Swico
Lagerstrasse 33
CH-8004 Zürich

Tel.: +41 44 446 90 90
www.swico.ch
info@swico.ch

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS
Schwarztorstrasse 59
3003 Bern

Ausschliesslich per E-Mail an:
ncsc@ncsc.admin.ch

Zürich, 13.09.2024

Vernehmlassung zur Cybersicherheitsverordnung (CSV)

Sehr geehrte Frau Bundespräsidentin Amherd
Sehr geehrte Damen und Herren

Gerne nehmen wir die Möglichkeit wahr, innerhalb der festgesetzten Frist Stellung zur Vernehmlassung zur Cybersicherheitsverordnung (CSV) zu nehmen.

Swico ist der Wirtschaftsverband der Digitalindustrie und vertritt die Interessen etablierter Unternehmen sowie Start-ups in Politik, Wirtschaft und Gesellschaft. Swico zählt über 750 Mitglieder aus der ICT- und Internetbranche. Diese Unternehmen beschäftigen 56'000 Mitarbeitende und erwirtschaften jährlich einen Umsatz von 40 Milliarden Franken.

Zusammenfassung: Grundsätzlich begrüsst Swico, dass mit der vorliegenden Ausführungsverordnung zum Bundesgesetz über die Informationssicherheit (ISG) insgesamt zielführend die Cyber-Resilienz der Schweiz gestärkt wird, sofern einige notwendige Verbesserungen erzielt werden. Wir begrüssen, dass die Rolle des Bundesamts für Cybersicherheit (BACS) gestärkt und geschärft wird. Aus den Beratungs- und Unterstützungsleistungen des neuen Bundesamtes darf aber keine Konkurrenz zur Privatwirtschaft entstehen. Dies würde Swico entschieden ablehnen. Zudem muss der Geltungsbereich bezüglich Unterlieferanten geschärft werden, Meldepflichten verhältnismässig, subsidiär und risikobasiert definiert sein sowie bestehende multiple Meldeverfahren zwingend harmonisiert werden. Nur so und verbunden mit einer breiter gefassten Ausnahme für KMUs welche mit bestehenden Regelungen (Verordnung über den Datenschutz) abgestimmt ist, lässt sich ein optimales Kosten-Nutzen-Verhältnis bezüglich Meldepflichten erzielen – im Sinne von Staat, Gesellschaft und Wirtschaft. Weiter erachten wir den sicheren und aktiven Einbezug und Anhörung der Hersteller bzw. Anbieter im Kontext der Behebung von Schwachstellen als zentral, um rasch und gleichzeitig nachhaltige Lösungen zu erzielen. In diesem Zusammenhang ist es wichtig sicherzustellen, dass bezüglich der Weitergabe und Verwendung von Informationen klare Schranken gesetzt werden und insgesamt eine Orientierung an internationalen Standards stattfindet.

1 Allgemeine Würdigung

Swico begrüsst, dass mit der Änderung des Bundesgesetzes über die Informationssicherheit (ISG) und den nun mit Augenmass zu entwickelnden und implementierenden Ausführungsbestimmungen insgesamt die Cyber-Resilienz der Schweiz gestärkt werden kann. Mit dem vorliegenden Entwurf der Cybersicherheitsverordnung werden die Rolle des BACS, als die für zuständig definierte Behörde, geschärft und dessen Möglichkeiten gezielt ausgebaut. Mittels der vorgesehenen Meldepflicht gewinnt das BACS eine verbesserte Übersicht über Cyberangriffe in der Schweiz. Dies ist die Grundlage, um Betroffene bei der Bewältigung von Cyberangriffen zu unterstützen und Betreiberinnen kritischer Infrastrukturen zweckmässig zu warnen. Voraussetzung dafür ist jedoch, dass Behörden und Wirtschaft kooperativ zusammenwirken. Zum einen bei der Erarbeitung und Weiterentwicklung des strategischen Rahmens («Nationale Cyberstrategie»). Andererseits bei der operativen Zusammenarbeit im Bereich Meldungen. Es muss sichergestellt sein, dass die Meldepflicht insgesamt einen positiven Effekt schafft und keinen Mehraufwand mit sich bringt, sodass die Cyber-Resilienz der Schweiz nachhaltig gestärkt wird und zu Gunsten von Staat, Gesellschaft und Wirtschaft ein effektiver Mehrwert geschaffen wird. Kurz: Mehr Cybersicherheit begrüssen wir. Mehr Bürokratie lehnen wir entschieden ab.

