SUISSEDIGITAL

per E-Mail an ncsc@gs-efd.admin.ch

Generalsekretariat EFD
Eidgenössisches Finanzdepartement
Manuel Suter, NCSC / Angelika Spiess, GS-EFD
Bundesgasse 3
CH-3003 Bern

Bern, 07. April 2022

Stellungnahme zur Einführung einer Meldepflicht bei Cyberangriffen

Sehr geehrter Herr Bundesrat
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 haben Sie interessierte Kreise eingeladen, bis zum 14. April 2022 zu den geplanten Änderungen des Informationssicherheitsgesetz (nachfolgend „E-ISG") betreffend die Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen bei Cyberangriffen, Stellung zu nehmen. Wir danken Ihnen für diese Möglichkeit der Meinungsäusserung, die für unsere Mitglieder und uns sehr wichtig ist, weil für Anbieterinnen von Fernmeldediensten (FDA) neu eine strafbewehrte Melde*pflicht* an das Nationale Zentrum für Cybersicherheit (NCSC) bei Cyberangriffen auf eine kritische Infrastruktur eingeführt werden soll und damit zusätzliche administrative Aufwände verursacht werden sollen. Die vorliegende Stellungnahme erfolgt innert Frist und äussert sich zu Themen, die unsere Mitglieder in ihrer Geschäftstätigkeit direkt betreffen.

SUISSEDIGITAL ist der Dachverband der Schweizer Telekommunikationsnetzunternehmen und vertritt die Interessen von ca. 180 privatrechtlich oder öffentlich-rechtlich organisierten Unternehmen verschiedener Grösse, die lokal, regional oder landesweit Telekommunikationsinfrastrukturen (Fest- und Mobilfunknetze) betreiben und darüber verschiedene Fernmelde- inklusive Radio- und Fernsehdienste erbringen. Die Bereitstellung dieser Fernmeldedienste erfolgt in arbeitsteiligen Prozessen, wobei je nach Grösse der Unternehmen in unterschiedlichem Ausmass und unterschiedlicher Organisation auf Vorleistungsprodukte von dritten Technologielieferanten zurückgegriffen wird. Unterschiedlich ausgestaltet sind deshalb auch die Diagnose- und Zugriffsmöglichkeiten der Mitglieder auf die einzelnen operativen Netzkomponenten.

1. Einleitung

Das Thema der Sicherheit von Informationen und Fernmeldeinfrastrukturen bildet bei SUISSEDIGITAL ein zentrales strategisches Verbandsthema. Wir beschäftigen uns schon seit längerem intensiv damit und begrüssen Massnahmen, welche bei Telekommunikationsinfrastrukturen zusätzliche Resilienz und Robustheit schafft. Dazu gehört auch der Informationsaustausch zu Methoden und Mustern von aktuellen Cyberattacken, welche die Errichtung eines Abwehrdispositivs und eines Frühwarnsystems ermöglichen. Wir gehen davon aus, dass

einige Mitglieder bereits auf freiwilliger Basis Informationen mit der Melde- und Analysestelle Informationssicherung Melani und nun mit dem NCSC austauschen. Die Mitglieder sind an einer guten Kooperation mit dem NCSC interessiert und anerkennen den Wert eines funktionierenden Zentrums für Cybersicherheit zur Eindämmung von Cyberbedrohungen für sie selbst, aber auch für die gesamte Wirtschaft und die Zivilgesellschaft in der Schweiz. Die Interessen der Schweizer Behörden und Unternehmen sind im Bereich der Abwehr von Cyberangriffen identisch. Wir begrüssen deshalb die gesetzliche Erfassung des NCSC im E-ISG und dessen Betrauung mit Aufgaben zum Schutze der Schweiz vor Cyberrisiken. Auch begrüssen wir die nun im Gesetzesentwurf ausdrücklich vorgesehene Möglichkeit der technischen Unterstützung und Erstanalyse im konkreten Einzelfall durch das NCSC als erste Hilfe bei der Bewältigung eines Angriffs aus dem Cyberraum. Gerade für kleinere Unternehmen kann dies sehr hilfreich sein und wir unterstützen diese Anpassungen des Gesetzes (vgl. Art. 73a, 73b Abs. 1 und 74 E-ISG).

