digitalswitzerland | Waisenhausplatz 14 | 3011 Bern

An den Ständerat ausschliesslich via E-Mail

Kenntnisnahme der Motion "Durchführung dringend notwendiger Cybersicherheitsprüfungen" (24.3810)

Bern, 13. September 2024

Sehr geehrte Damen und Herren Ständerätinnen und Ständeräte,

Wir teilen im Folgenden unsere Einschätzung zur Motion "Durchführung dringend notwendiger Cybersicherheitsprüfungen" (24.3810), über welche Sie am 18. September abstimmen werden.

Für den wahrscheinlichen Fall einer Annahme möchten wir vorbehaltlich auf folgenden Handlungsbedarf hinweisen, damit die Motion zu einem tatsächlichen Instrument zur Stärkung der Cybersicherheit in der Schweiz werden kann.

Das Wichtigste in Kürze:

- digitalswitzerland anerkennt, dass die Cybersicherheit der Schweiz weiter und stetig verbessert werden muss.
- **Für den Fall, dass der Ständerat der Motion zustimmt, fordern wir dringend notwendige Präzisierungen in der Kommission des Zweitrats.**
- Eine ganzheitliche Betrachtung der Cybersicherheit erfordert eine Kosten-Nutzen-Abwägung, kontinuierliche Verbesserung, klare Verantwortlichkeiten und Geltungsbereiche, Berücksichtigung wirtschaftlicher Anreize und Einbettung in den internationalen Kontext, während unnötige Bürokratie und Belastungen vermieden und Verhältnismässigkeit gewährleistet sein muss.

Erläuterungen:
digitalswitzerland teilt die grundsätzliche Ansicht der Motion die Stärkung der Cybersicherheit in der Schweiz zu stärken. digitalswitzerland erkennt auch an, dass die zunehmende Komplexität von Cyberbedrohungen robuste Massnahmen erfordert, einschliesslich unabhängiger Prüfungen, um die nationale Sicherheit, wirtschaftliche Stabilität und öffentliche Sicherheit zu gewährleisten.

Gleichzeitig betont digitalswitzerland, dass Anbieter und Betreiber digitaler Lösungen und Infrastrukturen bereits heute zahlreiche Pflichten im Bereich der Cybersicherheit erfüllen und ein grosses Interesse an sicheren Produkten, Infrastrukturen und Dienstleistungen haben. Bestehende Gesetze (bspw. Gewährleistungs- und Haftpflichtbestimmungen im Obligationenrecht, Datenschutzgesetz, Fernmeldegesetz, oder Informationssicherheitsgesetz sowie deren Ausführungsverordnungen) sowie internationale Standards und Zertifizierungen spielen dabei eine wichtige Rolle. Organisationen, welche bereits solche Vorschriften befolgen, sollten explizit aus dieser Motion ausgenommen werden. Damit stellt sich die Frage, welche digitalen Produkte, Dienstleistungen und Infrastrukturen noch ungenügend überprüft werden.

Um die Cybersicherheit in der Schweiz nachhaltig und zielgerichtet zu verbessern, schlägt digitalswitzerland vor, dass die Motion im Falle einer Annahme durch den Ständerat, in der zuständigen Kommission des Nationalrats zwingende Präzisierungen vorgenommen werden – welche nachfolgend detailliert erläutert sind:

1. Klare Definition des Test-Umfangs:

- **Präzise Definition des Anwendungsbereichs:** Es braucht eine klare Abgrenzung, welche digitalen Produkte, Infrastrukturen, Geräte und Anwendungen in den Anwendungsbereich der Motion fallen. Dabei sollte berücksichtigt werden, welche Systeme besonders kritisch für die Sicherheit und Funktionalität der Schweiz sind und welche bereits durch bestehende Regulierungen, Standards oder andere Vorschriften geprüft werden.
- **Kritikalitätsstufen:** Einführung eines abgestuften Systems zur Klassifizierung von Infrastrukturen, Geräten und Anwendungen nach ihrer Kritikalität für die nationale Sicherheit, Wirtschaft und öffentliche Ordnung. Cybersicherheitsprüfungen sollten sich primär auf Systeme mit hoher und sehr hoher Kritikalität konzentrieren.
- **Risikobasierter Ansatz:** Entwicklung eines risikobasierten Ansatzes, der die Wahrscheinlichkeit und das Ausmass potenzieller Cyberangriffe berücksichtigt. Prüfungen sollten sich auf Bereiche mit hohem Risiko konzentrieren, um Ressourcen effizient einzusetzen.
- **Ausschluss bestimmter Bereiche:** Expliziter Ausschluss von Bereichen, die bereits durch andere Gesetze und Vorschriften abgedeckt sind oder für die bereits angemessene Zertifizierungen und Sicherheitsstandards existieren.

