Deutscher Bundestag **Drucksache 20/14226**

20. Wahlperiode 17.12.2024

Kleine Anfrage

der Fraktion der CDU/CSU

Digitale Souveränität in der Bundesverwaltung – Beschaffung und Einsatz von IT-(Sicherheits-)Produkten durch den Bund als öffentlichen Auftraggeber

Am 19. Juli 2024 kam es weltweit zu IT-Ausfällen in zahlreichen Branchen. Betroffen waren auch Unternehmen und Betreiber Kritischer Infrastrukturen in Deutschland (www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240719_weltweite_IT-Ausfaelle.html). Ein fehlerhaftes Update einer IT-Sicherheitssoftware einer US-amerikanischen Firma sorgte für Abstürze von Computern mit Windows-Betriebssystemen. Gleichzeitig gab es auch Probleme bei der Verbindung zu Apps und Dienstleistungen des Clouddienstes Microsoft 365 innerhalb von Microsofts Cloudplattform Azure. Durch die Vorfälle kam es beispielsweise zur vorübergehenden Einstellung des Flugbetriebs am Flughafen Berlin-Brandenburg, der Schließung von Ambulanzen und der Verschiebung von aufschiebbaren Eingriffen am Universitätsklinikum Schleswig-Holstein und zu einem späteren Handelsstart an der Börse London. Die technischen Probleme hatten auch Folgen für Stadtverwaltungen. In Pforzheim etwa waren der E-Mail-Verkehr und die Telefonanlage gestört und das Bürgerzentrum, die Ausländerbehörde sowie die KfZ-Zulassungsbehörde nur eingeschränkt erreichbar (www.spiegel.de/netzwelt/web/flughafen-ber-muss-nach-it-stoerung-betrieb-einstellen-weltweite-netz-ausfaelle-a-f318d93e-aacd-4f46-870b-6de1fd9a8b6d). In der Presse firmierte das Ereignis als „größter IT-Ausfall der Geschichte“ (www.businessinsider.de/wirtschaft/crowdstrike-diese-firma-steckt-hinter-groesster-it-panne-der-geschichte/).

Die Bundesverwaltung und die Bundesregierung selbst waren von dem IT-Vorfall zwar nicht betroffen (www.spiegel.de/netzwelt/web/flughafen-ber-muss-nach-it-stoerung-betrieb-einstellen-weltweite-netz-ausfaelle-a-f318d93e-aacd-4f46-870b-6de1fd9a8b6d). Allerdings wurde die Brisanz von digitalpolitischen Abhängigkeiten und daher die Relevanz digitaler Souveränität im Allgemeinen deutlich. Das gilt erst recht vor dem Hintergrund, dass die Bundesverwaltung vom einwandfreien Funktionieren und der uneingeschränkten Verfügbarkeit von IT-Systemen abhängig ist (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).

In diesem Kontext gibt es eine Reihe von Vorschlägen für Maßnahmen zur Steigerung der digitalen Souveränität. Eine Studie des Leibniz-Zentrums für Europäische Wirtschaftsforschung (ZEW) in Mannheim vom Oktober 2024, die im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) angefertigt wurde, betont wie schon in der Vorgängerstudie aus dem Jahr 2021,

dass „…die Politik die digitale Souveränität mit einer innovativen Beschaffung, die die Spezifika von Start-ups oder Open-Source-Lösungen berücksichtigt, unterstützen [kann]. Dies kann zur Entstehung von alternativen Angeboten beitragen und Hürden hinsichtlich Interoperabilität und Lock-in-Effekten entgegenwirken.“ (de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-schwerpunkt-digitale-souveraenitaet.pdf?__blob=publicationFile&v=5, S. 42) Insbesondere dem Bereich der IT-Sicherheitstechnologien sollte die Bundesregierung den Ergebnissen der Studie zufolge die höchste Priorität bei der Vermeidung von digitalen Abhängigkeiten einräumen (de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-schwerpunkt-digitale-souveraenitaet.pdf?__blob=publicationFile&v=5, S. 25-26).

Die 2. Digitalministerkonferenz weiß offenbar um diese Priorisierungsnotwendigkeit. Mit ihrem Beschluss vom 18. Oktober 2024 stellt sie fest, dass angesichts der zunehmenden Digitalisierung EU-Mitgliedstaaten in der Lage sein müssen, Leistungen im Bereich Cybersicherheit einschließlich Informationssicherheit schnellst-möglich zu beschaffen, um ihre wesentlichen Sicherheitsinteressen zu wahren. Die bisherigen Vorschriften des Vergaberechts erlauben weitreichende Ausnahmen für militärische Zwecke. Sie schlägt vor, Änderungen im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) dahingehend vorzunehmen, damit auch die Beschaffung von Cyber- und Informationssicherheitsleistungen mit Ausnahmen belegt werden können beziehungsweise jedenfalls gesichert in den Vergabebereich Verteidigung und Sicherheit fallen. Denn nach aktuellem Stand ist es den EU-Mitgliedstaaten verwehrt, in vergleichbarer Art und Weise zu Beschaffungen für militärische Zwecke Beschaffungen zur Härtung der Cyber- und Informationssicherheit tätigen zu können. Den Mitgliedstaaten steht im Bereich Cyber- und Informationssicherheit aktuell keine mit Artikel 346 Absatz 1 Buchstabe b) AEUV vergleichbare Rechtsgrundlage zur Verfügung. Zudem wurde die in Artikel 346 Absatz 2 referenzierte Liste von Waren, Gütern und Dienstleistungen, auf die die Ausnahmen angewendet werden können, seit 15. April 1958 nicht mehr überarbeitet. Insbesondere stellt § 117 Absatz 1 Nummer 1 des Gesetzes gegen Wettbewerbsbeschränkungen (im Folgenden kurz: GWB) der 2. Digitalministerkonferenz zufolge keine vergleichbare Rechtsgrundlage dar. Zwar erlaubt § 117 Absatz 1 Nummer 1 GWB seinem Wortlaut nach Ausnahmen vom Vergaberecht auch dann, wenn ein Auftrag nicht der Erzeugung oder dem Handel mit Kriegsmaterial dient, sondern ausschließlich Verteidigungs- und Sicherheitsaspekte umfasst. Allerdings ist der Prüfungsmaßstab des § 117 Absatz 1 Nummer 1 GWB deutlich strenger (www.berlin-brandenburg.de/wp-content/uploads/TOP_9_SH_Beschluss_Leistungsbeschaffung_Info-_und-Cybersicherheit.pdf).

