scienceindustries
Wirtschaftsverband
Chemie Pharma Life Sciences

Nordstrasse 15
Postfach
8021 Zürich
Schweiz

T +41 44 368 17 11
F +41 44 368 17 70
info@scienceindustries.ch

Eidgenössisches Finanzdepartement
Bundesgasse 3
3003 Bern

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

Zürich, 11. April 2022

Vernehmlassung zur Einführung einer Meldepflicht für Cyberangriffe im Rahmen der Revision des Bundesgesetz über die Informationssicherheit beim Bund (ISG): Stellungnahme scienceindustries

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.

scienceindustries, der Wirtschaftsverband Chemie Pharma Life Sciences, nimmt hiermit gerne Stellung zur angedachten Meldepflicht von Cyberangriffen für Betreiberinnen kritischer Infrastrukturen. Alle diese Mitglieder sind an einem effizienten Schutz vor Cyber-Risiken interessiert. Als Branchenvertretung haben wir die verschiedenen Rückmeldungen zum Revisionsentwurf zusammengefasst und reichen diese Ihnen hiermit gerne zur Berücksichtigung ein.

Grundsätzlich ist scienceindustries der Ansicht, dass mit diesem Vorschlag die Verwaltung ihre Verantwortung an die Unternehmen auslagert und vom bisherigen, zielführenden Weg der Kooperation Abstand nimmt, indem Unternehmen lediglich als Informationslieferanten eingespannt werden. Unserem Verständnis nach muss eine primäre Aufgabe des NCSC dagegen sein, Betreibern kritischer Infrastrukturen und weiteren exponierten Industrien und Gewerben durch internationale Informationsbeschaffung und proaktiver zur Verfügungstellung relevanter Informationen bezüglich Cyber Security (Bring-Schuld NCSC) an eben diese einen möglichst hohen Stand der vorbereitenden Abwehrmassnahmen durch diese Unternehmen zu ermöglichen. Wir erachten deshalb eine Formalisierung der **Melde-Möglichkeit** als den zielführenderen Weg, sicherheitsrelevante Informationen an das NCSC weiterzureichen. Eine **Meldepflicht** mit Sanktionsandrohungen ist hingegen kaum zielführend.

Grundsätzliche Bemerkungen – Sicherheit und Prävention durch Kooperation
Wir stehen einer Meldepflicht skeptisch gegenüber und lehnen Sanktionsvorgaben gemäss vorliegendem Entwurf grundsätzlich ab. Wie im erläuternden Bericht festgehalten, funktioniert der freiwillige Informationsaustausch früher mit MELANI und heute mit dem NCSC. Im erläuternden Bericht wird erwähnt, dass eine Ausweitung des Modells nicht realistisch sei. Der Bericht bleibt aber schuldig, warum dies nicht realistisch sei. Wir teilen diese Einschätzung nicht. Wir sind im Gegenteil davon überzeugt, dass gerade der Ausbau dieses Ansatzes wesentlich zielführender ist als die Einführung einer Meldepflicht zusammen mit Sanktionsandrohungen. Aus dem Bereich der Nonproliferation kennt die Bundesverwaltung bereits seit

vielen Jahren etablierte Zusammenarbeiten mit der Industrie, die der Sensibilisierung dienen, allen voran seien hier das Programm des SECO im Bereich Exportkontrolle sowie PROPHYLAX der fedpol zu nennen. Diese Programme dienen vor allem auch dem Aufbau von Vertrauen zwischen Industrie, Verwaltung und Vollzugsbehörden, dem gegenseitigen Verständnis und der Sicherstellung, dass die Kommunikation zwischen Unternehmen und Verwaltung in beide Richtungen funktioniert. Eine Meldepflicht mit Sanktionsandrohung führt für einen solchen, auf Kooperation zwischen den Partnern angewiesenen Sicherheitsbereich zu mehr Schaden als Nutzen.