2. Finanzierung durch Private (Unternehmen)

- **Grundsätzlich sind Unternehmen selbst dafür verantwortlich, die Kosten für Cybersicherheitsprüfungen zu tragen, um ihre eigenen Systeme zu schützen:** Prüfungen sollten nur bei Bedarf oder Marktnachfrage durchgeführt werden. Dies entspricht der Haltung des Bundesrates, staatliche Prüfungen nur bei staatlichen Akteuren zu finanzieren. Eine öffentlich mandatierte Prüfpflicht für Unternehmen lehnt digitalswitzerland ab.
- **Vermeidung von Doppelbelastungen:** Unternehmen, die bereits anerkannte Sicherheitsstandards, bzw. Vorschriften erfüllen, sollen nicht zusätzlich finanziell belastet werden.

3. Harmonisierung mit internationalen Standards:

- **Äquivalenz der EU-Vorschriften:** Berücksichtigung und mögliche Anpassung an relevante EU-Vorschriften, wie den Cyber Resilience Act, um Doppelbelastungen zu vermeiden und den Handel mit der EU zu erleichtern.
- **Anerkennung internationaler Zertifizierungen:** Anerkennung von international anerkannten Cybersicherheitszertifizierungen, um den Aufwand für Unternehmen zu reduzieren und die internationale Zusammenarbeit zu fördern.
- **Mitarbeit in internationalen Gremien:** Aktive Teilnahme der Schweiz an internationalen Gremien zur Entwicklung und Harmonisierung von Cybersicherheitsstandards.

4. Weitere wichtige Präzisierungen:

- **Definition von "Lücken":** Klare Definition des Begriffs "Lücken" in Bezug auf Cybersicherheitsprüfungen um den Fokus der Prüfungen zu schärfen und klar einzugrenzen.
- **Verantwortlichkeiten:** Präzise Festlegung der Verantwortlichkeiten für die Durchführung und Finanzierung (siehe oben) von Cybersicherheitsprüfungen, auch auf Seiten des Bundes.
- **Evaluierung und Anpassung:** Einführung eines regelmässigen Evaluierungsprozesses, um die Wirksamkeit der Cybersicherheitsprüfungen zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

digitalswitzerland ist bereit, aktiv an der Ausgestaltung dieser Präzisierungen mitzuwirken und seine Expertise in den Bereichen Cybersicherheit und Digitalisierung einzubringen.

digitalswitzerland ist überzeugt, dass durch einen solchen kollaborativen Ansatz die Cybersicherheit in der Schweiz gestärkt werden kann, ohne unnötige Belastungen für die Wirtschaft zu schaffen. Wir ersuchen sie, bei dieser wichtigen Entscheidung eine Abwägung entlang unserer Überlegungen durchzuführen. Für jegliche Fragen und Anregungen stehen wir jederzeit zur Verfügung.

Mit freundlichen Grüssen,

Stefan Metzger
Managing Director digitalswitzerland
stefan@digitalswitzerland.com

Guillaume Gabus
Public Affairs & Extended Management
guillaume@digitalswitzerland.com

Über digitalswitzerland

Der Austausch zwischen Wirtschaft, Wissenschaft, Behördenorganisation und Politik steht im Zentrum der Arbeit von digitalswitzerland. Mit Impulsen und konkreten Beiträgen sollen die Möglichkeiten der digitalen Technologien genutzt werden. Darüber hinaus müssen die damit verbundenen Risiken gemanagt und das Vertrauen der Menschen in die Technologien gefördert werden, um die Schweiz in eine führende digitale Nation zu transformieren. Mit der künstlichen Intelligenz hat ein neues Kapitel in der Digitalisierung begonnen. Besondere Prioritäten sind die Bildung, eine vertrauenswürdige digitale Infrastruktur, Cybersecurity, eSustainability, Digital Health und eGovernment. Die damit verbundenen Herausforderungen geht digitalswitzerland in enger Zusammenarbeit mit den über 170 Mitgliedern, Partnern und anderen Verbänden an.