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement,

    i) IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente,

    j) IT-Sicherheitsprodukte des Produkttyps Key-Management-Software,

    k) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme,

    l) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme,

    m) IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen,

    n) IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung,

    o) IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung,

    p) IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger,

    q) IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung,

    r) IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung,

    s) IT-Sicherheitsprodukte des Produkttyps Funkgeräte,

    t) IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung,

    u) IT-Sicherheitsprodukte des Produkttyps VPN-Client,

    v) IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung,

    w) IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger,

    x) IT-Sicherheitsprodukte des Produkttyps VPN-Gateway,

    y) IT-Sicherheitsprodukte des Produkttyps Datenschleusen (optional auch mit Datenwäschekomponente),

    z) IT-Sicherheitsprodukte Verschlüsselung Layer 1,

    aa) IT-Sicherheitsprodukte Verschlüsselung Layer 2,

    bb) IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 3,

cc) IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 4,

dd) IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 7,

ee) IT-Sicherheitsprodukte des Produkttyps Web Application Firewall,

ff) IT-Sicherheitsprodukte des Produkttyps Email Security Gateway,

gg) IT-Sicherheitsprodukte des Produkttyps EDR (Endpoint Detection and Response), NDR (Network Detection and Response), XDR (Extended Detection and Response), Device/Port/Schnittstellenkontrolle, UTM (unified Threat Management), Backup/Recovery, DLP (Data Loss Prevention), Archivierung, ersetzendes Scannen, TR-ESOR Langzeitarchivierung, Labeling und APT-Abwehr (APT = Advanced Persistent Threat), ISMS (Information Security Management System) und SIEM (Security Information and Event Management),

hh) IT-Sicherheitsprodukte Threat Detection System?

12. Bei welchen der in Frage 11 erfragten IT-Sicherheitsprodukte befand sich der Hauptsitz des Herstellers des IT-Sicherheitsprodukts außerhalb der EU (bitte analog zu Frage 11 nach Produktname, Hersteller, Hauptsitz des Herstellers aufschlüsseln)?

13. Welche Form des Vergabeverfahrens (z. B. Teilnahmewettbewerb, EU-weite Ausschreibung, freihändige Vergabe, produktscharfe Ausschreibung, Vergabeverordnung Verteidigung und Sicherheit – VSVgV) wurde jeweils für die in Frage 11 erfragten IT-Sicherheitsprodukte gewählt, und wann war der jeweils letzte Zeitpunkt für die Ausschreibung für das jeweilige IT-Sicherheitsprodukt (bitte analog zu Frage 11 nach Produktnamen, gewähltem Vergabeverfahren, Zeitpunkt der letzten Ausschreibung aufschlüsseln)?

14. Welche der in Frage 11 erfragten IT-Sicherheitsprodukte kommen seit Vertragsschluss zur Beschaffung in der Bundesverwaltung bei welchem behördlichen Anwender jeweils tatsächlich zum Einsatz, und für welche der in Frage 11 erfragten IT-Sicherheitsprodukte wurden nach Vertragsschluss zur Beschaffung keine Abrufe durch die Bundesverwaltung getätigt (bitte analog zu Frage 11 aufschlüsseln)?

15. Wie hoch ist jeweils die Anzahl der Behörden, die die in Frage 11 erfragten IT-Sicherheitsprodukte in ihrer Verwaltung verwenden (bitte analog zu Frage 11 nach Produktnamen, Anzahl verwendender Bundesbehörden inklusive IT-Dienstleister des Bundes und dem ihr zuzuordnenden Geschäftsbereich der Bundesregierung aufschlüsseln)?

16. Wie hoch ist jeweils die Anzahl der Lizenzen für die in Frage 11 erfragten IT-Sicherheitsprodukte, die die Bundesverwaltung inklusive der IT-Dienstleister des Bundes für welchen behördlichen Anwender der Bundesverwaltung inklusive der IT-Dienstleister des Bundes jeweils bezogen hat (bitte analog zu Frage 11 nach Produktnamen, produktverwendenden Bundesbehörden, zuzuordnendem Geschäftsbereich der Bundesregierung und jeweiliger Anzahl der Produktlizenzen aufschlüsseln)?

17. Wie hoch ist jeweils die Anzahl der Installationen der in Frage 11 erfragten IT-Sicherheitsprodukte in den jeweils produktverwendenden Bundesbehörden inklusive der IT-Dienstleister des Bundes (bitte analog zu Frage 11 nach Produktnamen, produktverwendenden Bundesbehörden, zuzuordnendem Geschäftsbereich der Bundesregierung und jeweiliger Anzahl der Installationen aufschlüsseln)?

18. Wie stellt sich bei den in Frage 11 erfragten IT-Sicherheitsprodukten nach Kenntnis der Bundesregierung die Lieferkette hinsichtlich Transparenz von Inhaberstruktur und Firmensitz (nach Veröffentlichung der Panama Papers vom Bund gefordert) jeweils dar (bitte analog zu Frage 11 jeweils nach Produktnamen, Produkthersteller, Produktintegrator, Produktbetrieb, Produktwartung, Produktlieferant aufschlüsseln)?