Weiterhin bereitete das Bundesministerium für Wirtschaft und Klimaschutz unabhängig davon im Rahmen der Wachstumsinitiative ein sogenanntes Vergabetransformationspaket zur Reform des Vergaberechts ober- und unterhalb der EU-Schwellenwerte vor, insbesondere mit dem Ziel, Vergabeverfahren zu beschleunigen. Das Vorhaben beabsichtigt des Weiteren eine neue Möglichkeit einzuführen, Unternehmen aus bestimmten Drittstaaten in kritischen Bereichen von Auftragsvergaben auszuschließen. Darüber hinaus sollten umweltbezogene und soziale Aspekte als Vergabekriterien definiert werden (background.tagesspiegel.de/digitalisierung-und-ki/briefing/wirtschaftsministerium-will-vergaberecht-per-gesetz-vereinfachen; www.bmwk.de/Redaktion/DE/Pressemitteilungen/2024/09/20240930-habeck-vergabetransformation.html; background.tagesspiegel.de/digitalisierung-und-ki/briefing/vergabetransformationspaket-haelt-es-was-es-verspricht). Der zugehörige Gesetzentwurf wurde am 27. November 2024 im Kabinett von der Bundesregierung verabschiedet (www.bundesregierung.de/breg-de/bundesregierung/bundeskanzleramt/novelle-vergaberecht-2322048).

Vor diesem Hintergrund möchten die Fragesteller aufbauend auf ihrer Kleinen Anfrage vom 23. August 2023, die von der Bundesregierung am 9. Oktober 2023 auf Bundestagsdrucksache 20/8707 (dserver.bundestag.de/btd/20/087/2008707.pdf) beantwortet wurde, aktuelle Sachstände zur Entwicklung, zur Beschaffung und zum Einsatz von IT-Sicherheitsprodukten in der Bundesverwaltung sowie die Bestrebungen der Bundesregierung zur Umsetzung von Vorschläge zur Steigerung der digitalen Souveränität im Bereich der IT-Sicherheitsanwendungen abfragen (Hinweis: Bei den folgenden Fragen mit Bezug zur Bundesverwaltung sind die Nachrichtendienste des Bundes auszunehmen).

Wir fragen die Bundesregierung:

1. Für welche IT-Sicherheitsprodukte wurden mit Referenz zur Antwort der Bundesregierung auf die Frage 9 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 seit 4. Oktober 2023 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)?
   a) Für IT-Sicherheitsprodukte des Produkttyps Firewall?
   b) Für IT-Sicherheitsprodukte des Produkttyps Datendiode?
   c) Für IT-Sicherheitsprodukte des Produkttyps VS Guard?
   d) Für IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung?
   e) Für IT-Sicherheitsprodukte des Produkttyps Hypervisor?
   f) Für IT-Sicherheitsprodukte des Produkttyps Separation Kernel?
   g) Für IT-Sicherheitsprodukte des Produkttyps Mobile Device Management?
   h) Für IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement?
   i) Für IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente?
   j) Für IT-Sicherheitsprodukte des Produkttyps Key-Management-Software?
   k) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme?
   l) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme?
   m) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen?
   n) Für IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung?
   o) Für IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung?
   p) Für IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger?
   q) Für IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung?
   r) Für IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung?

s) Für IT-Sicherheitsprodukte des Produkttyps Funkgeräte?

t) Für IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung?

u) Für IT-Sicherheitsprodukte des Produkttyps VPN-Client?

v) Für IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung?

w) Für IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger?

x) Für IT-Sicherheitsprodukte des Produkttyps VPN-Gateway?

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

z) Für IT-Sicherheitsprodukte Verschlüsselung Layer 1?

aa) Für IT-Sicherheitsprodukte Verschlüsselung Layer 2?

bb) Für IT-Sicherheitsprodukte Für IT-Sicherheitsprodukte des Produkttyps Intrusion Detection System?

cc) Für IT-Sicherheitsprodukte Threat Detection System?

2. Für welche IT-Sicherheitsprodukte und -dienste 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)?

   a) Für IT-Sicherheitsprodukte und -dienste des Produkttyps DDoS-Schutz?

   b) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Web Application Firewall?

   c) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Domain Name Server?

   d) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Reverse Proxy?

   e) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Content Delivery Network?

