VUD | Verein Unternehmens-Datenschutz

Sehr geehrter Herr Bundesrat Maurer,
Sehr geehrte Damen und Herren,

Bezugnehmend auf die Medienmitteilung vom 12. Januar 2022 danken wir Ihnen für die Gelegenheit, uns zur Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen zu äussern. Wir freuen uns, Ihnen nachfolgend die Stellungnahme des Vereins Unternehmens-Datenschutz (VUD) zu unterbreiten.

Zum Verein Unternehmens-Datenschutz (VUD)

Im Verein Unternehmens-Datenschutz (VUD) schliessen sich juristische Personen, andere Organisationen und natürliche Personen zusammen, die sich mit der Umsetzung des Datenschutzes in ihrer eigenen betrieblichen Praxis befassen. Der VUD fördert den fachlichen Austausch unter seinen aktuell ca. 80 Mitgliedern und ist der selbständigen wie auch unabhängigen Meinungsbildung im Bereich Datenschutz verpflichtet. Zu seinen statutarischen Zwecken gehört auch, sich zu Entwicklungen des Datenschutzes öffentlich vernehmen zu lassen.

Stellungnahme

Allgemeine Bemerkungen

Die im Informationssicherheitsgesetz vom 18. Dezember 2020 (ISG) vorgesehenen Änderungen werfen aus Sicht des VUD eine Vielzahl von Fragen auf.

Besonders kritisch beurteilt der VUD die gesetzgeberische Lösung, den Kreis der von der Meldepflicht erfassten Ereignisse (Art. 5 Bst. d-e ISG) und Unternehmen bzw. Organisationen (Art. 74b ISG) extrem weit zu fassen, um ihn dann über zwei Ausnahmeregelungen (Art. 74c und 74d ISG) wieder einzuschränken. Diese Lösung führt zu Rechtsunsicherheit und unnötigem Aufwand bei den betroffenen Unternehmen und Organisationen. Der VUD schlägt deshalb vor, die Meldepflicht von vornherein auf Cyberangriffe zu begrenzen, die kritische Infrastrukturen im Sinne von Art. 5 Bst. c ISG erheblich gefährden und deshalb von nationalem Interesse sind.

Darüber hinaus empfiehlt der VUD, unklare bzw. widersprüchliche Bestimmungen (insbesondere Art. 74c, 74d und 74g ISG) zu konkretisieren bzw. zu präzisieren, um Rechtsunsicherheiten auf ein Minimum zu reduzieren. Eine deutliche Verbesserung der relevanten Bestimmungen erscheint auch deshalb zwingend, weil die Verletzung von Melde- und Auskunftspflichten strafbar ist (Art. 74h i.V.m. Art. 74i ISG).

Schliesslich ist der VUD der Ansicht, dass die Bekanntgabe von Informationen durch das NCSC (Art. 73c und 76) ausschliesslich auf anonymer Basis erfolgen sollte. Die von den meldepflichtigen Unternehmen und Organisationen an das NCSC gelieferten Informationen werden in der Praxis hochsensibel sein und bedürfen deshalb eines besonderen Schutzes. Die Bekanntgabe dieser Informationen ohne Anonymisierung und Kontrolle durch die betroffenen Unternehmen und Organisationen kann diesen nicht zugemutet werden.

Der VUD ist überzeugt, dass die zielgerichtete, klare und effiziente Regelung der Meldepflicht im Sinne der nachfolgenden Bemerkungen sich auf die Wirksamkeit und Akzeptanz der Meldepflicht sehr positiv auswirken wird.

Bemerkungen zu einzelnen Bestimmungen

Bemerkung zu Art. 5 Bst. d-e ISG

Der Begriff des Cybervorfalls ist zu weit gefasst. In der täglichen Praxis können mit dem Internet verbundene Informatikmittel einer extrem grossen Zahl von (automatisierten) Angriffen ausgesetzt sein. Jeder dieser Angriffe kann – zumindest theoretisch – eine Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit zur Folge haben und wäre gemäss Art. 74a ISG dem nationalen Zentrum für Cybersicherheit (NCSC) zu melden, sofern er absichtlich ausgelöst wurde. Indem die blosse Möglichkeit einer Beeinträchtigung für die Begründung einer Meldepflicht im Einzelfall ausreicht, müssten dem NCSC bei konsequenter Auslegung der gesetzlichen Bestimmungen eine extrem grosse Zahl von Cyberangriffen gemeldet werden, selbst wenn diese Angriffe aufgrund von bestehenden Sicherheitsmassnahmen keine unerwünschte Wirkung erzielen. Diese Konsequenz läuft den in Art. 1 Abs. 1 ISG formulierten Zielen zuwider, weil das NCSC mit unnötigen Meldungen überflutet würde. Zudem wäre der mit den Meldungen verbundene Aufwand für die meldepflichtigen Betreiberinnen unverhältnismässig. Jede Meldung zieht einen erheblichen Aufwand nach sich, indem die geforderten Informationen zusammengetragen und in eine kommunizierbare Form gebracht werden müssen. Je mehr Meldungen abzusetzen sind, desto höher ist der Aufwand.

Der VUD schlägt deshalb vor, die Begriffe in Art. 5 Bst. d-e ISG mit Blick auf das Risiko bzw. den Erfolg von Cybervorfällen und -angriffen zu definieren. Von nationalem Interesse sind jene Ereignisse, welche den Betrieb von kritischen Infrastrukturen ernsthaft gefährden. Nur diese sollten meldepflichtig sein. Dadurch wird auch sichergestellt, dass das NCSC seine Ressourcen dort einsetzen kann, wo sie dem Sinn und Zweck des Gesetzes gerecht werden.

Eine Einschränkung von Art. 5 Bst. d-e ISG ist auch dadurch gerechtfertigt, dass das NCSC vor allem aus statistischen Gründen an Informationen über Cybervorfälle interessiert ist. Art. 74 Abs. 3 ISG macht nämlich deutlich, dass das NCSC die betroffenen Unternehmen und Organisationen bei der Bewältigung von Vorfällen nur dann berät und unterstützt, wenn diese ein hohes Mass an Kritikalität aufweisen und eine rechtzeitige private Unterstützung nicht möglich ist. Durch diese weitgehenden Einschränkungen wird Art. 74 Abs. 3 ISG in der Praxis kaum je Anwendung finden.

Bemerkung zu Art. 73a ISG

Das NCSC kann gemäss Bst. b und c dieser Bestimmung vor Cyberrisiken und Schwachstellen von Informatikmitteln warnen und bestimmte Informationen veröffentlichen (siehe auch Art. 73b Abs. 2, erster Halbsatz). Hier ist zu beachten, dass durch die Veröffentlichung von Schwachstelleninformationen die Gefahr von Cyberangriffen auch erhöht werden kann, indem potenziellen Angreifer ebenfalls von einer Schwachstelle und deren Eigenheiten erfahren. Die Erfahrung zeigt, dass es in der Praxis mehrere Monate dauern kann, bis eine neu erkannte Schwachstelle durch die Betreiberinnen von betroffenen Informatikmitteln beseitigt wird. Bis dahin besteht ein erhöhtes Risiko von erfolgreichen Cyberangriffen. Aus unserer Sicht müssen sämtliche Informationen und Kommunikationsmassnahmen des NCSC deshalb unter dem gesetzlichen Vorbehalt stehen, dass Cyberangriffe dadurch nicht gefördert oder erleichtert werden.

Bemerkungen zu Art. 73b ISG

Das NCSC wird in Erfüllung seiner gesetzlichen Aufgaben eine Fülle von Informationen über die in der Schweiz betriebenen Informatikmittel und deren Schwachstellen erhalten. Diese Informationen stehen interessierten Parteien über das Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung vom 14. Dezember 2004 (BGÖ) zur Verfügung. Die ausgesprochen öffentlichkeitsfreundliche Anwen-

