

Kurzanalyse der Regierungsvorlage

NIS-2-Umsetzungsgesetzes (NIS2026)

Gegenstand

Die folgende Analyse des aktualisierten Entwurfs der Regierung zur Umsetzung der NIS2-Richtlinie¹ fokussiert auf die größten Kritikpunkte und gibt Empfehlungen für dringend notwendige Anpassungen.

Wir halten die rasche Umsetzung der NIS-2-Richtlinie für absolut notwendig. Diese hätte bereits deutlich früher erfolgen müssen, und das Versäumnis ist sowohl der aktuellen als auch der vorherigen Bundesregierung anzulasten. Eine frühzeitige und breite Einbindung relevanter Stakeholder wäre unerlässlich gewesen, um die komplexen Anforderungen der Cybersicherheit angemessen zu adressieren. Umso bedauerlicher ist es, dass die entstandene Verzögerung nicht genutzt wurde, um substantielle Verbesserungen zu erarbeiten. Statt einen offenen und transparenten Diskussionsprozess zu führen, wird dieses zentrale Gesetzesvorhaben nun in kurzer Zeit und ohne ausreichende öffentliche Debatte vorangetrieben. Dies stellt einen demokratiepolitischen Mischstand dar und schwächt das Vertrauen in den Gesetzgebungsprozess.

ZENTRALE ANALYSEPUNKTE

1.) Cybersicherheitsbehörde

Fehlende Unabhängigkeit der Behörde

Grundsätzlich begrüßen wir, dass im neuen Entwurf die Einrichtung einer eigenen Cybersicherheitsbehörde vorgesehen ist und die im abgelehnten Vorschlag aus dem Vorjahr enthaltene Konstruktion, wonach der Bundesminister für Inneres selbst diese Aufgaben wahrnehmen sollte, nicht weiterverfolgt wurde. Damit wird ein erster Schritt gesetzt, um die notwendige institutionelle Trennung zwischen operativer Cybersicherheitsarbeit und politischer Steuerung herzustellen.

Allerdings weist die gewählte Konstruktion weiterhin einen massiven strukturellen Mangel auf. Die neu zu errichtende Cybersicherheitsbehörde unterliegt vollumfänglich den Weisungen des Bundesministers für Inneres. Dadurch bleibt der inhärente Zielkonflikt zwischen dem Schutz staatlicher Sicherheitsinteressen und einer unabhängigen, fachlich getriebenen IT-Sicherheitsarbeit bestehen. Wir empfehlen daher dringend, die Cybersicherheitsbehörde analog zu anderen österreichischen Behörden mit besonders sensiblen Fachagenden wie der Datenschutzbehörde oder der RTR mit einem höheren Maß an politischer Unabhängigkeit auszustatten. Eine solche Unabhängigkeit würde nicht nur die Glaubwürdigkeit und Effektivität der Behörde stärken, sondern auch ihre Attraktivität erhöhen, um die dringend benötigten IT-Fachkräfte langfristig zu gewinnen und zu halten. Ähnliche Diskussionen werden auch im Ausland geführt, so empfiehlt etwa auch die Präsidentin des deutschen BSI klar eine unabhängige Positionierung ihrer Behörde².

¹ <https://www.parlament.gv.at/gegenstand/XXVIII/I/308>

² <https://www.bundestag.de/resource/blob/1027138/20-4-523-C.pdf>

Bestellung der Behördenleitung

Die Bestellung der Behördenleitung soll durch den Bundesminister für Inneres erfolgen. Zwar ist vorgesehen, dass die Begutachtungskommission neben einer Vertretung des BMI auch eine Person aus dem für Telekommunikation zuständigen Ministerium umfasst. Wir möchten jedoch zu bedenken geben, dass Cybersicherheit mehrere Fachressorts betrifft und nicht auf diese beiden Bereiche beschränkt ist. Zur Stärkung der Unabhängigkeit und zur Berücksichtigung der erforderlichen fachlichen Breite empfehlen wir daher, bereits bei der Benennung der Behördenleitung ein Einvernehmen mit weiteren betroffenen Ressorts herzustellen, insbesondere mit dem Infrastrukturministerium sowie dem Verteidigungsministerium, und diese Ressorts entsprechend einzubeziehen.

