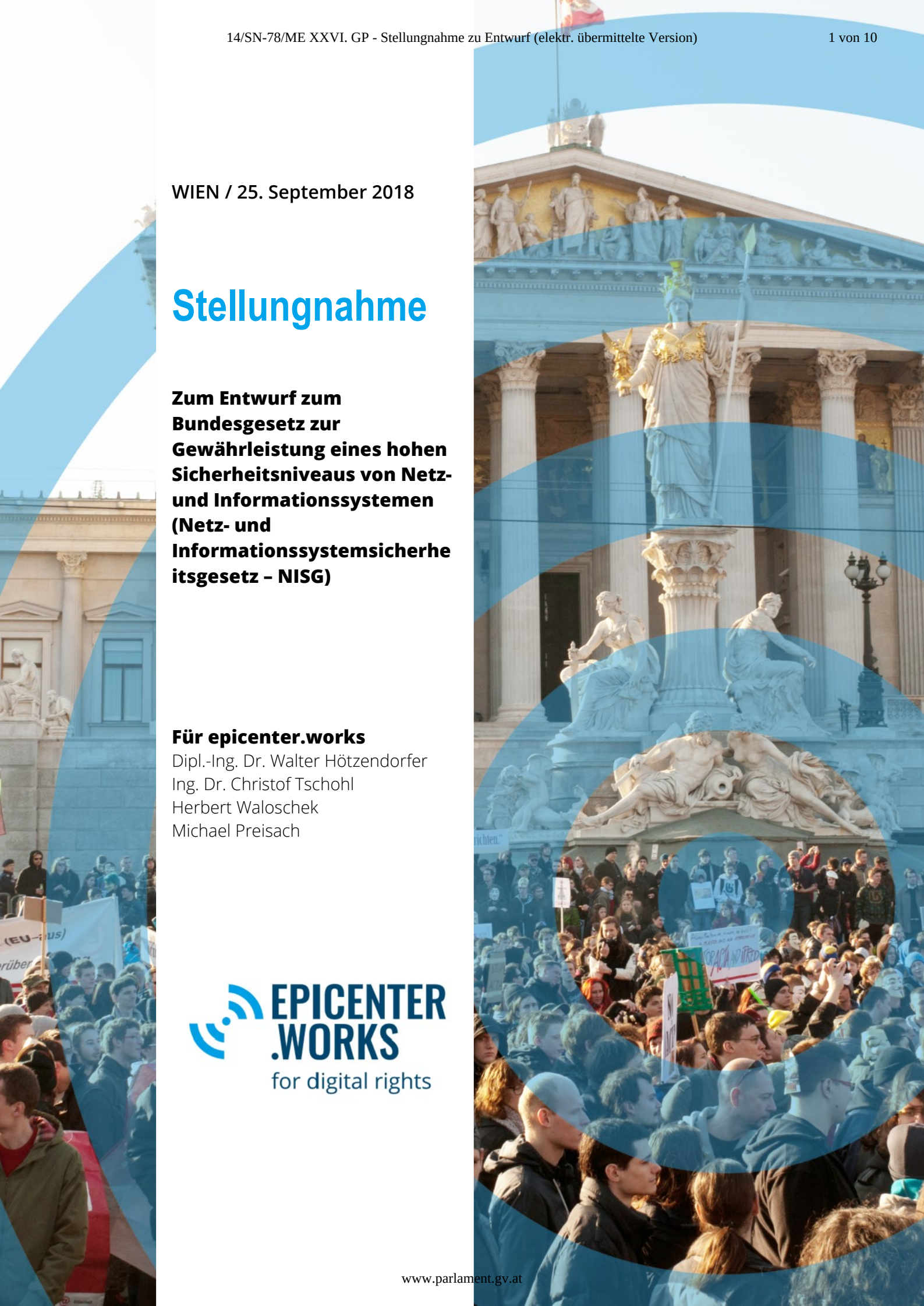

WIEN / 25. September 2018

Stellungnahme

Zum Entwurf zum Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)

Für epicenter.works
Dipl.-Ing. Dr. Walter Hötzendorfer
Ing. Dr. Christof Tschohl
Herbert Waloschek
Michael Preisach