19. Welche und wie viele der in der Antwort zu Frage 11 genannten Hersteller sind über welchen Zeitraum geheimschutzbetreut nach SÜG?

20. Für wie viele Mitarbeiterinnen und Mitarbeiter von Herstellern von IT-Sicherheitsprodukten, deren IT-Sicherheitsprodukte in der Bundesverwaltung inklusive der IT-Dienstleister des Bundes, zum Einsatz kommen, wurde ein Sicherheitsüberprüfungsverfahren gemäß Sicherheitsüberprüfungsgesetz durchgeführt (bitte nach Land des Sitzes des Herstellers der sicherheitsüberprüften Mitarbeiterinnen und Mitarbeiter aufschlüsseln)?

21. Betrachtet die Bundesregierung Technologien im Bereich der Cybersicherheit als Schlüsseltechnologien?

    a) Wenn ja, welche Technologien im Bereich der Cybersicherheit sind das genau?

    b) Wenn nein, plant die Bundesregierung, Technologien im Bereich der Cybersicherheit als Schlüsseltechnologien zu definieren, und welche genau?

22. Welches Ressort der Bundesregierung wird federführend für die Erfüllung des in der Nationalen Sicherheitsstrategie festgestellten Bedarfs eines „[…] gezielten Auswahlprozesses, der Wissensentwicklung und -verbreitung, der Rahmensetzung, der Ressourcenmobilisierung und Marktentwicklung für strategische Technologielinien“ (Nationale Sicherheitsstrategie, Bundestagsdrucksache 20/7220, S. 57) zuständig sein?

23. Welche strategischen Technologielinien im Zusammenhang mit digitaler Souveränität meint die Bundesregierung genau (bitte vollständig aufzählen)?

24. Was meint die Bundesregierung genau mit dem Auswahlprozess zu strategischen Technologielinien?

25. Welche Kriterien legt die Bundesregierung in diesem Auswahlprozess zur konkreten Auswahl der strategischen Technologielinien an?

26. Welche Förderprogramme der Bundesregierung zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität liefen und laufen seit dem Jahr 2018 (bitte jeweils die finanzielle Ausstattung jeweils für die Jahresscheiben von 2018 bis 2023 nennen)?

27. Plant die Bundesregierung derzeit, neue Förderprogramme zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität aufzulegen, und wenn ja, wie hoch wird die von der Bundesregierung angedachte finanzielle Ausstattung sein?

28. Welche Veranstaltungen der Bundesregierung (Gipfel, Wettbewerbe, Hackathons) zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität wurden seit dem Jahr 2018 organisiert und durchgeführt (bitte nach Veranstaltungsformat, Veranstaltung und Veranstaltungstermin aufschlüsseln)?

29. Welche Veranstaltungen plant die Bundesregierung derzeit im thematischen Zusammenhang mit der Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität?

30. Welche Kooperationen mit Universitäten und Hochschulen pflegt die Bundesregierung zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität?

31. Welche Kooperationen mit öffentlichen Forschungseinrichtungen pflegt die Bundesregierung zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität?

32. Welche Kooperationen mit privaten Forschungseinrichtungen pflegt die Bundesregierung zur Wissensentwicklung und Wissensverbreiterung zu Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität?

33. In Höhe welcher Summe sind finanzielle Mittel im Bundeshaushalt 2023 zur Erforschung und Entwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität hinterlegt (bitte nach Einzelplan, Kapitel und Titel aufschlüsseln)?

34. In Höhe welcher Summe sind finanzielle Mittel im Regierungsentwurf des Bundeshaushalts 2024 zur Erforschung und Entwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität enthalten (bitte nach Einzelplan, Kapitel und Titel aufschlüsseln)?

35. Ist es gesetzlich und vergaberechtlich möglich, bestimmte Hersteller von IT-Sicherheitsprodukten aufgrund der Verortung ihres Hauptsitzes in einem bestimmten Land kategorisch von Auftragsvergaben im Bereich der IT-Sicherheitsprodukte für die Bundesverwaltung auszuschließen, und wenn nein, plant die Bundesregierung dahin gehende Rechtsänderungen oder würde diese unterstützen?

36. Sind bestimmte Hersteller von IT-Sicherheitsprodukten aufgrund der Verortung ihres Hauptsitzes in einem bestimmten Land kategorisch von Auftragsvergaben im Bereich der IT-Sicherheitsprodukte für die Bundesverwaltung ausgeschlossen, und wenn ja, um welche Länder handelt es sich dabei aus welchen Gründen?

37. Plant die Bundesregierung, bestimmte Hersteller von IT-Sicherheitsprodukten aufgrund der Verortung ihres Hauptsitzes in einem bestimmten Land kategorisch von Auftragsvergaben im Bereich der IT-Sicherheitsprodukte für die Bundesverwaltung auszuschließen, und wenn ja, um welche Länder handelt es sich dabei aus welchen Gründen?