2 Wichtige Einbettung in strategischen Gesamtrahmen

Wir begrüssen, dass mit der Nationalen Cyberstrategie gemäss Art. 2 CSV ein zentraler, strategischer Rahmen, der gemeinsam mit dem Steuerungsausschuss Nationale Cyberstrategie (StA NCS) laufend weiterentwickelt wird, für die Prävention, Früherkennung sowie Reaktion auf Cyberbedrohungen definiert ist. Dieses Set-Up fördert die Akzeptanz sowie das zielgerichtete, gesamthafte und koordinierte Handeln aller Akteure.

3 Klare Rollen, Geltungsbereich und gezielte Kooperation als Erfolgsfaktor

Wir erachten klare Rollen und entsprechende Zuordnung der Verantwortlichkeiten sowie insgesamt die gezielte Kooperation zwischen Behörden und Wirtschaft - gerade auch im Bereich der Meldepflichten – als einer der zentralen Erfolgsfaktoren, um die Cybersicherheit der Schweiz nachhaltig zu stärken. Wir begrüssen, dass der «Erläuternde Bericht» dies explizit anerkennt (S. 8 - 9). Mit Blick auf diesen Erfolgsfaktor heben wir folgende Punkte hervor:

3.1 Aktiver Einbezug der Schweizer ICT- und Internetbranche zwingend (StA NCS)

Wir beurteilen die gemischte Zusammensetzung des StA NCS, insbesondere auch mit Vertreterinnen und Vertretern der Wirtschaft, und das damit verbunden Verständnis der Kooperation zwischen Behörden und Wirtschaft, als zielführend (Art. 4 & 5 CSV). Die Ernennung der vorsitzenden Person aus den Reihen der Wirtschaft, Gesellschaft und Hochschulen, um eine ausgewogene Führung des Ausschusses zu gewährleisten, sehen

wir positiv (Art. 4 Abs. 3 CSV sowie S. 9 Erläuternder Bericht). Die bereits erfolgten Ernennungen nehmen wir zur Kenntnis.[1]

Es ist für uns evident, dass es eine umfassende Betrachtung der verschiedenen Aspekte der Cybersicherheit und unterschiedliche Perspektiven braucht, um eine effiziente Umsetzung der Nationalen Cyberstrategie und den bestmöglichen Schutz der Schweiz vor Cybervorfällen und -bedrohungen zu gewährleisten. Speziell die Schweizer ICT- und Internetbranche als Anbieter von digitalen (Sicherheits-) Dienstleistungen und Produkten und in Teilen selbst Betreiber von kritischen Infrastrukturen[2], ist Dreh- und Angelpunkt einer starken nationalen Cybersicherheit und muss im Rahmen des StA NCS aktiv einbezogen werden. Einerseits weil die Branche besonders betroffen ist, andererseits, weil sie mit ihrem Know-How einen aktiven Mehrwert leisten kann und will. Infolgedessen schlagen wir vor, Art. 4 Abs. 1 CSV wie folgt zu präzisieren:

Art. 4 Zusammensetzung des StA NCS [Anpassung in Rot] [1] Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, der Gesellschaft der Hochschulen zusammen mit angemessener Vertretung von Betreiberinnen kritischer Infrastrukturen.

3.2 BACS als zentrale, koordinierende Behörde etablieren

Wir begrüssen, dass mit der vorliegenden Cybersicherheitsverordnung die Rolle des BACS als zentrale, koordinierende Stellung hinsichtlich Cybersicherheit in der Schweiz gestärkt wird (siehe insbesondere Art. 6 – 15 CSV). Zentral dabei ist auch, dass eine enge Koordination zwischen BACS und dem Bundesamt für Kommunikation (BAKOM) stattfindet, wie in Art. 9 Abs 6 & 7 CSV festgehalten – insgesamt sind jedoch multiple Meldeverfahren zu harmonisieren (siehe 4.3).

Weiter erachten wir es als positiv, dass Art. 15a Abs. 2 lit. h OV-VBS neu aufführt, dass das BACS die Schweiz zur technischen Analyse von Cyberbedrohungen und zur Bewältigung von Cybervorfällen in internationalen Gremien vertritt. Dieser Informationsaustausch stärkt die zentrale Stellung des BACS in der Schweiz und ist insofern auch wichtig, als dass Cyberbedrohungen ein globales Phänomen sind, welches globale Lösungen fordert.

3.3 Geltungsbereich klären – Einbezug von Unterlieferanten ist vertraglich zu regeln

Bereits bei der Revision des ISG haben wir den unklaren Geltungsbereich als kritischer Punkt hervorgehoben.[3] Auch im aktuellen Verordnungsentwurf bleiben Unsicherheiten, bspw. hinsichtlich Betroffenheit von Unterlieferanten, wie etwa Cloud-Computing-Dienstleistern, Anbieterinnen von Sicherheitssoftware oder Suchmaschinen. Wir sind hier klar der Meinung, dass der Einbezug solcher Lieferanten nicht regulatorisch,

[1] BACS, «VBS setzt den Steuerungsausschuss der Nationalen Cyberstrategie ein» abgerufen am 14.08.2024 von https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/sta-ncs.html
[2] Siehe Art. 74b Abs 1 lit q ff. ISG.
[3] Swico, 2022, «Stellungnahme re Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Vernehmlassungsantwort)», S. 2. abgerufen am 13.08.2024 von https://www.swico.ch/media/filer_public/8d/af/8dafc8da-ae27-4827-8229-cd38e2528d70/220413_stellungnahme_swico.pdf

sondern vertraglich zwischen den Betreiberinnen kritischer Infrastrukturen und ihren Lieferanten zu regeln ist.

3.4 Keine Konkurrenzierung privatwirtschaftlicher Angebote

Im Sinne der konstruktiven Kooperation und bezugnehmend auf Art 74 Abs. 3 und Art. 74a Abs. 3 ISG sowie Art. 8 CSV begrüssen wir einerseits die Beratung und Unterstützung bei Cyberangriffen durch das BACS verbunden mit den vorgeschlagenen Priorisierungs-Kriterien. Gleichzeitig halten wir ausdrücklich fest, dass gerade mit Blick auf Angriffe mit geringer Beratungs-Priorität keine staatliche Konkurrenz zu (Beratungs-) Angeboten von Privaten erwachsen darf, zumal hier im Sinne von Art. 74 Abs. 3 die Beschaffung gleichwertiger Unterstützung auf dem Markt rechtzeitig möglich ist.

4 Meldepflichten müssen insgesamt Mehrwert schaffen und umsetzbar sein

Wie im Rahmen unserer allgemeinen Würdigung (siehe 1.) betont, muss das Ziel dieser Vorlage sein, einen effektiven Mehrwert für die Gesellschaft, den Staat und die Wirtschaft zu schaffen, indem die Sicherheit erhöht wird und dabei die aus Cyberangriffen resultierende Schäden und Kosten reduziert werden. Konkret müssen die vorgesehenen Meldepflichten den betroffenen Unternehmen und der Volkswirtschaft letztlich mehr Nutzen stiften als Kosten generieren. Die Meldepflichten müssen daher verhältnismässig, subsidiär und risikobasiert definiert sein. Des Weiteren sollen sie internationalen Standards entsprechen, sodass ein optimales Kosten-Nutzen-Verhältnis erzielt wird. Administrative und finanzielle Aufwände sind auf ein Minimum zu reduzieren.