3. Für welche IT-Sicherheitsprodukte mit Referenz zur Antwort der Bundesregierung auf die Frage 10 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 wurden seit 4. Oktober 2023 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, beantragender behördlicher Anwender samt des ihm zuzuordnenden Geschäftsbereichs der Bundesregierung, Zulassungsaussage, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln)?

   a) Für IT-Sicherheitsprodukte des Produkttyps Firewall?

   b) Für IT-Sicherheitsprodukte des Produkttyps Datendiode?

   c) Für IT-Sicherheitsprodukte des Produkttyps VS Guard?

   d) Für IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung?

e) Für IT-Sicherheitsprodukte des Produkttyps Hypervisor?

f) Für IT-Sicherheitsprodukte des Produkttyps Separation Kernel?

g) Für IT-Sicherheitsprodukte des Produkttyps Mobile Device Management?

h) Für IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement?

i) Für IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente?

j) Für IT-Sicherheitsprodukte des Produkttyps Key-Management-Software?

k) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme?

l) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme?

m) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen?

n) Für IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung?

o) Für IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung?

p) Für IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger?

q) Für IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung?

r) Für IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung?

s) Für IT-Sicherheitsprodukte des Produkttyps Funkgeräte?

t) Für IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung?

u) Für IT-Sicherheitsprodukte des Produkttyps VPN-Client?

v) Für IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung?

w) Für IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger?

x) Für IT-Sicherheitsprodukte des Produkttyps VPN-Gateway?

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

z) Für IT-Sicherheitsprodukte Verschlüsselung Layer 1?

aa) Für IT-Sicherheitsprodukte Verschlüsselung Layer 2?

bb) Für IT-Sicherheitsprodukte Für IT-Sicherheitsprodukte des Produkttyps Intrusion Detection System?

cc) Für IT-Sicherheitsprodukte Threat Detection System?

4. 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, beantragender behördlicher Anwender samt des ihm zuzuordnenden Geschäftsbereichs der Bundesregierung, Zulassungsaussage, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln)?

a) Für IT-Sicherheitsprodukte und -dienste des Produkttyps DDoS-Schutz?

b) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Web Application Firewall?

c) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Domain Name Server?

d) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Reverse Proxy?

e) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Content Delivery Network?

5. Handelt es sich bei der genua GmbH um einen bundesbehördlichen Bedarfsträger, und wenn nein, warum ist es unter Bezugnahme auf Anlage 1 zu der Antwort der Bundesregierung auf Frage 10 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 möglich, dass unter Bezugnahme auf die Antwort der Bundesregierung auf Frage 4 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707, wonach eine Zulassung für ein Produkt nur durch einen bundesbehördlichen Bedarfsträger beantragt werden kann, die genua GmbH nicht nur der Hersteller, sondern auch gleichzeitig der Antragsteller für die Zulassung des Produkts vom Produkttyp Firewall mit dem Namen genuate NdB WebRTC ist?

6. Für welche IT-Sicherheitsprodukte mit Referenz zur Antwort der Bundesregierung auf die Frage 11 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 hat die Bundesverwaltung inklusive der IT-Dienstleister des Bundes für welchen behördlichen Anwender der Bundesverwaltung inklusive der IT-Dienstleister des Bundes seit dem 4. Oktober 2023 Verträge zur Beschaffung von IT-Sicherheitsprodukten geschlossen (bitte nach Produktname, Geschäftsbereich der vertragsschließenden Bundesbehörde, bedarfstragender behördlicher Anwender, Art der Zertifizierung beziehungsweise Zulassungsaussage des beschafften IT-Sicherheitsprodukts, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln)?

a) Für IT-Sicherheitsprodukte des Produkttyps Firewall?

b) Für IT-Sicherheitsprodukte des Produkttyps Datendiode?

c) Für IT-Sicherheitsprodukte des Produkttyps VS Guard?

d) Für IT-Sicherheitsprodukte des Produkttyps Schadsoftwareerkennung und Abwehr

e) Für IT-Sicherheitsprodukte des Produkttyps Hypervisor?

f) Für IT-Sicherheitsprodukte des Produkttyps Separation Kernel?

g) Für IT-Sicherheitsprodukte des Produkttyps Mobile Device Management?

h) Für IT-Sicherheitsprodukte des Produkttyps Netzwerkmanagement?

i) Für IT-Sicherheitsprodukte des Produkttyps Schlüsselspeicher- und Verteilkomponente?

j) Für IT-Sicherheitsprodukte des Produkttyps Key-Management-Software?

k) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Funksysteme?

l) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für Satellitensysteme?

m) Für IT-Sicherheitsprodukte des Produkttyps Verschlüsselungsgerät für analoge Leitungen?

n) Für IT-Sicherheitsprodukte des Produkttyps Dateiverschlüsselung?

o) Für IT-Sicherheitsprodukte des Produkttyps Festplattenverschlüsselung?

p) Für IT-Sicherheitsprodukte des Produkttyps Sicherer mobiler Datenträger?

q) Für IT-Sicherheitsprodukte des Produkttyps Faxverschlüsselung?

r) Für IT-Sicherheitsprodukte des Produkttyps Telefonverschlüsselung?

s) Für IT-Sicherheitsprodukte des Produkttyps Funkgeräte?

t) Für IT-Sicherheitsprodukte des Produkttyps E-Mail-Verschlüsselung?

u) Für IT-Sicherheitsprodukte des Produkttyps VPN-Client?

v) Für IT-Sicherheitsprodukte des Produkttyps Sichere mobile Lösung?

w) Für IT-Sicherheitsprodukte des Produkttyps Sicherer Messenger?

x) Für IT-Sicherheitsprodukte des Produkttyps VPN-Gateway?