EPICENTER .WORKS
for digital rights

VORWORT UND KURZFASSUNG

Die Grundrechts-NGO epicenter.works befürwortet die der NIS-Richtlinie zugrundeliegenden Ziele und weite Teile des vorgeschlagenen Umsetzungsgesetzes. Die Bedrohungen für Netz- und Informationssysteme nehmen stetig zu, ebenso wie deren Potenzial, gravierende Auswirkungen auf unsere Infrastruktur und somit auf unser tägliches Leben zu entfalten. Es ist daher sehr zu begrüßen, dass im NISG Mechanismen zur Prävention solcher Bedrohungen geschaffen werden und eine solide rechtliche Basis für bereits existierende Mechanismen und Institutionen geschaffen wird, wie insbesondere für die bewährte Arbeit der CERTs (Computer-Notfallteams) und den Austausch relevanter Information über Bedrohungen.

Im Sinne dieses und der weiteren Ziele der NIS-Richtlinie sowie des Grundrechts auf Datenschutz sollte der Entwurf jedoch noch an zahlreichen Stellen angepasst werden. Diese Stellungnahme enthält daher möglichst konkrete Kritikpunkte und Verbesserungsvorschläge zu einzelnen Bestimmungen des Entwurfs. Darüber hinaus sind jedoch auch einige grundlegende im Entwurf manifestierte Entscheidungen zu hinterfragen. Insbesondere ist die intensive Betrauung des Innenministeriums mit NIS-Agenden zu kritisieren, denn dort besteht potenziell ein Interessenkonflikt zwischen polizeilichen Aufgaben und den präventiven Aufgaben gemäß NISG und es sollte bereits der bloße Anschein möglichst vermieden werden, dass die umfassenden mit dem NISG geschaffenen Überwachungs- und Einschaubefugnisse missbräuchlich eingesetzt werden könnten.

Inhaltsverzeichnis

GRUNDLEGENDE BEMERKUNGEN

Vorgeschichte

Bereits in Vorbereitung der Jahrtausendwende gab es in Österreich eine sektorenübergreifende Koordination von Sicherheitsmaßnahmen. Das "Y2K-Problem" wurde vielfach als Bedrohung der Daseinsvorsorge empfunden, insbesondere Banken aus den USA versuchten, über ein weltweites Berichts-System Überblick zu erhalten über die Vorbereitung in den einzelnen Staaten und Sektoren.

In Österreich wurden ein einheitliches Berichtswesen und daraus abgeleitete koordinierte Maßnahmenbündel zur Gewährleistung eines sicheren Wechsels ins neue Jahrtausend etabliert. Das Risiko von Fehlern wurde zunächst als IT-Problem gesehen, doch das Risiko durch Auswirkungen solcher technischen Schwächen und Programmfehler bestand überall, wo elektronische Steuerungen in Infrastrukturbereichen verwendet wurden.

Ausgehend vom Bereich des Bankwesens wurde bereits damals die kritische Infrastruktur, insbesondere Telekommunikation, Energie- und Wasserversorgung, Verkehr und Gesundheitswesen mit einbezogen. Im Bundeskanzleramt wurde dazu eine eigene Koordinationsstelle eingerichtet. Nach erfolgreichem Wechsel ins neue Jahrtausend wurden die dafür geschaffenen Strukturen nicht weiter betrieben und aufgelöst.

Im Jahr 2008 wurde schließlich in erfolgreicher Kooperation zwischen dem Bundeskanzleramt und nic.at das GovCERT und CERT.at in Betrieb genommen. Diese Institutionen haben sich seither sehr bewährt und das NISG bettet diese nun in einen umfassenden rechtlichen Rahmen ein.

Rahmenbedingungen

Mit 6. Juli 2016 wurde die "RICHTLINIE (EU) 2016/1148 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union" (NIS-Richtlinie) erlassen.

Gem. Art 4 Z 4 iVm. Anhang II der Richtlinie umfasst diese wesentliche Dienste in den Sektoren

- Energie,
- Verkehr,
- Bankwesen,
- Finanzmarktinfrastruktur,
- Gesundheitswesen,
- Trinkwasserlieferung und -versorgung,
- digitale Infrastruktur

Mit dem Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)[1] wird diese Richtlinie in nationales Recht umgesetzt.

1 https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00078/index.shtml

Zuordnung von Infrastruktur

Angelegenheiten der Infrastruktur fallen in Österreich grundsätzlich in die Zuständigkeit des Bundesministeriums für Verkehr, Innovation und Technologie (BMVIT).

"Das BMVIT schafft den Rahmen für Österreichs Infrastruktur von der Schiene bis zur Straße, im Wasser und in der Luft, bis hin zur Telekommunikation und Technologieentwicklung" lautet die Eigendefinition des BMVIT auf seiner Website.

Risikoeinschätzung und Sicherheitsmanagement sind wesentlicher Teil von Planungs- und Entwicklungsprozessen. Nachträglich aufgesetzte Sicherheitsmaßnahmen können üblicherweise Fehler und Mängel der Systementwicklung nur kaschieren, aber nicht mehr vermeiden.

Daher wäre es angemessen, auch die Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen im Bereich des BMVIT anzusiedeln. In Österreich soll dies jedoch nicht so gehandhabt werden. Die Gewährleistung eines hohen Sicherheitsniveaus soll zwischen Bundeskanzleramt und Innenministerium geteilt werden ("strategischer" und "operativer" Teil), dementsprechend sind zwei NIS-Büros geplant.

Selbst wenn Sachkompetenz derzeit in einem dieser Bereiche angenommen wird, sollte eine strategisch orientierte Zuordnung zu einem Bereich erfolgen, dessen Aufgabe primär Entwicklung und Verbesserung von Infrastruktur ist, um von Anfang an in Entwicklungsprozesse eingreifen zu können. Die Erfahrung zeigt, dass Qualitäts- und Sicherheitsbewusstsein im täglichen Handeln und in Entwicklungsprozessen nicht durch nachträgliche Überprüfung und Kontrolle erreicht wird.

Die Bündelung der Zuständigkeit in einem Ministerium wäre gegenüber der geplanten Zweiteilung auch deswegen zu bevorzugen, weil eine Zweiteilung von Zuständigkeiten stets zu potenziellen Ineffizienzen, „Reibungsverlusten“ und Informationsdefiziten führen kann, die sich hier negativ auf die Netz- und Informationssystemsicherheit auswirken können.

Unabhängig davon ist im Lichte früherer Konzepte zur Umsetzung der NIS-RL zu hinterfragen, warum das Bundesministerium für Landesverteidigung (BMLV) entgegen früherer Planungen im vorliegenden Entwurf nur noch vereinzelt erwähnt wird. Nicht zuletzt da das BMLV dennoch in § 11 Befugnisse zur Datenverarbeitung erhält, wäre es höchst wünschenswert gewesen, die Kompetenzen des BMLV zur Aufrechterhaltung der Netz- und Informationssystemsicherheit im NISG präziser zu determinieren.

Sicherheit gewährleisten oder Überwachung und Kontrolle?

Sicherheit umfasst grundsätzlich die Bereiche Vertraulichkeit, Integrität und Verfügbarkeit. Sicherheitsmanagement ist ein laufender, umfassender Prozess, der vertrauensvolle Kommunikation aller Beteiligten auf Augenhöhe voraussetzt.

Dieser vertrauensvollen Kommunikationsprozess soll laut dem Entwurf in Österreich von einer Behörde, die primär mit sicherheitspolizeilichen Aufgaben und Aufgaben der Strafverfolgung befasst ist, gestaltet werden. Für Anbieter und Betreiber von sicherer Infrastruktur schafft das inhärente Konfliktsituationen in Bezug auf deren eigene Bedürfnisse und die Interessen der Kunden, die eine sichere, also verfügbare und vertrauliche Infrastruktur erwarten. Am deutlichsten wird dies in Bezug auf Personengruppen wie z.B.: Rechtsanwälte und Psychotherapeuten, die auch und gerade gegenüber der Polizei einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Der vorliegende Entwurf umfasst Berichtsaufgaben für Betreiber und Anbieter sowie eine umfassende Einschaubefugnis der Behörde in betriebliche Vorgänge. Eine umfassende Pflicht zur Information über bestehende Gefahren, auch an die breite Öffentlichkeit, ist darin nicht vorgesehen. Es fehlt die umfassende Informationspflicht über Mängel und Sicherheitslücken von weit verbreiteter Software und von Geräten, die an Netzwerke angeschlossen sind. Millionen unsicherer Router, gefährdeter IoT-Geräte, gefährdeter Betriebssysteme oder Anwendungen bei Endnutzern wegen nicht behobener – weil nicht publizierter – Sicherheitsmängel stellen eine immer stärker zunehmende Gefahr dar, die im vorliegenden Gesetzesentwurf nicht adäquat berücksichtigt wird.