4.1 Notwendige Präzisierungen und Eingrenzung bezüglich Fristen und Meldepflichten

Hinsichtlich der Meldepflichten gilt es aus unserer Sicht erstens, Rücksicht auf die Schwere eines Cyberangriffs beziehungsweise dessen Auswirkungen zu nehmen. Die vorgeschlagene Formulierung in Art. 18 Abs. 1 lit. a legt nahe, dass jegliche potenzielle Kompromittierung eines Systems dem BACS zu melden ist. Der erläuternde Bericht schafft hierbei keine Klarheit: «[d]ie Funktionsfähigkeit einer kritischen Infrastruktur kann durch einen Cyberangriff gefährdet sein, wenn die IT-Systeme, Netzwerke oder Steuerungssysteme, die für den Betrieb der Infrastruktur wesentlich sind, derart kompromittiert werden, dass es zu Systemunterbrüchen für Mitarbeitende und Dritte führt» (S. 27). Damit ist nicht abschliessend geklärt, was mit «für den Betrieb wesentlich» gemeint ist. Begrüssenswert ist dementsprechend eine Präzisierung, die klarstellt, dass es sich um Ereignisse handeln muss, die den Betrieb der Infrastruktur unmittelbar gefährden. Gleiches gilt für Art. 18 Abs. 2 lit. a, worin von «geschäftsrelevanten Informationen» die Rede ist. Es erscheint uns auch hier sinnvoll, zu präzisieren, dass es sich um kritische Informationen handeln muss, die tatsächlich in Zusammenhang mit dem unmittelbaren Betrieb der kritischen Infrastruktur stehen.

Darüber hinaus ist zweitens festzuhalten, dass «nur» Cyberangriffe der Meldepflicht unterliegen – also Cybervorfälle - die absichtlich ausgelöst wurden (Art. 5 lit. e ISG). Die vorgeschlagene Formulierung spricht jedoch lediglich von «Systemunterbrüchen», was

zu Verwirrung führen kann (Art. 18 Abs. 1 lit. a). Deshalb erachten wir es als sinnvoll, eine Präzisierung vorzunehmen.

Beide Änderungsvorschläge tragen zudem dazu bei, exzessive administrative Aufwände, sowohl für die Betreiberinnen der kritischen Infrastrukturen als auch das BACS, zu vermeiden und relevante Cyberangriffe mit entsprechendem Mehrwert hinsichtlich Effizienz und Reaktionsmöglichkeiten zu priorisieren.

Art. 18 Zu meldende Cyberangriffe [Anpassung in Rot]

[1]Die Funktionsfähigkeit einer kritischen Infrastruktur gilt als gefährdet, wenn:

a. Mitarbeitende oder Dritte, welche den unmittelbaren Betrieb der kritischen Infrastruktur verantworten, von absichtlich ausgelösten Systemunterbrüchen betroffen sind und dadurch der stabile Betrieb der Infrastruktur unmittelbar gefährdet ist; oder

b. die betroffene Organisation oder Behörde ihre Tätigkeiten nur noch mit Hilfe von Notfallplänen aufrechterhalten kann.

[2]Eine Manipulation oder Abfluss von Informationen liegt vor, wenn:

a. geschäftsrelevante Informationen, welche mit dem unmittelbaren Betrieb der kritischen Infrastrukturen in Zusammenhang stehen, von Unbefugten verändert oder offengelegt werden; oder

b. eine Verletzung der Datensicherheit nach Artikel 24 des Datenschutzgesetzes vom 25. September 2020 vorliegt.

4.2 Wichtige Ausnahme für KMU

Vor allem für KMU und Start-ups kann die Meldepflicht schnell zu erheblichen administrativen Aufwänden führen. Daher erachten wir es als sinnvoll, dass meldepflichtige Organisationen nach Art. 74b ISG von der Meldepflicht ausgenommen werden, wenn sie eine bestimmte Grösse nicht überschreiten. Die vorgeschlagene Regelung, wonach Organisationen ausgenommen sind, wenn sie weniger als 50 Personen im betroffenen Bereich beschäftigen und ihr Jahresumsatz bzw. ihre Jahresbilanz im betroffenen Bereich CHF 10 Mio. nicht übersteigt (Art. 16 Abs. 2 CSV), erscheint uns jedoch umständlich und wirft Auslegungsfragen auf, insbesondere hinsichtlich der Formulierung «im betroffenen Bereich». Zudem ist anzumerken, dass diese Definition ganz grundsätzlich nicht kohärent mit anderen Schweizer Bestimmungen ist.[4]