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

z) Für IT-Sicherheitsprodukte Verschlüsselung Layer 1?

aa) Für IT-Sicherheitsprodukte Verschlüsselung Layer 2?

bb) Für IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 3?

cc) Für IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 4?

dd) Für IT-Sicherheitsprodukte des Produkttyps DDoS-Schutz Layer 7?

ee) Für IT-Sicherheitsprodukte des Produkttyps Web Application Firewall?

ff) Für IT-Sicherheitsprodukte des Produkttyps Email Security Gateway?

gg) Für 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 (Advanced Persistent Threat)- Abwehr, ISMS (Information Security Management System) und SIEM (Security Information and Event Management)?

hh) Für IT-Sicherheitsprodukte Threat Detection System?

7. 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, bedarfstragender behördlicher Anwender, Art der Zertifizierung beziehungsweise Zulassungsaussage des beschafften IT-

Sicherheitsprodukts, Hersteller des IT-Sicherheitsprodukts, Hauptsitz des Herstellers des IT-Sicherheitsprodukts aufschlüsseln)?

a) Für IT-Sicherheitsprodukte und -dienste des Produkttyps DDoS-Schutz?

b) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Web Application Firewall?

c) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Domain Name Server?

d) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Reverse Proxy?

e) Für IT-Sicherheitsprodukte und -dienste des Produkttyps Content Delivery Network?

8. Welche Behörde der Bundesverwaltung hat unter Bezug auf die Gesamtheit der in Frage 6 abgefragten Informationen Beschaffungen in jeweils wie vielen Fällen durchgeführt und welche Vergabeverordnung (beispielsweise VgV, VSVgV, UVgO) und welche Vergabeverfahren (z. B. nichtoffenes Verfahren mit Teilnahmewettbewerb, Verhandlungsverfahren mit/ohne Teilnahmewettbewerb, wettbewerblicher Dialog mit Teilnahmewettbewerb) wurde dabei wie oft angewandt (bitte nach beschaffender Behörde, Anzahl Beschaffungen, Häufigkeit der dabei gewählten Vergabeverordnung und des ggf. darin gewählten Vergabeverfahrens aufschlüsseln)?

9. Welche Behörde der Bundesverwaltung hat unter Bezug auf die Gesamtheit der in Frage 7 abgefragten Informationen Beschaffungen in jeweils wie vielen Fällen durchgeführt und welche Vergabeverordnung (beispielsweise VgV, VSVgV, UVgO) und welche Vergabeverfahren (z. B. nichtoffenes Verfahren mit Teilnahmewettbewerb, Verhandlungsverfahren mit/ohne Teilnahmewettbewerb, wettbewerblicher Dialog mit Teilnahmewettbewerb) wurde dabei wie oft angewandt (bitte nach beschaffender Behörde, Anzahl Beschaffungen, Häufigkeit der dabei gewählten Vergabeverordnung und des ggf. darin gewählten Vergabeverfahrens aufschlüsseln)?

10. Wann war unter Bezug auf Frage 6 der jeweils letzte Zeitpunkt für die Ausschreibung für das jeweilige IT-Sicherheitsprodukt (bitte nach IT-Sicherheitsprodukt und Zeitpunkt der letzten Ausschreibung aufschlüsseln)?

11. Wann war unter Bezug auf Frage 7 der jeweils letzte Zeitpunkt für die Ausschreibung für das jeweilige IT-Sicherheitsprodukt (bitte nach IT-Sicherheitsprodukt und Zeitpunkt der letzten Ausschreibung aufschlüsseln)?

12. Warum sind unter Bezugnahme auf die Antwort der Bundesregierung auf Frage 13 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707 und der dazugehörenden Anlage 3 zur Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 20/8707 die Informationen nur für die zentral vom Beschaffungsamt geschlossenen Verträge angegeben?

13. Welche der in Frage 6 abgefragten IT-Sicherheitsprodukte kommen seit Vertragsschluss zur Beschaffung in der Bundesverwaltung bei welchem behördlichen Anwender jeweils tatsächlich zum Einsatz und für welche der in Frage 6 abgefragten IT-Sicherheitsprodukte wurden nach Vertragsschluss zur Beschaffung keine Abrufe durch die Bundesverwaltung getätigt (bitte analog zu Frage 6 aufschlüsseln)?

14. Welche der in Frage 7 abgefragten IT-Sicherheitsprodukte kommen seit Vertragsschluss zur Beschaffung in der Bundesverwaltung bei welchem

behördlichen Anwender jeweils tatsächlich zum Einsatz und für welche der in Frage 7 abgefragten IT-Sicherheitsprodukte wurden nach Vertragsschluss zur Beschaffung keine Abrufe durch die Bundesverwaltung getätigt (bitte analog zu Frage 7 aufschlüsseln)?

