Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 4. September 2024

908. Verordnung über die Cybersicherheit (Vernehmlassung)

Mit Schreiben vom 22. Mai 2024 hat das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport das Vernehmlassungsverfahren zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung) eröffnet.

Mit der Änderung vom 29. September 2023 des Bundesgesetzes vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG; SR 128) haben die eidgenössischen Räte die Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen beschlossen. Die Meldepflicht soll es dem Bundesamt für Cybersicherheit (BACS) ermöglichen, eine verbesserte Übersicht über Cyberangriffe in der Schweiz zu gewinnen, Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und Betreiberinnen kritischer Infrastrukturen zu warnen.

Mit der Cybersicherheitsverordnung legt der Bundesrat die Ausführungsbestimmungen zu dieser Gesetzesänderung vor. Die Verordnung legt fest, welche Ausnahmen von der Meldepflicht gelten, und konkretisiert, welche Cyberangriffe meldepflichtig sind. Zudem wird das Verfahren zur Erfüllung der Meldepflicht definiert. Dadurch wird klar, welche Organisationen und Behörden welche Art von Cyberangriffen wie und innerhalb welcher Frist zu melden haben. Zusätzlich regelt die Verordnung, wie das BACS die sich aus dem ISG ergebenden Aufgaben erfüllen soll, und definiert die Strukturen für die strategische Steuerung der Cybersicherheit in der Schweiz. Die Verordnung definiert damit wesentliche Elemente der Cybersicherheit in der Schweiz und legt die Grundlage für eine zielgerichtete Umsetzung der Meldepflicht für Cyberangriffe.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Schreiben an das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport, 3003 Bern (Zustellung auch per E-Mail als PDF- und Word-Version an ncsc@ncsc.admin.ch):

Mit Schreiben vom 22. Mai 2024 haben Sie uns eingeladen, zum Entwurf zur Verordnung über die Cybersicherheit (Cybersicherheitsverordnung) Stellung zu nehmen. Wir danken Ihnen für diese Gelegenheit und äussern uns wie folgt:

Wir unterstützen die vorgeschlagene Verordnung. Sie sollte mit einem angemessenen Mehrwert für die beteiligten Akteurinnen und Akteure verbunden sein. Mit den nachstehenden Bemerkungen möchten wir die Entwicklung in diesem Sinne unterstützen.

I. Allgemeine Bemerkungen

Mit RRB Nr. 541/2022 haben wir bereits zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen Stellung genommen. Wir unterstützen den Entwurf zur Cybersicherheitsverordnung und deren Beitrag zu einer nationalen Betrachtungsweise der Cybersicherheit. Durch die Cybersicherheitsverordnung wird eine Stärkung der kantonalen Cyberresilienz angestrebt, namentlich durch die Definition einer Nationalen Cyberstrategie in Abstimmung mit den Kantonen (Art. 2 und 4) und die Unterstützung der kantonalen Behörden durch das Bundesamt für Cybersicherheit (BACS; Art. 7 und 10).

In Bezug auf die Meldepflicht der kantonalen Behörden regen wir an, den Begriff der kritischen Infrastrukturen von Behörden (Art. 5 Bst. c Informationssicherheitsgesetz [ISG; SR 128] in Verbindung mit Art. 74b Abs. 1 Bst. b ISG) in der Cybersicherheitsverordnung zu konkretisieren. Eine Qualifikation sämtlicher Organisationseinheiten als «Betreiber kritischer Infrastrukturen» erscheint nicht als zielführend, da die Kritikalität der jeweiligen Dienste damit ausser Acht gelassen wird.

Durch die neue Meldepflicht erhält eine Bundesbehörde Kenntnis von strafbaren Handlungen, weshalb wir die Institutionalisierung der Zusammenarbeit des BACS mit den kantonalen Strafverfolgungsbehörden in der Cybersicherheitsverordnung empfehlen. Das BACS hat keine strafrechtlichen Kompetenzen oder Aufgaben, da es sich nur indirekt mit Cyberkriminalität befasst. Zur wirksamen Bekämpfung von Cyberkriminalität ist indessen die zeitnahe Einbindung der Strafverfolgungsbehörden erfolgskritisch, namentlich in Bezug auf die Beweissicherung. Angesichts der zeitlichen Dringlichkeit bei der Strafverfolgung von Cyberkriminalität ist es zweckdienlich, bei einer Meldung an das BACS gleichzeitig Strafanzeige bei der zuständigen Strafverfolgungsbehörde einzureichen.

