Regierung des Kantons St.Gallen, Regierungsgebäude, 9001 St.Gallen

Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

Regierung des Kantons St.Gallen
Regierungsgebäude
9001 St.Gallen
T +41 58 229 74 44
info.sk@sg.ch

St.Gallen, 11. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe; Vernehmlassungsantwort

Sehr geehrter Herr Bundesrat

Mit Schreiben vom 12. Januar 2022 laden Sie uns zur Vernehmlassung zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen (KI) für Cyberangriffe ein. Wir danken für diese Gelegenheit und nehmen gern wie folgt Stellung:

Wir begrüssen die vorgesehene Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen bei Cyberangriffen und die damit verbundene Definition der Aufgaben des Nationalen Zentrums für Cybersicherheit (NCSC).

Die Vorlage fokussiert auf die Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe gegenüber der NCSC und lässt dabei (fast) ausser Acht, dass auch die Kantone für den Schutz der Schweiz (bzw. ihres Kantons) vor Cyberrisiken, für den Bevölkerungsschutz und für kritische Infrastrukturen zuständig sind. Alle kritischen Infrastrukturen sind auf Kantonsgebiet. Auch deshalb müssen die Kantone stärker in die Vorlage miteinbezogen und berücksichtigt werden. Nur so können die Kantone ihrer Verantwortung gegenüber ihren kritischen Infrastrukturen beim Schutz vor Cyberrisiken nachkommen.

Aufgrund der Relevanz der kritischen Infrastrukturen für die Bevölkerung und deren Lebensgrundlagen genügt die Einführung einer Meldepflicht von KI-Betreiberinnen über bereits erfolgte Cyberangriffe allein nicht. Der Staat (Bund und Kantone) muss bereits präventiv die Möglichkeit haben, dort einzuschreiten, wo die KI-Betreiberinnen keine oder ungenügende Vorkehrungen für den Schutz vor Cyber-Risiken und weiteren Risiken treffen. Es sind daher verbindliche sektorenübergreifende Vorgaben für alle KI-Betreiberinnen auf Bundesebene zwingend erforderlich.

Entsprechend der EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) braucht es zwingend auch in der Schweiz Vorgaben, welche die Anbieter wesentlicher Dienste verpflichten, Sicherheitsvorkehrungen zu ergreifen.

Dazu gehören die Risikovorsorge, die Gewährleistung der Sicherheit von Netz- und Informationssystemen und Massnahmen, welche die Auswirkungen von Sicherheitsvorfällen so gering wie möglich halten.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und verweisen ergänzend auf den Anhang.

Im Namen der Regierung

Marc Mächler
Präsident

KANTON ST. GALLEN
REGIERUNG

Dr. Benedikt van Spyk
Staatssekretär

Beilage:
Anhang

Zustellung auch per E-Mail (pdf- und Word-Version) an:
ncsc@gs-efd.amdin.ch

Anhang zur Vernehmlassungsantwort «Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe»

Die Regierung des Kantons St.Gallen ersucht im Zusammenhang mit der genannten Vorlage um die Berücksichtigung der folgenden Punkte:

Grundsätzliches

- Die Vorlage fokussiert auf die Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe gegenüber der NCSC und lässt dabei (fast) ausser Acht, dass auch die Kantone für den Schutz der Schweiz (bzw. ihres Kantons) vor Cyberrisiken, für den Bevölkerungsschutz und für kritische Infrastrukturen zuständig sind.

- Alle kritischen Infrastrukturen sind auf Kantonsgebiet. Auch deshalb müssen die Kantone stärker in die Vorlage miteinbezogen werden; namentlich in die Aufgaben des NCSC (1. Abschnitt) und in den Strauss möglicher Aufgaben, die durch die Meldung ausgelöst werden können (u.a. Pflicht, umgehend die Kantone über eine Meldung zu informieren; Aufgaben des NCSC gegenüber den Kantonen; Zusammenarbeit von NCSC und Kantonen usw.). Nur so können die Kantone ihrer Verantwortung gegenüber ihren kritischen Infrastrukturen nachkommen.

- Die Zusammenarbeit zwischen dem NCSC und den Kantonen usw. ist im ISG zu regeln.

- Eines der Hauptmotive für die Einführung einer Meldepflicht ist die «Frühwarnung». Ausführungen zu Frühwarnungsmethoden sind in der Vorlage jedoch keine enthalten; solche sind ergänzend aufzunehmen.

- Es ist eine Anzeigepflicht gegenüber den zuständigen Strafverfolgungsbehörden im ISG zu statuieren.