15. Wie hoch ist jeweils die Anzahl der Behörden, die die in Frage 6 abgefragten IT-Sicherheitsprodukte in ihrer Verwaltung verwenden (bitte analog zu Frage 6 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 Behörden, die die in Frage 7 abgefragten IT-Sicherheitsprodukte in ihrer Verwaltung verwenden (bitte analog zu Frage 7 nach Produktnamen, Anzahl verwendender Bundesbehörden inklusive IT-Dienstleister des Bundes und dem ihr zuzuordnenden Geschäftsbereich der Bundesregierung aufschlüsseln)?

17. Wie hoch ist jeweils die Anzahl der Lizenzen für die in Frage 6 abgefragten 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 6 nach Produktnamen, produktverwendende Bundesbehörden, zuzuordnender Geschäftsbereich der Bundesregierung und jeweilige Anzahl der Produktlizenzen aufschlüsseln)?

18. Wie hoch ist jeweils die Anzahl der Lizenzen für die in Frage 7 abgefragten 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 7 nach Produktnamen, produktverwendende Bundesbehörden, zuzuordnender Geschäftsbereich der Bundesregierung und jeweilige Anzahl der Produktlizenzen aufschlüsseln)?

19. Wie hoch ist jeweils die Anzahl der Installationen der in Frage 6 abgefragten IT-Sicherheitsprodukte in den jeweils produktverwenden Bundesbehörden inklusive der IT-Dienstleister des Bundes (bitte analog zu Frage 6 nach Produktnamen, produktverwendende Bundesbehörden, zuzuordnender Geschäftsbereich der Bundesregierung und jeweilige Anzahl der Installationen aufschlüsseln)?

20. Wie hoch ist jeweils die Anzahl der Installationen der in Frage 7 abgefragten IT-Sicherheitsprodukte in den jeweils produktverwenden Bundesbehörden inklusive der IT-Dienstleister des Bundes (bitte analog zu Frage 7 nach Produktnamen, produktverwendende Bundesbehörden, zuzuordnender Geschäftsbereich der Bundesregierung und jeweilige Anzahl der Installationen aufschlüsseln)?

21. Sollten bei der Beantwortung der Fragen 17 und 19 sowie 18 und 20 deutliche Diskrepanzen zwischen der Anzahl der Lizenzen und der Anzahl der Installationen bei bestimmten IT-Sicherheitsprodukten, die von der Bundesverwaltung für einen behördlichen Anwender zur Nutzung beschafft wurden, zutage treten – wie erklärt sich die Bundesregierung gegebenenfalls diese Diskrepanzen?

22. Sollte im Rahmen der Beantwortung von Frage 6 hervorgehen, dass für die Bundesverwaltung IT-Sicherheitsprodukte von Herstellern mit einem Firmensitz in einem außereuropäischen Staat beschafft wurden – gab es für diese gelisteten und beschafften IT-Sicherheitsprodukte von Herstellern mit einem Firmensitz in einem außereuropäischen Staat zum Beschaffungszeitpunkt Alternativen von Herstellern mit einem Firmensitz in einem Staat des Europäischen Wirtschaftsraums, in der Schweiz oder in

Großbritannien, und wenn ja, warum wurden nicht eine der Alternativen beziehungsweise die Alternativen beschafft (bitte Alternative(n) bei betroffenen IT-Sicherheitsprodukten, Staat, in dem der Firmensitz des Herstellers der Alternative(n) liegt, und Begründungen für Entscheidung gegen die Alternative(n) anführen)?

23. Sollte im Rahmen der Beantwortung von Frage 7 hervorgehen, dass für die Bundesverwaltung IT-Sicherheitsprodukte von Herstellern mit einem Firmensitz in einem außereuropäischen Staat beschafft wurden – gab es für diese gelisteten und beschafften IT-Sicherheitsprodukte von Herstellern mit einem Firmensitz in einem außereuropäischen Staat zum Beschaffungszeitpunkt Alternativen von Herstellern mit einem Firmensitz in einem Staat des Europäischen Wirtschaftsraums, in der Schweiz oder in Großbritannien, und wenn ja, warum wurden nicht eine der Alternativen beziehungsweise die Alternativen beschafft (bitte Alternative(n) bei betroffenen IT-Sicherheitsprodukten, Staat, in dem der Firmensitz des Herstellers der Alternative(n) liegt, und Begründungen für Entscheidung gegen die Alternative(n) anführen)?

24. Welche und wie viele der in der Antwort auf Frage 6 genannten Hersteller sind über welchen Zeitraum geheimschutzbetreut nach SÜG?

25. Welche und wie viele der in der Antwort auf Frage 7 genannten Hersteller sind über welchen Zeitraum geheimschutzbetreut nach SÜG?

26. 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 (SÜG) durchgeführt (bitte aufschlüsseln nach Land des Sitzes des Herstellers der sicherheitsüberprüften Mitarbeiterinnen und Mitarbeiter)?

