Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 30. März 2022

541. Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), Vernehmlassung

Mit Schreiben vom 12. Januar 2022 hat das Eidgenössische Finanzdepartement das Vernehmlassungsverfahren zur Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (SR 126, BBl 2020 9975) betreffend Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe eröffnet.

Cyberrisiken sind zu einer der wichtigsten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden. Es ist von grosser Bedeutung, dass Angriffe auf Schweizer Unternehmen und Behörden frühzeitig erkannt und die Bedrohungslage möglichst genau eingeschätzt werden kann. Dazu soll eine Meldepflicht für Betreiberinnen kritischer Infrastrukturen eingeführt werden. Die Meldepflicht soll es dem Nationalen Zentrum für Cybersicherheit (NCSC) ermöglichen, eine verbesserte Übersicht über Cyberangriffe in der Schweiz zu gewinnen, Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und alle anderen Betreiberinnen kritischer Infrastrukturen zu warnen. Mit der Einführung einer Meldepflicht schliesst die Schweiz eine Lücke im Dispositiv der Cybersicherheit. Meldepflichten für Cyberangriffe sind in vielen Ländern bereits etabliert und gelten seit 2018 in allen EU-Mitgliedstaaten. Die Vorlage ist auf die bestehenden Meldepflichten (insbesondere die neu eingeführte datenschutzrechtliche Meldepflicht) abgestimmt und so ausgestaltet, dass sie für die betroffenen Unternehmen und Behörden einen möglichst geringen Mehraufwand bedeutet. Die Schaffung einer zentralen Meldestelle auf Bundesebene, das NCSC, ist dabei unumgänglich, da nur eine zentrale Stelle sicherstellen kann, dass die Meldepflicht die Zwecke der Frühwarnung und der besseren Übersicht über die Bedrohungslage erfüllt. Die Vorlage schafft auch die Grundlage für eine Zusammenarbeit des NCSC mit anderen Stellen, insbesondere mit den Strafvollzugsbehörden.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Schreiben an das Eidgenössische Finanzdepartement, 3003 Bern (Zustellung auch per E-Mail als PDF- und Word-Version an ncsc@gs-efd.admin.ch):

Mit Schreiben vom 12. Januar 2022 haben Sie uns eingeladen, zur Änderung des Bundesgesetzes über die Informationssicherheit beim Bund (SR 126) Stellung zu nehmen. Wir danken für diese Gelegenheit und äussern uns wie folgt:

Wir halten die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe für eine sinnvolle ergänzende Massnahme und ein wertvolles Instrument in einer koordinierten Cyberabwehr. Sie sollte jedoch mit einem angemessenen Mehrwert für die beteiligten Akteurinnen und Akteure verbunden sein. Mit den nachstehenden Bemerkungen möchten wir die Entwicklung in diesem Sinne unterstützen.

Allgemeine Bemerkungen

Der erläuternde Bericht setzt sich mit Anreizen und Sanktionen auseinander. Nach unserem Dafürhalten sollte insbesondere der Mehrwert für die verpflichteten Akteurinnen und Akteure im Sinne einer Unterstützung verstärkt werden. Neben der vorgesehenen technischen Einschätzung und Unterstützung steht dabei die frühzeitige Verteilung von Informationen an alle Akteurinnen und Akteure im Vordergrund, beispielsweise über auffällige Aktivitäten oder Anomalien sowie drohende oder laufende Angriffe. Art. 73b Abs. 2 E-ISG sollte daher weiter formuliert werden. In Art. 74 E-ISG sollte sodann klarer umschrieben werden, was mit «Informationen zu aktuellen Cyberrisiken» als Unterstützungsleistung gemeint ist.

Zudem weisen wir darauf hin, dass die Meldepflicht ein nach innen gerichtetes Instrument des Nationalen Zentrums für Cybersicherheit (NCSC) ist. Schutzbedarf besteht allerdings auch nach aussen. Deshalb sind an den Netzübergängen zwischen Ausland und Inland (CH data carriers) Instrumente und Sicherheitsmassnahmen einzusetzen, damit die Schweiz und damit auch der Kanton Zürich vor internationaler Cyberkriminalität geschützt werden kann. Dieses Thema ist allerdings nicht Gegenstand der Vorlage.

Bemerkungen zu einzelnen Bestimmungen

Art. 74 Unterstützung von Betreiberinnen von kritischen Infrastrukturen

Gemäss Art. 74 Abs. 3 E-ISG soll das NCSC private Betreiberinnen bei der Bewältigung von Cybervorfällen und der Behebung von Schwachstellen beraten und unterstützen, wenn die Beschaffung gleichwertiger Unterstützung auf dem Markt nicht rechtzeitig möglich ist. Dies birgt die Gefahr von Fehlanreizen: Eine von einem Cyberangriff betroffene Betreiberin kann sich so auf Staatskosten vom NCSC unterstützen lassen, ohne ein angemessenes Service-Level-Agreement mit einem Incident Containment Service abzuschliessen. Wir regen daher an, jede Betreiberin einer kritischen Infrastruktur zum Bezug eines Incident Containment Service mit vorgegebenen Mindestanforderungen zu verpflichten.

Art. 74b Bereiche

Wir regen an, die Meldepflicht stufenweise (z. B. nach Sektoren) einzuführen. So lassen sich Erfahrungen mit den ersten Beteiligten sammeln und daraus frühzeitig mögliche Verbesserungen ableiten. Zudem erhält das NCSC Zeit, um sich auf seine neue Aufgabe einzustellen. So kann eine Überlastung des NCSC durch viele gleichzeitige Meldungen vermieden werden, was trotz seiner langen Erfahrung im Umgang mit Meldungen eine Gefahr darstellt.

Des Weiteren setzt eine Meldepflicht voraus, dass Cyberangriffe erkannt werden können. Viele Betreiberinnen in den in Art. 74b E-ISG aufgeführten Bereichen verfügen jedoch nicht über die dafür notwendigen Mittel. Es ist daher zu überlegen, wie insbesondere Städte und Gemeinden bei der Erkennung von Cyberangriffen unterstützt werden können. Eine Möglichkeit wäre der Aufbau von kantonalen oder regionalen Cyber Defence Centers.

Art. 74d Zu meldende Cyberangriffe

Art. 74d E-ISG umschreibt die zu meldenden Cyberangriffe in allgemeiner Form. Diese Bestimmung lässt einen allzu grossen Auslegungsspielraum. Für die praktische Handhabung und die erforderliche Handlungssicherheit der verpflichteten Akteurinnen und Akteure bedürfte es einer leicht verständlichen und nachvollziehbaren Umschreibung der zu meldenden Cyberangriffe.

Das NCSC sollte zudem gesetzlich dazu verpflichtet werden, Meldungen von Cyberangriffen, die gemäss Art. 74d Abs. 2 E-ISG mit Erpressung, Drohung oder Nötigung verbunden sind, an die Strafverfolgungsbehörden weiterzuleiten, soweit sich diese Pflicht nicht aus dem Bundespersonalrecht ergibt.

Art. 74f Übermittlung der Meldung

Der organisatorische und technische Aufwand für die beteiligten Akteurinnen und Akteure muss überschaubar bleiben. Dies betrifft nicht nur die Vermeidung von Mehrfachmeldungen. Das zukünftige System muss einfach und eingängig zu bedienen sein. Der Meldeprozess muss sich einfach in die verschiedenen Organisations- und Systemlandschaften der betroffenen Akteurinnen und Akteure einfügen.

II. Mitteilung an die Geschäftsleitung des Kantonsrates, die Mitglieder des Regierungsrates sowie an die Finanzdirektion.

Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli