Bundeskammer der
ZiviltechnikerInnen | 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, Abt I/6
Büro für strategische Netz- und
Informationssystemsicherheit
Ballhausplatz 2
1010 Wien

Per E-Mail: nis@bka.gv.at

cc: begutachtungsverfahren@parlament.gv.at

Wien, am 29.10.2018

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen, Netz- und Informationssystemsicherheitsgesetz (NISG)

Sehr geehrte Damen und Herren!

Die Bundeskammer der ZiviltechnikerInnen bedankt sich für die Übermittlung des Begutachtungsentwurfs und erlaubt sich, dazu folgende Stellungnahme abzugeben:

- ***Verschwiegenheitsverpflichtung:***

Die Bundeskammer der ZiviltechnikerInnen ist Mitglied des Vereins „Kuratorium Sicheres Österreich“ (KSÖ), welcher sich auch mit dem Schutz strategischer Infrastrukturen bis hin zur Bekämpfung internationaler Cyberkriminalität auseinandersetzt. Anlässlich des geplanten „Cybersicherheitsgesetzes“ ist der Verein mit Vertretern von Ministerien, Behörden, der Wirtschaft und Wissenschaft sowie Regulatoren und Interessensvertretungen in einen Rechts- und Technologiedialog getreten. Die Ergebnisse dieses Dialogs wurden in einem „Whitepaper“ zusammengefasst. Darin finden sich auch folgende Überlegungen zu rechtlichen Regelungen operativer Koordinierung sowie die Empfehlung Nr 17 zur Verschwiegenheitsverpflichtung bei Cybervorfällen (vgl. Punkt 3.6.1, S 31):

„Cybervorfälle sind für die betroffenen Unternehmen und Behörden nach wie vor heikle Vorgänge. Umso wichtiger ist es für alle Beteiligten, dass die erlangten und ausgetauschten Informationen mit großer Sorgfalt behandelt werden. Insbesondere in den Workshops wurde diskutiert, dass sich mit dem Cybersicherheitsgesetz die Möglichkeit bieten würde, Verschwiegenheits- und Vertraulichkeitsregelungen zu normieren, so dass im Ereignisfall keine gesonderten Vereinbarungen getroffen werden müssen. In der Praxis gibt es dazu mit der Verschwiegenheitspflicht der Ziviltechniker bereits einen Ansatz, der analog angewandt werden könnte.

Empfehlung 17:
Analog zu §15 des Ziviltechnikergesetzes sollte das Cybersicherheitsgesetz eine generelle Regelung zur Verschwiegenheit bzw. Vertraulichkeit beinhalten. Auf welchen Personenkreis sich diese Regelung bezieht, sollte mit den Betreibern kritischer Infrastrukturen und den zuständigen Behörden erörtert und im Cybersicherheitsgesetz festgelegt werden."

Basierend auf dieser Empfehlung schlägt die Bundeskammer ergänzend folgenden § 13a vor:

§ 13a.
„Soweit einzelne Materiengesetze nicht ohnedies besondere Verpflichtungen zur Verschwiegenheit vorsehen, trifft alle an der Abwicklung eines Sicherheitsvorfalls Beteiligten die Verpflichtung zur Verschwiegenheit."

- ***Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste (§ 15):***

In Umsetzung des Art. 14 Abs. 1 NIS-RL wird den Betreibern wesentlicher Dienste vorgeschrieben, geeignete, dem Stand der Technik entsprechende Sicherheitsvorkehrungen zu treffen. Diese können sowohl technischer als auch organisatorischer Art sein und sollen in Hinblick auf die betriebenen wesentlichen Dienste dazu dienen, die Netz- und Informationssystemsicherheit (NIS) zu gewährleisten (§ 15 Abs. 1).

Die NIS-RL sieht vor, dass die Einhaltung der Sicherheitsvorkehrungen periodisch zu überprüfen ist. Dafür haben die Betreiber dem Bundesminister für Inneres die Erfüllung der Anforderungen mindestens alle drei Jahre in geeigneter Weise nachzuweisen (§ 15 Abs. 3). Hiefür kann eine Aufstellung der vorhandenen Sicherheitsvorkehrungen sowie ein Nachweis von Zertifizierungen oder durchgeführten Überprüfungen durch qualifizierte Stellen erbracht werden.

