Sehr geehrte Damen und Herren,

Ich[1] komme mit diesem Schreiben der Möglichkeit zur Stellungnahme zum Entwurf des NISG gerne wie folgt nach:

Ich sehe den verfolgten Ansatz (Überprüfung durch qualifizierte Stellen) als *möglicherweise* wirksamen Weg, die Versorgungssicherheit zu erhöhen. Der aus meiner Sicht derzeit angestrebte Weg, die Überprüfung durch externe Stellen (vgl. §15 (3)) durchzuführen verstehe ich und er zeigt sich auf den ersten Blick als plausibler Weg, allerdings aus meiner Sicht langfristig nicht – oder nur durch Zufall – zielführend und für die Betreiber nicht wirtschaftlich und wirksam und auch für die Behörde bestehen Optimierungspotentiale.

Der Ansatz, die Erreichung der Versorgungssicherheit über externe Prüfungen zu erhöhen ist durchaus ein möglicher Weg, um die Richtlinie umzusetzen. Allerdings schwingen hier zwei Nebenbedingungen mit, die für die Zielerreichung schädlich sein können:

- Zum einen ist natürlich der Prüfungs*markt* ein solcher und die Qualität der Prüfungen (hinsichtlich Zielgerichtetheit der Prüfungshandlungen, Fachkunde und Branchenkenntnis der Prüfer, Unabhängigkeit und somit Objektivität der Prüfer und auch deren Haftung) ist abstrakt nicht oder nur schwer [2] stabil und im Sinne des Auftrags der Versorgungssicherheit umzusetzen. Ich denke, hier ginge viel Energie und Aufwand in eine nicht zielorientierte Richtung und somit auf Kosten der Betreiber verloren. Neben den Aufwänden für die Betreiber aus meiner Sicht auch auf der Seite der zuständigen Behörde durch Akkreditierung und damit verbundene Tätigkeiten, die für die eigentliche Aufgabe der Versorgungssicherheit nicht mehr zur Verfügung stehen.
- Zum anderen führt die Verantwortung der Organisationen, sich einem externen Audit zu unterziehen bei den Betroffenen Personen fast reflexartig zu einer formalen Compliance mit keiner oder geringer nachhaltigen Auswirkung auf die Unternehmenskultur, die es ja langfristig zu verändern gilt. Die Audits führen aus meiner Erfahrung zu Qualitätsspitzen zum Zeitraum der Audit-Vorbereitung und durchaus auch zu einem hohen Bewusstsein im Audit- (oder Compliance-) Team und den direkt vom Audit betroffenen; nicht aber unbedingt, bzw. nur mit hohem Aufwand, zu einer Änderung der Unternehmenskultur aber tendenziell auch zu einer Abwehrhaltung, gerade in technischen Bereichen und bei den betroffenen Experten.

Mein Vorschlag geht in eine andere Richtung, die eben die beiden angeführten Themen nicht schlagend werden lassen. Sie sind auch für die Betreiber und für die Behörden mit weniger Aufwand verbunden und unterstützen die Erreichung der gesetzten Evaluierungsziele[3] besser.

Organisationen mit der Prägung von Expertokratien – insbesonders im technischen Umfeld – und auch öffentlichkeitsnahe Organisationen verfügen tendenziell über eine positiv ausgeprägte Führungskultur. Vorgaben vom Vorstand werden eher Umgesetzt, als Vorgaben aus der Linie oder Empfehlungen von Stabsstellen. Die etablierte Governance-Struktur ist ein wirksames Instrument zur Steuerung, dessen Potential auch im Sinne der Richtlinie genutzt werden sollte und genau hier würde ich ansetzen. Aus meiner Sicht ist die wirksamste Methode, die Unternehmen zu steuern, sich ihrer etablierten Steuerungseinheiten, also Vorstand und Aufsichtsrat, zu bedienen. Dies zeigte sich etwa auch im Rahmen des URÄG 2008, wo die Verantwortung für die Überwachung der Rechnungslegung in einen Ausschuss des Aufsichtsrats übertragen wurde (vgl. §92(4a) AktG). Diese haben Wirkung gezeigt und sind nach wie vor ein wirksames Mittel, den Jahresabschluss und die damit verbundenen Maßnahmen in den Unternehmen nachhaltig sicher zu stellen. Dies erfordert neben der Nennung einer Kontaktstelle aus dem Unternehmen aus meiner Sicht auch die Nominierung eines zuständigen Vorstandsmitglieds, das für die Umsetzung verantwortlich zeichnet und zusätzlich zumindest ein Mitglied des Aufsichtsrats, das fachlich in der Lage ist, die Wirksamkeit der Maßnahmen beurteilen zu können. Die Beurteilungsergebnisse könnten auch im Lagebericht der

Gesellschaft veröffentlicht werden, was auch die Transparenz weiter erhöhen würde, wie dies für das IKS und Risikomanagement für die Rechnungslegung etwa in §243a(2) UGB vorgesehen ist.