38. Plant die Bundesregierung, einerseits im Zuge der vom BMI in seiner Cybersicherheitsagenda angekündigten Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und andererseits der von der Bundesregierung in ihrer Digitalstrategie angekündigten ganzheitlichen Stärkung des Cybersicherheitsökosystems für die zuständigen Cybersicherheitsbehörden umfangreiche Ausnahmen vom Beschaffungsrecht des Bundes vorzusehen, damit deutsche IT-Sicherheitsbehörden zur Erfüllung ihres Auftrags innerhalb kürzester Zeit neueste Technologien und Software für die IT-Sicherheit und die Cyberabwehr beschaffen können?

39. Plant die Bundesregierung, einerseits im Zuge der vom BMI in seiner Cybersicherheitsagenda angekündigten Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und andererseits der von der Bundesregierung in ihrer Digitalstrategie angekündigten ganzheitlichen Stärkung des Cybersicherheitsökosystems künftig bei IT-Beschaffungsvorhaben des Bundes einen bestimmten Anteil der Sachmittel für IT-Vorhaben des Bundes für Cybersicherheit aufzuwenden (wenn nein, bitte begründen)?

40. Plant die Bundesregierung, einerseits im Zuge der vom BMI in seiner Cybersicherheitsagenda angekündigten Ausstattung der Bundesbehörden mit weiterentwickelten IT-Produkten und andererseits der von der Bundesregierung in ihrer Digitalstrategie angekündigten ganzheitlichen Stärkung des Cybersicherheitsökosystems im Bereich der materiellen Ausrüstung in bestimmten Fällen den Anbieterkreis bei Vergaben von Aufträgen zur Beschaffung von IT-Sicherheitsprodukten auf nationale Lieferketten zu beschränken, und wenn ja, in welchen Fällen?

41. Macht die Produktzertifizierung des BSI auch zukunftsbezogene Aussagen zur Sicherheit für Updates oder Patches eines zu zertifizierenden IT-Sicherheitsprodukts, und wenn nein, plant die Bundesregierung, dahin gehende Änderungen vorzunehmen?

42. Welche Vergabekriterien im Zusammenhang mit nationalen Sicherheitsaspekten, die über die reine technologische Sicherheit hinausgehen, sind in Vergabeverfahren zu IT-Sicherheitsprodukten berücksichtigt beziehungsweise spielen dort eine Rolle?

    a) Ist die Freiheit von sogenannten Backdoors (auch Hintertüren oder Trapdoors) ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

    b) Ist die Vertrauenswürdigkeit hinsichtlich der Inhaberstruktur von Herstellern von IT-Sicherheitsprodukten ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

    c) Ist der Firmenhauptsitz von Herstellern von IT-Sicherheitsprodukten ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

    d) Ist die nachhaltige Geheimschutzbetreuung des Herstellers eines in der Bundesverwaltung verwendeten IT-Sicherheitsprodukts ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

    e) Sind die Lieferketten eines Herstellers von IT-Sicherheitsprodukten ein Vergabekriterium in Vergabeverfahren zu IT-Sicherheitsprodukten, und wenn nein, plant die Bundesregierung dahin gehende Änderungen?

43. Welche Förderprogramme der Bundesregierung zur nationalen industriellen Marktentwicklung für Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität liefen und laufen seit dem Jahr 2018 (bitte jeweils die finanzielle Ausstattung jeweils für die Jahresscheiben von 2018 bis 2023 nennen)?

44. Plant die Bundesregierung, derzeit neue Förderprogramme zur nationalen industriellen Marktentwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität aufzulegen, und wenn ja, wie hoch wird die von der Bundesregierung angedachte finanzielle Ausstattung sein?

45. Welche Transferstellen, Cluster und Netzwerke hat die Bundesregierung für den Wissenstransfer von der Wissenschaft in die Industrie bezüglich Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität bisher eingerichtet (bitte immer Jahr der Einrichtung nennen)?

46. Plant die Bundesregierung derzeit, weitere Transferstellen, Cluster und Netzwerke für den Wissenstransfer von der Wissenschaft in die Industrie bezüglich Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität einzurichten, und wenn ja, welche?

47. In Höhe welcher Summe sind finanzielle Mittel im Bundeshaushalt 2023 zur Marktentwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität hinterlegt (bitte nach Einzelplan, Kapitel und Titel aufschlüsseln)?

48. In Höhe welcher Summe sind finanzielle Mittel im Regierungsentwurf des Bundeshaushalts 2024 zur Marktentwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität enthalten (bitte nach Einzelplan, Kapitel und Titel aufschlüsseln)?

49. Welche Beratungs- und Transferstellen hat die Bundesregierung für die Bundesverwaltung zu Fragen der Beschaffung von IT-Sicherheitsprodukten eingerichtet (bitte immer Jahr der Einrichtung nennen)?

Berlin, den 14. August 2023

Friedrich Merz, Alexander Dobrindt und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333