Auch in dieser Hinsicht ist die Ansiedelung wesentlicher NIS-Agenden beim Innenministerium zu hinterfragen, insbesondere solange dieses Ministerium zugleich an der Entwicklung, Beschaffung bzw. Evaluierung von Bundestrojaner-Software arbeitet (vgl. § 135a StPO, der am 01.04.2020 in Kraft treten wird), deren Einsatz potenziell davon abhängig ist, dass den Behörden Sicherheitslücken bekannt sind. Wir sprechen uns daher an dieser Stelle auch nochmals in aller Deutlichkeit gegen die Einführung eines Bundestrojaners und somit gegen § 135a StPO aus. Mit dem NISG kommt noch ein weiterer Grund für diese Ablehnung hinzu.

Ob die beim Innenministerium, also im polizeinahen Bereich, anzusiedelnden "technischen Einrichtungen“ nach § 9 des Entwurfs, „die Unregelmäßigkeiten oder Störungen von Netz- und Informationssystemen frühzeitig erkennen" sollen, als Beitrag zur Vertraulichkeit von Netz- und Informationssystemen erachtet werden können, oder (auch) als technische Vorbereitung umfassender Überwachung, ist dem Gesetzesentwurf nicht zu entnehmen.

Die Einbettung in dieses Gesetz, die Zuordnung beim Innenministerium und die unspezifizierten Möglichkeiten zur Übermittlungen an andere Stellen ohne inhaltliche, technische, formale und geografische Einschränkung (§ 11) stehen in deutlichem Widerspruch zur Intention von Grundrechtsschutz (Datenschutz und Schutz der Privatsphäre), wie sie in der Datenschutz-Grundverordnung (DSGVO) und der DatenschutzRichtlinie für den Bereich Polizei und Justiz (DSRL-PJ) zum Ausdruck kommt.

Im Lichte dieser Umstände regen wir die Schaffung eines Bundesamtes für Netz- und Informationssystemsicherheit an. Dieses sollte aus den genannten Gründen nicht in der Ressortzuständigkeit des Innenministeriums angesiedelt sein. Bei einem solchen Bundesamt könnten die Präventionskapazitäten im NIS-Bereich effektiv und effizient gebündelt, bestehende Expertise eingebracht und weitere Expertise aufgebaut werden.

Dabei wird nicht verkannt, dass die Sicherheitsbehörden eine wesentliche Rolle in der Bekämpfung von Angriffen auf Netz- und Informationssysteme spielen. Kernstoßrichtung der NIS-Richtlinie ist jedoch die Prävention und umso deutlicher muss durch die vorgeschlagene Eigenständigkeit klargestellt werden, dass NIS nicht nur aus Strafverfolgungsperspektive betrieben werden sollte.

DETAILBEMERKUNGEN

Zu den einzelnen Bestimmungen des Entwurfs äußert epicenter.works insbesondere folgende Kritikpunkte und Verbesserungsvorschläge, ohne damit eine generelle Zustimmung zu den im Folgenden nicht angesprochenen Bestimmungen zum Ausdruck bringen zu wollen.

Zu § 1:

Durch diese Bestimmung werden dem Bund Kompetenzen zugewiesen, ohne konkret zu benennen, um welche Kompetenzen es sich dabei überhaupt handelt. Stattdessen werden die Kompetenzen nur abstrakt durch einen Verweis auf die nachfolgenden (einfachgesetzlichen) Regelungen beschrieben. Dadurch würde der geschaffene Kompetenztatbestand exakt den einfachgesetzlichen Regelungen entlang verlaufen – gleichsam die für diesen Gesetzgebungsakt maßgeschneiderte Kompetenz.

Dabei handelt es sich – gelinde gesagt – um eine unsaubere Regelungstechnik, denn dies würde dazu führen, dass die Kompetenzverteilung zwischen Bund und Ländern nicht mehr ausdrücklich fassbar ist, sondern sich in Teilen nur noch implizit aus dem Inhalt des NISG ergibt. Darüber hinaus würde dies dazu führen, dass spätere Änderungen des NISG potenziell wieder einer entsprechenden Kompetenzbestimmung im Verfassungsrang bedürften.

Zudem treten wir generell dafür ein, dass Kompetenzfragen aus systematischen Gründen und Gründen der Übersichtlichkeit und Transparenz nur im B-VG geregelt werden sollten.

Zu § 3 Z 6:

Gemessen an den mit dem NISG und der NIS-Richtlinie verfolgten Zielen, insbesondere betreffend die Erstellung eines Lagebildes, ist die Definition des für die Meldepflicht zentralen Begriffs "Sicherheitsvorfall" zu eng, da dieser nur Vorfälle umfasst, in denen die Verfügbarkeit des betroffenen Dienstes tatsächlich beeinträchtigt wurde. Demgegenüber definiert die NIS-Richtlinie den Begriff „Sicherheitsvorfall“ als "alle Ereignisse, die tatsächlich nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben". Während also die NIS-Richtlinie ihrem Zweck folgend auf die Sicherheit der zugrundeliegenden Netz- und Informationssysteme abstellt, greift die Definition des österreichischen Gesetzgebers erst bei (spürbaren) Auswirkungen auf die von diesen Systemen abhängigen Dienste. Es muss somit erst gemeldet werden, wenn es im Einzelfall schon zu spät ist und die Funktionalität der Netz- und Informationssysteme möglicherweise bereits kompromittiert ist.

Um systematische, groß angelegte Angriffe möglichst früh zu erkennen und einen zentralen Überblick über Angriffe und sonstige (potenzielle) schwerwiegende Beeinträchtigungen der NIS zu erhalten, müssen jedoch alle Vorfälle meldepflichtig sein, die schwerwiegende Auswirkungen auf die einem Dienst zugrundeliegenden Netz- und Informationssysteme haben oder hätten können, auch wenn dies auf die Verfügbarkeit des betroffenen Dienstes im Einzelfall (noch) keine Auswirkungen hatte. Daher sollte die Definition eines Sicherheitsvorfalls mindestens dahingehend erweitert werden, dass auch Vorfälle umfasst sind, die mit hoher Wahrscheinlichkeit „zu einem Ausfall oder einer Einschränkung der Verfügbarkeit“ führen hätten können oder noch führen könnten. Mit anderen Worten: Gerade die Meldung schwerwiegender Vorfälle, die ansonsten von außen (noch) nicht wahrnehmbar sind, ist besonders wichtig.

Zu § 9:

Mit § 9 des Entwurfs soll der Innenminister die Befugnis erhalten, technische Einrichtungen zur Erkennung von Unregelmäßigkeiten und Störungen (Indicators-of-Compromise-basiertes Frühwarnsystem) zu betreiben. Es handelt sich dabei um eine (technische) Überwachungsbefugnis. Wir lehnen eine solche Befugnis nicht generell ab, kritisieren jedoch im Lichte der obigen grundsätzlichen Ausführungen die Zuweisung einer solchen Befugnis zum Innenministerium, denn es sollte auch bereits der bloße Anschein vermieden werden, dass diese Befugnis missbräuchlich zu anderen Zwecken eingesetzt werden könnte, insbesondere für andere dem Innenministerium zugewiesene Aufgaben.

Der Betrieb solcher technischen Einrichtungen sollte darüber hinaus im Gesetzestext deutlicher determiniert und eingegrenzt werden. Zu denken ist an eine Beschränkung auf solche Netz- und Informationssysteme, die für die Aufrechterhaltung des Betriebs wesentlicher Dienste, digitaler Dienste oder von Einrichtungen des Bundes notwendig sind.

Eine Besonderheit ergibt sich hierbei in Bezug auf Internet-Knoten (Internet Exchange Points, IXP), denn deren Betrieb ist nicht nur von Netz- und Informationssystemen abhängig, sondern der IXP-Dienst ist selbst ein Netz- und Informationssystem. § 9 soll jedoch nicht zur Überwachung des gesamten Datenverkehrs des IXP-Dienstes selbst – und somit in Österreich des zentralen Internet-Knotens Vienna Internet eXchange (VIX) – führen. Dies sollte direkt im Gesetzestext ausgeschlossen werden und zwar deutlicher, als dies in den Erläuterungen der Fall ist.

Die Verarbeitung der erhobenen Daten in personenbezogener Form sollte auf Zwecke des jeweiligen Betreibers wesentlicher Dienste oder Anbieters digitaler Dienste bzw. der jeweiligen Einrichtung des Bundes beschränkt sein. Darüber hinaus sollte die Weiterverarbeitung der aufgrund von § 9 erhobenen Daten zur Erstellung eines Lagebildes nur in nicht personenbezogener Form gestattet sein.

