Regierungsrat, Postfach, 6301 Zug

Nur per E-Mail
Eidgenössisches Finanzdepartement
Herr Bundesrat Ueli Maurer
Bernerhof
3003 Bern

Zug, 15. März 2022 rv

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe
Vernehmlassung des Kantons Zug

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 hat das Eidgenössische Finanzdepartement (EFD) das Vernehmlassungsverfahren eröffnet und die Kantonsregierungen zur Einreichung einer Stellungnahme bis am 14. April 2022 eingeladen.

Wir stellen folgende

Anträge:

1. nArt. 73b Abs. 2 sei dahingehend zu ergänzen, dass mit gemeldeten Sicherheitsvorfällen nicht vertrauliche interne Informationen wie interner Netzaufbau mit IP-Adressen oder Anmeldeinformationen an Dritte weitergeleitet werden dürfen. Ausserdem sei explizit festzuhalten, dass das NCSC aufgrund von gemeldeten Sicherheitsvorfällen kein Bewertungs-Dashboard im Sinne einer qualitativen Informationssicherheitsbewertung pro Unternehmen oder Behörden erstellt.

2. nArt. 73c Abs. 2 sei dahingehend zu ändern, dass durch eine nähere Definition der Schwere der Straftat der Ermessensspielraum der Leiterin oder des Leiters der NCSC bei der Weitergabe von Informationen an die Strafverfolgungsbehörden eingegrenzt wird.

3. Die Geltungsbereiche und die Menge der meldepflichtigen Betreiberinnen kritischer Infrastrukturen gemäss nArt. 74b sei zu überprüfen und zu reduzieren.

4. Der Adressatenkreis der Auswertungen und technischen Analysen gemäss nArt. 76a Abs. 1 sei auf die Strafverfolgungsbehörden auszuweiten.

Begründung:

Allgemeines
Kaum ein Risikofeld wird in den nächsten Jahren von der öffentlichen und privaten Hand einen derart hohen Effort fordern wie die Cyberkriminalität. Cyberrisiken sind zu einer der wichtigsten Bedrohungen der Sicherheit und der Wirtschaft der Schweiz geworden.

Das Nationale Zentrum für Cybersicherheit (NCSC) als geplante, neue Meldestelle kann auf die mehrjährige Erfahrung der vormaligen Stelle «MELANI» aufbauen. Das NCSC hat sich die Reputation erarbeitet, sehr professionelle und wertvolle Arbeit zu leisten. Die geplante Meldepflicht ermöglicht dem NCSC eine verbesserte Übersicht über Cyberangriffe und erlaubt, Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und andere Betreiberinnen kritischer Infrastrukturen zu warnen. Die Meldepflicht soll im Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) als Rechtsgrundlage verankert werden.

Aufgrund des Systemwechsels von einer bisher freiwilligen Meldung zu einer Pflichtmeldung wird der Aufwand steigen, zumal auch eine Unterstützungsleistung an die betroffenen Infrastrukturbetreiberinnen und -betreiber vorgesehen ist. Entsprechend muss der Bund das NCSC personell aufstocken.

Zum Antrag 1:
Art. 73b Abs. 2 umfasst den Schutz von datenschutzrelevanten Informationen. Bei Sicherheitsvorfällen fallen aber weitere vertrauliche Informationen wie Zugangsdaten, Benutzernamen, Netzwerkadressen, Systembeschreibungen, interne Organisationsdaten etc. an, die unter keinen Umständen an die Öffentlichkeit gelangen dürfen.

Gemäss Vorlage werden die gemeldeten Sicherheitsvorfälle ausgewertet. Die Auswertung darf nicht an die Öffentlichkeit gelangen, da sonst Rückschlüsse auf die Schwachstellen der einzelnen Vorfälle publik werden und dadurch durch Hacker ausgenutzt werden könnten. Zudem besteht die Gefahr, dass Politik und Gesellschaft Ranglisten erstellen und dadurch falsche Eindrücke der gemeldeten Vorfälle entstehen. Beispielsweise könnten Firmen, die viele auch weniger gravierende Vorfälle melden, als unsicher angesehen werden. Solche Vergleiche müssen vermieden werden, weil gerade in öffentlichen Unternehmen die Meldungen dann begründet werden müssten. Allfällige öffentlich zugängliche grafische Vergleiche zwischen den Unternehmen und Bereichen könnten deshalb dazu führen, dass weniger Sicherheitsvorfälle gemeldet werden, da die IT, anstelle Gegenmassnahmen einzuleiten, sich mit Rechtfertigungen beschäftigen muss.