Daher empfehlen wir, mit einer Anzeigepflicht des BACS sicherzustellen, dass Meldungen an die zuständigen Strafverfolgungsbehörden weitergeleitet werden (vgl. auch Bemerkungen zu Art. 7 und 15).

Sodann würden wir eine stärkere Berücksichtigung der Lieferkette in der Cybersicherheitsverordnung begrüssen, zumal sich diese als primäres Angriffstor für Cyberangriffe erweist. Namentlich regen wir an, den betroffenen Dienstleister als Meldeinhalt aufzunehmen (vgl. Bemerkung zu Art. 19). Zudem schlagen wir differenziertere Regelungen für Angriffe auf die Lieferkette vor:

– Bei Cyberangriffen auf Betreiberinnen von Informatikinfrastrukturen mit Auswirkungen auf eine grosse Zahl verschiedener meldepflichtiger Organisationen und Behörden (insbesondere Hyperscaler und Betreiberinnen von Rechenzentren) schlagen wir vor, dass anstelle der gleichzeitigen Meldung durch alle Meldepflichtigen in einem ersten Schritt nur die Betreiberin der Informatikinfrastruktur eine Meldung gegenüber dem BACS absetzt. Damit könnte das BACS seine Ressourcen zielgerichtet für die Behandlung des Cyberangriffs einsetzen, ohne dass diese zusätzlich oder gar vorrangig durch die Administration einer Vielzahl von Meldungen gebunden sind. Die weiteren betroffenen meldepflichtigen Organisationen sollten ihre eigenen Meldungen zeitverzögert absetzen können.
– Es wäre klarzustellen, dass die Frist von 24 Stunden für meldepflichtige Organisationen und Behörden erst mit der eigenen Kenntnisnahme des Cyberangriffs zu laufen beginnt. In diesem Zusammenhang wäre die Verankerung einer Mitteilungspflicht von Dienstleistern an meldepflichtige Organisationen und Behörden in der Cybersicherheitsverordnung begrüssenswert.

II. Bemerkungen zu einzelnen Bestimmungen

1. Cybersicherheitsverordnung

Art. 2 Nationale Cyberstrategie

Die koordinierte Definition einer Nationalen Cyberstrategie ist zu begrüssen, da sie den Kantonen eine frühzeitige Anpassung und Ergänzung eigener Cybersicherheitsstrategien erlaubt.

Namentlich beim Aspekt der «Bekämpfung der Cyberkriminalität» muss indessen der Beizug von Staatsanwaltschaft und Polizei als fachkompetente Behörden sichergestellt werden, und zwar unabhängig von deren Vertretung im Rahmen des Steuerungsausschusses Nationale Cyberstrategie. Es ist festzuhalten, dass die Strategie und die Befugnisse zur strafrechtlichen Verfolgung von Cybervorfällen bei den Strafverfolgungsbehörden verbleiben und dass deren Weisungsfreiheit durch Festlegungen in der Nationalen Cyberstrategie nicht berührt werden.

Art. 7 Technische Analyse von Cybervorfällen und Cyberbedrohungen

Zulässige Gegenmassnahmen

Mit Bezug auf die Zulässigkeit von Gegenmassnahmen bei einem Cyberangriff bestehen unterschiedliche Auffassungen und ein rechtlich enger Rahmen. Demgegenüber sind technisch viele Gegenmassnahmen möglich. Es ist zu definieren, was das Computer Emergency Response Team (CERT) unter Präventiv- und Gegenmassnahmen versteht. Je nach Verständnis und Umfang sind erweiterte gesetzliche Grundlagen für Massnahmen erforderlich, die in der Regel nur den Strafverfolgungsbehörden gemäss der Schweizerischen Strafprozessordnung (SR 312.0) oder dem Nachrichtendienst gemäss dem Nachrichtendienstgesetz (SR 121) offenstehen.

Wir empfehlen daher, Gegenstand, Wirkungsziele und Umfang der «Gegenmassnahmen» zu definieren und die dafür nötigen Kompetenzen des CERT zu umschreiben.

Zusammenarbeit mit den Strafverfolgungsbehörden

Bei Cyberangriffen besteht für die Strafverfolgungsbehörden üblicherweise Gefahr im Verzug hinsichtlich der Sicherung der nötigen Beweise. Zudem können Sicherungsmassnahmen der Betroffenen oder des CERT die forensische Erhebung von Beweismitteln vereiteln, da die Daten durch die vorgängig vorgenommenen Manipulationen kompromittiert werden. Dies kann einen faktischen oder rechtlichen Beweisverlust zur Folge haben.

