Was wichtig wird:
Erwartungen der Unternehmen der Schwarz Gruppe an die nächste Legislaturperiode

Themenschwerpunkt: Digitalpolitik

Digitale Transformation souverän und sicher gestalten

Relevanz und Zielbild

- **Mit gutem Beispiel voran:** Die Unternehmen der Schwarz Gruppe haben sich für den Standort Deutschland in einem wettbewerbsfähigen Europa entschieden und durch den Aufbau digitaler Infrastrukturen die eigene digitale Unabhängigkeit gestärkt.
- **Vier souveräne Säulen:** Dabei kombinieren wir bei Schwarz Digits, der IT- und Digitalsparte der Unternehmen des Schwarz Gruppe, auf höchstem Sicherheits- und Datenschutzniveau vier souveräne Säulen: Cloud, Cybersicherheit, Künstliche Intelligenz und sichere Kommunikation. Mit dieser Kombination sorgen wir dafür, dass unser wichtigstes digitales Gut, unsere Daten, sowohl in der Speicherung als auch der Verarbeitung in unserer Hoheit bleibt. Damit stellen wir eine langfristige Handlungsfähigkeit und Innovationskraft sicher.
- **Köpfe und Technologie als Erfolgsgarant:** Daran arbeiten 7.500 IT- und Digitalexperten, die 1.250 IT- und Digitallösungen verantworten und durch den Einsatz von modernen Technologien mehr als 44 Millionen digitale Identitäten schützen und vier eigene Rechenzentren betreiben. Souveränität beginnt im Rechenzentrum und setzt sich in der eigenen datensouveränen Cloud STACKIT konsequent fort. Sie zeichnet sich durch georedundante, zertifizierte Rechenzentren entsprechend der EU-Sicherheitsvorgaben und DSGVO-Konformität mit C5-Testat des Bundesamtes für Sicherheit in der Informationstechnik in Deutschland aus.

Status Quo

- **Digitale Souveränität heißt für uns:** (1) Kontrolle über unsere Daten, (2) Wechselmöglichkeit und (3) Einflussmöglichkeiten auf Anbieter. Wir bestimmen selbst, wo unsere Daten liegen, wer darauf Zugriff hat und wie wir sie nutzen. Ohne heimische Alternativen und mit einer nur halbherzig umgesetzten digitalpolitischen Strategie entsteht mittelfristig die Gefahr für Lock-in-Effekte sowie Abhängigkeiten bei politischen Instabilitäten.
- **Engerer Schulterschluss nötig:** Die Stärkung der digitalen Souveränität ist für uns dabei nicht nur eine Frage der Technik, sondern auch eine Frage der politischen und wirtschaftlichen Gestaltung. Der hohe digitale Abhängigkeitsgrad Deutschlands und die zunehmenden digitalen Angriffe auf Unternehmen erfordern damit in der neuen Legislatur einen viel engeren Schulterschluss zwischen Politik, öffentlicher Verwaltung und Wirtschaft[1].
- **Kritische Assets brauchen eine verbindliche Grundlage:** Kritische Anwendungen, Anlagen und Infrastrukturen benötigen in diesem Zusammenhang besondere Aufmerksamkeit. Das voraussichtlich nicht

[1] Digital Dependence Index: 82% der benötigten digitalen Technologien werden in Deutschland aus dem Ausland bezogen. Wirtschaftsschutzstudie (Bitkom, Deutschland, 2024): 74 % der Firmen sind von Datendiebstahl betroffen gewesen. Der Gesamtschaden durch Cybercrime beträgt 178,6 Milliarden Euro.

mehr in dieser Legislatur verabschiedete Umsetzungsgesetz zur NIS2-Richtlinie und KRITIS Dachgesetz sowie das nationale Durchführungsgesetz zum AI-Act sind wichtige Vorhaben, die schnellstmöglich abgeschlossen werden sollten. Sie stärken ein hohes gemeinsames (EU-weites) Cybersicherheitsniveau und den Einsatz sicherer und vertrauensvoller KI.

Notwendige Änderungen

Digitalpolitik mit einem eigenständigen Digitalministerium gestalten

- **Eigenständiges Digitalministerium:** Digitalpolitische Umsetzungserfolge brauchen klar gebündelte Zuständigkeiten, Koordinierungsrechte und ein zentrales Digitalbudget – in der neuen Legislatur betrachten wir daher ein eigenständiges Digitalministerium als Erfolgsgarant und konsequente Weiterentwicklung des aktuellen ministeriellen Status quo.
- **Ergebnisorientierte Zusammenarbeit:** Die Zuständigkeit für die Digitalstrategien und -projekte der jeweiligen Ressorts ist auch weiterhin eine Aufgabe der Fachministerien. Das eigenständige Digitalministerium gewährleistet jedoch in diesem Zusammenspiel das kohärente Vorgehen insb. bei den übergeordneten Themen der Verwaltungsdigitalisierung, IT des Bundes (über alle Ressorts), digitale Infrastruktur (einschl. Rechenzentren), horizontale Digitalregulierungen wie KI oder Plattformen, Förderung digitaler Schlüsseltechnologien und der Cybersicherheit aus einer Hand.

Cloudpolitik souverän und sicher gestalten

- **Cloud- und KI-Infrastruktur:** Zur Sicherung der digitalen Souveränität und der Zukunftsfähigkeit Deutschlands braucht es eine leistungsfähige Cloud- und KI-Infrastruktur, die dem Staat, Wirtschaft und Wissenschaft zur Verfügung steht und auf europäischen Werten basiert. Deutschland muss sich dabei strategisch aufstellen, um eine Leitrolle für die digitale und technologische Souveränität in Europa einnehmen zu können.
- **Praxisnahe Strategieumsetzung**: Die Deutsche Verwaltungscloud Strategie und die Multi-Cloud-Strategie der Bundesregierung bieten die Chance, die digitale Souveränität der öffentlichen Verwaltung unmittelbar zu stärken. Im Rahmen einer wohl gewählten und langfristig angelegten Multi-Cloud-Strategie ist damit ein Level Playing Field für alle Cloud Service Provider von besonderer Bedeutung (ohne dabei etablierte Abhängigkeiten zu zementieren).
- **Ankerkunde und Ausschreibungen:** Als investitionsstarker Marktakteur stellt der Staat einen der wichtigsten Nachfrager (Rolle: Ankerkunde) für digital souveräne Technologien und Dienste dar. Er hat damit die Chance und Verantwortung, eigene Bedarfe stärker als bisher durch konkrete Use Cases sichtbar zu machen und Anforderungen an Sicherheit, Interoperabilität, Open Source und Datenschutz in Ausschreibungen aktiv zu gestalten und damit Standards zu setzen. Die Ausschreibungen sind dabei so zu gestalten, dass sie je nach Anwendungsfall und Kritikalität (Schutzniveau der Daten) souveräne Mindeststandards erfüllen.

KI-Politik souverän und sicher gestalten

- **AI-Act ist der richtige regulatorische Weg:** Ein Akteur allein kann den KI-Standort Europa nicht aufbauen – dafür braucht es ein Ökosystem aus Forschung, Unternehmen, Start-ups und Staat. Dabei unterstützt der AI-Act aus unserer Sicht den Einsatz sicherer und vertrauensvoller KI mit den richtigen Motiven und Zielen.
- **Die Umsetzung entscheidet:** Wichtig ist jedoch die Umsetzung des AI-Acts bürokratiearm, anwenderfreundlich und global anschlussfähig auszugestalten. Dies umfasst a) klar geregelte Zuständigkeiten sowie ausreichende finanzielle und personelle Ausstattung der nach dem AI-Act zuständigen, nationalen Marktüberwachungs- und notifizierenden Behörden sowie der zentralen Anlaufstelle, b) schlank gestaltete Dokumentationspflichten und c) den Einsatz Deutschlands für eine in allen EU-Ländern möglichst einheitliche Implementierung des AI-Acts und die Entwicklung hin zu einem international anschlussfähigen Rahmenwerk.
- **Der Staat als Ankerkunde:** Bei KI-Use-Cases und Anwendungen kann sich der Staat als Ankerkunde (über Abnahmegarantien) noch zielgenauer platzieren und dabei die wachsenden europäischen

Angebote stärker nutzen. Für den kostenintensiven Auf- und Ausbau von souveränen Cloud– und KI-Infrastrukturen sollten daher Abnahmeverpflichtungen als weiteres Instrument (neben u.a. (EU-weiten) Förderprogrammen, Strukturförderung, Bürokratieentlastung) genutzt werden.