Welche Erfordernisse eine qualifizierte Stelle erfüllen muss, soll in einer im Einvernehmen mit dem Bundeskanzler erlassenen Verordnung des Bundesministers für Inneres festgelegt werden. Liegen besondere Kriterien vor, können bestimmte Stellen jedenfalls als qualifiziert angesehen werden (§ 15 Abs. 4).

Staatlich befugte und beeidete ***ZiviltechnikerInnen***, insbesondere ***aus dem Fachbereich der Informationstechnologie*** sind geradezu prädestiniert, die Überprüfung der bei den Betreibern wesentlicher Dienste vorzusehenden Sicherheitsvorkehrungen vorzunehmen. Als mit öffentlichem Glauben versehene, unabhängig tätige Personen sind ZiviltechnikerInnen in ihrem Fachgebiet vor allem zur Erbringung prüfender, überwachender, beratender, koordinierender Leistungen und zur Erstellung von Gutachten berechtigt (§ 4 ZTG). Aus dem Berufsgesetz der ZiviltechnikerInnen ergibt sich daher bereits das Vorliegen einer qualifizierten Stelle.

Die Bundeskammer regt daher an, ZiviltechnikerInnen aufgrund ihrer Qualifikation bereits von Gesetzes wegen jedenfalls als qualifizierte Stellen iSd § 15 Abs. 3 und Abs. 4 NISG anzusehen und schlägt dazu folgende Änderung des § 15 Abs 3. NISG vor:

„§ 15 [...]
(3) [...] Zu diesen Zwecken übermitteln die Betreiber wesentlicher Dienste eine Aufstellung der vorhandenen Sicherheitsvorkehrungen durch den Nachweis von

*Zertifizierungen oder durchgeführten Überprüfungen qualifizierter Stellen, **wzB ZiviltechnikerInnen**, (Abs. 4.), einschließlich der dabei aufgedeckten Sachmängel. […]"*

Jedenfalls sollte ein Hinweis in den Erläuterungen zu § 15 Abs. 3 und Abs. 4 NISG auf ZiviltechnikerInnen als bereits von Gesetzes wegen (§§ 1ff ZTG) zur Überprüfung berechtigte qualifizierte Stellen vorgesehen werden.

- ***Dem Stand der Technik entsprechende Sicherheitsvorkehrungen (§§ 15, 19):***

Die Betreiber wesentlicher Dienste sowie die Einrichtungen des Bundes haben in Hinblick auf die von ihnen betriebenen Dienste geeignete, dem ***Stand der Technik*** entsprechende Sicherheitsvorkehrungen zur Gewährleistung der NIS zu treffen (§ 15 Abs. 1 bzw. § 19 Abs. 1 NISG).

Da die technische Entwicklung schneller als die Gesetzgebung ist, hat es sich in vielen Rechtsbereichen bewährt, den juristischen Begriff „Stand der Technik" zu verwenden. Selbstverständlich können die notwendigen technischen Maßnahmen je nach konkreter Fallgestaltung unterschiedlich sein, sodass es nicht möglich ist, den Stand der Technik abschließend zu beschreiben. Dementsprechend fehlt es auch dem vorliegenden Gesetzesentwurf an einer abschließenden Begriffsdefinition. Aus Gründen der Rechtssicherheit erscheint es jedoch in hohem Maß sinnvoll, gewisse Grundlagen festzulegen. Angelehnt an die Gesetzesbegründung zum deutschen IT-Sicherheitsgesetz (Ad § 8a BSIK) bzw. an die Vorgaben der ISO 27001 sollte in den Erläuterungen zu §§ 15 und 19 NISG daher zumindest Folgendes festgehalten werden:

"Auf Grund der weitreichenden gesellschaftlichen Auswirkungen ist bei den technischen und organisatorischen Vorkehrungen der Stand der Technik zu berücksichtigen. Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Die Verpflichtung zur Berücksichtigung des Standes der Technik schließt die Möglichkeit zum Einsatz solcher Vorkehrungen nicht aus, die einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten."

Mit freundlichen Grüßen

BR h.c. Dipl.-Ing. Rudolf Kolbe
Präsident