Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

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

13. April 2022

Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe: Stellungnahme economiesuisse

Sehr geehrter Herr Bundesrat Maurer
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar haben Sie uns eingeladen, zur Einführung einer Meldepflicht für Betreiberinnen kritischer Infrastrukturen für Cyber-Angriffe Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit.

Als Dachverband der Schweizer Wirtschaft bündelt economiesuisse die Interessen von rund 100'000 Unternehmen mit etwa 2 Mio. Beschäftigten im Inland und weiteren 2 Mio. Beschäftigten im Ausland. Unser Mitgliederkreis umfasst 100 Branchenverbände, 20 Handelskammern und diverse Einzelfirmen. Alle diese Mitglieder sind an einem effizienten Schutz vor Cyber-Risiken interessiert.

economiesuisse teilt die Einschätzung, dass aufgrund der rasant steigenden Zahl der Cyber-Angriffe auf Schweizer Unternehmen und Institutionen in passende Schutzmassnahmen investiert werden muss. Dies gilt im Speziellen für sog. kritische Infrastrukturen, welche aus systemischer Sicht eine erhöhte Resilienz aufweisen müssen, damit sie ihre wichtige Funktion für Wirtschaft und Gesellschaft auch angesichts eines Cybervorfalls oder -angriffs erfüllen können. Folglich bestehen gegen eine Meldepflicht für die Betreiberinnen kritischer Infrastrukturen grundsätzlich keine Einwände. Dennoch muss diese aus Sicht der Wirtschaft gewisse entscheidende Anforderungen erfüllen:

1. Es braucht frühzeitige und umfassende Klarheit darüber, «wer» «wem» «was» unter welchen Bedingungen melden muss. Besonders über das «wer» und «was» gibt die Vernehmlassungsvorlage aus Sicht der Wirtschaft nicht ausreichend Aufschluss. Die im Gesetzesentwurf erwähnten Branchen und Bereiche lassen auf einen sehr umfassenden Geltungsbereich schliessen. Eine Meldepflicht, die weite Teile der Wirtschaft betrifft und bei der viele Akteure gerade zum aktuellen Zeitpunkt der Vernehmlassung noch nicht einmal wissen, ob sie nicht auch betroffen sind, ist nicht zielführend.

2. Die Meldepflicht muss den betroffenen Unternehmen und der Volkswirtschaft letztlich mehr bringen, als sie kostet. Sie muss einen verhältnismässigen, subsidiären, risikobasierten Ansatz verfolgen, der administrative und finanzielle Aufwände auf ein Minimum reduziert. Grundsätzlich sollte

economiesuisse
Hegibachstrasse 47
Postfach
CH-8032 Zürich
Telefon +41 44 421 35 35

Verband der Schweizer Unternehmen
Fédération des entreprises suisses
Federazione delle imprese svizzere
Swiss Business Federation
www.economiesuisse.ch

sie einer «Servicementalität» entspringen und nicht einseitig als Kontrollinstrument aufgesetzt werden. Die Interessen der Behörden und der Unternehmen sind umfassend identisch. Beide wollen einen bestmöglichen Schutz vor Cyber-Angriffen. Dies darf nur ein absolutes Minimum an Zwang mit sich bringen. Betroffene Unternehmen müssen aus der Meldepflicht schliesslich einen Mehrwert erhalten, der zu einer konstruktiven Zusammenarbeit animiert und eine an sich schon unerwünschte Situation nicht noch unnötig verkompliziert.

3. economiesuisse erkennt keinen Sinn darin, die neuen Pflichten mit Strafbestimmungen durchzusetzen und lehnt diese prinzipiell ab. Gerade im vorliegenden Fall wird klar, dass diese zu Fehlanreizen führen und insbesondere die Bereitschaft der zuständigen Personen reduzieren, in Fragen der Cyber-Security Verantwortung zu übernehmen. Die im Cyber-Bereich so wichtige Fehlerkultur und der kooperative Geist der Vernehmlassungsvorlage werden durch unnötige und schädliche Sanktionen beeinträchtigt.

Aus Sicht der Wirtschaft würden solche Präzisierungen und Änderungen der Vorlage für Betreiberinnen kritischer Infrastrukturen die Rechtssicherheit stärken und wohl auch Berührungsängste mit der Meldepflicht abbauen. Sollte die Vorlage in diesen Punkten nicht nachgebessert werden, behält sich economiesuisse vor, eine ablehnende Haltung einzunehmen.