Soll nun aber neu, wie im Revisionsentwurf zum Informationssicherheitsgesetz (E-ISG) vorgesehen, eine *Pflicht* zur Meldung von Cyberangriffen eingeführt werden, welche bei Missachtung sogar zu einer strafrechtlichen Verurteilung der im Unternehmen zuständigen Person führen kann, was wir ablehnen, müsste im Gesetz klar bezeichnet werden, welche Unternehmen in der kommunikationstechnischen Lieferkette unter dieses Obligatorium fallen und wann eine Meldung zwingend an das NCSC zu machen ist. Diesem Anspruch wird der Gesetzesentwurf noch nicht gerecht, die persönlichen und sachlichen Merkmale der Meldepflicht sind noch zu wenig klar und eindeutig bestimmt.

Wir werden nachfolgend einige Punkte in der Vorlage ansprechen, welche unseres Erachtens noch zu wenig präzise ausgearbeitet sind. Auch wenn dazu im erläuternden Bericht u.a. auf die noch zu erlassenden Ausführungsbestimmungen der Verordnung verwiesen wird, sollte der Geltungsbereich der vorgeschlagenen Meldepflicht bereits auf Gesetzesebene genügend eingegrenzt sein. Dies folgt aus dem strafrechtlichen Bestimmtheitsgebot, welches schon in der Gesetzesgrundlage zu berücksichtigen ist, wobei diesbezüglich unerheblich ist, dass das NCSC, wie vorgesehen, vor Erlass der konkreten Meldeverfügung den vermeintlich Meldepflichtigen zuerst in einem ersten Schritt aufzuklären hat, bevor dann die «umzusetzenden Pflichten» durch das NCSC verfügt werden (vgl. Art. 74h E-ISG).

Keine Kommentare haben wir zu den Themen Änderung des Zweckartikels, Ergänzung der Begriffsdefinitionen, Bearbeitungsgrundsätze inkl. Weitergabe der Informationen und Möglichkeit der strafrechtlichen Anzeige gegen den Angreifer sowie Vorgaben zum Datenschutz und Informationsaustausch.

2. Neue Meldepflicht nach E-ISG

Adressaten der Meldepflicht

Mit Art. 74a E-ISG sollen neu Betreiberinnen von kritischen Infrastrukturen einer Melde*pflicht* bei Cyberangriffen unterstellt werden, wobei die nachfolgenden Artikel 74b – 74d E-ISG diese Meldepflicht in persönlicher und sachlicher Hinsicht eingrenzen. Laut dem erläuternden Bericht bilden Betreiberinnen kritischer Infrastrukturen, die in bestimmten Bereichen tätig sind, die Adressaten der Meldepflicht[1]. Diese Tätigkeitsbereiche sind in Art. 74b E-ISG aufgelistet, die Auflistung ist abschliessend[2], was im Gesetz so angeführt werden sollte.

Im Bereich der Informations- und Kommunikationsinfrastrukturen (Begriffsdefinition kritische Infrastrukturen gemäss Art. 5c EIG) sollen sämtliche Anbieterinnen von Fernmeldediensten nach Art. 3 lit. b Fernmeldegesetz (FMG) unter die Meldepflicht fallen (Art. 74b lit. k E-ISG). Laut erläuterndem Bericht sollen auch Over the Top

[1] Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens vom 12.01.2022, Ziff. 3.3.1, S. 10

[2] a.a.O. Ziff. 4 zu Art. 74b, S. 17: «Art. 74b listet deshalb konkret auf, für welche Unternehmen und Organisationen die Meldepflicht gelten soll.»

(OTT)-Dienste als fernmeldetechnische Übertragungen gelten mithin deren Anbieterinnen als FDA[3]. Das Bundesgericht hat jedoch im Entscheid 2C_544/2020 vom 29.04.2020 festgestellt, dass es sich bei Anbieterinnen von OTT-Diensten nicht um Anbieterinnen von Fernmeldediensten i.S. von Art. 3 lit. b FMG handelt[4]. Internetdienste, wie Skype, Threema, etc. fallen demnach entgegen der Aufzählung im erläuternden Bericht nicht unter den Begriff der Fernmeldedienste nach FMG. Sollten die Anbieterinnen dieser Dienste im E-ISG nacherfasst werden, gilt es zudem zu bedenken, dass diese Anbieterinnen oft nicht in der Schweiz domiziliert sind und damit von einer innerstaatlichen Regelung nicht erfasst wären.

Weiter gilt es anzumerken, dass das FMG laut dessen Art. 2 auch für die Übertragung von Radio- und Fernsehprogrammen gilt, soweit das BG über Radio und Fernsehen (RTVG) keine abweichenden Bestimmungen enthält. Auch reine Radio- und Fernsehanbieterinnen gelten demnach als FDA und sollten schon auf Gesetzesstufe beim Adressatenkreis der Meldepflichtigen ausgenommen werden, da es sich bei Radio- und Fernsehnetzen sicher nicht um kritische Infrastrukturen handelt.

Zusammenfassend fordern wir, dass bereits auf Gesetzesstufe der Adressatenkreis der Meldepflicht bei Informations- und Kommunikationsinfrastrukturen mit Bezug auf die Kritikalität der betriebenen Netze und Dienste präziser ausgearbeitet und abgegrenzt wird. Gewisse Kategorien von FDA können bspw. von vornherein ausgeklammert werden. Übrigens auch in anderen Bereichen drängt sich eine präzisere Abgrenzung, meist aber eine Eingrenzung auf, da die Bereiche zu weitläufig umrissen sind. So bspw. auch der Bereich der Anbieterinnen von Online-Markplätzen etc. (Art. 74b lit. f E-ISG) oder die Hersteller von Hard- und Software (Art. 74b lit. s E-ISG). Auch ist, wie oben angesprochene, die Frage des Auslandsbezugs zu klären, viele der potenziellen Adressaten gemäss Entwurf haben keinen Firmensitz in der Schweiz.

Ausnahmen

Art. 74c E-ISG sieht nun Ausnahmen vom Adressatenkreis der Meldepflicht vor, die später in den Ausführungsbestimmungen weiter bestimmt werden sollen. Diese Ausnahmen auf Gesetzesstufe sind jedoch sehr offen formuliert und lassen einen grossen Interpretationsspielraum zu. Es ist deshalb völlig unklar, welche Unternehmen schliesslich von der vorgesehenen Meldepflicht betroffen sein werden. Dies sollte jedoch bereits auf Gesetzesstufe näher konkretisiert werden; wie oben angeführt, sollten bereits auf Gesetzesstufe entweder via engerem Adressatenkreis oder präziseren Ausnahmen bestimmte Anbieterinnen ausgenommen werden.

Insgesamt und unter Berücksichtigung der noch auszuformulierenden Ausführungsbestimmungen sollten die Ausnahmen im persönlichen Geltungsbereich so präzise beschrieben und abgegrenzt sein, dass die Subsumtion nur in ganz wenigen Fällen Anlass zu Diskussionen und Abwägung im Einzelfall geben. Gerade von kleineren FDA, die Opfer eines Cyberangriffs werden, kann nicht verlangt werden, dass sie in diesen ausserordentlichen Situation noch zu prüfen haben, ob eine Meldung an das NCSC für sie obligatorisch ist. Auch kann nicht von ihnen verlangt werden, dass sie Infrastrukturkomponenten überwachen, welche sie in der kommunikationstechnischen Lieferkette nicht selbst betreuen und betreiben. Für all diese Fälle wäre u.E. vor allem auf die freiwillige Kooperation zu setzen und diese mit entsprechender Öffentlichkeits- und Aufklärungsarbeit durch das NSCS zu fördern. Kurz, im Sinne der Sache wäre eher eine grosszügig abgegrenzte Ausnahmeregelung vorzusehen und stattdessen auf die Freiwilligkeit zur Kooperation zu setzen, was sicher auch vertrauensbildender wäre, als eine strafbewehrte Meldepflicht und einen Kooperationszwang vorzusehen.

Auslöser

Auch die definierten Auslösungsfälle für die zwingende Meldung ans NCSC in Art. 74d E-ISG d.h. die sachlichen Merkmale, sind in unseren Augen zu vage beschrieben, um verlässlich im Voraus abzugrenzen zu können,

[3] a.a.O., Ziff. 4 zu Art. 74b lit. k E-ISG, S. 19
[4] BGE 2C_544/2020, Ziff. 5.5.

wann eine Meldung ans NCSC zu ergehen hat und wann nicht. Bei der Implementation des NCSC-Meldeprozesses in die Unternehmensorganisation werden aber klare Kriterien benötigt, wann eine Meldung durch die zuständige Person an das NCSC zwingend ist. Der Wortlaut von Art. 74d Abs. 1 E-ISG weist zudem darauf hin, dass im vornherein nur Angriffe auf die *kritische* Infrastruktur zu melden sind, was umgekehrt bedeutet, dass auch Unternehmen im persönlichen Geltungsbereich der Meldepflicht (Art. 74b und 74c E-ISG) nur dann einen Angriff zu melden haben, falls die kritische Infrastruktur betroffen ist, Angriffe auf andere Infrastrukturbestandteile dann hinsichtlich Meldepflicht unbeachtlich wären. Das Gesetz lässt aber offen, was *kritische* Infrastrukturen sind. Mit Blick auf das Bestimmtheitsgebot für strafrechtliche Sanktionen im Falle einer Missachtung der Meldepflicht, ist es jedoch nicht zulässig, den Begriff der «kritischen Infrastruktur» nur ansatzweise zu definieren.

