Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Bern, 13. Dezember 2019

Varianten für Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen

Bericht des Bundesrates in Erfüllung des Postulates 17.3475 Graf-Litscher vom 15.06.17

Inhaltsverzeichnis

1 Einleitung

Die Einführung von Meldepflichten bei schwerwiegenden Sicherheitsvorfällen ist in der Schweiz ein vieldiskutiertes Thema und die Meinungen gehen dabei weit auseinander. Mit der Zunahme von Cyberrisiken hat es nochmals an Bedeutung gewonnen, da Informationen über Vorfälle in diesem sehr dynamischen Bereich besonders wertvoll sind.
Der vorliegende Bericht soll dazu beitragen, die Diskussionen um Meldepflichten auf einer fundierten Basis zu führen. Er beleuchtet deshalb die verschiedenen Facetten von Meldepflichten, beschreibt den Kontext der bestehenden Meldepflichten in der Schweiz sowie im Ausland und entwickelt verschiedene Grundmodelle für Meldepflichten als mögliche Varianten zur Umsetzung.
Zunächst wird in diesem Kapitel einleitend die Ausgangslage dargelegt, die verschiedenen Aufträge zur Prüfung von Meldepflichten beschrieben und die Struktur des Berichts erläutert.

1.1 Ausgangslage

Moderne Gesellschaften zeichnen sich durch eine starke Vernetzung aus. Infrastrukturen und ihre Systeme sind durch zahlreiche Schnittstellen miteinander verbunden und so möglichst optimal aufeinander abgestimmt. Die starke Vernetzung legt die Basis für ein effizientes Funktionieren der Gesellschaft. Dies ist nicht nur, aber auch, eine Folge der Digitalisierung dieser Infrastrukturen. Die digitale Transformation vereinfacht und beschleunigt den Austausch zwischen verschiedenen Systemen in einem Ausmass, welches die physischen Grenzen zwischen den Systemen zunehmend irrelevant werden lässt. Da wir erst am Anfang des Prozesses der digitalen Transformation stehen und noch längst nicht alle technologischen Möglichkeiten ausgeschöpft sind, ist davon auszugehen, dass die Vernetzung weiter zunimmt. Mit der zunehmenden Vernetzung der Infrastrukturen steigt aber auch das Risiko, dass Störungen und Ausfälle von einzelnen Infrastrukturen Auswirkungen haben, welche weit über das eigene System hinausgehen. Da moderne Gesellschaften stark von funktionierenden Infrastrukturen abhängen, ist es von zentraler Bedeutung, sich Gedanken darüber zu machen, wie dieser wachsenden gegenseitigen Abhängigkeit unserer Infrastrukturen begegnet werden kann.
Ein Schlüsselelement zum Schutz vor grossflächigen Ausfällen von kritischen Infrastrukturen[1] ist der sektorübergreifende Informationsaustausch. Wenn die physischen Infrastrukturen zunehmen vernetzt sind, muss auch sichergestellt werden, dass die verantwortlichen Stellen sich gegenseitig über Entwicklungen, Risiken und Vorfälle informieren. Ein solcher Informationsaustausch ermöglicht es den Entscheidungsträgern, die Risiken für ihre Infrastruktur richtig einzuschätzen und mögliche Gefahren frühzeitig zu erkennen. Besonders wichtig ist der Informationsaustausch für den Schutz der kritischen Infrastrukturen vor Cyberrisiken. Cybervorfälle können potentiell sehr unterschiedliche Organisationen gleichzeitig treffen und sich über die Schnittstellen zwischen den Infrastrukturen rasch zu einem sektorübergreifenden Problem entwickeln. Eine frühzeitige gegenseitige Warnung ist bei der Eindämmung der Auswirkungen von Cybervorfällen deshalb besonders wichtig.
Die Förderung des Informationsaustausches zwischen Betreibern kritischer Infrastrukturen ist deshalb seit vielen Jahren ein wichtiges Anliegen von Behörden. Viele Staaten haben Plattformen für den Informationsaustausch geschaffen und fördern den Austausch zwischen kritischen Infrastrukturen aktiv. In der Schweiz betreibt der Bund beispielsweise seit dem Jahr 2004 mit der Melde- und Analysestelle Informationssicherung MELANI eine solche Plattform. Vermehrt greifen Staaten aber auch auf regulatorische Instrumente zurück und verpflichten Betreiber kritischer Infrastrukturen dazu, Sicherheitsvorfälle zu melden.

[1] Als kritische Infrastrukturen (KI) werden in der Schweiz Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung sind. Dazu zählen etwa die Energieversorgung, der Personen- und Güterverkehr oder die medizinische Versorgung. (vgl. Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022)

Besonders wichtig ist in diesem Zusammenhang die EU-RICHTLINIE 2016/1148 vom 6. Juli 2016 über Massnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.[2] Diese Richtlinie fordert die Einführung von «Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste» in allen Mitgliedstaaten der EU. Zwar ist die NIS-Richtlinie noch nicht in allen Mitgliedsstaaten der EU umgesetzt, sie hat aber in vielen Ländern direkt zur Einführung oder Verstärkung von Meldepflichten bei Cybervorfällen geführt.
In der Schweiz sind zur Frage, ob und wie Meldepflichten in der Schweiz eingeführt werden können, sind schon verschiedene Ansätze entwickelt worden. Namentlich hat sich der Beirat Zukunft Finanzplatz 2017 in seinem Bericht mit den Vor- und Nachteilen von Meldepflichten für Cybervorfälle für den Finanzsektor auseinandergesetzt[3], ein Forschungsteam der Universität Lausanne, der Militärakademie und der Universität St. Gallen hat auf den Informationsaustausch über MELANI untersucht und dabei die wichtigsten Hindernisse und Anreize für das Teilen von Informationen zu Sicherheitsvorfällen identifiziert[4] und eine repräsentative Umfragestudie unter Geschäftsführenden von kleinen und mittleren Unternehmen (KMU) hat ergeben, dass unter den KMU noch keine klaren Meinungen (weder zustimmend noch ablehnend) gegenüber der Einführung von Meldepflichten stattgefunden hat.[5]

1.2 Auftrag

Angesichts des internationalen Trends zur Einführung von Meldepflichten und der diesbezüglich noch nicht weit fortgeschrittenen Diskussion in der Schweiz gilt es nun, Grundlagen zu erarbeiten, welche dazu dienen, die Frage zu klären, ob und wenn ja, welche Meldepflichten einzuführen sind. Bundesrat, Parlament und die Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit haben deshalb entsprechende Prüfauftrage formuliert:

- **17.3475 Po. Graf-Litscher «Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen»:** Der Bundesrat wird eingeladen, zu prüfen und darüber Bericht zu erstatten, wie und aufgrund welcher Kriterien die Betreiber von kritischen Infrastrukturen einer allgemeinen Meldepflicht bei potenziell schwerwiegenden Sicherheitsvorfällen bzw. Funktionsausfällen unterstellt werden könnten, wie die Meldungen und eigenen Erkenntnisse systematisch ausgewertet und wie gestützt darauf ein Frühwarn-, Beratungs- und Abwehrsystem aufgebaut werden könnte.