Weiter ist zu berücksichtigen, dass bei Schweizer Unternehmen, die Niederlassungen ausländischer Firmen sind, respektive ihrerseits Niederlassungen im Ausland unterhalten, die relevanten IT-Abteilungen, die zu Gunsten der ganzen Unternehmung arbeiten, häufig nicht in der Schweiz angesiedelt sind. Das hat zur Konsequenz, dass die Schweizer Unternehmensbereiche häufig gar nicht über erfolgte Cyberangriffe informiert sind. Entsprechend können sie keine Informationen weiterreichen. Dazu kommt, dass die im Ausland angesiedelten IT-Abteilungen den lokalen gesetzlichen Verpflichtungen entsprechen müssen und somit die Schweizerische Gesetzgebung nicht umsetzen müssen. Eine Meldepflicht kann also dazu führen, dass sich eine Firma also entweder dem Bruch von Datenschutzgesetzen im Sitzstaat oder der Widerhandlung gegen die Meldepflicht in der Schweiz verstösst. Dementsprechend kommt so ein Unternehmen unabhängig davon wie es sich verhält, in eine juristisch problematische Situation. Wir erachten dies als äusserst schädlich.

Sollte an einer Meldepflicht festgehalten werden, so ist für eine erfolgsversprechende Umsetzung zwingend zu berücksichtigen, dass:

- die Meldepflicht den betroffenen Unternehmen und der Volkswirtschaft letztlich mehr bringen muss, als sie kostet.
- sie einen verhältnismässigen, subsidiären, risikobasierten Ansatz verfolgen muss, der administrative und finanzielle Aufwände auf ein Minimum reduziert.
- sie einer kooperativen Grundeinstellung bedarf, da sowohl die Behörden als auch die Unternehmen an einem bestmöglichen Schutz vor Cyber-Angriffen interessiert sind.
- aus dem vorstehenden Argument bei der Durchsetzung der neu angedachten Pflichten prinzipiell auf Strafbestimmungen verzichtet wird.

Es muss überdies sichergestellt werden, dass Überschneidungen mit anderen, sektoriellen Meldepflichten im Bereich Cyber-Sicherheit nicht zu einem Mehraufwand für die Unternehmen führen.

Bemerkungen zu den Artikeln

2. Abschnitt: Pflicht zur Meldung von Cyberangriffen auf kritische Infrastrukturen

---

Art. 74a Meldepflicht

> Die Betreiberinnen von kritischen Infrastrukturen ~~müssen~~ melden dem NCSC Cyberangriffe 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.

Wir beantragen die obenstehende, gelb markierte Anpassung des Textes. Ausserdem ist zu definieren, was unter dem Begriff "so rasch als möglich" zu verstehen ist.

Begründung
Die Formulierung "so rasch als möglich" ist unpräzise. Beispiel: Alle Veterinärfirmen sind kleine KMUs mit max. 20-40 Mitarbeitern, selbst im Fall der Tochterfirmen grösserer pharmazeutischer Unternehmen. Im Falle einer Cyberattacke werden die internen Ressourcen extrem gefordert sein. Oberste Priorität hat dann die Lösung des Problems und die Eindämmung des möglichen Schadens. Die Meldung an das NCSC wird in dieser Phase wahrscheinlich nicht die oberste Priorität haben, weshalb hier auch ein Augenmass mit Bezug auf die zeitliche Abwicklung von Meldungen angezeigt ist. Offenbar ist diesbezüglich eigenes Ermessen vorgesehen, dazu gibt es allerdings im Gesetz keine präzisen Angaben, an welchen sich Unternehmen orientieren könnten, was insbesondere dann eine nicht mehr akzeptable Verzögerung bedeuten würde.

Art. 74b Bereiche

Die Meldepflicht gilt für

…

i. Unternehmen, die für die Herstellung, das Inverkehrbringen und die Einfuhr von Arzneimitteln eine Bewilligung nach dem Heilmittelgesetz vom 15. Dezember 200012 (HMG) haben oder Medizinprodukte nach Artikel 4 Absatz 1 Buchstabe b HMG herstellen oder vertreiben;

…

r. Unternehmen, die die Bevölkerung mit unentbehrlichen Gütern des täglichen Bedarfs versorgen;

Wir beantragen eine exakte Definition und unternehmensspezifische Bezeichnung der Betriebe, die unter die Definition fallen, wenn nicht hier direkt im Gesetz, was für uns nachvollziehbar ist, so doch auf Stufen einer Ausführungsverordnung, auf die hier explizit zu verweisen ist.