Cybersicherheitspolitik souverän und sicher gestalten

- **Cybersicherheitsregulierung ist der richtige regulatorische Weg:** Die Handlungsfähigkeit von morgen braucht Investitionen in präventive und reaktive Sicherheitsmaßnahmen. Die Verpflichtungen zur europaweiten Einhaltung der gesetzlichen Vorgaben sind daher der richtige Weg und sollten so schnell wie möglich verabschiedet werden. Mit einer künftigen NIS2-Evaluierung sollten allerdings - je nach Ergebnis - auch Verschärfungen in Betracht gezogen werden[2].
- **Zusammenarbeit stärken:** Sicherheit braucht in diesem Bezug auch eine verbesserte Zusammenarbeit über Behörden und föderale Strukturen hinaus – insb. bei Erkennung und Verwerten von Erkenntnissen von Cyberattacken und -bedrohungen.
- **Steuerliche Anreize, Förderprogramme und Versicherungsangebot:** Um das Sicherheitsniveau und die Attraktivität des Wirtschaftsstandorts Deutschland weiter signifikant zu erhöhen, sind weitere Instrumente in Betracht zu ziehen. Dazu zählen (1) steuerliche Anreize für neu beschaffte Produkte, Dienstleistungen und Schulungen, (2) KMU-freundliche Förderprogramme durch z.B. die KfW zur finanziellen Begleitung und Unterstützung bei Sicherheitsmaßnahmen und (3) ein Versicherungsangebot, das die Überwachung von präventiven Maßnahmen (eingebettet in ganzheitliche Cybersicherheitsmaßnahmen) stärker in den Vordergrund stellt und im Schadensfall durch Dienstleister und Dienstleistungen wirkt (u.a. Incident Response Teams).

Was wichtig wird

- **Digitalpolitische Governance:** Digitalpolitische Umsetzungserfolge brauchen ein eigenständiges Digitalministerium.
- **Cloud- und KI-Infrastruktur:** Es ist dringlicher denn je, eine Vision und klare Strategie für ein souveränes digitales Deutschland als Vorreiter in Europa zu entwickeln und sie umzusetzen. Dazu gehört eine Cloud- und KI-Infrastruktur, die dem Staat, Wirtschaft und Wissenschaft zur Verfügung steht und auf europäischen Werten basiert sowie ein Staat, der als Ankerkunde eine Vorbildfunktion einnimmt.
- **KI-Regulierung und Staat als Ankerkunde:** Ein Akteur allein kann den KI-Standort Europa nicht aufbauen. Es braucht neben der KI-Regulierung auch den Staat, der als Ankerkunde (über Abnahmegarantien) in der neuen Legislatur die wachsenden Angebote aus Deutschland und Europa stärker nutzt und eigene Anwendungsbedarfe einbringt (u.a. als direkter Beschleuniger für die Deutsche Verwaltungsmodernisierung und Bürokratieentlastung).
- **Ausgewogene Cybersicherheit:** Cybersicherheitspolitik erfordert eine Balance zwischen der europaweit einheitlichen Regulierung, die auf präventive und reaktive Sicherheitsmaßnahmen setzt und den Prinzipien der Anreizsetzung (steuerliche Anreize & Förderprogramme) und Risikoabsicherung (Versicherungsangebote) folgt.

[2] Weitere Handlungsbedarfe sind der Stellungnahme zum NIS2UmsuCG aus der Anhörung im Ausschuss Inneres und Heimat zu entnehmen.