Deshalb fordern wir, der Einfachheit und Kohärenz halber, dass Unternehmen und andere privatrechtliche Organisationen von der Meldepflicht ausgenommen werden, die am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, analog zur Verordnung über den Datenschutz (DSV). Dies entspricht im Übrigen auch der gängigen Definition von KMU.[5]

[4] Siehe bspw. Datenschutzverordnung (DSV) Art. 24 «Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten»

[5] Siehe Bundesamt für Statistik (BFS) «Kleine und mittlere Unternehmen»., abgerufen am 26.08.2024 von https://www.bfs.admin.ch/bfs/de/home/statistiken/industrie-dienstleistungen/unternehmen-beschaeftigte/wirtschaftsstruktur-unternehmen/kmu.html

Art. 16 Zu meldende Cyberangriffe [Anpassung in Rot]
[2] Unternehmen nach Artikel 74b Absatz 1 Buchstaben f, g, h, l und p ISG, für die Absatz 1 nicht anwendbar ist, sind von der Meldepflicht ausgenommen, sofern sie ~~im betroffenen Bereich weniger als 50 Personen beschäftigen und ihr Jahresumsatz beziehungsweise ihre Jahresbilanzsumme im betroffenen Bereich 10 Millionen Franken nicht übersteigt~~ jeweils am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen.

4.3 Gezielte Harmonisierung multipler Meldeverfahren

Bereits in unserer Stellungnahme zur «Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe»[6] haben wir darauf hingewiesen, dass auf nationaler Ebene zahlreiche Meldepflichten im Bereich Cybersicherheit und anderen Bereichen existieren. So müssen beispielsweise Fernmeldedienstanbieterinnen entsprechende Meldungen unter Umständen mit jeweils unterschiedlichen Inhalten und Fristen sowohl der Nationalen Alarmzentrale (Art. 96 FDV), dem EDÖB (Art. 15 DSV) wie auch dem BACS (Art. 74a nISG) melden. Im Kontext der öffentlichen Beschaffung müssen Leistungserbringerinnen basierend auf den Mustervertragsklausel der BKB betreffend Cyberangriffen» (Ziff. 3) Meldungen einerseits an «den Leistungsbezüger und andererseits an das BACS (ex NCSC) Meldung erstatten.

Im Hinblick auf die breite Betroffenheit Schweizer Unternehmen vom EU Digital Operational Resilience Act kommen nebst der nationalen auch auf internationaler Ebene zusätzliche Anforderungen. Es ist deshalb auf Lösungen für eine Harmonisierung / Koordination der einzelnen Meldeverfahren hinzuwirken. Denkbar ist bspw. die Fristen jenen der NIS-2-Richtlinie anzupassen (24 Stunden für eine Frühwarnung, 72 Stunden für die Meldung eines Vorfalls). Die Meldequalität sollte gegenüber der Meldegeschwindigkeit im Vordergrund stehen.

Diese multiplen Meldeverfahren sind aufwändig, ineffizient und bergen die Gefahr von Fehlern. Aus unserer Sicht ist darum dringen auf Lösungen für eine Harmonisierung und Koordination der verschiedenen Meldeverfahren hinzuwirken.

5 Sicherer Umgang mit und Behebung von Schwachstellen

Bezüglich dem sicheren Umgang mit und der nachhaltigen Behebung von Schwachstellen heben wir folgende Aspekte hervor:

5.1 Umgang gemäss international anerkannten Standards wichtig und richtig

Wir begrüssen, dass der Umgang mit identifizierten Schwachstellen in enger Abstimmung mit den Herstellern und ausdrücklich nach internationalen Standards (ISO/IEC Norm 29147:2018-10) erfolgen soll (Art. 9 Abs 1 CSV & Erläuternder Bericht, S. 14). Dies garantiert einen sicheren und gleichzeitig effizienten Umgang mit

[6] Swico, 2022, «Stellungnahme re Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe (Vernehmlassungsantwort)», S. 2. abgerufen am 13.08.2024 von https://www.swico.ch/media/filer_public/8d/af/8dafc8da-ae27-4827-8229-cd38e2528d70/220413_stellungnahme_swico.pdf

Schwachstellen, da die entsprechenden Prozesse den Akteuren bekannt und im Sinne von Best Practices erprobt sind.

