Bundesministerium
des Innern
und für Heimat

POSTANSCHRIFT Bundesministerium des Innern und für Heimat, 10557 Berlin

Mitglied des Deutschen Bundestages
Frau Anke Domscheit-Berg
Platz der Republik 1
11011 Berlin

[redacted]

INTERNET www.bmi.bund.de

DATUM 1. August 2024

BETREFF **Schriftliche Frage Monat Juli 2024**
HIER Arbeitsnummer 7/352

Sehr geehrte Frau Abgeordnete,

auf die mir zur Beantwortung zugewiesene schriftliche Frage übersende ich Ihnen die beigefügte Antwort.

Mit freundlichen Grüßen
in Vertretung

[redacted]

Rita Schwarzelühr-Sutter

ZUSTELL- UND LIEFERANSCHRIFT Alt-Moabit 140, 10557 Berlin
VERKEHRSANBINDUNG S-Bahnhof Berlin Hauptbahnhof
Bushaltestelle Berlin Hauptbahnhof

Schriftliche Frage der Abgeordneten Anke Domscheit-Berg
vom 24. Juli 2024
(Monat Juli 2024, Arbeits-Nr. 7/352)

Frage

Wie begründet die Bundesregierung angesichts der anhaltend hohen Gefährdungslage im Cybersicherheitsbereich die Zurückstellung von mindestens elf Maßnahmen der Cybersicherheitsagenda (s. Antwort des Bundesministeriums des Innern und für Heimat auf meine Nachfrage im Nachgang zu TOP 4 der 64. Sitzung des Ausschusses für Digitales des Deutschen Bundestages am 15. Mai 2024 bzw. www.heise.de/news/Kommentar-zur-Cybersicherheitsagenda-Von-Hochglanzstoryzum-nationalen-Drama-9774726.html), darunter auch die Maßnahme "Etablierung des Grundsatzes 'security by design and by default' in der Bundesverwaltung" (bitte jeweils jede zurückgestellte Maßnahme begründen, insbesondere hinsichtlich der genannten Maßnahme "security by design and by default") und welche Maßnahmen, die sich aktuell noch in Umsetzung befinden, wird die Bundesregierung noch bis zum 31. Dezember 2024 erledigen können?

Antwort

Die Umsetzung der Cybersicherheitsagenda behält für das Bundesministerium des Innern und für Heimat (BMI) hohe Priorität. Viele Maßnahmen der Cybersicherheitsagenda befinden sich in Umsetzung oder sind bereits umgesetzt. Auch bei den zurückgestellten Maßnahmen sind teilweise bereits Umsetzungsschritte erfolgt. Das BMI tritt für eine weitere Stärkung der Ressourcen in diesem Bereich ein, um die Cybersicherheit, insbesondere durch eine schnellere und umfassendere Umsetzung der Cybersicherheitsagenda, zu erhöhen.

Zu den zurückgestellten sowie die in der Umsetzung befindlichen Maßnahmen wird folgendes mitgeteilt:

a) (2.9) Ausbau der Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) als zentraler Dienstleister für die Sicherheitsbehörden sowie Auf- und Ausbau eigener nationaler Entwicklungsfähigkeiten und Bewertungskompetenzen bei der ZITiS und
b) (3.11) Konsequenter Ausbau der ZITiS, um digitale Ermittlungswerkzeuge für die Sicherheitsbehörden zur Stärkung der Auswerte- und

Analysefähigkeiten im Kampf gegen Cybercrime zu entwickeln.
Der Auf- und Ausbau eigener nationaler Entwicklungsfähigkeiten und Bewertungskompetenzen bei der ZITiS (2.9) sowie die Stärkung der Auswerte- und Analysefähigkeiten im Kampf gegen Cybercrime (3.11) erfolgt im Rahmen der verfügbaren Ressourcen.
Zurückgestellt werden jene Aktivitäten, die eine umfangreiche Ressourcenverstärkung (Stellen, Sachmittel und Personal) erfordern, welche sich in Anbetracht der angespannten Haushaltslage auch nicht durch Umpriorisierungen in angemessenen Rahmen abbilden lassen.
Die Maßnahmen 2.9 und 3.11 sind als auf Dauer angelegte Zielsetzung zu verstehen, weshalb eine abschließende Umsetzung in 2024 nicht zu erwarten ist.