Aus meiner Sicht ist dies eine kurz- und langfristig wirksame Maßnahme. Sie bedingt aber auch, dass der Aufsichtsrat, respektive zumindest ein Mitglied, über entsprechende Fachkenntnis verfügt. Diese sollte dann auch durch die einschlägigen Zertifizierungen (CISA, Ziviltechniker, Sachverständige) nachgewiesen werden, detailliertere Anforderungen sollten entfallen. Aufwändige Akkreditierungsverfahren und deren inhärente Schwächen [4] und die damit verbundenen Aufwände würden entfallen. Die Kern-Aufgabe des verantwortlichen Aufsichtsratsmitglieds bestünde darin, die Existenz und Wirksamkeit der Maßnahmen zur Sicherstellung der kontinuierlichen Versorgung zu beurteilen; externe Experten können, müssen aber nicht bei Bedarf beigezogen werden. Ebenso ist der Umsetzungsfortschritt von Verbesserungsmaßnahmen vom Vorstand zu verantworten und den zuständigen Aufsichtsrat zu überwachen (z.B. iRd §94 AkgG).
Damit wäre auch ein entsprechendes und für die MitarbeiterInnen der Unternehmen ein „Alpha“ vorhanden und die Umsetzung der Maßnahmen sowie allfällige Verbesserungen würden nicht nur „Compliant“ – also ein Erreichen von für den Prüfer gerade noch akzeptablen Mindeststandards – sondern im Sinne des Unternehmens und dessen Versorgungsauftrags identifiziert, verwirklicht, betrieben und - wo notwendig - im Eigeninteresse verbessert und angepasst werden.
Die Behörde hätte auch einen verantwortlichen und kompetenten Ansprechpartner, um die Angemessenheit der Maßnahmen und Fortschritte bei Verbesserungen beurteilen zu können und zusätzlich besteht natürlich auch die Möglichkeit, entsprechend verantwortliche Personen in die Haftung zu nehmen. Auch hier ist aus meiner Sicht eine persönliche Verantwortung und somit Haftung ein wirksamer Ansatz, das angestrebte Ziel zur Verbesserung der Versorgungssicherheit zu erreichen.

Mit besten Grüßen
Mag. Jimmy Heschl

[1] Ich, Mag. Jimmy Heschl, geb. 2. 1. 1972, bin seit fast 25 Jahren in der IT beschäftigt, allgemein beeideter und gerichtlich zertifizierter Sachverständiger für das Fachgebiet Informationstechnologie, Lektor an der FH Salzburg und am Technikum Wien und bin seit vielen Jahren als IT-Prüfer, Berater und als Sicherheitsverantwortlicher tätig.
[2] vgl. dazu auch die Ansätze, die Wirtschaftsprüfung, ein sehr etablierter Zweig und dessen reife qualitätssichernde Maßnahmen, die zu hohen Aufwänden führen, die aber auf Basis konkreter nationaler und internationaler Rechnungslegungs- und Steuervorschriften ertsellt und über viele Jahre verbessert wurden)
[3] „Betreiber wesentlicher Dienste, Anbieter digitaler Dienste und Einrichtungen des Bundes treffen organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Netz- und Informationssysteme. Bei Vorliegen eines Sicherheitsvorfalls erstatten die genannten Einrichtungen unverzüglich Meldung an das jeweils zuständige Computer-Notfallteam, welches die Meldungen an die Behörden weiterleitet.“ Sowie „Neue Koordinierungsstrukturen schaffen einen geeigneten Rahmen um angemessen auf Sicherheitsvorfälle zu reagieren. Dabei werden Meldungen über Sicherheitsvorfälle und aktuelle Bedrohungslagen gesamtstaatlich analysiert und regelmäßig Lagebilder erstellt. Ein nationales Computer-Notfallteam unterstützt die Betreiber wesentlicher Dienste sowie die Anbieter digitaler Dienste bei der Prävention, Erkennung, Reaktion und Folgenminderung von Sicherheitsvorfällen im Bereich von Netz- und Informationssystemen. Sektorenspezifische Computer-Notfallteams sind eingerichtet.“
[4] z.B.: Wer muss in einem prüfenden Unternehmen über die nachgewiesene Sachkenntnis verfügen? Ein zweitweise eingesetzter Mitarbeiter ist hier bei Einsatz eines Prüfungsteams sicherlich zu wenig. Welchen Anteil der Prüfung muss die jeweilige Expertin selbst durchführen und welcher Anteil kann über Hilfsgutachter erbracht werden? Was passiert bei Abwesenheit, Kündigung etc.