Weiter kann von den betroffenen Anbieterinnen nicht verlangt werden, dass sie Nachforschungen anstellen zur Frage, ob ein Merkmal der in Art. 74d E-ISG aufgeführten Auslösungsfällen vorliegt. Wie soll bspw. abgeklärt werden, ob ein fremder Staat hinter einem Angriff steckt (Art. 74d Abs. 1 lit. b E-ISG), diese Informationen werden kaum einfach ersichtlich sein. Schliesslich sollte klargestellt werden, dass Angriffe auf Endkundinnen und Endkunden bzw. deren Endgeräte und eigene Infrastrukturbestandteile (bspw. Heimvernetzung) keine Meldepflicht auslöst. Die FDA haben nicht zwingend Kenntnis von solchen Vorfällen.

Persönliche Strafbarkeit

Wir lehnen die in Art. 74i E-ISG vorgesehene persönliche Strafbarkeit der im Unternehmen zuständigen Person bei Missachtung der mit Verfügung des NCSC bestätigten Meldepflichten als ultima ratio -Massnahme ab, eine mögliche Busse des Unternehmens in einem solchen Fall erachten wir als ausreicheichenden Anreiz für die Unternehmen, die Meldepflicht einzuhalten. Der erläuternde Bericht geht an verschiedenen Stellen auf den kollaborativen Ansatz zwischen Behörden und privaten Unternehmen und den diesbezüglichen gemeinsamen Interessen bei der Abwehr von Cyberbedrohungen ein und anerkennt das Potential eines partnerschaftlichen Verhältnisses. Das Ziel sollte also eine freiwillige vertrauensvolle Zusammenarbeit sein, welche aus Sicht der Unternehmen nützlich ist. Die Möglichkeit der strafrechtlichen Verurteilung einzelner Mitarbeiter widerspricht dieser allgemeinen Stossrichtung. Der massgebliche Fachkräfte-Stellenmarkt steht zurzeit eh schon unter Druck und eine solche Regelung würde dies nur noch verstärken, weil die Bereitschaft naturgemäss klein ist, einen Verantwortung mit persönlicher Strafbarkeit im Unternehmen zu übernehmen.

3. Meldepflichten in Ausnahmesituationen an verschiedene Behörden

Wir erachten es als problematisch, wenn in ausserordentlichen Situationen, bspw. bei Netz- und Systemausfällen, die vielleicht auch auf einen Cyberangriff zurückgehen, verschiedene Meldepflichten gegenüber Behörden erfüllt werden müssen. Denn gerade in diesen Momenten sind die Ressourcen der Unternehmen durch die interne Problemlösung gebunden und entsprechend kontraproduktiv wäre es, gleichzeitig den administrativen Aufwand der betroffenen Unternehmen in solchen Fällen zu vergrössern. So sollten die Unternehmen bspw. bei einem Sicherheitsvorfall nicht mehrere Amtsstellen informieren müssen, vielmehr sollte eine zentrale Anlaufstelle, je nach Bedarf, automatisch weitere Stellen informieren («one stop shop»). Wie dies im vorliegenden Gesetzesprojekt mit den Meldungen nach Art. 24 des revidierten Datenschutzgesetzes vorgesehen ist, sollten gleiche Abstimmungen und Harmonisierungen auch mit anderen sektoriellen Anlaufstellen vorgenommen werden. Bspw. haben FDA nach Art. 96 der Verordnung über Fernmeldedienste das BAKOM oder neu nach dem Revisionsentwurf die Nationale Alarmzentrale zu verständigen, wenn ein qualifizierter Netzausfall vorliegt. Ein solcher Netzausfall kann auch auf einen Cyberangriff zurückgehen, weshalb auch hier eine entsprechende Harmonisierung vorgenommen werden sollte.

***

Wir danken Ihnen im Voraus, dass Sie unsere Bemerkungen und Argumente in die weitere Ausarbeitung der E-FDV einbeziehen und unsere Anträge berücksichtigen. Für Fragen dazu stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüssen

SUISSEDIGITAL – Verband für Kommunikationsnetze

Dr. Simon Osterwalder, Rechtsanwalt
Geschäftsführer

Stefan Flück, Fürsprecher LL.M.
Leiter Rechtsdienst