- **Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS), Massnahme 9 «Prüfung einer Meldepflicht für Cybervorfälle und Entscheid über ihre Einführung»:** Zur Verbesserung des Lagebilds zu Cyberbedrohungen ist die Einführung einer Meldepflicht für Cybervorfälle zu prüfen und über ihre Einführung zu befinden. Dabei sind zunächst die Fragen zu klären, für wen eine Meldepflicht gelten soll, welche Vorfälle sie betrifft und an wen sie gemeldet werden müssen und ob eine Meldepflicht im Vergleich zu heute das Lagebild substanziell verbessern kann. Es werden Varianten für die Umsetzung von Meldepflichten in den verschiedenen Sektoren erarbeitet und aufgezeigt, welche gesetzlichen Grundlagen dafür nötig sind. Dies erfolgt unter Einbezug der jeweils zuständigen Behörden, der Privatwirtschaft und der Verbände, in Koordination mit der nationalen Strategie zum Schutz kritischer Infrastrukturen und unter Berücksichtigung der internationalen Entwicklungen. Auf der Basis dieser Abklärungen wird anschliessend über die Einführung einer Meldepflicht entschieden und gegebenenfalls die nötigen Schritte eingeleitet.

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[3] Beirat Zukunft Finanzplatz, Rahmenbedingungen für die Versicherbarkeit und ein effizientes Management von Cyber Security Risiken.
[4] Mermoud et al., To share or not to share: a behavioral perspective on human participation in security information sharing, Journal of Cybersecurity, 2019, Vol. 5, No. 1.
[5] Gfs-zürich, Cyberrisiken in Schweizer KMUs, 2017.

- **Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI), Massnahme 8:** Es ist die Erarbeitung eines Vorschlags für Rechtsgrundlagen zu prüfen, mit der die Betreiber verpflichtet werden, schwerwiegende Sicherheitsvorfälle bzw. Funktionsausfälle den zuständigen Behörden zu melden.

- **Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit, Empfehlung 28 «Meldepflichten»:** Der Bund führt für die Betreiber kritischer Infrastrukturen eine Meldepflicht für Cybervorfälle ein. Er erarbeitet dabei zusammen mit den zuständigen Behörden, der Privatwirtschaft und den Verbänden die Grundlagen und berücksichtigt die internationale Entwicklung.

Der vorliegende Bericht fasst die bisherigen Arbeiten, welche im Rahmen dieser Aufträge unternommen worden sind, zusammen. Im Wesentlichen basiert er auf den Resultaten einer Auftragsstudie, in welcher der Ist-Zustand in der Schweiz bezüglich bestehender Meldepflichten erhoben, Meldepflichten in anderen Staaten analysiert und Interviews mit Schweizer Experten durchgeführt wurden.[6] Auf der Grundlage der dadurch gewonnenen Erkenntnisse sind Grundmodelle entwickelt worden, welche in einer vorgesehenen Diskussion verfeinert und weiter ausgearbeitet werden sollen. Die Studie fokussiert dabei stark auf Meldepflichten zu Cybervorfällen, nicht weil Expertinnen und Experten besonders in dieser Hinsicht Handlungsbedarf sehen, sondern weil sich die eingeführten Meldepflichten in anderen Staaten meist explizit auf Cybervorfälle beziehen. Es bleibt zu prüfen, ob und wie die vorgeschlagenen Modelle generell für die Meldung von Sicherheitsvorfällen verwendet werden können und wie die Modelle für Meldepflichten zu Cybervorfällen mit den in vielen Sektoren bereits bestehenden Meldepflichten für andere Sicherheitsvorfälle vereinbart werden können.

1.3 Aufbau des Berichts

Der Bericht beschreibt im nächsten Kapitel (Kapitel 2), welche Fragen sich in Bezug auf die mögliche Einführung oder Ausweitung von Meldepflichten stellen. Es ist wichtig festzuhalten, dass es nicht nur um die Grundsatzfrage geht, ob überhaupt weitere Meldepflichten eingeführt werden sollen, sondern auch darum abzuklären, welchen Zwecken Meldepflichten dienen, wen und was sie umfassen sollen und wie sie allenfalls ausgestaltet werden können.
Im Anschluss wird in den dritten und vierten Kapiteln die aktuelle Situation beschrieben. Es werden die bestehenden Meldepflichten in der Schweiz aufgezeigt und die in den letzten Jahren neu eingeführten Meldepflichten im Ausland beschrieben. Dies vermittelt einen Eindruck darüber, wo die Schweiz heute im Vergleich mit anderen Ländern steht und welche Lösungen bei der Einführung von Meldepflichten in anderen Staaten gewählt wurden.
Basierend auf den internationalen Vergleichen, der Bestandsaufnahme von Meldepflichten in der Schweiz und den Interviews mit Expertinnen und Experten präsentiert Kapitel 5 vier Grundmodelle zur Meldepflicht, welche in der Studie «Prüfung von Meldepflichten bei Sicherheitsvorfällen» entwickelt wurden. Der Bericht schliesst (Kapitel 6) mit einem kurzen Ausblick über das weitere Vorgehen zur Klärung, ob und wie Meldepflichten in der Schweiz eingeführt werden sollen.

[6] PwC Schweiz, Prüfung einer Meldepflicht bei Sicherheitsvorfällen, Oktober 2019.