Weitere Ausführungen zu dieser Position finden Sie nachfolgend:

1 Abschliessende und klare Bezeichnung der von der Regulierung adressierten Unternehmen

Generell stellen Meldepflichten an Behörden für Unternehmen eine zusätzliche administrative Belastung dar. Diese geht auf Kosten von Investitionen und Produktivitätssteigerungen. Klare Aussagen darüber, welche Unternehmen in welchen Bereichen konkret betroffen sind, sind deshalb im vorliegenden Fall besonders wichtig. Der Gesetzesentwurf und die begleitenden Unterlagen müssen eindeutig erkennbar machen, welche Firmen wann von der Meldepflicht betroffen sind. Im Kontext der kritischen Infrastrukturen ist dies nachvollziehbarerweise schwierig, da solche Definitionen sicherheitsrelevant sind. Dennoch sind genauere Anhaltspunkte nötig. Die Liste der Bereiche, welche einer Meldepflicht unterstehen (Art. 74b E-ISG), ist zu breit gefasst. Eine Meldepflicht ist auf diejenigen Bereiche zu beschränken, deren Ausfall oder Beeinträchtigung zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen würden. Der aktuelle Entwurf lässt auf eine breite und tiefe wirtschaftliche Betroffenheit der geplanten Meldepflicht schliessen, wobei sich «breit» auf die Anzahl Branchen und Unternehmen bezieht und «tief» auf die vor- und nachgelagerten Lieferketten der betroffenen Unternehmen. Insbesondere ist nicht nachvollziehbar, warum Hersteller (Art. 74b, Ziff. s E-ISG) eingebunden werden. Nicht nur nimmt dadurch die Unklarheit bezüglich Betroffenheit zu, die Hersteller passen zudem nicht in die Systematik der Betreiberinnen von kritischen Infrastrukturen, welcher das E-ISG zugrunde liegt. Sollte sich unsere Einschätzung einer derart ausgedehnten Betroffenheit in weiten Teilen der Wirtschaft bewahrheiten, ist zwingend eine Regulierungsfolgeabschätzung notwendig. Sodann wäre beispielsweise ein mehrstufiger Regulierungsansatz zu prüfen, der zuerst eine Meldepflicht für Infrastrukturen mit höchster Kritikalität vorsieht, bevor man die gesamte Wirtschaft mit neuen und vielleicht unverhältnismässigen Auflagen beschwert.

2 Abschliessende und klare Bezeichnung der zu meldenden Sachverhalte

Die vorgeschlagene Definition ist zu generisch und zu breit (Art. 5 E-ISG). Es gibt keine klare Differenzierung zwischen Vorfällen, welche keinen oder nur einen unwesentlichen Einfluss auf die Geschäftsprozesse haben und solchen, die den Betrieb kritischer Infrastrukturen grundsätzlich gefährden oder ein hohes Risiko bergen. Nach momentanem Wortlaut des Entwurfes müssten ausserdem sowohl erfolgreiche als auch nicht erfolgreiche Cyber-Angriffe dem NCSC gemeldet werden. Aufgrund der vorhandenen Informationen müssen wir davon ausgehen, dass bereits lediglich Anzeichen auf einen Angriff zur Meldepflicht führen könnten, was aus unserer Sicht über das Ziel hinausschiesst. Ausnahmen von der Meldepflicht sind nur für bestimmte Kategorien von Betreiberinnen nach Art. 74c E-ISG, nicht aber für bestimmte Arten von Angriffen geplant. Art. 74d E-ISG, welcher die zu meldenden Cyberangriffe definiert, ist deshalb zwingend zu überarbeiten. Die Kriterien sind zu weit gefasst und für die Unternehmen so kaum greif- oder umsetzbar. Zielführender wäre es eine eingeschränktere (Positiv-)Liste der zu meldenden Vorfälle zur Verfügung zu stellen und die Meldepflicht generell nur auf erfolgreiche oder besonders schwerwiegende Versuche zu begrenzen. Dass, z.B. Cyberangriffe, welche länger als 30 Tage unentdeckt blieben, gemeldet werden müssen (vor allem in Kombination mit der ebenfalls abzulehnenden Strafbarkeit) ist nicht sinnvoll und scheint auch für die Zielsetzung der Einführung einer Meldepflicht nicht relevant. Ebenso schwierig ist das Kriterium der Involvierung eines fremden Staates. Je nachdem kann ein Unternehmen dies zum Zeitpunkt der Entdeckung gar nicht wissen. Das Ziel einer Meldepflicht soll es sein, dass ein Unternehmen in bestimmten und klar definierten Fällen mit den Behörden in den Dialog tritt. In diesem Dialog können dann weitere Fragen geklärt werden, wie zum Beispiel auch der Absender. Die Anforderungen an die Meldung an sich müssen jedoch einfach gehalten werden, um die Hürden für die Unternehmen tief zu halten. Letztlich müssen auch die Grenzen der zu meldenden Sachverhalte klar abgesteckt sein, bspw. wenn sie das Anwaltsgeheimnis oder Fabrikations- und Geschäftsgeheimnisse eines Unternehmens tangieren.