27. Ist die Apple Inc., die in der Anlage 1 zur Antwort der Bundesregierung auf die Frage 10 der Kleinen Anfrage 20/8707 als Hersteller der Produkte INDIGO 15.x und INDIGO 16.x vom Produkttyp Sichere mobile Lösung, die auch für den Umgang mit Verschlusssachen (VS) gedacht ist (www.golem.de/news/apple-indigo-ein-ios-fuer-die-deutschen-behoerden-2407-187458.html), genannt ist, gemäß dem das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) (www.gesetze-im-internet.de/bsig_2009/) ändernde IT-Sicherheitsgesetz 2.0, wonach jedes Unternehmen, das Produkte zur Nutzung in Verschlusssachen-Umgebungen herstellt und damit als Unternehmen besonderen Interesses gilt (UBI I) (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Regulierte_Unternehmen/UBI/Flyer.pdf?__blob=publicationFile&v=5), seit dem 1. Mai 2023 gegenüber dem BSI bestimmten Pflichten nachkommen muss, den nun in § 8f BSIG festgeschriebenen Pflichten nachgekommen und kommt sie diesen Pflichten nach wie vor nach (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Regulierte_Unternehmen/UBI/Flyer.pdf?__blob=publicationFile&v=5; www.gesetze-im-internet.de/bsig_2009/__2.html; www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf)?

    a) Hat die Apple Inc. innerhalb der festgesetzten Fristen eine Selbsterklärung zur IT-Sicherheit beim BSI vorgelegt, und wenn ja, zu welchem Zeitpunkt genau?

    b) Welche Zertifizierungen im Bereich der IT-Sicherheit wurden in den letzten zwei Jahren gemäß der Selbsterklärung durchgeführt und

welche Prüfgrundlage und welcher Geltungsbereich wurden hierfür festgelegt?

c) Welche sonstigen Sicherheitsaudits oder Prüfungen im Bereich der IT-Sicherheit in den letzten zwei Jahren wurden gemäß der Selbsterklärung durchgeführt und welche Prüfgrundlage und welcher Geltungsbereich wurden hierfür festgelegt?

d) Wie wird gemäß der Selbsterklärung sichergestellt, dass die besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden, und wird dabei der Stand der Technik eingehalten?

e) Hat das BSI auf Grundlage der Selbsterklärung Hinweise zu angemessenen organisatorischen und technischen Vorkehrungen zur Einhaltung des Stands der Technik gegeben?

f) Hat sich die Apple Inc. gleichzeitig mit der Vorlage der Selbsterklärung zur IT-Sicherheit beim BSI registriert und eine zu den üblichen Geschäftszeiten erreichbare Stelle benannt, und wenn ja, wann erfolgte die Registrierung und welche Geschäftsstelle wurde benannt?

g) Hat die Apple Inc. seit dem 1. Mai 2023 dem BSI Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung geführt haben, oder erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung führen können, gemeldet (bitte aufgeschlüsselt nach Störung, technischen Rahmenbedingungen der Störung, vermutete oder tatsächliche Ursachen der Störung, betroffene Informationstechnik, betroffene Einrichtung oder Anlage auflisten)?

h) Wurde der Apple Inc. für das Produkt INDIGO das Sicherheitszertifikat vom BSI erteilt und entsprachen die dazugehörenden informationstechnischen Systeme, Komponenten, Produkte oder Schutzprofile den vom BSI festgelegten Kriterien, und wenn nein, warum nicht?

28. Welche Förderprogramme der Bundesregierung zur Wissensentwicklung und -verbreiterung 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)?

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

30. In Höhe welcher Summe sind finanzielle Mittel im Bundeshaushalt zur Erforschung und Entwicklung von Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität hinterlegt (bitte nach Einzelplan, Kapitel und Titel für die Jahre 2023 und 2024 sowie für den Entwurf der Bundesregierung zum Bundeshaushalt 2025 aufschlüsseln)?

31. Welche Förderprogramme der Bundesregierung zur nationalen industriellen Marktentwicklung für Sicherheitstechnologien im Zusammenhang mit digitaler Souveränität liefen und laufen seit dem Jahr 2018 (bitte je-

weils die finanzielle Ausstattung jeweils für die Jahresscheiben von 2018 bis 2024 nennen)?

32. 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?

33. Warum wird die Vereinbarung des Bundesministeriums des Innern und für Heimat (BMI) sowie des Bundesministeriums der Verteidigung (BMVg) über eine jeweils zur Hälfte getragene Finanzierung der Agentur für Innovationen in der Cybersicherheit (www.basecamp.digital/cyberagentur-vorgruendung-neue-details-und-viel-kritik/) unter Bezugnahme auf die Antwort der Bundesregierung auf die Schriftliche Einzelfrage 14 auf Bundestagsdrucksache 20/12372 und unter Bezugnahme auf die Antwort der Bundesregierung auf die Fragen 79 bis 81 der Kleinen Anfrage auf Bundestagsdrucksache 20/12829 für den Soll-Ansatz im Bundeshaushalt 2024, wonach das BMI im Jahr 2024 21 Mio. Euro und das BMVg 55 Mio. Euro finanziert, und für den Soll-Ansatz im Entwurf der Bundesregierung für den Bundeshaushalt 2025, wonach das BMI 19 Mio. Euro und das BMVg 40 Mio. Euro finanziert, nicht umgesetzt?

    a) Welche Finanzierungsgesamtsumme für die Agentur für Innovationen in der Cybersicherheit war ursprünglich unabhängig von der exakten Aufteilung auf das BMI und das BMVg von der Bundesregierung jeweils für das Jahr 2024 und für das Jahr 2025 vorgesehen?

    b) Welche Finanzierungsgesamtsumme für die Agentur für Innovationen in der Cybersicherheit ist unabhängig von der exakten Aufteilung auf das BMI und das BMVg von der Bundesregierung jeweils für die Jahre bis 2028 vorgesehen (bitte nach Jahresscheiben aufschlüsseln)?

    c) Wie stellen sich die vorgesehenen Ausgaben für die Agentur für Innovationen in der Cybersicherheit jeweils beim BMI und beim BMVg jeweils für die Jahre der mittelfristigen Finanzplanung von 2026 bis 2028 dar (bitte nach Ressort und Jahresscheiben aufschlüsseln)?