Wir regen daher die Formalisierung und Institutionalisierung der Zusammenarbeit mit der Staatsanwaltschaft und der Polizei an. Insbesondere schlagen wir vor, dass das BACS bzw. das CERT diese informieren und in die technische Analyse miteinbeziehen soll.

Art. 15 Übermittlung und Nutzung der Informationen

Gemäss Art. 15 soll das BACS über die Weitergabe der Informationen frei entscheiden können. Diese Regelung steht in einem Spannungsverhältnis zum Informationsbedarf der Strafverfolgungsbehörden. Es ist anzuerkennen, dass ein vertrauensbasierter Informationsaustausch mit den Informationslieferantinnen und -lieferanten schützenswert ist.

Eine effektive Strafverfolgung ist aber ohne rasche Informationen nicht möglich. Im Ergebnis und angesichts der betroffenen Rechtsgüter sind öffentliche Interessen, namentlich Strafverfolgungsinteressen, höher zu gewichten als die Ermessensfreiheit des BACS. Immerhin sind die Informationen bei den Strafverfolgungsbehörden auch durch das Amtsgeheimnis geschützt und werden nur zweckgebunden verwendet.

Daher regen wir an, dass das BACS verpflichtet wird, Meldungen über Cyberangriffe gemäss Art. 18 zur strafrechtlichen Beurteilung an die zuständigen Strafverfolgungsbehörden weiterzuleiten.

Sobald am Informationssystem angeschlossene Strafverfolgungsbehörden von einem Offizialdelikt erfahren, sind sie gesetzlich verpflichtet, die Ermittlungen aufzunehmen. Das BACS hat aus diesem Grund sicherzustellen, dass bei den veröffentlichten Informationen die angegriffene Betreiberin kritischer Infrastruktur nicht ersichtlich bzw. nicht ermittelbar ist. Allgemein sollte in der Verordnung genauer festgelegt werden, wie das BACS bzw. die Strafverfolgungsbehörden mit den strafrechtlich relevanten Informationen umzugehen haben, die sie über das Informationssystem erhalten (vgl. Art. 76 Abs. 3 Satz 2 ISG).

Art. 18 Zu meldende Cyberangriffe

Art. 18 Abs. 3 geht von einem längeren Zeitraum aus, wenn nach der Entdeckung festgestellt wird, dass der Cyberangriff bereits vor mehr als 90 Tagen erfolgt ist. Dies kann beispielsweise durch die Auswertung von Logdaten geschehen. Die Datenschutzstellen wiederum verlangen eine möglichst kurze Aufbewahrung von Logdaten. Daher wäre eine grundsätzliche Regelung wünschenswert, die sich darüber ausspricht, welche Logdaten wie lange aufbewahrt werden dürfen.

Art. 19 Inhalt der Meldung

Zur Berücksichtigung von Angriffen auf die Lieferkette und zur angemessenen Beurteilung der nationalen Bedrohungslage durch das BACS empfehlen wir, den Inhalt der Meldung um «involvierte Dienstleister oder andere Dritte» zu ergänzen, um Erkenntnisse über den Angriffsweg auf die betroffene Organisation oder Behörde sicherzustellen.

Die Meldung sollte auch die Information enthalten, bei welcher Behörde Strafanzeige erstattet wurde, damit das BACS mit dieser bei einer entsprechenden Datenfreigabe Informationen austauschen kann.

Zudem sollte festgehalten werden, dass die Meldungen auf dem jeweiligen Wissensstand zum Zeitpunkt der Meldung beruhen und auf der Grundlage neuer Erkenntnisse nachgeführt werden können und sollen.

2. Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport

Es wird weder in der vorgeschlagenen Regelung von Art. 15a Abs. 2 Bst. h der Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (SR 172.214.1) noch in den Erläuterungen dazu umschrieben, ob und inwieweit das BACS ausschliesslich zur Vertretung der Schweiz in internationalen Gremien berechtigt sein soll. Die Polizei nimmt im Bereich der Cyberbedrohungen

ähnliche Aufgaben wahr, und auch die Staatsanwaltschaften bewältigen Cybervorfälle. Ein nationaler und internationaler Austausch zwischen den Strafverfolgungsbehörden ist längst etabliert.

Entsprechend regen wir an, den Umfang, in dem das BACS in den Gremien mitwirkt, genauer zu umschreiben und auf den Bereich Cybersicherheit zu beschränken. Der nationale und internationale Austausch der Strafverfolgungsbehörden zum präventiven Schutz vor Cyberbedrohungen und zur repressiven Bewältigung von Cybervorfällen darf durch diese Bestimmung nicht eingeschränkt werden.

II. Mitteilung an die Mitglieder des Regierungsrates und die Finanzdirektion.

Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli