Bundeskammer der
Ziviltechniker:innen | Arch+Ing

A-1040 Wien, Karlsgasse 9
T +43.1.505 58 07
F +43.1.505 32 11
office@arching.at, www.arching.at

Bundeskanzleramt
Abteilung I/8 (Technologie- und Datenmanagement,
Cybersicherheit und Krisenrechenzentrum)
Ballhausplatz 2
1010 Wien

Per E-Mail an: nis@bka.gv.at
Via Webseite an Parlamentsdirektion

Wien, am 30. April 2024

Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem ein Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024) erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden

GZ: 2024-0.220.735

Sehr geehrte Damen und Herren!

Die Bundeskammer der Ziviltechniker:innen bedankt sich für die Übermittlung des oben genannten Entwurfs und erlaubt sich dazu folgende Stellungnahme abzugeben:

Vorausschicken möchten wir, dass sich weder die Bundeskammer noch die Länderkammern der Ziviltechniker:innen als berufliche Selbstverwaltungskörper vom Anwendungsbereich des vorliegenden Entwurfs betroffen sehen, weil sie weder unter die wesentlichen Einrichtungen im Sektor der öffentlichen Verwaltung auf Bundesebene iSd § 24 Abs. 1 Z 1 lit d iVm Abs. 4 noch unter die wichtigen Einrichtungen im Sektor er öffentlichen Verwaltung auf Landesebene iSd § 24 Abs. 2 Z 2 iVm Abs. 5 fallen. Insbesondere da die Bundeskammer bzw. die Länderkammern im Rahmen der sonstigen Selbstverwaltung iSd Art. 120a bis c B-VG tätig und in der Besorgung ihrer Aufgaben auch nicht weisungsgebunden sind.

Um Unklarheiten zu vermeiden, regt die Bundeskammer aus den oben genannten Gründen eine ausdrückliche Klarstellung – so wie sie in § 24 Abs. 3 für Gemeinden oder in § 24 Abs. 6 für Universitäten usw. vorgesehen ist – dahingehend an, dass Selbstverwaltungskörper, wie die Kammern der Ziviltechniker:innen sowie insgesamt die Kammern der freien Berufe, nicht als wesentliche oder wichtige Einrichtungen der öffentlichen Verwaltung gelten. Zumindest sollte aber jedenfalls eine entsprechende Klarstellung in den Erläuterungen zum Entwurf erfolgen.

Zu § 3 Z 1:

Der Ordnung halber wird darauf hingewiesen, dass es den Begriff „Netzsystem“, wie es wohl aus der Definition „Netz- und Informationssystem“ herauszulesen ist, im Bereich der Informationstechnologie nicht gibt. Ein Netzsystem ist unserer Ansicht nach dem Bereich der Elektrotechnik zuzuordnen.

Zu § 3 Z 26:

In Art. 6 Z 9 Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) wird der Begriff „Risiko“ als ein „Potenzial für Verluste oder Störungen, die durch Sicherheitsvorfall verursacht werden“ definiert. § 3 Z 26 des Gesetzesentwurfes spricht dagegen von einem Cybersicherheitsvorfall. Die Definitionen zu Sicherheitsvorfall (Art. 6 Z 6 Richtlinie (EU) 2022/2555) und Cybersicherheitsvorfall (§ 3 Z 30) sind jedoch gleichlautend. Ein Cybersicherheitsvorfall könnte eine Begrenzung auf kriminelle Attacken aus dem Internet suggerieren. Im Sinne des Betriebs wichtiger und wesentlicher Einrichtungen greift dies uE zu kurz.

Aus Sicht der Bundeskammer inkludieren Risiken auch im Kontext der NIS-2-Richtlinie alle Ursachen und Ereignisse, die die Zuverlässigkeit (Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität) eines ordnungsgemäßen Betriebs der Netz- und Informationssysteme negativ beeinflussen können. Darunter fallen auch potenziell fehlerhafte Betriebssoftware, Hardware und Steuergeräte, Störungen in der physischen Infrastruktur, Tätermodelle (Innentäter, Außentäter) usw.

Mit Verweis auf das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) sollte unter dem Begriff „Risiko“ auch der „All-Gefahren-Ansatz“ mitberücksichtigt werden. Ein All-Gefahren-Ansatz ist ein umfassender und integrierter Rahmen für die Vorbereitung auf Notfälle, der bei der Planung von Reaktions- und Eindämmungsmaßnahmen für "alle Gefahren", die auftreten können, angewendet wird. Sollten nur Vorfälle aus Cybergefahren vom Gesetz erfasst werden, sollte dieser Umstand präzisiert werden. Wenn dies nicht erfolgt, öffnet es Tür und Tor für individuelle Auslegungen bei Prüfer:innen.

Zu § 3 Z 33:

In der Begriffsbestimmung des § 3 Z 33 wird die Abkürzung „CSIRT“ mit Computer-Notfallteam übersetzt. Nachdem „CSIRT“ für „Computer Security Incident Response Team“ steht, wird angeregt, als deutsche Übersetzung „Computersicherheits-Ereignis- und Reaktionsteam“ oder „Computersicherheits-Reaktionsteam“ zu übernehmen.

Zu § 7:

Mit § 7 wird das im NISG bestehende Institut der qualifizierten Stellen (vgl. § 18 NISG) im Wesentlichen in das neue NISG 2024 überführt. Gemäß § 3 der Verordnung über qualifizierte Stellen – QuaSteV, BGBl. II Nr. 226/2019, hatten qualifizierte Stellen bislang „befähigte sicherheitsüberprüfte Prüfer“ einzusetzen. Die Anforderungen an diese Prüfer:innen waren in § 4 QuaSteV geregelt. Die Erfüllung dieser Anforderungen waren durch die qualifizierte Stelle gegenüber dem Bundesminister für Inneres bei der Antragstellung nachzuweisen.

Vergleichbar mit dem bisherigen Prüfsystem regelt Abs. 1, dass der Nachweis, dass eine wesentliche oder wichtige Einrichtung die gebotenen Risikomanagementmaßnahmen getroffen hat (§ 33 Abs. 2 und 3) durch eine unabhängige Stelle zu prüfen ist, die sich hierfür zumindest eines unabhängigen Prüfers zu bedienen hat. Unabhängige Stellen haben ihre Eignung gegenüber der Cybersicherheitsbehörde bei der Antragstellung nach Abs. 2 nachzuweisen. In einer

Verordnung des Bundesministers für Inneres sollen die Anforderungen, die eine unabhängige Stelle zur Zulassung erfüllen muss, festgelegt werden (Abs. 13 Z 1).

Unabhängige Prüfer:innen sind natürliche Personen, die von einer unabhängigen Stelle zur Beurteilung der Umsetzung von Risikomanagementmaßnahmen wesentlicher und wichtiger Einrichtungen gemäß § 33 Abs. 2 und 3 eingesetzt werden können (Abs. 5). Als Voraussetzungen dafür sind nach Z 1 eine vor nicht länger als drei Jahren durchgeführte Sicherheitsüberprüfung sowie nach Z 2 die positive Absolvierung einer Fachprüfung gemäß Abs. 8 nachzuweisen.

Zu einer solchen Fachprüfung ist gemäß Abs. 7 zuzulassen, wer über ein österreichisches Reifeprüfungszeugnis, Diplomprüfungszeugnis oder Berufsreifeprüfungszeugnis verfügt (Z 1) und eine facheinschlägige Berufserfahrung von mindestens drei Jahren im Ausmaß von zumindest zwanzig Wochenstunden im Bereich der Cybersicherheit nachweisen kann (Z 2). Im Rahmen der Fachprüfung hat der Prüfungskandidat ausreichende theoretische Fachkenntnisse über die Risikomanagementmaßnahmen gemäß § 32 und ausreichende praktische Fähigkeiten zur Beurteilung der Umsetzung von Risikomanagementmaßnahmen gemäß § 32 in organisatorischer oder technischer Hinsicht nachzuweisen (Abs. 8). Der Bundesminister für Inneres hat mit Verordnung nähere Regelungen zum Verfahren und zu den Inhalten dieser Überprüfung festzulegen (Abs. 13 Z 2).

In diesem Zusammenhang wird seitens der Bundeskammer nochmals ausdrücklich darauf hingewiesen, dass unabhängige, staatlich befugte und beeidete Ziviltechniker:innen im Bereich Informationstechnologie auf dem von ihrer Befugnis umfassten Fachgebiet zur Erbringung von planenden, prüfenden, überwachenden, beratenden, koordinierenden usw. Leistungen, insbesondere zur Vornahme von Messungen und zur Erstellung von Gutachten berechtigt und mit öffentlichem Glauben versehene Personen sind (§ 3 ZTG). Öffentliche Urkunden, welche von Ziviltechniker:innen errichtet werden, begründen vollen Beweis dessen, was darin von der Behörde amtlich verfügt oder erklärt wird (§ 292 ZPO).