5.2 Hersteller sind zwingend und jederzeit zu informieren

Eine zentrale Voraussetzung dafür, eine Schwachstelle sicher zu managen, ist es, jederzeit zwingend sicherzustellen, dass das BACS, wie vorgeschlagen, «keine Schwachstellen geheim behält oder anderen Behörden weiterleitet, ohne die Hersteller zu informieren». (Art. 9 Abs. 1 CSV & S. 14 Erläuternder Bericht). Nur wenn der Hersteller voll im Bilde ist, auch bezüglich Informationsträger betreffend Schwachstellen, kann eine sichere, nachhaltige und fristgerechte Behebung derselben umgesetzt werden.

5.3 Flexible Fristen unter Einbezug der Hersteller definieren

Wir können nachvollziehen, dass das BACS zwecks Behebung von Schwachstellen eine Frist setzt. Gleichzeitig halten wir fest, dass gerade auch die Hersteller daran interessiert und gewillt sind, Schwachstellen möglichst zeitnah und nachhaltig zu beheben, wobei der Komplexitäts-Grad einer entsprechenden Behebung ein einschränkender Faktor darstellt – entsprechende Realitäten sind zu berücksichtigen. Vor diesem Hintergrund schlagen wir vor, dass jeweils eine «angemessene» Frist (anstatt einer starren Frist) gesetzt wird und begrüssen, dass diese angemessene Frist gemäss Art. 9 Abs. 4 CSV verlängert werden kann. Wir nehmen gleichzeitig zur Kenntnis, dass gemäss Art. 9 Abs 3 CSV eine Frist Risiko-bedingt verkürzt werden kann. Eine allfällige Frist-Verkürzung soll jedoch nur nach Anhörung des betroffenen Herstellers stattfinden können, zumal genau dieser die oben beschriebenen Realitäten und limitierende Faktoren am besten kennt. Nur auf Basis effektiv machbarer, realitäts-bezogener Fristen und in enger Abstimmung zwischen Hersteller und BACS kann eine nachhaltige Schwachstellen-Behebung erzielt werden.

5.4 Vorabinformation an kritische Infrastrukturen umsichtig handhaben

Gemäss Art. 9 Abs. 5 CSV und dem Erläuternden Bericht (S. 15), kann das BACS, wenn ihm eine Schwachstelle bekannt ist, die für andere kritische Infrastrukturen eine «akute Cyberbedrohung» darstellen, die Betreiberinnen entsprechender Infrastrukturen informieren, bevor die Schwachstelle veröffentlicht oder durch die Herstellerin der Hard- oder Software behoben wurde. Entsprechende Vorabinformationen erachten wir als sinnvoll und zielführend verbunden damit, dass die oben genannten Aspekte (siehe 5.1 bis 5.3) berücksichtig werden und es sich, wie vorgeschlagen, effektiv um eine akute Bedrohung handelt.

Aufgrund unserer Ausführungen in Kapitel 5 regen wir folgende Anpassungen an:

Art. 9 Koordinierte Offenlegung [Anpassung in Rot]

[2] Es setzt der Herstellerin der betroffenen Hard- oder Software eine angemessene Frist ~~von 90 Tagen~~ zur Behebung der Schwachstellen.

[4] Es [das BACS] kann die Frist nach Anhörung der Herstellerin verkürzen, wenn eine Schwachstelle:

a. die Funktionsfähigkeit von kritischen Infrastrukturen gefährdet;
b. besonders leicht für einen Cyberangriff ausgenutzt werden kann; oder
c. weit verbreitete Systeme betrifft.