Anzumerken ist schließlich, dass solche technischen Einrichtungen gemäß Art 25 DSGVO nach dem Grundsatz des Datenschutzes durch Technikgestaltung (Privacy by Design) zu konzipieren sind und vor Inbetriebnahme solcher technischer Einrichtungen – sowie potenziell auch anderer Verarbeitungstätigkeiten personenbezogener Daten, die sich aus dem NISG ergeben – eine Datenschutz-Folgenabschätzung nach Art 35 DSGVO durchzuführen ist. Diese Pflicht ergibt sich aus Art 35 Abs 3 lit c DSGVO. Von der Durchführung einer allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass der Rechtsgrundlage für die Verarbeitung (Art 35 Abs 10 DSGVO) hat der Gesetzgeber bedauerlicherweise offenbar keinen Gebrauch gemacht.

Zu § 10 Abs 1:

Diese Bestimmung ist unseres Erachtens zu weit formuliert. Eine nähere Spezifizierung der Datenverarbeitungsbefugnisse und der zugehörigen Aufbewahrungsfristen wäre sowohl im Sinne des Datenschutzes als auch im Sinne der Rechtsklarheit für die Vollziehung dringend geboten.

Zu § 10 Abs 3:

Diese Bestimmung ist unseres Erachtens ebenfalls zu weit formuliert. Inhalte und Zwecke der Auskünfte sollten näher spezifiziert werden. In Bezug auf Betreiber und Anbieter sollte die Auskunftspflicht auf Informationen beschränkt werden, die sich auf die Sicherheit von deren eigenen Netz- und Informationssystemen beziehen.

In § 20 (siehe dazu unten) sind freiwillige Meldungen geregelt, inklusive einer Vertraulichkeitsregelung, die diesbezügliche Bedenken und Hemmnisse potenzieller freiwillig Meldender hintanhalten soll. § 10 Abs 3 des Entwurfs birgt die Gefahr, dass diese Vertraulichkeitsregelung umgangen werden könnte. Um freiwillige Meldungen zu fördern, sollten Inhalte von freiwilligen Meldungen, die über das hinausgehen, was gem. § 20 an das BMI zu melden ist, von der Auskunftspflicht nach § 10 Abs 3 ausgenommen sein.

Darüber hinaus bedarf es der Klarstellung, dass die jeweils einschlägigen Regeln der „Amtshilfe" einzuhalten sind und durch § 10 Abs 3 nicht umgangen werden dürfen, wenn Daten aus Meldungen für andere Zwecke (z.B.: Zwecke der Strafverfolgung) verwendet werden sollen.

Zu § 10 Abs 4:

Soll die Protokollierungspflicht in Bezug auf jede Abfrage, Übermittlung und Änderung personenbezogener Daten eine wirksame Datenschutzmaßnahme sein, dann muss eine Zuordnung jedes solchen Vorgangs auf die konkrete handelnde Person (Benutzerkennung) und nicht bloß auf das NIS-Büro möglich sein. Nur dadurch ist sichergestellt, dass jeder Zugriffsberechtigte weiß, dass seine Handlungen auf ihn zurückgeführt werden können, sodass Befugnisüberschreitungen und Missbrauch vorgebeugt werden.

Zu § 11 Abs 4:

Die Befugnisse zur Übermittlung von personenbezogenen Daten sind zu weit und zu unpräzise definiert, insbesondere die Befugnis, personenbezogene Daten zu übermitteln an „sonstige in- und ausländische Behörden oder Stellen, soweit dies zur Aufgabenerfüllung erforderlich ist". Die Befugnis zur Übermittlung personenbezogener Daten an ausländische Behörden oder Stellen sollte auf den in der NIS-Richtlinie vorgesehenen Informationsaustausch beschränkt sein.

Zu § 12 Abs 1:

Bedauerlicherweise scheint es bisher nicht gelungen zu sein, eine Formulierung zu finden, um im Gesetzestext ausdrücklich klarzustellen, dass es sich beim nationalen Computer-Notfallteam nach § 12 Abs 1 um das bewährte und allseits geschätzte CERT.at handeln wird.