- Der reibungslose Betrieb der ersten Säule der Sozialversicherungen hängt von unterschiedlichen Akteuren ab, die – je nach Bereich – stärker oder weniger stark miteinander kooperieren und Daten austauschen. So besteht ein Spannungsverhältnis zwischen den Betreiberinnen von kritischen Infrastrukturen i.S.v. Art. 74a ISG und den in Art. 74b Bst. s ISG aufgeführten Herstellern von Hard- und Software. Die Ausführungsbestimmungen zum ISG müssen diesem Umstand Rechnung tragen und die Verantwortlichkeiten für die Meldung generisch für unterschiedliche Konstellationen mit Beteiligung verschiedener Organisationen festlegen. So muss insbesondere die Verpflichtung für die IT-Lieferanten der Durchführungsstellen geklärt werden, deren Situation in Art. 74b Bst. s ISG nicht eindeutig festgeschrieben ist.

Gesetzesbestimmungen

Art. 73a
In Art. 73a werden die Aufgaben des NCSC zum Schutz der Schweiz vor Cyberrisiken aufgeführt. Der Schutz der Schweiz vor Cyberrisiken ist nicht allein Aufgabe des Bundes bzw. des NCSC. Für den Schutz der Schweiz vor Cyberrisiken sind insbesondere auch die Kantone (inkl. Gemeinden) zuständig. Auch für die KI sind die Kantone zuständig. Die

Aufgaben des NCSC sind daher auch mit Bezug auf die Kantone (inkl. Gemeinden) im Gesetzestext explizit zu nennen. So ist namentlich die Information und Weiterleitung von Informationen an die zuständigen kantonalen Behörden für Cybersicherheit und/oder Schutz Kritischer Infrastrukturen als Aufgabe explizit zu nennen. Die Aufgabenliste ist zusammen mit den Kantonen zu ergänzen. Auch ist die Zusammenarbeit und die Aufgabenteilung des NCSC und der Kantone im ISG zu regeln.

Art. 73b und Art. 73c
In Art. 73b und Art. 73c ist die Bearbeitung von Meldungen zu Cybervorfällen und Schwachstellen sowie die Weiterleitung von Informationen geregelt. Ungenügend ist diese Regelung mit Bezug auf die Kantone. Informationen über Vorfälle müssen zwingend und unverzüglich an die Kantone weitergeleitet werden. Auch muss das NCSC die Kantone informieren, wenn das NCSC Betriebe im Verantwortungsbereich der Kantone unterstützt. Nur so ist eine Lagebeurteilung hinsichtlich allfälliger Massnahmen auch für die Kantone möglich.

Art. 74b und Art. 74c
In Art. 74b werden die Bereiche aufgelistet, für welche die Meldepflicht gilt; Art. 74c nennt die Ausnahmen. Diese Bereiche und Kategorien sind nicht deckungsgleich mit der vom Bundesamt für Bevölkerungsschutz (BABS) verwendeten Systematik der Leistungsklassen und dementsprechend auch nicht mit den in den Kantonen erstellten und verwendeten KI-Inventaren. Die Identität der Begriffe ist conditio sine qua non – nur so lässt sich die Meldepflicht präzise umsetzen und ist eine Kommunikation der Behörden mit den KI-Betreiberinnen möglich.

Art. 74d
Art. 74d nennt die zu meldenden Cyberangriffe. Art. 74d Abs. 1 Bst. b sieht vor, dass «ein Cyberangriff gemeldet werden muss, wenn Anzeichen dafür bestehen, dass ein fremder Staat ihn ausgeführt oder veranlasst hat». Einerseits fragen wir uns, ob solche Anzeichen für KI-Betreiberinnen überhaupt erkennbar sein können. Andererseits würden wir die Aufnahme eines solchen Passus in Abs. 2 als zutreffender erachten. Auch würden wir die Aufnahme eines expliziten Melderechts im Gesetzestext (z.B. als Abs. 2 von Art. 74a) als hilfreich betrachten.

Art. 76a ISG
In Art. 76a ist die Unterstützung des NCSC für Behörden geregelt. Art. 76a Abs. 4 sieht vor, dass das NCSC die kantonalen Stellen unterstützen «kann». Die «Kann-Bestimmung» ist durch eine «Muss-Bestimmung» zu ersetzen:

[4] Es ~~kann~~gewährt den kantonalen Stellen, die für die Cybersicherheit zuständig sind, Zugriff auf Informationen im Abrufverfahren ~~gewähren~~, die für den Schutz kantonaler Behörden und kantonaler kritischer Infrastrukturen vor Cyberrisiken erforderlich sind.