dung des BGÖ durch Verwaltungsbehörden und Bundesgericht führt dazu, dass gestützt auf ein Öffentlichkeitsgesuch selbst äusserst sensible Informationen über kritische Infrastrukturen und ihre Schwachstellen in die Öffentlichkeit oder sogar in die Hände von potenziellen Angreifern gelangen können. Auch kann eine Offenlegung von Cybervorfällen mit Beteiligung von privaten Unternehmen oder Organisationen deren Ruf nachhaltig schädigen. Die gesetzlichen Einschränkungen der Öffentlichkeit gemäss Art. 7 Abs. 1 BGÖ erweisen sich als kaum wirksam, weil sie in der behördlichen bzw. gerichtlichen Praxis überaus restriktiv ausgelegt werden und kaum je erfolgreich angerufen werden können – selbst Vertraulichkeitszusagen werden in der Praxis erfahrungsgemäss nicht respektiert. Diese Konsequenz widerspricht dem gesetzgeberischen Ziel, die Widerstandsfähigkeit der Schweiz gegenüber Cyberrisiken zu erhöhen (Art. 1 Abs. 1 ISG). Sie widerspricht auch den Interessen der Betreiberinnen sowie den nationalen Interessen. Die Angst vor einer nachträglichen Offenlegung wird dazu führen, dass Informationen dem NCSC im Zweifel nicht offengelegt werden. Der VUD schlägt deshalb vor, Informationen in Bezug auf einzelne kritische Infrastrukturen und deren Schwachstellen und Cybervorfälle, einschliesslich deren Meldungen, im ISG vom Anwendungsbereich des BGÖ ausdrücklich auszunehmen.

Bemerkungen zu Art. 73c ISG

Die Weiterleitung von Informationen zu Cybervorfällen an den NDB gemäss Art. 7c Abs. 1 ISG wirft rechtsstaatliche Bedenken auf. Mit der Weiterleitung an den NDB werden die Informationen potenziell zweckentfremdet. Während das NCSC einen klar definierten gesetzlichen Auftrag erfüllt, liegt es in der Natur der Sache, dass eine nachrichtendienstliche Verarbeitung der Informationen nicht transparent sein kann. Es besteht das Risiko, dass die vom NDB erhaltenen Informationen auf für Zwecke verwendet werden, die ausserhalb des ISG stehen. Wie die betreffenden Informationen vom NDB verarbeitet werden, wird für die betroffenen Unternehmen und Organisationen kaum je erkennbar bzw. kontrollierbar sein. Dies ist umso stossender, als die von den Unternehmen und Organisationen gelieferten Informationen regelmässig sehr sensitiv sein werden. Art. 7c Abs. 4 ISG bietet für die betroffenen Unternehmen und Organisationen in diesem Zusammenhang kaum Schutz. Die Weiterleitung von Informationen gemäss Art. 73c ISG darf daher nur anonymisiert erfolgen. Die Anonymisierung der Informationen vor Weiterleitung an den NBD behindert den Zweck der Weiterleitung (*"Beurteilung von Bedrohungslage oder für die nachrichtendienstliche Früherkennung zum Schutz von kritischen Infrastrukturen"*) nicht.

Die Einverständnispflicht gemäss Art. 73c ISG muss auf alle Mitarbeitenden und Organe eines meldenden Unternehmens bzw. einer meldenden Organisation ausgeweitet werden. In der Praxis werden bei einem Cybervorfall regelmässig eine Vielzahl von Mitarbeitenden und Organen beteiligt bzw. mitverantwortlich sein. Dies gilt sowohl im Vorfeld eines Cybervorfalls (z.B. Ursachen des Vorfalls) wie auch bei der Vorbereitung einer Meldung. Es ist unter diesen Umständen nicht einzusehen, weshalb nur jene Person in die Verwendung der Informationen im Strafverfahren einwilligen muss, welche die Informationen tatsächlich bekanntgegeben hat. Diese Lösung ist willkürlich und wird der Realität der Arbeitsteilung im Unternehmen nicht gerecht. Dies umso mehr, als diese Person, welche die Informationen bekannt gibt, diese vielleicht nur aufgrund einer bestimmten Funktion im Unternehmen bzw. in der Organisation bekanntgibt. Der strafrechtlich fundamentale Grundsatz, wonach sich niemand selbst bezichtigen muss, muss zwingend auf alle Personen in einem Unternehmen oder einer Organisation ausgeweitet werden, welche direkt oder indirekt am Cybervorfall und dessen Meldung beteiligt bzw. dafür verantwortlich sind. Nur auf dieser Grundlage lässt sich eine gesetzliche Meldepflicht mit potenziell strafrechtlichen Konsequenzen rechtsstaatlich rechtfertigen.