Begründung:
In Anbetracht der Unklarheit darüber, was als kritische Infrastruktur zu betrachten ist, ist nicht klar, wer durch eine Meldepflicht letztlich erfasst würde. Der Bund hat verschiedene Publikationen mit unterschiedlichen Definitionen, was kritische Infrastrukturen letztlich umfasst. Aus unserer Sicht es es unzumutbar, , dass nun unzählige Unternehmen diese unterschiedliche Publikationen studieren und abwägen müssen, ob sie unter die jeweilige Definition fallen oder nicht. Wir stellen hier klar eine Rechtsunsicherheit fest. Gerade die Corona-Pandemie hat exemplarisch aufgezeigt, dass unter dem Begriff "untentbehrliche Güter des täglichen Bedarfs" schon innerhalb der Bevölkerung kaum ein Konsens besteht und sehr unterschiedlich interpretiert wird. Die Bereitstellung unentbehrlicher Güter des täglichen Bedarfs für die Bevölkerung ist aufgrund internationaler Lieferketten komplexer, als das Politik und Verwaltung annehmen. Denn hinter der Bereitstellung dieser Produkte für die Bevölkerung stehen Produktions- und Lieferketten, die auf den ersten Blick nicht kritisch erscheinen, aber bei Ausfall die Bereitstellung dennoch be- oder sogar verhindern.

Art. 74d Zu meldende Cyberangriffe

1 Ein Cyberangriff auf eine kritische Infrastruktur muss gemeldet werden, wenn Anzeichen dafür bestehen, dass:

…

~~b. ein fremder Staat ihn ausgeführt oder veranlasst hat;~~

…

2 Ein Cyberangriff auf eine kritische Infrastruktur muss immer gemeldet werden, wenn er mit Erpressung, Drohung oder Nötigung gegenüber der Betreiberin einer kritischen Infrastruktur oder ihren Mitarbeitenden verbunden ist.

Wir beantragen die Klärung der Frage der Reichweite der Pflicht. Die Meldepflicht muss auf Angriffe auf Anlagen in der Schweiz beschränkt sein. Ausländische Standorte, selbst wenn kritisch für die Versorgung in der Schweiz, unterstehen nicht dem Schweizer Gesetz.
Art. 74d. Abs. 1.b. ist ersatzlos zu streichen.
Art. 74d. Abs. 2. Die Meldepflicht ist auf Erpressung, Drohung oder Nötigung dahingehend zu beschränken, dass sie nur bei Vorliegen eines Bezuges zur Geschäftstätigkeit wirksam wird.

Begründung
Viele unserer Mitglieder sind Tochterunternehmen ausländischer Firmen, respektive sind Schweizer Unternehmen mit Tochterfirmen im Ausland. Viele von ihnen sind dadurch bereits heute nicht nur exponiert, sondern sehen sich ständig mit Cyber-kriminellen Aktionen konfrontiert. Das geht je nach Unternehmen in Grössenordnungen von einigen Hundert Attacken pro Tag, wovon die meisten bereits durch einfache Sicherheitsmassnahmen wie eine gute Firewall bewältigen lassen. Aber nicht in jedem Fall ist klar, wo ein Angriff seinen Ursprung hat.

Art. 74d. Abs. 1.b. ist deshalb ersatzlos zu streichen, da eine derartige Zuweisung fast nie, und wenn, dann nicht zeitgerecht erfolgen kann.

Art. 74e Inhalt der Meldung

1 Die Meldung muss Informationen zur kritischen Infrastruktur, zur Art und Ausführung des Cyberangriffs, zu seinen Auswirkungen und zum geplanten weiteren Vorgehen der Betreiberin der kritischen Infrastruktur enthalten.

Wir beantragen, dass sich die Meldepflicht auf die Bereitstellung sogenannter IOCs (Indicator of Compromises) fokussiert. Ausserdem ist zu berücksichtigen, dass seitens des NCSC davon ausgegangen werden muss, dass die verschiedenen Unternehmen sich in unterschiedlichsten Stadien der Abwehrbereitschaft sowie Informationslieferfähigkeiten befinden.

Art. 74e Inhalt der Meldung

3 Benötigt eine Stelle oder Behörde Informationen, die über Art. 74e hinausgehen, kann die Betreiberin diese über das System direkt an die betreffende Stelle oder Behörde übermitteln.

Und

Art. 74g Auskunftspflicht

Die Betreiberin der kritischen Infrastruktur ~~muss~~ erteilt, wenn möglich, dem NCSC ergänzende Auskünfte zu den Inhalten der Meldung nach Artikel 74e ~~erteilen~~, die es zur Erfüllung seiner Aufgaben in Bezug auf die Abwehr weiterer Cyberangriffe auf kritische Infrastrukturen benötigt.

Wir beantragen die obenstehende, gelb markierte Anpassung des Textes. Ausserdem ist zu definieren, welche Art der Informationen damit gemeint ist und wie die Begründung für solche zusätzlichen Informationsbegehren auszusehen hat.

Begründung:
Ein betroffenes Unternehmen kann Informationen nur zugänglich machen, wenn dies in seinen Fähigkeiten liegt. Allerdings sind die Spielregeln klar zu definieren, welche Informationen das NCSC noch zusätzlich einzuholen überhaupt berechtigt ist. Insbesondere bei multinationalen Firmen, bei denen für deren ausländischen Firmensitze auch ausländisches Recht tangiert wird, muss seitens des Schweizer Gesetzgebers hier ein Höchstmass an Genauigkeit und Transparenz geschaffen werden, wenn in einem Eintretensfall nicht Zeit durch nachträglich notwendig werdende juristische Abklärungen verloren gehen soll.

Art. 74h Verletzung der Melde- oder Auskunftspflicht

Und

Art. 74i Widerhandlungen gegen Verfügungen des NCSC

Wir beantragen die ersatzlos zu Streichung von Art. 74h und Art 74i.
Eventualiter ist eine Busse auf ein Prozentsatz des Ertrages, jedoch maximal CHF 100'000 zu beschränken.

Begründung
Durch die Formulierungen von Art. 74h und 74i wird bei den Unternehmen unweigerlich ein Fokus auf die Beherrschung der möglichen juristischen Risiken bezüglich Meldung von Cyberangriffen gelegt werden. Damit werden unnötigerweise in einem Bereich, bei dem gleichgerichtete Interessen bestehen und es keinerlei Sanktionsgründe gibt, Ressourcen für die Absicherung gegen die Sanktionsrisiken gebunden, die dadurch einer wirksamen Abwehr und Bewältigung ebensolcher Cyberrisiken entzogen werden.

Darüber hinaus wird durch die Höhe der angesetzten Maximalbussen neben dem potenziell existenzbedrohenden Cyberrisiko auch noch administrativ eine existenzielle Gefahr durch übertrieben hohe Bussandrohung geschaffen.
Eine Busse von CHF 100'000 ist speziell für kleine und mittlere Unternehmen unzumutbar und unverhältnismässig.

3. Abschnitt: Datenschutz und Informationsaustausch

Art. 75 Bearbeitung von Personendaten

Hier ist zu berücksichtigen, dass bei Ereignissen, die Personen ausserhalb der Schweiz (mit-)betreffen, die Weitergabe persönlicher Daten Konflikte mit der Datenschutzgesetzgebung in deren Jurisdiktion hervorrufen können.

Art. 76 Zusammenarbeit im Inland

Absätze 1 und 2
Scienceindustries steht der Weitergabe von vertraulichen Daten, insbesondere auch Personendaten, kritisch gegenüber.
Zumindest ist in den Absätzen 1 und 2 einschränkend vorzusehen, dass die Weitergabe solcher Informationen, speziell an Wettbewerber in ähnlichen Märkten nicht ohne Zustimmung des Dateninhabers erfolgen darf.

Art. 77 Internationale Zusammenarbeit

Scienceindustries steht der Weitergabe von vertraulichen Daten, insbesondere auch Personendaten, kritisch gegenüber.
Zumindest ist mit Gültigkeit für die Absätze 1, 2 und 3 einschränkend vorzusehen, dass die Weitergabe solcher Informationen nicht ohne Zustimmung des Dateninhabers erfolgen darf.

Abschliessend bedanken wir uns im Namen unserer Mitglieder für die Möglichkeit der Mitwirkung.

Wir stehen Ihnen bei allfälligen Fragen zu unserer Stellungnahme gerne zur Verfügung.

Mit freundlichen Grüssen

Dr. Michael Matthes
Stv. Direktor

Dominique Werner
Leiter Chemikalienrecht