2 Zu klärende Fragen in Bezug auf die Einführung von Meldepflichten

Die Diskussion um Meldepflichten wird oft zu rasch auf die Grundsatzfrage reduziert, ob solche eingeführt werden sollen oder nicht. Für eine Beurteilung dieser Frage muss zunächst aber klar definiert werden, um welche Art von Meldepflichten es bei der Beantwortung dieser Frage handelt, gegenüber wem gemeldet werden müsste und welche Konsequenzen konkret bei einer Einführung zu erwarten wären. Die im Rahmen der Studie «Prüfung einer Meldepflicht bei Sicherheitsvorfällen» geführten Interviews und die Analyse der Meldepflichten in anderen Ländern haben deutlich gemacht, wie wesentlich eine sorgfältige Beantwortung dieser Fragen bei der Entwicklung von Modellen für eine Meldepflicht ist. Dieses Kapitel beschreibt deshalb zunächst die wichtigsten zu klärenden Fragen, welche bei der Entwicklung und Bewertung von möglichen Lösungen für Meldepflichten stets beachtet werden müssen.

2.1 Zwecke der Meldepflichten

Meldepflichten dienen grundsätzlich dem Ziel, den Schutz der Wirtschaft und des Staates zu stärken. Im Detail unterscheiden sich die Begründungen zur Einführung von Meldepflichten jedoch deutlich. Grob lassen sich fünf Gründe unterscheiden, weshalb Behörden Unternehmen einer Meldepflicht zu Sicherheitsvorfällen unterstellen:

- **Aufsichtspflicht des Staates gegenüber der Wirtschaft:** Der Staat ist vom Gesetzgeber über die Regulatoren (in je nach Sektor unterschiedlicher Ausprägung) mit der Aufsicht über gewisse Wirtschaftsbereiche beauftragt. In dieser Funktion müssen die zuständigen Behörden Kenntnis von relevanten Störungen haben, um nötigenfalls Massnahen zu ergreifen, welche das Funktionieren des Sektors sicherstellen.
- **Prävention vor Sicherheitsvorfällen:** Durch die Einführung von Meldepflichten werden Unternehmen gezwungen, sich mit Sicherheitsvorfällen auseinanderzusetzen. Ihre eigenen Prozesse müssen so strukturiert sein, dass sie Vorfälle rechtzeitig erkennen und melden können. Über diese Effekte der Meldepflicht wird generell die Prävention vor Sicherheitsvorfällen gestärkt.
- **Beurteilung der Bedrohungslage:** Behörden sind bei der Beurteilung der Bedrohungslagen zunehmend auf Informationen aus der Wirtschaft angewiesen. Cyberangriffe beispielsweise können sich gezielt gegen einzelne Unternehmen richten und werden vom Staat ohne Meldung des betreffenden Unternehmens nicht oder erst zu spät erkannt.
- **Frühwarnung durch Informationsaustausch:** Weil durch die zunehmende Vernetzung die gegenseitigen Abhängigkeiten wachsen, ist ein Austausch über sicherheitsrelevante Vorfälle immer wichtiger. Über die Einführung von Meldepflichten können Behörden sicherstellen, dass wertvolle Informationen zum Beispiel über entdeckte Schwachstellen oder neue Angriffsmuster allen für das Funktionieren von Staat und Gesellschaft wesentlichen Organisationen rasch zur Verfügung gestellt werden.
- **Koordinierte Reaktion:** Durch die Meldung von Vorfällen wird eine koordinierte Reaktion erst ermöglicht. Wegen der gegenseitigen Abhängigkeiten ist es für die Bewältigung eines Vorfalls entscheidend, dass jene Stelle, welche wichtige Entscheide trifft, möglichst rasch und möglichst umfassend über alle relevanten Informationen verfügt.

Diese verschiedenen Zwecke schliessen sich nicht zwingendermassen gegenseitig aus. Es ist für die Ausgestaltung von Meldepflichten aber wichtig, klar zu definieren, welcher Hauptzweck verfolgt werden soll. Geht es beispielsweise um die Aufsichtspflicht des Staates, werden Meldepflichten

gegenüber Regulationsbehörden definiert, hingegen bieten sich für den Zweck der Erstellung der Bedrohungslage, der Frühwarnung oder der koordinierten Reaktion eher Modelle an, welche eine zentrale Meldestelle vorsehen. Auch für den Ablauf der Meldeerstattung ist der Zweck von ausschlaggebender Bedeutung. Geht es um die Frühwarnung und um die Koordination bei Vorfällen, muss die Meldung beispielsweise möglichst rasch erfolgen, während der Zeitfaktor für die Beurteilung der Bedrohungslage nicht in gleichem Masse ausschlaggebend ist. Bei jeder Diskussion um eine Einführung von Meldepflichten muss deshalb klar definiert werden, welchem Zweck die Meldepflicht in erster Linie dienen soll und welche weiteren Effekte davon erwartet werden.

2.2 Umfang der Meldepflichten

Der Umfang von Meldepflichten ist ebenfalls eine zentrale Frage, welche es bei der Erwägung, ob Meldepflichten einzuführen sind, vorgängig zu klären ist. Beim Umfang geht es um den Adressatenkreis der Meldepflicht (wer hat zu melden) ebenso wie um die Inhalte (was ist zu melden). Hinsichtlich des Adressatenkreises hat sich in vielen Ländern die Praxis durchgesetzt, dass Meldepflichten für Betreiber kritischer Infrastrukturen gelten sollen. Die Formulierung in der NIS-Richtlinie, welche Meldepflichten für «Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste» verlangt, es aber den Mitgliedsstaaten überlässt zu bestimmen, welche Dienste unter diese Definition fallen, zeigt aber, dass die Meinungen, wer einer Meldepflicht unterstellt werden sollte, weit auseinandergehen können.
Noch schwieriger zu beurteilen ist die Frage, welche Ereignisse konkret als Sicherheitsvorfall bezeichnet werden sollen und ab wann ein Vorfall meldepflichtig ist. Während hier einige Modelle Schwellenwerte definieren, verzichten andere Modelle bewusst auf die Festlegung solcher Grenzen, wodurch die Ausgestaltung der Meldepflicht flexibler, aber zugleich auch unschärfer wird. Besonders in Bezug auf Meldepflichten zu Cybervorfällen hat sich die Frage, welche Vorfälle zu melden sind, als äusserst schwierig zu beantworten erwiesen. Im sich rasch entwickelnden Umfeld von Cyberrisiken ist es in der grossen Menge an Vorfällen schwierig abzuschätzen, welche Informationen dringend erfasst werden müssen.