Bemerkungen zu Art. 74 ISG

Art. 74 Abs. 4 ISG sieht vor, dass das NCSC auf Informationen der betroffenen Betreiberin zugreifen kann. Diese Regelung ist zu unbestimmt. Insbesondere der Begriff des Zugriffs ist sowohl in technischer wie auch in rechtlicher Hinsicht unklar. Technisch wird in der Informatik unter *"Zugriff"* normalerweise die Möglichkeit verstanden, über einen technischen Zugang auf ein Speichermedium zuzugreifen (z.B. Remote-Zugriff). Das ist mit der gesetzlichen Regelung vermutlich aber nicht gemeint. Rechtlich lässt sich der Begriff nicht gut einordnen. Das schweizerische Recht kennt eine Vielzahl von Möglichkeiten, wie Behörden Informationen proaktiv beschaffen können. Die Bandbreite reicht von Informationsanfragen und Auskunftsrechten bis zu Hausdurchsuchungen und Beschlagnahmungen. Unter welche Kategorie der bisher gesetzlich geregelten Informationsrechte das Zugriffsrecht von Art. 74 Abs. 4 ISG fällt, ist nicht ersichtlich. Der VUD schlägt vor, die Art der Informationsbeschaffung gemäss Art. 74 Abs. 4 ISG mit einem Recht auf Information oder Auskunft zu ersetzen. Das Informationsrecht ist angesichts des Fokus des NCSC auf statistische Auswertungen und der besonderen Kritikalität der Informationen angemessen zu begrenzen. Das Verhältnismässigkeitsprinzip muss auch in diesem Punkt konsequent angewendet werden.

Bemerkungen zu Art. 74a ISG

Die Meldepflicht gemäss Art. 74a ISG schafft eine besondere Dringlichkeit (*"so rasch wie möglich"*), auch wenn diese nicht konkret bemessen wird. Ob diese zeitliche Dringlichkeit angemessen ist, muss in Frage gestellt werden. Wird die Meldepflicht unter dem ISG wie oben (siehe Bemerkung zu Art. 5 Bst. d-e ISG) auf Cybervorfälle begrenzt, die den Betrieb von kritischen Infrastrukturen ernsthaft gefährden, so ist zu bedenken, dass die von einem solchen Vorfall betroffenen Unternehmen oder Organisationen in der ersten Phase damit beschäftigt sind, den Vorfall und dessen Folgen abzuwehren bzw. zu beseitigen. Jede Aktivität, welche diesen Zielen nicht dient, muss unter diesen Umständen zurückstehen. Eine dringliche Meldung an das NCSC ist nur dann angezeigt, wenn der Cybervorfall innert kürzester Zeit und aller Voraussicht nach auch andere Unternehmen und Organisationen treffen kann. Denn nur dann wird das NCSC andere Unternehmen und Organisationen warnen. In allen anderen Fällen kann die Meldung an das NCSC später erfolgen. Der VUD schlägt deshalb vor, in Art. 74a ISG eine angemessene Frist vorzusehen.