Der Verleihung der Ziviltechniker:innenbefugnis hat eine Hochschulausbildung (§ 5 ZTG), eine mindestens dreijährige praktische Betätigung (§ 6 ZTG) sowie die Ablegung der Ziviltechnikerprüfung (§ 7 ZTG) voranzugehen. Zudem sind Ziviltechniker:innen auf dem Fachgebiet ihrer Befugnis zur laufenden Berufsfortbildung verpflichtet, die mittels Fortbildungsverordnungen seitens der Bundeskammer sichergestellt wird (§ 12 Abs. 8 ZTG). Ziviltechniker:innen (-Gesellschaften), die auf dem Fachgebiet der Informationstechnologie tätig sind, verfügen daher grundsätzlich über die in § 7 vorgeschriebene Befähigung zur Zulassung als unabhängige Stellen bzw. unabhängige Prüfer:innen und wären somit schon kraft ihrer Funktion nach entsprechendem Antrag durch die Cybersicherheitsbehörde zuzulassen.

Jedenfalls ist aber sicherzustellen, dass die durch Verordnung des Bundesministers für Inneres festzulegenden Kriterien so ausgestaltet werden, dass Ziviltechniker:innen (-Gesellschaften) insgesamt keine Schlechterstellung zu den bislang geltenden Qualitätsanforderungen erfahren. Insbesondere im Hinblick auf § 51 Abs. 5, wonach Bescheide, die gemäß § 18 Abs. 1 NISG idF 2018 erlassen wurden, mit Inkrafttreten dieses Bundesgesetzes gegenstandslos werden, sofern die qualifizierte Stelle nicht einen Antrag gemäß § 7 Abs. 2 binnen sechs Monaten ab Inkrafttreten der zu erlassenden Verordnung stellt.

Gemäß Abs. 4 hat die Cybersicherheitsbehörde die Zulassung der unabhängigen Stelle bei Nichteinhaltung der Anforderungen zu widerrufen, außer es ist ein Fall von höherer

Gewalt, der außerhalb der Einflusssphäre der unabhängigen Stelle liegt, eingetreten. Nach rechtskräftigem Widerruf kann erst nach Ablauf eines Jahres ein neuerlicher Antrag auf Zulassung gestellt werden. Wenn diese „Sperrfrist" in den Erläuterungen dadurch erklärt wird, dass damit Missbrauch hintangehalten werden soll, ist aus unserer Sicht die „Sperrfrist" dezidiert auf begründete Missbrauchsfälle im Gesetzeswortlaut oder in den Erläuterungen zu beschränken. So würde es für die unabhängige Stelle nämlich einen unverhältnismäßigen Eingriff in ihre Geschäftstätigkeit bedeuten, wenn ihre Zulassung deshalb widerrufen wird, weil sie etwa (unverschuldet) durch Kündigung/längere Krankheit einer Mitarbeiterin oder eines Mitarbeiters die Mindestanzahl an unabhängigen Prüfer:innen unterschreitet. In diesen Fällen kann wohl kein Missbrauch erkannt werden. Vielmehr soll es der unabhängigen Stelle hier möglich sein, innerhalb einer angemessenen Frist eine/n neue/n Prüfer:in zu nennen, bevor es zu einem Widerruf der Zulassung kommt. Ebenso denkbar wäre eine Ruhendstellung der Zulassung, solange die Mindestanforderungen nicht erfüllt werden. Dies insbesondere auch im Hinblick darauf, dass dem Bescheid zum Widerruf der Zulassung keine aufschiebende Wirkung zukommt. Da dies nachteilige Auswirkungen auf wichtige Abläufe in der Prüfung von Einrichtungen haben kann, sollte die aufschiebende Wirkung beibehalten werden. So können auch allfällige Schäden, die durch einen Bescheid, der später aufgehoben oder abgeändert wird, minimiert werden.

Die in § 7 Abs. 3 vorgesehenen umfangreichen Aufsichtsmaßnahmen der Cybersicherheitsbehörde gemäß § 38 Abs. 1 sollen aus den unten dargelegten Gründen nicht zur Kontrolle der unabhängigen Stellen zur Anwendung gelangen. Stattdessen wird angeregt, die notwendigen Kontrollmaßnahmen auf ein unbedingt erforderliches Ausmaß zu reduzieren, die von einer unabhängigen Institution überprüft werden sollen.