Zudem ist nicht ersichtlich, dass die Computer-Notfallteams künftig ausreichend Ressourcen erhalten werden, um ihren Aufgaben nachkommen zu können. Dies sollte gesetzlich ausdrücklich vorgesehen werden. Die Mitgliedstaaten sind gemäß Art 9 Abs 2 NIS-RL ausdrücklich verpflichtet, die Computer-Notfallteams mit angemessenen Ressourcen auszustatten.

Zu § 12 Abs 7:

Sowohl im Sinne der Klarheit für die Computer-Notfallteams als Rechtsanwender als auch im Sinne des Datenschutzes ist es sinnvoll, für die Verarbeitung personenbezogener Daten eine Löschfrist festzulegen. Wir regen daher folgende Ergänzung der Bestimmung an: „*Die verarbeiteten personenbezogenen Daten sind nach längstens drei Monaten zu löschen, außer in begründeten Ausnahmefällen, die unter Angabe der Begründung zu dokumentieren und zu protokollieren sind.*"

Zu § 20:

Den freiwilligen Meldungen kommt bei der Erreichung der Ziele des NISG und der NIS-Richtlinie, insbesondere zur Erstellung eines Lagebildes, eine hohe Bedeutung zu. Dies umso mehr, falls die Definition des Begriffs "Sicherheitsvorfall" so eng gefasst bliebe, wie das in § 3 Z 6 des Entwurfs derzeit vorgesehen ist (siehe oben), denn dies würde bedeuten, dass in der Praxis sehr wenige Pflichtmeldungen zu erwarten wären und damit Beitrag von Pflichtmeldungen für die Erstellung eines Lagebildes gering ausfallen würde. Ziel des § 20 muss es daher sein, die Abgabe freiwilliger Meldungen möglichst zu fördern und diesbezügliche Hürden möglichst gering zu halten.

Bisher existierte eine gewisse Rechtsunsicherheit betreffend die datenschutzrechtliche Zulässigkeit des Informationsaustauschs im NIS-Umfeld. Um solche Unsicherheiten auszuräumen, und damit freiwillige Meldungen zu fördern, sollte ausdrücklich klargestellt werden, dass eine freiwillige Meldung auch personenbezogene Daten enthalten darf, wenn dies zweckdienlich ist, z.B.: durch die Formulierung „*...sämtliche relevanten Angaben zur Störung einschließlich personenbezogener Daten [...] enthalten.*"

§ 20 sieht eine Vertraulichkeitsregelung vor, die diesbezügliche Bedenken und Hemmnisse potenzieller freiwillig Meldender hintanhalten soll. Um freiwillige Meldungen zu fördern ist es uE erforderlich, diese noch deutlicher zu formulieren. Insbesondere sollte es lauten "*die Nennung der meldenden Einrichtung und von Informationen, die auf diese schließen lassen, kann dabei auf ihr Verlangen entfallen.*"

§20 letzter Satz sieht vor, dass freiwillige Meldungen auch Angaben "zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik" enthalten können. Im Sinne der Ziele des NISG und der NIS-Richtlinie regen wir an, dass solche Informationen, insbesondere Informationen über Sicherheitslücken, auch ausschließlicher Inhalt einer freiwilligen Meldungen sein können (Responsible Disclosure). Die begriffliche Beschränkung freiwilliger Meldungen auf "Störungen" in § 20 Abs 1 ist daher zu eng.

Zu § 28:

Das Versäumnis, dass das Gesetz nicht innerhalb der Umsetzungsfrist bis 9. Mai 2018 erlassen wurde, soll nun offenbar durch ein rückwirkendes Inkrafttreten „saniert" werden. Dies wirft verfassungsrechtliche Bedenken auf, die im Entwurf selbst signalisiert werden, indem § 28 im Verfassungsrang beschlossen werden soll. Wir können eine Notwendigkeit zu dieser Rückwirkung nicht erkennen und auch in den Erläuterungen wird eine solche nicht begründet.

CONCLUSIO

Insgesamt begrüßt der Verein epicenter.works den vorliegenden Entwurf, kritisiert jedoch insbesondere die dominante Rolle des Innenministeriums und pocht auf Verbesserungen und Konkretisierungen in den dargelegten Punkten sowie auf die Umsetzung grundrechtlich gebotener Datenschutzgrundsätze, die Implementierung von Datenschutz durch Technikgestaltung (Privacy by Design) und die Durchführung der erforderlichen Datenschutz-Folgenabschätzungen nach Art 35 DSGVO. Für Gespräche steht unser Policy-Team gerne zur Verfügung.