Generalsekretariat des Eidgenössischen
Finanzdepartements
Nationales Zentrum für Cybersicherheit
NCSC

Per E-Mail an: ncsc@gs-efd.admin.ch

Bern, 12. April 2022

Stellungnahme zum Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund (ISG): Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe

Sehr geehrter Herr Bundesrat,
sehr geehrte Damen und Herren

Wir bedanken uns für die Möglichkeit zu oben genanntem Geschäft Stellung zu beziehen und nehmen diese hiermit gerne fristgerecht wahr.

asut, der Schweizerische Verband der Telekommunikation repräsentiert die Telekommunikations- und Netzwerkbranche und sämtliche Wirtschaftszweige sind im Verband vertreten. Wir gestalten und prägen gemeinsam mit unseren Mitgliedern die digitale Transformation der Schweiz und setzen uns für optimale politische, rechtliche und wirtschaftliche Rahmenbedingungen für die digitale Wirtschaft ein. Die vorgeschlagene Änderung des ISG ist für unsere Branche von hoher Relevanz.

asut unterstützt das Ziel, die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken zu erhöhen und begrüsst die vorgeschlagenen Anpassungen des ISG im Grundsatz. asut regt jedoch die Schaffung einer zentralen Meldestelle für sämtliche Cybervorfälle an. Zu präzisieren ist zudem die Meldepflicht (Art. 74a), die ausdrücklich nur bei Cybervorfällen auf die eigene kritische Infrastruktur bestehen soll. Abzulehnen ist zudem Art. 74h bezüglich Strafbestimmungen die zur persönlichen Strafbarkeit der Verantwortlichen führen. In diesem Zusammenhang ist der Grundsatz des Selbstbelastungszwangsverbots bei Cyberangriffen und Cybervorfällen in Art. 73c Abs. 3 zu präzisieren.

asut begrüsst die vorgeschlagenen Anpassungen des ISG im Grundsatz, schlägt jedoch folgende Anpassungen vor:

NCSC als zentrale Meldestelle definieren
Um das Schadensausmass eines Cybervorfalls zu minimieren, müssen diese unter Umständen rasch gemeldet und ebenso rasch bearbeitet werden können. Die innerbetrieblichen Ressourcen werden in einer ersten Phase jedoch vor allem für die Krisenbewältigung, also für die Abwehr und Schadensbegrenzung eingesetzt. Der bürokratische Aufwand für die Erfüllung der verschiedenen Meldepflichten muss deshalb so gering und der Prozess so einfach wie möglich sein.

asut schlägt vor, beim Bund eine einzige und zentrale Meldestelle für sämtliche Cybervorfälle zu schaffen, deren Meldung gesetzlich vorgeschrieben ist. Mit dieser zentralen Meldestelle würde die Wirtschaft administrativ entlastet und die Prozesse vereinfacht werden. Prädestiniert für diese Aufgabe dürfte das NCSC sein. Statt es den Meldenden zu überlassen, einen Vorfall auch anderen Bundesstellen weiterzuleiten, könnte dies durch die zentrale Meldestelle geschehen. Wo nötig, könnte der Meldepflichtige mit der Meldung auch gleich sein Einverständnis für die Weitergabe der Meldung geben. Im erläuternden Bericht ist ein solcher Prozess angedacht.

asut
Schweizerischer Verband der Telekommunikation
Hirschengraben 8
3011 Bern

+41 (0)31 560 66 66
info@asut.ch
www.asut.ch

@asut_ch

Wir schlagen zudem ein einheitliches Vorgehen in allen Bundesbereichen vor. Im Revisionsentwurf zur «FDV – Sicherheit von Informationen und von Fernmeldeinfrastrukturen und -diensten» (Vernehmlassung bis 18. März 2022) war beispielsweise vorgesehen, dass Störungen in Telekomnetzen (wie z.B. Störungen der Netze, Cyberangriffe und andere böswillige Eingriffe) künftig nicht mehr an das BAKOM, sondern an die Nationale Alarmzentrale (NAZ) gemeldet werden müssen. asut hat sich in ihrer Stellungnahme zur Revision der FDV ebenfalls für das NCSC als zentrale Meldestelle für Störungen in Telekommunikationsnetzwerken ausgesprochen. Wichtig ist, dass die Revision der FDV und die Anpassung des ISG koordiniert erfolgen.

Meldepflicht präzisieren

«Internet Access Provider» (IAP) stellen anderen kritischen Infrastrukturen den Zugang zum Internet zur Verfügung. Die IAP sind stets bestrebt, bei Cybervorfällen ihre Kunden zu unterstützen. Ein IAP kann jedoch unmöglich zur Meldung sämtlicher Cyberangriffe verpflichtet werden, die über sein Netzwerk auf Betreiberinnen von kritischen Infrastrukturen erfolgen. Auch ist unter Umständen eine Meldung durch den IAP aufgrund von Vorgaben des Datenschutzgesetzes oder von vertraglichen Vereinbarungen gar nicht möglich. asut schlägt darum in Art. 74a ISG folgende präzisierende Ergänzung vor (zu ergänzender Text ist unterstrichen):

Art. 74a	Die Betreiberinnen von kritischen Infrastrukturen müssen dem NCSC Cyberangriffe auf ihre eigenen Infrastrukturen nach deren Entdeckung so rasch als möglich melden, damit das NCSC Angriffsmuster frühzeitig erkennen, mögliche Betroffene warnen und ihnen geeignete Präventions- und Abwehrmassnahmen empfehlen kann.

Strafbestimmungen zur persönlichen Strafbarkeit

Die Stossrichtung der Vernehmlassungsvorlage lässt auf ein partnerschaftliches Vorgehen zwischen Staat und Wirtschaft bei der Eindämmung von Cyber-Bedrohungen schliessen. Dieses kooperative Vorgehen widerläuft Art. 74h E-ISG und ist gänzlich abzulehnen. Solche Bestimmungen, die zur persönlichen Strafbarkeit der Verantwortlichen führen, sind für die Bekämpfung von Cyber-Bedrohungen vielmehr schädlich als förderlich, führen zu Fehlanreizen und können insbesondere die Bereitschaft der zuständigen Personen reduzieren, in Fragen der Cyber-Security Verantwortung zu übernehmen.

Art. 74h	ist gänzlich abzulehnen

In diesem Zusammenhang ist zudem der Grundsatz des Selbstbelastungszwangsverbots bei Cyberangriffen und Cybervorfällen eminent wichtig. asut schlägt eine Präzisierung von Art. 73c Abs. 3 vor.

Art. 73c Abs. 3	Informationen, die dem NCSC im Rahmen einer Meldung bekanntgegeben wurden und die meldende Person selbst belasten könnten, dürfen in einem Strafverfahren gegen diese Person nur mit Einverständnis dieser Person verwendet werden.

Wir danken ihnen bestens für die Berücksichtigung unserer Anliegen und stehen Ihnen für Rückfragen gerne zur Verfügung.

Freundliche Grüsse

Peter Grütter
Präsident