Zu § 38:

Der Umfang der in § 38 definierten Aufsichtsmaßnahmen der Behörde ist, angesichts der potenziellen Eingriffsmöglichkeiten in sensible Unternehmensbereiche, zu unklar. Vor dem Hintergrund, dass die Behörde diese Maßnahme laut Abs. 1 in Wahrnehmung ihrer Aufsichtsaufgaben zur Einhaltung der Verpflichtungen nach dem NISG 2024 auch jederzeit („Ad-hoc-Prüfung" siehe § 38 Abs. 1 Z 5) ergreifen kann, fehlt es an einer klaren Präzisierung. So soll etwa klargestellt werden, dass sämtliche Kontrollmaßnahmen ausschließlich unter Mitwirkung der Einrichtung stattzufinden haben. Ebenso fehlt eine gesetzlich verankerte Interessenabwägung in Bezug auf die Erforderlichkeit, Verhältnismäßigkeit und mögliche alternative Maßnahmen. Daraus hat sich zu ergeben, dass eine behördliche Einschau bzw. ein Zugriff auf die Netz- und Informationssysteme nur innerhalb gesetzlicher Schranken, also insbesondere nur in Bezug auf konkrete sicherheits- bzw. prüfungsrelevante Teile und nur in einem unbedingt erforderlichen Ausmaß unter möglichster Schonung der Rechte der betroffenen Einrichtung und Dritter, gewährt werden muss.

Aus rechtsstaatlicher Sicht ist hier eine dringende Anpassung vorzunehmen, weil andernfalls im Anwendungsbereich dieses Gesetzes ein überschießender, umfassender Zugriff auf Systeme möglich wäre, der sonst nur den zuständigen (Strafverfolgungs-)Behörden mit richterlichem Beschluss vorbehalten ist. Ergänzend ist darauf hinzuweisen, dass ein direkter Zugriff auf die IT-Systeme in der Richtlinie nicht vorgesehen ist.

Zudem ist aus unserer Sicht eine dem Gesetzeszweck entsprechende Einschränkung der Aufsichts- und Kontrollrechte der gegenständlichen Behörde vorzunehmen. Der Bundesminister für Inneres als vorgesehene Cybersicherheitsbehörde unterliegt einer

politischen Verantwortung und ist nicht unabhängig, wie dies etwa bei der Datenschutzbehörde der Fall ist. Eine Ausgestaltung der Cybersicherheitsbehörde könnte derart erfolgen, dass diese als neue (unabhängige) Behörde eingerichtet wird oder die Befugnisse einer unabhängigen Behörde übertragen werden.

Zu § 39:
Unabhängige, staatlich befugte und beeidete Ziviltechniker:innen im Fachbereich der Informationstechnologie eignen sich besonders für die Rolle der „Überwachungsbeauftragten" in § 39 Abs. 3 Z 2. Also zur Überwachung der Anforderungen gemäß §§ 32 und 34, um die Umsetzung der mit Bescheid der Cybersicherheitsbehörde angeordneten Maßnahmen sicherzustellen. Die vorgesehenen Rechte des Überwachungsbeauftragten iSd § 3 Abs. 1 Z 37 sollten in dem Zusammenhang dagegen auf Auditrechte beschränkt werden, die nur gemeinsam mit dem/der Ziviltechniker:in und der Einrichtung ausgeübt werden können.

Abschließend wird darauf hingewiesen, dass Ziviltechniker:innen des einschlägigen Fachbereichs als unabhängige Fachexpertinnen und Fachexperten im Bereich der Informationstechnologie sowohl für Peer-Reviews als Sachverständige für Cybersicherheit (§ 23) als auch für die im Gesetzesentwurf vorgesehenen Stellen und Gremien (siehe § 3 Z 32 bis 36) beratend zur Verfügung stehen.

Die Bundeskammer bietet zudem gerne an, wie in der Vergangenheit bereits des Öfteren praktiziert, in weiterführenden Gesprächen zur erlassenden Verordnung hinsichtlich Qualitätssicherung von unabhängigen Stellen bzw. unabhängigen Prüfer:innen entsprechende fachliche Expertise einzubringen.

Mit bestem Dank für die Berücksichtigung der Stellungnahme und
freundlichen Grüßen

Architekt Dipl.-Ing. Daniel Fügenschuh
Präsident