34. Wie sind die Aussagen der Bundesregierung in ihrer Antwort auf die Frage 35 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707, wonach „…das im deutschen Vergaberecht geltende Gleichbehandlungsgebot bzw. das damit korrespondierende Diskriminierungsverbot (siehe etwa § 97 Absatz 2 des Gesetzes gegen Wettbewerbsbeschränkungen [GWB]) […] jede unmittelbare und mittelbare Benachteiligung von Bietern aus dem Ausland [verbieten]…“ und „…die Unterscheidung zwischen Unternehmen aus dem EU-Ausland und aus Drittstaaten […] das deutsche Vergaberecht nicht [trifft]…“, sowie in ihrer Antwort auf die Frage 36 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707, wonach es „…in Deutschland keine gesetzlichen Grundlagen für einen kategorischen Ausschluss von Herstellern aufgrund der Verortung ihres Hauptsitzes in einem bestimmten Land [gibt]…“, mit dem Vorhaben des sogenannten Vergabetransformationspakets, mit dem die Bundesregierung unter Bezugnahme auf ihre Antwort auf Frage 17 der Kleinen Anfrage auf Bundestagsdrucksache 20/13937 den „…bisher strenge[n] Grundsatz der Gleichbehandlung von Drittstaatsanbietern in Vergabeverfahren…“ einschränken möchte, widerspruchsfrei in Einklang zu bringen und warum hält die Bundesregierung eine derartige Einschränkung nun für möglich?

35. Plant die Bundesregierung mit ihrem Vorhaben des sogenannten Vergabetransformationspakets nicht nur die Einschränkung des bisher strengen Grundsatzes der Gleichbehandlung von Drittstaatsanbietern in Auftragsvergabeverfahren des öffentlichen Auftraggebers, wie in ihrer Antwort auf Frage 17 der Kleinen Anfrage auf Bundestagsdrucksache 20/13937 angegeben, sondern plant sie beziehungsweise beabsichtigt sie darüber hinausgehend mit dem Vergabetransformationspaket oder mit anderen Vorhaben die Möglichkeit zu schaffen, für bestimmte Auftragsvergabeverfahren im Bereich der Beschaffung von Cyber- und Informationssicherheitsleistungen und -produkten nur einen nationalen Anbieterkreis zuzulassen?

36. Hat sich die Bundesregierung seit Beginn der Legislaturperiode dahingehend auf europäischer Ebene eingesetzt, dass Änderungen im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) derart vorgenommen werden, dass in Artikel 346 AEUV die Cyber- und Informationssicherheit aufgenommen werden, damit auch Beschaffungen von Cyber- und Informationssicherheitsleistungen mit Ausnahmen belegt werden können beziehungsweise jedenfalls gesichert in den Vergabebereich Verteidigung und Sicherheit fallen, oder plant die Bundesregierung dies noch bis Ende der Legislaturperiode zu tun, und wenn nein, warum nicht?

37. Hat sich die Bundesregierung seit Beginn der Legislaturperiode dahingehend auf europäischer Ebene eingesetzt, dass eine Änderung der Richtlinie 2009/81/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Koordinierung der Verfahren zur Vergabe bestimmter Bau-, Liefer- und Dienstleistungsaufträge in den Bereichen Verteidigung und Sicherheit derart vorgenommen wird, damit Leistungen der Cybersicherheit und Informationssicherheit explizit vom Anwendungsbereich der Richtlinie 2009/81/EG erfasst werden und die Cyber- und Informationssicherheit dort genannt wird, oder plant die Bundesregierung dies noch bis Ende der Legislaturperiode zu tun, und wenn nein, warum nicht?

38. Hat sich die Bundesregierung seit Beginn der Legislaturperiode dahingehend auf europäischer Ebene eingesetzt, dass die in Artikel 346 Absatz 2 referenzierte und seit dem 15. April 1958 nicht mehr überarbeitete Liste von Waren, Gütern und Dienstleistungen, auf die Artikel 346 Absatz 1 Buchstabe b Anwendung findet, angesichts des technologischen Fortschritts überarbeitet wird oder plant die Bundesregierung dies noch bis Ende der Legislaturperiode zu tun, und wenn nein, warum nicht?

39. Sind in dem durch die Bundesregierung verabschiedeten Gesetzentwurf zur Vergabetransformation neben umweltbezogenen und sozialen Kriterien auch die Einführung von digitalen Aspekten als Kriterien jenseits der von der Bundesregierung in ihrer Antwort auf Frage 17 der Kleinen Anfrage auf Bundestagsdrucksache 20/13937 bereits genannten Einschränkung des „…bisher strenge[n] Grundsatz der Gleichbehandlung von Drittstaatsanbietern in Vergabeverfahren…“ für eine Vergabeentscheidung vorgesehen, und wenn ja, welche, und wenn nein, hat die Bundesregierung dies in anderen Vorhaben beabsichtigt oder vorgesehen?