6 Effizienter und sicherer Informationsaustausch gewährleisten

Wir begrüssen, dass der vorliegende Verordnungsentwurf die Anforderungen, Prozesse und Verantwortlichkeiten im Zusammenhang mit dem vorgesehenen Informationsaustausch regelt, wobei wir folgende Punkte explizit hervorheben:

6.1 Sicherheit der Kommunikationssysteme von grösster Bedeutung

Dass das BACS gemäss Art. 11 und 12 CSV ein zentrales Kommunikationssystem für den sicheren Informationsaustausch zu Cybervorfällen und -bedrohungen betreibt und registrierte Organisationen dadurch schnell und effizient mit Informationen über Vorfälle und Bedrohungen informiert, erachten wir als sinnvoll. Gleichzeitig weisen darauf hin, dass es sich bei genau solchen Informationssystemen für Cyberkriminelle um «lohnende Ziele» handeln kann. Ein hohes Mass an Sicherheit ist deshalb zwingend. Die Verantwortung dafür muss, wie vorgeschlagen, in erster Linie beim BACS liegen (Art. 11 Abs. 2 CSV & Art. 12 Abs. 2 CSV).

6.2 Sinnvolle Abgrenzung und Freiwilligkeit für Dienstleister

Wir begrüssen, dass Dienstleister von Betreiberinnen kritischer Infrastrukturen Zugang zu den genannten Informationssystemen (siehe oben) erhalten können – dies auf freiwilliger Basis. Die entsprechende, vorgesehene Meldung durch die Betreiberinnen und anschliessende Anmeldung durch die Dienstleister selbst erachten wir als sinnvoll (Art 14 CSV).

6.3 Notwendige Präzisierung bezüglich Kontaktperson(en)

Hinsichtlich der Registrierung für die Teilnahme am Informationsaustausch durch interessierte Organisationen sehen wir Präzisierungsbedarf. Gemäss Art. 13 Abs. 2 lit. b CSV muss eine Registrierung die «Kontaktangaben der gemeldeten Person» enthalten. Im Erläuternden Bericht wird ausgeführt, dass es sich hierbei um eine «Kontaktperson» handelt (S. 19). Die Formulierung im Verordnungsentwurf impliziert eine Verantwortlichkeit der gemeldeten Person, was dem Bericht widerspricht. Gleiches gilt darüber hinaus für Art. 14 Abs. 2 CSV, wo auch von «der gemeldeten Person» die Rede ist. Um Klarheit zu schaffen, schlagen wir deshalb vor, Art. 13 Abs. 2 lit. b CSV sowie Art. 14 Abs. 2 CSV wie folgt zu präzisieren:

Art. 13 **Registrierung** [Anpassung in Rot]

[2] Die Registrierung muss mindestens folgende Informationen enthalten:

a. Firma, Name oder Bezeichnung und Adresse;

b. ~~Kontaktangaben der gemeldeten Person~~ Angaben zu einer oder mehreren Kontaktpersonen.

Art. 14 **Dienstleister** [Anpassung in Rot]

[2] Die Dienstleister müssen sich mit der Firma oder dem Namen sowie ~~Kontaktangaben der gemeldeten Person~~ Angaben zu einer oder mehreren Kontaktpersonen registrieren.

6.4 Klare Schranken bezüglich Weitergabe und Verwendung von Informationen

Mit Blick auf die (potenzielle) Sensitivität der übermittelten Informationen und notwendigen Vertrauensbeziehung betreffend (freiwillig) erfolgender Meldungen von Cybervorfällen und -bedrohungen, ist es entscheidend, dass die übermittelnde Organisation oder Behörde gemäss Art. 15 Abs. 1 CSV bestimmt, ob und an wen diese gemeldeten Informationen weitergegeben werden dürfen. Die Abstützung auf internationale Standards (TLP-Protokoll) gemäss Erläuterndem Bericht (S. 20 – 21) erachten wir als zweckmässig. In diesem Zusammenhang begrüssen wir auch die Pflicht zum Schutz der Informationen durch die Informationsempfänger als auch deren ausschliessliche Verwendung zwecks Schutz kritischer Infrastrukturen (Art 15. Abs 3 und 4), um unlautere bzw. ungerechtfertigte Wettbewerbsvorteile zu verhindern.

Wir bedanken uns für die Berücksichtigung unserer Anliegen und stehen für Rückfragen gerne zu Verfügung.

Freundliche Grüsse
Swico

Jon Fanzun
CEO

Simon Ruesch
Head Legal & Public Affairs
Mitglied der Geschäftsleitung