c) (3.1) Ausbau der zentralen Kompetenz- und Service-Dienstleistungen des Bundeskriminalamtes (BKA) zur Bekämpfung von Cybercrime.
Der Ausbau der zentralen Kompetenz- und Service-Dienstleistungen des BKA wurde bereits begonnen. Die Weiterführung der Maßnahme erfolgt im Rahmen der verfügbaren Finanz- und Personalressourcen.

d) (4.1) Stärkere gesetzliche Verankerung der Informationssicherheit und Umsetzung eines Verstärkungsprogramms für die Cybersicherheit des Bundes mit der Einrichtung eines Chief Information Security Officers für den Bund (CISO BUND) und eines Kompetenzzentrums zur operativen Sicherheitsberatung des Bundes.
Die Einrichtung der Rolle des CISO Bund und die gesetzliche Verankerung der Rolle der Informationssicherheitsbeauftragten sind im Rahmen des NIS-2-Umsetzungs-und-Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) geplant und könnten daher in Abhängigkeit des Gesetzgebungsverfahrens abgeschlossen werden. Nur mit zusätzlichen Haushaltsmitteln wäre darüber hinaus der Aufbau eines Kompetenzzentrums zur operativen Sicherheitsberatung des Bundes möglich.

e) (4.2) Etablierung des Grundsatzes „security by design and by default“ in der Bundesverwaltung
Seit Inkrafttreten des IT-Sicherheitsgesetzes 2.0 2021 müssen die Stellen des Bundes gem. § 8 Abs. 4 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) „bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben des Bundes“ das Bundesamt für Sicherheit in der Informationstechnik (BSI) frühzeitig beteiligen und ihm Gelegenheit zur Stellungnahme geben. So werden Sicherheitsanforderungen direkt von Anfang an bei der Digitalisierung mitgedacht (Security-by-Design). Verantwortlich für ist hierfür im BSI die Sicherheitsberatung Bund..

f) (4.4) Investition in Quantencomputing beim BSI zur Gewährleistung der sicheren Regierungskommunikation
Investitionen in Quantencomputing beim BSI zur Gewährleistung der sicheren Regierungskommunikation wären mit zusätzlichen Haushalsmitteln möglich.

g) (5.1) Förderung von Investitionen für Cyber-Resilienz-Maßnahmen in kleine und mittlere Unternehmen (KMU), die dem KRITIS-Sektor angehören

h) (5.2) Einrichtung von Awareness und Cyber-Resilienz-Projekten, die vom BSI und von externen Dienstleistern angeboten werden
Für die Maßnahmen 5.1 und 5.2 stehen keine ausreichenden Haushaltsmittel zur Verfügung.

i) (6.2) Konzeption und initialer Aufbau eines zivilen Cyberabwehrsystems (ZCAS)
Die Maßnahme baut auf der Maßnahme 6.1, Aufbau eines BSI Information Sharing Portals (BISP) auf und kann nach deren Umsetzung starten.

j) (8.1) Modernisierung der Weitverkehrsnetze gemäß der „Netzstrategie 2030 für die öffentliche Verwaltung“
Die Maßnahme befindet sich in Umsetzung. Im Jahr 2024 erfolgt im Rahmen des IPv6 Programm des Bundes die weitere Umsetzung zur Modernisierung innerhalb der Netze des Bundes (NdB). Diese soll bis Ende 2024 den Datenaustausch mit dem neuen Protokoll IPv6 zwischen ersten Behörden und dem Informations-Technik-Zentrum des Bundes (ITZ-Bund) ermöglichen.

k) (8.5) Erweiterung des Digitalfunknetzes für die Behörden und Organisationen mit Sicherheitsaufgaben (Datenkommunikation)
Die Maßnahme 8.5 umfasst die Frage, wie ein hochsicheres, hochverfügbares modernes Breitbandnetz die bisherige TETRA-Technik künftig ersetzen kann, um eine zeitgemäße breitbandige Datenkommunikation zu ermöglichen. Hierfür sind weitere Abstimmungen zwischen Bund und Ländern erforderlich, um ein bundesweit einheitliches und wirtschaftliches Vorgehen zu gewährleisten. Der Bund ist hierzu mit den Ländern im ständigen Austausch. Die Maßnahme ist insofern als zurückgestellt bezeichnet, um den Eindruck zu vermeiden, der Bund würde von einem abgestimmten, gemeinsamen Vorgehen aller Beteiligten Abstand nehmen wollen.

l) Die weiteren in Umsetzung befindlichen Maßnahmen sind wegen fehlender notwendiger grundgesetzlicher und einfachgesetzlicher Änderungen sowie unzureichender Mittel und Stellen bis Ende 2024 nicht abzuschließen.