40. Beabsichtigt oder plant die Bundesregierung, Open Source als Vergabekriterium in Vergabeverfahren zur Beschaffung bei bestimmten Auftragsgegenständen im Zusammenhang mit IT-Produkten für die Bundesverwaltung einzuführen, und wenn ja, im Zusammenhang mit welchen Auftragsgegenständen, und wenn nein, warum nicht?

41. Beabsichtigt oder plant die Bundesregierung, Open Source als Vergabekriterium in Vergabeverfahren zur Beschaffung bei bestimmten Auftragsgegenständen im Zusammenhang mit Cyber- und Informationssicherheitsprodukten für die Bundesverwaltung einzuführen, und wenn ja, im Zu-

sammenhang mit welchen Auftragsgegenständen, und wenn nein, warum nicht?

42. 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 Cybersicherheitsökosystem künftig bei IT-Beschaffungsvorhaben des Bundes einen bestimmten Anteil der Sachmittel für IT-Vorhaben des Bundes für Cybersicherheit aufzuwenden?

43. Plant die Bundesregierung unter Bezugnahme auf ihre Antwort der Bundesregierung auf die Frage 41 der Kleinen Anfrage auf Bundestagsdrucksache 20/8707, wonach eine Produktzertifizierung nach den Zertifizierungsschemata der Common Criteria, der Technischen Richtlinie, der BSZ und der NESAS keine zukunftsbezogenen Aussagen zur Sicherheit von Updates und Patches eines zu zertifizierenden IT-Sicherheitsprodukts machen, und unter dem Eindruck ihrer Aussagen beispielsweise in ihrer Antwort auf die Fragen 8 bis 12 der Kleinen Anfrage auf Bundestagsdrucksache 20/10149, wonach „…mit zunehmender informationstechnischer Komplexität von kritischen (Software-)Komponenten […] ein wesentlicher Teil der Beherrschbarkeit der Technologie im Rahmen der Produktpflege (Softwareupdates, Firmware-Updates, Schließen von Sicherheitslücken) beim Hersteller selbst oder innerhalb der weiteren Lieferkette [verbleibt]…“ und wonach „…aufgrund der hohen Komplexität kritischer Komponenten und der zu erwartenden stetigen Software/Firmware-Updates […] etwa hohe technische Sicherheitsanforderungen keine ausreichende Sicherheit dahingehend [bieten], dass Hersteller keine missbräuchlichen Zugriffmöglichkeiten auf Hard- und Software implementieren oder sonstige Handlungen vornehmen, die Sabotage oder Spionage ermöglichen…“, Änderungen dahingehend vorzunehmen, dass Produktzertifizierungen des BSI auch zukünftig zu Updates und Patches Aussagen machen können, und wenn nein, warum nicht, und welche anderen Maßnahmen ergreift die Bundesregierung, um zukunftsbezogene Aussagen zur Sicherheit von Updates und Patches eines zu zertifizierenden IT-Sicherheitsprodukts machen zu können?

44. Welche Möglichkeiten haben die in die Beschaffung von IT-Sicherheitsprodukten betreffenden Vergabeverfahren unterlegenen Bieter jeweils im Rahmen der Verordnung über die Vergabe öffentlicher Aufträge (VgV) und im Rahmen der Vergabeverordnung für die Bereiche Sicherheit und Verteidigung (VSVgV), gegen eine Vergabeentscheidung Beschwerde beziehungsweise Klage einzureichen, welche Fristen gelten dabei jeweils und bis zu wie viele Instanzen können hinsichtlich einer Beschwerde beziehungsweise Klage dabei durchlaufen werden?

    a) Wie viele Verfahren im Zusammenhang mit Beschwerden beziehungsweise Klagen gegen eine Vergabeentscheidung hinsichtlich eines Vergabeverfahrens zur Beschaffung von IT-Sicherheitsprodukten gab beziehungsweise gibt es jeweils in den Jahren 2022, 2023, 2024?

    b) Wie viele Instanzen wurden dabei im Schnitt durchlaufen?

    c) Wie lange dauerten die Verfahren dabei im Schnitt?

    d) Wie viele der Verfahren sind abgeschlossen und wie viele Verfahren dauern noch an (bitte für die Jahre 2022, 2023, 2024 angeben)?

45. Wie viele Software-Entwicklungsaufträge bezüglich IT-Sicherheitsprodukten hat die Bundesregierung seit Beginn der 20. Legislaturperiode erteilt (bitte nach Jahren aufschlüsseln)?

    a) Wie viele davon sind bereits fertig entwickelt?

    b) Wie viele befinden sich noch in Entwicklung?

    c) Wie lange dauert die Entwicklung im Schnitt?

    d) Welche Vertragstypen (beispielsweise Werkverträge, Dienstverträge etc.) lagen dabei in jeweils wie vielen Fällen den Aufträgen zugrunde?

    e) Gibt es ein Standard-Vertragsmuster zur Beschaffung von IT-(Sicherheits-)Produkten, und wenn ja, welcher Vertragstyp liegt dem Standard-Vertragsmuster zugrunde?

    f) In wie vielen Fällen der Gesamtzahl an vergebenen Software-Entwicklungsaufträgen bezüglich IT-Sicherheitsprodukten wurde das Standard-Vertragsmuster verwendet?

Berlin, den 9. Dezember 2024

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