3 Keinen Mehraufwand durch Überschneidungen mit anderen Meldepflichten schaffen

Als problematisch beurteilen wir darüber hinaus Überschneidungen mit anderen, sektoriellen Meldepflichten im Bereich Cyber-Sicherheit oder weiteren Bereichen. Diesbezüglich stellt der erläuternde Bericht zur Vernehmlassungsvorlage klar, dass a priori keine Synergien mit der neuen Meldepflicht genutzt werden können. economiesuisse ist derweil der Ansicht, dass einem zusätzlichen Aufwand für die Unternehmen entgegenzuwirken ist. Ein diesbezüglich prüfenswerter Ansatz könnte ein One-Stop-Shop sein. Aus Sicht der Wirtschaft ist der Bund hier in der Pflicht, eine optimale Koordination sicherzustellen. Dies gilt sowohl für die Meldepflicht seitens des Unternehmens als auch für eine allfällige Reaktion seitens der Behörden. Dabei sollte aber beachtet werden, dass, im Sinne der Datensparsamkeit, die unterschiedlichen Behörden nur die für sie relevanten Informationen erhalten, unabhängig von der Ausgestaltung der Datenablieferung.

4 Massnahmen müssen ein positives Kosten-Nutzen-Verhältnis aufweisen

Gemäss Vernehmlassungsunterlagen sollen die Betreiberinnen kritischer Infrastrukturen als Mehrwert aus der Meldepflicht technische Einschätzungen und Unterstützung bei schwerwiegenden Cyber-Vorfällen erhalten. Darüber hinaus erlaubt die Meldepflicht eine verlässlichere Einschätzung der Bedrohungslage und ein «Frühwarnsystem» aufgrund besserer Kenntnisse über Angriffsmethoden und -muster. Dies ist voll und ganz im Sinne der Wirtschaft. Eine Meldepflicht muss generell einem Service-Gedanken folgen und darf nicht als Kontrollinstrument gegenüber den betroffenen Firmen eingesetzt werden. Nur so kann das Vertrauen der Unternehmen in den Nutzen der Institution gestärkt werden. Damit die Meldepflicht akzeptiert wird, muss bereits jetzt plastisch dargelegt werden, wie diese Unterstützungsleistungen ganz konkret den betroffenen Unternehmen zugutekommen sollen. Ebenso muss klar dargelegt werden, wie weit die neuen Pflichten in einem sinnvollen Verhältnis zum Ertrag stehen, dies insbesondere bei KMU und kleineren Betreiberinnen kritischer Infrastrukturen, bei denen der Zusatzaufwand stärker ins Gewicht fällt. Eine Meldepflicht «als Selbstzweck» einzuführen, um

Handlungsbereitschaft in einem die Unternehmen stark belastenden Bereich zu markieren, ist nicht akzeptabel. Es braucht einen klaren Gegenwert, der sich aktuell aus der Vorlage noch zu wenig erschliesst.

5 Fehlanreize vermeiden

Insgesamt lässt die Stossrichtung der Vernehmlassungsvorlage auf eine partnerschaftliche Grundhaltung hinter den vorgeschlagenen Massnahmen schliessen. Dies ist für die Wirtschaft entscheidend und muss entsprechen konsequenter herausgearbeitet werden. Nur gemeinsam und im Sinne einer Partnerschaft zwischen der Wirtschaft und dem Staat lassen sich Cyber-Bedrohungen eindämmen. Ein wesentlicher Punkt im Vorentwurf sind daher die Strafbestimmungen in Art. 74h und 74i E-ISG. Diese lehnen wir gänzlich ab. Solche Bestimmungen, die zur persönlichen Strafbarkeit der Verantwortlichen führen, sind für die Compliance von Unternehmen eher schädlich als förderlich. Personen, die in einem inhärent fehleranfälligen Bereich wie der Cyber-Sicherheit mit Sanktionen rechnen müssen, obwohl sie alle zumutbaren Vorkehrungen getroffen haben, werden klar weniger zur Übernahme dieser Verantwortung bereit sein. Dadurch wird ein Stellenmarkt, der bereits heute ausgetrocknet ist und nicht ausreichend Experten und Fachkräfte anbietet, noch weiter unter Druck gesetzt. Durch den unnötigen Fokus auf Strafbestimmungen in einem Themenfeld, bei dem gleichgerichtete Interessen bestehen und es keinerlei Sanktionsgründe gibt, wird darüber hinaus noch die Gefahr geschaffen, dass knappe Ressourcen in die Absicherung gegen die Sanktionsrisiken anstelle der Cyber-Risken fliessen.

Wir danken Ihnen vielmals für die Berücksichtigung unserer Argumente. Ergänzend unterstützten wir die Stellungnahmen unserer Mitglieder (unter anderem von scienceindustries, SwissBanking, Schweizerischer Versicherungsverband und Swissmem) und stehen für eine Zusammenarbeit im Sinne eines Austausches zum Gesetzesentwurf sowie für Fragen gerne zur Verfügung.

Freundliche Grüsse
economiesuisse

Erich Herzog
Leiter Wettbewerb & Regulatorisches
Mitglied der Geschäftsleitung

Lukas Federer
Projektleiter Infrastruktur, Energie & Umwelt