Fehlende Kontrolle bei der Ernennung des nationalen CSIRT

Die Cybersicherheitsbehörde hat gemäß § 9 NISG im Entwurf die Befugnis, eigenständig eine Einrichtung mit der Wahrnehmung der Aufgaben des nationalen CSIRT zu betrauen. Das nationale CSIRT ist jedoch eine zentrale sicherheitskritische Institution mit weitreichenden Einsichts- und Interventionsrechten. Angesichts dieser enormen Relevanz halten wir es für höchst problematisch, dass eine derart gewichtige Entscheidung ohne jede nachgelagerte Kontrolle oder Mitwirkung weiterer sicherheitspolitisch verantwortlicher Stellen getroffen werden kann. Wir schlagen daher vor, die Ermächtigung, ebenso wie den möglichen Widerruf gemäß § 10 Abs 7, dem „Inneren Kreis der operativen Koordinierungsstruktur“ (IKDOK) zu übertragen. Dieser umfasst Vertreter des Bundeskanzlers, des Innenministeriums, des Verteidigungsministeriums, des Außenministeriums sowie der Cybersicherheitsbehörde und bietet damit einen deutlich besser legitimierten und fachlich breiter abgestützten Rahmen für derartige Entscheidungen.

Fehlende Kompetenzbündelung

Weiterhin erachten wir es als verfehlt, die Kompetenz zur Verhängung von Verwaltungsstrafen bei den Bezirksverwaltungsbehörden anzusiedeln. Es ist nicht nachvollziehbar, warum hier eine Trennung zwischen materienzuständiger Fachbehörde und Strafbehörde vorgenommen wird, zumal es sich um ein hochspezialisiertes Gebiet handelt, dessen technische und organisatorische Komplexität von den 79 Bezirkshauptmannschaften und 15 Magistraten kaum abgedeckt werden kann. Selbst bei erfolgreicher Rekrutierung entsprechender Fachkräfte wäre dies aufgrund des Lohnniveaus im IT-Bereich außerordentlich kostenintensiv. Wir empfehlen daher, die Strafkompetenz bei jener Behörde zu verorten, die auch mit der übrigen Materie betraut ist.

2.) Aufsichtsrechte & Meldung von Schwachstellen

Zumindest für die Meldung von Schwachstellen braucht es zwingend Weisungsfreiheit und klare Grenzen bei der Weitergabe von Informationen. Die aktuellen Aufsichtsrechte der Cybersicherheitsbehörde über das nationale Computer Security Incident Response Team (CSIRT) sind hierfür zu weit gefasst. Nur durch eine organisatorisch abgesicherte Unabhängigkeit kann gewährleistet werden, dass das CSIRT seine Aufgaben frei von politischen Einflussnahmen erfüllt und Meldungen nicht über interne Weisungsketten letztlich beim Ministerium landen. Da betroffene Einrichtungen nur dann Schwachstellen vollständig und zeitnah melden, wenn sie dem Verfahren vertrauen, ist eine solche unabhängige Struktur unverzichtbar.

3.) Einbindung von Zivilgesellschaft und Wissenschaft

Der Entwurf bleibt zudem hinsichtlich der strukturellen Einbindung externer Expertise weit hinter den Anforderungen zurück. Die komplexen Herausforderungen der IT-Sicherheit können von der Verwaltung allein nicht bewältigt werden. Nur durch eine systematische Einbindung von Forschung, Wirtschaft und Zivilgesellschaft kann das notwendige Resilienz- und Kompetenzniveau erreicht werden, um modernen Bedrohungen auf Augenhöhe zu begegnen. Italien zeigt mit seinem technisch wissenschaftlichen Beirat³, wie externe Fachleute dauerhaft und strukturiert in die nationale Cybersicherheitsstrategie eingebunden werden können. Ein vergleichbares Modell wäre auch für Österreich dringend geboten.