Bemerkungen zu Art. 74b ISG

Die Liste der meldepflichtigen Unternehmen und Organisationen gemäss Art. 74b ISG ist unverhältnismässig. In Verbindung mit den extensiven Begriffen von Art. 5 Bst. d-e ISG wird das NCSC mit Meldungen überflutet werden (siehe dazu Bemerkung zu Art. 5 Bst. d-e ISG oben). Wenn man zusätzlich bedenkt, dass die überwiegende Mehrheit von Cyberangriffen nicht von nationalem Interesse sein werden und deshalb nur in die Statistik des NCSC eingehen, so ist der Aufwand, der durch Art. 74b ISG bei den betroffenen Unternehmen und Organisationen bewirkt wird, nicht zu rechtfertigen. Die Einhaltung der aktuell vorgesehenen Meldepflicht lässt sich in der Unternehmenspraxis nur gewährleisten, wenn die meldepflichtigen Unternehmen eine entsprechende Organisation mit den erforderlichen Schlüsselrollen (z.B. Cyber-Team mit Betriebs-, Sicherheits- und Rechtspezialist:innen) und geeignete Prozesse implementieren. Dazu müssen die erforderlichen Budgets bereitgestellt, entsprechende Ressourcen aufgebaut und Schlüsselpersonen geschult werden. Dieser Aufwand lässt sich nur rechtfertigen, wenn der einzelne Cybervorfall für sich von nationalem Interesse ist. In allen anderen Fällen müssen die Unternehmen und Organisationen von jeglichem Aufwand entlastet werden. Aus diesem Grund ist die gesetzgeberische Lösung, wonach die zu meldenden Ereignisse (Art. 5 Bst. d-e ISG) und die meldepflichtigen Unternehmen und Organisationen (Art. 74b ISG) möglichst breit gefasst werden, die Meldepflicht aber begrenzt wird (Art. 74d ISG), abzulehnen. Der grosse Aufwand für die betroffenen Unternehmen und Organisationen entsteht bereits bei den erforderlichen Vorbereitungsarbeiten

zur Gewährleistung der Meldepflicht (Organisation, Prozesse, Schulung). Diese Investitionen sind nur gerechtfertigt, wenn die betroffenen Unternehmen und Organisationen tatsächlich kritische Infrastrukturen im Sinne von Art. 5 Bst. c ISG betreiben.

Dies ist bei vielen der in Art. 74b ISG aufgelisteten Unternehmen und Organisationen nicht der Fall. Nicht jede noch so kleine Privatbank betreibt eine kritische Infrastruktur und ist deshalb staatstragend. Und Ärzt:innen, die nebenbei auch noch ein kleines Labor für ihre Patient:innen betreiben, sind es auch nicht. Man könnte die Beispiele von Unternehmen und Organisationen, die von Art. 74b ISG erfasst sind, aus nationaler Sicht aber keine kritischen Infrastrukturen betreiben, beliebig verlängern. Es ist absehbar, dass nur der kleinste Teil der von Art. 74b ISG erfassten Unternehmen und Organisationen (in der Mehrheit KMU) aus nationaler Sicht tatsächlich kritische Infrastrukturen betreiben. Dies umso mehr, als Art. 74b ISG einzig für digitale Dienste Grössenschwellen für eine Unterstellung vorsieht, andere Unternehmen hingegen ungeachtet jeglicher Grössenschwellen der Meldepflicht unterstellt. Ohne solche Grössenschwellen würde jeder Quartierladen und jeder Marktstand der Meldepflicht unterstehen, da er die Bevölkerung mit Gütern des täglichen Bedarfs versorgt. Nimmt man diese Unternehmen vom Anwendungsbereich von Art. 74b ISG aber nicht aus, so müssen diese die mit der Gewährleistung der Meldepflicht verbundenen Investitionen leisten, obwohl sie von der Meldung eines Cyberangriffs gemäss Art. 74c ISG ausgenommen wären, weil sie keine kritischen Infrastrukturen im Sinne von Art. 5 Bst. c ISG betreiben.

Der VUD deshalb schlägt vor, die Meldepflicht von vornherein auf Cyberangriffe zu begrenzen, welche kritische Infrastrukturen im Sinne von Art. 5 Bst. c ISG erheblich gefährden und deshalb von nationalem Interesse sind. Für eine Meldepflicht kann nur die Kritikalität eines Cyberangriffs aus nationaler Sicht massgebend sein. Dies würde zunächst bedeuten, dass nur jene Unternehmen und Organisationen der Meldepflicht unterliegen würden, welche für solche kritischen Infrastrukturen und deren Betrieb tatsächlich verantwortlich sind. Die Meldepflicht auf bestimmte Arten von Unternehmen und Organisationen auszurichten, ist nicht zielführend, weil sie aufgrund von zahlreichen unklaren Rechtsbegriffen erhebliche Rechtsunsicherheiten schafft und nicht jede der von diesen Unternehmen und Organisationen betriebenen Infrastruktur kritisch ist. Ebenfalls nicht sachgerecht ist es, die Meldepflicht auf jegliche Infrastruktur auszuweiten, die angegriffen werden können, denn nicht jede Infrastruktur ist aus nationaler Sicht kritisch. Schliesslich ist bei der Ausgestaltung von Art. 74b ISG auch darauf zu achten, dass die Meldepflicht in persönlicher Hinsicht klar zugewiesen wird. Die Wertschöpfungskette im Bereich der Informationstechnologie ist komplex und erfasst meist eine Vielzahl von Akteuren (z.B. Auftraggeber, Auftragnehmer, Unterauftragnehmer) auf unterschiedlichen Ebenen (Netzwerk, Infrastruktur, Applikation, User Interface). Ohne klare Bezeichnung der meldepflichtigen Unternehmen und Organisationen droht ein Verantwortlichkeits- und Informationschaos. Der Fokus auf Unternehmen und Organisationen, Infrastrukturen und Cybervorfälle von nationaler Bedeutung erlaubt demgegenüber den allseitig effizienten Einsatz von (begrenzten) Ressourcen und erhöht die Wirksamkeit und Akzeptanz der Meldepflicht.

Bemerkungen zu Art. 74c ISG

Die vom Gesetzgeber vorgeschlagene Lösung mit einer langen Liste von meldepflichtigen Unternehmen bzw. Organisationen (Art. 74b ISG) und deren Begrenzung gemäss Art. 74c ISG ist unnötig und schafft Rechtsunsicherheiten. Es ist ferner nicht ersichtlich, weshalb die Konkretisierung von Art. 74c Bst. b ISG gemäss Ingress von Art. 74c ISG nur auf "bestimmte Kategorien von Betreiberinnen" anwendbar sein soll. Wenn ein Cyberangriff die Voraussetzungen von Art. 74c Bst. b ISG erfüllt, so sollte er unabhängig von der Unternehmensbranche nicht meldepflichtig sein. Massgebend kann nur die Frage sein, ob ein Cyberangriff die nationale Sicherheit erheblich beeinträchtigt. Ist dies nicht der Fall, so ist von einer Meldepflicht abzusehen.

Die Bestimmungen von Art. 74c Bst. a und b ISG sind widersprüchlich bzw. unklar. So können *"ausgelöste"* Funktionsausfälle oder Fehlfunktion nicht "unwahrscheinlich" sein, denn sie wurden nach dem Wortlaut ja bereits ausgelöst. Die Frage der Wahrscheinlichkeit stellt sich somit nicht mehr. Unklar ist, was mit *"einer geringen Abhängigkeit von Informatikmitteln"* (Art. 74c Bst. a ISG) gemeint ist. Unklar ist auch, wann ein Cybervorfall *"nur geringe Auswicklungen auf das Funktionieren der Wirtschaft oder das Wohlergehen der Schweiz"* hat. Ebenso ist nicht klar, wann eine Personenzahl *"gering"* ist oder wann die Auswirkungen *"von anderen kritischen Infrastrukturen"* aufgefangen werden. Durch solche Formulierungen entstehen bei der Rechtsanwendung erhebliche Rechtsunsicherheiten.

Der VUD schlägt vor, die Meldepflicht generell auf Cyberangriffe zu begrenzen, die kritische Infrastrukturen im Sinne von Art. 5 Bst. c ISG erheblich gefährden und deshalb von nationalem Interesse sind. Der VUD empfiehlt zudem, die unklaren bzw. widersprüchlichen Regelungen zu präzisieren. Dies umso mehr, als die Verletzung der Meldepflicht gemäss Art. 74h i.V.m. 74i ISG strafbar ist. Es ist den meldepflichtigen Unternehmen und Organisationen nicht zuzumuten, unklare Rechtsbegriffe auslegen zu müssen, wenn der Verzicht auf eine Meldung aufgrund einer sich nachträglich als falsch erweisende Auslegung mit Strafe bedroht ist. Es ist Aufgabe des Gesetzgebers, die gesetzlichen Anforderungen an die Unternehmen und Organisationen so klar zu formulieren, dass diese ohne Auslegungsrisiko eingehalten werden können.