Zum Antrag 2:
Die Weitergabe von Informationen an die Strafverfolgungsbehörden betrachten wir als sinnvoll (vgl. den erläuternden Bericht, Seiten 5 und 15 zu nArt. 73c Abs. 2). Problematisch erachten wir jedoch die Möglichkeit einer von erheblichem Ermessen abhängigen *eingeschränkten* Wei-

tergabe von Informationen an die Strafverfolgungsbehörden, sei es hinsichtlich der Meldung an sich oder deren Vollständigkeit. Die Leiterin oder der Leiter des NCSC entscheidet hiernach mittels eigenem Ermessen über die Schwere der Straftat und die Abwägung zwischen dem Interesse des Staates an einer Strafverfolgung und dem Interesse der meldenden Person an der Vertraulichkeit der Meldung. Dies birgt das Risiko eines unvollständigen Lagebildes einerseits und Wissenslücken, insbesondere bezüglich des Auftretens neuer Phänomene, andererseits. Die koordinierte Strafverfolgung wird damit erschwert.

Begrüsst wird dagegen die Spezifizierung der Meldepflicht gemäss nArt. 74d Abs. 2 (vgl. Seite 21 des erläuternden Berichts) hinsichtlich der Vorgabe, dass ein Cyberangriff bei strafrechtlich relevanten Begleitumständen immer zu melden ist. Dies erlaubt eine umfassende Einschätzung der Bedrohungslage für kritische Infrastrukturen durch Cyberkriminelle.

Zum Antrag 3:
Wir begrüssen die Einführung einer Meldepflicht bei Cyberangriffen für Betreiberinnen kritischer Infrastrukturen, die Schaffung der erforderlichen gesetzlichen Grundlage durch entsprechende Ergänzung des Informationssicherheitsgesetzes (ISG) sowie die Verankerung des nationalen Zentrums für Cybersicherheit als zentrale Meldestelle.

Gleichzeitig sehen wir, dass mit der Meldepflicht ein potenziell grosser administrativer Aufwand auf das NCSC und die Betreiberinnen kritischer Infrastrukturen zukommt. Zu wenig erkennbar ist, wie stark und mit welchen Aufgaben allenfalls die Kantone von dieser Gesetzesrevision betroffen sein werden. So liegt etwa die Zuständigkeit für die Verfolgung und Beurteilung von Widerhandlungen einer Verfügung des NCSC gemäss nArt. 74i bei den Kantonen. Es scheint uns, dass die Liste der Betreiberinnen kritischer Infrastrukturen (nArt. 74b) grosszügig ausgefallen ist.

Zum Antrag 4:
Die Bestimmung von nArt. 76a regelt Art, Umfang und Zweck der Zurverfügungstellung von Informationen des NCSC gegenüber anderen Behörden (vgl. auch Seite 24 des erläuternden Berichts). Während Abs. 2, 3 und 4 die Zurverfügungstellung von Informationen gegenüber dem Nachrichtendienst des Bundes (NDB), den Strafverfolgungsbehörden und den kantonalen Cybersicherheitsstellen in genereller Hinsicht regeln, beschränkt Abs. 1 die Auswertungs- und Analyseunterstützung durch das NCSC auf den NDB.

Wir danken Ihnen für die Gelegenheit zur Stellungnahme und bitten Sie, unsere Anliegen zu berücksichtigen.

Zug, 15. März 2022

Freundliche Grüsse
Regierungsrat des Kantons Zug

sign.

Martin Pfister
Landammann

sign.

Tobias Moser
Landschreiber

Kopie per E-Mail an:
- Eidgenössisches Finanzdepartement (ncsc@gs-efd.admin.ch) im Word- und PDF-Format
- Zuger Mitglieder der Bundesversammlung
- Finanzdirektion (info.fd@zg.ch)
- Volkswirtschaftsdirektion (info.vd@zg.ch)
- Sicherheitsdirektion (info.sd@zg.ch)