2.3 Definition der Meldestelle(n) und ihren Aufgaben

Es ist aber nicht nur wichtig, wer was zu melden hat, es muss auch festgelegt werden, an wen die Meldung zu erfolgen hat. Wie erwähnt ist es je nach Zweck der Meldepflicht sinnvoller, die Meldestelle sektoriell auszugestalten oder eine nationale zentrale Meldestelle einzurichten. In dieser Frage besteht ein gewisser Spielraum, da diverse Mischformen zwischen zentralen und dezentralen Meldestellen möglich sind.
Es braucht aber sorgfältige Abklärungen darüber, welche Stellen am besten als Meldestellen geeignet sind, da diese Frage direkt mit der Frage nach dem Zweck der Meldepflicht verbunden ist. Wenn Unternehmen verpflichtet werden, den Behörden Vorfälle zu melden, stehen diese umgekehrt in der Pflicht, die erhaltenen Informationen so zu verarbeiten, dass wiederum ein Mehrwert für die Gesellschaft entsteht. Es muss festgelegt werden, welche Aufgaben die Meldestelle übernimmt, wie sie die erhaltenen Informationen bearbeitet und mit wem sie die Informationen in welcher Form teilt. Zudem werden je nach Art der Meldestelle unterschiedlich hohe Mehraufwände für die Meldenden generiert. Für die Akzeptanz von Meldepflichten ist es wichtig, den bürokratischen Aufwand möglichst gering zu halten. Vor allem gilt es zu vermeiden, dass Betroffene den gleichen Vorfall an mehrere Stellen melden müssen.

2.4 Prozedurale Ausgestaltung der Meldepflicht

Neben den Fragen nach dem Zweck der Meldepflichten und den geeigneten Meldestellen gilt es ebenfalls zu definieren, welche Vorgaben zum Meldeprozess gemacht werden. Konkret muss festgelegt werden, in welchem Zeitraum die Betroffenen die Meldepflicht zu erfüllen haben, ob anonyme Meldungen möglich sind (und falls ja, wie sichergestellt werden kann, dass nachvollziehbar bleibt, ob die Meldepflicht erfüllt wurde) und welche Sanktionen im Falle eines Nichtbefolgens der Meldepflicht vorzusehen sind.
All diese Elemente sind wiederum direkt mit dem Zweck der Meldepflicht verknüpft, dürften aber darüber hinaus einen grossen Einfluss auf die Akzeptanz von Meldepflichten haben. Die im Rahmen der Studie «Prüfung einer Meldepflicht bei Sicherheitsvorfällen» durchgeführten Interviews mit Vertretungen der kritischen Sektoren haben deutlich gezeigt, dass es wichtig ist, die Betroffenen bei der prozeduralen Ausgestaltung von Meldepflichten einzubeziehen, damit eine für alle Involvierten tragbare Lösung gefunden werden kann.

3 Bestehende Meldepflichten in der Schweiz

Bevor neue Modelle für Meldepflichten bei Sicherheitsvorfällen für die Schweiz entwickelt werden, ist es wichtig, die bereits heute bestehenden Meldepflichten zu kennen. Eine Analyse der bestehenden Rechtsgrundlagen zeigt, dass in den kritischen Sektoren bereits verschieden Meldepflichten für Sicherheitsvorfälle bestehen.
Die Autoren der Studie «Prüfung von Meldepflichten bei Sicherheitsvorfällen» haben für alle neun kritischen Sektoren der Schweiz (Energie, Entsorgung, Finanzen, Gesundheit, Information und Kommunikation, Nahrung, öffentliche Sicherheit, Verkehr und Behörden) in den entsprechenden sektoriellen Gesetzen Meldepflichten für die Betreiber identifiziert. Die rechtlichen Grundlagen sind in der erwähnten Studie aufgeführt. In diesem Kapitel sollen kurz die für die Frage nach einer Einführung einer generellen Meldepflicht relevantesten Erkenntnisse zusammengefasst werden.

3.1 Grundlagen und Umfang bestehender Meldepflichten

Die Meldepflichten sind je nach Sektor unterschiedlich ausgestaltet. In stark regulierten Märkten, wie beispielsweise der Kernenergie, sind die Meldepflichten differenziert festgehalten und es werden Sanktionen definiert. Ebenfalls bereits recht weit ausdifferenzierte Meldepflichten bestehen im stark international regulierten Sektor der Zivilluftfahrt. In anderen Sektoren beschränken sich die Meldepflichten auf «ausserordentliche Ereignisse» (Art. 8 Abs. 3 StromVG), «Vorkommnisse, die für die Aufsicht von wesentlicher Bedeutung sind» (Art. 29 Abs. 2 FINMAG), «Störungen im Betrieb der Netze, welche eine relevante Anzahl Kundinnen und Kunden betreffen» (Art. 96 Abs. 2 FDV). Auf Schwellenwerte, ab welcher eine Meldung verpflichtend ist, und Sanktionen im Unterlassungsfall werden bei diesen meist verzichtet.
Da in vielen Sektoren die Meldepflichten nicht differenziert beschrieben werden, werden auch keine spezifischen Meldepflichten bei Cybervorfällen erwähnt. Die generell formulierten Meldepflichten schliessen Cybervorfälle dann ein, wenn diese zu grossen Störungen führen. Alle Meldungen von abgewehrten Angriffen oder Vorfällen ohne schwerwiegenden Konsequenzen im Sinne eines aktiven Informationsaustausches, erfolgen auf freiwilliger Basis, über die Melde- und Analysestelle Informationssicherung (MELANI) des Bundes oder über sektorielle Computer Emergency Response Teams (CERTs). Gesetzlich sind die Betreiber kritischer Infrastrukturen nicht verpflichtet, an diesem Informationsaustausch teilzunehmen.
Ergänzend zu den Meldepflichten bei Sicherheitsvorfällen sehen viele Gesetze grundsätzliche Auskunftspflichten der Unternehmen gegenüber dem Regulator vor. Die regulierten Unternehmen sind

verpflichtet, Anfragen des Regulators nachzukommen. Diese Auskunftspflichten können von den Regulatoren ebenfalls genutzt werden, um Informationen zu Vorfällen zu erhalten, welche keine oder keine schwerwiegenden Konsequenzen gehabt haben.
Generell lässt sich in Bezug auf die rechtlichen Grundlagen und den Umfang bestehender Meldepflichten festhalten, dass in vielen Sektoren (aber nicht in allen Teilsektoren) die Forderung nach einer Meldepflicht bei schwerwiegenden Sicherheitsvorfällen grundsätzlich bereits erfüllt ist. Die Pflichten sind aber üblicherweise sehr generell formuliert, meist nicht mit Sanktionen verbunden und beschränken sich auf eine Meldung gegenüber einer für den Sektor zuständigen Meldestelle.