4.) Absicherung von Sicherheitsforschung: Notwendige Reform des § 118a StGB

Problematisch ist, dass der Entwurf den § 118a StGB (Hackingparagraph) weiterhin unverändert lässt. Damit fehlt nach wie vor ein sicherer Rechtsrahmen für Sicherheitsforscherinnen und Sicherheitsforscher, die Schwachstellen melden wollen. Genau dies war jedoch ein zentrales Ziel der NIS-2-Richtlinie. Ohne eine klare rechtliche Absicherung bleibt verantwortungsvolle Sicherheitsforschung in Österreich mit erheblichen Risiken verbunden, was die Bereitschaft zur Meldung von Sicherheitslücken und damit die gesamte Cybersicherheitsarchitektur schwächt.

5.) Weitreichende Datenverarbeitungen und Übermittlungsbefugnisse

Bereits im früheren Entwurf, der von SPÖ⁴ und NEOS⁵ unter anderem aufgrund datenschutzrechtlicher Bedenken abgelehnt wurde, waren weitreichende Datenverarbeitungs- und Übermittlungsbefugnisse vorgesehen. Trotz dieser Kritikpunkte enthält der aktuelle Entwurf diesbezüglich keine wesentlichen Verbesserungen.

Besondere Sorgen bereitet § 17, der das BMI zum Betrieb von IKT-Lösungen zur Früherkennung von Cyberbedrohungen verpflichtet. Obwohl die Teilnahme für wesentliche Einrichtungen formal freiwillig ist, ist angesichts der angespannten IT-Sicherheitslage davon auszugehen, dass viele Unternehmen teilnehmen werden. Dadurch entsteht faktisch ein umfangreicher Datenzugriff des Ministeriums. § 42 erweitert den Zweck der Datenverarbeitungen im Kontext des Gesetzes auf den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit, was eine weit gefasste und potenziell missbrauchsanfällige Auslegung erlaubt. § 43 schafft darüber hinaus unpräzise definierte Möglichkeiten der Übermittlung personenbezogener Daten an andere inländische und ausländische Behörden oder Stellen. Insgesamt besteht somit die Gefahr eines unverhältnismäßig breiten staatlichen Zugriffs auf sensible Daten.

Die nun in § 42 Abs 11 neu vorgesehene Bestimmung, dass der zuständige Datenschutzbeauftragte halbjährlich einen zusammenfassenden Bericht über die Datenverarbeitungen auf der Homepage des Bundesministeriums für Inneres zu veröffentlichen hat, mag unsere diesbezüglichen Bedenken nicht zu verstreuen.

3 <https://www.acn.gov.it/portale/en/comitato-tecnico-scientifico>

4 https://www.ots.at/presseaussendung/OTS_20240704_OTS0053/spoe-einwallnerkucharowits-fuer-sicherheit-ohne-anlasslose-massenueberwachung

5 <https://futurezone.at/netzpolitik/nis-2-gesetz-entwurf-abgelehnt-cybersecurity-sicherheit-nationalrat-kritik-opposition/402921577>

SCHLUSSBEMERKUNGEN

Weiters verweisen wir auf unsere umfangreiche Stellungnahme im Rahmen der Begutachtung⁶, der Rede unseres Experten Mag. Sebastian Kneidinger im Innenausschuss⁷ und unserem Forderungspapier im Rahmen der Koalitionsverhandlungen⁸.

6 <https://epicenter.works/content/stellungnahme-zum-nis-gesetz-2024>

7 <https://epicenter.works/content/hearing-im-innenausschuss-it-sicherheitsgesetz-nis2>

8 <https://epicenter.works/content/forderungspapier-nis2>