Bemerkungen Art. 74d ISG

Die gesetzgeberische Lösung, wonach die zu meldenden Ereignisse möglichst breit gefasst werden (Art. 5 Bst. d-e ISG), nur um die Meldepflicht danach wieder zu begrenzen (Art. 74d ISG), ist abzulehnen. Diese Lösung verursacht unnötigen Aufwand bei den betroffenen Unternehmen und Organisationen (siehe dazu Bemerkungen zu Art. 74b ISG oben).

Will der Gesetzgeber an dieser Lösung festhalten, so sollte Art. 74d Bst. a ISG nach Ansicht des VUD nur greifen, wenn die Gefährdung erheblich ist. Eine noch so kleine Gefährdung lässt sich in der Praxis nie ganz ausschliessen, weshalb ein Cyberangriff nach dieser Bestimmung immer gemeldet werden muss. Diese Konsequenz entspricht nicht der in Art. 74d ISG verfolgten Absicht.

Die Konkretisierung in Art. 74d ISG dürfte in der Praxis ins Leere laufen, weil die Beteiligung eines fremden Staates an einem Cyberangriff kaum je eruiert werden kann. Diese Bestimmung dürfte kaum je relevant werden, weshalb sie ersatzlos gestrichen werden kann.

Art. 74d ISG ist nach Ansicht des VUD ersatzlos zu streichen. Wie lange ein Cyberangriff nicht entdeckt wurde, ist für dessen Kritikalität nicht entscheidend, solange die damit verbundene Gefährdung nicht erheblich ist.

Bemerkung zu Art. 74g ISG

Diese Bestimmung ist zu ungenau und sollte ersatzlos gestrichen werden. Der Inhalt der Meldung wird durch Art. 74e ISG erschöpfend geregelt. Welche Informationen das NCSC sonst noch brauchen könnte, die in Art. 74e ISG nicht vorgesehen sind, ist nicht erkennbar. Eine Pflicht der meldepflichtigen Unternehmen und Organisationen zur Auskunftserteilung über Art. 74e ISG hinaus ist ohne weitere Konkretisierung und Begrenzung der zu leistenden Auskunft aus rechtsstaatlichen Gründen abzulehnen. Das Informationsbedürfnis des NCSC muss gesetzlich konkretisiert werden und lässt sich nicht mit einem pauschalen Hinweis auf den gesetzlichen Auftrag rechtfertigen. Dies umso mehr, als sich die Meldepflicht auf einen hochsensiblen Bereich der betroffenen Unternehmen und Organisationen richtet und die Widerhandlung gegen eine Verfügung des NCSC gemäss Art. 74h ISG strafbar ist.

Bemerkungen zu Art. 77 ISG

Der Austausch von Informationen mit ausländischen Behörden gemäss Art. 77 ISG darf nur anonymisiert erfolgen. Die von den betroffenen Unternehmen und Organisationen an das NCSC gelieferten Informationen werden sehr sensitiv sein. In welchem Umfang und zu welchen Zwecken die Informationen ausgetauscht werden, wird für die betroffenen Unternehmen und Organisationen kaum je erkennbar bzw. kontrollierbar sein. Der Austausch von Informationen gemäss Art. 77 ISG darf daher zum Schutz der beteiligen Unternehmen und Organisationen nur anonymisiert erfolgen.

* * * * * * *

Der guten Ordnung halber weisen wir darauf hin, dass die in dieser Stellungnahme vorgetragenen Ansichten und Anregungen nicht in jedem Fall der Meinung aller VUD-Mitglieder entspricht. Wir danken für die wohlwollende Aufnahme und verbleiben

Mit freundlichen Grüssen

Heribert Grab
Präsident VUD

Dr. Nicolas Passadelis
Vorstandsmitglied