3.2 Bestehende Meldestellen

Die Meldepflichten existieren in verschiedenen sektoriellen Gesetzen, womit unterschiedliche Meldestellen bezeichnet sind. Typischerweise handelt es sich dabei um die Regulierungs- und Aufsichtsbehörden der Teilsektoren. In einzelnen Teilsektoren, wie beispielsweise in den Teilsektoren «Nahrung» und «Entsorgung» sind keine nationalen, sondern kantonale Meldestellen definiert. Für die Meldung von Cybervorfällen steht mit der Melde- und Analysestelle Informationssicherung seit 2004 eine zentrale Stelle zur Verfügung. In verschiedenen Sektoren (z.B. Finanzen, Forschung, Energie) bestehen zudem sektorielle Cybermeldestellen (Sektoren-CERTs). Sowohl die Meldungen an MELANI als auch jene an die Sektoren-CERTs erfolgen freiwillig.
Die grundsätzliche Zuständigkeit der Regulierungsbehörden erleichtert den Unternehmen die Meldung von Vorfällen, weil ihnen durch den regelmässigen Austausch mit den für sie zuständigen Behörden üblicherweise klar ist, an wen sie sich zu wenden haben. Umgekehrt können die Regulierungsbehörden dank ihrem Fachwissen die Relevanz eines Vorfalls für ihren Sektor gut einschätzen und falls nötig entsprechende Massnahmen ergreifen.
Im Rahmen der Studie «Prüfung einer Meldepflicht bei Sicherheitsvorfällen» wurde aus den Interviews mit Fachpersonen aus der Wirtschaft aber auch verdeutlicht, dass bei einer Ausweitung der bestehenden Meldepflicht über besonders gravierende Vorfälle hinaus, Skepsis gegenüber einem Modell besteht, welches Meldungen an die Regulierungsbehörde vorsieht. Dies gilt vor allem dann, wenn von Meldepflichten bei Cybervorfällen gesprochen wird. Erstens gehen bei Meldepflichten gegenüber der Regulierungsbehörde der Aspekt der sektorübergreifenden Information verloren, welcher gerade bei Cybervorfällen besonders wichtig ist. Zweitens wird erwähnt, dass Meldungen an die Regulierungsbehörde aus Sicht der Unternehmen heikel sind, weil sie potentiell zu Nachprüfungen führen können. Dies kann dazu führen, dass Unternehmen Meldungen nicht, unvollständig oder erst nach vertieften rechtlichen Abklärungen absetzen, was in Bezug auf Cybervorfälle schwerwiegende Nachteile mit sich bringen würde. Drittens verfügen die Regulierungsbehörden zwar für ihren Sektor über das nötige Fachwissen, dieses fehlt ihnen typischerweise aber für die spezifischen Fragen der Cybersicherheit.
Die bestehenden Meldestellen sind also nach den heute in den Gesetzen festgehaltenen Meldepflichten ausgerichtet. Sie sind geeignet, um Meldungen von schwerwiegenden Sicherheitsvorfällen entgegenzunehmen. Bei einer Ausweitung der Meldepflichten – insbesondere bei einer Meldepflicht für Cybervorfälle – ist zu prüfen, ob und wie das heute bestehende System mit einer Vielzahl von sektorspezifischen Meldestellen anzupassen ist.

4 Meldepflichten im Ausland

Wie in der Schweiz sind auch in vergleichbaren Ländern Meldepflichten für Unternehmen gegenüber Behörden nicht etwas grundsätzlich Neues und bestehen in vielen Sektoren bereits seit Jahren. Als Reaktion auf die digitale Vernetzung und auf die zunehmende Bedrohung durch Cyberrisiken sind die Meldepflichten in den letzten Jahren aber teilweise beträchtlich erweitert und ausgebaut worden. Treiber für diese Entwicklung waren zu einem grossen Teil die Beschlüsse der EU zur Einführung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) 2016. Seit diesem Beschluss ist grundsätzlich klar, dass alle EU-Mitgliedstaaten Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste einführen müssen.
Für den Entscheid über die Einführung von Meldepflichten und deren allfällige Ausgestaltung in der Schweiz, bieten die in anderen Ländern gewählten Lösungen interessantes Anschauungsmaterial. In der Studie «Prüfung einer Meldepflicht bei Sicherheitsvorfällen» wurden die Meldepflichten in Deutschland, Österreich, Frankreich, Norwegen und Israel analysiert. Die detaillierten Resultate der Analyse sind in der Studie aufgeführt. In Bezug auf die in Kapitel 2 beschriebenen Grundsatzfragen lassen sich folgende Erkenntnisse festhalten:

- **Zweck der Meldepflichten:** bei in den letzten Jahren eingeführten Meldepflichten (welche vor allem Cybervorfälle betreffen), steht üblicherweise der Zweck der Frühwarnung durch Informationsaustausch im Vordergrund. Diesen zu fördern ist explizites Anliegen der NIS-Richtlinie, welche bei vielen EU-Staaten zur Einführung von Meldepflichten geführt hat. Auch in nicht EU-Staaten wie Israel und Norwegen steht dieser Aspekt, zusammen mit der Koordination bei Vorfällen, im Vordergrund. Meldepflichten werden in dem Sinne als Verpflichtung zur Zusammenarbeit und gegenseitigen Unterstützung über den Informationsaustausch verstanden. Damit unterscheiden sich die neu eingeführten Meldepflichten von den traditionell bestehenden Meldepflichten, bei welchem es vor allem darum geht, die Aufsichtsfunktion der Regulatoren eines Sektors zu stärken.

- **Umfang der Meldepflichten:** bezüglich Adressaten stehen bei allen untersuchten Staaten die kritischen Infrastrukturen im Vordergrund. Die NIS-Richtlinie erweitert den Adressatenkreis mit «Anbietern digitaler Dienste». Darunter fallen beispielsweise in Deutschland Anbieter von Online-Suchmaschinen, Cloud-Computing-Dienste oder Online-Marktplätze.[7] Es scheint insgesamt für viele Länder eine Herausforderung zu sein, den Adressatenkreis der Meldepflichten präzise einzugrenzen.
  Meldepflichtig sind in allen untersuchten Ländern schwerwiegende Vorfälle. Die Schwellenwerte dafür werden in allen Ländern sektorspezifisch festgelegt. Unterschiede gibt es bei der Behandlung von Cybervorfällen. In Deutschland und Österreich werden Cybervorfälle nicht separat gelistet und unter bestehenden Meldepflichten der jeweiligen Teilsektoren subsumiert. In Frankreich und Israel werden Cybervorfälle separat gelistet. In Norwegen werden Cybervorschriften zurzeit implementiert.

- **Meldestellen:** keines der untersuchten Länder hat eine einzige Meldestelle für alle sicherheitsrelevanten Meldungen eingerichtet. Gemeldet wird jeweils an die für den Sektor zuständige Behörde. In Bezug auf Meldepflichten bei Cybervorfällen haben die meisten Staaten aber zentralere Lösungen gewählt. Entweder werden Cybervorfälle direkt einer zuständigen Stelle gemeldet (z.B. in Deutschland das Bundesamt für Sicherheit in der Informationstechnik, BSI oder in Frankreich an die Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI) oder gelangen über sektorspezifische Computer Emergency Response Teams (CERTs) an eine zentrale Stelle.

[7] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/DigitaleDienste/digitaledienste_node.html

- **Prozedurale Ausgestaltung:** die Ausgestaltung der Meldepflichten unterscheiden sich je nach Land und sogar innerhalb des gleichen Landes je nach Sektor stark. Es gibt in keinem Land generell gültige zeitliche Vorgaben. Diese werden pro Sektor festgelegt.
  Bezüglich Sanktionen spielt für EU-Mitgliedstaaten die Datenschutz-Grundverordnung eine wichtige Rolle, da diese bei nicht gemeldeten datenschutzrelevanten Vorfällen vergleichsweise hohe Bussen vorsieht. Deutschland, Österreich und Frankreich haben für die Nichtmeldung von relevanten Sicherheitsvorfällen bei kritischen Infrastrukturen zusätzlich Sanktionen definiert. In Norwegen und Israel sind aktuell keine rechtlich definierten Sanktionen für unterlassene Meldungen definiert.
  Anonymisierte Meldungen sind für kritische Infrastrukturen nicht in allen Ländern möglich. In Frankreich und Österreich ist dies ganz ausgeschlossen, in Deutschland sind anonyme Meldungen nur möglich, wenn sie keine schwerwiegenden Folgen hatten. In Norwegen ist es grundsätzlich möglich anonym zu melden, dies gilt jedoch nicht für den Finanzsektor. In Israel hingegen sind anonyme Meldungen akzeptiert.

Der Vergleich der Umsetzung von Meldepflichten in anderen Staaten zeigt vor allem die Wesentlichkeit, dass die bestehenden Systeme von Meldepflichten gegenüber den Regulatoren mit den neu dazukommenden Meldepflichten für Cybervorfälle in Einklang zu bringen sind. Dies ist nicht einfach, da die bisherigen Regulierungen sich stark auf den Sektor beziehen, während die Einführung von Meldepflichten für Cybervorfälle möglichst sektorübergreifend ausgestaltet werden sollten, um die Frühwarnung effektiv zu stärken. Die verschiedenen Varianten der Meldepflichten in den untersuchten Ländern zeigen aber auch, dass es gut möglich ist, Meldepflichten so anzupassen, dass sie auf die Bedürfnisse und die bestehenden Strukturen passen.

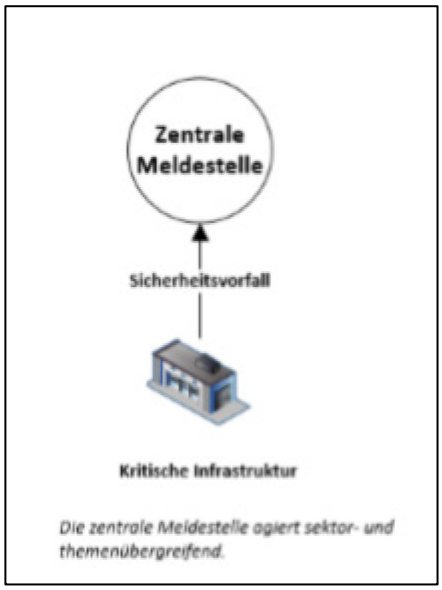
5 Varianten für Meldepflichten in der Schweiz

Aufgrund der Analysen zu den bestehenden Meldepflichten, den Gesprächen mit Fachpersonen aus Wirtschaft und Behörden und den internationalen Beispielen identifizieren die Autorinnen und Autoren der Studie «Prüfung einer Meldepflicht» vier Varianten für die Frage, ob Meldepflichten in der Schweiz eingeführt werden sollen:

1. **Einführung einer zentralen Meldestelle für sicherheitsrelevante Vorfälle**
2. **Auf- und Ausbau der bisherigen dezentralen Meldestellen in den Sektoren**
3. **Dezentrale Meldestellen mit zentraler Meldestelle für Cybervorfälle**
4. **Keine Meldepflicht**

In diesem Kapitel sollen die vier Grundmodelle aus der Studie kurz beschrieben werden, wobei vor allem die Konsequenzen der jeweiligen Modelle auf die in Kapitel 2 beschriebenen Grundfragen (Zweck der Meldepflicht, Umfang der Meldepflicht, Meldestellen und prozedurale Ausgestaltung) beleuchtet werden.

5.1 Variante 1: Zentrale Meldestelle

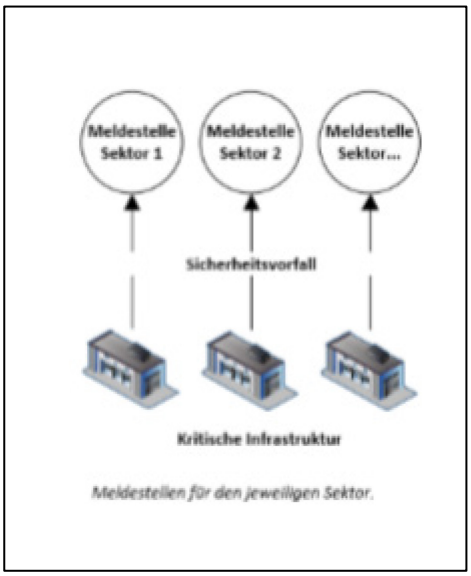


Beschreibung: Es wird eine zentrale, sektorübergreifende Meldestelle für alle Sicherheitsvorfälle von kritischen Infrastrukturen geschaffen.
Vorteile: Alle Informationen werden zentral erfasst, was die sektorübergreifende Koordination erleichtert. Es besteht grosse Klarheit, wem gemeldet werden muss und die Abläufe sind für alle Sektoren einheitlich.
Nachteile: Eine starke Zentralisierung würde zu grossen Anpassungen am bestehenden System führen, sowie zu schwierigen Zuständigkeitsfragen hinsichtlich des Verhältnisses zwischen der Meldestelle und den Regulatoren führen, und eine zentrale Stelle könnte nicht (oder nur schwer) bei der Ausgestaltung der Meldepflicht auf die Eigenheiten der einzelnen Sektoren eingehen.

Einschätzung des Modells hinsichtlich der Grundfragen:

- **Stärken / Schwächen mit Bezug auf die Zwecke von Meldepflichten:** Eine zentrale Lösung hat Vorteile für die Erstellung des Bedrohungslagebilds, bei der Frühwarnung und bei der Koordination der Reaktion, da alle Informationen an einer Stelle zusammenfliessen. Für die Stärkung der Aufsichtspflicht der Regulatoren ist das Modell aber wenig geeignet, da diese die Informationen nicht mehr oder nur noch indirekt über die zentrale Meldestelle erhalten. Damit dürfte auch die Stärkung der Prävention bei den Unternehmen nicht in gleichem Ausmass erfolgen.
- **Umfang der Meldepflichten:** Die Adressatengruppe müsste breit definiert sein, da bei einer zentralen Lösung eine weiter ausdifferenzierte Auswahl der verpflichteten Unternehmen schwierig umsetzbar ist. Eine grosse Herausforderung des Modells besteht auch bei der Definition von Schwellenwerten für die Meldepflicht, da je nach Sektor unterschiedliche Werte sinnvoll sind. Solche sektoriell angepassten Lösungen sind in einem zentralen Modell schwieriger umsetzbar.
- **Auswirkung auf bestehende Meldestellen:** Das Modell würde das bisher bestehende System komplett verändern und wäre mit einem grossen initialen Aufwand verbunden. Diverse rechtliche Zuständigkeiten müssten neu geregelt und das Verhältnis zwischen der zentralen Meldestelle und den sektorspezifischen Regulatoren müsste definiert werden.
- **Prozedurale Ausgestaltung:** Im Modell schwierig umsetzbar sind sinnvolle zeitliche Vorgaben, da die Dringlichkeit einer Meldung nicht in allen Sektoren gleich hoch ist. Das Modell lässt hingegen sowohl anonyme wie auch nicht-anonyme Meldeverfahren zu. Bei der Sanktionierung im Unterlassungsfall stellt sich wiederum das Problem der rechtlichen Zuständigkeiten, da eine zentrale Meldestelle nicht beim jeweiligen Regulator angesiedelt wäre.

5.2 Variante 2: Dezentrale Meldestellen

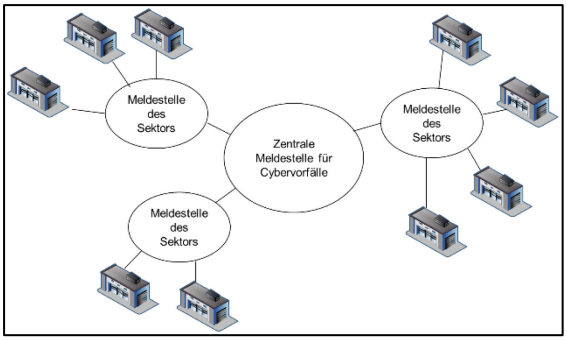


Beschreibung: Die bestehenden dezentral aufgestellten Meldestellen in den verschiedenen Sektoren werden gestärkt und die Meldepflichten ihnen gegenüber ausgebaut (insbesondere in Bezug auf Cybervorfälle). In Sektoren, wo keine Meldestellen vorhanden sind, werden solche aufgebaut.
Vorteile: Das Modell wäre vergleichsweise rasch umsetzbar, da es bestehende Strukturen ausweitet. Auch rechtliche Grundlagen für Meldepflichten bestehen bereits in verschiedenen Sektoren. Regulatoren haben gute Kenntnisse ihres Sektors und könnten die Meldepflicht auf die Bedürfnisse ihres Sektors anpassen.
Nachteile: Die übergreifende Koordination ist nicht gewährleistet. Die bestehenden Meldestellen sind nicht auf die Meldung von Cybervorfällen ausgerichtet.

Einschätzung des Modells hinsichtlich der Grundfragen:

- **Stärken / Schwächen mit Bezug auf die Zwecke von Meldepflichten:** Die Rolle der Regulatoren wird durch einen dezentralen Ausbau der Meldepflichten gestärkt. Sektorübergreifende Zwecke, wie die Verbesserung der Frühwarnung, die Koordination der Reaktion und die Erstellung der Bedrohungslage können nur erfüllt werden, wenn zwischen den sektoriellen Regulatoren ein gut funktionierender Informationsaustausch stattfindet. Dies ist insbesondere bei Cybervorfällen eine grosse Herausforderung.
- **Umfang der Meldepflichten:** Die Sektoren bestimmen selber, welche Unternehmen meldepflichtig sind und welche Vorfälle gemeldet werden müssen. So kann der für den Sektor optimale Umfang der Meldepflichten bestimmt werden.
- **Auswirkung auf bestehende Meldestellen:** Das bestehende System wird ausgebaut. Dazu werden die rechtlichen Grundlagen der existierenden Meldestellen wo nötig erweitert. Zu prüfen wäre, wie MELANI als Meldestelle für Cybervorfälle in das System integriert wird. Ebenfalls müsste geklärt werden, wie den Bedenken der Unternehmen gegen eine Ausweitung von Meldepflichten gegenüber den Meldestellen der Regulatoren entgegengetreten werden kann.
- **Prozedurale Ausgestaltung:** Zeitliche Vorgaben für die Meldepflicht werden vom Regulator für jeden Sektor separat bestimmt. Dieser definiert auch allfällige Sanktionen. Die Möglichkeit, anonyme Meldungen zu machen, dürften in den meisten Sektoren beschränkt sein, da in der Praxis selbst bei anonymen Meldungen dem Regulator rasch ersichtlich sein dürfte, welches Unternehmen die Meldung abgesetzt hat.

5.3 Variante 3: Ergänzung der dezentralen Meldestellen mit einer zentralen Meldestelle für Cybervorfälle



Beschreibung:
Dieses Modell sieht eine gemischte Form von Meldestellen vor. Primärer Ansprechpartner für Sicherheitsvorfälle ist die sektorspezifische Meldestelle. Für die Aufarbeitung aller Cybervorfälle wird eine übergreifende, zentrale Meldestelle festgelegt. Dabei ist noch zu klären, ob die Meldung direkt an die zentrale Meldestelle für Cybervorfälle, über eine sektorspezifische Cybermeldestelle (Sektor-CERT) erfolgen soll.
Vorteile: Das Modell kombiniert bestehende Lösungen in den Sektoren mit einer Cybermeldestelle. Physische Sicherheitsvorfälle, welche vor allem für den Sektor und den Regulator von Bedeutung sind, bleiben im Sektor, Informationen zu Cybervorfälle werden übergreifend geteilt. Das Modell ist flexibel ausgestaltbar.
Nachteile: Es verbleiben viele verschiedene Meldestellen. Die Aufgaben und Kommunikationswege zwischen diesen Stellen müssen sorgfältig definiert werden. Bei mehreren Meldestellen ist es für Unternehmen nicht immer klar, an wen sie sich wenden sollen, insbesondere, weil die Unterscheidung zwischen physischen Vorfällen und Cybervorfällen nicht in jedem Fall einfach zu machen ist.

Einschätzung des Modells hinsichtlich der Grundfragen:

- **Stärken / Schwächen mit Bezug auf die Zwecke von Meldepflichten:** Das Modell bleibt sektoriell verankert, wodurch die Aufsicht bei den Regulatoren bleibt. Gleichzeitig ermöglicht es im Cyberbereich sektorübergreifende Frühwarnsysteme, eine Stärkung der Koordination bei Vorfällen und eine umfassende Darstellung der Bedrohungslage. Wichtig ist dabei aber, dass die Aufgaben und Kommunikationswege zwischen den Meldestellen klar definiert sind und allen Betreibern von kritischen Infrastrukturen klar aufgezeigt wird, welche Vorfälle wo zu melden sind.
- **Umfang der Meldepflichten:** Das Modell sieht vor, dass grundsätzlich der Entscheid, wer von der Meldepflicht betroffen ist, bei den Regulatoren der verschiedenen Sektoren bleibt. Die zentrale Meldestelle für Cybervorfälle macht umgekehrt Vorgaben, welche Cybervorfälle ihr zu melden sind.
- **Auswirkung auf bestehende Meldestellen:** Die bestehenden Meldestellen werden beibehalten. Meldungen von Cybervorfällen direkt an MELANI oder an ein Sektoren-CERT sind nicht mehr freiwillig, sondern fallen unter die Meldepflicht. Diese Meldestellen für Cybervorfälle würden dadurch gestärkt, das Verhältnis zu den sektoriellen Meldestellen muss aber genau definiert werden.
- **Prozedurale Ausgestaltung:** Bei den Verfahren ist zu unterscheiden zwischen physischen Vorfällen und Cybervorfällen, wobei diese Unterscheidung nicht in jedem Fall einfach vorzunehmen ist. Von Vorteil ist, dass bei einer Unterscheidung zwischen physischen Vorfällen und Cybervorfällen jeweils unterschiedliche zeitliche Vorgaben gemacht und verschiedene Sanktionen festgelegt werden können. Es ist auch möglich, dass Cybervorfälle anonymisiert der zentralen Meldestelle gemeldet werden.

5.4 Variante 4: Keine Ausweitung bestehender Meldepflichten

Beschreibung: Am bestehenden System wird nichts geändert und die Meldepflichten nicht ausgeweitet. Auf eine Meldepflicht für Cybervorfälle wird verzichtet.
Vorteile: Der bestehende freiwillige Austausch von Vorfällen, wie er mit MELANI in Bezug auf Cybervorfälle besteht, hat im Vergleich zur Meldepflicht den Vorteil, dass Unternehmen unbürokratisch und ohne vorherige rechtliche Abklärungen Vorfälle melden können. Der freiwillige Informationsaustausch stösst auf eine breite Akzeptanz bei den Unternehmen. Dies erhöht die Chancen, dass auch Informationen geteilt werden, welche nicht unter eine Meldepflicht fallen würden.
Nachteile: Eine umfassende Übersicht, welche auch statistische Analysen zulässt, kann nicht erreicht werden. Die Schweiz ist bei einem Verzicht auf eine Meldepflicht auch nicht kompatibel mit den durch die NIS-Richtlinie erlassenen Vorgaben, welche für EU-Mitgliedstaaten gelten.

6 Ausblick und weiteres Vorgehen

Die vorgestellten Grundmodelle werden mit Vertretungen der Wirtschaft, der Kantone, den zuständigen Regulatoren und der Politik weiter vertieft. Dazu gehört es auch, im Detail abzuklären, welche gesetzgeberischen Schritte für welches Modell nötig sind. Die Diskussionen werden im ersten Halbjahr 2020 unter der Leitung des Delegierten des Bundes für Cybersicherheit geführt.
Ziel der Diskussionen ist es, sich darauf zu einigen, welches Modell von Meldepflichten für die Schweiz umgesetzt werden soll, so dass ab Sommer 2020 mit der Erarbeitung der entsprechenden gesetzlichen Grundlagen begonnen werden kann.